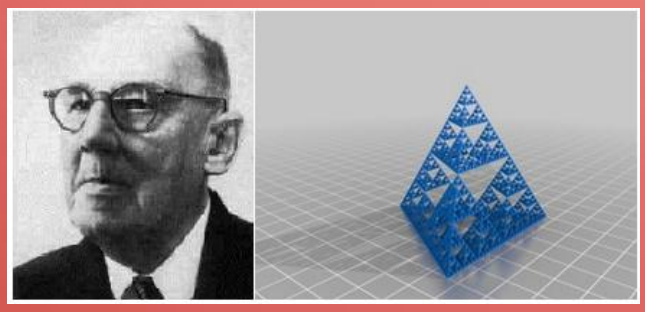
TỦ SÁCH TOÁN HỌC TRẺ THẾ KỶ 21

001



LÝ THUYẾT SƠ CẤP CỦA CÁC SỐ

TÁC GIẢ: W. SIERPINSKI

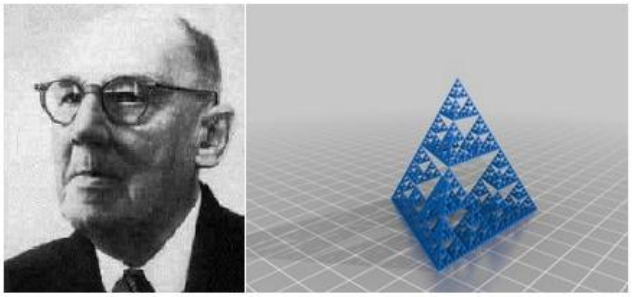
Biên tập: A. Schinzel

Khánh Nguyễn *dịch từ bản in lần hai năm 1988 cuốn* ***Elementary theory of numbers*** *của* **Sierpinski**. *Bản thảo hoàn thành lần thứ nhất tháng 10/2012 tại Sài Gòn Chợ Lớn. In thử nghiệm 300 cuốn trên giấy thường theo bản chỉnh sửa tháng 12/2012. Ngoài ra có in thêm 30 bản trên giấy trắng. In xong tháng 1/2013. Bản dịch (mang mã số 001) thuộc chương trình xây dựng tủ sách toán học trẻ thế kỷ 21 chủ trương bởi* **{K@}** *và do dịch giả nắm bản quyền*

LƯU HÀNH NỘI BỘ

TỦ SÁCH TOÁN HỌC TRẺ THẾ KỶ 21

001



LÝ THUYẾT SƠ CẤP CỦA CÁC SỐ

TÁC GIẢ: W. SIERPINSKI

Biên tập: A. Schinzel

Khánh Nguyễn *dịch từ bản in lần hai năm 1988 cuốn* ***Elementary theory of numbers*** *của* **Sierpinski***. Bản thảo hoàn thành lần thứ nhất tháng 10/2012 tại Sài Gòn Chợ Lớn. In thử nghiệm 300 cuốn trên giấy thường theo bản chỉnh sửa tháng 12/2012. Ngoài ra có in thêm 30 bản trên giấy trắng. In xong tháng 1/2013. Bản dịch (mang mã số 001) thuộc chương trình xây dựng tủ sách toán học trẻ thế kỷ 21 chủ trương bởi* **{K@}** *và do dịch giả nắm bản quyền*

LƯU HÀNH NỘI BỘ

Lý thuyết sơ cấp của các số có lẽ là một trong những chủ đề tốt nhất để xây dựng những hiểu biết toán học đầu tiên. Nó yêu cầu rất ít các kiến thức mở đầu và các chủ đề của nó là rất quen thuộc và rõ ràng. Các lập luận được sử dụng cũng rất đơn giản và không quá nhiều. Hơn nữa nó là chủ đề duy nhất trong toán học được hình thành một cách tự nhiên bởi sự tò mò của con người. - ***G.H.Hardy***

LỜI GIỚI THIỆU CỦA TÁC GIẢ

Waclaw Sierpinski

Ngày nay các nhánh mới phát triển trong toán học thường được đặt tên theo những cách gọi truyền thống đã trở nên quen thuộc trước đó. Tuy nhiên những tên gọi như vậy nhiều khi không thực sự cho biết một cách chính xác sự phát triển cũng như các chủ đề mà nó đề cập tới. Điều này cũng xảy ra với lý thuyết của các số. Lý thuyết của các số (cùng với những sự liên hệ với các ngành khoa học khác của nó) là một lĩnh vực chứa đựng những chủ đề và phương pháp có vị trí đặc biệt trong rất nhiều nhánh toán học khác nhau.

Tên gọi ***Lý thuyết của các số*** phù hợp với một lý thuyết đại cương nghiên cứu về các số và các dạng mở rộng của nó. Chẳng hạn bắt đầu từ số nguyên, ta có các số hữu tỷ, số thực và số phức. Từ các loại số khác nhau ta xây dựng những phép toán ***(các toán tử)*** trên các số đó. Tuy nhiên đây đúng ra là ***Số học cao cấp.*** Nguyên nhân là vì Lý thuyết của các số thường chỉ liên quan tới tính chất của các số nguyên trong khi Số học cao cấp sử dụng tới cả các ***lý thuyết đại số về các toán tử***. Tất nhiên lý thuyết của các số sẽ không chỉ xoay quanh các số nguyên vì trên thực tế có rất nhiều tính chất của các số nguyên được phát hiện và chứng minh dựa trên sự tìm hiểu các số vô tỷ và các số phức. Hơn nữa đã có rất nhiều các định lý về các số nguyên có thể được chứng minh theo cách đơn giản nếu ta không chỉ sử dụng các số vô tỷ và các số phức mà còn sử dụng tới giải tích và ***lý thuyết về các hàm***. Lý thuyết của các số với sự kết hợp với một số chủ đề của giải tích hình thành nên bộ môn ***Số học giải tích***. Bộ môn này có sự khác biệt với ***Lý thuyết sơ cấp của các số*** ở điểm căn bản là nó sử dụng tới ***khái niệm giới hạn***. Tuy vậy mặc dù chủ đề chính của cuốn sách này là Lý thuyết sơ cấp của các số nhưng vẫn sẽ có một số ứng dụng của Số học giải tích được xét tới.

Cuốn sách được xây dựng dựa trên hai cuốn sách khác của tôi trong những năm 1914 và 1959 là

1. ***Teoria Liczb (Lý thuyết các số), Ấn bản lần thứ nhất, Warszawa 1914; ấn bản lần thứ hai, Warszawa 1925; ấn bản lần thứ ba, Warszawa-Wroclaw 1950 (544 trang)***
2. ***Teoria Liczb, Phần II, Warszawa 1959 (487 trang).***

Để minh họa cho sự phát triển Lý thuyết của các số trong một thập kỷ vừa qua chỉ cần nhắc lại rằng số nguyên tố lớn nhất được tìm ra vào năm 1950 là số $2^{127}-1$ (số này có 39 chữ số) trong khi ngày nay số nguyên tố lớn nhất đã tìm được là số $2^{11213}-1$ (số này có 8376 chữ số). Vào năm 1950 ta mới chỉ biết 12 số hoàn hảo trong khi ngày nay ta đã tìm được 23 số như thế.

Trong cuốn sách này tôi sẽ trình bày rất nhiều kết quả đặc biệt của Lý thuyết sơ cấp của các số đã được công bố trong những năm gần đây bởi các nhà toán học tới từ rất nhiều quốc gia khác nhau.

Tiến sỹ ***A.Hulanicki*** là người đã dịch bản thảo cuốn sách sang tiếng Anh. Tiến sỹ ***A.Schinzel*** là người đã chuẩn bị phụ lục và thêm vào rất nhiều đề nghị và ghi chú liên quan tới các kết quả được công bố gần đây. Tiến sỹ ***A.Makowski*** là người đọc các chứng minh. Tôi đặc biệt cảm ơn các đồng nghiệp nói trên. Tôi cũng cảm ơn Biên tập viên ***L.Izertowa*** tới từ Nhà xuất bản khoa học Ba Lan, người đã chuẩn bị rất nhiều cho bản in của cuốn sách này.

Ba Lan
1963

LỜI NÓI ĐẦU CỦA NGƯỜI BIÊN TẬP CHO BẢN IN LẦN THỨ HAI

Andrzej Schinzel

Trong quá trình biên tập cuốn sách ***"Elementary theory of numbers"*** của ***Sierpinski*** để chuẩn bị cho lần in thứ hai, tôi ***(Schinzel)*** đã giữ nguyên các chủ để và thứ tự trình bày mà tác giả đã lựa chọn. Trong khoảng 20 năm kể từ khi bản in lần đầu ra đời thì đã có rất nhiều công trình nghiên cứu mới đã được thực hiện. Các công trình đó đã cho nhiều câu trả lời cho các câu hỏi được đặt ra trong bản in lần thứ nhất. Vì vậy tôi cho rằng nhiệm vụ của mình là bổ sung và hoàn chỉnh lại một số mục và làm đầy đủ hơn các trích dẫn, đồng thời sửa lại một số lỗi sai.

Để thực hiện công việc này tôi đã nhận được sự hỗ trợ của các đồng nghiệp ***Jerzy Browkin*** và ***Andrzej Makowski***. Tôi cảm ơn sự cộng tác của họ. Tôi cũng nhận được những gợi ý về những sự chỉnh sửa từ các nhà toán học khác là các Giáo sư ***John Brillhart***, ***Eckford Cohen***, Tiến sỹ ***Waldemar Gorzkowski***, các Giáo sư ***Erich Michalup***, ***M.V.Subbarao***, ***Antoni Wakulicz*** và Giáo sư ***Gregory Wulczyn***. Biên tập viên ***Krystyna Regulska*** tới từ Nhà xuất bản khoa học Ba Lan đã kiểm tra các yếu tố kĩ thuật của bản thảo, trong đó có bảng tra cứu danh sách các nhà toán học đã được trích dẫn.

Ba Lan
Tháng 2 năm 1985

LỜI GIỚI THIỆU CỦA NGƯỜI DỊCH

Khánh Nguyễn

Tôi còn nhớ những ngày học đầu tiên thời cấp 2 khi bắt đầu tìm hiểu về phương trình nghiệm nguyên thì một ai đó đã đố tôi cùng các bạn học giải phương trình $x^n + y^n = z^n$ với $n > 2$ và nói rằng người nào giải được sẽ được coi là ***một nhà toán học thực thụ***. Sự đơn giản của phương trình và danh hiệu nhà toán học thực thụ khiến chúng tôi cảm thấy vô cùng hào hứng. Chúng tôi trên thực tế đã sử dụng rất nhiều giấy nháp và nhiều buổi tính toán triền miên mà không dẫn tới kết quả. Sự hào hứng ban đầu đã nhanh chóng chuyển thành sự thất vọng nặng nề. Tình trạng này còn trở nên tệ hơn khi chúng tôi thậm chí còn không giải quyết được trường hợp riêng khi $n = 3$. Trong trường hợp đó dựa vào phân tích quen thuộc $x^3 + y^3 = (x+y)(x^2 - xy + y^2) = z^3$ có thể suy ra mỗi nhân tử trong biểu thức ở giữa đều là lũy thừa bậc ba với các điều kiện bổ sung và chúng tôi cảm giác mình đã có thể xây dựng được một nghiệm mới nhỏ hơn nghiệm ban đầu (nếu có) và cứ như thế. Tuy nhiên cuối cùng thì các tính toán chi tiết vẫn không được hoàn thiện. Sự thất vọng khiến chúng tôi chán nản và thậm chí còn không trở lại nghiên cứu gì thêm về phương trình Pythagoras $x^2 + y^2 = z^2$ vì coi rằng đây là một trường hợp tầm thường không cần xét tới. Mặt khác các tài liệu về toán những năm đó trong trường học là không đủ phong phú do đó chúng tôi có cảm giác mình giống như vẫn đang chơi với những bài toán đơn lẻ và không có gì đặc biệt.

Chỉ tới khi lên cấp 3 thì tôi mới được tiếp cận với thư viện thực sự của một trường Đại học (tôi học lớp 10 tại khối chuyên Toán – Tin Đại học Khoa học tự nhiên và do đó được sử dụng gần như toàn bộ hệ thống thư viện của trường Đại học Quốc Gia Hà Nội). Sau khi tra cứu trong hộp phích thì tôi đã chọn một cuốn sách tương đối dày và có tựa đề tiếng Việt tương đối dễ hiểu là ***Lý thuyết sơ cấp của các số***. Cũng cần nói thêm là tôi đã cố chọn cuốn sách có tựa đề đơn giản vì ngày đó tôi chưa đọc thạo sách toán bằng tiếng Anh.

Tuy nhiên rất bất ngờ là một cuốn sách có tựa đề ***có vẻ sơ cấp*** như vậy lại có riêng một mục để nói về phương trình $x^3 + y^3 = z^3$ mà chúng tôi đã loay hoay hết cả thời cấp 2. Theo đó thì phương trình này là không có nghiệm nào ngoài các nghiệm tầm thường và cuốn sách thậm chí đã cho tới hai chứng minh cho kết quả đó. Trong đó một chứng minh dựa trên tính toán và biến đổi sơ cấp cùng với ***phương pháp xuống thang***, chứng minh kia dựa trên ***các số nguyên phức***. Sự hào hứng những ngày cấp 2 đã thực sự trở lại vì hai chứng minh này rất gần gũi với những ý tưởng ban đầu mà chúng tôi đã cố gắng phát triển nhưng không đem lại kết quả. Tất nhiên ngay sau đó tôi đã nhận ra tuy ý tưởng ban đầu là giống nhau nhưng chúng tôi đã không có những phát triển mang tính quyết định. Khoảng cách giữa các tính toán không có kết quả và một chứng minh trọn vẹn trong trường hợp này nằm ở các ý niệm về các số nguyên phức, về các chuẩn của số nguyên phức, tính chia hết của số nguyên phức (những ý tưởng của Gauss) chứ không chỉ đơn thuần là một vài đẳng thức mang tính chất kỹ thuật nào đó.

Một điểm thú vị là ngay sau đó thì tôi đã nhanh chóng bị cuốn hút bởi một vấn đề khác. Cuốn sách này thực sự là một tài liệu rất có giá trị với vô số các định lý, các kết quả, các chứng minh, trích dẫn các nhà toán học và mối liên kết giữa các bài toán. Từ việc đọc về các phương trình Diophante có dạng ***quen thuộc*** một cách có hệ thống tôi chuyển qua đọc về ***các số nguyên phức*** và nhanh chóng tiếp xúc với chứng minh ***luật tương hỗ bậc hai***. Sau đó là các mở đầu về ***lý thuyết đồng dư*** và các định lý cùng chứng minh đẹp đẽ của ***Jacobi*** về ***tổng bốn bình phương***. Nhưng ấn tượng nhất có lẽ là các nghiên cứu về ***sự xuất hiện các số nguyên tố trong một cấp số cộng cho trước***. Các ước lượng về ***số lượng các số nguyên tố*** đặc biệt ấn tượng. Sự phong phú trong các định lý cùng với bảng danh sách dày đặc các nhà toán học được trích dẫn đã khiến tôi lần đầu tiên có cảm giác rằng toán học là rất rộng lớn, xuyên suốt và có ý nghĩa hơn một phương trình riêng rẽ rất nhiều.

Sau này trong quá trình tiếp tục đọc và học lên tôi đã biết rằng phương trình $x^n + y^n = z^n$ và định lý cuối cùng của ***Fermat*** mãi tới vài năm sau (kể từ khi chúng tôi nhận được câu đố) mới được giải bởi ***Andrew Wiles***. Chứng minh hoàn thiện được Wiles công bố năm 1995 và tại Đại hội Toán học thế giới 1998 thì Wiles đã được trao huy chương danh dự cho chứng minh đó (huy chương ***Fields***

giới hạn độ tuổi nhận giải là 40). Hơn nữa giá trị của việc giải phương trình này không thực sự nằm ở kết quả mà lại chính là những lý thuyết đẹp đẽ mà trong quá trình tìm lời giải cho nó các nhà toán học đã xây dựng nên. Đó là các lý thuyết về các dạng modular, lý thuyết về phương trình elliptic và các ngành khoa học hiện đại mà chúng tôi thời đó chưa hề nghe nói tới và cũng không thể hình dung nổi, chẳng hạn là ***hình học đại số số học.***

Tôi đã cho rằng cuốn sách này là một tài liệu tốt mà ngay cả các bạn học sinh cấp 2 cũng có thể bắt đầu đọc mà không cần một sự chuẩn bị nào trước về mặt kiến thức. Hơn nữa tinh thần cốt lõi trong các phép chứng minh cũng chính là dấu vết của sự đẹp đẽ của toán học mà các bạn nên tiếp xúc càng sớm càng tốt. Theo đó, sau một thời gia chuẩn bị thì cuối cùng thì tôi đã dịch toàn bộ cuốn sách này sang tiếng Việt. Và đây là bản dịch cuốn sách đó. Tức là cuốn ***"Elementary theory of numbers"*** của nhà toán học ***Wacław Sierpinski*** (1882-1969). Cuốn sách này được in lần thứ nhất vào năm 1964 (nghĩa là vài năm trước khi tác giả qua đời) và được in lần thứ hai năm vào năm 1988 với sự biên tập của nhà toán học ***Andrzej Schinzel*****.** Bản dịch này dựa trên bản in lần thứ hai. Theo tôi các bạn học sinh cấp 2 và cấp 3 sẽ có thể đọc toàn bộ cuốn sách này một cách tương đối thoải mái. Hơn nữa trong cuốn sách này thì ngoài sự phong phú về các kết quả thì các kiến thức sơ cấp về lý thuyết số cũng được trình bày đầy đủ với trình tự rất hiện đại. Do đó cũng có thể sử dụng cuốn sách như là một giáo trình nâng cao về số học dành cho các bạn học sinh khá giỏi.

Chương trình bày về các phương trình Diophante là một chương tuyệt hay vì trong đó các phương pháp và ý tưởng được chứa đựng ngay trong các lời giải và các đề bài thì được sắp xếp theo trình tự có tính gắn kết rất cao. Tuy nhiên trong cuốn sách này lại không đề cập tới chứng minh của ***Matijasevich*** về việc không tồn tại phương pháp tổng quát để giải các phương trình Diophante tổng quát ***(bài toán Hilbert số 10)***. Điều này cũng dễ hiểu vì định lý này được trình bày năm 1970, nghĩa là một năm sau khi Sierpinski qua đời.

Sierpinski được biết tới với những cống hiến xuất sắc trong lý thuyết tập hợp, đặc biệt là về tiên đề chọn và giả thuyết continuum. Cụ thể ông đã chứng minh được trong hệ tiên đề Zermelo-Fraenkel thì từ giả thuyết continuum dạng mở rộng có thể suy ra tính đúng đắn của tiên đề chọn. Bên cạnh đó mặc dù Cantor là cha đẻ của lý thuyết tập hợp nhưng Sierpinski lại là người đầu tiên giảng dạy về lý thuyết tập hợp ở bậc đại học (1909). Ông đã công bố 724 bài báo và 50 cuốn sách. Có ba hình fractal được đặt theo tên ông là tam giác Sierpinski, thảm Sierpinski và đường cong Sierpinski. Đường cong Sierpinski có ứng dụng quan trọng trong việc giải quyết bài toán người đưa thư và là cơ sở xây dựng đường cong liên tục phủ kín hình vuông đơn vị. Sierpinski đã giảng dạy tại Lwów từ năm 1908 tới 1914. Lwów là nơi (sau đó vài năm) trường phái Banach nổi tiếng ra đời. Trường phái Banach ra đời năm 1920 là một trong một số trường phái quan trọng đối với việc phát triển và hoàn thiện giải tích hàm hiện đại vào năm 1932.

Sài Gòn
Tháng 12 năm 2012

MỤC LỤC

CHƯƠNG 1
TÍNH CHIA HẾT VÀ PHƯƠNG TRÌNH BẤT ĐỊNH BẬC MỘT

CHƯƠNG 2
GIẢI TÍCH DIOPHANTE BẬC HAI VÀ CAO HƠN

CHƯƠNG 3
SỐ NGUYÊN TỐ

CHƯƠNG 4
SỐ CÁC ƯỚC SỐ VÀ TỔNG CỦA CHÚNG

CHƯƠNG 5
ĐỒNG DƯ

CHƯƠNG 6
HÀM CHỈ EULER VÀ ĐỊNH LÝ EULER

CHƯƠNG 7
BIỂU DIỄN HỆ CƠ SỐ TÙY Ý

CHƯƠNG 8
LIÊN PHÂN SỐ

CHƯƠNG 9
KÝ HIỆU LEGENDRE VÀ KÝ HIỆU JACOBI

CHƯƠNG 10
CÁC SỐ MERSENNE VÀ CÁC SỐ FERMAT

CHƯƠNG 11
BIỂU DIỄN CÁC SỐ TỰ NHIÊN THÀNH TỔNG CÁC LŨY THỪA BẬC k KHÔNG ÂM

CHƯƠNG 1

TÍNH CHIA HẾT VÀ PHƯƠNG TRÌNH BẤT ĐỊNH BẬC MỘT

1. Tính chia hết

Các số tự nhiên là các số $1,2,\ldots$. Các số nguyên là các số tự nhiên, số 0 và các số âm $-1,-2,-3,\ldots$. Số nguyên a chia hết cho số nguyên b nếu tồn tại số nguyên c mà $a=bc$. Khi đó ta viết $b|a$ và nói b là ước số của a, a là bội số của b. Ta viết $b\not|a$ nếu b không là ước số của a. Vì với mọi số nguyên b ta có $0=0.b$ nên mọi số nguyên đều là ước số của 0. Vì với mọi số nguyên a ta có $a=a.1$ nên 1 là ước số của mọi số nguyên.

Giả sử x,y,z là các số nguyên thỏa mãn

(1) $\qquad x|y$ ***và*** $y|z$

Khi đó tồn tại các số nguyên t và u thỏa mãn $y=xt$ và $z=yu$. Số $v=tu$ là một số nguyên (vì nó là tích của hai số nguyên). Vì vậy từ $z=xv$ suy ra $x|z$. Vậy từ ***(1)*** suy ra $x|z$. Do đó ước số của ước số của một số nguyên thì cũng là ước số của số nguyên đó. Quan hệ chia hết là quan hệ có tính bắc cầu. Do đó nếu $x|y$ thì $x|ky$ với mọi số nguyên k.

Dễ dàng chứng minh ước số chung của hai số nguyên cũng là ước số của tổng và hiệu các số đó. Hơn nữa nếu $d|a$ và $d|b$ thì với mọi số nguyên x và y ta có $d|ax+by$. Thật vậy, vì $d|a$ và $d|b$ suy ra tồn tại các số nguyên k và l mà $a=kd$, $b=ld$, suy ra $ax+by=(kx+ly)d$ và lưu ý $kx+ly$ là số nguyên suy ra $d|ax+by$. Quan hệ chia hết là quan hệ có tính kết hợp.

Các công thức $a=bc,-a=b(-c),a=(-b)(-c),-a=(-b)c$ là tương đương. Vì vậy các công thức $b|a$, $b|-a$, $-b|a$, $-b|-a$ cũng tương đương với nhau. Do đó để nghiên cứu tính chia hết giữa các số nguyên ta chỉ cần nghiên cứu tính chia hết giữa các số tự nhiên.

Từ định nghĩa $b|a$ ta nhận thấy nếu $0|a$ thì $a=0$. Tuy nhiên nếu $a\neq 0$ thì mọi ước số b của a là khác 0 và $-b$ cũng là ước số của a. Vì vậy với mọi số nguyên $a\neq 0$ thì các ước số b của a có thể sắp xếp thành các cặp $(b,-b)$. Do đó để tìm tất cả các ước số của một số nguyên ta chỉ cần tìm các ước số tự nhiên của số đó và bổ sung thêm các số đối của các số vừa tìm được.

Như vậy tập hợp các ước số và các bội số của một số là các tập hợp đối xứng. Mặt khác việc tìm các ước số của một số cho trước là khó hơn việc tìm tất cả các bội số của số đó. Thật vậy, tất cả các bội số của số nguyên a là các số nguyên có dạng ka với k là số nguyên tùy ý. Các bội số này được sắp xếp thành dãy vô hạn về cả hai phía $\ldots,-2a,a,0,a,2a,\ldots$. Trong khi đó việc tìm tất cả các ước số của a là không đơn giản. Điều này có vẻ đặc biệt vì tập hợp các ước số của một số nguyên cho trước là hữu hạn trong khi tập hợp các bội số của số nguyên đó là vô hạn.

Nếu số tự nhiên a chia hết cho số tự nhiên d thì $d\leq a$. Vì vậy để tìm tất cả các ước số dương của số nguyên a thì ta chỉ cần chia a lần lượt cho các số tự nhiên $1,2,\ldots,a$ và chọn ra các số mà thương số là số nguyên (phép chia không có dư). Do các phép tính toán theo cách này là hữu hạn nên về lý thuyết ta có một phương pháp để tìm tất cả các ước số của một số nguyên cho trước. Tuy nhiên có những khó khăn khi tiến hành tính toán cụ thể. Chẳng hạn thời gian để thực hiện phương pháp này đối với số $a=2^{293}-1$ (có 89 chữ số) là rất lớn ngay cả với các máy tính điện tử. Tuy nhiên ta có thể tìm tất cả các ước số của số 2^{293} (lớn hơn a). Số này có đúng 294 ước số lập thành một cấp số nhân là $1,2,2^2,2^3,\ldots,2^{293}$. Ta cũng chưa tìm được bất kỳ ước số không tầm thường nào của số $2^{163B4}+1$. Hơn nữa mặc dù ta biết rằng có những ước số như vậy (so sánh với Chương 10) nhưng ta chưa biết số này có tất cả bao nhiêu ước số không tầm thường.

Trong một số trường hợp các ước số của một số tự nhiên được tìm ra bằng cách sử dụng các máy tính điện tử. Chẳng hạn với số $(18!-1):59=108514808571661$. Sử dụng máy tính SWAC, D.H.Lehmer đã chỉ ra số này có đúng bốn ước số tự nhiên là 1, 226663, 478749547 và chính nó (Gabard [1] trang 218-220). Trong Chương 4 ta sẽ nghiên cứu số các ước số của một số tự nhiên.

Vấn đề nghiên cứu xem một số cho trước có phải là ước số của một số cho trước khác hay không là thực sự khó khăn. Trong một số trường hợp ta cần tới sự trợ giúp của máy tính. Chẳng hạn sử dụng máy tính ta biết số $a=2^{65536}+1$ chia hết cho $m=825753601$. Trường hợp này đặc biệt thú vị (xem Chương 10 mục 4). Số a có 19729 chữ số vì vậy việc viết cụ thể số đó dưới dạng thập phân là không khả thi. Tuy nhiên ta sẽ không đem a chia cho m để quyết định xem a có chia hết cho m hay không. Ta cần một cách biên dịch khác để máy tính có thể tính toán được. Một ví dụ khác là sự chia hết của số $2^{2^{23471}}+1$ đối với số $5\cdot 2^{23473}+1$. Số thứ nhất có hơn 10^{7064} chữ số trong khi số thứ hai có 7067 chữ số. Ta sẽ trở lại bài toán này trong Chương 10 mục 4.

Bài tập. ***1.*** Chứng minh rằng nếu a và b là các số tự nhiên thì $a!b!|(a+b)!$.

Chứng minh. Tính chất này là hiển nhiên đúng nếu ít nhất một trong các số a và b bằng 1 vì với mọi số tự nhiên b ta có $(b+1)!=b!(b+1)$ suy ra $1!b!|(1+b)!$. Do đó bài toán đúng với $a+b\le 3$. Giả sử n là số tự nhiên lớn hơn 2 và bài toán đúng với mọi cặp hai số tự nhiên có tổng không lớn hơn n. Xét hai số tự nhiên a và b có tổng bằng $n+1$. Ta đã biết bài toán đúng nếu ít nhất một trong hai số a và b bằng 1. Giả sử $a>1$ và $b>1$. Do bài toán đúng với mọi cặp hai số tự nhiên có tổng bằng n và $(a-1)+b=n, a+(b-1)=n$ suy ra $(a-1)!b!|(a+b-1)!$ và do đó $a!(b-1)!|(a+b-1)!$. Nhưng ta có $(a+b)!=(a+b-1)!(a+b)=(a+b-1)!a+(a+b-1)!b$, vì $(a-1)!b!|(a+b-1)!$ và $(a-1)!a=a!$ nên $a!b!|(a+b-1)!a$. Tương tự từ $a!(b-1)!|(a+b-1)!$ suy ra $a!b!|(a+b-1)!b$. Cộng lại ta có $a!b!|(a+b)!$. Suy ra định lý đúng với các số tự nhiên có tổng bằng $n+1$. Theo nguyên lý quy nạp suy ra bài toán đúng với mọi a và b. □

2. Chứng minh rằng với số tự nhiên k thì tích $P=(a+1)(a+2)...(a+k)$ chia hết cho $k!$.

Chứng minh. Rõ ràng $P=(a+k)!/a!$ vì vậy theo bài tập 1 với $b=k$ ta có điều phải chứng minh.

3. Chứng minh rằng nếu $a_1,a_2,...,a_m$ là các số tự nhiên $(m\ge 2)$ thì $a_1!a_2!...a_m!|(a_1+a_2+...+a_m)!$.

Chứng minh. Theo bài tập 1 thì bài toán đúng với $m=2$. Giả sử bài toán đúng với số tự nhiên m. Đặt $a_1,a_2,...,a_m,a_{m+1}$ là các số tự nhiên. Ta có $(a_1+a_2+...+a_m)!a_{m+1}!|(a_1+a_2+...+a_m+a_{m+1})!$, sử dụng giả thiết quy nạp, suy ra bài toán đúng với $m+1$. Điều phải chứng minh. Trường hợp riêng với $m=3, a_1=n, a_2=2n, a_3=3n$ và $n=1,2,..,$ ta có $n!(2n)!(3n)!|(6n)!$ với $n=1,2,....$ □

4. Chứng minh rằng nếu S là tập hợp gồm các số tự nhiên mà tổng và hiệu của hai phần tử bất kỳ thuộc S cũng là phần tử thuộc S, giả sử d là số tự nhiên nhỏ nhất thuộc S, thì S là tập hợp các bội số tự nhiên của d (ở đây các hiệu được lấy theo hai phần tử phân biệt và theo thứ tự số lớn trừ số bé).

Chứng minh. Theo giả thiết thì tổng của hai phần tử bất kỳ thuộc S cũng là một phần tử thuộc S nên bằng quy nạp ta chứng minh được tổng hữu hạn các phần tử thuộc S cũng là một phần tử thuộc S. Trong trường hợp đặc biệt khi tất cả các phần tử đó đều bằng d ta suy ra các số có dạng nd với $n=1,2,...$ đều thuộc S. Nghĩa là S chứa mọi bội số tự nhiên của d. Mặt khác giả sử k là phần tử thuộc S nhưng không phải bội số của d. Thế thì khi chia k cho d ta nhận được số dư dương $r<d$. Ta có $k=qd+r$ với q là số tự nhiên. Nếu $q=0$ thì $k\le r<d$ tức là $k<d$. Điều này mâu thuẫn với giả thiết d là phần tử nhỏ nhất thuộc S. Vậy qd là bội số tự nhiên của d và do đó là một phần tử thuộc S. Hệ quả là số tự nhiên $r=k-qd$, là hiệu của hai phần tử thuộc S, là một

phần tử thuộc S. Điều này không thể có vì $r < d$. Vậy mọi phần tử của S đều là bội số tự nhiên của d và ta có điều phải chứng minh. □

2. Bội số chung nhỏ nhất

Ký hiệu $a_1, a_2, ..., a_n$ là dãy hữu hạn các số nguyên. Mọi số nguyên chia hết cho tất cả các số $a_i \left(i = 1, 2, ..., n\right)$ được gọi là bội số chung của các số $a_1, ..., a_n$. Một bội số như vậy là tích của tất cả các số $a_1, a_2, ..., a_n$. Nếu ít nhất một trong các số đó bằng 0 thì 0 là bội số chung duy nhất của chúng. Nếu tất cả các số $a_i \left(i = 1, 2, ..., n\right)$ đều khác 0 thì tồn tại vô hạn các bội số chung của các số đó chẳng hạn các số nguyên có dạng $k\, a_1\, a_2 \ldots a_n$, k là số nguyên. Trong trường hợp này các số đó có bội số chung là số tự nhiên chẳng hạn $\left|a_1 a_2 \ldots a_n\right|$ với $\left|x\right|$ ký hiệu giá trị tuyệt đối của x. Vì trong mọi tập hợp các số tự nhiên đều tồn tại số nhỏ nhất nên trong các bội số chung tự nhiên của các số $a_1, a_2, ..., a_n$ tồn tại số nhỏ nhất, số này được gọi là bội số chung nhỏ nhất của các số $a_1, a_2, ..., a_n$ và được ký hiệu là $\left[a_1, a_2, ..., a_n\right]$.

Định lý 1. *Mọi bội số chung của các số tự nhiên $a_1, a_2, ..., a_n$ đều chia hết cho bội số chung nhỏ nhất của các số đó.*

Chứng minh. Sử dụng phản chứng. Giả sử tồn tại bội số chung M của các số nguyên $a_1, a_2, ..., a_n$ mà không chia hết cho bội số chung nhỏ nhất N của các số đó thì $M = qN + r$ với r là số tự nhiên $< N$. Vì vậy $r = M - qN$. Ký hiệu i là chỉ số tùy ý trong các số $1, 2, ..., n$. Vì M và N đều là các bội số của a_i nên tồn tại các số nguyên x_i và y_i mà $M = x_i a_i$ và $N = y_i a_i$. Do đó $r = M - qN = \left(x_i - qy_i\right)a_i$ suy ra $a_i \mid r$ với mọi $i = 1, 2, ..., n$ suy ra số tự nhiên r là bội số chung của các số nguyên $a_1, a_2, ..., a_n$ và nhỏ hơn bội số chung nhỏ nhất N. Vô lý. □

3. Ước số chung lớn nhất

Ký hiệu S là tập hợp cho trước (hữu hạn hoặc vô hạn) gồm các số nguyên thỏa mãn ít nhất một trong chúng, chẳng hạn a_0, là khác 0. Mọi số nguyên d là ước số của mọi phần tử thuộc S được gọi là ước số chung của các số nguyên thuộc S. Rõ ràng 1 là ước số chung của các số nguyên thuộc S. Mọi ước số chung d của các số nguyên thuộc S đều là ước số của số tự nhiên $\left|a_0\right|$ và do đó nó không lớn hơn $\left|a_0\right|$. Từ đây suy ra số các ước số chung của các số nguyên thuộc S là hữu hạn và do đó trong các ước số chung đó tồn tại số lớn nhất. Số này được gọi là ước số chung lớn nhất của các số nguyên thuộc S và ký hiệu là d_S. Rõ ràng d_S là số tự nhiên. Bây giờ ký hiệu d là ước số chung tùy ý của các số nguyên thuộc S và đặt $N = \left[d, d_S\right]$. Hơn nữa ký hiệu a là số nguyên thuộc S. Ta có $d \mid a$ và $d_S \mid a$ suy ra a là bội số chung của các số d và d_S nên theo Định lý 1 thì $\left[d, d_S\right] \mid a$. Vậy $N = \left[d, d_S\right]$ là ước số chung của các số nguyên thuộc S và vì d_S là ước số chung lớn nhất của các số nguyên đó nên $N \le d_S$. Nhưng số tự nhiên N là bội số chung nhỏ nhất của các số d và d_S nên nó chia hết cho d_S suy ra $N \ge d_S$. Vì vậy $N = d_S$ và do đó $d \mid d_S$. Ta có định lý

Định lý 2. *Nếu S là tập hợp (hữu hạn hay vô hạn) các số nguyên mà trong đó có ít nhất một phần tử khác 0 thì tồn tại ước số chung lớn nhất của các số nguyên thuộc S. Hơn nữa ước số chung lớn nhất này chia hết cho mọi ước số chung khác của các số nguyên thuộc S.*

Có thể chứng minh rằng (Hensel [1]) nếu $f\left(x\right)$ là đa thức bậc n với hệ số nguyên và k là số nguyên tùy ý thì ước số chung lớn nhất của các số $f\left(x\right)$ khi x nhận mọi giá trị nguyên là bằng với ước số chung lớn nhất của $n+1$ số nguyên $f\left(k\right), f\left(k+1\right), f\left(k+2\right), ..., f\left(k+n\right)$. Vì vậy chẳng hạn

với $f(x)=x^3-x$ thì ước số chung lớn nhất của các số $f(x)$ khi x nhận mọi giá trị nguyên là bằng với ước số chung lớn nhất của các số nguyên $f(-1)=0, f(0)=0, f(1)=0, f(2)=6,$ nghĩa là bằng 6.

4. Các số nguyên tố cùng nhau

Hai số nguyên a và b có ước số chung lớn nhất bằng 1 gọi là các số nguyên tố cùng nhau.

Định lý 3. *Khi chia các số nguyên a và b cho ước số chung lớn nhất của chúng thì ta nhận được các số nguyên tố cùng nhau.*

Chứng minh. Gọi d là ước số chung lớn nhất của hai số nguyên a và b. Đặt $a_1=a/d$, $b_1=b/d$. Nếu các số nguyên a_1 và b_1 không nguyên tố cùng nhau thì ước số chung lớn nhất của chúng là d_1 sẽ lớn hơn 1 và ta có $a_2=a_1/d_1$ và $b_2=b_1/d_1$ là các số nguyên. Nhưng khi đó $a=dd_1a_2, b=dd_1b_2$ suy ra số nguyên dd_1 là ước số chung của các số nguyên a và b suy ra $dd_1\le d$. Điều này không thể có vì $d_1>1$. Vậy a_1 và b_1 nguyên tố cùng nhau. Định lý 3 được chứng minh. □

Ước số chung lớn nhất của các số nguyên $a_1,a_2,...,a_n$ được ký hiệu là $(a_1,a_2,...,a_n)$.

Lập luận sử dụng trong chứng minh Định lý 3 cho ta kết quả sau

Định lý 3^a**.** *Khi chia các số nguyên $a_1,a_2,...,a_n$ cho ước số chung lớn nhất của chúng thì ta nhận được các số nguyên có ước số chung lớn nhất bằng* 1.

Giả sử r là một số hữu tỷ (nghĩa là tỷ số a/b của hai số nguyên a và b với $b\neq 0$. Có thể giả sử $b>0$. Nếu $(a,b)=d$ thì đặt $a/d=a_1, b/d=b_1$ thì theo Định lý 3 ta nhận được các số nguyên tố cùng nhau a_1 và b_1 với $b_1>0$. Khi đó ta có $r=a/b=a_1/b_1$. Vì vậy mọi số hữu tỷ đều có thể biểu diễn dưới dạng một phân số tối giản (nghĩa là phân số với tử số và mẫu số nguyên tố cùng nhau) với tử số là số nguyên và mẫu số là số tự nhiên.

Bây giờ ta chứng minh rằng nếu $(a,b)=1$ và $c\mid a$ thì $(c,b)=1$. Thật vậy, nếu $(c,b)=d$ thì $d\mid b$ và $d\mid c$ mà $c\mid a$ suy ra $d\mid a$. Hệ quả là d là ước số chung của các số nguyên a và b và theo Định lý 2 thì nó là ước số của ước số chung lớn nhất ($=1$) của hai số đó. Suy ra $d=1$ chứng tỏ $(c,b)=1$.

Với mọi dãy hữu hạn các số tự nhiên $a_1,a_2,...,a_n$ ta dễ dàng tìm được số tự nhiên a nguyên tố cùng nhau với mọi phần tử của dãy. Chẳng hạn số $a=a_1a_2...a_n+1$. Khi đó mọi ước số chung d_i của các số nguyên a và a_i, với i là chỉ số bất kỳ trong các số $1,2,...,n,$ cũng là ước số của $a_1a_2...a_n$ nên nó cũng là ước số của hiệu $a-a_1a_2...a_n=1$ và do đó bằng 1.

Từ nhận xét này ta kết luận rằng tồn tại dãy vô hạn các số tự nhiên mà mọi phần tử khác nhau trong dãy đều nguyên tố cùng nhau. Tuy nhiên công thức cụ thể cho phần tử thứ n của một dãy như vậy là không đơn giản. Một dãy đơn giản nhất thuộc dạng này là dãy các số đôi một nguyên tố cùng nhau $F_k=2^{2^k}+1(k=0,1,2,...)$. Thật vậy xét các số nguyên $m>n\ge 0$. Ta đã biết với mỗi số nguyên x và số tự nhiên k thì $x-1\mid x^k-1$ vì $x^k-1=(x-1)(x^{k-1}+x^{k-2}+...+x+1)$. Áp dụng tính chất này với $x=2^{2^{n+1}}, k=2^{m-n-1}$ ta có $2^{2^{n+1}}-1\mid 2^{2^m}-1$. Vì $F_n=2^{2^n}+1\mid 2^{2^{n+1}}-1$ và $2^{2^m}-1=F_m-2,$ ta có $F_n\mid F_m-2$. Do đó nếu $d\mid F_n$ và $d\mid F_m$ thì $d\mid F_m-2$ suy ra $d\mid 2$. Nhưng d là ước số của số lẻ F_m nên bản thân nó cũng là số lẻ. Vì vậy từ $d\mid 2$ suy ra $d\mid 1$. Chứng tỏ $(F_m,F_n)=1$ với $m>n\ge 0$.

Kết quả tổng quát hơn cũng đúng: *nếu a và b là các số nguyên tố cùng nhau và nếu $2\mid ab$ thì mọi phần tử phân biệt trong dãy $a^{2^k}+b^{2^k}$ $(k=0,1,2,...)$ là nguyên tố cùng nhau.*

Có thể chứng minh nếu k là số tự nhiên ≤ 16 thì trong k số tự nhiên liên tiếp luôn tồn tại ít nhất một số nguyên tố với $k-1$ số còn lại (Pilai [4]). Mặt khác có thể chứng minh rằng với mọi số tự nhiên $k \ge 17$ thì tồn tại dãy k số tự nhiên liên tiếp $m, m+1, \ldots, m+k-1$ mà không có phần tử nào trong dãy nguyên tố cùng nhau với tất cả các phần tử còn lại (Pillai [5],[6] và Brauer [2]). Với $k=17$ thì $m=2184$ thỏa mãn các điều kiện nêu trên. Nói cách khác trong các số tự nhiên 2184,2185,...,2200 không có số nào nguyên tố cùng nhau với tất cả các số còn lại. Các số trong dãy trên mà chia hết cho một trong các số 2,3,5,7 thì không phải là số nguyên tố cùng nhau với tất cả các số còn lại vì với mỗi $n=2,3,5,7$ thì tồn tại ít nhất hai phần tử trong dãy trên chia hết cho n. Ngoài ra chỉ còn lại hai phần tử khác là 2189 và 2197. Nhưng số thứ nhất cùng với 2200 là chia hết cho 11 còn số thứ hai cùng với 2184 là chia hết cho 13.

Bài tập. *1.* Chứng minh rằng nếu m và n là các số tự nhiên, m lẻ, thì $\left(2^m-1, 2^n+1\right)=1$.

Chứng minh (J. Browkin). Gọi d là ước số chung lớn nhất của các số 2^m-1 và 2^n+1. Khi đó d là số lẻ và $2^m-1=kd$, $2^n+1=ld$, với k và l là các số tự nhiên. Vì vậy $2^m=kd+1, 2^n=ld-1$ suy ra $2^{mn}=(kd+1)^n=td+1$, $2^{mn}=(ld-1)^m=ud-1$ với t và u là các số tự nhiên. Hệ quả là từ $td+1=ud-1$ suy ra ta có $d \mid 2$ và do d lẻ nên $d=1$. □

2. Chứng minh rằng với mọi số tự nhiên n ta có $\left(n!+1,(n+1)!+1\right)=1$.

Chứng minh. Nếu $d \mid n!+1$ và $d \mid (n+1)!+1$ thì từ đẳng thức $(n!+1)(n+1)=(n+1)!+n+1$ ta thấy $d \mid (n+1)!+n+1$, suy ra $d \mid n$ và vì $d \mid n!+1$, ta có $d \mid 1$. □

5. Quan hệ giữa ước số chung lớn nhất và bội số chung nhỏ nhất

Định lý 4. *Tích của hai số tự nhiên bằng với tích của ước số chung lớn nhất và bội số chung nhỏ nhất của hai số đó.*

Chứng minh. Với hai số tự nhiên a và b ký hiệu $N=[a,b]$. Vì ab là bội số chung của a và b nên từ Định lý 1 suy ra $N \mid ab$. Đặt $ab=dN$ với d là số tự nhiên. Vì N là bội số chung của a và b nên ta có $N=ka=lb$ với k và l là các số tự nhiên. Từ đây suy ra $ab=dN=dka=dlb$ và do đó $a=dl$ và $b=dk$ chứng tỏ d là ước số chung của a và b. Bây giờ ký hiệu t là ước số chung tùy ý của a và b. Ta có $a=ta_1$, $b=tb_1$ suy ra ta_1b_1 là bội số chung của các số a và b. Do đó từ Định lý 1 ta có $N \mid ta_1b_1$. Vì vậy với số nguyên u ta có $ta_1b_1=Nu$. Nhưng $dN=ab=t^2a_1b_1$, suy ra $tNu=dN$. Hệ quả là $d=tu$ và $t \mid d$. Vì vậy số tự nhiên d là ước số chung của a và b và hơn nữa mọi ước số chung của các số đó đều là ước số của d. Vậy d là ước số chung lớn nhất của các số a và b. Từ công thức $ab=dN$ suy ra Định lý 4 được chứng minh. □

Khi a và b là các số nguyên tố cùng nhau, nghĩa là $d=(a,b)=1$, thì công thức $ab=Nd$ trở thành $N=ab$. Ta có hệ quả sau

Hệ quả. *Bội số chung nhỏ nhất của hai số tự nhiên nguyên tố cùng nhau chính là tích của hai số đó.*

6. Định lý cơ bản của số học

Giả sử a và b là các số tự nhiên nguyên tố cùng nhau và c là số tự nhiên mà $b \mid ac$. Số ac chia hết cho cả hai số a và b do đó theo Định lý 1 thì nó chia hết cho bội số chung nhỏ nhất của các số đó. Bội số này theo Định lý 4 thì chính là tích ab. Vì vậy $ac=tab$ với t là số nguyên. Suy ra $c=tb$ và do đó $b \mid c$. Ta có định lý sau đây

Định lý 5. *Số tự nhiên là ước số của một tích hai số tự nhiên và nguyên tố cùng nhau với một trong hai số đó sẽ là ước số của số còn lại.*

Định lý 5 thường được gọi là định lý cơ bản của số học. Ta đã chứng minh định lý này đúng với các số tự nhiên. Định lý cũng đúng với các số nguyên vì phép đổi dấu không ảnh hưởng tới tính chia hết của các số.

Hệ quả. *Nếu* a,b,c *là các số nguyên thỏa mãn* $a\mid c, b\mid c$ *và* $(a,b)=1$ *thì* $ab\mid c$.

Chứng minh. Nếu $a\mid c$ thì $c=at$ với t là số nguyên. Vì $b\mid c$ ta có $b\mid at$ và vì $(a,b)=1$, từ Định lý 5 suy ra $b\mid t$ nghĩa là $t=bu$ với u là số nguyên. Do đó $c=at=abu$ suy ra $ab\mid c$. □

Từ Định lý 5 ta chứng minh được

Định lý 6. *Nếu* a,b,c *là các số nguyên thỏa mãn* $(a,b)=(a,c)=1$ *thì* $(a,bc)=1$.

Chứng minh. Ký hiệu $d=(a,bc)$ và $d_1=(b,d)$. Ta có $d_1\mid b$ và $d_1\mid d$. Vì $d\mid a, d_1\mid a$ nên ta thấy vì $d_1\mid a, d_1\mid b$ và $(a,b)=1$ nên $d_1=1$. Do đó $(b,d)=1$. Nhưng do $d=(a,bc), d\mid bc$, từ Định lý 5 suy ra $d\mid c$. Vì $d\mid a$ và $(a,c)=1$ suy ra $d=1$ nghĩa là $(a,bc)=1$. □

Sử dụng quy nạp ta có

Định lý 6^a**.** *Giả sử n là số tự nhiên* ≥ 2. *Nếu* $a_1,a_2,...,a_n$ *và a là các số nguyên thỏa mãn* $(a_i,a)=1$ *với mọi* $i=1,2,...,n$ *thì* $(a_1a_2...a_n,a)=1$.

Nói cách khác Định lý 6^a chỉ ra rằng một số nguyên nguyên tố cùng nhau với các số nguyên cho trước thì nó cũng nguyên tố cùng nhau với tích của các số đó.

Lập luận trong chứng minh Định lý 5 cho ta kết quả tổng quát hơn: *nếu* a,b *và* c *là các số nguyên thỏa mãn* $b\mid ac$ *thì* $b\mid (a,b)(b,c)$.

Từ Định lý 6^a ta suy ra

Hệ quả 1. *Nếu* $(a,b)=1$ *và* n *là số tự nhiên thì* $(a^n,b^n)=1$.

Chứng minh. Nếu $(a,b)=1$ thì theo Định lý 6^a (với $a_1=a_2=...=a_n=a$) ta có $(a^n,b)=1$ suy ra (lại theo Định lý 6^a với $a_1=a_2=...=a_n=b$) ta có $(a^n,b^n)=1$. □

Từ Hệ quả 1 ta có

Hệ quả 2. *Với mọi số tự nhiên* a,b,n *mà* $a^n\mid b^n$ *suy ra* $a\mid b$.

Chứng minh. Đặt $(a,b)=d$. Ta có $a=da_t, b=db_t$ với $(a_t,b_1)=1$. Vì vậy theo Hệ quả 1 ta có $(a_1^n,b_1^n)=1$. Vì $a^n\mid b^n$, hoặc tương đương $a_1^nd^n\mid b_1^nd^n$, ta có $a_1^n\mid b_1^n$ suy ra $a_1^n\mid (a_1^n,b_1^n)$ chứng tỏ $a_1^n\mid 1$ suy ra $a_t=1$, $a=d$ và hệ quả là, vì $b=db_1=ab_1$, $a\mid b$, điều phải chứng minh. □

Lưu ý rằng với hai số tự nhiên a và b thì từ điều kiện $a^a\mid b^b$ không suy ra $a\mid b$ được. Chẳng hạn $4^4\mid 10^{10}$ nhưng $4\not\mid 10$ và tương tự $9^9\mid 21^{21}$ nhưng $9\not\mid 21$.

Ghi chú. Khái niệm về tính chia hết có thể được mở rộng cho các số thực theo cách như sau. Cho trước hai số thực α và β khi đó ta nói α là ước số của β và viết $\alpha\mid\beta$ nếu tồn tại số nguyên k mà $\beta=k\alpha$. Trong trường hợp này thì từ $\alpha^2\mid\beta^2$ không suy ra $\alpha\mid\beta$. Chẳng hạn $2\mid 6$ nhưng ta không có $\sqrt{2}\mid\sqrt{6}$ vì nếu ngược lại thì tồn tại số nguyên k mà $\sqrt{6}=k\sqrt{2}$ suy ra $k=\sqrt{3}$ suy ra $3=k^2$ và vì vậy $k>1$ tức là $k\geq 2$ và do đó $3=k^2\geq 4$. Điều này không đúng.

Hệ quả 3. *Với các số tự nhiên* a,b *và* $n>1$ *thì từ* $a^n\mid 2b^n$ *suy ra* $a\mid b$.

Chứng minh. Đặt $(a,b)=d$ suy ra $a=da_1$, $b=db_1$ với $(a_1,b_1)=1$. Vì vậy theo Hệ quả 1 thì vì $(a_1^n,b_1^n)=1$ và từ $a^n \mid 2b^n$ suy ra $d^n a_1^n \mid 2d^n b_1^n$ do đó $a_1^n \mid 2b_1^n$. Sử dụng $(a_1^n,b_1^n)=1$ và Định lý 5 suy ra $a_1^n \mid 2$ mà $n>1$ suy ra $a_1=1$ và do đó $a=d$ chứng tỏ $a \mid b$. □

Định lý 7. *Nếu một số tự nhiên là lũy thừa bậc m của một số hữu tỷ và m là số tự nhiên thì số đó là lũy thừa bậc m của một số tự nhiên.*

Chứng minh. Giả sử số tự nhiên n là lũy thừa bậc m của số hữu tỷ p/q. Trong mục 4 ta biết có thể giả sử p và q là các số tự nhiên và $(p,q)=1$. Vì vậy theo Định lý 6^a suy ra $(p^m,q)=1$. Mặt khác vì $n=(p/q)^m$ ta có $nq^m=p^m$ suy ra $q \mid p^m$ và vì vậy $q \mid (p^m,q)=1$. Do đó $q=1$ (vì q là số tự nhiên) và hệ quả là $n=p^m$ nghĩa là n là lũy thừa bậc m của một số tự nhiên. □

Ta có hệ quả trực tiếp của Định lý 7

Hệ quả. *Căn bậc m của số tự nhiên không phải lũy thừa bậc m của một số tự nhiên là số vô tỷ.*

Đặc biệt các số $\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{6},\sqrt{7},\sqrt{8},\sqrt{10},\sqrt[3]{2},\sqrt[3]{3},\sqrt[3]{4}$ đều là số vô tỷ.

Bài tập. ***1.*** Chứng minh rằng nếu a,b,d là các số nguyên thỏa mãn $(a,b)=1$ và $d \mid a+b$ thì $(d,a)=1$ và $(d,b)=1$.

Chứng minh. Giả sử $(a,b)=1$ và $d \mid a+b$. Nếu $(d,a)=\delta$ thì $\delta \mid d$ và $\delta \mid a$ do đó vì $d \mid a+b$, $\delta \mid a+b$ nên $\delta \mid (a+b)-a$ suy ra $\delta \mid b$. Vì vậy $\delta \mid b$ do đó $\delta \mid (a,b)$. Ta có $\delta=(d,a)=1$. Tương tự chứng minh được $(d,b)=1$. □

2. Chứng minh rằng nếu n, n_1 và n_2 là các số tự nhiên mà $n \mid n_1 n_2$ và các số n_1, n_2 đều không chia hết cho n thì số

(*) $$d=\frac{n_1}{\left(n_1,\frac{n_1 n_2}{n}\right)}$$

là ước số của n và $1<d<n$.

Chứng minh. Theo ***(*)*** ta có $\frac{n_1}{d}=\left(n_1,\frac{n_1 n_2}{n}\right)$ nên $\frac{n_1}{d}$ là số tự nhiên và do đó $n_1=\frac{n_1}{d}k, \frac{n_1 n_2}{n}=\frac{n_1}{d}l$, với k và l là các số tự nhiên nguyên tố cùng nhau. Ta cũng có $k=d, n_2 d=nl$ và vì $(d,l)=1, d \mid n$. Vì vậy d là ước số của n. Nếu $d=1$, ta có $n_2=nl$ và vì vậy $n \mid n_2$, mâu thuẫn với giả thiết. Nếu $d=n$ thì theo ***(*)*** suy ra $d \mid n_1$, ta có $n \mid n_1$, mâu thuẫn với giả thiết. Vậy d là ước số của n với $1<d<n$, điều phải chứng minh. □

3. Chứng minh rằng nếu a và b là các số tự nhiên nguyên tố cùng nhau và m là số tự nhiên tùy ý thì trong cấp số cộng $a+bk\,(k=0,1,2,\ldots)$ tồn tại vô hạn số nguyên tố cùng nhau với m.

Chứng minh. Giả sử $(a,b)=1$ và m là số tự nhiên tùy ý. Số m có các ước số nguyên tố cùng nhau với a (chẳng hạn ước số 1). Ký hiệu c là ước số lớn nhất như vậy. Ta sẽ chứng minh rằng số $a+bc$ nguyên tố cùng nhau với m. Ta có $(a,b)=1$ và theo định nghĩa của c thì $(a,c)=1$. Vì vậy $(a,bc)=1$. Từ bài tập 1 suy ra nếu $d \mid a+bc$ thì $(d,a)=1$ và $(d,bc)=1$ do đó $(d,c)=1$. Mặt khác nếu $d \mid m$ thì vì $c \mid m$, $(d,c)=1$, hệ quả Định lý 5 suy ra $dc \mid m$. Hơn nữa vì $(d,a)=1$ và $(a,c)=1$

thì $(a,dc)=1$. Do đó dc là ước số của m và nguyên tố cùng nhau với a. Nhưng vì c là ước số lớn nhất có tính chất này nên $d=1$. Vậy ta đã chứng minh nếu d là ước số chung của các số $a+bc$ và m thì $d=1$. Suy ra $(a+bc,m)=1$. Vậy nếu l là số tự nhiên tùy ý thì với $k=c+lm$ các số $a+bk$ và m nguyên tố cùng nhau. Điều phải chứng minh. □

4. Chứng minh rằng nếu a và b là các số tự nhiên nguyên tố cùng nhau thì cấp số cộng $a+kb(k=0,1,2,...)$ chứa dãy con vô hạn các phần tử thuộc dãy là đôi một nguyên tố cùng nhau.

Chứng minh. Ta xây dựng dãy con $u_1,u_2,...$ thỏa mãn yêu cầu bài toán bằng quy nạp. Đặt $u_1=a$. Xét n là số tự nhiên tùy ý. Giả sử ta đã xác định được dãy các số $u_1,u_2,...,u_n$ đôi một nguyên tố cùng nhau. Theo bài toán 3 thì với số tự nhiên $u_1u_2...u_n$ tồn tại phần tử thuộc dãy $a+kb(k=0,1,2,...)$ mà nguyên tố cùng nhau với $u_1u_2...u_n$. Ký hiệu số như vậy là u_{n+1}. Chứng tỏ dãy $u_1,u_2,...$ xác định theo cách này có tính chất yêu cầu. □

Định lý 8. *Giả sử a và b là các số tự nhiên nguyên tố cùng nhau mà tích của chúng là lũy thừa bậc n của một số tự nhiên, nghĩa là $ab=c^n$ với n là số tự nhiên, thì các số a và b cũng là các lũy thừa bậc n của các số tự nhiên.*

Chứng minh. Đặt $(a,c)=d$ thì $a=da_1, c=dc_1$ với $(a_1,c_1)=1$. Theo giả thiết $ab=c^n$ ta có $da_1b=d^nc_1^n$ suy ra $a_1b=d^{n-1}c_1^n$. Mà $d\mid a$ và $(a,b)=1$ ta có $(d,b)=1$ suy ra theo Định lý 6^a thì $(d^{n-1},b)=1$. Đẳng thức $a_1b=d^{n-1}c_1^n$ chứng tỏ $b\mid d^{n-1}c_1^n$. Vì vậy theo Định lý 5 thì $b\mid c_1^n$. Mặt khác vì $(a_1,c_1)=1$, từ Định lý 6^a suy ra $(a_1,c_1^n)=1$ và vì $a_1b=d^{n-1}c_1^n$ suy ra $c_1^n\mid a_1b$ do đó theo Định lý 5 ta có $c_1^n\mid b$. Do $b\mid c_1^n$ và $c_1^n\mid b$ suy ra $b=c_1^n$ nên $a_1=d^{n-1}$ và $a=da_1=d^n$. Chứng tỏ các số a và b cũng là lũy thừa bậc n các số tự nhiên. □

Hệ quả. *Giả sử k,c và n là các số tự nhiên và $a_1,a_2,...,a_k$ là dãy các số tự nhiên đôi một nguyên tố cùng nhau và $a_1a_2...a_k=c^n$. Khi đó mọi số thuộc dãy $a_1,a_2,...,a_k$ là lũy thừa bậc n các số tự nhiên.*

7. Các công thức $(a_1,a_2,...,a_{n+1})=((a_t,a_2,...,a_n),a_{n+1})$ và $[a_1,a_2,...,a_{n+1}]=[[a_1,a_2,...,a_n],a_{n+1}]$

Ta chứng minh các công thức

(2) $$(a_1,a_2,...,a_{n+1})=((a_1,a_2,...,a_n),a_{n+1})$$

(3) $$[a_1,a_2,...,a_{n+1}]=[[a_1,a_2,...,a_n],a_{n+1}]$$

Định lý 9. *Với các số tự nhiên $n>2$ và $a_1,a_2,...,a_{n+1}$ thì công thức **(2)** đúng.*

Chứng minh. Đặt $d=((a_1,a_2,...,a_n),a_{n+1})$ thì d là ước số chung của các số $(a_1,a_2,...,a_n)$ và a_{n+1}. Vì $(a_1,a_2,...,a_n)$ là ước số của các số $a_1,a_2,...,a_n$ nên d là ước số của các số $a_1,a_2,...,a_n,a_{n+1}$. Ký hiệu d' là ước số tùy ý của các số $a_1,a_2,...,a_n,a_{n+1}$. Theo Định lý 2 ta có $d'\mid(a_1,a_2,...,a_n)$. Vì $d'\mid a_{n+1}$ nên ta có theo định nghĩa của d và sử dụng Định lý 2 thì $d'\mid d$. Vì vậy d là ước số chung của các số $a_1,a_2,...,a_n,a_{n+1}$ và chia hết cho mọi ước số chung của các số đó. Do đó d là ước số chung lớn nhất của $a_1,a_2,...,a_{n+1}$. Công thức ***(2)*** được chứng minh. □

Từ lập luận trong chứng minh này ta thấy để tính ước số chung lớn nhất $(a_1,a_2,...,a_n)$ thì ta có thể tính lần lượt $d_2=(a_1,a_2),d_3=(d_2,a_3),d_4=(d_3,a_4),...,d_{n-1}=(d_{n-1},a_{n-1}),(a_1,a_2,...,a_n)=(d_{n-1},a_n)$,

như vậy phép tính toán ước số chung lớn nhất của các số tự nhiên tùy ý quy về các phép tính liên tiếp các ước số chung lớn nhất của hai số tự nhiên.

Định lý 10. *Với các số tự nhiên* $n \geq 2$ *và* $a_1, a_2, ..., a_{n+1}$ *thì công thức (3) đúng.*

Chứng minh. Đặt $N = \left[\left[a_1, a_2, ..., a_n\right], a_{n+1}\right]$ thì N là bội số chung của các số $\left[a_1, a_2, ..., a_n\right]$ và a_{n+1}. Vì $\left[a_1, a_2, ..., a_n\right]$ là bội số của các số $a_1, a_2, ..., a_n$ nên N là bội số của các số $a_1, a_2, ..., a_n, a_{n+1}$. Ký hiệu M là bội số chung tùy ý của các số $a_1, a_2, ..., a_n, a_{n+1}$. Theo Định lý 1 ta có $\left[a_1, a_2, ..., a_n\right] | M$. Mà $a_{n+1} | M$ nên lại sử dụng Định lý 1 và suy ra $\left[\left[a_1, a_2, ..., a_n\right], a_{n+1}\right] | M$ hoặc tương đương $N | M$. Vậy N là bội số chung của các số $a_1, a_2, ..., a_n, a_{n+1}$ và là ước số của mọi bội số chung khác của các số này. Do đó N là bội số chung nhỏ nhất của các số đó. Công thức ***(3)*** được chứng minh. □

Vậy để tính bội số chung nhr nhất $\left[a_1, a_2, ..., a_n\right]$ ta lần lượt tính bội số chung nhỏ nhất của các cặp $N_2 = \left[a_1, a_2\right], N_3 = \left[N_2, a_3\right], ..., N_{n-1} = \left[N_{n-2}, a_{n-1}\right]$ $\left[a_1, a_2, ..., a_n\right] = \left[N_{n-1}, a_n\right]$.

Định lý 11. *Nếu* n *là số tự nhiên và các số* $a_1, a_2, ..., a_n$ *đôi một nguyên tố cùng nhau thì* $\left[a_1, a_2, ..., a_n\right] = a_1 a_2 ... a_n$.

Chứng minh. Từ hệ quả Định lý 4 suy ra bài toán đúng với $n = 2$. Bây giờ xét n là số tự nhiên tùy ý ≥ 2. Giả sử bài toán đúng với số tự nhiên n và $a_1, a_2, ..., a_n, a_{n+1}$ là các số tự nhiên đôi một nguyên tố cùng nhau. Khi đó $\left(a_i, a_{n+1}\right) = 1$ với mọi $i = 1, 2, ..., n$. Theo Định lý 6^a và hệ quả Định lý 4 thì $\left[a_1 a_2 ... a_n\, a_{n+1}\right] = a_1 a_2 ... a_n\, a_{n+1}$. Nhưng theo giả thiết quy nạp thì bài toán đúng với n nên $a_1 a_2 ... a_n = \left[a_1, a_2, ..., a_n\right]$ và theo ***(3)*** thì $a_1 a_2 ... a_n\, a_{n+1} = \left[\left[a_1, a_2, ..., a_n\right], a_{n+1}\right] = \left[a_1, a_2, ..., a_n, a_{n+1}\right]$, suy ra bài toán đúng với $n+1$ và vì vậy đúng với mọi số tự nhiên. □

Điều ngược lại cũng đúng: *nếu với các số tự nhiên* $n \geq 2$ *và* $a_1, a_2, ..., a_n$ *ta có công thức* $\left[a_1, a_2, ..., a_n\right] = a_1 a_2 ... a_n$ *thì các số* $a_1, a_2, ..., a_n$ *là đôi một nguyên tố cùng nhau.*

Mệnh đề sau đây cũng đúng: *tích của* $n > 2$ *số tự nhiên bằng với tích của ước số chung lớn nhất và bội số chung nhỏ nhất của chúng khi và chỉ khi các số đó là đôi một nguyên tố cùng nhau.*

Mệnh đề này không đúng với $n = 2$ chẳng hạn $2 \cdot 4 = (2, 4) \cdot [2, 4]$.

8. Quy tắc tính các ước số chung lớn nhất của hai số

Giả sử a và b là hai số tự nhiên cho trước. Chia a cho b ta nhận được thương số q và số dư r nhỏ hơn b. Ta có $a = qb + r$. Từ đẳng thức này suy ra mọi ước số chung của a và b cũng là ước số của số dư $r = a - qb$ và mọi ước số chung của b và r cũng là ước số của a. Vậy ước số chung của a và b chính là các ước số chung của b và r. Do đó $(a, b) = (b, r)$. Ta ký hiệu $a = n_0, b = n_1, r = n_2$ và có đẳng thức $(n_0, n_1) = (n_1, n_2)$. Nếu $n_2 = 0$ thì $(n_0, n_1) = n_1$. Nếu $n_2 \neq 0$ thì ta có thể chia n_1 cho n_2 và ký hiệu số dư là n_3 và lại có $(n_1, n_2) = (n_2, n_3)$. Quá trình này lặp lại và ta thu được

$$(n_0, n_1) = (n_1, n_2),$$
$$(n_1, n_2) = (n_2, n_3),$$
$$(n_2, n_3) = (n_3, n_4),$$

(4) $\quad ...$

$$(n_{k-2}, n_{k-1}) = (n_{k-1}, n_k),$$
$$(n_{k-1}, n_k) = (n_k, n_{k+1})$$

Vì n_{i+1} ký hiệu số dư nhận được khi chia n_{i-1} cho $n_i\,(i = 1,2,\ldots,k)$ nên ta có $n_{i+1} < n_i$ với $i = 1,2,\ldots,k$ suy ra dãy các số n_i là giảm nghiêm ngặt, nghĩa là $n_1 > n_2 > n_3 > \ldots \geq 0.$ Dãy này hữu hạn vì chỉ có n số nguyên không âm phân biệt nhỏ hơn n. Vì vậy trong dãy ***(4)*** tồn tại phần tử cuối cùng, nghĩa là $(n_{k-1}, n_k) = (n_k, n_{k+1})$. Nếu ta có $n_{k+1} \neq 0$ thì ta có thể chia n_k cho n_{k+1} và nhận được đẳng thức $(n_k, n_{k+1}) = (n_{k+1}, n_{k+2})$, mâu thuẫn với giả thiết chỉ có k đẳng thức trong ***(4)***. Vì vậy $n_{k+1} = 0$ và do đó $(n_{k-1}, n_k) = n_k$. Các đẳng thức trong ***(4)*** suy ra $(n_0, n_1) = (n_1, n_2) = (n_2, n_3) = \ldots = (n_{k-1}, n_k) = n_k$, suy ra $(n_0, n_1) = n_k$. Từ các lập luận này ta nhận được quy tắc tính ước số chung lớn nhất của hai số tự nhiên cho trước: *để tính ước số chung lớn nhất của hai số tự nhiên n_0 và n_1 ta chia n_0 cho n_1 và tìm số dư n_2. Sau đó ta chia n_1 cho n_2 và tìm được số dư n_3. Tiếp tục như vậy ta chia n_2 cho n_3 và cứ như thế. Ở bước cuối cùng ta nhận được số dư bằng 0. Số dư nhận được trong bước trước đó chính là ước số chung lớn nhất của các số n_0 và n_1.*

Quy tắc vừa nhận được cũng được gọi là thuật toán chia hoặc thuật toán Euclid hoặc là thuật toán liên phân số. Tên gọi cuối cùng sẽ được trình bày cụ thể trong mục 9.

Từ thuật toán Euclid suy ra ước số chung lớn nhất của hai số tự nhiên cho trước có thể nhận được sau hữu hạn phép chia. Tuy nhiên số các phép chia lại có thể lớn tùy ý. Nghĩa là với mọi số tự nhiên n thì tồn tại các số tự nhiên a_n và b_n mà để tìm ước số chung lớn nhất của chúng bằng thuật toán Euclid thì cần tới n phép chia. Để chứng minh tính chất này ta xét dãy

(5) $$u_1 = u_2 = 1,\ \ u_n = u_{n-1} + u_{n-2},\ \text{với}\ n = 3,4,\ldots$$

Ta có

(6) $$u_1 = 1,\ \ u_2 = 1,\ \ u_3 = 2,\ \ u_4 = 3,\ \ u_5 = 5,\ \ u_6 = 8,\ \ u_7 = 13,\ \ u_8 = 21,\ \ u_9 = 34,\ldots$$

Đây là dãy số Fibonacci: hai phần tử đầu tiên của dãy bằng 1 và các phần tử tiếp theo bằng tổng của hai phần tử liền trước nó. Đặt $a_n = u_{n+2}$, $b_n = u_{n+1}$. Áp dụng thuật toán Euclid để tìm $(a_n, b_n) = (u_{n+2}, u_{n+1})$. Ta nhận được dãy các phép chia

$$u_{n+2} = 1 \cdot u_{n+1} + u_n,$$
$$u_{n+1} = 1 \cdot u_n + u_{n-1},$$
$$\ldots$$
$$u_4 = 1 \cdot u_3 + u_2,$$
$$u_3 = 2 \cdot u_2.$$

Rõ ràng có n phép chia tất cả. Chẳng hạn để tìm ước số chung lớn nhất của các số $u_{12} = 144$ và $u_{11} = 89$ bằng thuật toán Euclid thì ta cần 10 phép chia. Có thể chứng minh rằng các số nhỏ nhất mà cần đúng n phép chia để tìm ước số chung lớn nhất của chúng bằng thuật toán Euclid chính là u_{n+2} và u_{n+1}. Ta chứng minh kết quả sau đây

Định lý 12. *Số các phép chia cần thiết để tìm ước số chung lớn nhất của hai số tự nhiên bằng thuật toán Euclid là không lớn hơn năm lần số các chữ số thập phân của số nhỏ hơn (Lame [1]).*

Chứng minh. Đầu tiên ta chứng minh tính chất sau đây của dãy số Fibonacci $u_n\,(n = 1,2,\ldots)$ được định nghĩa ở trên

(7) $$u_{n+5} > 10u_n \ \text{với}\ n = 2,3,\ldots$$

Tính toán trực tiếp chứng tỏ với $n=2$ thì công thức ***(7)*** đúng (với $u_7=13>10u_2=10$). Với $n\ge 3$ thì theo ***(5)*** ta có

$$\begin{aligned} u_{n+5}&=u_{n+4}+u_{n+3}=2u_{n+3}+u_{n+2}=3u_{n+2}+2u_{n+1}\\ &=5u_{n+1}+3u_n=8u_n+5u_{n-1}. \end{aligned}$$

Dãy ***(6)*** không giảm, $u_n=u_{n-1}+u_{n-2}\le 2u_{n-1}$, $2u_n\le 4u_{n-1}$ và $u_{n+5}=8u_n+5u_{n-1}>8u_n+4u_{n-1}\ge 10u_n$ nên suy ra $u_{n+5}>10u_n$.

Từ ***(7)***, bằng quy nạp ta chứng minh được

(8) $$u_{n+5l}>10^l u_n,\qquad n=2,3,\ldots;\ l=1,2,\ldots$$

Ký hiệu n_o và $n_1<n_0$ là hai số tự nhiên cho trước. Giả sử để tìm ước số chung lớn nhất (n_0,n_1) bằng thuật toán Euclid cần tới k phép chia

(9)
$$\begin{aligned} &n_0=q_1n_1+n_2,\\ &n_1=q_2n_2+n_3,\\ &\ldots\\ &n_{k-2}=q_{k-1}n_{k-1}+n_k,\\ &n_{k-1}=q_kn_k. \end{aligned}$$

Ta có $q_k\ge 2$ vì nếu $q_k=1$ thì $n_k=n_{k-1}$, điều này vô lý vì n_k là số dư nhận được khi chia n_{k-2} cho n_{k-1}. Vì vậy $n_{k-1}=q_kn_k\ge 2n_k\ge 2=u_3$ nên

$$n_{k-2}\ge n_{k-1}+n_k\ge u_3+u_2=u_4,\ \ n_{k-3}\ge n_{k-2}+n_{k-1}\ge u_4+u_3=u_5,\ldots,n_1\ge u_{k+1}.$$

Do đó nếu $k>5l$, hoặc tương đương $k\ge 5l+1$, thì $n_1\ge u_{5l+2}$ và theo ***(8)*** (với $n=2$) thì $n_1>10^l$. Nghĩa là n_1 có ít nhất $l+1$ chữ số trong biểu diễn thập phân. Vì vậy nếu n_1 có l chữ số thì $k\le 1$. Định lý 12 được chứng minh. □

Từ Định lý 12 suy ra để tìm ước số chung lớn nhất của hai số tự nhiên cho trước bằng thuật toán Euclid mà số nhỏ hơn có nhiều nhất 6 chữ số thì cần nhiều nhất 30 phép chia. Trong Định lý 12 thì số 5 không thể thay bởi 4 vì ta cần 10 phép chia để tìm ước số chung lớn nhất của 144 và 89 (Brown J.L Jr. [1], Dixon [1],[2]).

9. Biểu diễn số hữu tỷ thành liên phân số

Ký hiệu n_0,n_1 là các số tự nhiên và ***(9)*** là dãy các đẳng thức nhận được bằng cách sử dụng thuật toán Euclid cho các số n_0 và n_1. Với mọi $i=1,2,\ldots,k-1$ ta có $\dfrac{n_{i-1}}{n_i}=q_i+\dfrac{1}{n_i/n_{i+1}}$ và $\dfrac{n_{k-1}}{n_k}=q_k$. Do đó

(10)
$$\frac{n_0}{n_1}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{q_4+\ddots+\cfrac{1}{q_{k-1}+\cfrac{1}{q_k}}}}},$$

Ta viết gọn công thức này thành $\frac{n_0}{n_1} = q_1 + \frac{1|}{|q_2} + \frac{1|}{|q_3} + \frac{1|}{|q_4} + \ldots + \frac{1\ |}{|q_{k-1}} + \frac{1|}{|q_k}$. Trong ***(9)*** thì q_1 là số nguyên dương là thương số nhận được khi chia số tự nhiên n_0 cho số tự nhiên n_1, các số q_i với $i = 2,3,\ldots,k$ là các số tự nhiên vì $n_{i-1} > n_i$. Biểu thức trong vế phải của ***(10)***, q_1 là số nguyên và $q_2, q_3, \ldots, q_n$ là các số tự nhiên, được gọi là liên phân số đơn (hoặc gọn hơn là liên phân số).

Vì vậy sử dụng thuật toán Euclid thì mọi số hữu tỷ đều biểu diễn được thành một liên phân số đơn.

Ví dụ. Xét số 314159/100000. Áp dụng thuật toán Euclid ta nhận được

$$\begin{aligned}
314159 &= 3\cdot 100000 + 14159,\\
100000 &= 7\cdot 14159 + 887,\\
14159 &= 15\cdot 887 + 854,\\
887 &= 1\cdot 854 + 33,\\
854 &= 25\cdot 33 + 29,\\
33 &= 1\cdot 29 + 4,\\
29 &= 7\cdot 4 + 1,\\
4 &= 4\cdot 1.
\end{aligned}$$

Vì vậy $\frac{314159}{100000} = 3 + \frac{1|}{|7} + \frac{1|}{|15} + \frac{1|}{|1} + \frac{1|}{|25} + \frac{1|}{|1} + \frac{1|}{|7} + \frac{1|}{|4}$. Một ví dụ khác khi ta xét các số u_{n+1}/u_n trong đó $u_k\ (k = 1,2,\ldots)$ là các số Fibonacci (mục 8). Từ ***(10)*** suy ra với mọi số tự nhiên n ta có $\frac{u_{n+1}}{u_n} = 1 + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \ldots + \frac{1|}{|1}$. Trong đó dấu $\frac{|}{|}$ xuất hiện $n-1$ lần. Vì vậy chẳng hạn ta có $\frac{u_2}{u_1} = 1,\quad \frac{u_3}{u_2} = 1 + \frac{1|}{|1},\quad \frac{u_4}{u_3} = 1 + \frac{1|}{|1} + \frac{1|}{|1}$ và cứ như thế. Ta cũng có thể viết $\frac{u_4}{u_3} = 1 + \frac{1|}{|2}$.

Ta sẽ tìm hiểu chi tiết hơn về các liên phân số trong chương 8.

10. Dạng tuyến tính của ước số chung lớn nhất

Định lý 13. *Nếu $a_1, a_2, \ldots, a_m$ là $m > 1$ số nguyên mà ít nhất có một số trong chúng là khác 0 thì tồn tại các số nguyên $t_1, t_2, \ldots, t_m$ thỏa mãn*

(11) $$(a_1, a_2, \ldots, a_m) = a_1 t_1 + a_2 t_2 + \ldots + a_m t_m.$$

Chứng minh. Ký hiệu D là tập hợp các số tự nhiên xác định bởi quy tắc: số n thuộc D khi và chỉ khi tồn tại các số nguyên $x_1, x_2, \ldots, x_m$ thỏa mãn

(12) $$n = a_1 x_1 + a_2 x_2 + \ldots + a_m x_m.$$

Nói cách khác D là tập hợp tất cả các số tự nhiên có dạng $a_1 x_1 + a_2 x_2 + \ldots + a_m x_m$ với $x_1, x_2, \ldots, x_m$ là các số nguyên. Tập hợp này không rỗng (nghĩa là nó chứa ít nhất một phần tử) vì $a_k \neq 0$ (với $1 \le k \le m$) nên $|a_k|$ thuộc D bởi vì nó có dạng $a_1 x_1 + a_2 x_2 + \ldots + a_m x_m$, với $x_i = 0$ với $i \neq k$ và x_k bằng $+1$ hoặc -1 tương ứng với $a_k > 0$ hoặc $a_k < 0$.

Ký hiệu d là số tự nhiên nhỏ nhất thuộc tập hợp D (số d tồn tại vì trong một tập hợp các số tự nhiên luôn tồn tại phần tử nhỏ nhất). Nếu d thuộc D thì theo định nghĩa tồn tại các số nguyên $t_1, t_2, \ldots, t_m$ thỏa mãn

(13) $$d = a_1 t_1 + a_2 t_2 + \ldots + a_m t_m.$$

Nhưng vì d là phần tử nhỏ nhất của D nên với mọi số tự nhiên n có dạng ***(12)*** với $x_1, x_2, ..., x_m$ là các số nguyên thì $n \geq d$. Ta sẽ chứng minh rằng với các số nguyên $x_1, x_2, ..., x_m$ bất kỳ thì số $a_1 x_1 + a_2 x_2 + ... + a_m x_m$ chia hết cho d. Giả sử phản chứng thì tồn tại các số nguyên $y_1, y_2, ..., y_m$ mà khi chia $a_1 y_1 + a_2 y_2 + ... + a_m y_m$ cho d thì ta nhận được thương số q và số dư dương r. Ta có $a_1 y_1 + a_2 y_2 + ... + a_m y_m = qd + r$ suy ra theo ***(13)***

$$r = a_1 y_1 + a_2 y_2 + ... + a_m y_m - q(a_1 t_1 + a_2 t_2 + ... + a_m t_m) = a_1 x_1 + a_2 x_2 + ... + a_m x_m$$

Với $x_i = y_i - qt_i$ là các số nguyên với $i = 1, 2, ..., m$. Vì vậy số tự nhiên r có dạng ***(12)*** suy ra r thuộc D. Nhưng mặt khác r là số dư nhận được khi chia một số cho d nên nó nhỏ hơn d, mâu thuẫn với giả thiết d là phần tử nhỏ nhất của D. Vậy ta đã chứng minh với các số nguyên $x_1, x_2, ..., x_m$ bất kỳ thì số $a_1 x_1 + a_2 x_2 + ... + a_m x_m$ chia hết cho d. Đặc biệt $d \mid a_1 x_1 + a_2 x_2 + ... + a_m x_m$, với $x_k = 1$ và $x_i = 0$ với $i \neq k$. Vì vậy với $k = 1, 2, ..., m, d \mid a_k$ nghĩa là d là ước số chung của $a_1, a_2, ..., a_m$.

Ký hiệu δ là ước số chung tùy ý của các số $a_1, a_2, ..., a_m$. Khi đó tồn tại các số nguyên $z_1, z_2, ..., z_m$ mà $a_k = \delta z_k \ (k = 1, 2, ..., m)$. Theo ***(13)*** ta có $d = a_1 t_1 + a_2 t_2 + ... + a_m t_m = (t_1 z_1 + t_2 z_2 + ... + t_m z_m)\delta$, suy ra $\delta \mid d$. Từ đây ta kết luận rằng ước số chung d bằng với $(a_1, a_2, ..., a_m)$ bởi vì nó chia hết cho mọi ước số chung khác của các số $a_1, a_2, ..., a_m$. Vậy từ ***(13)*** suy ra ***(11)*** và định lý được chứng minh. □

Giả sử $a_1, a_2, ..., a_m$ là $m > 1$ số nguyên thỏa mãn $(a_1, a_2, ..., a_m) = 1$. Theo Định lý 13 suy ra tồn tại các số nguyên $t_1, t_2, ..., t_m$ thỏa mãn

(14) $$a_1 t_1 + a_2 t_2 + ... + a_m t_m = 1.$$

Ngược lại, giả sử với các số nguyên cho trước $a_1, a_2, ..., a_m$ tồn tại các số nguyên $t_1, t_2, ..., t_m$ thỏa mãn ***(14)***. Vế trái của phương trình chia hết cho mọi ước số chung của các số $a_1, a_2, ..., a_m$. Nhưng vế phải của phương trình là 1 suy ra $(a_1, a_2, ..., a_m) = 1$. Ta có định lý sau đây

Định lý 14. *Với $m > 1$ thì $(a_1, a_2, ..., a_m) = 1$ khi và chỉ khi tồn tại các số nguyên $t_1, t_2, ..., t_m$ thỏa mãn $a_1 t_1 + a_2 t_2 + ... + a_m t_m = 1$.*

Hệ quả. *Nếu với các số nguyên d, k và $a_1, a_2, ..., a_m$ với $m > 1$ ta có $(a_1, a_2, ..., a_m) = 1$ và $d \mid ka_i$ với $i = 1, 2, ..., m$, thì $d \mid k$.*

Chứng minh. Theo Định lý 14 thì từ $(a_1, a_2, ..., a_m) = 1$ suy ra tồn tại các số nguyên $t_1, t_2, ..., t_m$ thỏa mãn $a_1 t_1 + a_2 t_2 + ... + a_m t_m = 1$. Nhưng vì $d \mid ka_i$ với mọi $i = 1, 2, .., m, d \mid ka_i t_i$ với $i = 1, 2, ..., m$ suy ra $d \mid k(a_1 t_1 + a_2 t_2 + ... + a_m t_m)$ và hệ quả là $d \mid k$. Điều phải chứng minh. □

Mệnh đề tương tự các Định lý 13 và 14 đúng với đa thức một biến nhưng không đúng với các đa thức nhiều biến. Thật vậy nếu $f(x, y) = x$ và $g(x, y) = y$ thì ước số chung lớn nhất của các đa thức $f(x, y)$ và $g(x, y)$ là hằng số. Biểu thức $xp(x, y) + yq(x, y)$ không thể là hằng số khác 0 với các đa thức $p(x, y), q(x, y)$ bất kỳ (Bochner [1]).

Trở lại với Định lý 13. Một vấn đề được đặt ra là với các số $a_1, a_2, ..., a_m$ cho trước làm sao tìm được các số $t_1, t_2, ..., t_m$ thỏa mãn ***(11)***. Chứng minh ở trên của định lý không cho một gợi ý nào để làm điều này (ta gọi đây là một chứng minh sự tồn tại trên lý thuyết mà không có tính kiến thiết, tức là một chứng minh dạng ẩn). Tuy nhiên ta có thể giải quyết vấn đề này bằng cách sử dụng thuật toán

Euclid. Bắt đầu với trường hợp $m=2$. Bỏ qua trường hợp tầm thường khi một trong các số bằng 0. Đổi dấu nếu cần thiết các số t_1 và t_2 và giả sử a_1 và a_2 là các số tự nhiên, ký hiệu các số này là n_0 và n_1. Sử dụng thuật toán Euclid ta nhận được công thức ***(9)***. Ta đã biết $n_k=(n_0,n_1)$. Đẳng thức áp chót trong ***(9)*** tương đương với

(15) $$n_k=n_{k-2}-q_{k-1}n_{k-1}$$

Thế giá trị của n_{k-1} từ đẳng thức trước đó trong ***(9)*** ta có

$$\begin{aligned} n_k &= n_{k-2}-q_{k-1}(n_{k-3}-q_{k-2}n_{k-2}) \\ &= -q_{k-1}n_{k-3}+(1+q_{k-1}q_{k-2})n_{k-2}. \end{aligned}$$

Ta lại thế giá trị của n_{k-2} nhận được từ đẳng thức trước đó trong ***(9)*** và cứ như vậy. Sau $k-2$ phép thế ta nhận được $n_k=n_0x+n_1y,$ với x và y là các số nguyên. Rõ ràng thủ tục này cho ta cách tính toán hữu hiệu các số $x=t_1$ và $y=t_2$.

Trong trường hợp tổng quát khi m là số tự nhiên tùy ý >1 ta thực hiện bằng quy nạp. Giả sử với mọi số nguyên $a_1,a_2,\dots,a_m$ ta có quy tắc để tính $t_1,t_2,\dots,t_m$ thỏa mãn ***(11)***. Giả sử $a_1,a_2,\dots,a_m,a_{m+1}$ là các số nguyên cho trước. Theo Định lý 9 ta có $(a_1,a_2,\dots,a_{m+1})=((a_1,a_2,\dots,a_m),a_{m+1})$. Ta đã biết từ lập luận ở trên thì ta có một quy tắc để tìm các số x và y thỏa mãn

(16) $$((a_1,a_2,\dots,a_m),a_{m+1})=(a_1,a_2,\dots,a_m)x+a_{m+1}y.$$

Đặt $x_i=t_ix$ với $t=1,2,\dots,m$ và $x_{m+1}=y$. Theo ***(16)*** và ***(11)*** ta có

(17) $$(a_1,a_2,\dots,a_{m+1})=a_1x_1+a_2x_2+\dots+a_mx_m+a_{m+1}x_{m+1},$$

Với $x_1,x_2,\dots,x_{m+1}$ là các số nguyên. Vì vậy ta đã có một quy tắc để tìm $x_1,x_2,\dots,x_{m+1}$ thỏa mãn ***(17)*** dựa theo quy tắc đã biết để tìm các số $t_1,t_2,\dots,t_m$. Vì vậy theo quy nạp chứng tỏ: *với mọi* $m>1$ *và các số nguyên* $a_1,a_2,\dots,a_m$ *mà ít nhất một trong số chúng là khác* 0 *thì tồn tại quy tắc để tìm các số* $t_1,t_2,\dots,t_m$ *thỏa mãn* ***(11)***.

11. Phương trình bất định m biến bậc 1

Định lý 15. *Cho trước* $m>1$ *số nguyên* $a_1,a_2,\dots,a_m$ *mà ít nhất một số là khác* 0. *Phương trình*

(18) $$a_1x_1+a_2x_2+\dots+a_mx_m=b,$$

có nghiệm nguyên $x_1,x_2,\dots,x_m$ *khi và chỉ khi* $(a_1,a_2,\dots,a_m)\mid b.$

Chứng minh. Giả sử tồn tại các số nguyên $x_1,x_2,\dots,x_m$ thỏa mãn ***(18)***. Từ ***(18)*** suy ra ước số chung của các số $a_1,a_2,\dots,a_m$ là ước số của b. Vì vậy $(a_1,a_2,\dots,a_m)\mid b,$ suy ra điều kiện cần.

Mặt khác giả sử $d=(a_1,a_2,\dots,a_m)\mid b$. Khi đó tồn tại số nguyên k mà $b=kd$. Vì ít nhất một trong các số $a_1,a_2,\dots,a_m$ là khác 0 nên theo Định lý 13 thì tồn tại các số nguyên $t_1,t_2,\dots,t_m$ thỏa mãn ***(11)***. Đặt $x_i=kt_i$ với mọi $i=1,2,\dots,m$. Vì $d=(a_1,a_2,\dots,a_m)$ nên theo ***(11)*** ta có

$$a_1x_1+a_2x_2+\dots+a_mx_m=k(a_1t_1+a_2t_2+\dots+a_mt_m)=kd=b.$$

Điều kiện đủ được chứng minh. □

Định lý 15 có thể phát biểu dưới dạng sau đây: *phương trình hệ số nguyên bậc 1 với* $m>1$ *biến là có nghiệm tự nhiên khi và chỉ khi hệ số tự do của phương trình này chia hết cho ước số chung lớn nhất của các hệ số của các biến.*

Từ chứng minh Định lý 15 và tính chất với mọi số nguyên cho trước $a_1, a_2, \ldots, a_m$ thì có thể tìm các số $t_1, t_2, \ldots, t_m$ thỏa mãn ***(11)***, ta suy ra nếu phương trình ***(11)*** là có nghiệm nguyên thì ta có thể tìm các số nguyên $x_1, x_2, \ldots, x_m$ thỏa mãn ***(11)***, nghĩa là tồn tại quy tắc tìm ít nhất một nghiệm nguyên của phương trình ***(18)***. Câu hỏi đặt ra là làm thế nào để tìm mọi nghiệm nguyên như vậy.

Bắt đầu với trường hợp $m=2$. Xét phương trình

(19) $$ax+by=c$$

Với a,b,c là các số nguyên và $(a,b)\,|\,c$. Có thể giả sử cả a và b đều khác 0 vì nếu ngược lại ta có phương trình một biến và dễ dàng tìm được nghiệm của nó. Do $(a,b)\,|\,c$ ta có thể tim các số nguyên x_0, y_0 thỏa mãn

(20) $$ax_0+by_0=c$$

Giả sử x và y là các số nguyên bất kỳ thỏa mãn phương trình ***(19)***. Từ ***(19)*** và ***(20)*** suy ra

(21) $$a(x-x_0)=b(y_0-y)$$

Vì $d=(a,b)$ là ước số chung lớn nhất của a và b nên ta có $a=da_1, b=db_1$ với a_1 và b_1 là các số nguyên nguyên tố cùng nhau. Từ ***(21)*** ta có

(22) $$a_1(x-x_0)=b_1(y_0-y).$$

Do $(a_1,b_1)=1$ và theo Định lý 6 suy ra $b_1\,|\,x-x_0$ do đó $x-x_0=b_1t$ với t là số nguyên. Theo ***(22)*** thì $a_1b_1t=b_1(y_0-y)$ mà $b_1\neq 0$ nên $y_0-y=a_1t$. Từ các đẳng thức $x-x_0=b_1t, y_0-y=a_1t$ suy ra

(23) $$x=x_0+b_1t,\qquad y=y_0-a_1t.$$

Vậy nếu x,y là nghiệm nguyên của ***(19)*** thì chúng có dạng ***(23)*** với t là số nguyên.

Bây giờ ký hiệu t là số nguyên tùy ý. Ta tìm x và y từ ***(23)*** và tính giá trị của

$$ax+by=a(x_0+b_1t)+b(y_0-a_1t)=ax_0+by_0+(ab_1-ba_1)t.$$

Từ ***(20)*** và $ab_1-ba_1=da_1b_1-db_1a_1=0$ suy ra ***(19)***. Vì vậy: *các số nguyên* x *và* y *là nghiệm của* ***(19)*** *khi và chỉ khi với số tự nhiên* t *nào đó ta có công thức* ***(23)*** *được thỏa mãn.*

Vậy với $t=0,\pm1,\pm2,\ldots$ công thức ***(23)*** cho tất cả các nghiệm nguyên của ***(19)***. Vì ít nhất một trong hai số a_1, b_1 là khác 0, nếu ***(19)*** có ít nhất một nghiệm nguyên thì nó có vô hạn nghiệm như vậy.

Ta chứng minh định lý sau đây

Định lý 16. *Nếu* a *và* b *là các số tự nhiên nguyên tố cùng nhau thì tồn tại các số tự nhiên* u *và* v *thỏa mãn* $au-bv=1$.

Chứng minh. Theo Định lý 15 thì tồn tại các số nguyên x_0 và y_0 thỏa mãn $ax_0+by_0=1$. Ta chọn số nguyên t_0 thỏa mãn $t_0>x_0/b$ và $t_0>y_0/a$, đặt $u=x_0+bt_0>0$ và $v=-(y_0-at_0)>0$. Khi đó u và v là các số tự nhiên và $au-bv=ax_0+by_0=1$. □

Từ Định lý 16 ta suy ra ba hệ quả sau đây

Hệ quả 1. *Nếu các số tự nhiên* a,b,l,m *thỏa mãn* $a^l=b^m$ *và* l,m *là các số nguyên tố cùng nhau thì tồn tại ít nhất một số tự nhiên n thỏa mãn* $a=n^m$ *và* $b=n^l$.

Chứng minh. Vì $(l,m)=1$ nên theo Định lý 16 suy ra tồn tại các số tự nhiên r và s mà $lr-ms=1$. Vì vậy từ $a^l=b^m$ suy ra $a=a^{lr-ms}=a^{lr}\big/a^{ms}=\left(b^r/a^s\right)^m$. Do đó a là lũy thừa bậc m của số hữu tỷ b^r/a^s nên theo Định lý 7 suy ra nó là lũy thừa bậc m của một số tự nhiên $n=b^r/a^s$. Vì vậy $a=n^m$ suy ra $b^m=a^l=n^{ml}$ chứng tỏ $b=n^l$. Vậy $a=n^m$ và $b=n^l$ với n là số tự nhiên. □

Hệ quả 2. *Nếu* a *và* b *là các số tự nhiên nguyên tố cùng nhau thì mọi số tự nhiên* $n>ab$ *đều có thể biểu diễn dưới dạng* $n=ax+by$, *với* x,y *là các số tự nhiên.*

Chứng minh. Xét a và b là các số tự nhiên nguyên tố cùng nhau và u,v là các số tự nhiên thỏa mãn Định lý 16. Khi đó $au-bv=1$ suy ra với $n>ab$ thì $anu-bnv=n>ab$ nên $nu/b-nv/a>1$. Do đó tồn tại số nguyên t thỏa mãn $nv/a<t<nu/b$ (đây là số nguyên lớn nhất nhỏ hơn nu/b). Đặt $x=nu-bt, y=at-nv$. Ta có $x>0$ và $y>0$ và $ax+by=a(nu-bt)+b(at-nv)=n$ suy ra điều phải chứng minh. □

Lưu ý rằng trong Hệ quả 2 thì số ab không thể thay bằng một số nhỏ hơn. Vì nếu $(a,b)=1$ thì số ab tự nó không có biểu diễn dạng $ax+by=ab$ với x,y là các số tự nhiên. Thật vậy, giả sử $ab=ax+by$ thì $ax=(a-y)b$ suy ra vì $(a,b)=1,\ b\mid x$ nên $x\ge b$. Vậy $ab=ax+by\ge ab+by>ab$, nhưng điều này là không thể.

Hệ quả 3. *Với các số tự nhiên cho trước* $a>1,m,n$ *thì* $\left(a^m-1,a^n-1\right)=a^{(m,n)}-1$.

Chứng minh. Đặt $\delta=(m,n)$ thì $m=\delta m_1, n=\delta n_1$ với m_1 và n_1 là các số tự nhiên nguyên tố cùng nhau. Theo Định lý 16 thì tồn tại các số tự nhiên u,v thỏa mãn $m_1u-n_1v=1$ suy ra $\delta=mu-nv$. Đặt $d=\left(a^m-1,a^n-1\right)$. Rõ ràng $a^{(m,n)}-1\mid a^m-1$ và $a^{(m,n)}-1\mid a^n-1$ suy ra $a^{(m,n)}-1\mid d$. Mặt khác ta có $d\mid a^m-1$ suy ra $d\mid a^{mu}-1$ và $d\mid a^n-1$ suy ra $d\mid a^{nv}-1$. Vì vậy

$$d\mid a^{mu}-a^{nv}=a^{nv}\left(a^{mu-nv}-1\right)=a^{nv}\left(a^{\delta}-1\right)$$

Do $d\mid a^m-1$ và $a>1$ suy ra $(d,a)=1$ và vì vậy $d\mid a^{\delta}-1$. Hệ quả là $d\mid a^{(m,n)}-1$ mà theo công thức $a^{(m,n)}-1\mid d$ thì suy ra $a^{(m,n)}-1=d=\left(a^m-1,a^n-1\right)$, điều phải chứng minh. □

Vậy ta đã chứng minh các nghiệm nguyên của phương trình ***(19)*** được cho bởi công thức ***(23)***. Bây giờ ta xét trường hợp tổng quát hơn dạng ***(18)*** với số biến tùy ý m. Phương pháp tìm các nghiệm của phương trình ***(18)*** trình bày dưới đây là một trong các phương pháp đơn giản nhất.

Đầu tiên lưu ý rằng ta chỉ cần xét phương trình ***(18)*** với a_i ($i=1,2,..,m$) là các số tự nhiên bởi vì các hệ số bằng 0 không ảnh hưởng tới các nghiệm và nếu có hệ số $a_i<0$ thì ta chỉ cần thay a_i bởi $-a_i$ và đổi dấu của biến số tương ứng. Nếu có hai hệ số a_i bằng nhau chẳng hạn $a_1=a_2$ thì đặt $x_1+x_2=x$ ta có phương trình

(24) $$a_1x+a_3x_3+a_4x_4+...+a_mx_m=b.$$

Từ mọi nghiệm nguyên $x_1,x_2,...,x_m$ của ***(18)*** ta có thể nhận được nghiệm $x,x_3,x_4,...,x_m$ của ***(24)*** bằng cách đặt $x=x_1+x_2$. Ngược lại từ mọi nghiệm nguyên $x,x_3,x_4,...$ của ***(24)*** ta có thể nhận được nghiệm của ***(18)*** bằng cách đặt x_1 là số nguyên tùy ý và $x_2=x-x_1$. Vì vậy việc tìm tất cả các

nghiệm nguyên của ***(18)*** trong trường hợp có hai hệ số bằng nhau được quy về việc tìm các nghiệm nguyên của ***(24)*** với số biến ít hơn.

Nếu có hai hệ số trong ***(24)*** bằng nhau thì ta lại có thể tiến hành giảm biến như vậy. Vậy ta có thể giả sử các hệ số của phương trình ***(18)*** là các số tự nhiên phân biệt. Giả sử a_1 là số lớn nhất trong các hệ số đó. Khi đó $a_1 > a_2$. Giả sử khi chia a_1 cho a_2 ta nhận được thương số k và số dư a_2'. Khi đó ta có $a_1 = a_2 k + a_2'$ với k là số tự nhiên và a_2' là số nguyên thỏa mãn $0 < a_2' < a_2$. Đặt $x_1' = kx_1 + x_2,\ x_2' = x_1,\ a_1' = a_2$. Ta có $a_1 x_1 + a_2 x_2 = a_2 \left(kx_1 + x_2\right) + a_2' x_1 = a_1' x_1' + a_2' x_2'$. Vì vậy ***(24)*** có thể viết lại thành

(25) $$a_1' x_1' + a_2' x_2' + a_3 x_3 + \ldots + a_m x_m = b.$$

Từ mọi nghiệm nguyên $x_1, x_2, \ldots, x_m$ của ***(24)*** ta nhận được nghiệm nguyên $x_1', x_2', x_3, \ldots, x_m$ của ***(25)*** bằng cách đặt $x_1' = kx_1 + x_2,\ x_2' = x_1$. Ngược lại từ mọi nghiệm $x_1', x_2', x_3, \ldots, x_m$ của ***(25)*** ta nhận được nghiệm nguyên của ***(18)*** bằng cách đặt $x_1 = x_2', x_2 = x_1' - kx_2'$.

Vì vậy bài toán tìm các nghiệm tự nhiên của ***(18)*** được quy về việc giải phương trình ***(25)*** với số lớn nhất trong các hệ số của các biến là nhỏ hơn số lớn nhất trong các hệ số của ***(18)***. Tiếp tục như vậy, từ phương trình ***(25)*** ta lại nhận được phương trình với số lớn nhất trong các hệ số của các biến là nhỏ hơn số lớn nhất trong các hệ số của các biến của ***(25)***. Quá trình này dẫn tới một phương trình một biến mà đã biết cách giải.

Vậy ta đã chứng minh được với phương trình tuyến tính hệ số nguyên thì tồn tại phương pháp tìm tất cả các nghiệm nguyên của nó. Tuy nhiên phương pháp trình bày ở trên chưa đưa ra một quy tắc thuận tiện nhất để tìm tất cả các nghiệm của phương trình tuyến tính trong thực tế mà mới chỉ là một chứng minh sự tồn tại của các nghiệm.

Nếu trong ***(18)*** có một hệ số $a_1, a_2, \ldots, a_m$, chẳng hạn a_1, bằng 1 thì tất cả các nghiệm nguyên của ***(18)*** nhận được bằng cách lấy $x_2, x_3, \ldots, x_m$ tùy ý và đặt $x_1 = b - a_2 x_2 - a_3 x_3 - \ldots - a_m x_m$.

Dễ thấy nếu phương trình ***(18)*** có nghiệm nguyên và $m > 1$ thì nó có vô hạn nghiệm nguyên. Thật vậy, nếu $y_1, y_2, \ldots, y_m$ là các số nguyên thỏa mãn $a_1 y_1 + a_2 y_2 + \ldots + a_m y_m = b$ thì đặt $x_i = y_i + a_m t_i$ với $i = 1, 2, \ldots, m-1$ và $x_m = y_m - a_1 t_1 - \ldots - a_{m-1} t_{m-1}$ với $t_1, t_2, \ldots, t_{m-1}$ là các số nguyên tùy ý ta nhận được các số nguyên $x_1, x_2, \ldots, x_m$ thỏa mãn ***(18)***.

Cũng dễ dàng chứng minh rằng nếu ***(18)*** có nghiệm nguyên $x_1, x_2, \ldots, x_m$ thì các số nguyên $x_1, x_2, \ldots, x_m$ có thể biểu diễn thành tổ hợp tuyến tính của $m-1$ tham số nguyên.

Tính chất này cho phép chúng ta tìm các nghiệm nguyên của hệ n phương trình tuyến tính m biến. Để làm điều đó ta khai triển các biến của phương trình thứ nhất thành tổ hợp tuyến tính của $m-1$ tham số với hệ số nguyên và thế vào $n-1$ phương trình còn lại. Khi đó có thể coi các tham số như là các biến số và ta nhận được hệ $n-1$ phương trình $m-1$ biến. Quá trình này lặp lại và cuối cùng ta nhận được hoặc là một phương trình (một hoặc nhiều biến) mà đã biết cách giải hoặc là một hoặc nhiều phương trình một biến.

12. Định lý số dư Trung Hoa

Định lý 17. *Giả sử m là số tự nhiên $\geq 2, a_1, a_2, \ldots, a_m$ là các số tự nhiên đôi một nguyên tố cùng nhau và $r_1, r_2, \ldots, r_m$ là các số nguyên tùy ý. Khi đó tồn tại các số nguyên $x_1, x_2, \ldots, x_m$ thỏa mãn*

(26) $$a_1 x_1 + r_1 = a_2 x_2 + r_2 = \ldots = a_m x_m + r_m.$$

Chứng minh. Định lý đúng với $m = 2$ vì nếu a_1, a_2 là các số nguyên tố cùng nhau thì phương trình $a_1 x - a_2 y = r_2 - r_1$ có nghiệm nguyên x và y. Giả sử m là số tự nhiên tùy ý ≥ 2. Giả sử định lý

đúng với m. Đặt $a_1, a_2, ..., a_m, a_{m+1}$ là các số tự nhiên đôi một nguyên tố cùng nhau và đặt $r_1, r_2, ..., r_m, r_{m+1}$ là các số nguyên tùy ý. Từ giả thiết định lý đúng với m suy ra tồn tại các số nguyên $x_1, x_2, ..., x_m$ thỏa mãn ***(26)***. Vì các số $a_1, a_2, ..., a_m$ là nguyên tố cùng nhau với a_{m+1} nên theo Định lý 6^a thì số $a_1 a_2 ... a_m$ nguyên tố cùng nhau với a_{m+1} và do đó tồn tại các số nguyên t và u thỏa mãn $a_1 a_2 ... a_m t - a_{m+1} u = r_{m+1} - a_1 x_1 - r_1$. Đặt $x_i' = \frac{a_1 a_2 ... a_m}{a_l} t + x_i$, với $i = 1, 2, ..., m$ và $x_{m+1}' = u$. Rõ ràng các số $x_1', x_2, ..., x_{m+1}'$ nguyên và $a_1 x_1' + r_1 = a_2 x_2' + r_2 = ... = a_{m+1} x_{m+1}' + r_{m+1}$, theo quy nạp suy ra định lý được chứng minh. □

Từ Định lý 17 suy ra nếu có hai trong $m \geq 2$ số tự nhiên $a_1, a_2, ..., a_m$ là nguyên tố cùng nhau và $r_1, r_2, ..., r_m$ là các số nguyên tùy ý thì tồn tại số nguyên k thỏa mãn khi chia k cho $a_1, a_2, ..., a_m$ ta lần lượt nhận được các số dư $r_1, r_2, ..., r_m$. Đây là lý do định lý được gọi là định lý các số dư.

Hiển nhiên khi cộng vào k các bội số tùy ý của số $a_1 a_2 ... a_m$ thì ta nhận được số nguyên mà khi chia cho $a_1, a_2, ..., a_m$ cũng lần lượt cho các số dư $r_1, r_2, ..., r_m$. Suy ra tồn tại vô hạn các số nguyên có tính chất này.

Ta trình bày một ứng dụng đơn giản của Định lý 17. Cho trước hai số tự nhiên m và s. Ta đã chứng minh trong mục 4 rằng dãy các số $F_k = 2^{2^k} + 1$ $(k = 0, 1, 2, ...)$ là đôi một nguyên tố cùng nhau. Đặt $a_i = F_i^s$ và $r_l = -i$ với mọi $i = 1, 2, ..., m$. Với $c = a_1 x_1 + r_1$ công thức ***(26)*** suy ra $F_i^s x_i = a_i x_i = a_1 x_1 + r_1 - r_i = c + i$ nên $F_i^s \mid c + i$ với mọi $i = 1, 2, ..., m$. Vì $F_i > 1$ với $i = 1, 2, ...,$ nên các số $c+1, c+2, ..., c+m$ đều chia hết cho lũy thừa bậc s của một số tự nhiên lớn hơn 1.

Vì vậy ta có kết quả sau: *với mọi số tự nhiên s tồn tại dãy dài tùy ý các số tự nhiên liên tiếp mà mỗi số đều chia hết cho một lũy thừa bậc s của một số tự nhiên lớn hơn 1.*

13. Định lý Thue

Định lý 18 (Thue [1]). *Nếu m là số tự nhiên và a là số nguyên nguyên tố cùng nhau với m thì tồn tại các số tự nhiên x và y đều nhỏ hơn $\sqrt{m}$ và các số $ax \pm y$ đều chia hết cho m với các dấu $\pm$ thích hợp.*

Chứng minh. Định lý đúng với $m = 1$ vì trong trường hợp này ta đặt $x = y = 1$. Giả sử m là số tự nhiên lớn hơn 1. Ký hiệu q là số tự nhiên lớn nhất nhỏ hơn hoặc bằng $\sqrt{m}$. Khi đó $q + 1 > \sqrt{m}$ và $(q+1)^2 > m$. Xét biểu thức $ax - y$ với x, y nhận các giá trị $0, 1, 2, ..., q$. Có đúng $(q+1)^2 > m$ biểu thức như vậy mà chỉ có thể có m số dư khác nhau có thể nhận được khi chia một số cho m nên tồn tại hai cặp phân biệt x_1, y_1 và x_2, y_2 với $x_1 \geq x_2$ mà các biểu thức $ax - y$ có cùng số dư khi chia cho m. Hệ quả là số $ax_1 - y_1 - (ax_2 - y_2) = a(x_1 - x_2) - (y_1 - y_2)$ chia hết cho m. Ta không thể có $x_1 = x_2$ vì nếu như thê thì $y_1 - y_2$ chia hết cho m mà vì $0 \leq y_1 \leq q \leq \sqrt{m} < m$ (vì $m > 1$) và $0 \leq y_2 < m$ nên ta có mâu thuẫn vì các cặp x_1, y_1 và x_2, y_2 là phân biệt. Đẳng thức $y_1 = y_2$ cũng không xảy ra vì nếu như thế thì $a(x_1 - x_2)$ chia hết cho m mà a nguyên tố cùng nhau với m nên $m \mid (x_1 - x_2)$ và vì $0 \leq x_1 \leq q \leq m$, $0 \leq x_2 \leq q$ và $x_1 \neq x_2$ suy ra mâu thuẫn. Vậy ta phải có $x_1 \neq x_2$ và $y_1 \neq y_2$. Vì $x_1 \geq x_2$, $x = x_1 - x_2$ là số tự nhiên. Số $y_1 - y_2$ có thể là số nguyên âm nhưng nó khác 0 nên $y = |y_1 - y_2|$ là số tự nhiên. Ta có $x = x_1 - x_2 \leq x_1 \leq q \leq \sqrt{m}$, $y \leq q \leq \sqrt{m}$ và do đó chọn các dấu + và – thích hợp ta có $a(x_1 - x_2) - (y_1 - y_2) = ax \pm y$ chia hết cho m. Điều phải chứng minh. □

Với một số thay đổi từ chứng minh ở trên ta nhận được kết quả tổng quát hơn sau đây được trình bày bởi Scholz và Schoenberg ([1] trang 44): *nếu* m,e *và* f *là các số tự nhiên thỏa mãn* $e \le m,\ f \le m < ef$ *thì với số nguyên* a *mà* $(a,m)=1$ *tồn tại các số nguyên* x *và* y *mà với các dấu + và– thích hợp ta có* $m \mid ax \pm y$ *và* $0 \le x \le f$, $0 \le y \le e$. Về các tổng quát khác của Định lý Thue có thể xem trong Brauner và Reynolds [1], Modell [6] và Nagell [6].

14. Các số không có ước số chính phương

Số nguyên không có ước số chính phương nếu nó không chia hết cho mọi bình phương các số tự nhiên >1. Các số tự nhiên không có ước số chính phương ≤ 20 là: 1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19.

Từ kết quả đã được chứng minh trong mục 12 suy ra tồn tại dãy dài tùy ý các số tự nhiên liên tiếp mà tất cả các số đó đều có ước số chính phương. Trong bốn số tự nhiên liên tiếp luôn tồn tại số có ước số chính phương (vì có ít nhất một số chia hết cho $4=2^2$). Có thể chứng minh rằng tồn tại vô hạn các bộ ba số tự nhiên liên tiếp mà các số đó đều không có ước số chính phương.

Có thể chứng minh rằng mọi số tự nhiên >1 đều là tổng của hai số không có ước số chính phương và có vô hạn cách biểu diễn số đó thành hiệu của các số như vậy (Nagell [1]. Sierpinski [36]). Hơn nữa mỗi số tự nhiên đủ lớn đều là tổng của một số không có ước số chính phương và một số tự nhiên (Estermann [1], Hooley [1]). Ta chứng minh định lý sau đây

Định lý 19. *Mỗi số tự nhiên* n *đều có biểu diễn duy nhất dưới dạng* $n=k^2l$ *với* k *và* l *là các số tự nhiên và* l *không có ước số chính phương.*

Chứng minh. Với mọi số tự nhiên n, ký hiệu k là số tự nhiên lớn nhất thỏa mãn $k^2 \mid n$. Ta có $n=k^2l$ với l là số tự nhiên. Nếu l có ước số chính phương thì đặt $l=r^2s$ với r,s là các số tự nhiên và $r>1$. Vì vậy $n=(kr)^2 s$ và do đó $(kr)^2 \mid n$ với $kr>k$, mâu thuẫn với định nghĩa của k. Bây giờ giả sử $n=k_1^2 l_1$ với k_1, l_1 là các số tự nhiên và l_1 không có ước số chính phương. Đặt $d=(k,k_1)$ ta có $k=dh,\ k_1=dh_1$ với h,h_1 là các số tự nhiên và $(h,\ h_1)=1$. Vì $n=d^2h^2l=d^2h_1^2l_1,$ ta có $h^2l=h_1^2l_1$ và vì $(h^2,h_1^2)=1$ nên theo Định lý 5 suy ra $h^2 \mid l_1$ chứng tỏ $h=1$ vì l_1 không có ước số chính phương. Suy ra $k=dh=d.$ Nhưng vì $d \mid k_1$ ta có $k \mid k_1$ suy ra $k \le k_1$ mà theo định nghĩa của k và đẳng thức $n=k_1^2 l_1$ suy ra $l=l_1.$ □

CHƯƠNG 2

GIẢI TÍCH DIOPHANTE BẬC HAI VÀ CAO HƠN

1. Giải tích Diophantine một biến

Giải tích Diophante là một nhánh của lý thuyết số tập trung nghiên cứu các phương trình nghiệm nguyên. Các phương trình này được gọi là ***phương trình Diophante***. Chúng được đặt theo tên của nhà toán học Hy Lạp Diophantus, người sống trong triều đại Alexandria vào thế kỷ thứ 3 trước Công Nguyên và đã nghiên cứu về những phương trình thuộc dạng nói trên từ rất sớm.

Ta bắt đầu với các phương trình một biến bậc tùy ý.

Giả sử vế trái của phương trình là một đa thức với hệ số nguyên, nghĩa là có dạng

(1) $$a_0 x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m = 0,$$

trong đó m là số tự nhiên cho trước và $a_0, a_1, \ldots, a_m$ là các số nguyên với $a_0 \neq 0$ và $a_m \neq 0$. Nếu tồn tại số nguyên x thỏa mãn phương trình ***(1)*** thì

$$\left(a_0 x^{m-1} + a_1 x^{m-2} + \ldots + a_{m-1}\right) x = -a_m.$$

suy ra x phải là ước số nguyên của a_m. Mặt khác vì a_m khác 0 nên nó chỉ có hữu hạn ước số do đó tất cả các nghiệm nguyên của phương trình ***(1)*** có thể tìm được bằng hữu hạn các phép thử. Ta chỉ cần lần lượt thay thế các ước số (cả âm và dương) của a_m vào phương trình ***(1)***. Nếu $a_m = 0$ thì rõ rằng $x = 0$ là nghiệm của phương trình. Các nghiệm khác là nghiệm của phương trình rút gọn

$$a_0 x^{m-1} + a_1 x^{m-2} + \ldots + a_{m-2} x + a_{m-1} = 0$$

trong đó các nghiệm tìm được theo cách tương tự cho trường hợp $a_{m-1} \neq 0$. Nếu $a_{m-1} = 0$ thì phương trình được rút gọn xuống bậc $m-2$ và ta áp dụng quy nạp.

Xét ví dụ phương trình $x^7 + x + 2 = 0.$ Các nghiệm nguyên của phương trình này đều là ước số nguyên của -2. Thử trực tiếp ta thấy chỉ có -1 thỏa mãn phương trình vậy suy ra đó là nghiệm nguyên duy nhất cần tìm.

Với phương pháp vừa trình bày ta có thể nhận thấy về mặt kĩ thuật thì không khó để tìm tất cả các nghiệm nguyên cho các phương trình Diophante dạng đa thức. Tình huống này rất khác với việc giải các phương trình đại số mà như chúng ta đã biết thì công thức nghiệm tổng quát cho các đa thức bậc ba và bốn là rất phức tạp. Hơn nữa với một số đa thức bậc cao hơn bốn thì các nghiệm không thể tìm được bằng các phép giải đại số.

Tương tự như thế, việc tìm tất cả các nghiệm hữu tỷ của các đa thức với hệ số nguyên cũng không phức tạp hơn. Giả sử số hữu tỷ r thỏa mãn phương trình ***(1)*** với hệ số nguyên $a_0, a_1, \ldots, a_m$. Ta giả thiết $a_0 \neq 0$ và nếu bỏ qua trường hợp $r = 0$ thì có thể giả thiết thêm $a_m \neq 0$. Biểu diễn r dưới dạng $r = k/s$, trong đó s là số tự nhiên, k là số nguyên và $(k, s) = 1.$ Thay $x = k/s$ vào ***(1)*** ta có

$$a_0 k^m = -\left(a_1 k^{m-1} + a_2 k^{m-2} s + \ldots + a_m s^{m-1}\right) s,$$
$$a_m s^m = -\left(a_0 k^{m-1} + a_1 k^{m-2} s + \ldots + a_{m-1} s^{m-1}\right) k.$$

Phương trình thứ nhất chứng tỏ $s \mid a_0 k^m$ mà $(k, s) = 1$ suy ra $s \mid a_0$. Phương trình thứ hai chứng tỏ $k \mid a_m s^m$ mà $(k, s) = 1$ suy ra $k \mid a_m$. Vậy nghiệm hữu tỷ của phương trình ban đầu có thể tìm được bằng hữu hạn các phép thử như sau: lần lượt thay x bởi các phân số tối giản $\frac{k}{s}$ trong đó k là ước số nguyên của a_m và s là ước số tự nhiên của a_0 sau đó tìm xem phân số nào thỏa mãn.

2. Các phương trình Diophante nhiều biến

Đối với các phương trình Diophante nhiều biến có một số vấn đề sau đây được đặt ra: *phương trình có ít nhất một nghiệm nguyên hay không? Số nghiệm nguyên của phương trình là hữu hạn hay vô hạn? Tìm tất cả các nghiệm nguyên của phương trình đó?*

Các vấn đề này có mức độ khó tăng dần theo trình tự được đặt ra ở trên. Đối với một số phương trình thì ta không có câu trả lời cho cả ba câu hỏi nêu trên. Ví dụ hiện nay ta chưa biết phương trình $x^3+y^3+z^3=30$ có nghiệm hay không. Nhưng ta đã tìm được ít nhất bốn nghiệm nguyên của phương trình $x^3+y^3+z^3=3$ là $(x,y,z)=(1,1,1),(4,4,-5),(4,-5,4),(-5,4,4)$. Hơn nữa mặc dù ta chứng minh được phương trình này không còn nghiệm nào khác trong trường hợp $|x+y+z|\le 150000$ (Scarowsky và Boyarsky [1]) nhưng ta vẫn không biết nó còn những nghiệm khác hay không. Mức độ phức tạp của phép giải phương trình này được L.J.Mordell [5] so sánh với sự xuất hiện của các chữ số 1,2,...,9 trong biểu diễn thập phân của π.

Một ví dụ khác, ta biết phương trình $x^3+y^3+z^3=2$ có vô hạn nghiệm nguyên vì ta đã tìm được một họ nghiệm vô hạn của nó là $(x,y,z)=\left(1+6n^3,1-6n^3,-6n^2\right)$ với n là số tự nhiên tùy ý. Nhưng ta vẫn chưa biết đó có phải tất cả các nghiệm của phương trình này hay không. Mặt khác ta có thể chứng minh phương trình $x^3+y^3+z^3=4$ không có nghiệm nguyên bởi vì một lập phương chia cho 9 sẽ có số dư là 0,1 hoặc 8, như thế tổng của hai lập phương khi chia cho 9 sẽ dư 0,1,2,7,8. Do đó tổng của ba lập phương khi chia cho 9 sẽ dư 0,1,2,3,6,7,8 nhưng không thể là 4 hoặc 5. Do đó cả hai phương trình $x^3+y^3+z^3=4$ và $x^3+y^3+z^3=5$ đều không có nghiệm nguyên. Tổng quát hơn, phương trình $x^3+y^3+z^3=k$ là vô nghiệm trong trường hợp k chia 9 dư 4 hoặc 5).

Phương trình $x^3+y^3+z^3=6$ có các nghiệm $(x,y,z)=(-1,-1,2),(-43,-58,65),(-55,-235,236)$ nhưng ta không biết số nghiệm của phương trình này là hữu hạn hay không.

Trong một số trường hợp khó khăn của việc tìm tất cả các nghiệm nguyên của một phương trình chỉ thuần túy là vấn đề tính toán sơ cấp bởi vì ngay cả khi ta đã biết phương pháp tìm tất cả các nghiệm vẫn có thể tốn rất nhiều thời gian để tính toán cụ thể.

Ví dụ xét phương trình $xy=2^{293}-1$. Ta có thể chứng minh được phương trình này có nghiệm không tầm thường (x và y đều lớn hơn 1) nhưng ta không thể tính được cụ thể dù cho trên lý thuyết ta có thể đem $2^{293}-1$ chia lần lượt cho các số nhỏ hơn $2^{293}-1$ để tìm được các ước số của nó. Các tính toán này đòi hỏi rất nhiều thời gian.

Mặt khác ta cũng chưa biết có một phương pháp nào mà sau một quá trình tính toán hữu hạn có thể quyết định rằng phương trình $x^3+y^3+z^3=30$ có thể giải được hay không. Tất nhiên là có thể chứng minh phương trình này không có nghiệm nguyên dương khá dễ dàng.

3. Phương trình $x^2+y^2=z^2$

Ta xét một phương trình đặc biệt bậc hai với ba biến: *phương trình Pythagoras*

(2) $$x^2+y^2=z^2$$

Phương trình này đặc biệt quan trọng trong lĩnh vực tam giác lượng và hình học giải tính. Hơn nữa trường hợp riêng của nó khi $x=y$ có liên quan trực tiếp với chứng minh đơn giản nhất cho sự tồn tại của các số hữu tỷ.

Ta sẽ tìm tất cả các nghiệm hữu tỷ của ***(2)***.

Bỏ qua các nghiệm tầm thường khi một trong các biến x,y triệt tiêu, ta chỉ xét các nghiệm tự nhiên vì dấu của biến số không ảnh hưởng tới phương trình. Nếu x,y,z là các số tự nhiên thỏa

mãn ***(2)*** thì ta nói (x,y,z) là một *bộ số tam giác Pythagoras* (xem thêm cuốn sách nói riêng về các tam giác này được soạn bởi Sierpinski [35]).

Một nghiệm của ***(2)*** được gọi là *nghiệm nguyên thủy* nếu x,y,z là các số tự nhiên và không có ước số chung lớn hơn 1. Nếu ξ,η,ζ là nghiệm nguyên thủy của ***(2)*** và d là số tự nhiên tùy ý thì

(3) $$x=d\xi,\quad y=d\eta,\quad z=d\zeta$$

cũng là nghiệm của ***(2)***.

Ngược lại nếu x,y,z là nghiệm tự nhiên của ***(2)*** thì đặt $(x,y,z)=d$ ta có $x=d\xi, y=d\eta, z=d\zeta$ trong đó $(\xi,\eta,\zeta)=1$ (Chương 1 Định lý 3^a). Thay vào ***(2)*** ta có $(d\xi)^2+(d\eta)^2=(d\zeta)^2$. Chia cả hai vế cho d^2 ta nhận được bộ số ξ,η,ζ là nghiệm nguyên thủy của ***(2)***.

Ta nói rằng nghiệm tự nhiên (x,y,z) của ***(2)*** thuộc lớp thứ d nếu $(x,y,z)=d$. Ta nhận thấy để nhận được tất cả các nghiệm tự nhiên thuộc lớp d ta chỉ cần nhân tất cả các nghiệm nguyên thủy của ***(2)*** với d. Vì vậy ta chỉ cần tìm tất cả các nghiệm nguyên thủy của ***(2)***.

Giả sử rằng x,y,z là nghiệm nguyên thủy của ***(2)***. Ta chứng minh rằng một trong các số x,y là chẵn và số còn lại là lẻ. Giả sử ngược lại nghĩa là cả hai số đó là cùng chẵn hoặc cùng lẻ. Trong trường hợp đầu tiên thì $x^2+y^2=z^2$ chẵn do đó z chẵn và vì vậy x,y,z có ước chung là 2, mâu thuẫn. Để chỉ ra trường hợp thứ hai cũng không xảy ra ta chứng minh rằng bình phương của một số lẻ chia cho 8 dư 1. Thật vậy, một số lẻ bất kỳ sẽ có dạng $2k-1$ với k nguyên nào đó. Ta có biểu diễn $(2k-1)^2=4k^2-4k+1=4k(k-1)+1$. Do một trong hai số k và $k-1$ là số chẵn nên nó chia hết cho 2 vì vậy $4k(k-1)$ chia hết cho 8 và do đó $(2k-1)^2$ chia 8 dư 1. Hệ quả là tổng của hai bình phương lẻ chia 8 dư 2. Suy ra tổng của hai bình phương lẻ không thể là một bình phương lẻ và cũng không thể là một bình phương chẵn vì một bình phương chẵn sẽ chia hết cho 4 nên chia 8 chỉ có thể dư 0 hoặc 4. Điều phải chứng minh.

Ta có thể giả thiết y là chẵn và x là lẻ. Khi đó z cũng là lẻ. Phương trình ***(2)*** có thể viết dưới dạng

(4) $$y^2=(z+x)(z-x).$$

Các số $z+x$ và $z-x$ là tổng và hiệu của hai số lẻ nên bản thân chúng đều là số chẵn. Đặt

(5) $$z+x=2,\qquad z-x=2b,$$

trong đó a và b là các số tự nhiên. Vì vậy $z=a+b, x=a-b$. Các đẳng thức này suy ra a và b nguyên tố cùng nhau vì nếu ngược lại ta giả sử chúng có ước số chung $\delta>1$ thì $z=k\delta, x=l\delta$ trong đó k và l là các số tự nhiên. Khi đó $y^2=z^2-x^2=(k^2-l^2)\delta^2$ trong đó y^2 chia hết cho δ^2 suy ra y chia hết cho δ (Chương 1 mục 6 Hệ quả 2). Điều này mâu thuẫn với giả thiết x,y,z là nghiệm nguyên thủy vì $\delta>1$ lại trở thành ước số chung lớn hơn 1 của x,y,z.

Theo giả thiết y chẵn nên $y=2c$ trong đó c là số tự nhiên nào đó. Thay vào ***(5)*** và rút gọn, phương trình ***(4)*** trở thành

(6) $$c^2=ab.$$

Nhưng do $(a,b)=1$, áp dụng Định lý 8 Chương 1, đẳng thức ***(6)*** suy ra các số a,b đều là bình phương. Nghĩa là $a=m^2, b=n^2$, trong đó m, n là số tự nhiên và $(m,n)=1$ (do $(a,b)=1$). Vì vậy

$$z=a+b=m^2+n^2,\qquad x=a-b=m^2-n^2,$$

và do $c^2=ab=m^2n^2$ mà y = 2c nên y = 2mn.

Vậy ta đã chứng minh được nếu x,y,z là nghiệm nguyên thủy của ***(2)*** và y là số chẵn thì

(7) $$x=m^2-n^2,\quad y=2mn,\quad z=m^2+n^2,$$

trong đó m,n là số tự nhiên với $(m,n)=1$ và $m>n$ vì x là số tự nhiên. Hơn nữa một trong các số m,n là chẵn, số còn lại là lẻ. Thật vậy, chúng không thể cùng chẵn vì chúng nguyên tố cùng nhau. Chũng cũng không thể cùng lẻ bởi vì nếu chúng cùng lẻ thì từ ***(7)*** suy ra tất cả các số x,y,z phải chẵn, mâu thuẫn với $(x,y,z)=1$. Vậy $2\mid mn$ suy ra $y=2mn$ chia hết cho 4.

Ta chứng mnh điều ngược lại cũng đúng, nghĩa là nếu m,n là hai số tự nhiên nguyên tố cùng nhau, $m>n$ và một trong hai số là lẻ, số còn lại là chẵn thì các số x,y,z nhận được từ m,n theo công thức ***(7)*** trở thành nghiệm nguyên thủy của ***(2)***.

Đầu tiên ta chú ý rằng các số x,y,z thu được bởi công thức ***(7)***, m,n là các số tự nhiên và $m>n$ trở thành nghiệm của ***(2)***. Ta chỉ cần kiểm tra rằng

(8) $$\left(m^2-n^2\right)^2+\left(2mn\right)^2=\left(m^2+n^2\right)^2.$$

Bây giờ sử dụng giả thiết m,n nguyên tố cùng nhau ta chứng minh $(x,y,z)=1$. Giả sử ngược lại thì tồn tại ước số chung $\delta>1$ của các số x,y,z. Số δ không thể chẵn vì $z=m^2+n^2$ là tổng của một bình phương lẻ và một bình phương chẵn sẽ là lẻ. Nhưng theo ***(7)***

(9) $$2m^2=x+z,\quad 2n^2=z-x;$$

Do đó m^2 và n^2 đều chia hết cho δ. Điều này không thể vì $(m,n)=1$ suy ra $\left(m^2,n^2\right)=1$. Công thức ***(9)*** chứng tỏ rằng ứng với các số m,n khác nhau ta có các nghiệm x,y,z khác nhau. Các kết quả trên dẫn ta tới với định lý sau đây

Định lý 1. *Tất cả các nghiệm nguyên thủy của phương trình* $x^2+y^2=z^2$ *với* y *chẵn được cho bởi*

(10) $$x=m^2-n^2,\quad y=2mn,\quad z=m^2+n^2,$$

với m,n *là các số tự nhiên nguyên tố cùng nhau và trong đó có một số chẵn, một số lẻ,* $m>n$.

J.Ginsburg [1] đã lưu ý đối với một nghiệm nguyên thủy của phương trình $x^2+y^2=z^2$ thì để liệt kê một cách có hệ thống các cặp số m,n thỏa mãn điều kiện trong Định lý 1 (đôi khi còn gọi là phần tử sinh của nghiệm) thì chỉ cần xét tỷ số $(x+z)/y$ như là một phân số tối giản m/n là đủ.

Để liệt kê một cách trình tự tất cả các nghiệm nguyên thủy của ***(2)*** ta lần lượt xét các giá trị 2, 3, 4, ... của m và với mỗi giá trị đó ta xét các số n nguyên tố cùng nhau với m, nhỏ hơn m và là số chẵn nếu m lẻ. Theo cách này ta có bảng 20 nghiệm nguyên thủy đầu tiên như sau

m	n	x	y	z	diện tích	m	n	x	y	z	diện tích
2	1	3	4	5	6	7	6	13	84	85	546
3	2	5	12	13	30	8	1	63	16	65	504
4	1	15	8	17	60	8	3	55	48	73	1320
4	3	7	24	25	84	8	5	39	80	89	1560
5	2	21	20	29	210	8	7	15	112	113	840
5	4	9	40	41	180	9	2	77	36	85	1386
6	1	35	12	37	210	9	4	65	72	97	2340
6	5	11	60	61	330	9	8	17	144	145	1224
7	2	45	28	53	630	10	1	99	20	101	990
7	4	33	56	65	924	10	3	91	60	109	2730

Như đã biết để thu được tất cả các nghiệm tự nhiên của phương trình ***(2)*** ta phải nhân mỗi nghiệm nguyên thủy lần lượt với các số tự nhiên 1, 2, 3,... rồi bổ sung thêm nghiệm bằng cách đổi vai trò của x và y. Hơn nữa mọi nghiệm tự nhiên của ***(2)*** sẽ thu được một lần duy nhất theo cách này.

Mặt khác theo đẳng thức ***(8)*** thì khi thay các số tự nhiên m,n với $m>n$ vào công thức ***(7)*** ta thu được nghiệm tự nhiên của ***(2)***. Theo cách này thì dù cho bổ sung thêm các nghiệm bằng cách đổi vai trò của x và y ta cũng không thu được tất cả các nghiệm tự nhiên của ***(2)***. Chẳng hạn ta không thể thu được từ ***(7)*** nghiệm 9,12,15 do không tồn tại số tự nhiên m và $n<m$ thỏa mãn $15=m^2+n^2$ (bởi vì không có số nào trong các số $15-1^2=14, 15-2^2=11, 15-3^2=6$ là bình phương đúng).

Tất cả các nghiệm của ***(2)*** được cho bởi công thức sau đây

$$x=\left(m^2-n^2\right)l, \qquad y=2mnl, \qquad z=\left(m^2+n^2\right)l,$$

trong đó $m, n<m$ và l là số tự nhiên, sau đó bổ sung thêm các nghiệm thu được bằng cách đổi vai trò x và y. Tuy nhiên công thức ở trên lại cho các nghiệm trùng nhau đối với một số bộ số m,n,l khác nhau. Chẳng hạn nghiệm 12,16,20 thu được khi $m=2,\ n=1,\ l=4$ và $m=4,\ n=2,\ l=1$. Nghiệm 48,64,80 thu được khi $m=8,\ n=4,\ l=1;\ \ m=4,\ n=2,\ l=4$ và $m=2,\ n=1,\ l=16.$

Nghiệm đầu tiên được liệt kê trong bảng ở trên là nghiệm của phương trình ***(2)*** với x,y,z là các số tự nhiên nhỏ nhất có thể. Hơn nữa trong nghiệm này thì các số x,y,z còn là số tự nhiên liên tiếp. Không khó để chứng minh đó chính là nghiệm duy nhất chứa các số tự nhiên liên tiếp. Thật vậy, nếu ba số tự nhiên liên tiếp $n-1,n,n+1$ thỏa mãn phương trình $\left(n-1\right)^2+n^2=\left(n+1\right)^2$ thì $n^2=4n$ suy ra $n=4$ và ta thu lại nghiệm 3,4,5. Dễ dàng chứng minh phương trình $3^n+4^n=5^n$ không có nghiệm tự nhiên n nào trừ nghiệm $n=2$. Thật vậy, ta có $3+4>5$ do đó $n=1$ không phải nghiệm cần tìm. Hơn nữa $3^2+4^2=5^2$ và với $n>2$ thì

$$5^n=5^2\cdot5^{n-2}=3^2\cdot5^{n-2}+4^2\cdot5^{n-2}>3^2\cdot3^{n-2}+4^2\cdot4^{n-2}=3^n+4^n.$$

Vì vậy $3^n+4^n\neq5^n$ với mọi $n>2$. Tương tự ta chứng minh được nếu $a^2+b^2=c^2$ thì $a^n+b^n<c^n$ với mọi $n>2$. Mặt khác phương trình $3^x+4^y=5^z$ chỉ có nghiệm tự nhiên duy nhất $x=y=z=2$ nhưng chứng minh điều này không dễ (Sierpinski [17], Nagell [11]).

L.Jesmanowicz [1] đã chứng minh các phương trình $5^x+12^y=13^z$, $7^2+24^y=25^z$, $9^x+40^y=41^z$, $11^x+60^y=61^z$ chỉ có nghiệm tự nhiên $x=y=z=2$ và từ đó đặt ra câu hỏi rằng có tồn tại các số tự nhiên a,b,c thỏa mãn $a^2+b^2=c^2$ mà phương trình $a^x+b^y=c^z$ có nhiều hơn một nghiệm $x=y=z=2$ hay không (Ko Chao [2],[3],[4]).

Ngoài ra ta đã biết có vô hạn các bộ số Pythagoras nguyên thủy $\left(a,b,c\right)$ mà phương trình $a^x+b^y=c^z$ chỉ có đúng một nghiệm tự nhiên $x=y=z=2$ (Lu Wen Twan [1], Jozefiak [2], Podsypanin [1], Demyanenko [1]).

Ta đã chứng minh rằng với mỗi nghiệm nguyên thủy của ***(2)*** thì số chẵn trong các số x,y sẽ chia hết cho 4. Vì vậy trong mọi nghiệm x,y,z của ***(2)*** thì có ít nhất một trong hai số x,y chia hết cho 4. Ta sẽ chứng minh trong hai số đó cũng có một số chia hết cho 3. Giả sử ngược lại ta viết $x=3k\pm1,\ y=3l\pm1,\ k$ và l là số nguyên. Vì vậy $x^2+y^2=3\left(3k^2+3l^2\pm2k\pm2l\right)+2$. Nhưng đây không thể là bình phương đúng vì bình phương của một số chỉ có thể chia hết cho 3 hoặc chia 3 dư 1, điều này là hiển nhiên vì ta có biểu diễn $\left(3t\pm1\right)^2=3\left(3t^2\pm2t\right)+1$.

Bây giờ ta sẽ chứng minh rằng trong mọi nghiệm tự nhiên của ***(2)*** thì ít nhất một trong các số x,y,z chia hết cho 5. Để chứng minh điều này ta hãy xét một số nguyên tùy ý m không chia hết

cho 5. Ta có $m=5k\pm 1$ hoặc $m=5k\pm 2$ trong đó k là số nguyên nào đó. Trong trường hợp thứ nhất thì $m^2=5\left(5k^2\pm 2k\right)+1$ và trong trường hợp thứ hai $m^2=5\left(5k^2\pm 4k\right)+4$. Như thế bình phương của một số không chia hết cho 5 khi chia cho 5 sẽ có số dư là 1 hoặc 4. Bây giờ giả sử x,y,z đều không chia hết cho 5 thì khi đó x^2 và y^2 chia 5 dư 1 hoặc 4 suy ra x^2+y^2 chia 5 dư 2,3 hoặc 0. Do $x^2+y^2=z^2$ nên loại trừ hai trường hợp đầu tiên vì z^2 chia 5 không thể có số dư là 2 hoặc 3. Vì vậy trường hợp thứ ba phải xảy ra. Suy ra z chia hết cho 5. Điều phải chứng minh.

Do $(3,4,5)$ là tam giác Pythagoras suy ra các số 1,2,3,4,5 là tất cả các số tự nhiên n mà ta có thể kết luận rằng mọi bộ số Pythagoras đều có ít nhất một cạnh chia hết cho n.

Bây giờ ta sẽ tìm tất cả các nghiệm của ***(2)*** mà hai trong số các số x,y,z là số tự nhiên liên tiếp. Rõ ràng các nghiệm như thế đều là nghiệm nguyên thủy. Vì vậy z là số lẻ và $z-y=1$ chỉ có thể xảy ra khi y chẵn. Do đó theo ***(10)*** ta có $m^2+n^2-2mn=z-y=1$ hoặc tương đương $(m-2)^2=1$ trong đó từ $m>n$ suy ra $m-n=1$ nghĩa là $m=n+1$. Vì vậy $x=m^2-n^2=(n+1)^2-n^2=2n+1$, $y=2n(n+1)$, $z=y+1=2n(n+1)+1$. Do đó tất cả các nghiệm của ***(2)*** mà $z-y=1$ đều được cho bởi công thức $x=2n+1,\ y=2n(n+1),\ z=2n(n+1)+1$ với $n=1,2,3,\ldots$

Dưới đây là 10 nghiệm đầu tiên

n	x	y	z
1	3	4	5
2	5	12	13
3	7	24	25
4	9	40	41
5	11	60	61

n	x	y	z
6	13	84	85
7	15	112	113
8	17	144	146
9	19	180	181
10	21	220	221

Và một số nghiệm khác thuộc dạng này

n	x	y	z
10	21	220	221
100	201	20200	20201
1000	2001	2002000	2002001

n	x	y	z
20	41	840	8004001
200	401	80400	80401
2000	4001	8004000	8004001

Về các nghiệm này xem thêm Willey [1]. Tiếp theo ta xét trường hợp $x-y=\pm 1$.

4. Nghiệm tự nhiên của phương trình $x^2+y^2=z^2$ với $x-y=\pm 1$

Trong các nghiệm nguyên thủy của ***(2)*** được liệt kê trong mục 3 ta chú ý hai nghiệm 3,4,5 và 21,20,29. Dễ dàng chứng minh rằng có vô hạn nghiệm thỏa mãn tính chất trong mục này. Thật vậy, nếu ta có hai số tự nhiên x và z thỏa mãn $x^2+(x+1)^2=z^2$ thì ta có

$$(3x+2z+1)^2+(3x+2z+2)^2=(4x+3z+2)^2.$$

Thật vậy, ta có $(3x+2z+1)^2+(3x+2z+2)^2=18x^2+24xz+8z^2+18x+12z+5$

Từ $x^2+(x+1)^2=z^2$ suy ra $2x^2+2x+1=z^2$ trong đó

$$(3x+2z+1)^2+(3x+2z+2)^2=16x^2+24xz+9z^2+16x+12z+4$$
$$=(4x+3z+2)^2.$$

Vì vậy từ một tam giác Pythagoras cho trước gồm hai cạnh góc vuông là hai số tự nhiên liên tiếp thì ta có thể thu được một tam giác Pythagoras khác với cùng tính chất. Bắt đầu với tam giác nguyên thủy 3,4,5 ta thu được tam giác mới có các cạnh là $3\cdot3+2\cdot5+1=20$, 21 và $4\cdot3+3\cdot5+2=29$. Tương tự từ tam giác mới này ta thu được tam giác với các cạnh $3\cdot20+2\cdot29+1=119$, 120 và $4\cdot20+3\cdot29+2=169$. Dưới đây là sáu tam giác đầu tiên thu được theo cách này

3	4	5
20	21	29
119	120	169
696	697	985
4059	4060	5741
23660	23661	33461

Không khó để chứng minh rằng quá trình này cho một dãy các tam giác mà cạnh góc vuông có độ dài lớn hơn sẽ lần lượt là chẵn và lẻ. Đặt $x_1=3, y_1=4, z_1=5$ và với $n=1,2,3,\ldots$ đặt

(11) $$x_{n+1}=3x_n+2z_n+1,\ y_{n+1}=x_{n+1}+1,\ z_{n+1}=4x_n+3z_n+2.$$

Ta sẽ chứng minh $(x_n,y_n,z_n)(n=1,2,\ldots)$ đều là các tam giác Pythagoras với các cạnh góc vuông là các số tự nhiên liên tiếp.

Bổ đề. *Nếu các số tự nhiên x,z thỏa mãn phương trình*

(12) $$x^2+(x+1)^2=z^2$$

và nếu $x>3$ thì

(13) $$x_0=3x-2z+1,\qquad z_0=3z-4x-2$$

là các số tự nhiên thỏa mãn phương trình

(14) $$x_0^2+(x_0+1)^2=z_0^2,$$

và $z_0<z$.

Chứng minh. Theo ***(13)*** ta có

(15) $$x_0^2+(x_0+1)^2=2x_0^2+2x_0+1=18x^2+8z^2-24xz+18x-12z+5,$$
$$z_0^2=16x^2+9z^2-24xz+16x-12z+4.$$

Theo ***(2)*** thì $z^2=2x^2+2x+1$. Ta có

$$16x^2+9z^2+24xz+16x-12z+4=8z^2+18x^2-24xz+18x-12z+5$$

Và từ ***(15)*** suy ra ***(14)***.

Theo ***(13)*** ta cần chứng minh x_0,z_0 là các số tự nhiên và $z_0<z$.

Tức là cần chứng minh $3x-2z+1>0$ và $0<3z-4x-2<z$ hoặc tương đương

(16) $$2z<3x+1,\quad 3z>4x+2 \quad \text{và} \quad z<2x+1.$$

Do $x>3$ suy ra $x^2>3x=2x+3$. Theo ***(12)*** thì

$$4z^2=8x^2+8x+4=9x^2+8x+4-x^2<$$
$$<9x^2+8x+4-(2x+3)=9x^2+6x+1=(3x+1)^2.$$

Suy ra $2z<3x+1$ và do $x>0$, $2z<4x+1$ ta có $z<2x+1$. Sử dụng ***(12)*** và $x>0$ suy ra

$$9z^2=18x^2+18x+9>16x^2+16x+4=(4x+2)^2,$$

trong đó $3z>4x+2$ và ta chứng minh được ***(16)***. Bổ đề được chứng minh. □

Bây giờ giả sử tồn tại các tam giác Pythagoras $(x,\ x+1,\ z)$ khác với các tam giác $(x_n,\ x_n+1,\ z_n)$ định nghĩa ở trên. Trong số các tam giác như vậy tồn tại tam giác (x,y,z) với z nhỏ nhất. Khi đó x không thể nhỏ hơn hoặc bằng 3 bởi vì nếu ngược lại ta có $(x,y,z)=(3,4,5)$. Đặt

(17) $$u=3x-2z+1,\ v=3z-4x-2.$$

Theo bổ đề thì $(u,\ u+1,v)$ là tam giác Pythagoras với $v<z$. Do z là nhỏ nhất trong các tam giác Pythagoras không có dạng (x_n,x_n+1,z_n) nên với n nào đó ta có $u=x_n$, $v=z_n$ và

$$x_{n+1}=3u+2v+1,\ y_{n+1}=x_{n+1}+1,\ z_{n+1}=4u+3v+2.$$

Vì vậy, theo ***(17)*** $$x_{n+1}=3(3x-2z+1)+2(3z-4x-2)+1=x,$$
$$z_{n+1}=4(3x-2z+1)+3(3z-4x-2)+2=z.$$

Do đó tam giác $(x,x+1,z)$ lại là một trong số các tam giác (x_n,y_n,z_n). Mâu thuẫn. Vậy ta đã chứng minh được các tam giác (x_n,x_n+1,z_n) $(n=1,2,...)$ là tất cả các tam giác Pythagoras mà trong đó hai cạnh góc vuông là các số tự nhiên liên tiếp.

Có thể chứng minh được nếu dãy vô hạn $u_1,u_2,...$ và $v_1,v_2,...$ được định nghĩa như sau: $u_0=0$, $u_1=3$, $u_{n+1}=6u_n-u_{n-1}+2$ với $n=1,2,...$ và $v_0=1$, $v_1=5$, $v_{n+1}=6v_n-v_{n-1}$ với $n=1,2,...,$ thì $u_n^2+(u_n+1)^2=v_n^2$ với $n=1,2,...,$ và (u_n,u_n+1,v_n) là tam giác thứ *n* trong dãy ***(11)***.

Ta cũng có thể chứng minh rằng nếu $(1+\sqrt{2})^{2n+1}=a_n+b_n\sqrt{2}$ với $n=1,2,...,a_n$ và b_n là các số nguyên thì $\left(\frac{a_n+(-1)^n}{2},\frac{a_n-(-1)^n}{2},b_n\right)$ là tam giác thứ *n* trong dãy ***(11)***.

Bây giờ ta giả sử các số tự nhiên x và z thỏa mãn ***(12)***. Do một trong hai số $x,x+1$ là chẵn, số còn lại là lẻ, z là lẻ và rõ ràng $z>x+1$. Hơn nữa $z^2<(2x+1)^2$. Vì thế $u=z-x-1$ và $v=\frac{1}{2}(2x+1-z)$ là các số tự nhiên. Vì vậy theo đẳng thức

$$\frac{(z-x-1)(z-x)}{2}-\left(x+\frac{(1-z)}{2}\right)^2=\frac{1}{4}\left(z^2-x^2-(x+1)^2\right)$$

và $x^2+(x+1)^2=z^2$ ta thu được

(18) $$\frac{1}{2}u(u+1)=v^2.$$

Số $t_u = \frac{1}{2}u(u+1)$ với u là số tự nhiên được gọi là *số tam giác* (xem mục 16).

Công thức ***(18)*** chứng tỏ rằng số tam giác là một bình phương đúng.

Vì vậy ứng với mỗi nghiệm tự nhiên của phương trình $x^2+(x+1)^2=z^2$ đều cho một nghiệm tự nhiên của ***(18)*** bằng cách đặt $u=z-x-1,\ v=x+(1-z)/2$. Điều ngược lại cũng đúng: nếu nghiệm tự nhiên u và v thỏa mãn ***(18)*** thì ta đặt $x=u+2v,\ z=2u+2v+1$. Sử dụng đẳng thức

$$(u+2v)^2+(u+2v+1)^2-(2u+2v+1)^2=4\left(v^2-\frac{1}{2}u(u+1)\right)$$

Ta thu được nghiệm của phương trình $x^2+(x+1)^2=z^2$ và $u=z-x-1,\ v=\frac{1}{2}(2x+1-z)$. Như vậy các công thức này biến đổi tất cả các nghiệm tự nhiên x,z của phương trình $x^2+(x+1)^2=z^2$ thành tất cả các nghiệm tự nhiên u và v của ***(18)*** hoặc nói cách khác là thành tất cả các số tam giác là bình phương đúng. Từ đây suy ra tính vô hạn của các số tam giác loại này. Ta liệt kê sáu số tam giác như thế

$$t_1=1^2,\ t_8=6^2,\ t_{49}=35^2,\ t_{288}=204^2,\ t_{1681}=1189^2,\ t_{9800}=6930^2.$$

Suy ra đẳng thức

(19) $$(2z-2x-1)^2-2(2x-z+1)^2-1=2\left(z^2-x^2-(x+1)^2\right)$$

Nghĩa là nếu các số tự nhiên $x,\ z$ thỏa mãn ***(12)*** thì đặt

(20) $$a=2z-2x-1, b=2x-z+1,$$

Ta thu được

(21) $$a^2-2b^2=1,$$

với a,b là các số tự nhiên vì theo ***(12)*** ta có $z<2x+1$ và $4z^2>(2x+1)^2$ trong đó $2z>2x+1$. Công thức ***(20)*** tương đương với

(22) $$x=b+\frac{1}{2}(a-1), z=a+b.$$

Nếu a và b là các số tự nhiên và thỏa mãn ***(21)*** thì a là số lẻ lớn hơn 1 và các số được cho bởi ***(22)*** đều là số tự nhiên. Hơn nữa từ ***(20)*** suy ra ***(22)*** nên theo ***(21)***, ***(20)*** và ***(19)*** ta thấy x và z thỏa mãn ***(12)***. Vậy từ tất cả các nghiệm tự nhiên x,z của ***(12)***, sử dụng công thức ***(20)***, ta thu được tất cả các nghiệm tự nhiên a và b của ***(21)***. Bốn nghiệm đầu tiên của ***(12)*** được liệt kê ở trên cho ta bốn nghiệm (a,b) của phương trình $(21):(3,2),\ (17,12),\ (99,70),\ (577,408)$.

Ngược lại, từ tất cả các nghiệm tự nhiên của ***(21)***, sử dụng công thức ***(22)*** ta thu được tất cả các nghiệm của phương trình ***(12)***.

5. Các tam giác Pythagoras có cùng diện tích

Từ danh sách các tam giác Pythagoras được liệt kê trong mục 1 ta nhận thấy các tam giác (21, 20, 29) và (35, 12, 37) có cùng diện tích (210 đơn vị diện tích) và vì thế có ít nhất hai tam giác nguyên thủy Pythagoras với cạnh huyền khác nhau có cùng diện tích.

Xét các tam giác không nguyên thủy với cạnh huyền ≤ 37 ta nhận được 8 tam giác $(6,8,10)$, $(9,12,15)$, $(12,16,20)$, $(15,20,25)$, $(10,24,26)$, $(18,24,30)$, $(30,16,34)$, $(21,28,35)$ với diện tích

lần lượt là 24, 54, 96, 150, 120, 216, 240, 294. Vì vậy ta nhận thấy không có cặp tam giác nào trong các tam giác Pythagoras với cạnh huyền ≤ 37 có cùng diện tích trừ cặp $(21,20,29)$, $(35,12,37)$.

Ta chú ý rằng nếu hai tam giác Pythagoras có cùng diện tích và các cạnh huyền bằng nhau thì chúng trùng nhau. Thật vậy, nếu (a_1,b_1,c_1) và (a_2,b_2,c_2) là cặp tam giác như vậy với $a_1 \ge b_1$, $a_2 \ge b_2$ thì theo giả thiết ta có các đẳng thức $a_1 b_1 = a_2 b_2$ và $c_1 = c_2$ trong đó $a_1^2 + b_1^2 = a_2^2 + b_2^2$ suy ra $(a_1 - b_1)^2 = (a_2 - b_2)^2$ và $(a_1 + b_1)^2 = (a_2 + b_2)^2$ với $a_1 - b_1 = a_2 - b_2$ và $a_1 + b_1 = a_2 + b_2$ suy ra $a_1 = a_2$ và $b_1 = b_2$.

Theo danh sách trong mục 3 ta xét tam giác Pythagoras (15, 112, 113). Tam giác này có diện tích là $840 = 4 \cdot 210$ tức là bốn lần lớn hơn diện tích tam giác (21, 20, 29) và (35, 12, 37). Nhân hai vế của các tam giác đó lên hai lần ta lần lượt thu được hai tam giác (42, 40, 58) và (70, 24, 74) với diện tích đúng bằng 840. Vì vậy ta nhận được ba tam giác Pythagoras (15, 112, 113), (42, 40, 58), (70, 24, 74) đều có cùng diện tích. Tất cả các tam giác này đều không nguyên thủy. Ta đã biết rằng diện tích chung nhỏ nhất của ba tam giác nguyên thủy là 13123110 và các tam giác đó là (4485, 5852, 7373), (19019, 1390, 19069), (3059, 8580, 9089). Các phần tử sinh tương ứng lần lượt là (39, 38), (138, 5), (78, 55). Câu hỏi đặt ra là khi nào thì tồn tại một số lượng lớn các tam giác Pythagoras có cùng diện tích và có cạnh huyền khác nhau. Kết quả cho câu hỏi này có trong định lý sau đây.

Định lý 2 (Fermat). *Với mọi số tự nhiên n đều tồn tại n tam giác Pythagoras có cùng diện tích và các cạnh huyền khác nhau.*

Định lý được chứng minh bằng quy nạp dựa trên kết quả sau đây

Bổ đề. *Cho trước n tam giác Pythagoras có cùng diện tích và các cạnh huyền khác nhau. Ta có có thể xây dựng $n+1$ tam giác Pythagoras với cùng diện tích và cạnh huyền khác nhau trong đó ít nhất có một tam giác có cạnh huyền lẻ.*

Chứng minh. Cho trước số tự nhiên n. Giả sử (a_k,b_k,c_k) với $a_k < b_k < c_k$, $k = 1,2,\ldots,n$ là n tam giác Pythagoras với cùng diện tích và các cạnh huyền khác nhau, hơn nữa c_1 lẻ. Đặt

(23) $$a'_k = 2c_1\left(b_1^2 - a_1^2\right)a_k,\ b'_k = 2c_1\left(b_1^2 - a_1^2\right)b_k,$$

$$c'_k = 2c_1\left(b_1^2 - a_1^2\right)c_k,\ \text{với } k = 1,2,\ldots,n$$

(24) $$a'_{n+1} = \left(b_1^2 - a_1^2\right)^2,\ b'_{n+1} = 4a_1 b_1 c_1^2,\ c'_{n+1} = 4a_1^2 b_1^2 + c_1^4.$$

với $k = 1,2,\ldots,n$. Khi đó các tam giác (a'_k,b'_k,c'_k) đều là tam giác Pythagoras do chúng lần lượt đồng dạng với các tam giác (a_k,b_k,c_k), $k = 1,2,\ldots,n$. Hơn nữa $(a'_{n+1},b'_{n+1},c'_{n+1})$ cũng là tam giác Pythagoras. Điều này được suy trực tiếp từ ***(24)***, phương trình $a_1^2 + b_1^2 = c_1^2$ và đẳng thức

$$\left(b^2 - a^2\right)^4 + 16a^2b^2\left(a^2 + b^2\right)^2 = \left(4a^2b^2 + \left(a^2 + b^2\right)^2\right)^2.$$

Bây giờ ta chứng minh các tam giác (a'_k,b'_k,c'_k) với $k = 1,2,\ldots,n+1$ thỏa mãn các điều kiện còn lại. Kí hiệu Δ là diện tích của các tam giác (a_k,b_k,c_k), $k = 1,2,\ldots,n$. Ta có $a_k b_k = 2\Delta$ với $k = 1,2,\ldots,n$. Diện tích của các tam giác (a'_k,b'_k,c'_k) với $k = 1,2,\ldots,n$ theo ***(23)*** sẽ bằng $\frac{1}{2}a'_k b'_k = 2c_1^2\left(b_1^2 - a_1^2\right)^2 a_k b_k = 4c_1^2\left(b_1^2 - a_1^2\right)^2\Delta$. Diện tích của tam giác $(a'_{n+1},b'_{n+1},c'_{n+1})$, theo ***(24)***, bằng với $\frac{1}{2}a'_{n+1}b'_{n+1} = 2\left(b_1^2 - a_1^2\right)^2 c_1^2 a_1 b_1 = 4c_1^2\left(b_1^2 - a_1^2\right)^2\Delta$. Vì vậy các tam giác (a'_k,b'_k,c'_k) với $k = 1,2,\ldots,n+1$ đều có cùng diện tích. Để chứng minh rằng cạnh huyền của các tam giác này đều

khác nhau ta chú ý rằng các số $c_k, k=1,2,\ldots,n,$ đều khác nhau. Mặt khác theo ***(23)***, $c_k^{'}\ (k\le n)$ đều là số chẵn. Ta lại có theo ***(24)*** thì số $c_{n+1}^{'}$ là lẻ do c_1 lẻ. Bổ đề được chứng minh. □

Áp dụng bổ đề cho trường hợp $n=1$. Tam giác Pythagoras nhỏ nhất được áp dụng trong bổ đề là $(3,4,5)$. Ta có hai tam giác có cùng diện tích $\left(a_1^{'},b_1^{'},c_1^{'}\right)$ và $\left(a_2^{'},b_2^{'},c_2^{'}\right)$ thì theo ***(23)*** ta có $2\left(b_1^2-a_1^2\right)c_1=2\cdot 7\cdot 5=70$ và do đó $a_1^{'}=3\cdot 70=210,\ b_1^{'}=4\cdot 70=280,\ c_1^{'}=5\cdot 70=350$. Nên theo ***(24)*** thì $a_2^{'}=\left(4^2-3^2\right)^2=49,\ b_2^{'}=4\cdot 3\cdot 4\cdot 5^2=1200,\ c_2^{'}=4\cdot 3^2\cdot 4^2+5^2=1201$. Ta có hai tam giác Pythagoras cần tìm là (210, 280, 350) và (49, 1200, 1201) có cùng diện tích là 29400 và các cạnh huyền khác nhau, một trong số đó là lẻ. Áp dụng bổ đề lần nữa cho hai tam giác này ta thu được ba tam giác Pythagoras với cạnh huyền khác nhau và cùng diện tích nhưng các cạnh của chúng đều lớn hơn 10^{10}. Mặt khác, sử dụng một phương pháp khác ta đã tìm ra ba tam giác như vậy nhưng các cạnh đều nhỏ hơn 10^4. Hơn nữa cũng tồn tại bốn tam giác Pythagoras với cạnh huyền khác nhau và có cùng diện tích với độ dài các cạnh đều nhỏ hơn 10^5. Đó là các tam giác $(518,\ 1320,\ 1418)$, $(280,\ 2442,\ 2458)$, $(231,\ 2960,\ 2969)$, $(111,\ 6160,\ 6161)$ và diện tích chung của chúng là 314880. Năm tam giác Pythagoras với cạnh nhỏ hơn 10^6 có cạnh huyền khác nhau và có cùng diện tích là các tam giác phân biệt $(2805, 52416, 52491)$, $(3168, 46410, 46518)$, $(5236, 14040, 28564)$, $(6006,\ 24480,\ 25206)$, $(8580, 17136, 19164)$ với diện tích chung 73513440.

Hiển nhiên là chỉ tồn tại hữu hạn tam giác với diện tích Δ cho trước. Hơn nữa các cạnh góc vuông của tam giác đó phải là ước số của 2Δ.

Mặt khác từ bổ đề dễ dàng suy ra tồn tại vô hạn các tam giác vuông với cạnh hữu tỷ và diện tích là 6. Thật vậy, từ chứng minh của bổ đề suy ra nếu ta có n tam giác Pythagoras có cùng diện tích Δ với các cạnh huyền phân biệt và một trong số chúng là lẻ thì tồn tại $n+1$ tam giác Pythagoras có cùng diện tích Δd^2 với cạnh huyền phân biệt và một trong số chúng là lẻ, trong đó d là một số tự nhiên. Bắt đầu với tam giác $(3,\ 4,\ 5)$ và sử dụng bổ đề $n-1$ lần ta thu được n tam giác Pythagoras với cạnh huyền phân biệt và có cùng diện tích là $6m^2$, trong đó m là số tự nhiên phụ thuộc vào n. Chia tất cả các cạnh của các tam giác này cho m ta nhận được n tam giác vuông không trùng nhau với độ dài các cạnh hữu tỷ và diện tích đều bằng 6. Do n là số tự nhiên tùy ý nên ta suy ra số tam giác vuông có cạnh hữu tỷ và diện tích bằng 6 không thể hữu hạn được.

Có thể chứng minh khá đơn giản rằng với mọi số tự nhiên n đều tồn tại $\ge n$ tam giác Pythagoras không trùng nhau với cùng chu vi. Thật vậy, không có hai tam giác nguyên thủy không trùng nhau nào là đồng dạng, nhưng số tam giác như vậy là vô hạn, ta có thể chọn n tam giác không trùng nhau $\left(a_k,b_k,c_k\right)\ (k=1,2,\ldots,n)$ như vậy và đặt $a_k+b_k+c_k=s_k$ với $k=1,2,\ldots,n$.

Với $k=1,2,\ldots,n$ đặt

$$s=s_1\,s_2\ldots s_n,\qquad a_k^{'}=\frac{a_k s}{s_k},\ \ b_k^{'}=\frac{b_k s}{s_k},\quad c_k^{'}=\frac{c_k s}{s_k}.$$

Ta có $a_k^{'}+b_k^{'}+c_k^{'}=s$ với $k=\ 1,\ 2,\ldots,n$ và hơn nữa không có cặp $\left(a_k^{'},b_k^{'},c_k^{'}\right)\ (k=1,2,\ldots,n)$ nào đồng dạng. Do đó chúng cũng không trùng nhau. Danh sách tất cả các tam giác Pythagoras nguyên thủy với cạnh nhỏ hơn 10000 được dẫn đầy đủ bởi A.A.Krishnawami trong [1]. Hai tam giác bị thiếu được tìm ra bởi D.H.Lehmer trong [5]. Kiểm tra trực tiếp ta thấy có 70 tam giác với chu vi không vượt quá 1000 và có 703 tam giác có chu vi không vượt quá 10000.

Dễ dàng chứng minh với mỗi số tự nhiên s đều tồn tại tam giác nguyên thủy mà chu vi của nó là lũy thừa bậc s của một số tự nhiên. Thật vậy, xét t là số tự nhiên $\ge s>1$ và đặt $m=2^{s-1}t^2, n=\left(2t-1\right)^s-m$. Do $t\ge s$ ta có $\left(1-\frac{1}{2t}\right)^s\ge\left(1-\frac{1}{2s}\right)^s\ge 1-\frac{s}{2s}=\frac{1}{2}$. Hơn nữa từ $s>1$ suy

ra $(2t-1)^s > 2^{s-1}t^s$. Từ đó n là số tự nhiên nhỏ hơn m (vì $(2t-1)^s < 2^s t^s = 2m$). Hiển nhiên $(m,n)=1$. Tìm các số x,y,z từ công thức ***(9)*** ta thu được tam giác Pythagoras mà chu vi của nó là

$$x+y+z = 2m(mm+n) = \left[2t(2t-1)\right]^s.$$

Với $s=2$ ta có tam giác (63, 16, 65) với chu vi là 12^2.

Dễ dàng tìm tất cả các tam giác Pythagoras có độ lớn diện tích và chu vi bằng nhau (Comberousse [1], trang 190-191). Các cạnh x,y,z của các tam giác như vậy thỏa mãn các phương trình $x^2+y^2=z^2$ và $x+y+z=\frac{1}{2}xy$. Thế z vào ta thu được phương trình

(25) $$(x-4)(y-4)=8.$$

Suy ra $x-4|8$. Ta không thể có $x-4<0$ vì nếu $x-4=-1$ hoặc $x-4=-2$ ta sẽ lần lượt có $y-4=-8$ hoặc $y-4=-2$ suy ra $y=-4$ hoặc $y=0$, vô lý. Nếu $x-4=-4$ hoặc $x-4=-8$ thì $x\le 0$, vô lý. Vậy $x-4>0$ và do đó vì $x-4|8$ suy ra $x-4=1,2,4$ hoặc 8 và do đó $x=5,6,8$ hoặc 12. Từ đó sử dụng ***(25)*** ta thu được $y=12,8,6$ hoặc 5. Từ đây ta thu được hai tam giác $(5,\ 12,\ 13)$ và $(6,\ 8,\ 10)$. Rõ ràng hai tam giác này không trùng nhau. Diện tích và chu vi của tam giác thứ nhất là 30 và thứ hai là 24.

Dễ dàng chứng minh tồn tại vô hạn tam giác Pythagoras có cạnh là hữu tỷ và diện tích của chúng có độ lớn bằng chu vi. Có thể chứng minh rằng tất cả các tam giác (u,v,w) như vậy đều có dạng

$$u=\frac{2(m+n)}{n},\quad v=\frac{4m}{m-n},\quad \mathrm{w}=\frac{2(m^2+n^2)}{(m-n)n}$$

trong đó m và $n<m$ là các số tự nhiên.

6. Về các bình phương có tổng và hiệu đều là bình phương

Ta sẽ nghiên cứu về sự tồn tại các số tự nhiên x,y,z,t thỏa mãn

(26) $$x^2+y^2=z^2,\quad x^2-y^2=t^2$$

Nói cách khác ta sẽ đi tìm các số tự nhiên x và y thỏa mãn tổng và hiệu các bình phương của chúng đều là bình phương đúng. Ta có định lý Fermat sau đây

Định lý 3. *Không tồn tại các số tự nhiên mà tổng và hiệu các bình phương của chúng đều là bình phương đúng.*

Chứng minh. Giả sử tồn tại các số tự nhiên x và y thỏa mãn $x^2+y^2=z^2$ và $x^2-y^2=t^2$ với z và t là các số tự nhiên và $z>t$. Trong tất cả các cặp số x,y như vậy tồn tại cặp số mà x^2+y^2 là nhỏ nhất. Ký hiệu x,y là cặp số đó. Ta có $(x,y)=1$ vì nếu $d|x$ và $d|y$ thì do $x^2+y^2=z^2, x^2-y^2=t^2$ ta sẽ suy ra $d^2|z^2, d^2|t^2$ do đó $d|z$ và $d|t$ từ đó suy ra phương trình có thể giản ước cho d^2 mà ta đã giả thiết (x,y) là bộ số mà x^2+y^2 nhỏ nhất có thể, mâu thuẫn. Vậy $d=1$.

Theo ***(26)*** suy ra $2x^2=z^2+t^2$. Vì vậy các số z và t có cùng tính chẵn lẻ. Suy ra các số $z+t$ và $z-t$ đều chẵn và vì vậy $\frac{1}{2}(z+t)$ và $\frac{1}{2}(z-t)$ là số tự nhiên.

Nếu $d|\frac{1}{2}(z+t)$ và $d|\frac{1}{2}(z-t)$ và d lớn hơn 1 thì $d|z$. Do

(27) $$x^2=\left(\frac{z+t}{2}\right)^2+\left(\frac{z-t}{2}\right)^2$$

suy ra $d^2 \mid x^2$ và $d \mid x$. Từ đó vì $x^2+y^2=z^2$ ta cũng có $d \mid y$, mâu thuẫn với $(x,y)=1$. Vì vậy

(28 $$\left(\frac{z+t}{2},\frac{z-t}{2}\right)=1$$

Từ ***(28)*** và ***(27)*** ta nhận thấy các số $\frac{1}{2}(z+t),\frac{1}{2}(z-t),x$ tạo thành một nghiệm nguyên thủy của phương trình Pythagoras, theo định lý 1 thì suy ra tồn tại các số tự nhiên nguyên tố cùng nhau m,n với $m>n$ và một trong hai số là chẵn, số kia lẻ, trong đó $\frac{1}{2}(z-t)=m^2-n^2,\ \frac{1}{2}(z+t)=2mn$ hoặc $\frac{1}{2}(z+t)=m^2-n^2,\ \frac{1}{2}(z-t)=2mn$. Do $2y^2=z^2-t^2$ nên trong cả hai trường hợp ta có $2y^2=2\left(m^2-n^2\right)4mn$ hay $y^2=\left(m^2-n^2\right)4mn$. Do y chẵn nên $y=2k$ với k là số tự nhiên nào đó. Sử dụng công thức của y^2 ta nhận được

(29) $$\left(m^2-n^2\right)mn=k^2$$

Do $(m,n)=1$ ta có $(m\pm n,m)=1$ vì vậy $\left(m^2-n^2,m\right)=1$ và $\left(m^2-n^2,n\right)=1.$

Từ ***(29)*** áp dụng hệ quả Định lý 8 Chương 1, tất cả các số m^2-n^2,m,n là bình phương đúng, vì vậy $m=a^2,n=b^2,m^2-n^2=c^2,$ với a,b,c là các số tự nhiên.

Do $(m,n)=1$ và một trong các số m,n là chẵn và số còn lại là lẻ nên ta thu được $(m+n,m-n)=1.$ Thật vậy, mọi ước số chung của các số lẻ $m+n$ và $m-n$ đều lẻ, nhưng nó cũng là ước của $2m$ và $2n$ vì vậy từ $(m,n)=1$ suy ra ước số này bằng 1.

Từ $(m+n,m-n)=1$ và $(m+n)(m-n)=m^2-n^2=c^2$ suy ra $m+n$ và $m-n$ là các bình phương. Vì vậy từ $m=a^2,n=b^2$ suy ra các số a^2+b^2 và a^2-b^2 cũng là các bình phương.

Nhưng $a^2+b^2<x^2+y^2,$ trái với giả thiết ở trên của cặp x,y. Ta có điều phải chứng minh.

Mặt khác tồn tại vô hạn các cặp số tự nhiên x,y mà tồn tại số tự nhiên z và t thỏa mãn $x^2+y^2=z^2+1$ và $x^2-y^2=t^2+1.$ Chẳng hạn q chẵn thì với $x=\frac{q^4}{2}+1,y=q^3$ ta có

$$x^2+y^2=\left(q^2+q^4/2\right)^2+1,\ x^2-y^2=(q^4/2-q^2)^2+1$$

Ta cũng có $\left(2n^2\right)^2\pm(2n)^2=\left(2n^2\pm1\right)^2-1$ với $n=1,2,\ldots$

Tồn tại cặp số tự nhiên x,y thỏa mãn với các số tự nhiên z,t nào đó ta có $x^2+y^2=z^2-1,x^2-y^2=t^2-1,$ chẳng hạn $21^2+12^2=14^2-1,21^2-12^2=10^2-1.$

Không khó để tìm các số tự nhiên x,y mà tồn tại các số tự nhiên z,t thỏa mãn $x^2+y^2=z^1+1$ và $x^2-y^2=t^2-1,$ chẳng hạn

$13^2+11^2=17^2+1,\ 13^2-11^2=7^2-1,\ 89^2+79^2=119^2+1,89^2-79^2=41^2-1.$

Từ định lý ***(3)*** suy ra hệ phương trình sau

(*) $x^2+y^2=u^2$ *và* $x^2+2y^2=v^2$

không có nghiệm tự nhiên x,y,u,v.

Thật vậy nếu tồn tại các số tự nhiên x,y,u,v thỏa mãn ***(*)*** thì $u^2+y^2=v^2, u^2-y^2=x^2$, mâu thuẫn với Định lý 3.

Hệ quả 1. *Không tồn tại các số tự nhiên* a,b,c *thỏa mãn* $a^4-b^4=c$.

Chứng minh. Nếu tồn tại các số tự a,b,c như vậy thì ta giả sử $(a,b)=1$ vì nếu $(a,b)=d>1$ thì đặt $a=da_1, b=bd_1$ ta có $d^4(a_1^4-b_1^4)=c^2$ suy ra $d^2 \mid c^2$ vì vậy $c=d^2c_1$ và ta có $a_1^4-b_1^4=c_1^2$ với $(a_1,b_1)=1$. Giả sử $(a,b)=1,$ suy ra $(a^2,b^2)=1$ vì vậy phương trình trở $b^4+c^2=a^4$. Các số b^2,c,a^2 tạo thành một nghiệm nguyên thủy của phương trình Pythagoras. Khi đó theo Định lý 1 ta suy ra tồn tại các số tự nhiên $m,n,m>n,$ thỏa mãn $a^2=m^2+n^2$ và $b^2=m^2-n^2$ hoặc $b^2=2mn$. Trường hợp thứ nhất là không thể xảy ra vì nó mâu thuẫn với Định lý 3. Trong trường hợp thứ hai ta có $a^2+b^2=(m+n^2)$ và $a^2-b^2=(m-n)^{2,}$ cũng mâu thuẫn với Hệ quả 1.

Từ đây suy ra không tồn tại các số tự nhiên mà tổng và hiệu các bình phương của chúng đều là bội số thứ k của bình phương các số tự nhiên nào đó vì nếu ngược lại ta sẽ có $a^4-b^4=(kuv)^2$, mâu thuẫn với Hệ quả 1.

Theo Hệ quả 1 thì hiệu của hai lũy thừa bậc bốn của các số tự nhiên không phải bình phương đúng. Nhưng tích của hai hiệu như vậy vẫn có thể là bình phương đúng. Chẳng hạn

$$(3^4-2^4)(11^4-2^4)=975^2,\ (2^4-1^4)(23^4-7^4)=2040^2,$$

$$(5^4-4^4)(21^4-20^4)=3567^2,\ (9^4-7^4)(11^4-2^4)=7800^2,$$

Hệ quả 2. *Không tồn tại nghiệm tự nhiên của phương trình* $x^4+y^4=z^4$ *(đây là định lý cuối cùng của Fermat trong trường hợp bậc 4, xem thêm mục 18).*

Chứng minh. Nếu x,y,z thỏa mãn phương trình thì $z^4-y^4=(x^2)^2$, mâu thuẫn với Hệ quả 1.

Hệ quả 2 nói rằng không tồn tại tam giác Pythagoras với các cạnh là bình phương đúng.

K.Zarankiewicz đã đặt ra câu hỏi có tồn tại hay không các tam giác Pythagoras với độ dài các cạnh là các số tam giác (nghĩa là các số dạng $t_n=n(n+1)/2$). Có thể kiểm tra các số tam giác $t_{132}=8778, t_{143}=10296, t_{164}=13530$ lập thành một tam giác Pythagoras. Ngoài ra ta không biết thêm nghiệm nào khác. Tuy nhiên tồn tại vô hạn các tam giác Pythagoras mà các cạnh góc vuông là các số tam giác liên tiếp. Trong mục 4 ta đã chứng minh phương trình $x^2+(x+1)^2=z^2$ có vô hạn nghiệm tự nhiên x,z. Với mỗi nghiệm x,z như vậy thì $t_{2x}^2+t_{2x+1}^2=\left[(2x+1)z\right]^2$. Ví dụ ta có $t_6^2+t_7^2=35^2, t_{40}^2+t_{41}^2=(41.29)^2$. Hơn nữa cũng tồn tại vô hạn các tam giác Pythagoras nguyên thủy mà các cạnh góc vuông là các số tam giác. Trong số đó có tam giác $(t_7,t_9,53)$.

Nếu với các số tự nhiên a,b,c ta có $t_a^2+t_b^2=t_c^2,$ thì có thể kiểm tra

$$\left((2a+1)^2-1\right)^2+\left((2b+1)^2-1\right)^2=\left((2c+1)^2-1\right)^2.$$

Phương trình $\left(x^2-1\right)^2+\left(y^2-1\right)^2=\left(z^2-1\right)^2$ có nghiệm tự nhiên lẻ là $x=263, y=287, z=329$. Phương trình này cũng có nghiệm khác mà tất cả các số x, y, z đều lẻ, ví dụ $x=10, y=13, z=14$. Ta không biết phương trình này có vô hạn nghiệm hay không

Dễ dàng chứng minh rằng không có tam giác Pythagoras nguyên thủy mà nếu cộng thêm 1 vào độ dài cạnh huyền thì ta có một bình phương đúng. Thật vậy theo Định lý 1 thì cạnh huyền của một tam giác nguyên thủy có dạng m^2+n^2 với một trong hai số m,n là chẵn và số còn lại là lẻ. Xét số dư của m^2+n^2+1 khi chia cho 4 là 2 do đó nó không thể là bình phương đúng.

Dễ dàng chứng minh rằng phương trình $\left(x^2-1\right)^2+\left(y^2-1\right)^2=\left(z^2+1\right)^2$ có vô hạn nghiệm tự nhiên.

Kết quả này có thể rút ra từ đẳng thức $\left(\left(2n^2+2n\right)^2-1\right)^2+\left(\left(2n+1\right)^2-1\right)^2=\left(\left(2n^2+2n\right)^2+1\right)^2$.

Thay $n=1,2,\ldots,$ vào lần lượt ta thu được

$$\left(4^2-1\right)^2+\left(3^2-1\right)^2=\left(4^2+1\right)^2$$

$$\left(12^2-1\right)^2+\left(5^2-1\right)^2=\left(12^2+1\right)^2,$$

$$\left(24^2-1\right)^2+\left(7^2-1\right)^2=\left(24^2+1\right)^2$$

Chú ý rằng các số $2n^2+2n$ và $2n+1$ đều có thể là cạnh góc vuông của tam giác Pythagoras vì ta có $\left(2n^2+2n\right)^2+\left(2n+1\right)^2=\left(2n^2+2n+1\right)^2$ với $n=1,2,\ldots.$

Phương trình $\left(x^2-1\right)^2+\left(y^2\right)^2=\left(z^2-1\right)^2$ cũng có vô hạn nghiệm. Kết quả này suy ra từ đẳng thức

$$\left(\left(8n^4-1\right)^2-1\right)^2+\left(\left(2n\right)^6\right)^2=\left(\left(8n^4+1\right)^2-1\right)^2$$

Đặc biệt $\left(7^2-1\right)^2+\left(8^2\right)^2=\left(9^2-1\right)^2.$

Tuy nhiên không tồn tại tam giác Pythagoras nào mà khi đem các cạnh góc vuông trừ đi 1 ta đều nhận được các bình phương đúng. Điều này được suy ra từ tính chất tam giác Pythagoras luôn có ít nhất một cạnh góc vuông chia hết cho 4.

Bên cạnh đó có thể chứng minh rằng với mỗi tam giác Pythagoras (a,b,c) và số tự nhiên n cho trước thì đều tồn tại tam giác đồng dạng với tam giác đó và thỏa mãn mỗi cạnh của nó là lũy thừa bậc m với $m\geq n$. Để xây dựng tam giác này cần nhân các cạnh của tam giác (a,b,c) với $a^{2\left(4n^2-1\right)}b^{4n(n-1)(2n+1)}c^{4n^2(2n-1)}$. Sử dụng đẳng thức $a^2+b^2=c^2$ ta có

$$\left(\left(a^{2n}b^{(n-1)(2n+1)}c^{n(2n-1)}\right)^{2n}\right)^2+\left(\left(a^{2n+1}b^{2n^2-1}c^{2n^2}\right)^{2n-1}\right)^2=\left(\left(a^{2n-1}b^{2(n-1)n}c^{2n^2-2n+1}\right)^{2n+1}\right)^2$$

Với $n=2,$ $\left(\left(a^4b^5c^6\right)^4\right)^2+\left(\left(a^5b^7c^8\right)^3\right)^2=\left(\left(a^3b^4c^5\right)^5\right)^2.$

Ta chưa biết có tồn tại các nghiệm tự nhiên của phương trình $x^4+y^4+z^4=t^4$ hay không. Phương trình này vô nghiệm với t nhỏ hơn 220000 (Lander, Parkin và Selfridge [1]).

Ta có đẳng thức $30^4+120^4+274^4+315^4=353^4$ (Norrie, 1991) và $133^4+134^4=59^4+158^4$ (Euler, 1778). Ta không biết phương trình $x^4+y^4+z^4+t^4=u^4$ có vô hạn nghiệm tự nhiên thỏa mãn $(x,y,z,t)=1$ hay không. Ngoài các nghiệm ở trên thì có chính xác 81 nghiệm nữa với $u\leq 20469$

và $(x,y,z,t)=1$ (Rose và Brudno [1]), chẳng hạn $240^4+340^4+430^4+599^4=651^4$ (J.O.Patterson, 1942). Mặt khác tồn tại vô hạn bộ số x,y,z,t thỏa mãn $(x,y,z,t)=1$ và $x^4+y^4=z^4+t^4$ (Lander và Parkin [1], Lander, Parkin và Selfridge [1], Zaita [1]).

Ta cũng có

$$2^4+2^4+3^4+4^4+4^4=5^4,$$
$$4^4+6^4+8^4+9^4+14^4=15^4,$$
$$1^4+8^4+12^4+32^4+64^4=65^4.$$

Trở lại với Hệ quả 1 ta chú ý phương trình $x^4-y^4=z^3$ có nghiệm tự nhiên. Thật vậy, với mọi số tự nhiên k ta đều có $\left(k\left(k^4-1\right)^2\right)^4-\left(\left(k^4-1\right)^2\right)^4=\left(\left(k^4-1\right)^3\right)^3$. Đặc biệt $k=2,\ 450^4-225^4=\left(15^3\right)^3$.

E.Swift [1] đã chứng minh phương trình $x^4-y^4=z^3$ không có nghiệm tự nhiên mà $(x,y)=1$.

Hệ quả 3. *Không tồn tại ba bình phương lập thành một cấp số cộng với công sai bình phương.*

Chứng minh. Nếu tồn tại các số tự nhiên x,y,z,t mà $y^2-x^2=t^2$ và $z^2-y^2=t^2$ thì $y^2-t^2=x^2, y^2+t^2=z^2,$ mâu thuẫn với Định lý 3. □

Hệ quả 4 (Định lý Fermat). *Không tồn tại tam giác Pythagoras mà diện tích là bình phương [(1)].*

Chứng minh. Phản chứng. Giả sử tồn tại tam giác (a,b,c) như vậy. Khi đó $a^2+b^2=c^2$ và $ab=2d^2$, trong đó d và c là các số tự nhiên. Không mất tính tổng quát giả sử $a>b$. Không xảy ra trường hợp $a=b$ vì không thể có $2a^2=c^2$. Vì vậy $c^2+\left(2d\right)^2=\left(a+b\right)^2, c^2-\left(2d\right)^2=\left(a-b\right)^2$, mâu thuẫn với định lý 3. □

Có thể chứng minh không tồn tại các số hữu tỷ khác 0 mà tổng và hiệu bình phương của chúng là các bình phương hữu tỷ.

Cũng vậy, có thể chứng minh không tồn tại các số hữu tỷ $a,b,c,$ khác 0 thỏa mãn $a^4-b^4=c^4$. Phản chứng. Giả sử tồn tại các số a,b,c như vậy. Có thể giả sử chúng đều dương. Đặt $a=l/m$, $b=r/s, c=u/v$, l,m,r,s,u,v là số tự nhiên. Do $a^4-b^4=c^4$ suy ra $\left(lvs\right)^4-\left(rvm\right)^4=\left(uvm^2s^2\right)^2$, mâu thuẫn với Hệ quả 1.

Dễ dàng chứng minh rằng không tồn tại các bình phương hữu tỷ khác 0 mà tạo thành cấp số cộng với công sai bình phương hữu tỷ. Từ đây suy ra không tồn tại số hữu tỷ x mà các số $x, x+1, x+2$ đều là bình phương hữu tỷ.

7. Phương trình $x^4+y^4=z^2$

Một câu hỏi khá tự nhiên được đặt ra là có tồn tại hay không các tam giác Pythagoras mà các cạnh góc vuông đều là các bình phương. Câu trả lời phủ định có trong định lý Fermat dưới đây.

Định lý 4. *Phương trình*

(30) $$x^4+y^4=z^2$$

không có nghiệm tự nhiên x,y,z.

Chứng minh. Phản chứng. Giả sử phương trình ***(30)*** có nghiệm tự nhiên và ký hiệu z là số tự nhiên nhỏ nhất có bình phương là tổng của hai lũy thừa bậc 4. Ta có $(x,y)=1$ vì nếu ngược lại đặt

---

[(1)] C.M.Walsh đã viết một bài báo dài về định lý này [1]. Bài báo này bao gồm các chỉ dẫn lịch sử chi tiết cùng với các ghi chú của tác giả.

$(x,y)=d>1,$ ta có $x=dx_1, y=dy_1, x_1, y_1$ là các số tự nhiên, như thế $z^2=d^4\left(x_1^4+y_1^4\right),$ suy ra $d^4 \mid z^2$, do đó $d^2 \mid z$ vì thế $z=d^2z_1, z_1$ là số tự nhiên. Do đó theo ***(30)*** ta có $x_1^2+y_1^2=z_1^2<z^2,$ mâu thuẫn với giả thiết về tính nhỏ nhất của z. Vậy $(x,y)=1.$ Suy ra $\left(x^2,y^2\right)=1.$ Các số x^2, y^2, z lập thành một nghiệm nguyên thủy của phương trình

(31) $$\left(x^2\right)^2+\left(y^2\right)^2=z^2.$$

Theo Định lý 1 thì có thể giả thiết y^2 chẵn và ta có

(32) $$x^2=m^2-n^2, \quad y^2=2mn, \quad z=m^2+n^2,$$

với $(m,n)=1, m>n,$ trong hai số m,n có một số chẵn, một số lẻ. Nếu m chẵn và n lẻ thì theo hệ quả của ***(32)*** phương trình $x^2+n^2=m^2$ có cả x và n đều lẻ. Điều này dẫn tới mâu thuẫn. Bởi vì theo những gì ta đã chứng minh trong mục 3 thì bình phương của một số lẻ chia 8 dư 1, do đó vế trái của phương trình $x^2+n^2=m^2$ chia 8 dư 2 và vì thế không thể là một bình phương đúng. Vì vậy m lẻ và $n=2k$ trong đó k là số tự nhiên. Do $(m,n)=1$ suy ra $(m,k)=1$. Theo đẳng thức thứ hai của ***(32)*** ta kết luận rằng $y^2=2^2mk$ từ đó suy ra y chẵn và có dạng $y=2l,$ suy ra $l^2=mk$. Do $(m,k)=1,$ theo Định lý 8 Chương 1 thì suy ra các số m và k là các bình phương đúng, nghĩa là $m=a^2, k=b^2,$ trong đó a,b là các số tự nhiên. Ta có $n=2k=2b^2.$ Vì vậy theo ***(32)***, $x+n^2=m^2$ trong đó $(m,n)=1$ suy ra $(x,n)=1.$

Vậy các số x,n,m tạo thành một nghiệm nguyên thủy và theo Định lý 1, n chẵn suy ra

(33) $$n=2m_1n_1, \qquad m=m_1^2+n_1^2$$

trong đó m_1, n_1 là các số tự nhiên nguyên tố cùng nhau. Do $n=2b^2,$ ta có $b^2=m_1n_1,$ mà $(m_1,n_1)=1$ suy ra các số m_1, n_1 là bình phương đúng, vậy $m_1=a_1^2,$ $n_1=b_1^2$ và do $m=a^2,$ sử dụng ***(33)*** ta kết luận $a^2=m_1^2+n_1^2=a_1^4+b_1^4.$ Nhưng $a\le a^2=m<m^2+n^2=z,$ suy ra $a<z,$ mâu thuẫn với tính nhỏ nhất của z. Vậy phương trình ***(30)*** không có nghiệm tự nhiên. □

Từ Định lý 4 suy ra không tồn tại các tam giác Pythagoras mà các cạnh góc vuông đều là bình phương. Cũng có thể chứng minh không tồn tại các tam giác Pythagoras mà các cạnh góc vuông là lập phương. Chứng minh này thì khó hơn.

Mặt khác ta có $12^4+15^4+20^4=481^2$. Tổng quát hơn nếu ta có $x^2+y^2=z^2$ thì

(34) $$(xy)^4+(xz)^4+(yz)^4=\left(z^4-x^2y^2\right)^2.$$

Nếu $(x,y)=(x,z)=(y,z)=1$ thì suy $(xy,xz,yz)=1.$ Vì thế theo ***(34)*** và vì tồn tại vô hạn các nghiệm nguyên thủy của phương trình Pythagoras nên ta kết luận phương trình $t^2+u^2+v^2=w^2$ có vô hạn nghiệm tự nhiên $t,u,v,w,$ với $(t,u,v)=1.$ Ta lưu ý rằng $2^4+4^4+6^4+7^4=63^2.$ Hơn nữa như ta đã chứng minh trong mục 6 thì tổng của bốn lũy thừa bậc bốn có thể là lũy thừa bậc bốn. Mặt khác ta chưa có phản ví dụ cho giả thuyết Euler nói rằng không tồn tại lũy thừa bậc bốn có thể biểu diễn như là tổng của ba lũy thừa bậc bốn khác.

Ta lưu ý hệ phương trình

$$x^4+y^4+z^4=2t^4, \qquad x^2+y^2+z^2=2t^2$$

có vô hạn nghiệm tự nhiên $x,y,z,t.$ Điều này được suy ra từ các đẳng thức

$$\left(n^2-1\right)^4+\left(2n\pm1\right)^4+\left(n^2\pm2n\right)^4=2\left(n^2\pm n+1\right)^4.$$

$$\left(n^2-1\right)^2+\left(2n\pm1\right)^2+\left(n^2\pm2n\right)^2=2\left(n^2\pm n+1\right)^2$$

$$\left(4n\right)^4+\left(3n^2-1\right)^4+\left(3n^2-2n-1\right)^4=2\left(3n^2+1\right)^4,$$

$$\left(4n\right)^2+\left(3n^2+2n-1\right)^2+\left(3n^2-2n-1\right)^2=2\left(3n^2+1\right)^2.$$

Đặc biệt ta có

$$3^4+5^4+8^4=2\cdot7^4,\qquad 3^2+5^2+8^2=2\cdot7^2,$$
$$7^4+8^4+15^4=2\cdot13^4,\qquad 7^2+8^2+15^2=2\cdot13^2.$$

Theo Định lý 4 ta lưu ý rằng phương trình $x^4+y^4=2z^2$ có nghiệm tầm thường $x=y, z=x^2, x$ là số tự nhiên tùy ý. Legendre đã chứng minh rằng đây là tất cả các nghiệm của phương trình này. Thật vậy nếu ta có $x^4+y^4=2z^2$ với các số tự nhiên x,y,z mà $x\neq y,$ giả sử $x>y,$ khi đó các số x,y có cùng tính chẵn lẻ. Vì thế $a=\frac{1}{2}\left(x^2+y^2\right)$ và $b=\frac{1}{2}\left(x^2-y^2\right)$ là các số tự nhiên. Vì vậy $x^2=a+b,\ y^2=a-b,\ 2z^2=x^4+y^4=2\left(a^2+b^2\right)$ và $a^2+b^2=z^2,\ a^2-b^2=\left(xy\right)^2,$ mâu thuẫn với Định lý 3. Từ đó suy ra không tồn tại ba số tự nhiên phân biệt mà lũy thừa bậc bốn của chúng tạo thành một cấp số cộng. Phép chứng minh cho sự không tồn tại ba lập phương lập thành một cấp số cộng khó hơn và có thể tìm thấy trong mục 14.

Dễ thấy phương trình $x^4+y^4=3z^2$ không có nghiệm tự nhiên. Điều này được suy ra từ việc phương trình $x^2+y^2=3z^2$ không có nghiệm tự nhiên. Cũng vậy, phương trình $x^4+y^4=4z^2$ cũng không có nghiệm tự nhiên. Để chứng minh ta viết phương trình này thành $x^4+y^4=\left(2z\right)^2$ và sử dụng Định lý 4. Tương tự phương trình $x^4+y^4=9z^2$ cũng không có nghiệm tự nhiên. Bây giờ ta chứng minh rằng phương trình $x^4+y^4=5z^2$ cũng không có nghiệm tự nhiên. Có thể giả sử không có số nào trong hai số x,y chia hết cho 5, do đó chúng sẽ có dạng $5k\pm1$ hoặc $5k\pm2.$ Ta có $\left(5k\pm1\right)^2=5\left(5k^2\pm2k\right)+1,\ \left(5k\pm2\right)^2=5\left(5k^2\pm4k+1\right)-1.$ Vì thế khi chia lũy thừa bậc bốn của x,y cho 5 ta nhận được số dư là 1. Do đó x^4+y^4 chia 5 dư 2 và vì vậy $x^4+y^4=5z^2$ không thể xảy ra.

Cũng có thể chứng minh được nếu k là số tự nhiên $\neq8$ thỏa mãn $3\le k\le16$ thì phương trình $x^4+y^4=kz^2$ không có nghiệm tự nhiên. Mặt khác phương trình $x^4+y^4=17z^4$ có nghiệm tự nhiên $x=2, y=z=1.$ Phương trình $x^4+y^4=8z^2$ chỉ có các nghiệm tầm thường $x=y=2k,$ trong đó k là số tự nhiên, $z=x^2/2.$

Từ đẳng thức $\left(a^3-3ab^2\right)^2+\left(3a^2b-b^3\right)^2=\left(a^2+b^2\right)^3$ suy ra phương trình $x^2+y^2=z^3$ có vô hạn nghiệm tự nhiên. Dễ dàng chứng minh các số $x=8n\left(n^2-4\right),\quad y=n^4-24n^2+16,\quad z=n^2+4,$ với n là số lẻ $>1,$ là nguyên tố cùng nhau và thỏa mãn phương trình $x^2+y^2=z^4.$

8. Về ba bình phương có tổng đôi một là bình phương đúng

Gọi x,y,z là nghiệm của phương trình Pythagoras. Đặt

(35) $$a=x\left(4y^2-z^2\right).\ b=y\left(4x^2-z^2\right).\ c=4xyz\,.$$

Do $x^2+y^2=z^2$ ta có $a^2+b^2=z^6,\quad a^2+c^2=x^2\left(4y^2+z^2\right)^2,\quad b^2+c^2=y^2\left(4x^2+z^2\right)^2.$

Vì vậy với nghiệm cho trước của phương trình Pythagoras ta nhận được các số a,b,c mà tổng đôi một của các bình phương của chúng là bình phương đúng. Các số a,b,c khi đó là độ dài các cạnh

của một hình hộp chữ nhật mà đường chéo các mặt của nó đều là số tự nhiên. Đặc biệt khi cho $x=3, y=4, z=5$ ta có $a=117,\ b=44,\ c=240,\ a^2+b^2=125^2,\ a^2+c^2=267^2,\ b^2+c^2=244^2$. Các số này tìm được bởi P.Halcke vào năm 1719. Có thể chứng minh sự tồn tại các số a,b,c không có dạng ***(35)*** mà tổng đôi một các bình phương của chúng đều là bình phương đúng. Chẳng hạn các số $a=252, b=240, c=275, a^2+b^2=348^2, a^2+c^2=373^2, b^2+c^2=365^2$; với c không thể bằng $4xyz$, mặt khác vì $x<z, y<z$, c phải là số lớn nhất trong ba số a,b,c có dạng ***(35)***.

Ta đã biết đối với nghiệm u,v,w của phương trình $u^2+v^2=w^2$ thì có ít nhất một trong hai số u,v chia hết cho 3 và ít nhất một số chia hết cho 4. Vì vậy nếu tổng đôi một các bình phương của a,b,c là bình phương thì ít nhất hai trong các số a,b,c phải chia hết cho 3 và ít nhất hai trong số đó phải chia hết cho 4. Giả sử ngược lại các số a và b đều không chia hết cho 3 thì tổng các bình phương của chúng không phải bình phương. Hệ quả là không phải tất cả các cặp nhận được từ ***(35)*** là nguyên tố cùng nhau. Tuy nhiên nếu x,y,z là nghiệm nguyên thủy của phương trình Pythagoras thì các số a,b,c nhận được từ ***(35)*** thỏa mãn $(a,b)=1$. Điều này chứng tỏ tồn tại vô hạn các bộ số a,b,c thỏa mãn $(a,b,c)=1$ và tổng đôi một bình phương của chúng là bình phương đúng.

Dễ dàng chứng minh nếu a,b,c là các số tự nhiên thỏa mãn tổng đôi một các bình phương của chúng là bình phương thì các số ab, ac, bc cũng có tính chất đó. M.Kraitchik phát triển cách tìm các bộ ba a,b,c như vậy trong các chương từ 4 tới 6 trong [3]. Xem thêm Leech [2], Korec [1].

Ta chưa biết có tồn tại hay không ba số tự nhiên a,b,c thỏa mãn các số a^2+b^2, a^2+c^2, b^2+c^2 và $a^2+b^2+c^2$ đều là bình phương. Hay nói cách khác chúng ta chưa biết có tồn tại hình hộp chữ nhật mà đường chéo các mặt và đường chéo chính của nó đều là số tự nhiên hay không.

Mặt khác tồn tại ba số tự nhiên $a,b,c,$ chẳng hạn $a=124, b=957, c=13852800,$ mà các số a^2+b^2, a^2+c, b^2+c và a^2+b^2+c đều là bình phương đúng (Bromhead [1]). Cũng tồn tại bốn số tự nhiên x,y,z,t mà bất kỳ ba bình phương nào của chúng cũng đều là bình phương đúng. S.Tebay (xem thêm Dickson [7] tập 2 trang 55) đã tìm ra công thức cho các số như thế

$$x=\left(s^2-1\right)\left(s^2-9\right)\left(s^2+3\right),\quad y=4s\left(s-1\right)\left(s+3\right)\left(s^2+3\right),$$
$$z=4s\left(s+1\right)\left(s-3\right)\left(s^2+3\right),\quad t=2s\left(s^2-1\right)\left(s^2-9\right),$$

trong đó s là số tự nhiên lớn hơn 3. Bằng tính toán trực tiếp ta có

$$x^2+y^2+z^2=\left(\left(s^2+3\right)\left(s^4+6s^2+9\right)\right)^2,$$
$$x^2+y^2+t^2=\left(\left(s-1\right)\left(s+3\right)\left(s^4-2s^3+10s^2+6s+9\right)\right)^2,$$
$$x^2+z^2+t^2=\left(\left(s-1\right)\left(s-3\right)\left(s^4+2s^3+10s^2-6s+9\right)\right)^2,$$
$$y^2+z^2+t^2=\left(2s\left(3s^4+2s^3+27\right)\right)^2.$$

Khi $s=4$ ta có $x=1995,\ y=6384,\ z=1520,\ t=840$.

Euler đã tìm ra nghiệm $x=168,\ y=280,\ z=105,\ t=60,$ nghiệm này không có dạng như trên (Jean Lagrange [1]). Euler cũng quan tâm tới việc tìm ba số tự nhiên x,y,z mà các số $x\pm y, x\pm z, y\pm z$ đều là bình phương. Đây là một bộ số như vậy $(x=434657,\ y=420968,\ z=50568)$. Có vô hạn các bộ ba như vậy (Dickson [7] tập 2 trang 449).

Để kết thúc mục này ta sẽ chứng minh *tồn tại vô hạn dãy số tự nhiên* $a_1, a_2, \ldots.$ *thỏa mãn mỗi số* $a_1^2+a_2^2+\ldots.+a_n^2$, *với* $n=1,2,\ldots,$ *đều là bình phương.*

Chứng minh bằng quy nạp. Giả sử với n cho trước ta có các số $a_1, a_2, ...a_n$ thỏa mãn tính chất số $a_1^2 + a_2^2 + ... + a_n^2$ là bình phương của một số lẻ >1. Nghĩa là $a_1^2 + a_2^2 + ... + a_n^2 = (2k+1)^2$, với số tự nhiên k nào đó. Với $n=1$ lấy $a_1 = 3$. Sử dụng $(2k+1)^2 + (2k^2+2k)^2 = (2k^2+2k+1)^2$, đặt $a_{n+1} = 2k^2 + 2k$ thì $a_1^2 + a_2^2 + ... + a_{n+1}^2 = (2k^2+2k+1)^2$, đây lại là một bình phương lẻ. Điều phải chứng minh. Cụ thể với $a_1 = 3$ ta có $a_2 = 4, a_3 = 12, a_4 = 84, a_5 = 3612$ và tiếp tục như thế. Vì vậy ta có chuỗi $3^2 + 4^2 = 5^2$, $3^2 + 4^2 + 12^2 = 13^2$, $3^2 + 4^2 + 12^2 + 84^2 = 85^2$, ...

9. Các số điều hòa

Số tự nhiên h được gọi là số điều hòa nếu tồn tại số hữu tỷ v mà các số $v^2 + h, v^2 - h$ là bình phương của các số hữu tỷ.

Giả sử h là số điều hòa nghĩa là tồn tại các số tự nhiên a, b, c thỏa mãn $z^2 + hc^2 = a^2, z^2 - hc^2 = b^2$.

Ta có $a > b$ và $2z^2 = a^2 + b^2$. Suy ra a và b có cùng tính chẵn lẻ. Vậy $a+b$ và $a-b$ đều chẵn, đặt $a+b = 2x$, $a-b = 2y$, trong đó x, y là các số tự nhiên.

Ta có $a = x+y, b = x-y$ nên $2z^2 = a^2 + b^2 = (x+y)^2 + (x-y)^2 = 2x^2 + 2y^2$, vậy $z^2 = x^2 + y^2$.

Hơn nữa từ $z^2 + hc^2 = a^2, z^2 - hc^2 = b^2$, suy ra $2hc^2 = a^2 - b^2 = (x+y)^2 + (x-y)^2 = 4xy$, vì vậy $hc^2 = 2xy$. Do đó nếu h là số điều hòa thì tồn tại nghiệm của phương trình $x^2 + y^2 = z^2$ thỏa mãn $hc^2 = 2xy$. Ngược lại nếu các số tự nhiên x, y, z thỏa mãn phương trình $x^2 + y^2 = z^2$ thì ta có $z^2 \pm 2xy = (x \pm y)^2$.

Kết hợp các kết quả nêu trên ta có mệnh đề: *mọi nghiệm tự nhiên của phương trình $x^2 + y^2 = z^2$ ứng với một số điều hòa $h = 2xy$. Ngược lại, mọi số điều hòa cũng có thể nhận được bằng cách này, sai khác một tỷ lệ bình phương.*

Nghiệm nhỏ nhất của phương trình Pythagoras là $3, 4, 5$ cho ta số điều hòa $2 \cdot 3 \cdot 4 = 24 = 2^2 \cdot 6$ (ta có $5^2 + 24 = 7^2, 5^2 - 24 = 1^2$). Nghiệm $(5, 12, 13)$ cho số điều hòa $2 \cdot 5 \cdot 12 = 120 = 2^2 \cdot 30$ (và $13^2 + 120 = 17^2, 13^2 - 120 = 7^2$). Nghiệm không nguyên thủy $(6, 8, 10)$ cho số điều hòa $96 = 4^2 \cdot 6$ (với $10^2 + 96 = 14^2, 10^2 - 96 = 2^2$). Nghiệm $(8, 15, 17)$ cho số diều hòa $240 = 4^2 \cdot 15$ (ở đây $17^2 + 240 = 23^2, 17^2 - 240 = 7^2$). Nghiệm $(9, 40, 41)$ cho số $720 = 12^2 \cdot 5$ với các đẳng thức $41^2 + 720 = 49^2, 41^2 - 720 = 31^2$. Suy ra $\left(\frac{41}{12}\right)^2 + 5 = \left(\frac{49}{12}\right)^2$, $\left(\frac{41}{12}\right)^2 - 5 = \left(\frac{31}{12}\right)^2$.

Bài toán sau đây xuất hiện từ những năm 1220: *tìm số hữu tỷ r mà $r^2 + 5$ và $r^2 - 5$ đều là bình phương hữu tỷ.* Ngay khi bài toán được đặt người ta đã tìm được nghiệm $r = \frac{41}{12}$. Một nghiệm khác được tìm ra bởi J.D.Hill [1] là $r = \frac{3344161}{1494696}$. Khi đó $r^2 + 5 = \left(\frac{4728001}{1494696}\right)^2$ và $r^2 - 5 = \left(\frac{113279}{1494696}\right)^2$.

J.V.Uspensky và M.A.Heaslet ([1] trang 419-427) đã chứng minh hai nghiệm nêu trên là hai nghiệm tối giản với mẫu số nhỏ nhất có thể. Họ cũng đã tìm ra nghiệm khác với tử số và mẫu số có tới 15 chữ số thập phân và cũng đã trình bày phương pháp để chỉ ra vô hạn nghiệm số như vậy.

Ta sẽ chứng minh tồn tại vô hạn các số hữu tỷ r mà các số $r^2 + 5$, $r^2 + 5$ là bình phương hữu tỷ.

Giả sử rằng $r = x/y$, với các số tự nhiên x, y và y chẵn, $(x, y) = 1$ thỏa mãn tính chất các số $r^2 + 5$ và $r^2 - 5$ đều là bình phương hữu tỷ. Do các số $\left(x^2 + 5y^2\right)/y^2$ và $\left(x^2 - 5y^2\right)/y^2$ đều là bình phương hữu tỷ suy ra điều đó cũng đúng với $x^2 + 5y^2$ và $x^2 - 5y^2$. Nhưng vì chúng là các số tự nhiên nên chúng là bình phương của các số tự nhiên, đặt $x^2 + 5y^2 = z^2$, $x^2 - 5y^2 = t^2$ và

(36) $$r_1 = \frac{x^4 + 25y^4}{2xyzt}.$$

Tính toán trực tiếp ta có $r_1^2 \pm 5 = \left(\frac{x^4 \pm 10x^2y^2 - 25y^4}{2xyzt}\right)^2$. $x_1 = x^4 + 25y^4$ và $y_1 = xyzt$ là các số tự nhiên, y_1 chẵn và lớn hơn y. Có thể chứng minh $(x_1, y_1) = 1$.

Vì vậy với mỗi số hữu tỷ r biểu diễn dưới dạng phân số tối giản x/y trong đó x là số tự nhiên, y chẵn và cả hai số $r^2 + 5$ và $r^2 - 5$ đều là bình phương hữu tỷ. Theo ***(36)*** ta tìm được số hữu tỷ r_1 cũng có tính chất nêu trên và mẫu số tối giản lớn y. Từ đó suy ra tồn tại vô hạn số hữu tỷ r mà cả hai số $r^2 + 5$ và $r^2 - 5$ đều là bình phương hữu tỷ.

Bắt đầu với số $r = \frac{41}{12}$ được tìm ra bởi Leonardo Pisano (Fibonacci), theo ***(36)*** ta nhận được số $r_1 = \frac{3344161}{1494696}$, số này tìm được bởi Hill. Tiếp tục sử dụng ***(36)*** cho r_1 ta nhận được r_2 là một phân số có tử số có tới 27 chữ số. Như ở trên đã đề cập, Uspensky và Heaslet đã tìm ra số hữu tỷ r thỏa mãn cả hai số $r^2 + 5$ và $r^2 - 5$ đều là bình phương hữu tỷ và tử số trong dạng biểu diễn phân số tối giản của r chỉ có 15 chữ số. Như thế dựa vào công thức ***(36)*** ta không thể thu được tất cả các số r mà $r^2 + 5$ và $r^2 - 5$ đều là bình phương hữu tỷ.

Lý do chính khiến mọi người quan tâm tới việc tìm các số r mà $r^2 \pm 5$ đều là bình phương hữu tỷ có lẽ là vì với các số $h < 5$ thì không tồn tại các số hữu tỷ r mà $r^2 \pm h$ là bình phương hữu tỷ. Chứng minh kết quả này khi $h = 1$ hoặc $h = 4$ được suy ra trực tiếp từ Định lý 3. Chứng minh cho trường hợp $h = 2$ khó hơn một chút. Giả sử tồn tại số hữu tỷ r mà các số $r^2 + 2$ và $r^2 - 2$ là bình phương hữu tỷ. Đặt $r = x/y$, với x, y là các số tự nhiên thì $r^2 + 2y^2$ và $x^2 - 2y^2$ là bình phương hữu tỷ. Mà chúng là các số tự nhiên nên chúng phải là bình phương của các số tự nhiên. Vậy tồn tại z và t mà $x^2 + 2y^2 = z^2$, $x^2 - 2y^2 = t^2$. Vì vậy $2x^2 = z^2 + t^2$, $4y^2 = z^2 - t^2$, suy ra $4x^2 = (z+t)^2 + (z-t)^2$. Từ đó $\left[2x(z-t)\right]^2 = \left(z^2 - t^2\right)^2 + (z-t)^4 = (2y)^4 + (z-t)^4$. Nhưng $z \neq t$ nên ta có mâu thuẫn với Định lý 4. Chứng minh khi $h = 3$ cũng khó hơn một chút.

Mặt khác ta có $\left(\frac{5}{2}\right)^2 + 6 = \left(\frac{7}{2}\right)^2$, $\left(\frac{5}{2}\right)^2 - 6 = \left(\frac{1}{2}\right)^2$, $\left(\frac{337}{120}\right)^2 + 7 = \left(\frac{463}{10}\right)^2$, $\left(\frac{337}{120}\right)^2 - 7 = \left(\frac{113}{120}\right)^2$.

Bảng đầy đủ các số điều hòa nhỏ hơn 1000 được trình bày bởi Tunnel trong [1].

Dễ dàng chứng minh rằng không tồn tại các số tự nhiên x, y mà $x^2 + y$ và $x + y^2$ đều là bình phương đúng. Thật vậy nếu ta có $x^2 + y = t^2$ thì $t > x$ do đó $t \geq x + 1$, suy ra $t^2 \geq x^2 + 2x + 1$. Vì vậy $y = t^2 - x^2 \geq 2x + 1 > x$. Lập luận tương tự ta có $x > y$, mâu thuẫn.

Mặt khác tồn tại vô hạn số hữu tỷ dương x, y mà $x^2 + y$ và $x + y^2$ đều là bình phương hữu tỷ. Thật vậy, với $x = \left(n^2 - 8n\right)/16(n+1)$, $y = 2x + 1$, n là số tự nhiên > 8, ta có

$$x^2+y=\left(\frac{n^2+8n+16}{16(n+1)}\right)^2, x+y^2=\left(\frac{n^2+2n-8}{8(n+1)}\right)^2.$$

Dựa vào mối liên hệ được đề cập ở trên giữa các số điều hòa với nghiệm của phương trình Pythagoras và công thức nghiệm của phương trình Pythagoras trong mục 3, thì điều kiện cần và đủ để h là số điều hòa là $hc^2=4mn\left(m^2-n^2\right)l^2$ trong đó c,m,n,l là các số tự nhiên, $(m,n)=1$, $m>n, 2\mid mn$. Ta có $\left(\left(m^2+n^2\right)l\right)^2\pm hc^2=\left(\left(m^2-n^2\pm 2mn\right)l\right)^2$. Nếu h là số điều hòa, $z^2+hc^2=a^2$, $z^2-hc^2=b^2$, thì các số b^2,z^2,a^2 tạo thành một cấp số cộng công sai hc^2. Từ đó nếu các số b^2,z^2,a^2 tạo thành một cấp số cộng với công sai hc^2 thì h là số điều hòa. Vì vậy số điều hòa có thể định nghĩa sai khác một tỷ lệ bình phương như là công sai của một cấp số cộng bao gôm ba bình phương đúng. Tất cả các cấp số cộng như vậy đều có dạng $l^2\left(m^2-n^2-2mn\right)^2$, $l^2\left(m^2+n^2\right)^2$, $l^2\left(m^2-n^2+2mn\right)^2$ với m,n là các số tự nhiên, $m>n$.

Có thể chứng minh *với số tự nhiên k cho trước thì điều kiện cần và đủ để tồn tại số tự nhiên x thỏa mãn $k+x^2$ và $k-x^2$ đều là bình phương đúng là $k=\left(4m^4+n^4\right)l^2$, trong đó m,n,l là các số tự nhiên (không giảm tổng quát có thể giả sử m,n* nguyên tố cùng nhau). Với $m=n=1$ ta có $5+2^2=3^2$, $5-2^2=1^2$, với $m=1,n=2$ ta có $20+4^2=6^2$, $20-4^2=2^2$, với $m=2,n=1$ ta có $65+4^2=9^2$, $65-4^2=7^2$, với $m=1,n=3$ ta có $85+6^2=11^2$, $85-6^2=7^2$.

10. Phương trình $x^2+y^2+z^2=t^2$

Ta sẽ tìm tất cả các nghiệm tự nhiên của phương trình

(37) $$x^2+y^2+z^2=t^2$$

Đầu tiên ta chú ý rằng ít nhất hai trong các số x,y,z là chẵn. Giả sử ngược lại là tất cả các số x,y,z đều lẻ, khi đó t^2 là tổng của ba bình phương lẻ sẽ có dạng $8k+3$ bởi vì mỗi bình phương lẻ chia 8 đều dư 1. Điều này là không thể vì bản thân t^2 cũng là một bình phương lẻ. Nếu chỉ có duy nhất một trong ba số x,y,z là chẵn thì tổng $x^2+y^2+z^2=t^2$ sẽ có dạng $4k+2$, điều này cũng không thể xảy ra vì bình phương của một số chẵn sẽ có dạng $4k$. Vậy ta có thể giả sử y và z chẵn. Khi đó

(38) $$y=2l,\quad z=2m,$$

trong đó l và m là các số tự nhiên. Từ ***(37)*** ta thấy $t>x$. Đặt

(39) $$t-x=u$$

Ta nhận được số tự nhiên u và từ ***(37), (38), (39)*** ta có $(x+u)^2=x^2+4l^2+4m^2$ và suy ra $2xu+u^2=4l^2+4m^2$, hơn nữa

(40) $$u^2=4l^2+4m^2-2xu.$$

Vế phải của đẳng thức ***(40)*** là tổng của các số chẵn, vì thế u chẵn. Đặt

(41) $$u=2n,$$

với số tự nhiên n nào đó. Thế ***(41)*** vào ***(40)*** và chia cả hai vế cho 4 ta có $n^2=l^2+m^2-nx$. Hay là

(42) $$x=\frac{l^2+m^2-n^2}{n},$$

Mà từ ***(39)*** suy ra $t = x + u = x + 2n = \dfrac{l^2 + m^2 + n^2}{n}$. Hơn nữa vì x là số tự nhiên, từ ***(42)*** ta suy ra $n^2 < l^2 + m^2$. Vậy tất cả các nghiệm tự nhiên x, y, z, t, với y, z chẵn, của ***(37)*** đều có dạng

(43) $$x = \frac{l^2 + m^2 - n^2}{n},\ y = 2l,\ z = 2m,\ t = \frac{l^2 + m^2 + n^2}{n},$$

với m, n, l là các số tự nhiên và n là ước số của $l^2 + m^2$ và nhỏ hơn $\sqrt{l^2 + m^2}$.

Bây giờ ta chứng minh điều ngược lại, nghĩa là nếu l, m, n thỏa mãn điều kiện nêu trên thì các số x, y, z, t thu được từ ***(43)*** sẽ trở thành nghiệm tự nhiên của phương trình ***(37)***. Từ các điều kiện trên ta có x, y, z là các số tự nhiên. Để chứng minh chúng thỏa mãn ***(37)*** ta sử dụng đẳng thức

$$\left(\frac{l^2 + m^2 - n^2}{n}\right)^2 + (2l)^2 + (2m)^2 = \left(\frac{l^2 + m^2 + n^2}{n}\right)^2.$$

Dễ dàng chứng minh rằng mọi nghiệm tự nhiên x, y, z, t với y, z chẵn của ***(37)*** đều thu được duy nhất một lần từ công thức ***(43)***. Sử dụng ***(43)*** ta có $l = \dfrac{y}{2}$, $m = \dfrac{z}{2}$, $n = \dfrac{t - x}{2}$ và vì vậy các số l, m, n xác định duy nhất theo x, y, z, t. Lập luận này dẫn tới kết quả sau

Định lý 5. *Tất cả các nghiệm tự nhiên x, y, z, t với y, z chẵn của phương trình $x^2 + y^2 + z^2 = t^2$ đều có dạng $x = \dfrac{l^2 + m^2 - n^2}{n}$, $y = 2l$, $z = 2m$, $t = \dfrac{l^2 + m^2 + n^2}{n}$, l, m là các số tự nhiên tùy ý, n* là ước số của $l^2 + m^2$ *và nhỏ hơn $\sqrt{l^2 + m^2}$. Hơn nữa mọi nghiệm đều được liệt kê duy nhất theo cách này.*

Định lý 5 không chỉ ra sự tồn tại nghiệm của phương trình ***(37)*** nhưng lại cho chúng ta phương pháp để tìm chúng. Bỏ qua các cặp l, m mà $m > l$ và chỉ lấy các giá trị của n mà x lẻ. Ta cũng loại ra các nghiệm mà x, y, z, t đều chẵn. Để thu lại các nghiệm đó ta chỉ cần nhân các nghiệm mà x lần lượt với các lũy thừa của 2. Dưới đây là 10 nghiệm đầu tiên của ***(37)*** nhận được theo cách này

l	m	l^2+m^2	n	x	y	z	t
1	1	2	1	1	2	2	3
2	2	8	1	7	4	4	9
3	1	10	1	9	6	2	11
3	1	10	2	3	6	2	7
3	3	18	1	17	6	6	19
3	3	18	2	7	6	6	11
3	3	18	3	3	6	6	9
4	2	20	1	19	8	4	21
4	2	20	4	1	8	4	9
4	4	32	1	31	8	8	33

R.D.Carmichael (xem [4] trang 39-43) đã chỉ ra rằng tất cả các nghiệm tự nhiên của ***(37)*** đều có thể thu được từ đẳng thức

$$d^2\left(m^2 - n^2 - p^2 + q^2\right)^2 + d^2\left(2mn - 2pq\right)^2 + d^2\left(2mp + 2nq\right)^2 = d^2\left(m^2 + n^2 + p^2 + q^2\right)^2$$

11. Phương trình $xy = zt$

Giả sử rằng các số tự nhiên x,y,z,t thỏa mãn $xy=zt$ và đặt $(x,z)=a$. Thế thì $x=ac$, $z=ad$, trong đó c và d là các số tự nhiên và $(c,d)=1$. Vì vậy $acy=adt$, nghĩa là $cy=dt$ và từ $(c,d)=1$, ta suy ra $d\mid y$ và như thế $y=bd$ trong đó b là số tự nhiên, hơn nữa $t=bc$. Điều này chứng tỏ rằng nếu các số tự nhiên x,y,z,t thỏa mãn phương trình $xy=zt$ thì tồn tại các số tự nhiên a,b,c,d mà $(c,d)=1$ và $x=ac$, $y=bd$, $z=ad$, $t=bc$. Ngược lại thì với các số tự nhiên cho trước a,b,c,d ta định nghĩa các số x,y,z,t theo công thức trên thì $xy=zt$. Ta có định lý

Định lý 6. *Tất cả các nghiệm tự nhiên của phương trình $xy=zt$ được cho bởi công thức $x=ac$, $y=bd$, $z=ad$, $t=bc$ với a,b,c,d là các số tự nhiên tùy ý. Hơn nữa kết quả vẫn đúng khi bổ sung thêm điều kiện $(c,d)=1$.*

Dễ dàng chứng minh $(c,d)=1$, vậy công thức trên cho ta tất cả các nghiệm và mỗi nghiệm nhận được đúng một lần.

Để tìm được các nghiệm của phương trình $xy=zt$, ta bắt đầu với các số tự nhiên tùy ý x,z.

Do $\frac{x}{(x,z)},\frac{x}{(x,z)}$ nguyên tố cùng nhau và dựa vào đẳng thức $\frac{x}{(x,z)}y=\frac{z}{(x,z)}t$ ta thấy $\left.\frac{z}{(x,z)}\right| y$ và do đó $y=\frac{uz}{(x,z)}$ suy ra $t=\frac{ux}{(x,z)}$. Mặt khác, lấy các số tự nhiên tùy ý x,z,u và đặt $y=\frac{uz}{(x,z)}$, $t=\frac{ux}{(x,z)}$ ta nhận được nghiệm tự nhiên của $xy=zt$. Vì vậy tất cả các nghiệm tự nhiên của $xy=tz$ được cho bởi công thức $y=\frac{uz}{(x,z)}$, $t=\frac{ux}{(x,z)}$ với x,z,u tùy ý.

Không khó để nhận thấy tất cả các nghiệm tự nhiên của phương trình $xy=z^2$ đều được cho bởi công $x=u^2t$, $y=v^2t$, $z=uvt$ với u,v,t tùy ý. Ta giả thiết thêm $(u,v)=1$ thì khi đó mỗi nghiệm đều nhận được đúng một lần từ các công thức này. Có thể chứng minh rằng tất cả các nghiệm tự nhiên của phương trình $xy=z^3$ đều được cho bởi công thức $x=uv^2t^3$, $y=u^2vw^3$, $z=uvtw$ với u,v,t,w tùy ý.

Tổng quát hơn tồn tại công thức nghiệm tổng quát của phương trình $x_1x_2\ldots x_n=z^k$ với $n\geq 2$ và số tự nhiên k cho trước (Ward [1], Schinzel [4]).

Dễ dàng chứng minh với các số tự nhiên cho trước n và m thì tất cả các nghiệm tự nhiên của $x_1x_2\ldots x_n=y_1y_2\ldots y_m$ đều được cho bởi

$$x_n=\frac{y_1y_2\ldots y_{m-1}t}{(x_1x_2\ldots x_{n-1},y_1y_2\ldots y_{m-1})},\ y_m=\frac{x_1x_2\ldots x_{n-1}t}{(x_1x_2\ldots x_{n-1},y_1y_2\ldots y_{m-1})}$$

với $x_1,x_2,\ldots,x_{n-1},y_1,y_2,\ldots,y_{m-1}$, t là các số tự nhiên tùy ý. Phương trình này còn có công thức nghiệm khác như sau: với mn tham số tự nhiên tùy ý t_{ij} $(i=1,2,\ldots,m,\ j=1,2,\ldots,n)$ thì các nghiệm đều có dạng $y_i=t_{i,1}t_{i,2}\ldots t_{i,n}$ $(i=1,2,\ldots,m)$, $x_j=t_{1.j}t_{2.j}\ldots t_{m.j}$ $(j=1,2,\ldots,n)$. Để chứng minh rằng công thức này cho ta tất cả các nghiệm của phương trình ban đầu là khá phức tạp (Bell [1]).

Bài tập. ***1.*** Tìm tất cả các nghiệm nguyên của phương trình $(x+y+z)^3=x^3+y^3+z^3$.

Lời giải. Ta có đẳng thức $(x+y+z)^3-(x^3+y^3+z^3)=3(x+y)(y+z)(z+x)$. Vậy chỉ cần giải phương trình nghiệm nguyên $(x+y)(y+z)(z+x)=0$.

2. Tìm tất cả các nghiệm nguyên của hệ phương trình

(44) $$x+y+z=t,\ x^2+y^2+z^2=t^2,\ x^3+y^3+z^3=t^3$$

Lời giải. Từ hệ ***(44)*** suy ra $xy+yz+zx=0$ và $(x+y)(y+z)(z+x)=0$ (so sánh với bài tập 1). Nếu $x+y=0$ thì do $xy+yz+zx=xy+(x+y)z=0$, suy ra $xy=0$ cho nên $x=y=0$. Vì vậy nếu các số nguyên x,y,z,t thỏa mãn hệ ***(44)*** thì hai trong số x,y,z phải bằng 0 và số thứ ba bằng t với t tùy ý. Vì vậy hệ ***(44)*** chỉ có các nghiệm tầm thường.

3. Tìm tất cả các cặp số tự nhiên x,y mà xy chia hết cho $x+y$.

Lời giải. Tất cả các cặp số như vậy được cho bởi công thức

(45) $$x=k(m+n)m,\qquad y=k(m+n)n,$$

với k là số tự nhiên tùy ý và m,n nguyên tố cùng nhau. Từ ***(45)*** suy ra $xy/(x+y)=kmn$ do đó $x+y\mid xy$. Mặt khác nếu với các số tự nhiên $x,y,x+y\mid xy$ được thỏa mãn thì ta có thể đặt $d=(x+y), x=dm, y=dn,$ và thu được $(m,n)=1,$ hơn nữa $d(m+n)\mid d^2mn,$ suy ra $m+n\mid dmn$. Từ $(m,n)=1$ suy ra $(m+n,mn)=1.$ Hệ quả là $m+n\mid d$ và do đó $d=k(m+n)$ với số tự nhiên k nào đó. Vì vậy đặt $x=dm$ và $y=dn$ ta nhận lại công thức ***(45)***. Dễ dàng chứng minh rằng với các số tự nhiên k,m,n mà $(m,n)=1$ thì tất cả các cặp x,y thỏa mãn điều kiện $x+y\mid xy$ được nhận lại đúng một lần từ công thức ***(45)***. Thật vậy, theo công thức ***(45)*** ta có $(m,n)=1,$ $\dfrac{m}{n}$ là phân số tối giản và bằng với $\dfrac{x}{y}$. Hệ quả là các số x,y xác định m,n một cách duy nhất. Vì vậy theo ***(45)*** thì k cũng xác định một cách duy nhất bởi x,y.

4. Tìm tất cả các nghiệm tự nhiên của phương trình

(46) $$\frac{1}{x}+\frac{1}{y}=\frac{1}{z}$$

Lời giải. Tất cả các nghiệm tự nhiên của ***(46)*** được cho bởi công thức sau đây

(47) $$x=k(m+n)m,\quad y=k(m+n)n,\quad z=kmn,$$

với k là số tự nhiên và $(m,n)=1.$ Thật vậy, nếu các số tự nhiên x,y,z thỏa mãn ***(46)*** thì $(x+y)z=xy$ suy ra $x+y\mid xy$ và theo bài tập 3 thì ta thấy công thức ***(45)*** được thỏa mãn với x,y. Vì vậy $z=xy/(x+y)=kmn$ suy ra công thức ***(47)***. Mặt khác dễ dàng kiểm tra lại các số x,y,z thỏa mãn công thức ***(47)*** cũng thỏa mãn phương trình ***(46)***.

5. Tìm tất cả các nghiệm nguyên của phương trình

(48) $$(x+y+z)^2=x^2+y^2+z^2$$

Lời giải. Phương trình ***(48)*** tương đương với

(49) $$xy+yz+zx=0.$$

Nếu các số nguyên x,y,z thỏa mãn phương trình ***(49)*** và ít nhất một trong số chúng, giả sử là x, bằng 0 thì theo ***(49)*** ta có $yz=0$ suy ra một trong hai số z,y cũng bằng 0. Vì vậy nếu một trong các số x,y,z bằng 0 thì ít nhất hai trong số chúng bằng 0. Mặt khác nếu hai trong các x,y,z bằng 0 và số thứ ba tùy ý thì phương trình ***(48)*** được thỏa mãn. Bây giờ ta giả sử x,y,z đều khác 0. Khi đó theo ***(49)*** suy ra hai trong các số này phải cùng dương hoặc cùng âm và số còn lại có dấu ngược lại. Đổi dấu nếu cần thiết ta có thể giả sử $x>0,\ y>0,\ z<0$. Từ ***(49)*** ta suy ra $xy=-(x+y)z$. Như

thế $x+y \mid xy$. Bây giờ ta có thể áp dụng công thức ***(45)*** trong bài tập 3 với $z = -\dfrac{xy}{x+y} = -kmn$. Vì vậy nếu các số nguyên x, y, z thỏa mãn phương trình ***(48)***, $x>0, y>0$, thì với số các số tự nhiên k, m, n nào đó mà $(m,n)=1$ ta nhận được

(50) $$x = k(m+n)m, \quad y = k(m+n)n, \quad z = -km.$$

Mặt khác, tính toán trực tiếp cho thấy các số tự nhiên k, m, n trong công thức ***(50)*** cho ta nghiệm của phương trình ***(48)***. Vì vậy tất cả các nghiệm x, y, z với $x>0, y>0$ của ***(48)*** đều được cho bởi công thức ***(50)*** với k, m, n là các số tự nhiên. Hơn nữa ta có thể giả thiết $(m,n)=1$. Từ đây tất cả các nghiệm của phương trình ***(48)*** có thể tìm được một cách dễ dàng.

6. Chứng minh hai mệnh đề sau là tương đương

(i) Tồn tại các số nguyên dương a, b, c, d, ef, g thỏa mãn

(51) $$a^2+b^2 = e^2, \quad b^2+c^2 = f^2, \quad a^2+c^2 = g^2, \quad a^2+b^2+c^2 = d^2$$

(ii) Tồn tại các số hữu tỷ x, y, z lớn hơn 1 thỏa mãn

(52) $$\left(\frac{x}{1+x^2}\right)^2 + \left(\frac{v}{1+y^2}\right)^2 = \left(\frac{z}{1+z^2}\right)^2.$$

Lời giải (M.Skalba). (i) $\to$ (ii). Không mất tính tổng quát giả sử $(a,b,c,d)=1$. Suy ra d lẻ và có đúng một trong các số a, b, c lẻ, giả sử là a.

Từ Định lý 1 và ***(51)*** suy ra tồn tại các số nguyên dương d_i, m_i, n_i $(i=1,2,3)$ thỏa mãn

$$a = d_1\left(m_1^2 - n_1^2\right); \qquad b = d_2 2m_2n_2, \qquad c = d_3 2m_3n_{3,}$$

(53) $$d = d_1\left(m_i^2 + n_i^2\right) \text{ với } i = 1,2,3.$$

Đẳng thức $a^2+b^2+c^2 = d^2$ trở thành $\left(d_2m_2n_2\right)^2 + \left(d_3m_3n_3\right)^2 = \left(d_1m_1n_1\right)^2$.

Chia cả hai vế cho $d^2 = d_1^2\left(m_i^2+n_i^2\right)^2$ ta thu được ***(52)*** với

$$x = \frac{m_2}{n_2} > 1, \qquad y = \frac{m_3}{n_3} > 1, \qquad z = \frac{m_1}{n_1} > 1$$

(ii) $\to$ (i). Với các số hữu tỷ x, y, z lớn hơn 1 thỏa mãn ***(52)***. Ta viết

$$x = \frac{m_2}{n_2}, \qquad y = \frac{m_3}{n_3}, \qquad z = \frac{m_1}{n_1},$$

với m_i, n_i là các số nguyên dương. Đặt $d = \prod_{i=1}^{3}\left(m_i^2+n_i^2\right)$.

Nếu ta định nghĩa d_i $(i=1,2,3)$ và a, b, c theo công thức ***(53)*** và lấy

$$e = d_3\left(m_3^2 - n_3^2\right), \qquad f = d_1 2m_1n_1, \qquad g = d_2\left(m_2^2 - n_2^2\right),$$

thì ta nhận được các số nguyên dương a, b, c, d, e, f, g thỏa mãn ***(51)***.

12. Phương trình $x^4 - x^2y^2 + y^4 = z^2$

Phương trình

(54) $x^4 - x^2y^2 + y^4 = z^2$

có nghiệm tầm thường $x = y,\ z = y^2$ trong đó y là số tự nhiên tùy ý.

Giả sử rằng x, y, z là nghiệm tự nhiên của ***(54)*** với $x \neq y$. Rõ ràng ta có thể giả sử $(x, y) = 1$ vì nếu ngược lại nghĩa là $(x, y) = d > 1$ thì ta có $x = dx_1, y = dy_1$ suy ra theo ***(54)*** thì $d^4 \mid z^2$ và do đó $z = dz_1^2$. Chia cả hai vế của ***(54)*** cho d^4 ta nhận được $(x_1, y_1) = 1$ và $x_1^4 - x_1^2y_1^2 + y_1^4 = z_1^2$. Gọi x, y, z là nghiệm tự nhiên của ***(54)*** thỏa mãn $(x, y) = 1$ và $x \neq y$. Hơn nữa giả sử rằng đối với nghiệm x, y, z này thì tích xy đạt giá trị bé nhất có thể.

Ta giả sử rằng một trong các số x, y là chẵn, giả sử là y. Do $(x, y) = 1$ suy ra x lẻ. Phương trình ***(54)*** có thể viết lại dưới dạng $\left(x^2 - y^2\right)^2 + (xy)^2 = z^2$ trong đó $x^2 - y^2 \neq 0$ (vì $x \neq y$). Từ $(x, y) = 1$ suy ra $\left(x^2 - y^2, xy\right) = 1$. Hơn nữa do xy chẵn nên áp dụng công thức nghiệm nguyên thủy của phương trình Pythagoras ta suy ra tồn tại các số tự nhiên m, n thỏa mãn $(m, n) = 1, 2 \mid mn$, $x^2 - y^2 = m^2 - n^2$, $xy = 2mn$. Do x lẻ và y chẵn nên số $x^2 - y^2$ và $m^2 - n^2$ có dạng $4k + 1$ suy ra n chẵn và m lẻ. Đặt $y = 2y_0$ với y_0 là số tự nhiên. Từ $xy = 2mn$ ta tìm được $xy_0 = mn$ với $(x, y_0) = (m, n) = 1$. Từ Định lý 6 suy ra tồn tại các số tự nhiên a, b, c thỏa mãn $x = ac$, $y_0 = bd$, $m = ad$, $n = bc$ với $(c, d) = 1$. Từ $(x, y_0) = (m, n) = 1$ suy ra các số a, b, c, d là nguyên tố cùng nhau đôi một. Do x, m lẻ nên các số số a, c, d lẻ. Và do n chẵn nên b chẵn.

Thay $x = ac,\ y = 2y_0 = 2bd,\ m = ad,\ n = bc$ vào phương trình $x^2 - y^2 = m^2 - n^2$ ta thu được $\left(a^2 + b^2\right)c^2 = \left(a^2 + 4b^2\right)d^2$. Đặt $\delta = \left(a^2 + b^2, a^2 + 4b^2\right)$. Ta có $\delta \mid a^2 + 4b^2 - \left(a^2 + b^2\right) = 3b^2$ và $\delta \mid 4\left(a^2 + b^2\right) - \left(a^2 + 4b^2\right) = 3a^2$. Và do $(a, b) = 1$ suy ra $\delta \mid 3$. Nhưng 3 không phải ước số của $a^2 + b^2$ vì nếu $3 \mid a^2 + b^2$ thì a, b đều chia hết cho 3, mâu thuẫn với $(a, b) = 1$. Vậy $\delta = 1$ nghĩa là $\left(a^2 + b^2, a^2 + 4b^2\right) = 1$, từ $\left(a^2 + b^2\right)c^2 = \left(a^2 + 4b^2\right)d^2$ suy ra $a^2 + b^2 \mid d^2$ và $c^2 \mid a^2 + 4b^2$.

Mặt khác từ $(c, d) = 1$ suy ra $d^2 \mid a^2 + b^2$ và $c^2 \mid a^2 + 4b^2$. Vì vậy $a^2 + b^2 = d^2$ và $a^2 + 4b^2 = c^2$. Nhưng $(a, b) = 1$ và do a lẻ nên $(a, 2b) = 1$. Vì vậy theo công thức nghiệm nguyên thủy của phương trình Pythagoras thì từ đẳng thức $a^2 + (2b)^2 = c^2$ suy ra sự tồn tại của các số tự nhiên x_1, y_1 thỏa mãn $(x_1y_1) = 1, 2 \mid x_1y_1$, $a = x_1^2 - y_1^2$, $b = x_1y_1$. Ta có $a^2 + b^2 = d^2$. Vì vậy $x_1^4 - x_1^2y_1^2 + y_1^4 = d^2$ và một trong các số x_1, y_1 là chẵn. Nhưng $x_1y_1 = b < 2bd = y \leq xy$ suy ra $x_1y_1 < xy$. Điều này mâu thuẫn với giả thiết ban đầu của nghiệm x, y, z. Chứng tỏ các số x, y đều lẻ.

Do $x \neq y$ nên ta có thể giả sử $x > y$. Từ $\left(x^2 + y^2\right)^2 + (xy)^2 = z^2$ và số $x^2 - y^2 > 0$ là chẵn nên tồn tại các số tự nhiên m, n thỏa mãn $(m, n) = 1,\ 2 \mid mn$, $x^2 - y^2 = 2mn$ và $xy = m^2 - n^2$. Từ đó

$$m^4 - m^2n^2 + n^4 = \left(m^2 - n^2\right)^2 + m^2n^2$$
$$= (xy)^2 + \left(\frac{x^2 - y^2}{2}\right)^2 = \left(\frac{x^2 + y^2}{2}\right)^2$$

và $(m, n) = 1$, một trong các số m, n là chẵn. Nhưng điều này là không thể. Ta có định lý sau đây

Định lý 7. *Phương trình* $x^4 - x^2y^2 + y^4 = z^2$ *chỉ có các nghiệm tự nhiên tầm thường* $x = y,\ z = x^2$.

Chứng minh ở trên thuộc về H.C.Pocklington [1].

Từ định lý này Pocklington đã đi tới định lý Fermat sau đây

Định lý 8. *Không tồn tại bốn bình phương khác nhau tạo thành một cấp số cộng.*

Chứng minh. Giả sử phản chứng x^2, y^2, z^2, w^2 là các số tự nhiên thỏa mãn tính chất cấp số cộng $y^2-x^2=z^2-y^2=w^2-z^2$. Do đó ta có $2y^2=x^2+z^2$, $2z^2=y^2+w^2$ suy ra $2y^2w^2=x^2w^2+z^2w^2$, $2x^2z^2=x^2y^2+z^2w^2$ từ đó $2x^2z^2-2y^2w^2=x^2y^2-z^2w^2$. Số $x^2y^2-z^2w^2$ chẵn suy ra xy và zw có cùng tính chẵn lẻ. Đặt $u=xz$, $v=yw, r=(xy+zw)/2$, $s=(xy-zw)/2$. Rõ ràng u,v,r,s đều là số tự nhiên. Dễ dàng kiểm tra $u^2-v^2=2rs, uv=r^2-s^2$. Suy ra $u^4-u^2v^2+v^4=\left(r^2+s^2\right)^2$ và theo Định lý 7 suy ra $u=v$. Do x^2, y^2, z^2, w^2 lập thành một cập số cộng phân biệt nên ta có thể giả sử $x<y<z<w$ suy ra $xz<yw$ nghĩa là $u<v$, mâu thuẫn. □

13. Phương trình $x^4+9x^2y^2+27y^4=z^2$

Lời giải sau đây thuộc về J.Cel [1]. Ta sẽ chứng minh phương trình này không có nghiệm tự nhiên. Giả sử phương trình

(55) $$x^4+9x^2y^2+27y^4=z^2$$

có nghiệm nguyên dương và gọi x,y,z là nghiệm mà z đạt giá trị nhỏ nhất. Nếu $(x,y)=d>1$ thì $x=dx_1$, $y=dy_1$ và từ ***(55)*** suy ra $d^4\mid z^2$, $d^2\mid z$, $z=d^2z_1, x_1, y_1, z_1$ là các số nguyên dương. Chia cả hai vế của ***(55)*** cho d^4 ta nhận được $x_1^4+9x_1^2y_1^2+27y_1^4=z_1^2$. Mâu thuẫn với giả thiết về tính nhỏ nhất z. Vì vậy $(x,y)=1$. Nếu $2\mid x$ thì từ ***(55)*** suy ra $4\mid 27y^2-z^2$ vì vậy $2\mid y$ mâu thuẫn với $(x,y)=1$. Do đó x lẻ. Nếu y cũng lẻ thì từ ***(55)*** suy ra $8\mid z^2-5$. Điều này không thể có. Vì vậy

(56) $$x \text{ lẻ, } y \text{ chẵn.}$$

Nếu $3\mid x$ thì rõ ràng ta có $27\mid z^2$ vì vậy $9\mid z$, $81\mid 27y^4$, $3\mid y$ mâu thuẫn với $(x,y)=1$. Vậy $(x,3)=1$. Ta cũng có $(x,z)=1$. Thật vậy, đặt (x,z) bởi d và từ ***(55)*** thì $d\mid 27y^4$. Từ $(x,3y)=1$ ta có $\left(d,27y^4\right)=1$ vì vậy $d=1$. Đặt $y=2y_1$. Phương trình ***(55)*** có thể biểu diễn dưới dạng

$$27y_1^4=\left(\frac{z+x^2}{2}+9y_1^2\right)\left(\frac{z-x^2}{2}-9y_1^2\right).$$

Các nhân tử ở vế phải là dương vì tổng và tích của chúng là dương. Đặt d_1 là ước chung lớn nhất của chúng. Ta có $d_1^2\mid 27y_1^4$ vì vậy theo Hệ quả 2 Định lý 6a Chương 1 ta có $d_1\mid 9y_1^2$ và vì vậy $d_1\mid\left(x_1^2,z\right)$. Từ $(x,z)=1$ ta có thể áp dụng Định lý 6a suy ra $\left(x^2,z\right)=1$ vì vậy $d_1=1$ và theo Định lý 8 Chương 1 tjhì ta sẽ có một trong hai khả năng sau xảy ra

(57₁) $$\frac{z+x^2}{2}+9y_1^2=27a^4,\ \frac{z-x^2}{2}-9y_1^2=b^4,\ y_1=ab,$$

(57₂) $$\frac{z+x^2}{2}+9y_1^2=a^4,\ \frac{z-x^2}{2}-9y_1^2=27b^4,\ y_1=ab,$$

với a,b là các số nguyên dương nguyên tố cùng nhau.

Hệ ***(57₁)*** không thể xảy ra vì nó dẫn tới $x^2+18a^2b^2=27a^4-b^4$, $3\mid b^4+1$. Hệ ***(57₂)*** dẫn tới

(58) $$x^2+18a^2b^2=a^4-27b^4,$$

suy ra a hoặc b chẵn. Lưu ý x lẻ. Nếu a chẵn thì $a^4 = x^2 + 18a^2b^2 + 27b^4 = 8k+4$, mâu thuẫn. Vậy b chẵn suy ra $27b^4 = \left(\frac{a^2+x}{2} - \frac{9}{2}b^2\right)\left(\frac{a^2-x}{2} - \frac{9}{2}b^2\right)$. Đặt $d_2 = \left(\frac{a^2+x}{2} - \frac{9}{2}b^2, \frac{a^2-x}{2} - \frac{9}{2}b^2\right)$. Ta có $d_2^2 \mid 27b^4$ vì vậy $d_2 \mid 9b^2$ và $d_2 \mid x$. Suy ra $d_2 \mid \left(9y^2, x\right)$ và do $(3y, x) = 1$ ta suy ra $d_2 = 1$. Nếu các số $\frac{a^2 \pm x}{2} - \frac{9}{2}b^2$ đều âm ta sẽ có $a^2 < 9b^2$ mâu thuẫn với ***(58)***. Vậy $\frac{a^2+x}{2} - \frac{9}{2}b^2$, $\frac{a^2-x}{2} - \frac{9}{2}b^2$ là các số nguyên dương nguyên tố cùng nhau. Áp dụng Định lý 8 chương 1 ta có $\frac{a^2 \pm x}{2} - \frac{9}{2}b^2 = m^4$, $\frac{a^2 \mp x}{2} - \frac{9}{2}b^2 = 27n^4$, $b = mn$, với m, n là các số nguyên dương. Hơn nữa $a^2 = m^4 + 9m^2n^2 + 27n^4$ và $a \le y_1 < y < z$, mâu thuẫn với giả thiết ban đầu của nghiệm x, y, z. Điều phải chứng minh. □

Ở đây ta chú ý tới hai bài báo lớn (Lind [1], Reichardt [1]) đã nghiên cứu các phương trình dạng $ax^4 + bx^2y^2 + cy^4 = dz^2$.

14. Phương trình $x^3 + y^3 = 2z^3$

Giả sử rằng phương trình này có nghiệm nguyên x, y, z thỏa mãn $x \ne y$ và $z \ne 0$. Ta có thể giả sử $(x, y) = 1$ vì nếu $(x, y) = d > 1$ thì ta có thể đặt $x = dx_1$, $y = dy_1$ và suy ra $d^3 \mid 2z^3$ do đó $d \mid z$ và vì vậy $z = dz_1$. Ta sẽ có $x_1^3 + y_1^3 = 2z_1^3$ với $(x_1, y_1) = 1$. Do $x^3 + y^3 = 2z^3$ nên các số $x+y$ và $x-y$ là chẵn suy ra các số $u = (x+y)/2$ và $v = (x-y)/2$ nguyên. Hơn nữa ta có $x = u+v$, $y = u-v$ và do $(x, y) = 1$ nên $(u, v) = 1$. Ta cũng có $(u+v)^3 + (u-v)^3 = 2z^3$. Vì vậy $u\left(u^2 + 3v^2\right) = z^3$ mà vì $x \ne y$ và $z \ne 0$ suy ra $uvz = \frac{1}{4}\left(x^2 - y^2\right)z \ne 0$.

Nếu $(u, 3) = 1$, thì vì $(u, v) = 1$, ta có $\left(u, u^2 + 3v^2\right) = 1$. Hơn nữa tồn tại các số nguyên z_1 và z_2 thỏa mãn $u = z_1^3$ và $u^2 + 3v^2 = x_2^3$. Vì vậy $z_2^3 - z_1^6 = 3v^2$ và do đó $\left(z_2 - z_1^2\right)\left[\left(z_2 - z_1^2\right)^2 + 3z_2z_1^2\right] = 3v^2$. Đặt $t = z_2 - z_1^2$ khi đó vì $(z_1, z_2) = 1$ ta có $(t, z_1) = 1$ và $t\left(t^2 + 3tz_1^2 + 3z_1^4\right) = 3v^2$. Suy ra $3 \mid t$. Ta đặt $t = 3t_1$ và $t_1\left(9t_1^2 + 9t_1z_1^2 + 3z_1^4\right) = v^2$ suy ra $3 \mid v$. Vì vậy $v = 3v_1$ và vì $(z_1, 3) = 1$ suy ra số $9t_1^2 + 9t_1z_1^2 + 3z_1^4$ không chia hết cho 9, mà $9 \mid v^2$ ta suy ra $3 \mid t_1$. Vì vậy $t_1 = 3t_2$. Ta có $t_2(27t_2^2 + 9t_2z_1^2 + z_1^4) = v_1^2$ mà $(t, z_1) = 1$ suy ra $(t_2, z_1) = 1$ và $(t_2, 27t_2^2 + 9t_2z_1^2 + z_1^4) = 1$. Hơn nữa $t_2 = b^2$ và $27b^4 + 9b^2z_1^2 + z_1^4 = c^2$. Các số b và $|z_1|$ là các số tự nhiên vì nếu $b = 0$ thì $t_2 = 0$ và từ đó $t = 0$, do đó $z_2 = z_1^2$ mà $(z_1, z_2) = 1$ nên $z_1 = \pm 1$, $z_2 = 1$ suy ra $v = 0$ do đó $x = y$ mâu thuẫn với giả thiết của x, y, z. Mặt khác nếu $z_1 = 0$ thì $u = 0$, do đó $3v^2 = z_2^2$ và hệ quả là $v = 0$, mâu thuẫn. Vậy ta kết luận rằng phương trình $x^4 + 9x^2y^2 + 27y^4 = z^2$ không có nghiệm tự nhiên.

Nếu $3 \mid u$ thì vì $(u, v) = 1$ ta có $(v, 3) = 1$ do đó $u = 3u_1$ và bởi vì $u\left(u^2 + 3v^2\right) = z^3$ nên $z = 3z_1$ và $u_1\left(3u_1^2 + v^2\right) = 3z_1^3$ mà $(v, 3) = 1$ suy ra $3 \mid u_1$. Hệ quả là $u_1 = 3u_2$ và $u_2\left(27u_2^2 + v^2\right) = z_1^3$. Nhưng do $(u_2, v) = 1$ suy ra $\left(u_2, 27u_2^2 + v^2\right) = 1$, ta có $u_2 = a^3$, $27u_2^2 + v^2 = b^3$ với $(a, b) = 1$ và bởi vì $(v, 3) = 1$ nên $(b, 3) = 1$. Ta có $27a^6 + v^2 = b^3$. Đặt $t = b - 3a^2$ ta nhận được $(t, 3) = 1$ và $t\left(t^2 + 9a^2t + 27a^4\right) = v^2$. Nhưng vì $(a, b) = 1$ ta suy ra $(a, t) = 1$. Từ $(t, 3) = 1$ ta suy ra

$\left(t, t^2+9a^2t+27a^4\right)=1$. Hệ quả là $t=a_1^2$ và $t^2+9a^2t+27a^4=b_1^2$. Do đó $a_1^4+9a^2a_1^2+27a^4=b_1^2$ với $a_1\neq 0$, $a\neq 0$ vì nếu $a_1=0$ thì $t=0$ mâu thuẫn với $(t,3)=1$ và nếu $a=0$ thì $u=0$ và hệ quả là $z=0$ mâu thuẫn với $z\neq 0$. Vậy ta kết luận rằng phương trình $x^4+9x^2y^2+27y^4=z^2$ không có nghiệm tự nhiên.

Từ hai trường hợp trên suy ra điều phải chứng minh. Lời giải này thuộc về Antoni Wakulicz [1].

Định lý 9. *Phương trình $x^3+y^3=2z^3$ không có nghiệm nguyên với $x\neq y$ và $z\neq 0$.*

Định lý này suy ra không có ba lập phương phân biệt lập thành một cấp số cộng.

Cho $y=1$ hoặc $y=-1$ ta nhận thấy phương trình $x^3-2z^3=1$ không có nghiệm nguyên z, x nào ngoại trừ $x=z=-1$ và $x=1$, $z=0$ và phương trình $x^3-2z^3=-1$ không có nghiệm nguyên nào ngoại trừ $x=z=1$ và $x=-1$, $z=0$.

Hệ quả 1. *Không có số tam giác >1 nào là lập phương của một số tự nhiên.*

Chứng minh. Giả sử tồn tại số tam giác >1 là lập phương đúng. Thế thì tồn tại các số tự nhiên $m>1$ và n thỏa mãn $m(m+1)=2n^3$. Nếu m chẵn thì $m=2k$, k là số tự nhiên và $k(2k+1)=n^3$, do đó vì $(k,2k+1)=1$ ta suy ra tồn tại số tự nhiên x, z thỏa mãn $k=z^3$, $2k+1=x^3$, do đó $x^3-2z^3=1$ mà như chúng ta đã chứng minh ở trên thì điều này là không thể. Nếu m lẻ thì $m=2k-1$ trong đó k là số tự nhiên >1 (vì $m>1$) và $(2k-1)k=n^3$, do đó vì $(2k-1,k)=1$ ta suy ra tồn tại các số tự nhiên x, z thỏa mãn $2k-1=x^3$, $k=z^3$. Vì vậy $x^3-2z^3=-1$. Điều này cũng không thể xảy ra. Hệ quả được chứng minh xong. □

Hệ quả 2. *Phương trình $x^2-y^3=1$ không có nghiệm tự nhiên nào ngoại trừ $x=3$, $y=2$.*

Chứng minh. Giả sử tồn tại số tự nhiên $x\neq 3$ và y thỏa mãn $x^2-y^3=1$. Nếu x chẵn thì ta có $(x-1,x+1)=1$ và bởi vì $(x-1)(x+1)=y^3$ suy ra tồn tại các số tự nhiên a và b thỏa mãn $x-1=a^3$, $x+1=b^3$. Do đó $(b-a)(b^2+ab+a^2)=b^3-a^3=2$ và từ đó $b^2+ab+a^2\mid 2$, vô lý. Vì vậy x lẻ và do đó $x=2k+1$ trong đó k là số tự nhiên >1 (nếu $k=1$ thì $x=3$, mâu thuẫn với giả thiết). Từ $x^2-1=y^3$ suy ra y chẵn và do đó $y=2n$, ta có $k(k+1)=2n^3$ với k là số tự nhiên >1, mâu thuẫn với Hệ quả 1. Hệ quả 2 được chứng minh. □

Liên quan tới Hệ quả 2 ta nhắc lại giả thuyết Catalan nổi tiếng nói rằng phương trình $x^z-y^t=1$ chỉ có duy nhất một nghiệm tự nhiên x, y, z, t mà mỗi số đều lớn hơn 1 là $x=3$, $y=2$, $z=2$, $t=3$. Giả thuyết này chưa được chứng minh.

R.Tijdeman [1] đã hạn chế được việc giải phương trình thành các tính toán hữu hạn bằng cách đặt ra một chặn hữu hiệu cho các nghiệm. Giới hạn này được xác định cụ thể bởi M.Langevin [1]. Langevin cũng đã chứng minh giả thuyết trong trường hợp $x^z<\exp\exp\exp\exp 730$.

Nếu z và t là các số nguyên tố thì theo J.W.S.Cassels [3] ta có $z\mid y$, $t\mid x$.

A.Makowski [6] và S.Hyyro [1] đã dựa vào nhận xét này để chứng minh không tồn tại ba số tự nhiên liên tiếp mà mỗi số đều là một lũy thừa không tầm thường. Mặt khác rất dễ để chứng minh không tồn tại bốn số tự nhiên liên tiếp mà mỗi số trong chúng đều là các lũy thừa không tầm thường. Thật vậy trong bốn số tự nhiên liên tiếp luôn có một số chia 4 dư 2, nghĩa là không thể là một lũy thừa không tầm thường.

Giả thuyết của S.S.Pillai nói rằng nếu $u_1, u_2, \ldots$ là dãy vô hạn các số tự nhiên phân biệt mà mỗi số trong chúng đều là lũy thừa không tầm thường thì $\lim\limits_{n\to\infty}(u_{n+1}-u_n)=+\infty$ (Pillai [8]). Giả thuyết này

tương đương với mệnh đề: *với mỗi số tự nhiên* m *thì chỉ có hữu hạn các bộ số tự nhiên* x,y,z,t *mà mỗi số đều lớn hơn 2 và thỏa mãn phương trình* $x^y - z^t = m$.

Một vấn đề khá thú vị được đặt ra là với giá trị nào của m thì tồn tại các số tự nhiên x,y,z,t lớn hơn 1 thỏa mãn phương trình nêu trên. Dễ dàng chứng minh rằng tính chất này là khả dĩ với mọi số tự nhiên không có dạng $4k+2$ với $k=0,1,2,...$

Trong mối liên hệ này một câu hỏi khác được đặt ra là có phải với mọi số tự nhiên n đều tồn tại số tự nhiên m mà phương trình $x^y - z^t = m$ có ít nhất n nghiệm tự nhiên phân biệt x,y,z,t mà mỗi số đều lớn hơn 1 hay khổn? Câu trả lời là khẳng định. Với $k=1,2,...,n$ và $m=2^{2n}$ thì

$$m = 2^{2n} = \left(2^{2n-k-1} + 2^{k-1}\right)^2 - \left(2^{2n-k-1} - 2^{k-1}\right)^2.$$

Ta có $$3^{2n} - 2^{2n} = \left(2^{2n-k}\right)^{2k} - \left(2^{2n-k}\right)^{2k} \text{ với } k=1,2,...,n.$$

Trong dãy u_n được đề cập ở trên các phần tử nhỏ hơn 400 lần lượt là 1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, 169, 196, 216, 225, 243, 256, 289, 324, 343, 361, 400 và tương ứng dãy $u_{n+1} - u_n$ là 3, 4, 1, 7, 9, 2, 5, 4, 13, 15, 17, 19, 21, 4, 3, 16, 25, 27, 20, 9, 18, 13, 33, 35, 19, 18, 39.

Hệ quả 2^a. *Phương trình* $x^2 - y^3 = 1$ *không có nghiệm hữu tỷ ngoại trừ các nghiệm* $x=0,\ y=1,\ x=\pm 1,\ y=0,\ x=\pm 3,\ y=2$.

Chứng minh. Giả sử các số hữu tỷ x,y thỏa mãn $x^2 - y^3 = 1$. Đặt $x = h/g$, $y = r/s$ với g,s là các số tự nhiên và h,r là các số nguyên thỏa mãn $(h,g) = (r,s) = 1$. Do $x^2 - y^3 = 1$ ta có $h^2 s^3 - g^2 r^3 = g^2 s^3$. Vì vậy $h^2 s^3 = g^2\left(r^3 + s^3\right)$. Vì $(g,h) = 1$ ta có $g^2 \mid s^3$. Mặt khác, $g^2 r^3 = \left(h^2 - g^2\right)s^3$ do đó vì $(r,s) = 1$ ta có $s^3 \mid g^2$. Từ đây ta suy ra $g^2 = s^3$. Vì vậy với số tự nhiên m nào đó ta có $g = m^3$, $s = m^2$ và suy ra $h^2 - r^3 = m^6$. Vậy $r^3 = \left(h + m^3\right)\left(h - m^3\right)$ với $(m,h) = 1$. Nếu một trong các số h và m là chẵn và số còn lại là lẻ thì $\left(h + m^3, h - m^3\right) = 1$ và từ đó suy ra tồn tại a và b thỏa mãn $h + m^3 = a^3$, $h - m^3 = b^3$, do đó $a^3 + \left(-b\right)^3 = 2m^3$. Nhưng vì $m \neq 0$ suy ra $a = -b$ do đó $h = 0$ và suy ra $x = 0$, $y = 1$. Nếu cả m và h đều lẻ thì $\left(\frac{h+m^3}{2}, \frac{h-m^3}{2}\right) = 1$ và $2 \mid r$ do đó $r = 2r_1$ và $2r_1^3 = \left(\frac{h+m^3}{2}\right)\left(\frac{h-m^3}{2}\right)$. Suy ra tồn tại các số nguyên a và b thỏa mãn $h \pm m^3 = 4a^3$, $h \mp m^3 = 2b^3$. Vì vậy $b^3 + \left(\pm m\right)^3 = 2a^3$. Nếu $a = 0$ thì $h = \mp m^3 = \mp g$ do đó $x = \mp 1$, $y = 0$. Nếu $a \neq 0$ thì như ta đã biết b bằng $\pm m = a$. Vì vậy $h = 4a^3 \mp m^3 = \pm 3m^3 = \pm 3g$ do đó $x = \pm 3$, $y = 2$. Hệ quả 2^a được chứng minh. □

Hệ quả 3. *Nếu* n *là số tự nhiên lớn hơn* 1 *thì* $1^3 + 2^3 + ... + n^3$ *không phải lập phương đúng.*

Chứng minh. Ta đã biết $1^3 + 2^3 + ... + n^3 = \left(\frac{n(n+1)}{2}\right)^2 = t_n^2$.

Nếu các số t_n^2 là lập phương đúng thì t_n cũng là lập phương đúng . Mâu thuẫn với Hệ quả 1. Ở đây cần nhắc lại định lý trong chương trước (hệ quả của Định lý 16) nói rằng nếu các số tự nhiên a,b,l,m thỏa mãn $(l,m) = 1$, $a^l = b^m$ thì tồn tại số tự nhiên n thỏa mãn $a = n^m$ và $b = n^l$. □

Khó hơn một chút để chứng minh rằng với $n>1$ thì số $1^2+2^2+\ldots+n^2$ là bình phương của một số tự nhiên chỉ trong trường hợp $n=24$ [(1)]. Có một bài toán liên quan là khi nào thì phương trình $1^n+2^n+\ldots+(m-1)^n=m^n$ có nghiệm tự nhiên $m,n>1$. Bài toán này vẫn chưa được giải. Giả thuyết của P.Erdos đưa ra câu trả lời phủ định. L.Moser [2] đã chứng minh giả thuyết trong trường hợp $m\le 10^{10^6}$ (xem thêm Best và Riele [1]). Cuối cùng ta chú ý rằng có thể chứng minh phương trình $x^3+y^3=z^3$ không có nghiệm nguyên $x,y,z\neq 0$. Từ đây suy ra 1 không phải là tổng của hai lập phương hữu tỷ (Chương 11 mục 10).

15. Phương trình $x^3+y^3=az^3$ với $a>2$

Định lý 10. *Nếu a là số tự nhiên lớn hơn 2 và không chia hết cho lập phương nào lớn hơn 1 và*

(59) $$x^3+y^3=az^3$$

có nghiệm x,y,z với $(x,y)=1$, $z\neq 0$, thì phương trình này có vô hạn nghiệm như thế (xem thêm Nagell [5], trang 246).

Chứng minh. Giả sử $x,y,z,(x,y)=1$, $z\neq 0$ thỏa mãn ***(59)***. Ta có $(x,z)=1$. Đặt $d=(x,z)$ ta có $d^3\mid az^3-x^3=y^3$ do đó $d\mid y$ mà do $(x,y)=1$ suy ra $d=1$. Tương tự $(y,z)=1$. Đặt

(60) $$\delta=\left(x\left(x^3+2y^3\right),-y\left(2x^3+y^3\right),z\left(x^3-y^3\right)\right).$$

Ta có

(61) $$x\left(x^3+2y^3\right)=\delta x_1,$$

(62) $$-y\left(2x^3+y^3\right)=\delta y_1,$$

(63) $$z\left(x^3-y^3\right)=\delta z_1,$$

trong đó x_1,y_1,z_1 là các số nguyên và $(x_1,y_1,z_1)=1$.

Dựa vào đẳng thức

$$\left(x\left(x^3+2y^3\right)\right)^3-\left(y\left(2x^3+y^3\right)\right)^3=\left(x^3+y^3\right)\left(x^3-y^3\right)^3$$

Từ ***(59)*** suy ra các số x_1,y_1,z_1 thỏa mãn phương trình $x_1^3+y_1^3=az_1^3$. Nếu $x=y$ thì vì $(x,y)=1$ ta có $x=y=\pm 1$ và từ ***(59)*** suy ra $az^3=\pm 2$, vô lý vì $a>2$. Vì vậy $x\neq y$ và theo ***(63)*** suy ra $z_1\neq 0$. Nếu $d=(x_1,y_1)$ thì $d^3\mid x_1^3+y_1^3=az_1^3$. Nếu $d>1$ và $(d,z_1)=1$ thì ta có $(d^3,z_1^3)=1$ và vì $d^3\mid az_1^3$ suy ra $d^3\mid a$, mâu thuẫn với giả thiết a không có ước lập phương lớn hơn 1. Vì vậy hoặc $d=1$ hoặc $d>1$ và $(d,z_1)>1$ do đó $(x_1,y_1,z_1)>1$, vô lý.

Vì vậy ta kết luận $d=1$ và do đó $(x_1,y_1)=1$.

Hơn nữa do $x_1^3+y_1^3=az_1^3$ ta thấy $(x_1,z_1)=1$. Từ $(x,y)=1$ suy ra $(x,y^4)=1$ và vì ***(62)*** suy ra $(\delta y_1,x)=1$ (nếu $d_1\mid \delta y_1$ và $d_1\mid x$ thì theo ***(62)*** suy ra $d_1\mid y^4$ và như thế $(\delta,x)=1$.

Tương tự từ ***(61)*** ta suy ra $(\delta x_1,y)=1$ do đó $(\delta,y)=1$.

[(1)] Bài toán này được đặt ra bởi E.Lucas [1]. Lời giải đầu tiên dựa trên lý thuyết về các hàm elliptic được đưa ra bởi G.N.Watson [1]. Lời giải dựa trên lý thuyết về trường số học được đưa ra bởi Ljunggren [5]. Xem thêm Trost [1]

Vì $(x,z)=(y,z)=1$ nên ta có $(xy^3,z)=1$. Nếu $d\mid\delta$ và $d\mid z$ thì theo ***(59)*** và ***(61)*** ta có $d\mid x^3+y^3\mid x^4+xy^3$ và $d\mid x^4+2yx^3$ do đó $d\mid xy^3$. Từ đó vì $d\mid z$ và $(xy^3,z)=1$ nên $d=1$, nghĩa là $(\delta,z)=1$. Vì vậy $(\delta,x)=(\delta,y)=(\delta,z)=1$ và từ ***(61), (62), (63)*** suy ra δ là ước số của x^3+2y^3, $2x^3+y^3, x^3-y^3$ và do đó nó cũng là ước số của $x^3+2y^3+2(x^3-y^3)=3x^3$.

Vì vậy từ $(\delta,x)=1$ ta thấy $\delta\mid 3$. Vậy $\delta=1$ hoặc $\delta=3$ và trong mọi trường hợp ta đều có $\delta\le 3$. Nếu $x=0$ thì vì $(x,y)=1$ ta có $y=\pm 1$, mâu thuẫn với ***(59)*** vì $a>2$. Tương tự ta có $y\neq 0$. Mỗi một trong các số x và y là khác 0 và vì $x\neq y$ nên ta có $|x^3-y^3|\ge 1$.

Nếu các số x,y cùng dương hoặc cùng âm thì $x^2+xy+y^2=(x-y)^2+3xy\ge 1+3xy\ge 4$ và $|x^3-y^3|=|x-y|\left|(x-y)^2=3xy\right|\ge 4$. Nếu một trong các số x,y là dương và số còn lại là âm thì $xy<0$ và $x^2-xy+y^2=(x+y)^2-3xy\ge 4$; vì $x+y\neq 0$, giả sử ngược lại $x=-y$ thì theo ***(59)*** và $a>2$ suy ra $z=0$, mâu thuẫn với giả thiết. Vì vậy trong mọi trường hợp ta đều có $|x^3-y^3|\ge 4$.

Do $\delta\le 3$ nên từ công thức ***(63)*** suy ra $|z_1|>|z|$. Chứng tỏ nếu a thỏa mãn điều kiện bài toán thì từ mỗi nghiệm nguyên x,y,z với $(x,y)=1$ và $z\neq 0$ của ***(59)*** ta có thể nhận được một nghiệm khác x_1,y_1,z_1 với $(x_1,y_1)=1$ và $|z_1|>|z|$. Từ đây suy ra có vô hạn nghiệm như vậy. Định lý 10 được chứng minh. □

Các phương trình $x^3+y^3=3z^3$, $x^3+y^3=4z^3$, $x^3+y^3=5z^3$ đều không có nghiệm nguyên x,y,z với $z\neq 0$ (Selmer [1], [2]). Mặt khác từ Định lý 10 suy ra mỗi phương trình $x^3+y^3=6z^3$, $x^3+y^3=7z^3$, $x^3+y^3=9z^3$ đều có vô hạn nghiệm nguyên x,y,z với $(x,y)=1$ và $z\neq 0$. Thật vậy, ta sử dụng Định lý 10 và chú ý rằng các số 17, 37, 21 thỏa mãn phương trình thứ nhất, các số 2, $-1,1$ thỏa mãn phương trình thứ hai và các số $2,1,1$ thỏa mãn phương trình thứ ba (Nagell [5], trang 247-248). Từ đây ta suy ra một số hệ quả trong chương 11 mục 9.

16. Số tam giác

Như ta đã biết trong mục 4, số $t_n=n(n+1)/2$ được gọi là số tam giác thứ n. Danh sách 20000 số tam giác được liệt kê vào năm 1762 bởi E. de Joncourt [1]. K.Zarankiewicz [1] đã lưu ý rằng các số 21, 2211, 222111, ... đều là số tam giác. Ta có $21=\frac{6\cdot 7}{2}$, $2211=\frac{66\cdot 67}{2}$, $222111=\frac{666\cdot 667}{2}$. Bạn đọc có thể tự chứng minh nhận xét này. Các ví dụ tương tự được đưa ra bởi T.Jozefiak [1]

55, 5050, 500500, 50005000, ...
5151, 501501, 50015001, 5000150001, ...
78, 8778, 887778, 88877778, ...
45, 4950, 499500, 49995000, ...
45, 2415, 224115, 22241115, ...

Dễ dàng chứng minh tồn tại vô hạn các cặp số tam giác mà tổng đôi một của chúng đều là số tam giác. Thật vậy, dễ dàng kiểm tra rằng với số tự nhiên k ta có $t_{k-1}+k=t_k$ (với $t_0=0$). Vì vậy với $k=t_n\,(n=1,2,...)$ ta có $t_{t_n-1}+t_n=t_{t_n}$. Đặc biệt $t_2+t_2=t_3$, $t_5+t_3=t_6$, $t_9+t_4=t_{10}$, $t_{14}+t_5=t_{15}$. M.N.Khatri [1] đã tìm ra $t_{3k}+t_{4k+1}=t_{5k+1}$, $t_{5k+4}+t_{12k+9}=t_{13k+10}$, $t_{8k+4}+t_{15k+9}=t_{17k+10}$ với $k=0,1,2,...$

Đặc biệt $t_6+t_9=t_{11}$, $t_9+t_{13}=t_{16}$, $t_9+t_{21}=t_{23}$, $t_{12}+t_{24}=t_{27}$. Ta cũng có $t_{4k^2+5k+2}=t_{4k^2+5k}+t_{4k+2}$ với $k=1,2,\ldots$. Ta sẽ chứng minh tồn tại vô hạn cặp các số tự nhiên x,y thỏa mãn hệ phương trình

(64) $t_x+t_{2y}=t_{3y}$ và $t_x-t_{2y}=t_{y-1}$.

Dễ dàng chứng minh mỗi phương trình trong ***(64)*** đều tương đương với

(65) $x^2+x=5y^2+y$.

Cho nên ta chỉ cần chứng minh ***(65)*** có vô hạn nghiệm tự nhiên x,y. Sử dụng đẳng thức

$$\left(161x+360y+116\right)^2+161x+360y+116-5\left(72x+161y+52\right)^2$$
$$-\left(72x+161y+52\right)=x^2+x-5y^2-y$$

Suy ra nếu x,y tạo thành nghiệm tự nhiên của ***(65)*** thì các số $u=161x+360y+116$ và $v=72x+161y+52$ là nghiệm tự nhiên u,v của ***(65)*** mà lần lượt lớn hơn x,y. Do $x=2$ và $y=1$ thỏa mãn ***(65)*** suy ra ***(65)*** có vô hạn nghiệm tự nhiên x,y (Sierpinski [32]).

J.Browkin [1] đã sử dụng các kết quả của P.F.Teilhet [1] để đưa ra một phương pháp tìm tất cả các cặp số tam giác mà tổng và hiệu của các số trong mỗi cặp đều là số tam giác.

Với $x\le 100$ thì tồn tại t_x,t_y với $(x,y)=(6,5),(18,16),(37,27),(44,39),(86,65),(91,54)$.

Như ta đã biết (so sánh với Chương 1 mục 4) tồn tại vô hạn các số tam giác là bình phương đúng. Nhắc lại rằng từ thời Euler ta đã biết với mỗi số tự nhiên n thì số $\dfrac{\left(3+2\sqrt{2}\right)^n-\left(3-2\sqrt{2}\right)^n}{4\sqrt{2}}$ là số tự nhiên và bình phương của nó là số tam giác (Sierpinski [30]). Mặt khác, W.Ljunggren [4] đã chứng minh rằng chỉ tồn tại hai số tam giác mà bình phương là số tam giác, ký hiệu là t_1 và t_6.

Định lý 11. *Không tồn tại số tam giác >1 là lũy thừa bậc bốn.*

Chứng minh. Giả sử phản chứng tồn tại số tự nhiên m và $n>1$ mà $\frac{1}{2}n(n+1)=m^4$ được thỏa mãn. Khi đó $n(n+1)=2m^4$ và do đó $n=2k$ suy ra $k(2k+1)=m^4$. Vì $(k,k+1)=1$ nên suy ra tồn tại các số tự nhiên x,y thỏa mãn $k=y^4$, $2k+1=x^4$ và do đó $2y^4+1=x^4$. Nếu n lẻ thì $n=2k-1$ và do đó $(2k-1)k=m^4$. Vì $(2k-1,k)=1$ suy ra tồn tại các số tự nhiên x,y thỏa mãn $2k-1=x^4,k=y^4$. Từ đây ta có $2y^4-1=x^4$ và từ $2k-1=n>1$ suy ra $y>1$. Vậy $y^4=k>1$.

Để hoàn tất chứng minh ta cần chứng minh rằng

1) Không tồn tại x,y thỏa mãn $2y^4+1=x^4$,

2) Không tồn tại x và $y>1$ thỏa mãn $2y^4-1=x^4$.

Để chứng minh 1) ta chú ý rằng nếu $2y^4+1=x^4$ thì ta có $\left(y^2\right)^4+x^4=\left(y^4+1\right)^2$, mâu thuẫn với Hệ quả 2 mục 6. Để chứng minh 2) ta giả sử $2y^4-1=x^4$ và do đó $\left(y^2\right)^4-x^4=\left(y^4-1\right)^2$. Nhưng do $y^4>1, y^4-1$ là số tự nhiên, mâu thuẫn với Hệ quả 1 mục 6. Định lý được chứng minh. □

Tuy nhiên vẫn có thể xảy ra tình huống với các số hữu tỷ t và u thì $\dfrac{1}{2}t(t+1)=u$ chẳng hạn với $t=\dfrac{32}{49}$ ta có $\dfrac{1}{2}t(t+1)=\left(\dfrac{6}{7}\right)^2$. Chú ý rằng phương trình $2y^4+1=z^2$ không có nghiệm tự nhiên y,z

ngoại trừ $2\cdot 13^4-1^4=239^2$. Có thể chứng minh rằng phương trình $2y^4-1=z^2$ chỉ có hai nghiệm tự nhiên y,z là $y=z=1$ và $y=13,\ z=239$ (Ljunggren [1]).

Có thể sử dụng kết quả quen thuộc về phương trình $x^n+y^n=2z^n$ (Denes [1]) để suy ra rằng các số tam giác đều không thể là lũy thừa bậc n của một số tự nhiên với $2<n\le 30$. Mặt khác theo định lý tổng quát hơn (Schinzel và Tijdeman [1]) thì phương trình $P(x)=y^m$, trong đó P là đa thức với hệ số hữu tỷ với ít nhất hai hệ số khác 0, có thể có vô hạn nghiệm nguyên x,y với $y>1,m>2$. Vì vậy số tam giác không thể là lũy thừa bậc n của một số tự nhiên với n lớn hơn một giác trị n_0 nào đó. Theo E.Z.Chein [2] thì có thể chọn $n_0=7.877\cdot 10^8$.

Dễ dàng nhận thấy với số tự nhiên n thì $n(n+1)$ không thể là bình phương đúng. Thật vậy, nếu ta có $n(n+1)=a^2$ thì vì $(n,n+1)=1$ suy ra các số n, $n+1$ đều là bình phương. Vậy $n=k^2, n+1=l^2$ và do đó $(l-k)(l+k)=l^2-k^2=1$. Vô lý. Tuy nhiên với $n=\frac{2}{3}$ thì ta có $\frac{1}{3}\left(\frac{1}{3}+1\right)=\left(\frac{2}{3}\right)^2$.

Tương tự ta có thể chứng minh tích của hai số tự nhiên liên tiếp không thể là lũy thừa bậc lớn hơn 1. Chứng minh cho định lý Goldbach nói rằng tích của ba số tự nhiên liên tiếp không thể là bình phương cũng tương đối đơn giản. Thật vậy, ta có thể chứng minh rằng tích của ba số tự nhiên liên tiếp không thể là lũy thừa bậc lớn hơn 1. Giả sử tồn tại các số tự nhiên n,k và $s>1$ mà $n(n+1)(n+2)=k^s$. Do $(n+1,n(n+2))=1$ áp dụng Định lý 8 Chương 1 suy ra tồn tại a,b thỏa mãn $n+1=a^s$ và $n(n+2)=b^s$. Từ đó $1=(n+1)^2-n(n+2)=(a^2)^s-b^s$ vô lý.

P.Erdos và J.L. Selfridge [1] đã chứng minh tích của k số nguyên dương liên tiếp với $k>1$ không thể là lũy thừa bậc lớn hơn 1 và tích của k số lẻ liên tiếp với $k>1$ cũng không thể là lũy thừa bậc lớn hơn 1 (Erdos [5]). Hơn nữa với số tự nhiên $k>3$ và $n\ge 2k$ thì số $\binom{n}{k}$ không thể là lũy thừa bậc lớn hơn 1 (P.Erdos [11]).

Các số có dạng $T_n=\frac{1}{6}n(n+1)(n+2)$ (với n là số tự nhiên) được gọi là số tứ diện. Tên gọi này được đặt theo số các hình cầu có cùng bán kính có thể chứa trong các tứ diện. Mười số tứ diện đầu tiên là $1,4,10,20,35,56,84,120,165,220$. Với $n=1,2,48$ ta nhận được các số tứ diện $1^2,2^2,140^2$ là bình phương đúng. Có thể chứng minh đây là tất cả các số tứ diện có tính chất này. Tính chất này được chứng minh bởi A.Meyl [1] dựa trên sự kiện là các số $s_n=1^2+2^2+\ldots+n^2$ là bình phương khi và chỉ khi $n=1$ hoặc $n=24$ (xem thêm mục 14). Ngược lại, giả sử với số tự nhiên n ta có $s_n=m^2$ với m là số tự nhiên. Khi đó ta có thể kiểm tra $4s_n=T_{2n}$. Suy ra $T_{2n}=(2m)^2$ vì $2n$ bằng 2 hoặc 48 nghĩa là $n=1$ hoặc $n=24$.

Tồn tại các số tự nhiên vừa là số tứ diện vừa là số tam giác. E.T.Avanesov [1] đã chứng minh tất cả các số như vậy là $n=1,10,120,1540,7140$. Với các số này thì ta có $n=\frac{1}{2}x(x+1)=\frac{1}{6}y(y+1)(y+2)$ lần lượt với $x=1,4,15,55,119; y=1,3,8,20,34$.

Ta có $T_n-T_{n-1}=t_n$ và $T_n+T_{n+1}=1^2+2^2+\ldots+(n+1)^2$.

Có thể chứng minh tồn tại vô hạn cặp các số tứ diện mà tổng (hoặc hiệu) của các số trong mỗi cặp cũng là số tứ diện (Rohr [1], Sierpinski [33], Wunderlich [1], Bremner [1]). Ta chưa biết có cặp số tứ diện nào mà cả tổng và hiệu của chúng đều là số tứ diện hay không. H.E.Salzer [1] đã đưa ra giả thuyết nói rằng mọi bình phương đều là tổng của nhiều nhất là bốn số tứ diện và ông ta đã chứng minh tính chất này với mọi bình phương $\le 10^6$. Đặc biệt

$$1^2 = T_1, 2^2 = T_2, 3^2 = T_1 + T_2 + T_2, 4^2 = T_1 + T_1 + T_2 + T_3, 5^2 = T_1 + T_2 + T_4 = T_1 + T_2 + T_3 + T_3,$$
$$6^2 = T_1 + T_5, 7^2 = T_2 + T_3 + T_5, 8^2 = T_2 + T_2 + T_6, 9^2 = T_1 + T_2 + T_4 + T_6, 10^2 = T_2 + T_4 + T_4 + T_6.$$

Dễ dàng chứng minh mọi số tự nhiên đều là tổng của bốn số tứ diện. Thật vậy ta có $1 = T_1 + T_4 - T_3 - T_3, 2 = T_4 - T_3 - T_3 - T_2$ và với số tự nhiên n > 2 ta có $n = T_n + T_{n-2} - T_{n-1} - T_{n-1}$. Tuy nhiên chứng minh mọi số tự nhiên đều là tổng của nhiều nhất 8 số tứ diện là khó hơn (Watson [2]). Các số tự nhiên $\le 10^7$ đều là tổng của nhiều nhất 5 số tứ diện (Salzer và Levine [1]).

17. Phương trình $x^2 - Dy^2 = 1$

Trong mục này ta nghiên cứu các phương trình nghiệm nguyên với số tự nhiên D cho trước

(66) $x^2 - Dy^2 = 1$

Phương trình này được gọi là phương trình Fermat hoặc là phương trình Pell. Phương trình này có các nghiệm tầm thường $x = 1, y = 0$ và $x = -1,\ y = 0$. Ta chỉ cần tìm các nghiệm tự nhiên của ***(66)***. Nếu D là bình phương thì ***(66)*** có thể viết thành $(x - ny)(x + ny) = 1,$ do đó $x + ny \mid 1$, vô lý vì x, y là các số tự nhiên. Vì vậy nếu D là bình phương thì phương trình ***(66)*** không có nghiệm tự nhiên. Để chứng minh phương trình cũng vô nghiệm trong trường hợp còn lại ta xét bổ đề

Bổ đề. *Nếu* D *không phải bình phương đúng thì tồn tại vô hạn cặp số phân biệt* x, y *thỏa mãn*

(67) $y \ne 0$ và $|x^2 - Dy^2| < 2\sqrt{D} + 1$

Chứng minh. Với mỗi $k = 0, 1, 2, \ldots, n$ ký hiệu l_k là số tự nhiên lớn nhất $\le k\sqrt{D} + 1$.

Ta có $l_k \le k\sqrt{D} + 1$ và $l_k + 1 > k\sqrt{D} + 1$. Vì vậy

(68) $0 < l_k - k\sqrt{D} \le 1$

Ta có $n+1$ số $l_k - k\sqrt{D} (k = 0, 1, 2, \ldots, n)$ là phân biệt vì nếu $l_k - k\sqrt{D} = l_{k'} - k'\sqrt{D}$ thì ta có $l_k - l_{k'} = (k - k')\sqrt{D}$ trong đó $k \ne k'$ là không thể xảy ra vì nếu ngược lại thì $\sqrt{D}$ là bình phương hữu tỷ và suy ra D là bình phương đúng, mâu thuẫn với giả thiết.

Theo ***(68)*** thì các số $u = l_k - k\sqrt{D} (k = 0, 1, 2, \ldots, n)$ phải thỏa mãn một trong các bất đẳng thức $0 < u \le \frac{1}{n},\ \frac{1}{n} < u \le \frac{2}{n},\ \ldots,\ \frac{n-1}{n} < u \le \frac{n}{n}$. Suy ra ít nhất có hai giá trị phân biệt u' và u'' thỏa mãn cùng một ước lượng, nghĩa là $\frac{j-1}{n} < u' \le \frac{j}{n},\quad \frac{j-1}{n} < u'' \le \frac{j}{n},$ trong đó $j = 1, 2, \ldots, n$.

Từ giả thiết $u' \ne u''$ ta có thể giả sử rằng $u' > u''$. Bất đẳng thức $u' \le k/n$ và $u'' > (k-1)/n$ suy ra $0 < u' - u'' < \frac{1}{n}$. Do $u' = l_k - k\sqrt{D}, u'' = l_i - i\sqrt{D}$ trong đó k, i thuộc về $0, 1, 2, \ldots, n$ thì đặt $x = l_k - l_i, y = i - k$ ta suy ra

(68ª) $0 < x - y\sqrt{D} < \frac{1}{n}$

Hiển nhiên vì x, y là các số nguyên và $y = i - k$. Vì vậy y là hiệu của hai chỉ số khác nhau từ dãy $0, 1, 2, \ldots, n$, nên nó khác 0 và không lớn hơn n nghĩa là

(69) $0 < |y| \le n$

Theo ***(68ª)*** ta có $y\sqrt{D} < x < y\sqrt{D} + \frac{1}{n}$.

Theo ***(69)*** suy ra $-\left(n\sqrt{D} + \frac{1}{n}\right) < -n\sqrt{D} < x < n\sqrt{D} + \frac{1}{n}$, và hệ quả là $|x| < n\sqrt{D} + \frac{1}{n}$.

Từ đó theo ***(69)*** thì $\left|x + y\sqrt{D}\right| \le |x| + |y|\sqrt{D} < 2n\sqrt{D} + \frac{1}{n}$.

Nhân hai vế với ***(68ª)*** suy ra $\left|x^2 - Dy^2\right| < 2\sqrt{D} + 1$. Vì vậy tồn tại x, y thỏa mãn ***(67)*** và ***(68ª)***. Từ đây suy ra tồn tại vô hạn cặp số tự nhiên x, y thỏa mãn ***(67)*** và

(70) $$0 < x - y\sqrt{D}.$$

Giả sử ngược lại, nghĩa là chỉ tồn tại hữu hạn cặp số như vậy. Ký hiệu

(71) $$(x_1, y_1), \quad (x_2, y_2), \quad ..., \quad (x_s, y_s)$$

là tất cả các cặp số đó. Khi đó các số

(72) $$x_1 - y_1\sqrt{D}, \quad x_2 - y_2\sqrt{D}, \quad ..., \quad x_s - y_s\sqrt{D}$$

đều là dương. Gọi α là số nhỏ nhất trong đó. Số tự nhiên n thỏa mãn

(73) $$\frac{1}{n} < \alpha .$$

Ở trên ta đã chứng minh tồn tại ít nhất một cặp số x, y thỏa mãn cả ***(67)*** và ***(68ª).*** Từ ***(68ª)*** và ***(73)*** ta có $0 < x - y\sqrt{D} < \alpha$. Nhưng do α là nhỏ nhất trong các số ở dãy ***(72)*** nên $x - y\sqrt{D}$ không thuộc về dãy đó, nghĩa là cặp (x, y) không trùng với cặp nào trong ***(71)*** và đều thỏa mãn ***(67),(68ª)*** và do đó thỏa mãn cả ***(70)***. Điều này mâu thuẫn với định nghĩa trong ***(71)***. Vậy có vô hạn các cặp số x, y thỏa mãn ***(67)*** và ***(70)***. Bổ đề được chứng minh. □

Định lý 12. *Nếu số tự nhiên D không phải bình phương đúng thì phương trình $x^2 - Dy^2 = 1$ có vô hạn nghiệm tự nhiên x, y.*

Chứng minh. Do số các số nguyên với trị tuyệt đối nhỏ hơn $2\sqrt{D} + 1$ là hữu hạn và theo bổ đề thì tồn tại vô hạn cặp (x, y) thỏa mãn bất đẳng thức ***(67)*** nên tồn tại vô hạn cặp số nguyên x, y mà $x^2 - Dy^2$ bằng với một số k xác định và khác 0 (trường hợp $D = x^2 / y^2$ được loại bỏ). Ký hiệu tập hợp tất cả các cặp số x, y như vậy là Z. Với số nguyên t ký hiệu $r(t)$ là phần dư nhận được khi chia t cho k. Với x, y thuộc Z ta xét cặp $r(x), r(y)$. Rõ ràng có nhiều nhất k^2 cặp số phân biệt như vậy. Bây giờ ta chia Z thành các lớp với giả thiết x, y và x', y' thuộc cùng một lớp nếu và chỉ nếu $r(x) = r(x')$ và $r(y) = r(y')$. Do số cặp $r(x), r(y)$ phân biệt là hữu hạn mà Z vô hạn nên ít nhất một trong các lớp là vô hạn. Trong lớp đó tồn tại hai cặp a, b và c, d mà ít nhất một trong các đẳng thức $|a| = |c|, |b| = |d|$ sai bởi vì với cặp a, b cho trước tồn tại nhiều nhất 4 cặp c, d như vậy. Các hiệu $a^2 - Db^2$ và $c^2 - Dd^2$ đều bằng k (vì các cặp a, b và c, d đều thuộc Z). Nhưng do a, b và c, d thuộc cùng một lớp nên suy ra $r(a) = r(c)$ và $r(b) = r(d)$. Vì vậy tồn tại các số nguyên t và v thỏa mãn $a - c = kt$ và $b - d = kv$. Từ đó

(74) $$a = c + kt, \; b = d + kv,$$

Trong đó t và v đều nguyên. Nhân các đẳng thức

(75) $a^2-Db^2=k,\ c^2-\mathrm{D}\mathrm{d}^2=k$

và sử dụng đẳng thức $\left(a^2-Db^2\right)\left(c^2-Dd^2\right)=\left(ac-Dbd\right)^2-D\left(ad-cb\right)^2$ ta suy ra

(76) $\left(ac-Dbd\right)^2-D\left(ad-cb\right)^2=k^2$

Từ ***(74)*** và ***(75)*** suy ra $ac-Dbd=\left(c+kt\right)c-D\left(d+kv\right)d=c^2-Dd^2+k\left(ct-Ddv\right)$ và cũng có $ad-cb=\left(c+kt\right)d-c\left(d+kv\right)=k\left(dt-cv\right)$. Vì vậy nếu ta chia cả hai vế của ***(76)*** cho k^2 thì ta có $\left(1+ct-Ddv\right)^2-D\left(dt-cv\right)^2=1$. Từ đây đặt $x=\left|1+ct-Ddv\right|, y=\left|dt-cv\right|$ ta suy ra $x^2-Dy^2=1$. Ta sẽ chứng minh $y\neq 0$. Nếu $y=0$ suy ra $|x|=1$ vì vậy $1+ct-Ddv=\pm 1,\quad dt-cv=0$.

Nhân đẳng thức thứ nhất với c và thứ hai với $-Dd$ sau đó cộng lại ta suy ra $c+\left(c^2-Dd^2\right)t=\pm c,$ từ đó theo ***(74)*** và ***(75)*** suy ra $a=\pm c$, nghĩa là $\left|a\right|=\left|c\right|$.

Tương tự nhân đẳng thức thứ nhất với d và thứ hai với –c sau đó cộng lại ta có $d+\left(c^2-Dd^2\right)v=\pm d,$ do đó theo ***(74)*** và ***(75)*** ta suy ra $b=\pm d$, nghĩa là $\left|b\right|=\left|d\right|$. Nhưng từ đẳng thức này và $\left|a\right|=\left|c\right|$ suy ra mâu thuẫn với định nghĩa của a,b và c,d.

Vì vậy ta đã chứng minh tồn tại ít nhất một cặp x,y thỏa mãn $x^2-Dy^2=1$ với $y\neq 0$ (như thế $x\neq 0$). Đổi dấu nếu cần ta thu được nghiệm tự nhiên của ***(66)***. Nếu đẳng thức $x^2-Dy^2=1$ đúng với các số tự nhiên x,y nào đó thì rõ ràng $\left(2x^2-1\right)^2-D\left(2xy\right)^2=1$ với $2xy>y$. Vì vậy từ một nghiệm tự nhiên x,y bất kỳ của ***(66)*** ta thu được nghiệm tự nhiên x',y' mà $x'>x$ và $y'>y$. Suy ra ***(66)*** có vô hạn nghiệm tự nhiên. Định lý 12 được chứng minh. □

Để tìm các nghiệm của ***(66)*** một cách hữu hiệu ta áp dụng thủ tục sau: trong $1+Dy^2$ ta lần lượt thay y bởi các số tự nhiên $1,2,3,\ldots$ và ký hiệu u là số y đầu tiên mà $1+Dy^2$ là bình phương đúng. Khi đó ta đặt $1+Du^2=t^2$. Cặp $\left(t,u\right)$ là nghiệm của ***(66)*** với t,u là các số tự nhiên nhỏ nhất như thế vì với mọi nghiệm x,y khác của ***(66)*** ta có $y>u$ suy ra $x=\sqrt{1+Dy}>\sqrt{1+Du^2}=t$ nên $x>t$.

Trong các trường hợp riêng thì rất dễ để tìm nghiệm của ***(66)***. Đặc biệt nếu D có dạng a^2-1 trong đó a là số tự nhiên $\left(>1\right)$ thì nghiệm nhỏ nhất của ***(66)*** là $t=a,u=1$. Tương tự nếu $D=a\left(a+1\right)$ với a là số tự nhiên thì nghiệm nhỏ nhất là $t=2a+1,u=2$ vì ta có $\left(2a+1\right)^2-D\cdot 2^2=1$ và nếu với số tự nhiên $x,x^2-D\cdot 1^2=1$ thì ta sẽ có $x^2=a^2+a+1$ do đó $x^2>a^2$ suy ra $x>a$ nên $x\geq a+1$ và vì vậy $x^2\geq a^2+2a+1>a^2+a+1$ mâu thuẫn. Trong trường hợp $D=a^2+2$ với a là số tự nhiên thì ta chứng minh được nghiệm nhỏ nhất của ***(66)*** là $t=a^2+1,u=a$ và cũng vậy nếu $D=a^2+1$ thì các nghiệm nhỏ nhất là $t=2a^2+1,u=2a$.

Ví dụ. Với $D=2$ phương trình ***(66)*** trở thành $x^2-2y^2=1$. Lần lượt thay 1 và 2 cho y trong $1+2y^2$ ta nhận được 2 và 9. Nghiệm nhỏ nhất là $x=3,y=2$. Với $D=3$ phương trình ***(66)*** trở thành $x^2-3y^2=1$. Thay 1 cho y trong $1+3y^2$ ta nhận được bình phương của 2. Vì vậy nghiệm nhỏ nhất là $t=2,u=1$. Với $D=5$ ta có phương trình $x^2-5y^2=1$, thay $1,2,3,4$ cho y trong $1+5y^2$ ta nhận được $6,21,46,81$. Nghiệm nhỏ nhất là $t=9,u=4$. Với $D=11$ ta có phương trình $x^2-11y^2=1$, thay $1,2,3$ cho y trong $1+11y^2$ ta nhận được $12,45,100$. Nghiệm nhỏ nhất là $t=10,u=3$.

Phương pháp tìm nghiệm trên mặc dù đơn giản nhưng trên thực tế nó không thực sự hữu dụng vì trong nhiều trường hợp thì phương pháp này yêu cầu một lượng phép thử rất lớn. Ví dụ xét phương trình $x^2-13y^2=1$ ta tìm được $t=649, u=180$ với 180 phép thử. Đặc biệt với phương trình

(77) $$x^2-991y^2=1$$

Nghiệm nhỏ nhất là

$$t=379516400906811930638014896080,$$
$$u=12055735790331359447442538767.$$

Như thế nếu ta sử dụng 10^{28} phép thử sau đó kết luận rằng phương trình ***(77)*** vô nghiệm thì ta sẽ thu được một kết luận không đúng. Trong Chương 8 mục 5 ta sẽ trình bày một phương pháp hữu hiệu hơn để tìm nghiệm nhỏ nhất của ***(66)***. Phương pháp này sẽ không quá tốn thời gian để tính toán. Mặt khác ta để ý rằng nếu D không phải bình phương đúng thì có thể tìm tất cả các nghiệm hữu tỷ của ***(66).*** Thật vậy, với số hữu tỷ r tùy ý ta đặt $x=\left(r^2+D\right)/\left(r^2-D\right), y=2r/\left(r^2-D\right)$ thì

$$1+Dy^2=1+D\left(\frac{2r}{r^2-D}\right)^2=\frac{\left(r^2-D\right)+4Dr^2}{\left(r^2-D\right)^2}=\left(\frac{r^2+D}{r^2-D}\right)^2=x^2,$$

Do đó $x^2-Dy^2=1$. Dễ dàng chứng minh tất cả các nghiệm của ***(66)*** đều thu được theo cách này. Việc tìm tất cả các nghiệm hữu tỷ của ***(66)*** tương đương với việc tìm nghiệm nguyên của phương trình $x^2-Dy^2=z^2$. Bây giờ ta trở lại với việc tìm tất cả các nghiệm tự nhiên của phương trình ***(66)***.

Định lý 13. *Tất cả các nghiệm tự nhiên của phương trình* $x^2-Dy^2=1$ *là*

(78) $$(t_0,x_0),(t_1,x_1),(t_2,x_2),\ldots$$

Trong đó $\left(t_0,u_0\right)$ *là nghiệm nhỏ nhất và* $\left(t_k,u_k\right)$ *được xác định bởi*

(79) $$t_{k+1}=t_0t_k+Du_0u_k, u_{k+1}=u_0t_k+t_0u_k, k=0,1,2,\ldots$$

Chứng minh. Để chứng minh các bộ số trong ***(78)*** đều thỏa mãn phương trình ***(66)*** thì ta giả sử với $k\geq 0$ cặp $\left(t_k,u_k\right)$ thỏa mãn ***(66)***. Rõ ràng các số trong ***(79)*** là tự nhiên và từ đẳng thức $t_{k+1}^2-Du_{k+1}^2=(t_0t_k+Du_0u_k)^2-D(u_0t_k+t_0u_k)^2=(t_0^2-Du_0^2)(t_k^2-Du_k^2)$ suy ra $\left(t_{k+1},u_{k+1}\right)$ cũng thỏa mãn phương trình ***(66)***. Vì vậy ta chỉ cần chỉ ra tất cả các nghiệm $\left(x,y\right)$ của phương trình $x^2-Dy^2=1$ đều chứa trong dãy ***(78)***. Ta chứng minh bổ đề sau đây

Bổ đề. *Nếu* $\left(x,y\right)$ *là nghiệm tự nhiên của* $x^2-Dy^2=1$ *mà* $u_0<y$ *thì với*

(80) $$\zeta=t_0x-Du_0y, \eta=-u_0x+t_0$$

với ζ,η đều là các số tự nhiên, $\eta<y$ và $\zeta^2-D\eta^2=1$.

Chứng minh. Từ ***(80)*** ta có $\zeta^2-D\eta^2=\left(t_0x-Du_0y\right)^2-D\left(-u_0x+t_0y\right)^2=\left(t_0^2-Du_0^2\right)\left(x^2-Dy^2\right)$.

Hệ quả là từ $t_0^2-Du_0^2=1$ và $x^2-Dy^2=1$ suy ra $\zeta^2-D\eta^2=1$. Do đó chỉ cần chứng minh rằng nếu ζ và η là các số tự nhiên và $\eta<y$ thì các bất đẳng thức $0<t_0x-Du_0y$ và $0<-u_0x+t_0y<y$ là đúng. Đầu tiên ta chú ý $D^2u_0^2y^2=\left(t_0^2-1\right)\left(x^2-1\right)<t_0^2x^2$ do đó $Du_0y<t_0x$ và từ $u_0<y$ ta có $\left(\frac{x}{y}\right)^2=D+\frac{1}{y^2}<D+\frac{1}{u_0^2}=\left(\frac{t_0}{u_0}\right)^2$. Hệ quả là $x/y<t_0/u_0$ suy ra $u_0x<t_0y$ do đó $0<-u_0x+t_0y$.

Để chứng minh $-u_0x + t_0y < y$ ta chú ý vì $t_0^2 = Du_0^2 + 1$ suy ra $t_0 > 1$ do đó $x^2(2 - 2t_0) < 0 < (t_0 - 1)^2$. Cộng $x^2(t_0^2 - 1)$ vào mỗi vế của bất đẳng thức cuối ta suy ra $x^2(t_0^2 - 2t_0 + 1) < x^2(t_0^2 - 1) + (t_0 - 1)^2$. Do đó $(x^2 - 1)(t_0 - 1)^2 < x^2(t_0^2 - 1)$ và hệ quả là $Dy^2(t_0 - 1)^2 < x^2Du_0^2$ suy ra $y^2(t_0 - 1)^2 < x^2u_0^2$ vì vậy $y(t_0 - 1) < xu_0$ nghĩa là $-xu_0 + t_0y < y$. Bổ đề được chứng minh. □

Bây giờ giả sử tồn tại nghiệm tự nhiên của phương trình $x^2 - Dy^2 = 1$ mà không thuộc dãy ***(78)*** thì trong số đó ta chọn nghiệm (x, y) mà y lấy giá trị nhỏ nhất. Khi đó y vẫn lớn hơn u_0 vì nghiệm (t_0, u_0) là nghiệm nhỏ nhất và nếu $y = u_0$ suy ra $x = t_0$, mâu thuẫn với giả thiết (x, y) không thuộc dãy ***(78).*** Từ bổ đề lấy các số ζ, η có dạng ***(80)*** định nghĩa từ nghiệm x, y ta nhận thấy chúng thỏa mãn phương trình $x^2 - Dy^2 = 1$ và $\eta < y$. Từ định nghĩa của nghiệm (x, y) suy ra (ζ, η) thuộc dãy ***(78)***. Vì vậy tồn tại $k \geq 0$ mà $\zeta = t_k, \eta = u_k$. Khi đó theo các công thức ***(79), (80)*** và $t_0^2 - Du_0^2 = 1$ suy ra

$$t_{k+1} = t_0\zeta + Du_0\eta = t_0(t_0x - Du_0y) + Du_0(-u_0x + t_0y) = (t_0^2 - Du_0^2)x = x,$$

$$u_{k+1} = u_0\zeta + t_0\eta = u_0(t_0x - Du_0y) + t_0(-u_0x + t_0y) = (t_0^2 - Du_0^2)y = y,$$

Từ đó suy ra (x, y) lại thuộc về dãy ***(78)***. Mâu thuẫn. Định lý 13 được chứng minh. □

Đặc biệt với phương trình $x^2 - 2y^2 = 1$ mà $t_0 = 3, u_0 = 2$ thì theo công thức ***(79)*** ta tìm được dãy tất cả các nghiệm của nó là $t_1 = 3^2 + 2 \cdot 2^2 = 17$, $u_1 = 2 \cdot 3 + 3 \cdot 2 = 12$, $t_2 = 99$, $u_2 = 70$, $t_3 = 577$, $u_3 = 408$, ...

Antoni Wakulicz đã chỉ ra từ ***(79)*** suy ra $t_{k+1} = 2t_0t_k - t_{k-1}$, $u_{k+1} = 2t_0u_k - u_{k-1}$ với $k = 0, 1, 2, \ldots$

Bây giờ ta chứng minh rằng

(81) $$t_{n-1} + u_{n-1}\sqrt{D} = (t_0 + u_0\sqrt{D})^n \text{ với } n = 0, 1, 2, \ldots$$

Công thức ***(81)*** đúng với $n = 1$. Giả sử nó đúng với n. Sử dụng ***(79)*** với $k = n - 1$ suy ra

$$t_n + u_n\sqrt{D} = t_0t_{n-1} + Du_0u_{n-1} + (u_0t_{n-1} + t_ou_{n-1})\sqrt{D}$$
$$= (t_0 + u_0\sqrt{D})(t_{n-1} + u_{n-1}\sqrt{D}),$$

Do đó theo (81) suy ra $t_n + u_n\sqrt{D} = (t_0 + u_0\sqrt{D})^{n+1}$, chứng tỏ ***(81)*** đúng với $n + 1$ và vì vậy theo quy nạp suy ra điều phải chứng minh. Từ Định lý 13 và công thức ***(81)*** dẫn tới định lý sau

Định lý 14. *Nếu t_0, u_0 là nghiệm tự nhiên nhỏ nhất phương trình $x^2 - Dy^2 = 1$ thì cặp số tự nhiên t, u là nghiệm của phương trình này khi và chỉ khi*

(82) $$t + u\sqrt{D} = (t_0 + u_0\sqrt{D})^n \quad \text{với n nào đó.}$$

Với các số tự nhiên a, b, c, d tùy ý đẳng thức $a + b\sqrt{D} = c + d\sqrt{D}$ suy ra $a = c, b = d$ (vì $\sqrt{D}$ vô tỷ). Vì vậy khai triển vế phải của ***(81)*** theo công thức nhị thức và thu gọn nó về dạng $c + d\sqrt{D}$ với c, d là các số tự nhiên ta suy ra $t_{n-1} = c, u_{n-1=d}$. Ta chú ý rằng theo công thức ***(82)*** của tất cả các nghiệm tự nhiên của ***(66)*** thì ta có thể thu được tất cả các nghiệm nguyên của nó. Thật vậy nếu t, u là nghiệm tự nhiên của ***(66)*** thì theo Định lý 14 đẳng thức ***(82)*** đúng với số n nào đó. Mà $t - u\sqrt{D} = 1/(t + u\sqrt{D})$ (ta giả sử $t^2 - Du^2 = 1$) suy ra $t - u\sqrt{D} = 1/(t_0 + u_0\sqrt{D})^{-n}$. Các số $t, -u$ thu được từ t, u bằng cách đổi dấu, hai nghiệm còn lại thuộc lớp này là $(-t, -u), (-t, u)$. Ta có

Định lý 15. *Mọi nghiệm nguyên của phương trình* ***(66)*** *đều có dạng* $t+u\sqrt{D}=\pm(t_0+u_0\sqrt{D})^k$ *với* k *là số nguyên thích hợp và* u_0,t_0 *là nghiệm tự nhiên nhỏ nhất. Ngược lại, tất cả các bộ số nguyên* t,u *nhận được từ công thức trên đều là nghiệm của phương trình* ***(66).*** *Nghiệm* $t=\pm1,u=0$ *có được khi* $k=0$.

Các nghiệm của phương trình ***(66)*** cho ta một phương pháp xấp xỉ căn bậc hai của một số tự nhiên bởi các số hữu tỷ. Thật vậy, từ ***(66)*** ta có $x-y\sqrt{D}=1/\left(x+y\sqrt{D}\right),$ cho nên

$$0<x/y-\sqrt{D}=1/y\left(x+y\sqrt{D}\right)<1/y^2\sqrt{D}<1/y^2.$$

Vì vậy nếu x,y là nghiệm tự nhiên của ***(66)*** thì phân số x/y xấp xỉ số $\sqrt{D}$ với sai số nhỏ hơn nghịch đảo bậc 2 của mẫu số. Rõ ràng x/y là tối giản. Đặc biệt bốn nghiệm đã được liệt kê của phương trình $x^2-2y^2=1$ cho ta phân số $577/408$ là xấp xỉ của $\sqrt{2}$ với độ chính xác 5 chữ số sau dấu phẩy thập phân (vì $408^2>10^5$).

Tiếp theo để có ước lượng chính xác với ít bước thử hơn ta sử dụng công thức sau đây. Công thức này cho phép ta *nhảy* trực tiếp từ nghiệm t_{n-1},u_{n-1} tới nghiệm t_{2n-1},u_{2n-1}.

Từ ***(81)*** ta có $t_{2n-1}+u_{2n-1}\sqrt{D}=\left(t_0+u_0\sqrt{D}\right)^{2n}=\left(t_{n-1}+u_{n-1}\sqrt{D}\right)^2$, do đó từ $t_{n-1}^2-Du_{n-1}^2=1$ suy ra

$$t_{2n-1}=t_{n-1}^2+Du_{n-1}^2=t_{n-1}^2+\left(t_{n-1}^2-1\right)=2t_{n-1}^2-1,\ u_{2n-1}=2t_{n-1}u_{n-1}.$$

Vì vậy ta có $t_{2n-1}/u_{2n-1}=\left(2t_{n-1}^2-1\right)/\left(2t_{n-1}u_{n-1}\right)$. Đặc biệt do $t_2/u_2=99/70$ là một xấp xỉ $\sqrt{2}$, ta có phân số $t_5/u_5=19601/13860$ là xấp xỉ $\sqrt{2}$ với độ chính xác 8 chữ số sau dấu phẩy thập phân.

Về số $\sqrt{2}$ ta lưu ý rằng năm 1950 R.Coustal [1] đã tìm ra ước lượng với 1033 chữ số (xem thêm E.Borel [2]) và năm 1951 H.S.Uhler [1] đã tìm ra khai triển với 1543 chữ số của nó. Trong công trình đó tác giả cũng chỉ ra biểu diễn với 1301 chữ số của $\sqrt{3}$. Cho tới bây giờ thì ta đã biết biểu diễn $\sqrt{2}$ với 10^6 chữ số và 24576 chữ số đối với $\sqrt{3}$ (Beyer, Metropolia và Neuregerard [1]).

Trở lại với phương trình $x^2-2y^2=1$ ta sẽ chứng minh rằng phương trình này không có các nghiệm tự nhiên x,y nào mà x là bình phương đúng. Thật vậy nếu tồn tại nghiệm tự nhiên x,y mà $x=u^2$ thì u phải là số lẻ lớn hơn 1. Từ đó $u^2=8k+1$. Hơn nữa do $\left(u^2-1\right)\left(u^2+1\right)=u^4-1=2y^2$ suy ra $8k\left(4k+1\right)=y^2$ mà $\left(2k,4k+1\right)=1$ suy ra $2k=a^2$. Vì vậy $u^2-1=8k=\left(2a\right)^2$, vô lý vì hai số tự nhiên liên tiếp không thể đều là bình phương đúng. Suy ra phương trình $x^4-2y^4=1$ không có nghiệm tự nhiên. Dễ dàng *c*hứng minh phương trình $v^4-2u^2=-1$ không có nghiệm tự nhiên ngoại trừ $u=v=1$. Thật vậy, nếu $u>1$ và v thỏa mãn $v^4-2u^2=-1$ thì $u^4-v^4=\left(u^2-1\right)^2$ với u,v,d^2-1 là các số tự nhiên. Nhưng điều này mâu thuẫn với Hệ quả 1 Định lý 3 mục 6. Tuy nhiên có thể chứng minh các phương trình $x^4-2y^4=z^2,\ \ u^4-2v^4=-w^2$ đều có vô hạn nghiệm tự nhiên. Đặc biệt $\left(3,2,7\right)$ và $\left(113,84,7967\right)$ là các nghiệm của phương trình thứ nhất, $\left(1,13,239\right)$ và $\left(1343,1525,2165017\right)$ là các nghiệm của phương trình thứ hai. Hầu hết các phương trình Diophante bậc hai với hai biến đều có thể biến đổi về phương trình Pell (Skolem [2] trang 46).

Xét phương trình

(83) $$(x+1)^3-x^3=y^2$$

Rõ ràng phương trình này tương đương với $(2y)^2-3(2x+1)^2=1$. Do đó ta chỉ cần tìm nghiệm nguyên u,v của phương trình $u^2-3v^2=1$ mà u chẵn, v lẻ. Phương trình này có nghiệm tầm thường $u=1,v=0$. Nghiệm tự nhiên nhỏ nhất của nó là $u_0=2,v_0=1$ do đó theo Định lý 13 thì tất cả các nghiệm tự nhiên của phương trình này được xác định bởi dãy vô hạn $(u_k,v_k),k=0,1,2,\ldots$, trong đó $u_{k+1}=2u_k+3v_k$ và $v_{k+1}=u_k+2v_k$. Suy ra nếu u_k chẵn và v_k lẻ thì u_{k+1} lẻ và v_{k+1} chẵn. Ngược lại nếu u_k lẻ và v_k chẵn thì u_{k+1} chẵn và v_{k+1} lẻ. Từ đây ta suy ra tất cả các nghiệm tự nhiên của phương trình $u^2-3v^2=1$ với u chẵn v lẻ là (u_{2k},v_{2k}) trong đó $k=0,1,2,\ldots$ Tương tự tất cả các nghiệm tự nhiên của ***(83)*** được chứa trong dãy vô hạn $(x_k,y_k),k=0,1,2,\ldots$, với $x_0=0,y_0=1$ và $x_k=7x_{k-1}+4y_{k-1}+3,y_k=12x_{k-1}+7y_{k-1}+6,k=0,1,2,\ldots$. Ngoài ra nếu các số tự nhiên x,y thỏa mãn phương trình ***(83)*** thì các số y đều là tổng của hai bình phương tự nhiên liên tiếp. Đặc biệt ta có

$$8^3-7^3=(2^2+3^2)^2,105^3-104^3=(9^2+10^2)^2.$$

A.Rotkiewicz [3] đã nhận xét rằng việc giải phương trình nghiệm tự nhiên

(84) $\qquad (u-v)^5=\mathrm{u}^3-\mathrm{v}^3$

với $u>v$ có thể được quy về việc giải phương trình ***(83)*** trong tập số tự nhiên.

Thật vậy, ta chú ý rằng nếu các số tự nhiên x,y thỏa mãn ***(83)*** thì đặt $u=y(x+1),v=yx$, ta có $u-v=y$ và $u^3-v^3=y^3\left[(x+1)^3-x^3\right]=y^5=(u-v)^5$. Đây chính là công thức ***(84)***.

Đặt $y=(u,v),x=v/y,t=u/y$, ta có $(x,t)=1$ và bởi vì $u>v,t>x$ suy ra theo ***(84)*** ta có $y^5(t-x)^5=y^3(t^3-x^3)$ do đó $y^2(t-x)^4=(t^3-x^3)/(t-x)$ và từ $(t^3-x^3)/(t-x)=(t-x)^2+3tx$ suy ra $(t-x)^2|3tx$. Vì vậy từ $(t,x)=1$ ta suy ra $t-x=1$, hệ quả là $t=x+1,u=y(x+1)$ và $y^2=(x+1)^3-x^3$ suy ra ***(83)***. Do đó tất cả các nghiệm tự nhiên của ***(84)*** với $u>v$ đều thu được từ các nghiệm của ***(83)*** bằng phép đặt $u=y(x+1),v=yx$.

18. Phương trình $x^2+k=y^3$ với k nguyên

Các phương trình này được phát hiện và nghiên cứu bởi nhiều tác giả. Ta bắt đầu với định lý tổng quát sau. Định lý này có thể áp dụng cho nhiều giá trị k khác nhau (xem thêm Mordell [1]).

Định lý 16. *Nếu a lẻ và b là số chẵn không chia hết cho 3 và không có ước số chung dạng* $4t+3$ *với a và nếu* $k=b^2-a^3$ *và* k *không có dạng* $8t-1$ *thì phương trình* $x^2+k=y^3$ *vô nghiệm.*

Chứng minh. Giả sử phản chứng rằng tồn tại các số nguyên x,y mà $x^2+k=y^3$. Do b chẵn và a lẻ nên số $k=b^2-a^3$ lẻ. Vì vậy nếu y chẵn thì x lẻ và suy ra $8|x^2-1,8|y^3$ do đó từ $k+1=y^3-(x^2-1)$ ta suy ra $8|k+1$, mâu thuẫn với giả thiết k không có dạng $8t-1$. Vậy y lẻ và hệ quả là x chẵn. Do đó $x=2u$ và từ $b=2c$ ta có

$$x^2+b^2=4(u^2+c^2)=y^3+a^3=(y+a)(y^2-ay+a^2).$$

Do $y-a$ chẵn và a lẻ nên $y^2-ay+a^2=(y-a)y+a^2$ lẻ. Hệ quả là $4|y+a$ và $y+a=4v$. Vì vậy $y-a=4v-2a,y=4v-a$ và $(y-a)y=4w+2a^2$. Suy ra $y^2-ay+a^2=4w+3a^2$. Do a lẻ nên vế phải có dạng $4t+3$. Hệ quả là (Chương 5) nó có ước số nguyên tố p có cùng dạng mà lũy thừa cao

nhất s thỏa mãn p^s là ước của $4w+3a^2$ là lũy thừa bậc lẻ. Đặt $s=2\alpha-1$ thì do $p^{2\alpha-1}|y^2-ay+a^2$ và $y^2-ay+a^2|x^2+b^2$ ta có $p^{2\alpha-1}|x^2+b^2$. Đặt $d=(x,b), x=dx_1, b=db_1$ thì $(x_1,b_1)=1$ và $p^{2\alpha-1}|d^2\left(x_1^2+b_1^2\right)$. Ta đã biết (Chương 11) tổng bình phương của hai số mà ít nhất một số không chia hết cho số nguyên tố p có dạng $4t+3$ không thể chia hết cho p. Ta có $p^{2\alpha-1}|d^2$ do đó $p^{2\alpha}|d^2$ và $p^\alpha|d$. Từ đó $p^\alpha|x$ và $p^\alpha|b$ do đó $p^{2\alpha}|(y+a)\left(y^2-ay+a^2\right)$. Do s lớn nhất mà $s^s|\left(y^2-ay+a^2\right)$ là lẻ nên ta có $p|y+a$. Cũng vậy từ $p|y^2-ay+a^2=(y+a)(y-2a)+3a^2$ ta suy ra $p|3a^2$. Lại do $p|b$ và b không chia hết cho 3 suy ra $p|a$, mâu thuẫn với giả thiết của a và b. Định lý 16 được chứng minh. □

Hệ quả. *Phương trình $x^2+k=y^3$ không có nghiệm tự nhiên với $k=3,5,17,-11,-13$ (để ý rằng $3=2^2-1^3, 5=2^2-(1)^3, -11=4^2-3^3, 17=4^2-(-1)^3, -13=70^2-17^3$.*

Định lý 17. *Nếu a là số nguyên có dạng $4t+2$ và b lẻ không chia hết cho 3 và không có ước số chung dạng $4t+3$ với a thì với $k=b^2-a^3$ phương trình $x^2+k=y^3$ vô nghiệm.*

Chứng minh. Phản chứng. Giả sử tồn tại các số nguyên x, y thỏa mãn $x^2+k=y^3$. Do $k=b^2-a^3$ và từ giả thiết của a và b suy ra số k có dạng $8t+1$. Từ đó nếu y chẵn thì $x^2=y^3-k$ có dạng $8t-1$, vô lý. Vậy y lẻ và do đó x chẵn. Nếu y có dạng $4t+1$ thì $y+a$ có dạng $4t+3$ và do đó nó có ước số nguyên tố p có dạng này mà lũy thừa μ của p trong phân tích thành ước số nguyên tố của $y+a$ là số lẻ, nghĩa là $\mu=2\alpha-1$. Hơn nữa từ $x^2+b^2=y^3+a^3$ ta có $p^{2\alpha-1}|x^2+b^2$. Do đó như trong chứng minh Định lý 16 ta suy ra $p^\alpha|b$ và $p^\alpha|x$. Vậy $p|3a^2$. Nhưng $p|b$ mà b không chia hết cho 3 suy ra $p\neq 3$. Vậy ta có $p|a$, mâu thuẫn với giả thiết. Do đó ta chỉ cần xét trường hợp y có dạng $4t+3$. Khi đó $y-a$ có dạng $4t+1$ và $y(y-a)$ có dạng $4t+3$. Do y^2-ay+a^2 có dạng $4t+3$ nên tương tự chứng minh Định lý 16 thì ta chứng minh được $x^2+b^2=y^3+a^3=(y+a)\left(y^2-ay+a^2\right)$ có ước số nguyên tố p có dạng $4t+3$ với lũy thừa lẻ trong phân tích thành ước số nguyên tố. Mâu thuẫn. Định lý 17 được chứng minh. □

Hệ quả. *Phương trình $x^2+k=y^3$ không có nghiệm nguyên với $k=9$ và $k=-7$ (để ý $9=1^2-(-2)^3$ và $-7=1^2-2^3$) (V.A.Lebesgue [2] đã tìm ra một chứng minh cho trường hợp $k=-7$ vào năm 1869)*

Định lý 18. *Phương trình $x^2+12=y^3$ không có nghiệm nguyên x, y.*

Chứng minh. Giả sử phản chứng tồn tại x, y thỏa mãn $x^2+12=y^3$. Nếu x chẵn thì $x=2x_1$ và y cũng chẵn thì $y=2y_1$. Vậy $x_1^2+3=2y_1^3$ và x_1 lẻ, từ đó x_1^2 có dạng $8t+1$ suy ra $2y_1^3=x_1^2+3$ có dạng $8t+4$ nên y_1^3 có dạng $4t+2$. Vô lý vì lập phương của một số chẵn chia hết cho 4. Suy ra x và y đều lẻ. Ta có $x^2+4=y^2-8=(y-2)\left(y^2+2y+4\right)$. Do y lẻ nên suy ra số y^2+2y+4 có dạng $4t+3$. Do đó số x^2+2^2, với $(x,2)=1$, có ước số có dạng $4k+3$, vô lý. Định lý 18 được chứng minh. □

Ta lưu ý rằng Mordell đã chứng minh định lý tổng quát hơn: *nếu $k=(2a)^2-(2b)^3$ với a là số lẻ không chia hết cho 3 và b có dạng $4t+3$, hơn nữa (a,b) không có ước số có dạng $4t+3$ thì phương trình $x^2+k=y^3$ vô nghiệm. Đặc biệt vì $12=2^2-(2)^3, -20=14^2-6^3$ nên phương trình $x^2+k=y^3$ không có nghiệm nguyên với $k=12, k=-20$.*

Định lý 19. *Phương trình $x^2+16=y^3$ vô nghiệm.*

Chứng minh. Nếu x chẵn thì y cũng chẵn và do đó $x=2x_1, y=2y_1, x_1$ và y_1 là các số nguyên. Vì vậy $x_1^2+4=2y_1^3$ và hệ quả là x_1 chẵn và do đó $x_1=2x_2$ suy ra $2x_2^2+2=y_1^3$. Từ đó $y_1=2y_2$ suy ra $x_2^2+1=4y_2^3$, vô lý. Vậy x lẻ suy ra y^3 có dạng $8t+1$. Nhưng từ đây suy ra y có dạng $8t+1$. Hệ quả là $y-2$ có dạng $8t-1$. Do $y-2 \mid y^3-8=x^2+8$ nên các số x^2+8 có ước số có dạng $8t-1$. Suy ra x^2+8 có ước số nguyên tố p có dạng $8k+5$ hoặc $8k+7$. Nhưng như thế thì $p \mid x^2+8$ mà đây lại là điều là không thể xảy ra (Chương 9). Định lý 19 được chứng minh. □

Định lý 20. *Phương trình* $x^2-16=y^3$ *không có nghiệm nào ngoại trừ* $x=\pm 4, y=0$.

Chứng minh. Giả sử x, y thỏa mãn $x^2-16=y^3$. Nếu x lẻ thì ta có $(x+4, x-4)=1$ do đó từ $(x+4)(x-4)=y^3$ suy ra tồn tại các số lẻ a, b thỏa mãn $x+4=a^3$, $x-4=b^3$ do đó $a^3-b^3=8$ vô lý vì 8 không phải hiệu của hai lập phương lẻ. Suy ra x chẵn tức là $x=2x_1$. Từ đó y cũng chẵn, $y=2y_1$. Vì vậy $x_1^2-4=2y_1^3$, Suy ra x_1 chẵn, $x_1=2x_2$ và do đó y_1 cũng chẵn, nghĩa là $y_1=2y_2$. Ta có $x_2^2-1=4y_2^3$. Từ đây suy ra x_2 lẻ, nghĩa là $x_2=2x_3+1$. Vì vậy $4x_2^3+4x_3=4y_2^3$ và từ đó $x_3(x_3+1)=y_2^3$, mà $(x_3, x_3+1)=1$ suy ra tồn tại các số nguyên a và b thỏa mãn $x_3=a^3, x_3+1=b^3$ nhưng từ đây suy ra $y_2=0$ và từ đó y = 0 và $x \pm 4$. Định lý 20 được chứng minh.. □

A.Thue [2] (xem Mordell [2]) đã chứng minh rằng với mọi số nguyên $k \neq 0$ thì phương trình $x^2+k=y^3$ chỉ có hữu hạn nghiệm nguyên.

Hệ quả 2 Định lý 9 cho ta lời giải hoàn chỉnh cho phương trình $x^2-1=y^3$. Phương trình $x^2+1=y^3$ không có nghiệm nguyên và cũng không có nghiệm hữu tỷ. Phương trình $x^2+2=y^3$ có nghiệm tự nhiên duy nhất $x=5, y=3$. Kết quả này mặc dù được biết tới từ thời Fermat nhưng lời giải của nó vẫn là rất khó (Fermat [1] trang 345 và 434; chứng minh đầy đủ đầu tiên được cho bởi T.Pepin [1] và sau đó bởi Euler). Lời giải này có thể tìm thấy trong Uspensky và Heaslet [1]. Chứng minh được trình bày ở đây không sử dụng tới trường $Q(\sqrt{-2})$.

Chứng minh phương trình $x^2-2=y^3$ chỉ có nghiệm $x=1, y=-1$ cũng là rất khó. Lời giải đầu tiên được trình bày bởi A.Brauer [1] năm 1926 dựa trên lý thuyết về các idean, lời giải trong Uspensky và Heaslet [1] đã tránh sử dụng lý thuyết đó.

Số nghiệm của phương trình $x^2+k=y^3$ có thể lớn tùy ý.

T.Nagell [3] vào năm 1930 đã chứng minh rằng với $k=-17$ thì phương trình có đúng 16 nghiệm là $(x, y)=(\pm 3, -2), (\pm 4, -1), (\pm 5, 2), (\pm 9, 4), (\pm 23, 8), (\pm 282, 3), (\pm 375, 52), (\pm 378661, 5234)$.

Cũng về các phương trình này, O.Hemer đã bảo vệ luận án của mình (Hemer [1]). Các chỉnh sửa và thông tin bổ sung được tìm thấy trong bản ghi chú sau đó (Hemer [2]) và cuốn sách của London và Finkelstein [1]. Hermer đã tìm tất cả các nghiệm của phương trình $x^2+k=y^3$ với mọi k mà $-100 \leq k < 0$. Với số dương $k \leq 100$ công việc tương tự được hoàn thành bởi F.B.Conghlan và N.M.Stephens [1].

Về mặt lý thuyết bài toán cũng được giải bởi A.Baker [1]: $\left|x^3-y^2\right| > 10^{-10}(\log|x|)^{10^{-4}}$ nếu $x^3 \neq y^2$ với mọi số nguyên x, y (Stark [2]). M.Hall, Jr [3] đã đặt ra giả thuyết rằng với số $c>0$ nào đó thì bất đẳng thức $0<\left|x^3-y^2\right|<c\sqrt{|x|}$ không có nghiệm nguyên. Gần đây Danilov [1] đã chứng minh rằng với vô hạn các số nguyên x, y thì $0<\left|x^3-y^2\right|<0.97\sqrt{|x|}$. Ý tưởng của Danilov dẫn tới định lý mạnh hơn sau đây

Định lý 21. *Với vô hạn số tự nhiên* x, y *ta có bất đẳng thức* $0 < x^3 - y^2 < \frac{54}{25}\sqrt{\frac{x}{5}}$

Chứng minh. Ta có $(t^2+6t-11)^3 - (t^2-5)^2[(t+9)^2+4] = 1728t - 3456$. Theo Định lý 14 với $\xi_0 = 930249, \eta_0 = 83204$, n lẻ thì phương trình $\xi^2 - 125\eta^2 = 1$ có vô hạn nghiệm tự nhiên ξ, η mà $125 \mid \xi + 1$.

Đặt $t = 1364\xi + 1525\eta - 9, \quad u = 61\xi + 682\eta$,

khi đó ta thấy t lẻ, $125 \mid t-2$, $(t+9)^2 + 4 = 500u^2$, $\left(\frac{t^2+6t-11}{20}\right)^3 - \left(\frac{(t^2-5)}{4} - 4\right)^2 = \frac{27}{125}(t-2)$.

Đặt $x = \frac{t^2+6t-11}{20}, \quad y = \frac{(t^2-5)}{4}u$.

Ta có $t = \sqrt{20x+20} - 3 < \sqrt{20x}$, $0 < t - 2 < \sqrt{20x}$ và từ đó suy ra điều phải chứng minh.

Phương trình $x^2 + k = y^3$ với $2 < |k| \le 20$ có nghiệm $x, y \ne 0$ với k = 4,7,11,13,15,18,19,20, -3, -5, -8, -9, -10, -12, -15, -17, -18, -19 do $2^2 + 4 = 2^3$, $1^2 + 7 = 2^3$, $4^2 + 11 = 3^3$ (cũng vậy $58^2 + 11 = 15^3$), $70^2 + 13 = 17^3$, $7^2 + 15 = 4^3$, $3^2 + 18 = 3^3$, $18^2 + 19 = 7^3$, $14^2 + 20 = 6^3$, $2^2 - 3 = 1^3$, $2^2 - 5 = (-1)^3$, $4^2 - 8 = 2^3$, $1^2 - 9 = (-2)^3$, $3^2 - 10 = (-1)^3$, $2^2 - 12 = (-2)^3$, $4^2 - 15 = 1^3$ (cũng vậy $1138^2 - 15 = 109^3$), $4^2 - 17 = (-1)^3$ (cũng vậy $3^2 - 17 = (-2)^3$), $19^2 - 18 = 7^3$, $12^2 - 19 = 5^3$, với tất cả các giá trị khác của k mà $2 < |k| \le 20$ thì phương trình không có nghiệm hữu tỷ $x, y \ne 0$ ngoại trừ với $k = -11$ thì không có nghiệm nguyên nhưng có nghiệm hữu tỷ, cụ thể $\left(\frac{19}{8}\right)^2 - 11 = \left(\frac{7}{4}\right)^3$. Từ đẳng thức

$$\left(\frac{27y^6 - 36x^2y^3 + 8x^4}{8x^3}\right)^2 + y^3 - x^2 = \left(\frac{9y^4 - 8x^2y}{4x^2}\right)^3$$

suy ra mọi nghiệm hữu tỷ của phương trình $x^2 + k = y^3$ mà $x, y \ne 0$ đều cho thêm một nghiệm khác.

Theo R.Fueter [1] thì nếu tồn tại một nghiệm như vậy thì với $k \ne -1, 432$ ta sẽ có vô hạn nghiệm.

Hiển nhiên các nghiệm hữu tỷ của phương trình $x^2 + k = y^3$ thu được từ các nghiệm nguyên của phương trình $u^2 + kw^6 = v^3$ với $w \ne 0$ bằng cách đặt $x = u/w^3, y = v/w^2$.

Thật vậy, dễ dàng kiểm tra được $x^2 + k = y^3$. Đặt $x = m/n, y = r/s$ với m, r là các số nguyên và n, s là các số tự nhiên. Khi đó đặt $u = mn^2s^3, v = rn^2s, w = ns$, ta thấy các số u, v, w nguyên, $w \ne 0$ và thỏa mãn $u^2 + kw^6 = v^3$ với $u/w^3 = m/n, v/w^2 = r/s$.

Các nghiệm hữu tỷ của phương trình $x^2 + k = y^3$ được tìm ra bởi J.W.Cassels [1], [2] và E.S.Selmer [3]. J.W.Cassels [1] đã chỉ ra các nghiệm cơ bản của phương trình $u^2 + kw^6 = v^3$ với các giá trị k có giá trị tuyệt đối ≤ 50 mà tồn tại nghiệm không tầm thường (trang 268). Selmer đã tiếp tục phát triển bảng của Cassels tới 100.

Ta chú ý rằng việc phương trình $u^3 + v^3 = w^3$ không có nghiệm nguyên với $uvw \ne 0$ là tương đương với việc phương trình $x^2 + 432 = y^3$ không có nghiệm hữu tỷ nào ngoại trừ $x = \pm 36, y = 12$.

Thật vậy, giả sử các số hữu tỷ x, y thỏa mãn $x^2 + 432 = y^3, x \ne \pm 36$. Hiển nhiên $y > 0$. Các số x/36 và y/12 là hữu tỷ, 7/12 > 0. Giản ước ta có $x/36 = k/n$, $y/12 = m/n$ với k là số nguyên và m, n là các số tự nhiên. Không giảm tổng quát giả sử k và n chia hết cho 2 do ta có thể thay n, k, m bởi $2n, 2k, 2m$ lần lượt nếu cần. Đặt $u = \frac{n+k}{2}, v = \frac{n-k}{2}, w = m$. Rõ ràng u, v, m nguyên và hơn nữa

$w>0$. Ta có $u^3+v^3-w^3=\left(\frac{n+k}{2}\right)^3+\left(\frac{n-k}{2}\right)^3-m^3=\frac{n^3}{4}+\frac{3nk^2}{4}-m^3$. Nhưng $k=\frac{nx}{46}, m=\frac{ny}{12}$ vì vậy $u^3+v^3-w^3=\frac{n^3}{4}+\frac{3n^3x^2}{4.36^2}-\frac{n^3y^3}{12^3}=\frac{n^3}{1728}\left(432-x^2+y^3\right)=0$. Suy ra nếu phương trình $x^2+432=y^3$ có nghiệm hữu tỷ x,y và $x\neq\pm 36$ thì phương trình $u^3+v^3=w^3$ có nghiệm nguyên u,v,w với $uvw\neq 0$. Mặt khác giả sử các số nguyên u,v,w với $uvw\neq 0$ thỏa mãn $u^3+v^3=w^3$. Ta có $u^3+v^3=(u+v)\left(u^2-uv+v^2\right)$ và $w\neq 0$ suy ra $u+v\neq 0$. Vì vậy đặt $x=36(u-v)/(u+v)$, $y=12\mathrm{w}/(u+v)$ ta có các số hữu tỷ u,v thỏa mãn

$$y^3-x^2=\frac{12^3\left(u^3+v^3\right)}{(u+v)^3}-\frac{36^2(u-v)^2}{(u+v)^2}$$
$$=\frac{12^3\left(u^2-uv+v^2\right)-36^2\left(u^2-2uv+v^2\right)}{(u+v)^2}=432$$

và suy ra $x^2+432=y^3$.

Tương tự chứng minh này ta có nhận xét rằng phương trình $u^3+v^3=A\mathrm{w}^3$ với A là số tự nhiên là có nghiệm nguyên với $uv\mathrm{w}\neq 0$ khi và chỉ khi phương trình $x^2+432A^2=y^3$ có nghiệm hữu tỷ. Từ đây suy ra để chứng minh phương trình $x^3+y^3=z^3$ không có nghiệm nguyên $\neq 0$ ta chỉ cần chứng minh phương trình $x^3-16=y^3$ không có nghiệm hữu tỷ x,y khác 0. Để ý rằng nếu u,v,w khác 0 và thỏa mãn $u^3+v^3=w^3$ thì các số hữu tỷ $x=\left(v^3+w^3\right)/v^3$ và $y=4vw/2$ đều khác 0 và thỏa mãn $x^2-16=y^3$.

T.R.Bendz [1] đã chỉ ra định lý Fermat lớn nói rằng phương trình $x^n+y^n=z^n$ không có nghiệm tự nhiên với $n>2$ tương đương với việc phương trình $x^4-4^{n-1}=y^n$ không có nghiệm hữu tỷ khác 0.

Để kết thúc mục này ta lưu ý định lý nói rằng các phương trình $x^2+k=y^n$ với $0<k\leq 10, k\neq 7$ đều vô nghiệm với $n>3$ đã được chứng minh bởi O.Korhonen [1], V.A.Lebesgue [1], W.Ljunggren [2],[3] và T.Nagell [2],[8],[9],[10].

Bài tập. ***1.*** Chứng minh định lý V.Bouniakowsky [1] (năm 1848) nói rằng phương trình

(i) $$x^mt^n+y^mu^n=z^mu^n$$

với các số m, n nguyên tố cùng nhau sẽ có vô hạn nghiệm tự nhiên x,y,z,t,u,v.

Chứng minh. Theo Định lý 16 Chương 1 tồn tại các số tự nhiên r,s mà $mr-ns=1$. Chọn a,b là các số tự nhiên tùy ý. Đặt $c=a+b$. Dễ thấy $x=a^r$, $y=b^r$, $z=c^r$, $t=b^sc^s$, $u=a^sc^s$, $v=a^sb^s$ thỏa mãn ***(i)***.

2. Chứng minh rằng phương trình $x^2=y^3+z^5$ có vô hạn nghiệm tự nhiên.

Chứng minh. Các số $x=n^{10}(n+1)^8, y=n^7(n+1)^5, z=n^4(n+1)^3$, $n=1,2,\ldots$, thỏa mãn phương trình.

3. Chứng minh rằng với $n>1$ phương trình $x^n+y^n=z^{n-1}$ có vô hạn nghiệm tự nhiên.

Chứng minh. Ta có $\left(\left(1+k^n\right)^{n-2}\right)^n+\left(k\left(1+k^n\right)n-2\right)^n=\left(\left(1+k^n\right)^{n-1}\right)^{n-1}$ với $n\geq 2$.

4. Chứng minh rằng phương trình $x^n+y^n=z^{n+1}$ có vô hạn nghiệm.

Chứng minh. Ta có $\left(1+k^n\right)^n+[k\left(1+k^n\right)^n]^n=\left(1+k^n\right)^{n+1}$.

Ghi chú. Phương trình $Ax^m+By^n=z^p$ và tổng quát hơn là $\sum_{t=1}^{n} Aix_t^9 i=0$ được đề cập tới bởi một số tác giả (Tchacaloff et Karanicoloff [1], Vijayaraghavan [1], Georgiev [1], Schinzel [12]).

5. Chứng minh mệnh đề dạng Fermat lớn sau đây: *nếu n là số tự nhiên lớn hơn 2 thì phương trình $x^n+\left(x+1\right)^n=\left(x+2\right)^n$ không có nghiệm tự nhiên.*

Chứng minh. Giả sử n là số lẻ >2; nếu với x tự nhiên nào đó ta có $x^n+\left(x+1\right)^n=\left(x+2\right)^n$ thì với $y=x+1$ ta có $y^n=\left(y+1\right)^n-\left(y-1\right)^n$, do đó $y^n-2\binom{n}{1}y^{n-1}-2\binom{n}{3}y^{n-3}-\ldots-2\binom{n}{n-2}y^2=2$. Suy ra y^2 là ước số của 2 mà $y=x+1>1$ suy ra vô lý. Nếu n chẵn và > 2 thì đặt $y=x+1$ suy ra $y^n-2\binom{n}{1}y^{n-1}-2\binom{n}{n-1}y=0$. Do đó $y^{n-1}-2\binom{n}{1}y^{n-2}-2\binom{n}{3}y^{n-4}-\ldots-2n=0$. Đẳng thức thứ nhất suy ra $y^n>2ny^{n-1}$ do đó $y>2n$; đẳng thức thứ hai suy ra y là ước của $2n$; mâu thuẫn.

Ghi chú. B.Leszczynski [1] đã chứng minh bộ số nguyên dương duy nhất n,x,y,z với $y>1$ mà $n^x+\left(n+1\right)=\left(n+2\right)^y$ là $n=1$, x tùy ý, $y=3,z=2$ và $n=3,x=x=z=2$. Trường hợp $y=1$ được đặt ra bởi Demyanenko [4] và theo cách đơn giản hơn bởi Chain [1].

19. Một số phương trình mũ

1. **Phương trình $x^y=y^x$.** Ta tìm tất cả các nghiệm hữu tỷ dương của phương trình này mà $y>x$. Ta có $r=x/\left(y-x\right)$ là số hữu tỷ dương và $y=\left(1+1/r\right)x$. Do đó $x^y=x^{(1+1/r)x}$ và từ $x^y=y^x$ suy ra $x^{(1+1/r)x}=y^x$, từ đó $x^{1+1/r}=y=\left(1+1/r\right)x$. Vì vậy $x^{1/r}=1=1/r$ và hệ quả là $x=\left(1+\frac{1}{r}\right)^r$, $y=\left(1+\frac{1}{r}\right)^{r+1}$. Đặt $r=n/m,$ ta có $\left(\frac{m+n}{n}\right)^{n/m}=\frac{t}{s}$, do đó $\frac{\left(m+n\right)^n}{n^n}=\frac{t^m}{s^m}$. Cả hai vế đều là phân số tối giản vì $\left(m,n\right)=1,$ ta có $\left(m+n,n\right)=1,$ do đó $\left((m+n)^n,n^n\right)=1,$ và vì $\left(t,s\right)=1,$ ta có $\left(t^m,s^m\right)=1.$ Vậy $\left(m+n\right)^n=t^m$ và $n^n=s^m$. Từ đây theo Hệ quả 1 Định lý 16 Chương 1, do $\left(m,n\right)=1$ suy ra tồn tại các số tự nhiên k và l thỏa mãn $m+n=k^m,t=k^n$ và $n=l^m,s=l^n$. Do đó $m+l^m=k^m$. Từ đây suy ra $k\geq l+1$. Nếu $m>1$ thì ta sẽ có $k^m\geq\left(l+1\right)^m\geq l^m+ml^{m-1}+1>l^m+m=k^m$, vô lý. Hệ quả là $m=1$ do đó $r=n/m=n$. Suy ra

(85) $$x=\left(1+\frac{1}{n}\right)^n,\ y=\left(1+\frac{1}{n}\right)^{n+1},$$

trong đó n là số tự nhiên. Ngược lại, dễ thấy các x,y được định nghĩa bởi ***(85)*** thỏa mãn phương trình ban đầu. Vì vậy tất cả các nghiệm hữu tỷ của phương trình $x^y=y^x$ với $y>x>0$ đều được cho bởi ***(85)*** với n là số tự nhiên. Từ đây suy ra $n=1$ là trường hợp duy nhất mà phương trình có nghiệm tự nhiên. Trong trường hợp này nghiệm sẽ là $x=2,y=4$. Vì vậy ta kết luận rằng phương trình $x^y=y^x$ có duy nhất một nghiệm tự nhiên x,y với $y>x$. Tính chất này cũng được suy ra từ $\sqrt[3]{3}>\sqrt[2]{2}=\sqrt[4]{4}>\sqrt[5]{5}>\sqrt[6]{6}>\ldots>\sqrt[1]{1}$. Phương trình $x^y=y^x$ lại có vô hạn nghiệm hữu tỷ x,y với $y>x$. Khi $n=2$ ta có $\left(\frac{9}{4}\right)^{\frac{27}{8}}=\left(\frac{27}{8}\right)^{\frac{9}{4}}$.

2. **Phương trình $x^y-y^x=1$.** Theo định lý Moret Blanc [1] thì phương trình

(86) $x^y - y^x = 1$

có đúng hai nghiệm tự nhiên là $x = 2, y = 1$ và $x = 3, y = 2$.

Ta sẽ chứng minh định lý này. Giả sử các số tự nhiên x, y thỏa mãn ***(86)***. Khi đó $x^y > 1$ và do đó $x > 1$. Nếu $x = 2$ thì theo ***(86)*** ta có $2^y = y^2 + 1$ suy ra y lẻ và hệ quả là $4 \mid y^2 - 1$. Từ đây suy ra $4 \mid 2^y - 2$ và $2 \mid 2^{y-1} - 1$. Vậy $y = 1$. Ta có

(87) $\sqrt[3]{3} > \sqrt[2]{2} = \sqrt[4]{4} > \sqrt[5]{5} > \sqrt[6]{6} > ... > \sqrt[1]{1}.$

Và theo ***(86)*** thì $x^y > y^x, x^{1/x} > y^{1/y}$. Các số $x = 3, y = 1$ không thỏa mãn ***(86)*** nhưng $x = 3, y = 2$ thỏa mãn. Vì vậy nếu x, y là nghiệm của ***(86)*** khác với $(2,1)$ và $(3,2)$ thì $x = 3, y \geq 4$ hoặc, vì $x^{1/x} > y^{1/y}$ và ***(87)***, $x \geq 4, y \geq x + 1$. Vậy trong cả hai trường hợp ta đều có $y \geq x + 1$. Đặt $y - x = a$. Hiển nhiên a là số tự nhiên và các đẳng thức sau là đúng

(88) $$\frac{x^y}{y^x} = \frac{x^{x+a}}{(x+a)^x} = \frac{x^a}{\left(1 + \frac{a}{x}\right)^x}$$

Mà $e^t > 1 + t$ với $t > 0$ suy ra với $t = a / x$ ta có $(1 + a/x)^x < e^a$. Vậy theo ***(88)*** và $x \geq 3 > e$ suy ra

$$\frac{x^y}{y^x} > \frac{x^a}{e^a} = \left(\frac{x}{e}\right)^a \geq \frac{x}{e} \geq \frac{3}{e} > 1.1.$$

Do đó $x^y - y^x > \frac{y^x}{10} \geq \frac{4^3}{10} > 1$, mâu thuẫn với giả thiết về bộ (x, y) là nghiệm của ***(86)***. Suy ra phương trình ***(86)*** không có nghiệm nào ngoại trừ $x = 2, y = 1$ và $x = 3, y = 2$.

3. **Phương trình** $x^x y^y = z^z$. Phương trình này có vô hạn nghiệm tự nhiên khác 1. Như đã chỉ ra bởi Chao Ko [2] thì với số tự nhiên n ta có các số

$$x = 2^{n+1(2^n - n - 1) + 2n} (2^n - 1)^{2(2^{n-1})},\ y = 2^{2n+1(2^n - n - 1)} (2^n - 1)^{2(2^{n-1})+2},\ z = 2^{2n+1(2^n - n - 1)+n+1} (2^n - 1)^{2(2^n - 1)+1}.$$

thỏa mãn phương trình $x^x y^y = z^z$. Với $n = 2$ ta có $x = 2^{12} \cdot 3^6 = 2985984$, $y = 2^8 \cdot 3^8 = 1679616$, $z = 2^{11} \cdot 3^7 = 4478976$. Chao Ko cũng chứng minh rằng phương trình $x^x y^y = z^z$ không có nghiệm tự nhiên x, y, z mà mỗi số đều lớn hơn 1 và $(x, y) = 1$.

V.A.Demyanenko [3] đã chứng minh rằng nếu x, y, z là các số tự nhiên lớn hơn 1 thỏa mãn phương trình $x^x y^y = z^z$ thì x, y phải có cùng các ước số nguyên tố (Chương 3 mục 1).

Ta chưa biết phương trình $x^x y^y = z^z$ có nghiệm lẻ lớn hơn 1 hay không.

4. **Phương trình** $x! y! = z!$. Không khó để chứng minh rằng phương trình này có vô hạn nghiệm tự nhiên x, y, z mà mỗi số đều lớn hơn 1. Thật vậy với mọi số tự nhiên n lớn hơn 2 thì các số $x = n! - 1, y = n, z = n!$ thỏa mãn phương trình. Khi $n = 3$ ta có $5!3! = 6!$. Phương trình này còn có các nghiệm khác không có dạng này chẳng hạn $6!7! = 10!$. Ta chưa biết có tồn tại các nghiệm khác nữa hay không (Guy [1] trang 44). Mặt khác, rất dễ để tìm tất cả các nghiệm tự nhiên của phương trình $x! + y! = z!$. Thật vậy nếu x, y, z là nghiệm thì ta có thể giả sử $x \leq y$ và do đó $z > y$, nghĩa là $z \geq y + 1$, suy ra $z! \geq (y+1)!$. Nhưng $z! = x! + y! \leq y!2$, do đó $y!2 \geq (y+1)! = y!(y+1)$

và hệ quả là $y+i\le 2$, nghĩa là $y=1$, suy ra $x=1$ và $z=2$. Phương trình $x!+y!=z!$ chỉ có đúng một nghiệm tự nhiên là $x=1, y=1, z=2$. Các phương trình dạng giai thừa được nghiên cứu bởi P.Erdos, R.Oblath [1] và R.M.Pollack và H.N.Shapiro [1].

CHƯƠNG 3

SỐ NGUYÊN TỐ

1. Số nguyên tố và phân tích số tự nhiên thành tích các số nguyên tố

Các số tự nhiên lớn hơn 1 không có ước số nào ngoài 1 và chính nó được gọi là số nguyên tố hoặc gọn hơn là nguyên tố. Điều kiện cần và đủ để một số tự nhiên $m>1$ là nguyên tố là m không thể phân tích thành tích của hai số tự nhiên nhỏ hơn m. Thật vậy nếu m là số nguyên tố thì m không thể biểu diễn thành tích $a\cdot b$ của hai số tự nhiên nhỏ hơn m vì nếu ngược lại thì các số a và b là các ước số tự nhiên lớn hơn 1 và nhỏ hơn m của m. Điều kiện cần được chứng minh. Mặt khác nếu m không phải số nguyên tố thì nó có ước số a với $1<a<m$ và do đó $m=a.b$ với b là số tự nhiên nhỏ hơn m vì $a>1$. Điều kiện đủ được chứng minh.

Từ định nghĩa của các số nguyên tố ta có ngay một phương pháp để quyết định một số tự nhiên cho trước $n>1$ là nguyên tố hay không. Theo đó ta chỉ cần lần lượt chia n cho các số $2,3,\ldots,n-1$ và nếu có một phép chia hết thì n không phải số nguyên tố, ngược lại thì n là số nguyên tố.

Một số tự nhiên không bằng 1 và cũng không nguyên tố được gọi là hợp số. Đó là các số có thể biểu diễn như là tích của hai số nguyên dương lớn hơn 1.

Xét hợp số $n=a.b$ ta có thể giả sử $a\le b$ khi đó $a^2\le ab=n,$ suy ra $a\le\sqrt{n}.$ Vì vậy ta có định lý

Định lý 1. *Nếu số tự nhiên n là hợp số thì nó có ước số a thỏa mãn $1<a\le\sqrt{n}$.*

Do đó để xét xem một số tự nhiên $n>1$ có là số nguyên tố hay không ta chỉ cần đem số đó chia cho các số lớn hơn 1 và không vượt quá $\sqrt{n}$. Bây giờ ta chứng minh định lý

Định lý 2. *Mọi số tự nhiên >1 có ít nhất một ước số nguyên tố.*

Chứng minh. Xét số tự nhiên $n>1$. Hiển nhiên n có các ước số lớn hơn 1. Ký hiệu p là ước số nhỏ nhất lớn hơn 1 của n. Nếu p không phải số nguyên tố thì ta có $p=a.b$ với các số tự nhiên $1<a,b<p$ vì vậy a là ước số lớn hơn 1 của n và nhỏ hơn p. Mâu thuẫn suy ra p là ước số nguyên tố của n. Định lý được chứng minh. □

Từ hai định lý cơ bản này ta có

Hệ quả 1. *Mọi hợp số n có ít nhất một ước số nguyên tố $\le\sqrt{n}$.*

Hệ quả 2. *Mọi số tự nhiên >1 đều là tích của hữu hạn số nguyên tố.*

Chứng minh. Phản chứng. Giả sử $n>1$ là số tự nhiên nhỏ nhất mà không là tích của các số nguyên tố. Từ Định lý 2 suy ra n có ước số nguyên tố p tức là $n=p.n_1$ với n_1 là số tự nhiên. Ta không thể có $n_1=1$ vì như thế $n=p$ mâu thuẫn với giả thiết. Vì vậy $n_1>1$ và $n>n_1$ và từ giả thiết về tính nhỏ nhất của n suy ra n_1 là tích của hữu hạn các số nguyên tố. Khi đó $n=p.n_1$ lại là tích của hữu hạn các số nguyên tố. Vậy Hệ quả 2 được chứng minh. □

Một vấn đề được đặt ra là làm sao tìm được cách biểu diễn một số tự nhiên cho trước thành tích của các số nguyên tố. Ta sẽ chỉ ra một phương pháp như vậy mặc dù các phép tính toán cụ thể có thể sẽ rất dài. Ta sẽ chứng minh rằng việc tìm phân tích thành thừa số nguyên tố của số tự nhiên cho trước có thể chuyển về bài toán tìm phân tích thành thừa số nguyên tố của các số tự nhiên nhỏ hơn số cho trước đó. Giả sử n là số tự nhiên >1. Chia n lần lượt cho $2,3,\ldots,n$ ta sẽ tìm được ước số nguyên tố nhỏ nhất p của nó. Ta có $n=p.n_1$ với n_1 là số tự nhiên. Nếu $n_1=1$ thì $n=p$ và ta có biểu diễn cần tìm. Nếu ngược lại ta lặp lại quá trình này với $n_1<n$. Sau hữu hạn bước ta sẽ thu được biểu diễn thành thừa số nguyên tố $n=pp'p''\ldots p^{(k-1)}$. Nếu trong tích này các thừa số lặp lại thì ta thay chúng bằng các lũy thừa thích hợp và ta nhận được

(1) $$n = q_1^{a_1} q_2^{a_2} \ldots q_s^{a_s}$$

trong đó $q_1, q_2, \ldots, q_s$ đều là các số nguyên tố phân biệt, nghĩa là $q_1 < q_2 < \ldots < q_s$ và $a_i (i = 1,2,\ldots,s)$ là các số tự nhiên. Biểu diễn dạng này được gọi là phân tích thành thừa số nguyên tố của số tự nhiên n. Rõ ràng $q_1, q_2, \ldots, q_s$ là tất cả các ước số nguyên tố của n. Thật vậy nếu n có ước số nguyên tố q không trùng với số nào trong các số $q_1, q_2, \ldots, q_s$ thì với $i = 1, 2, \ldots, s$ ta có $(q, q_i) = 1$ và do số nguyên tố q chỉ có hai ước số là q và 1 với $q \neq q_i$ nên chúng là các số nguyên tố khác nhau nguyên tố cùng nhau. Ta cũng có $\left(q, q_i^{a_i}\right) = 1$ với $i = 1, 2, \ldots, s$ vì vậy từ ***(1)*** và Định lý 6^a Chương 1 ta có $(q, n) = 1$ mâu thuẫn với giả thiết. Ta cũng có các số $q_i (i = 1,2,\ldots,s)$ được xác định duy nhất theo n (như là các ước số nguyên tố của n). Hơn nữa các lũy thừa $a_1, a_2, \ldots, a_s$ cũng xác định duy nhất theo n. Đặc biệt số a_1 có thể định nghĩa như là lũy thừa lớn nhất mà $q_1^{a_1} \mid n$ vì nếu $q_1^{a_1+1} \mid n$ ta có $q_1 \left| q_2^{a_2} \ldots q_s^{a_s} \right. \mid n$ là điều vô lý. Vì ta đã giả sử $q_1, q_2, \ldots, q_s$ là dãy tăng nên phân tích ***(1)*** là duy nhất.

Ta có định lý sau đây

Định lý 3. *Mọi số tự nhiên có thể biểu diễn duy nhất thành tích của các số nguyên tố nếu không tính tới thứ tự của các thừa số nguyên tố trong phân tích.*

Mặc dù ta có thể xác định phân tích thành thừa số nguyên tố của mọi số tự nhiên nhưng các phép tính toán cụ thể có thể sẽ rất dài. Đặc biệt trong trường hợp của số $2^{293} - 1$. Ta đã biết số này có 89 chữ số và là hợp số và ước số nhỏ nhất của nó có 11 chữ số. Tuy nhiên ta vẫn chưa biết tất cả các ước số của số đó. Ta cũng chưa biết $F_{20} = 2^{2^{20}} + 1$ có những ước số nguyên tố nào, hơn nữa ta cũng chưa biết nó có phải số nguyên tố hay không. Ta đã biết một ước số của F_{9448} là $19 \cdot 2^{9450} + 1$ nhưng ta chưa xác định được tất cả các ước số nguyên tố của nó. Một hợp số khác chưa xác định được các ước số nguyên tố là F_{20}^2.

Định lý 4. *Nếu số tự nhiên $n > 2$ thì giữa n và $n!$ có ít nhất một số nguyên tố.*

Chứng minh. Vì $n > 2$ nên số $N = n! - 1$ lớn hơn 1 vì vậy theo Định lý 2 thì nó có ước số nguyên tố p. Ước số này không thể nhỏ hơn hoặc bằng n vì nếu ngược lại nó chia hết 1, vô lý. Do đó $p > n$. Mặc khác ta lại có $p \leq N$ vì p là ước số của N suy ra $n < p \leq n! - 1 < n!$. □

Từ đây suy ra với mọi số tự nhiên đều có số nguyên tố lớn hơn nó. Vậy có vô hạn số nguyên tố. Đặc biệt ta biết tồn tại các số nguyên tố có hàng trăm nghìn chữ số, nhưng ta chưa biết một số nào như vậy. Số nguyên tố lớn nhất tìm được là $2^{216091} - 1$ có 65050 chữ số. Số này được tìm ra năm 1985

Bài tập. *1.* Chứng minh rằng số chữ số của một số nguyên tố mà biểu diễn thập phân của nó gồm toàn chữ số 1 phải là số nguyên tố (lưu ý rằng điều ngược lại không đúng).

Chứng minh. Giả sử n là số nguyên tố như vậy có s chữ số 1 trong biểu diễn thập phân. Giả sử s là hợp số, nghĩa là $s = ab$ với a, b là các số tự nhiên lớn hơn 1. Khi đó ta có $n = \frac{10^s - 1}{9} = \frac{10^{ab} - 1}{9}$.

Nhưng $10^a - 1 \mid 10^{ab} - 1$ vì vậy $\frac{10^a - 1}{9} \Big| n$. $\frac{10^a - 1}{9}$ là số tự nhiên >1 vì $a > 1$. Vì $b > 1$ ta có $\frac{10^a - 1}{9} < \frac{10^{ab} - 1}{9} = n$. Từ đây suy ra n có ước số $\frac{10^a - 1}{9}$ nhỏ hơn n và lớn hơn 1. Mâu thuẫn. □

Chiều ngược lại không đúng chẳng hạn $111 = 3 \cdot 37$ và $11111 = 41 \cdot 271$. Ta chưa biết dãy số $11, 111, 1111, \ldots$ có chứa vô hạn số nguyên tố hay không. M.Kraitchik [2] (Chương 3) đã chứng

minh số $\left(10^{23}-1\right)/9$ là nguyên tố. Williams và Dubner [1] đã chứng minh với $p<10000$ thì $\left(10^{p}-1\right)/9$ nguyên tố chỉ trong các trường hợp p bằng $2, 19, 23, 317$ hoặc 1031.

2. Chứng minh rằng tồn tại vô hạn các số tự nhiên không có dạng a^2+p với a là số nguyên và p nguyên tố.

Chứng minh. Các số $(3n+2)^2$ với $n=1,2,\ldots$ không có dạng đó. Phản chứng. Giả sử với số tự nhiên n nào đó ta có $(3n+2)^2=a^2+p$ với a là số nguyên dương, p nguyên tố. Khi đó $3n+2>a,$ suy ra $3n+2-a>0$. Nhưng $p=(3n+2-a)(3n-2+a)$ suy ra $3n+2-a=1$ và $3n+2+a=p$, suy ra $p=6n+3=3(2n+1)$. Điều này là không thể. □

Ghi chú. Có thể chứng minh rằng với mọi số tự nhiên k tồn tại vô hạn các lũy thừa bậc k các số tự nhiên không có dạng a^k+p với a nguyên và p nguyên tố (Clement [2]). Euler đã chứng minh rằng mỗi số tự nhiên lẻ n với $1<n<2500$ đều không có dạng $n=2a^2+p$ với n nguyên và p nguyên tố. Điều này không đúng với 5777 và 5993 (Dickson [7] tập 1 trang 424). Ta chưa biết có tồn tại vô hạn các số tự nhiên lẻ không có dạng $2a^2+p$ với a nguyên, p nguyên tố hay không.

3. Chứng minh rằng tất cả các số có dạng 8^n+1 đều là hợp số.

Chứng minh. Ta có $2^n+1 \mid 2^{3n}+1=8^n+1$ và rõ ràng $1<2^n+1<8^n+1$. Suy ra 8^n+1 là hợp số.

Ghi chú. Ta chưa biết có tồn tại vô hạn các số nguyên tố có dạng 10^n+1 hay không. Ta cũng chưa biết có phải mọi số có dạng 12^n+1 đều là hợp số hay không $(n>1)$.

2. Sàng Eratosthenes và bảng các số nguyên tố

Từ Hệ quả 1 trong mục 1 suy ra nếu số tự nhiên $n>1$ không chia hết cho mọi số nguyên tố $\le\sqrt{n}$ thì n là số nguyên tố. Vậy để tìm được tất cả các số nguyên tố trong dãy $2,3,4\ldots,m,$ với số tự nhiên cho trước m thì ta chỉ cần bỏ ra khỏi dãy tất cả các bội số kp của các số nguyên tố $p\le\sqrt{m}$ với $k>1$. Vì vậy trong trường hợp riêng để tìm được tất cả các số nguyên tố trong dãy $2,3\ldots,100$ ta chỉ cần bỏ ra khỏi dãy tất cả các bội số của $2,3,5$ và 7.

Một phương pháp đơn giản để tìm ra tất cả các số nguyên tố liên tiếp được đưa ra bởi nhà toán học Hy Lạp Eratosthenes. Xét dãy $2,3,4,\ldots$ thì vì 2 là số nguyên tố đầu tiên ký hiệu là p_1 ta bỏ ra khỏi dãy tất cả các số chẵn lớn hơn 2. Số đầu tiên còn lại là $3=p_2$. Ta lại bỏ đi tất cả các số lớn hơn p_2 và chia hết cho p_2. Số đầu tiên còn lại là $5=p_3$. Giả sử sau bước thứ n ta tìm được số nguyên tố thứ n là p_n thì ta loại bỏ ra khỏi dãy tất cả các số lớn hơn p_n và chia hết cho p_n. Số đầu tiên thu được trong các số còn lại p_{n+1} chính là số nguyên tố thứ $n+1$. Nếu ta chỉ xét dãy $2,3,\ldots,N,$ thì quá trình trên sẽ dừng lại ở bước thứ k với p_k là số nguyên tố lớn nhất $\le\sqrt{N}$. Ta nhận được

$p_1=2,\ p_2=3,\ p_3=5,\ p_4=7,\ p_5=11,\ p_6=13,\ p_7=17,\ p_8=19,\ p_9=23,\ p_{10}=29,\ p_{25}=97,$

$p_{100}=541,\ p_{200}=1223,\ p_{1000}=7917,\ p_{1229}=9973,\ p_{1230}=10007.$

Gần đây ta tính được $p_{6000000}=104395301$ (xem ghi chú [1]).

D.Blanusa [1] đã chỉ ra phương pháp hình học tương ứng cho sàng Eratosthenes.

Trong hệ trục tọa độ Castesian ta xét tập hợp A gồm các điểm $\left(0,\frac{1}{m}\right), m=1,2,...,$ và tập hợp B gồm các điểm $(n+1,0),\ n=1,2,...,$ mỗi điểm của tập hợp A được nối với mỗi điểm của tập hợp B bằng một đường thẳng. Khi đó tập hợp các hoành độ của các giao điểm của các đường thẳng này với đường thẳng $y=-1$ là tập hợp các hợp số. Thật vậy phương trình đường thẳng đi qua $\left(0,\frac{1}{m}\right)$ và $(n+1,0)$ là $x/(n+1)+my=1.$ Đường thẳng này cắt đường thẳng $y=-1$ tại điểm có hoành độ $x=(m+1)(n+1)$. Vì m và n là các số tự nhiên nên x là hợp số. Ngược lại, nếu x là hợp số thì $x=(m+1)(n+1)$ với m,n là các số tự nhiên và do đó nó là hoành độ giao điểm của đường thẳng nối $\left(0,\frac{1}{m}\right)$ và $(n+1,0)$ với đường thẳng $y=-1.$

Đã có một bảng đầy đủ các số nguyên tố nhỏ hơn 7 triệu (D.N.Lehmer [1]). Trong bảng này các ước số lớn hơn $2,3,5,7$ của từng số tự nhiên không lớn hơn 10170000 được trình bày đầy đủ. Trong Kulik, Poletti [1] các số nguyên tố nhỏ hơn 11 triệu được trình bày đầy đủ. Nhà toán học Ba Lan Jacob Philip Kulik sinh năm 1793 tại Lwów và mất năm 1863 tại Prague đã dành 20 năm để soạn một bản thảo có tên là ***Magus Canon Divisorum pro omnibus numbers par*** $2,3,5$ ***non divisilibus et numerorum primorum interjacentium ad Millies centum millia, accuratius ad*** 100330201 ***usque. Authore Jacobo Philippo Kulik Galiciano Leopolensis Universitate Pragensi Matheseos sublimioris Prof. publ.ac ord.*** Hiện nay bản thảo này được bảo quản bởi Viện khoa học Vienna. Bảng liệt kê các số nguyên tố nhỏ hơn 7 triệu có sử dụng bản thảo này với những chỉnh sửa một số lỗi. Bài báo nói về J.P.Kulik và công việc của ông cùng các phác thảo chân dung vừa được phát hành gần đây bởi I.Ya.Depman [1]. Về lịch sử của bảng các số nguyên tố xem tài liệu đã dẫn trang $594-601$. Vào năm 1959 C.L.Baker và F.J.Gruenberger đã xây dựng một bảng chứa tất cả các số nguyên tố nhỏ hơn 104395301 (Baker và Gruenberger [1]).

3. Hiệu của các số nguyên tố liên tiếp

Ký hiệu p_n là số nguyên tố thứ n và đặt $d_n = p_{n+1} - p_n$ với $n=1,2,...$

Các số đầu tiên của dãy vô hạn $d_1, d_2, ...$ là

1,	2,	2,	4,	2,	4,	2,	4,	6,	2
6,	4,	2,	4,	6,	6,	2,	6,	4,	2
6,	4,	6,	8,	4,	2,	4,	2,	4,	14
4,	6,	2,	10,	2,	6,	6,	4,	6,	6
2,	10,	2,	4,	2,	12,	12,	4,	2,	4
6,	2,	10,	6,	6,	6,	2,	6,	4,	2
10,	14,	4,	2,	4,	14,	6,	10,	2,	4
6,	8,	6,	6,	4,	6,	8,	4,	8,	10
2,	10,	2,	6,	4,	6,	8,	4,	2,	4
12,	8,	4,	8,	4,	6,	12,	2,	18,	6

Số 2 là số nguyên tố chẵn duy nhất. Vì vậy số p_n với $n>1$ là lẻ và do đó $d_n = p_{n+1} - p_n$ chẵn.

Quan sát bảng trên một câu hỏi đặt ra là với số tự nhiên k nào thì tồn tại n mà $d_n = 2k$? Ta chưa biết câu trả lời. Dưới dây là bảng các số tự nhiên nhỏ nhất n mà $d_n = 2k$ với $2k \le 30$ và các số nguyên tố p_n, p_{n+1} thỏa mãn $p_{n+1} - p_n = 2k$ (Lander và Parkin [3]).

$2k$	n	p_n	p_{n+1}
2	2	3	5
4	4	7	11
6	9	23	29
8	24	89	97
10	34	139	149

$2k$	n	p_n	p_{n+1}
12	46	199	211
14	30	113	127
16	282	1831	1847
18	99	523	541
20	154	887	907

$2k$	n	p_n	p_{n+1}
22	189	1129	1151
24	263	1669	1693
26	367	2477	2503
28	429	2971	2999
30	590	4297	4327

Các số nguyên tố liên tiếp nhỏ nhất có hiệu bằng 100 là 396733 và 396833. Bảng các số d_{n-1} với $n<600$ được trình bày bởi P.Erdos, A.Renyi [1] (1). Bảng d_n với $n\le 1233$ được trình bày bởi M.Colombo [1].

Bảng các số nhỏ nhất p_n mà $p_{n+1}-p_n=2k$ với $2k\le 314$ được trình bày bởi Lander và Parkin [3] và Brent [1] (xem thêm Brent [4], Weintraub [1]).

Hơn một trăm năm trước giả thuyết sau đã được đặt ra: *với mọi số chẵn* $2k$ *tồn tại vô hạn các số tự nhiên* n *thỏa mãn* $d_n=2k$ *(de Plignac [1]).*

Với $k=2$ giả thuyết này tương đương với việc tồn tại vô hạn cặp số nguyên tố sinh đôi, nghĩa là cặp các số lẻ liên tiếp mà mỗi số đều là số nguyên tố. Mười cặp số đầu tiên như vậy là (3,5), (5,7), (11,13), (17,19), (29,31), (41,43), (59,61), (71, 73), (101,103), (107,109). H.Tietze đã trình bày bảng các cặp số nguyên tố sinh đôi nhỏ hơn 300000. Có 2994 cặp như vậy (Tietze [1] và Frucht [1], xem Selmer và Nesheim [1] trong đó các số n thỏa mãn $6n+1$ và $6n-1$ đều là số nguyên tố nhỏ hơn 200000. So sánh với Sexton [1] và [2].) Brent [3] đã tìm ra có 152892 cặp các số nguyên tố sinh đôi nhỏ hơn 10^{11}. Cặp số lớn nhất được biết là $260497545\cdot 2^{6625}\pm 1$ (Atkin và Rickert, xem Yates [1]). Bài toán chứng minh tồn tại vô hạn các cặp số nguyên tố sinh đôi tương đương với việc chứng minh tồn tại vô hạn các số tự nhiên n mà n^2-1 có đúng 4 ước số tự nhiên.

Từ dãy các số tự nhiên liên tiếp $1,2,\ldots,n$ để tìm được số nguyên tố p mà $p+2$ cũng là số nguyên tố thì với mỗi hợp số k đã được bỏ ra khỏi sàng Eratosthenes ta cũng bỏ đi số $k-2$ (Golomb [1]), W.A.Golubew [2] đã đặt ra câu hỏi với số tự nhiên n nào thì tồn tại ít nhất một cặp số nguyên tố nằm giữa n^3 và $(n+1)^3$. Ta đã biết chuỗi tổng các cặp nghịch đảo của các cặp số nguyên tố sinh đôi là hội tụ (Brun [1]) (1). Chuỗi

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{17}+\frac{1}{19}\right)+\left(\frac{1}{29}+\frac{1}{31}\right)+\ldots$$

đã được tính chính xác tới 6 chữ số thập phân bởi Brent [2]. Trong mục 17 ta sẽ thấy tổng nghịch đảo của tất cả các số nguyên tố là phân kỳ.

Một câu hỏi khác chưa có câu trả lời là có tồn tại vô hạn các số nguyên tố p mà $p, p+2, p+6$ và $p+8$ đều là số nguyên tố hay không? Một bộ bốn số nguyên tố như vậy gọi là một bộ số nguyên tố sinh bốn. Sáu bộ số nguyên tố sinh bốn đầu tiên nhận được với $p=5,11,101,191,821,1481$. K.Fruchtl [1], [2], [3], [4] đã liệt kê tất cả các bộ như vậy nhỏ hơn

---

(1) Dưới đây là một số lỗi trong bảng được trích dẫn (theo J. Galgowski và L. Kacperek):

Thay vì $d_{265}=12$ ta có $d_{256}=2$, thay vì $d_{314}=6$ ta có $d_{314}=4$, thay vì $d_{344}=12$ ta có $d_{344}=22$,

Thay vì $d_{429}=18$ ta có $d_{429}=28$, thay vì $d_{465}=4$ ta có $d_{465}=6$, thay vì $d_{462}=18$ ta có $d_{462}=28$,

Ta có $d_{579}=2$.

(1) Chứng minh sơ cấp của định lý Brun có trong cuốn sách của E. Landau [2], tập 1

15000000. Có tất cả 1209 bộ số như vậy. Gần đây J.Bohuman [2] đã chỉ ra có đúng 49262 bộ bốn nhỏ hơn 2.10^9. Một bộ bốn số nguyên tố như vậy mà số nhỏ nhất lớn hơn 5 sẽ có các chữ số tận cùng lần lượt là $1, 3, 7$ và 9.

Rõ ràng mỗi bộ bốn như vậy cho ta hai cặp số nguyên tố sinh đôi. Tuy nhiên có các cặp số nguyên tố sinh đôi mà giữa chúng không có số nguyên tố nào và không tạo thành bộ bốn, Ví dụ như cặp (179,181) và (191,193). Cặp thứ hai cùng với (197,199) tạo thành một bộ bốn nguyên tố. Giữa hai cặp (419,421) và (431,433) không có số nguyên tố nào.

Các cặp $809, 811, 821, 823$ và 1019 1021; 1031, 1033 cũng như vậy. Một câu hỏi được đặt ra là có tồn tại số lượng tùy ý các cặp số nguyên tố sinh đôi liên tiếp mà giữa chúng không có số nguyên tố nào hay không. Ta đã biết có các bộ ba như vậy là

$179, 181, 191, 193, 197, 199$

$809, 811, 821, 823, 827, 829$ $3359, 3361, 3371, 3373, 3389, 3391$; $4217, 4219, 4229, 4231, 4241, 4243$;
$6761, 6763, 6779, 6781, 6791, 6793$.

Một bộ bốn như vậy là $9419, 9421, 9431, 9433, 9437, 9439, 9461, 9463$.

Có thể chứng minh rằng nếu $p \neq 5$ và các số $p, p+2, p+6$ và $p+8$ là số nguyên tố thì khi chia p cho 210 ta nhận được số dư là 11,101 hoặc 191.

Có thể chứng minh các số d_n có thể lớn tùy ý. Thật vậy ký hiệu m là số tự nhiên lớn tùy ý. Ký hiệu p_n là số nguyên tố lớn nhất $\leq m!+1$. Số $m!+k$ là hợp số với $k=2,3,...,m$ (vì $k \mid m!+k$ với $k = 2, 3, ..., m$). Vì vậy $p_{n+1} \geq m!+m+1$ và hệ quả là $d_n = p_{n+1} - p_n \geq m$.

Vậy ta có thể chứng minh $d_n \left(n = 1, 2, ...\right)$ tiến tới vô hạn.

Có các số tự nhiên n mà $d_n = d_{n+1}$. Chẳng hạn $n = 2, 15, 36, 39, 46$.

Tồn tại các số tự nhiên n mà $d_n = d_{n+1} = d_{n+2}$ chẳng hạn với $n = 54, 464, 682, 709, 821, 829$.

Tuy nhiên ta không biết với số tự nhiên k nào thì tồn tại số tự nhiên n thỏa mãn $d_n = d_{n+1} = d_{n+2} = ... = d_{n+k}$ (Lander và Parkin [4] và Bohman [2]). P.Erdos và P.Turan [2] đã chứng minh rằng tồn tại vô hạn các số tự nhiên n mà $d_n > d_{n+1}$. Với mọi số tự nhiên m và k thì tồn tại số tự nhiên n mà các số $d_n, d_{n+1}, ..., d_{n+k}$ đều lớn hơn m. Nói cách khác tồn tại vô hạn các cặp số nguyên tố sinh đôi mà hiệu của chúng lớn tùy ý (Erdos [7]).

Các hiệu của các số nguyên tố sinh đôi được nghiên cứu rất rộng bởi G.Ricci (Ricci [1],[2])

4. Giả thuyết Goldbach

Giả thuyết Goldbach nói rằng mọi số chẵn lớn hơn 2 đều là tổng của hai số nguyên tố. Giả thuyết này đã được kiểm tra với các số chẵn nhỏ hơn 10^8 (Light, Forrest, Hammond, Roe [1]). Năm 1973 Chen [2] đã chứng minh mọi số chẵn đủ lớn đều là tổng của một số nguyên tố và một số tự nhiên có nhiều nhất hai ước số nguyên tố. Kết quả đầu tiên thuộc dạng này được tìm ra bởi Brun [2] vào năm 1920.

Giả thuyết Golbach kéo theo mọi số lẻ có thể biểu diễn vô hạn cách dưới dạng $p+q-r$ với p, q, r là các số nguyên tố. Kết quả không đơn giản này được tìm ra bởi J.G.Van der Corput [2]. Ông ta cũng chứng minh rằng hầu hết các số chẵn là tổng của hai số nguyên tố lẻ. Nghĩa là với mỗi số dương ε thì với số tự nhiên đủ lớn N ta có số các số chẵn $< N$ mà không phải tổng của hai số nguyên tố sẽ nhỏ hơn εN (Van der Corput [1]).

A.Desboves [1] đã chỉ ra mọi số tự nhiên ≤ 10000 có dạng $4k+2$ đều là tổng của hai số nguyên tố, mỗi số đều có dạng $4k+1$. Điều này chỉ đúng nếu ta coi 1 cũng là số nguyên tố. Khi đó $2 = 1+1, 6 = 1+5, 14 = 1+13, 38 = 1+37, 62 = 1+61$.

Một bài toán khá gần với giả thuyết Golbach là có phải với số tự nhiên cho trước n thì số $G(n)$ tất cả các phép phân tích n thành tổng của hai số nguyên tố sẽ tiến tới vô cùng khi n tăng. N.Pipping [1], [2] đã tính hàm $G(n)$ với mọi số chẵn n nhỏ hơn 5000 và một số số khác. Các tính toán cho hàm $G(n)$ với $n \le 2000000$ được thực hiện bởi M.L.Stein và P.R.Stein (Stein và Stein [1]).

Ta có $G(4)=G(6)=1$, $G(8)=2$, $G(10)=3$, $G(12)=2$, $G(14)=3$, $G(16)=G(18)=G(20)=4$, $G(22)=5$, $G(24)=6$. Hơn nữa $G(158)=9$ và $G(2n)\ge 10$ với $2n>158$. Tương tự $G(188)=10$ và $G(2n)>10$ với $2n>188$. Số chẵn nhỏ nhất $2n$ mà $G(2n)\ge 100$ là 840. Thật ra ta có $G(840)=102$. Số $2n$ lớn nhất mà $G(2n)<100$ có thể là số $2n=4574$.

Từ giả thuyết Golbach suy ra mỗi số lẻ lớn hơn 7 đều là tổng của ba số lẻ. Thật vậy, nếu n là số lẻ >7 thì $n-3$ là số chẵn > 4 và theo giả thuyết Goldbach thì nó là tổng của hai số nguyên tố lẻ. Vì vậy mọi số lẻ lớn hơn 7 đều là tổng của ba số nguyên tố lẻ. Nhận xét này cũng chưa được chứng minh một cách chặt chẽ. Tuy nhiên các khó khăn chỉ là vấn đề kỹ thuật vì vào năm 1937 I.Vinogradov đã chứng minh các số lẻ lớn hơn một hằng số xác định được a thì đều có tính chất như vậy. Sau đó K.G. Borozdkin [1] đã chứng minh rằng $a \le \exp(\exp 16,038) < 3^{3^{15}}$. Vậy ta chỉ cần kiểm tra lại với các số $7 < n \le a$, tuy nhiên các phép tính toán lớn như vậy là chưa thực hiện được.

Tình huống lại rất khác đối với câu hỏi rằng có phải mọi số chẵn đều là hiệu của hai số nguyên tố? Hiện tại ta chưa có phương pháp nào để tiếp cận bài toán này. A.Schinzel [11] đã chứng minh rằng giả thuyết Goldbach suy ra mọi số lẻ >17 đều là tổng của ba số nguyên tố lẻ phân biệt. Từ kết quả trên của Vinogradov suy ra tính chất này là đúng với các số đủ lớn. Giả thuyết nói rằng mọi số chẵn >6 đều là tổng của hai số nguyên tố phân biệt tương đương với giả thuyết nói rằng mọi số tự nhiên >17 đều là tổng của ba số nguyên tố phân biệt (Sierpinski [23]).

Năm 1930 L.Schnireiman [1] đã đưa ra một chứng minh sơ cấp rằng tồn tại các số s mà mọi số tự nhiên >1 đều là tổng của nhiều nhất s số nguyên tố. Riesel và Vaughan [1] đã sử dụng lại phương pháp của Schnireman để chứng minh rằng mọi số chẵn >1 đều là tổng của nhiều nhất 19 số nguyên tố. Từ kết quả nêu trên của Vinogradov ta thấy mọi số tự nhiên đủ lớn đều có thể biểu diễn như là tổng của nhiều nhất 4 số nguyên tố, các trường hợp khác có thể kiểm tra bằng máy tính nhưng nó yêu cầu nhiều thời gian. Có thể dễ dàng chứng minh tồn tại vô hạn các số tự nhiên không thể biểu diễn như là tổng của ít hơn 3 số nguyên tố (so sánh với bài tập 2 ở dưới). Một giả thuyết khác được đặt ra là có phải mọi số lẻ >5 đều là tổng của một số nguyên tố và một số có dạng $2p$, với p nguyên tố (Dickson [7] trang 424)? Mayah [1] đã kiểm tra giả thuyết này với $n < 42.10^5$.

Bài tập. ***1.*** Chứng minh rằng mọi số tự nhiên >11 đều là tổng của hai hợp số.

Chứng minh. Xét số tự nhiên n>11. Nếu n chẵn tức là $n=2k$, thì $k\ge 6$ và $n-6=2(k-3)$, suy ra $n-6$ là hợp số. Nếu n lẻ nghĩa là $n=2k+1$, thì $k\ge 6$ và $n-9=2(k-4)$ là hợp số. □

2. Chứng minh rằng tồn tại vô hạn số tự nhiên lẻ không biểu diễn được thành tổng của ít hơn 3 số nguyên tố.

Chứng minh. Các số $(14k+3)^2$, với $k=1,2,\ldots$ có tính chất như vậy. Thật vậy các số này đều không nguyên tố. Hơn nữa chúng không thể biểu diễn thành tổng của hai số nguyên tố vì nếu ngược lại thì do chúng là lẻ nên một trong hai hạng tử nguyên tố phải bằng 2 và ta có $(14k+3)^2 = 2+p$, suy ra $p = 7(28k^2+12k+1)$, nhưng đây không phải số nguyên tố. Mâu thuẫn. □

Ghi chú. Có thể chứng minh một cách sơ cấp rằng tồn tại vô hạn các số lẻ là tổng của ba số nguyên tố phân biệt nhưng không là tổng của ít hơn ba số nguyên tố (Sierpinski [31]).

3. Chứng minh rằng giả thuyết Golbach tương đương với giả thuyết nói rằng mọi số chẵn >4 là tổng của ba số nguyên tố.

Chứng minh. Từ giả thuyết Goldbach suy ra với số tự nhiên $n>1$ ta có $2n=p+q,$ với p và q là các số nguyên tố. Vì vậy $2(n+1)=2+p+q,$ nghĩa là mọi số chẵn được chọn đủ lớn >4 đều được biểu diễn thành tổng của ba số nguyên tố. Mặt khác nếu mọi số chẵn >4 đều là tổng của ba số nguyên tố nghĩa là nếu với $n>2$ ta có $2n=p+q+r,$ với p,q,r là các số nguyên tố thì ít nhất một trong các số p,q,r là chẵn và do đó bằng 2. Giả sử $r=2.$ Khi đó $2(n-1)=p+q$ với $n-1>1,$ suy ra giả thuyết Goldbach. □

4. Chứng minh rằng các phương trình $x^2+y^2=z^2, x^2+y^2+z^2=t^2, x^2+y^2+z^2+t^2=u^2$ đều không có nghiệm là các số nguyên tố.

Chứng minh. Để chứng minh phương trình thứ nhất không có nghiệm nguyên tố ta nhớ lại trong chương 2 mục 3 ta đã chứng minh mọi nghiệm tự nhiên của phương trình này có ít nhất một số chia hết cho 4. Bây giờ xét phương trình thứ hai. Giả sử tồn tại các số nguyên tố x,y,z,t thỏa mãn $x^2+y^2+z^2=t^2$. Như đã chứng minh trong Chương 2 mục 10 thì ít nhất hai trong các số x,y,z là chẵn, mà vì chúng là nguyên tố nên chúng đều bằng 2. Vì vậy $t^2-z^2=8.$ Nhưng do z,t là nguyên tố và ít nhất có 1 số lẻ nên từ đẳng thức $(t-z)(t+z)=8$ suy ra $t-z\geq 2$ và hệ quả là $t+z\leq 4$, vô lý vì trong hai số t,z có một số nguyên tố lẻ. Cuối cùng xét phương trình thứ ba. Giả sử tồn tại các số nguyên tố x,y,z,t,u thỏa mãn $x^2+y^2+z^2+t^2=u^2.$ Rõ ràng u > 2 và do đó là lẻ. Vì vậy ít nhất một trong các số x,y,z,t lẻ. Nếu chỉ có đúng một số trong chúng là lẻ, giả sử là t, thì ta có $x=y=z=2,$ suy ra $12+t^2=u^2$ và từ đó $(t-u)(t+a)=12,$ suy ra $t-u\geq 2, t+u\leq 6.$ Nhưng điều này không thể xảy ra vì u,t là các số nguyên tố lẻ phân biệt. Ngược lại nếu ba trong các số nguyên tố x,y,z,t là lẻ và số còn lại chẵn thì $u^2=x^2+y^2+z^2+t^2$ đều có dạng $4k+3,$ vô lý. □

5. Tìm các nghiệm nguyên tố của phương trình $x^2+y^2+z^2+t^2=v^2$ với $x\leq y\leq z\leq t\leq u\leq v.$

Lời giải. Có duy nhất một nghiệm là $2^2+2^2+2^2+2^2+3^2=5^2,$ vì dễ dàng chứng minh chỉ có đúng một trong các số $x,y,z,t,u,$ là lẻ và do đó $4\cdot 2^2+u^2=v^2,$ suy ra $(v-u)(v+u)=16, v-u\leq 8,$ vì vậy $u=3, v=5.$ □

5. Các số nguyên tố lập thành cấp số cộng

Một cấp số cộng gồm 18 phần tử đều là số nguyên tố là $4808316343+71777060k,\ k=0,1,2,\ldots,17.$ P.A. Pritchard [1] đã tìm ra các số $4180566390k+8297644387\ (k=0,1,2,..,18)$ lập thành cấp số cộng gồm 19 số nguyên tố phân biệt. Ta chưa biết có tồn tại cấp số cộng có 100 số nguyên tố hay không. Ta sẽ chứng minh nếu cấp số cộng như thế tồn tại thì công sai của cấp số này sẽ phải là một số có nhiều hơn 30 chữ số thập phân.

Định lý 5. *Nếu n và r là các số tự nhiên, $n>1$ và nếu n phần tử của cấp số cộng $m, m+r, \ldots, m+(n-1)r$ đều là số nguyên tố lẻ thì công sai r chia hết cho mọi số nguyên tố nhỏ hơn n (Dickson [7] tập 1 trang 425).*

Chứng minh. Giả sử $m,n>1$ và r là các số tự nhiên cho trước và các số $m, m+r, \ldots, m+(n-1)r$ đều là số nguyên tố lẻ. Ta phải có $m\geq n,$ vì nếu ngược lại thì hợp số $m+mr=m(1+r)$ sẽ là phần tử của dãy số trên. Ký hiệu p là số nguyên tố nhỏ hơn n và đặt $r_0, r_1, \ldots, r_{p-1}$ là phần dư nhận được khi lần lượt chia các số $m, m+r, \ldots, m+(p-1)r$ cho p. Các số dư này là nhỏ hơn p và hơn nữa chúng đều khác 0 vì nếu ngược lại thì một trong các số nguyên tố sẽ không nhỏ hơn $m\geq n>p$ và chia hết cho $p,$ mâu thuẫn. Vì vậy các số dư trên chỉ có thể nhận các giá trị $1,2,\ldots, p-1,$ nghĩa là có $p-1$ khả năng. Từ đây suy ra tồn tại hai số nguyên k và l thỏa mãn $0\leq k<l\leq p-1$ mà $r_k=r_l.$

Hệ quả là $p|(m-lr)-(m+kr)$ và vì vậy $p|(l-k)r$. Nhưng $0<l-k\le p-1<p$, do đó $p|r$. Vì p là số nguyên tố tùy ý nhỏ hơn n, ta có điều phải chứng minh. □

Từ Định lý 5 ta có hệ quả sau đây

Hệ quả. *Nếu tồn tại cấp số cộng tăng chứa $n>2$ số nguyên tố thì công sai của dãy này sẽ chia hết cho tích P_n tất cả các số nguyên tố nhỏ hơn n, và vì vậy bản thân công sai đó $\ge P_n$.*

Đặc biệt, công sai của cấp số cộng gồm ba số nguyên tố phân biệt phải $\ge P_3=2$. Tồn tại duy nhất một cấp số cộng công sai 2 là 3,5,7. Tồn tại vô hạn cấp số cộng gồm ba số nguyên tố. Chứng minh kết quả này không đơn giản (xem Van der Corput [2] và Chowla [2]).

Bài toán chứng minh tồn tại vô hạn cấp số cộng như vậy là tương đương với câu hỏi khi nào thì phương trình $p+r=2q$ có vô hạn nghiệm nguyên tố p,q,r, với $p\ne r$. Từ giả thuyết H (mục 8) suy ra với mọi số tự nhiên n và số nguyên tố $p\ge n$ thì tồn tại vô hạn cấp số cộng tăng có n phần tử là số nguyên tố mà phần tử thứ nhất là p.

Ta liệt kê ở đây một số cấp số cộng gồm ba số nguyên tố mà số đầu tiên là 3: 3, 7, 11; 3,11,19; 3, 13, 23; 3, 31, 59; 3, 37, 71; 3, 23, 43; 3, 31, 59; 3, 37, 71; 3, 41, 79; 3, 43, 83. Công sai của cấp số cộng gồm 4 số nguyên tố phải $\ge P_4=6$. Có rất nhiều cấp số cộng 4 số nguyên tố công sai bằng 6 chẳng hạn: 5, 11, 17, 23; 11, 17, 23, 29; 41, 47, 53, 59; 61, 67, 73, 79. Từ giả thuyết H suy ra tồn tại vô hạn cấp số cộng như vậy, hơn nữa chúng còn là các số nguyên tố liên tiếp. Đặc biệt ta có dãy 251, 257, 263, 269; 1741, 1747, 1753, 1759. Công sai của cấp số cộng gồm 5 số nguyên tố phải lớn hơn hoặc bằng 6. Tồn tại duy nhất một cấp số cộng gồm 5 số nguyên tố mà công sai bằng 6 là 5, 11, 17, 23, 29. Ta lưu ý rằng trong một cấp số cộng như vậy thì phải có một số chia hết cho 5. Tương tự ta dễ dàng chứng minh rằng tồn tại đúng một cấp số cộng gồm 5 số nguyên tố mà công sai bằng 12 là 5, 17, 29, 41, 49. Không có cấp số cộng nào như vậy có công sai là 18 hoặc 24. Tuy nhiên từ giả thuyết H suy ra tồn tại vô hạn cấp số cộng gồm 6 số nguyên tố mà công sai bằng 30. Chẳng hạn 7, 37, 67, 97, 127, 157; 541, 571, 601, 631, 661, 691. Từ hệ quả ở trên suy ra mọi cấp số cộng gồm 7 số nguyên tố thì công sai của dãy chia hết cho 30. Dễ dàng chứng minh rằng không có cấp số cộng nào như vậy mà công sai nhỏ hơn 150. Có đúng một cấp số cộng gồm 7 số nguyên tố công sai 150 là 7, 157, 307, 457, 607, 757, 907. Lý do là vì trong bảy số nguyên tố này sẽ có một số chia hết cho 7. Từ hệ quả cũng suy ra một cấp số cộng 10 phần tử nguyên tố thì có công sai $\ge P_{10}=210$. Cấp số cộng như vậy có công sai 210 là $199+210k$, với $k=0,1,2,\ldots,9$. Từ giả thuyết H suy ra có vô hạn cấp số cộng như vậy. Từ hệ quả suy ra công sai của cấp số cộng gồm 100 số nguyên tố phải chia hết cho tích của mọi số nguyên tố nhỏ hơn 100, và do đó công sai này có hơn 30 chữ số trong biểu diễn thập phân. Ta chưa tìm được một cấp số cộng nào như vậy. Ta cũng chưa biết có tồn tại cấp số cộng như vậy hay không (Grosswald và Hagis [1]).

6. Các số nguyên tố trong một cấp số cộng cho trước

Khác với mục 5, trong mục này ta xem xét vấn đề với các số tự nhiên a và b nào thì cấp số cộng $ak+b=1,2,\ldots,$ chứa vô hạn số nguyên tố? Rõ ràng nếu $(a,b)=d>1$, thì không có số nguyên tố nào trong cấp số cộng $ak+b=1,2,..,$ bởi vì với mọi $k, ak+b=d(ka/d+b/d)$ đều là hợp số ($a/d, b/d$ là các số tự nhiên).

Vì vậy điều kiện cần để tồn tại vô hạn số nguyên tố trong cấp số cộng $ak+b$ là $(a,b)=1$.

Năm 1837 Lejeune Dirichlet đã chứng minh điều kiện trên cũng là điều kiện đủ. Lời giải đơn giản nhất của định lý này (vẫn rất phức tạp) được trình bày trong Chương 8 cuốn sách của E.Trost [3].

Ta sẽ chứng minh định lý này trong một vài trường hợp riêng. Trong Chương 5 là với $a=4,b=1,3$ (Định lý 7 và 7a), trong Chương 6 với $b=1,a$ tùy ý (Định lý 11a), trong Chương 9 với $a=8,b=3,5,7$ (Định lý 1,2,3) và với $a=5,b=4$ (Định lý 4).

Hai định lý sau là tương đương

T. *Nếu* a,b *và* k *là các số tự nhiên,* $(a,b)=1$, *thì tồn tại vô hạn số nguyên tố có dạng* $ak+b$.

T₁. *Nếu* a *và* b *là các số tự nhiên thỏa mãn* $(a,b)=1$, *thì tồn tại ít nhất một số nguyên tố* p *có dạng* $ak+b$ *với* k *tự nhiên* [(2)].

Chứng minh. Rõ ràng ***T*** suy ra ***T₁***. Ta chỉ cần chứng minh chiều ngược lại, nghĩa là ***T₁*** suy ra ***T***. Ta giả sử $a>1$ vì với $a=1$ thì ***T*** hiển nhiên đúng. Giả sử a,b là các số tự nhiên cho trước thỏa mãn $(a,b)=1$. Khi đó rõ ràng $(a^m,b)=1$. Vì vậy theo ***T₁*** suy ra tồn tại số nguyên tố p thỏa mãn $p=a^mk+b$, với số tự nhiên k. Nhưng do $a>1, a^m\geq 2^m>m$. Suy ra $p>m$. Vì vậy ta đã chứng minh với mọi số tự nhiên m thì đều tồn tại số nguyên tố có dạng $ak+b$ và lớn hơn m. Từ đây suy ra tồn tại vô hạn số nguyên có dạng như vậy. □

Trong Chương 5 Định lý 9 ta sẽ chứng minh với mọi số nguyên tố có dạng $4t+1$ đều là tổng của hai bình phương hoàn hảo. Sử dụng kết quả này ta chứng minh hệ quả sau đây của Định lý ***T***

Hệ quả. *Với mọi số tự nhiên* n *đều tồn tại số nguyên tố* p *thỏa mãn* $p=a^2+b^2$, *với* a,b *là các số tự nhiên >* n.

Chứng minh. Giả sử n là số tự nhiên. Theo ***T*** thì tồn tại số nguyên tố $q>n$ có dạng $4t-1$. Suy ra $\left(4\left(1^2+q\right)^2\left(2^2+q^2\right)^2\ldots\left(n^2+q\right)^2,q\right)=1$. Vì vậy theo ***T*** suy ra tồn tại số tự nhiên k thỏa mãn số $p=4\left(1^2+q\right)^2\left(2^2+q\right)^2\ldots\left(n^2+q\right)^2k-q$ là số nguyên tố và có dạng $4t+1$. Vì vậy tồn tại a,b thỏa mãn $p=a^2+b^2$, với $a<b$, giả sử $a\leq n$. thì

$$b^2=p-a^2=4\left(1^2+q\right)^2\left(2^2+q\right)^2\ldots\left(n^2+q\right)^2k-\left(a^2+q\right)$$
$$=\left(a^2+q\right)\left(4\left(1^2+q\right)^2\ldots\left((a-1)^2+q\right)^2\left((a+1)^2+q\right)\ldots\left(\left(n^2+q\right)^2k-1\right)\right),$$

Với các nhân tử ở vế phải đều là nguyên tố cùng nhau. Hệ quả là chúng đều là các bình phương đúng. Nhưng điều này là không thể vì nhân tử thứ hai có dạng $4t-1$. Vì vậy $b>a>n$, suy ra hệ quả được chứng minh. □

Ta lưu ý rằng theo định lý của E.Hecke [1] thì với mọi số thực $c>d\geq 0$ đều tồn tại số nguyên tố p thỏa mãn $p=a^2+b^2$ với a,b là các số tự nhiên và $c>\frac{a}{b}>d$ (Maknis [1]).

7. Tam thức Euler x^2+x+41

Dễ dàng chứng minh rằng không tồn tại đa thức $f(x)=a_0x^m+a_1x^{m-1}+\ldots+a_{m-1}x+a_m$ với hệ số nguyên và $a_0m>0$ mà các số $f(x)$ là nguyên tố với mọi giá trị nguyên của x. Thật vậy với giá trị đủ lớn của x, giả sử $x>x_0$, hàm $f(x)$ tăng. Với giá trị $x_1>x_0, f(x_1)=p$ là số nguyên tố thì $p\mid f(x_1+p)$, mà $f(x_1+p)>f(x_1)=p$, suy ra $f(x_1+p)$ là hợp số. Ta cũng chứng minh được không có hàm hữu tỷ nào nhận mọi giá trị nguyên tố với đối số nguyên ngoại trừ hàm hằng (Buck [1]). Tuy nhiên tồn tại đa thức bậc hai với hệ số nguyên nhận giá trị nguyên tố với dãy rất dài các số tự nhiên liên tiếp. Ví dụ tam thức Euler $f(x)=x^2+x+41$, nhận mọi giá trị nguyên tố với $x=0,1,\ldots,39$. Để ý rằng $f(x+1)=f(x)+2(x+1)$. Từ đây suy ra với $x=0,1,2,\ldots$ thì $f(x)$ nhận các giá trị riêng của dãy $41+2.1+2.2+2.3+\ldots$ vì vậy ta có 41, 43, 47, 53, 61, 71, 83,..., 1601. Có thể kiểm tra trong bảng các số nguyên tố để thấy tất cả các số này đều nguyên tố.

[(2)] Chứng minh sự tương đương của ***T*** và ***T₁*** được tôi ***(Sierpinski)*** đưa ra vào năm 1950 (Sierpinski [12] trang 526). Sáu năm sau bài toán về sự tương đương này được trình bày trong The Amer. Math. Monthly trong số E1218 (1956) trang 342 và được chứng minh bởi D.Zeitlin (1957, trang 46). Xem thêm V.S.Hanly [1].

Do $f(-x)=f(x-1)$, suy ra $f(-x)$ nguyên tố với $x=1,2,\ldots,40$.

Vậy với $x=-40,-39,\ldots,-1,0,1,\ldots,39$ thì $f(x)$ nhận giá trị nguyên tố (không nhất thiết phân biệt).

Hàm $f(x)$ còn có một tính chất thú vị khác: với mọi số nguyên x thì không có số d nào mà $1<d<41$ là ước của $f(x)$. Thật vậy, giả sử với số nguyên x ta có $d \mid f(x)$, với $1<d<41$. Ký hiệu r là số dư nhận được khi chia x cho d. Thế thì $x=kd+r$, với k là số nguyên và $0\le r<d$. Nhưng $f(kd+r)=kd(kd+2r+1)+f(r)$, do $d \mid f(x)$ suy ra $d \mid f(r)$; tuy nhiên từ đây ta có mâu thuẫn. Thật vậy, bởi vì $0\le r<d<41$, ta phải có $0\le r\le 39$; suy ra như ta đã biết $f(r)$ là số nguyên tố ≥ 41, và nó không có ước số d thỏa mãn $1<d<41$. Vì vậy với mọi số nguyên x thì $f(x)$ không có ước số d thỏa mãn $1<d<41$.

Tính chất này có liên quan tới việc tìm xem với số tự nhiên $x\ge 40$ nào thì $f(x)$ là số nguyên tố. Với $x=40$ ta có $f(40)=40\cdot 41+41=41^2$, do đó $f(x)$ là hợp số. Số $f(41)=41\cdot 42+41=41\cdot 43$ cũng là hợp số. Nếu $x>41$ và nếu số $f(x)$ là hợp số thì vì $(x+1)^2=x^2+2x+1$và $x^2+x+41=f(x)$, suy ra $f(x)<(x+1)^2$. Do đó số $f(x)$ có ước số $p<x+1$ và do ta đã chứng minh ở trên $41\le p<x$ (khi chia $f(x)$ cho x ta nhận được số dư là 41). Vì vậy $f(42)=42\cdot 43+41$ nguyên tố.

E.Trost trong [3] trang 41 đã chỉ ra với x không vượt quá 11000 thì hàm $f(x)$ nhận 4506 giá trị nguyên tố khác nhau. Ta chưa biết dãy $f(x)(x=1,2,\ldots)$ có chứa vô hạn số nguyên tố hay không. Kết quả của câu hỏi này được suy ra từ giả thuyết H trong mục 8.

Từ các tính chất của $f(x)$ suy ra tam thức $g(x)=f(x-40)=x^2-79x+1601$ nhận các giá trị nguyên tố (không nhất thiết phân biệt) với $x=0,1,2,\ldots,79$. Ta có $g(t)=g(79-t)$ với mọi t.

Từ các kết quả của G.Frobenius [1] và H.M.Stark [1] suy ra không tồn tại số A lớn hơn 41 mà tam thức x^2+x+A nhận các giá trị nguyên tố với $x=0,1,2,\ldots,A-2$. Với $x=0,1,\ldots,28$ thì các giá trị $6x^2+6x+31$ là các số nguyên tố phân biệt có dạng $6k+1$; chúng nằm giữa 31 và 4909 với các giới hạn kèm theo (C.Coxe, Van der Pol và Speziali [1]).

Các giá trị của $2x^2+29$ đều là nguyên tố với $-28\le x\le 28$.

Dễ dàng chứng minh rằng tồn tại đa thức bậc n nhận các giá trị nguyên tố với $x=0,1,\ldots,n$; tuy nhiên ta chưa biết đa thức bậc 2 hoặc cao hơn với biến số x nào nhận vô hạn giá trị nguyên tố với các giá trị của x. Đặc biệt ta cũng không biết đa thức x^2+1 có tính chất đó hay không.

W.A.Golubew [5] đã trình bày một danh sách các số tự nhiên $x\le 120000$ mà x^2+1 nguyên tố. M.Wunderlich [2] đã tìm ra có đúng 624535 số $x\le 14\cdot 10^6$ có tính chất như vậy. H.Iwaniec [1] đã chứng minh rằng tồn tại vô hạn số x^2+1 là tích của nhiều nhất hai số nguyên tố và B.M.Bredihin [1] đã chứng minh rằng tồn tại vô hạn số nguyên tố có dạng x^2+y^2+1.

Nếu đa thức $f(x)$ với hệ số nguyên nhận các giá trị nguyên tố với vô hạn các giá trị của x thì hệ số a_0 của lũy thừa bậc cao nhất của x phải là dương vì với giá trị đủ lớn của x thì đa thức có cùng dấu với a_0. Hơn nữa đa thức $f(x)$ không thể là tích của hai đa thức với hệ số nguyên vì nếu ngược lại thì với giá trị đủ lớn của x thì số $f(x)$ sẽ là hợp số. Vì vậy đa thức $f(x)$ là bất khả quy.

Tuy nhiên các điều kiện này không đủ để suy ra $f(x)$ nhận các giá trị nguyên tố thậm chí là với ít nhất một giá trị của x. Thật vậy, đa thức x^2+x+4 bất khả quy và không có nghiệm thực, nhưng với mọi giá trị nguyên của x thì các số x^2+x+4 đều là hợp số bởi vì chúng đều là các số chẵn lớn hơn 3 vì $x^2+x=(x+1)x$, tích này luôn chẵn và không âm.

Năm 1857 W.Bouniakowsky [2] đã đặt ra giả thuyết sau: *nếu* $f(x)$ *là đa thức bất khả quy hệ số nguyên và* N *ký hiệu ước chung lớn nhất của các số* $f(x), x$ *nhận mọi giá trị nguyên thì đa thức* $f(x)/N$ *nhận giá trị nguyên tố với vô hạn giá trị của* x*. (Dickson [7] tập 1 trang 333).*

Xét đa thức $f(x)=x^2+x+4$. Vì $f(0)=4, f(1)=6$ và $f(x)$ là số chẵn suy ra ước chung lớn nhất của $f(x)$ khi x nhận mọi giá trị nguyên là 2. Do đó giả thuyết trên nói rằng có vô hạn số nguyên tố có dạng $x(x+1)/2+2$.

8. Giả thuyết H

Ký hiệu s là số tự nhiên và $f_1(x), f_2(x),..., f_s(x)$ là các đa thức hệ số nguyên. Giả sử tồn tại vô hạn số tự nhiên x mà các số $f_1(x), f_2(x),..., f_s(x)$ đều là số nguyên tố. Như ta đã biết trong mục 7 thì các đa thức $f_i(x), i=1,2,...,s$ là bất khả quy và các hệ số cao nhất đều dương. Do đó với giá trị đủ lớn của x thì tất cả các số $f_1(x), i=1,2,...,s,$ là lớn tùy ý. Có thể kiểm tra rằng tính chất này suy ra không tồn tại số tự nhiên $d>1$ là ước của $P(x)=f_1(x)f_2(x)...f_s(x)$ với mọi số tự nhiên x. Thật vậy nếu tồn tại ước số như thế thì nó sẽ là ước số của tích s số nguyên tố lớn tùy ý, điều này là không thể. Vì vậy ta đã chứng minh rằng nếu s là số tự nhiên và $f_1(x), f_2(x),..., f_s(x)$ là các đa thức hệ số nguyên và có vô hạn các giá trị tự nhiên của x mà các số $f_1(x), f_2(x),..., f_s(x)$ đều nguyên tố thì các đa thức này phải thỏa mãn

Điều kiện C. *Các đa thức* $f_i(x), (i=1,2,...,s,)$ *đều bất khả quy với hệ số cao nhất dương và không tồn tại số tự nhiên* $d>1$ *là ước của* $P(x)=f_1(x)f_2(x)...f_s(x), x$ *nguyên tùy ý.*

Năm 1958 A.Schinzel đã đặt ra giả thuyết sau

Giả thuyết H. *Nếu* s *là số tự nhiên và* $f_1(x), f_2(x),..., f_s(x)$ *là các đa thức hệ số nguyên thỏa mãn Điều kiện C thì tồn tại vô hạn số tự nhiên* x *mà các số* $f_1(x), f_2(x),..., f_s(x)$ *đều nguyên tố (Schinzel et Sierpinski [3], trang 188).*

Trường hợp riêng khi các đa thức f_1 là tuyến tính ta thu lại giả thuyết đặt ra sớm hơn bởi L.E.Dickson [1]. Ta trình bày ở đây một số hệ quả của giả thuyết H.

Với số tự nhiên cho trước n và $f_1(x)=x^{2^n}+1, f_2(x)=x^{2^n}+3, f_3(x)=x^{2^n}+7, f_4(x)=x^{2^n}+9.$

Với $P(x)=f_1(x)f_2(x)f_3(x)f_4(x)$ ta có $P(0)=1\cdot3\cdot7\cdot9$ và $P(1)=2\cdot4\cdot8\cdot10.$ Hệ quả là $(P(0),P(1))=1.$ Suy ra điều kiện C được thỏa mãn và giả thuyết H suy ra: *với mọi số tự nhiên* n *tồn tại vô hạn số tự nhiên* x *mà các số* $x^{2^n}+1, x^{2^n}+3, x^{2^n}+7, x^{2^n}+9$ *đều là nguyên tố* (Sierpinski [34]). Từ đây suy ra tồn tại vô hạn bộ các số nguyên tố sinh bốn (xem mục 3) và tồn tại vô hạn các số nguyên tố có dạng x^2+1 hoặc dạng $x^4+1.$

W.A.Golubew [6] đã tính toán và chỉ ra chỉ có 5 số tự nhiên x nhỏ hơn 10.000 mà các số $x^2+1, x^2+3, x^3+7, x^2+9$ đều là nguyên tố. Đó là $x=2,10,1420,2080,2600.$

Ký hiệu k là số nguyên tùy ý và $f_1(x)=x, f_2(x)=x+2k.$ Với $P(x)=f_1(x)f_2(x)$ ta có $P(1)=2k+1, P(2)=4(k+1).$ Rõ ràng $(2k+1,4(k+1))=1,$ suy ra các đa thức này thỏa mãn điều kiện C. Từ giả thuyết H suy ra tồn tại vô hạn các số tự nhiên x mà các số $p=x$ và $q=x+2k$ đều là số nguyên tố. Vì vậy $2k=p-q,$ suy ra $2k$ có thể biểu diễn vô hạn cách như là hiệu của hai số nguyên tố. Nghĩa là từ giả thuyết H có thể suy ra mọi số chẵn đều có thể biểu diễn vô hạn cách như là hiệu của hai số nguyên tố. Từ giả thuyết H cũng có thể suy ra mọi số chẵn có thể biểu diễn dưới dạng hiệu của hai số nguyên tố liên tiếp (Schinzel và Sierpinski [3] trang 190).

Từ giả thuyết H suy ra nếu a và b là các số tự nhiên thỏa mãn $(a,b)=(a,b(b+2))=1,$ thì tồn tại vô hạn số nguyên tố p có dạng $ak+b,$ với k là số tự nhiên thỏa mãn $p+2$ cũng là số nguyên tố. Thật vậy, xét các đa thức $f_1(x)=ax+b, f_2(x)=ax+b+2.$ Với $P(x)=f_1(x)f_2(x)$ ta có $P(0)=b(b+2), P(1)=(a+b)(a+b+2)$ và $P(1)+P(-1)=2a^2+2b(b+2).$ Nếu tồn tại số nguyên tố q thỏa mãn $q\mid P(x)$ với mọi số nguyên $x,$ thì nếu b lẻ ta có $P(0)$ lẻ kéo theo q lẻ và nếu b chẵn thì vì $(a,b)=1, a$ lẻ; vì vậy cả $a+b$ và $a+b+2$ đều lẻ và do đó $P(1)$ lẻ suy ra q lẻ. Do đó trong mọi trường hợp q đều lẻ. Vậy ta có thể giả sử $q\mid P(0),$ nghĩa là $q\mid b(b+2)$ và $q\mid P(1)+P(-1),$ ta có $q\mid 2a^2$ do đó vì q lẻ nên $q\mid a.$ Nhưng điều này vô lý vì $(a,b(b+2))=1.$ Vì vậy điều kiện C được thỏa mãn. Do đó từ giả thuyết H suy ra tồn tại vô hạn số tự nhiên x mà các số $f_1(x)=ax+b$ và $f_2(x)=ax+b+2$ đều nguyên tố. Hệ quả được chứng minh.

Dễ dàng nhận thấy điều kiện $(a,b(b+2))=1$ là cần thiết đối với sự tồn tại vô hạn các số p có dạng $ak+b$ mà $p+2$ cũng là số nguyên tố.

Xét số nguyên tùy ý k và đặt $f_1(x)=x, f_2(x)=2k+1+2x.$ Với $P(x)=f_1(x)f_2(x)$ ta có $P(1)=2k+3, P(-1)=-(2k-1).$ Do $(2k-1,2k+3)=1$ với mọi số nguyên $k,$ ta nhận thấy các đa thức này thỏa mãn điều kiện C. Khi đó theo giả thuyết H thì tồn tại vô hạn các số tự nhiên x mà các số $q=x$ và $p=2k+1+2x$ đều nguyên tố. Vì vậy $2k+1=p-2q.$ Do đó từ giả thuyết H suy ra mọi số lẻ (>0 hoặc <0) đều có thể biểu diễn vô hạn cách như là hiệu của một số nguyên tố và bội 2 của một số nguyên tố khác.

G.de Rocquigny [1] đặt ra câu hỏi có phải mọi số nguyên chia hết cho 6 đều là hiệu của hai số nguyên tố có dạng $6k+1.$ Câu trả lời khẳng định là hệ quả của giả thuyết H. Thật vậy với $f_1(x)=6x+1$ và $f_2(x)=6x+6k+1,$ $P(x)=f_1(x)f_2(x)$ ta có $P(0)=6k+1, P(-k)=-(6k-1)$ và $(6k-1,6k+1)=1$ với mọi số nguyên $k.$

Từ giả thuyết H suy ra tồn tại cấp số cộng dài vô hạn mà các phần tử là các số nguyên tố liên tiếp (Schinzel và Sierpinski [13]). Có rất nhiều hệ quả khác được suy ra từ giả thuyết H, ví dụ giả thuyết Bouniakowsky (xem Schinzel và Sierpinski [3] và Schinzel [13]).

Bài tập. Chứng minh rằng từ giả thuyết H suy ra: với hai số nguyên nguyên tố cùng nhau a và b thỏa mãn một trong hai số là chẵn và $a>0.$ Khi đó tồn tại vô hạn số nguyên tố p thỏa mãn $ap+b$ đều là số nguyên tố.

Chứng minh. Đặt $f_1(x)=ax+b, f_2(x)=x.$ Với $P(x)=f_1(x)f_2(x)$ ta có $P(1)=a+b,$ $P(-1)=a-b,$ và do một trong hai số a,b là chẵn, số còn lại là lẻ vì $(a,b)=1.$ Và từ $(a,b)=1$ suy ra $(a+b,a-b)=1.$ Do đó $(P(1),P(-1))=1$ và điều kiện C được thỏa mãn. Khi đó từ giả thuyết H suy ra tồn tại vô hạn x mà $f_2(x)=x$ và $f_1(x)=ax+b$ đều là các số nguyên tố. Ta có điều phải chứng minh.

9. Hàm số $\pi(x)$

Với mọi số thực x ký hiệu $\pi(x)$ là số các số nguyên tố không vượt quá x.

Ta có

$\pi(1)=0, \pi(2)=1, \pi(3)=\pi(4)=2, \pi(5)=\pi(6)=3, \pi(7)=\pi(8)=\pi(9)=\pi(10)=4,$
$\pi(100)=25, \pi(1000)=168, \pi(10000)=1229, \pi(10^5)=9592, \pi(10^6)=78498, \pi(10^7)=664579,$
$\pi(10^8)=5761455, \pi(10^9)=50847534.$

Năm 1972 J.Bohman [1] đã tính được $\pi(10^9)=455052511$ (đây là kết quả chỉnh sửa từ kết quả của Lebmer [8] vào năm 1958), $\pi(10^{11})=4118054813, \pi(10^{12})=37607912018$. Gần đây J.C.Lagarias, V.S.Miller và A.M.Odlyzko [1] đã tính được $\pi(10^{13})=346065536839$ (đây là kết quả chỉnh sửa từ kết quả của Bohman [1]), $\pi(10^{14})=3204941750802, \pi(10^{15})=298445704422669$ và $\pi(10^{16})=279238341033925$. Hiển nhiên ta có $\pi(p_n)=n$ với $n=1,2,\ldots$

P.Erdos (Trost [3] trang 52-53) đã tìm ra lời giải đơn giản của bất đẳng thức

(2) $$\pi(n)\geq\frac{\log n}{2\log 2} \text{ với } n=1,2,\ldots$$

Như ta đã chứng minh trong Chương 1 mục 14, mọi số tự nhiên đều có thể biểu diễn duy nhất dưới dạng k^2l, với k và l là các số tự nhiên và hơn nữa l là không có ước chính phương. Với mỗi số trong các số $1,2,\ldots,n$, ta có biểu diễn $k^2l\leq n$; do đó $k^2\leq n$. Vì vậy $k\leq\sqrt{n}$. Suy ra k có thể nhận nhiều nhất $\sqrt{n}$ giá trị khác nhau. Số l không có ước số chính phương và nhỏ hơn n nên có thể biểu diễn như là tích của một số số nguyên tố thuộc dãy $p_1, p_2, \ldots, p_{\pi(n)}$. Số lượng các số như vậy (tính cả 1) là $2^{\pi(n)}$. Hệ quả là số l có thể nhận nhiều nhất $2^{\pi(n)}$ giá trị khác nhau. Do đó số lượng các tích lk^2 phân biệt và không lớn hơn n, tối đa là $\sqrt{n}2^{\pi(n)}$. Vì mọi số tự nhiên $\leq n$ đều được biểu diễn dưới dạng đó suy ra $n\leq\sqrt{n}2^{\pi(n)}$. Vậy $\sqrt{n}\leq 2^{\pi(n)}$ và lấy logarithm cả hai vế ta có $\frac{1}{2}\log n\leq\pi(n)\log 2$, từ đây suy ra ***(2)***.

Sau đây trong mục 14 ta sẽ chứng minh các bất đẳng thức chặt hơn cho $\pi(n)$. Tuy nhiên điều thú vị của bất đẳng thức ***(2)*** nằm ở tính đơn giản trong cách chứng minh của nó.

Ký hiệu k là số tự nhiên tùy ý và $n=p_k$. Theo công thức ***(2)*** và $\pi(p_k)=k$, ta có $k\geq\log p_k/2\log 2$. Do đó $p_k\leq 2^{2k}$ với $k=1,2,\ldots$, hơn nữa 2^{2k} là hợp số với mọi $k=1,2,\ldots$, suy ra

(3) $$p_k<2^{2k} \text{ với } k=1,2,\ldots$$

Bài tập. ***1.*** Chứng minh rằng với mọi số tự nhiên $n>1$ bất đẳng thức

(4) $$\frac{\pi(n-1)}{n-1}<\frac{\pi(n)}{n}$$

đúng nếu và chỉ nếu n là số nguyên tố. Với mọi hợp số n ta có

(5) $$\frac{\pi(n-1)}{n-1}>\frac{\pi(n)}{n}.$$

Chứng minh. Nếu n là hợp số thì $\pi(n)=\pi(n-1)$ và ***(5)*** đúng. Nếu n là số nguyên tố thì $\pi(n)=\pi(n-1)+1,$

(6) $$\frac{\pi(n)}{n}-\frac{\pi(n-1)}{n-1}=\frac{1}{n}\left(1-\frac{\pi(n-1)}{n-1}\right).$$

Nhưng $\pi(k)<k$ với $k=1,2,\ldots$ nên từ ***(6)*** suy ra ***(4)***. □

2. Cho trước số tự nhiên $m,$ tìm tất cả các nghiệm tự nhiên của phương trình $\pi(n)=m$.

Lời giải. Các nghiệm tự nhiên n thỏa mãn $p_m \le n < p_{m+1}$. Vậy có đúng $p_{m+1}-p_m$ nghiệm cần tìm.

10. Chứng minh định đề Bertrand (Định lý Tchebycheff)

Với số thực cho trước x ký hiệu $[x]$ là số nguyên lớn nhất $\le x$.

Ta có $\left[\frac{3}{4}\right]=0,\left[-\frac{3}{4}\right]=-1,\left[\sqrt{2}\right]=1,[\pi]=3.$

Từ định nghĩa suy ra với mọi số thực x ta có $x-1<[x]\le x$. Đẳng thức $[x]=x$ xảy ra nếu và chỉ nếu x là số nguyên. Nếu k là số nguyên thì với các số thực x ta có $[x+k]=[x]+k$. Với mọi số thực x, y ta có $[x]+[y]\le[x+y]$. Ví dụ $0=\left[\frac{1}{2}\right]+\left[\frac{2}{3}\right]<\left[\frac{1}{2}+\frac{2}{3}\right]=1$ và $\left[\frac{1}{3}\right]+\left[\frac{1}{2}\right]=\left[\frac{1}{3}+\frac{1}{2}\right]=0.$

Định lý 6. *Lũy thừa của số nguyên tố p trong phân tích thành thừa số nguyên tố của $n!$ là*

(7) $$a=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots$$

Chứng minh. Giả sử n,k là hai số tự nhiên cho trước và số nguyên tố $p \le n$. Các số trong dãy $1,2,\ldots,n$ chia hết cho p^k đều có dạng lp^k, với l là số tự nhiên thỏa mãn $lp^k \le n,$ nghĩa là $l \le n/p^k$. Số các số l như vậy là $\left[n/p^k\right]$. Mặt khác rõ ràng số mũ a của số nguyên tố p trong phân tích thành thừa số nguyên tố của $n!$ chính là tổng của số các số trong dãy $1,2,\ldots,n$ mà chia hết cho p với số các số chia hết cho p^2 và số các số chia hết cho p^3 và cứ như thế. Từ đây suy ra ***(7)***. □

Ứng dụng đơn giản nhất của Định lý 6 là tính số chữ số 0 tận cùng của 100!. Theo công thức ***(7)*** (với $n=100$ và $p=2$) thì số mũ của 2 trong phân tích thành thừa số nguyên tố của 100! Là $\left[\frac{100}{2}\right]+\left[\frac{100}{2^2}\right]+\left[\frac{100}{2^3}\right]+\ldots=50+25+12+6+3+1=97.$

Số mũ của 5 là $\left[\frac{100}{5}\right]+\left[\frac{100}{5^2}\right]=20+4=24.$ Vì vậy số 100! có 24 chữ số 0 tận cùng.

Bổ đề 1. *Với mọi số tự nhiên $n>1$ ta có*

(8) $$\binom{2n}{n}>\frac{4^n}{2\sqrt{n}}.$$

Chứng minh. Bất đẳng thức ***(8)*** đúng với $n=2$ bởi vì $\binom{4}{2}=6>\frac{4^2}{2\sqrt{2}}.$ Giả sử bất đẳng thức ***(8)*** đúng với số tự nhiên $n>1.$ Ta có

$$\binom{2n+2}{n+1}=2\frac{2n+1}{n+1}\binom{2n}{n}>\frac{2(2n+1)4^n}{(n+1)2\sqrt{n}}$$

$$=\frac{2(2n+1)4^n}{\sqrt{4n(n+1)}\sqrt{n+1}}>\frac{4^{n+1}}{2\sqrt{n+1}}.$$

Vì $(2n+1)^2>4n(n+1),$ suy ra $2n+1>\sqrt{4n(n+1)}.$ Theo quy nạp suy ra ***(8)*** được chứng minh. □

Bổ đề 2. *Tích* P_n của các số nguyên tố $\le n,$ với số tự nhiên n cho trước, là không vượt quá 4^n.

Chứng minh. Bổ đề hiển nhiên đúng với $n=1$ và $n=2.$ Ký hiệu n là số tự nhiên $>2.$ Giả sử bổ đề đúng với các số tự nhiên $<n.$ Nếu n là số chẵn $>2,$ thì $P_n=P_{n-1}.$ Vì vậy bổ đề đúng với $n.$ Nếu $n=2k+1,$ với k là số tự nhiên thì mỗi số nguyên tố p thỏa mãn $k+2\le p\le 2k+1$ đều là ước số của

(9) $$\binom{2k+1}{k}=\frac{(2k+1)2k(2k-1)\ldots(k+2)}{1\cdot 2\ldots k}.$$

Do $(1+1)^{2k+1}>\binom{2k+1}{k}+\binom{2k+1}{k+1}=2\binom{2k+1}{k},$ ta có $\binom{2k+1}{k}<4^k.$ Vậy tích của tất cả các số nguyên tố phân biệt thỏa mãn $k+2\le p\le 2k+1$ là ước của ***(9)*** không vượt quá $4^k.$ Nhưng theo giả thiết thì bổ đề đúng với mọi số nhỏ hơn $n,$ nên tích của các số nguyên tố $\le k+1$ là nhỏ hơn $4^{k+1},$ ta có $P_n=P_{2k+1}<4^k\cdot 4^{k+1}=4^{2k+1}=4^n.$ Vì vậy $P_n<4^n.$ Theo quy nạp bổ đề được chứng minh. □

Bổ đề 3. Nếu p *là ước số nguyên tố của số* $\binom{2n}{n}$ *với* $p\ge\sqrt{2n},$ *thì* $p=\sqrt{2n}$ *chỉ khi lũy thừa của* p *trong phân tích thành thừa số nguyên tố của* $\binom{2n}{n}$ *bằng 1.*

Chứng minh. Theo Định lý 6 thì lũy thừa của p trong phân tích thành thừa số nguyên tố của $(2n)!$ là $\left[\frac{2n}{p}\right]+\left[\frac{2n}{p^2}\right]+\left[\frac{2n}{p^3}\right]+\ldots$ và trong phân tích của $n!$ là $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots$ Do $\binom{2n}{n}=\frac{(2n)!}{(n!)^2}$ suy ra lũy thừa của p trong $\binom{2n}{n}$ là $a=\sum_{k=1}^{x}\left[\frac{2n}{p^k}\right]-2\sum_{k=1}^{x}\left[\frac{n}{p^k}\right]=\sum_{k=1}^{x}\left(\left[\frac{2n}{p^k}\right]-2\left[\frac{n}{p^k}\right]\right).$

Nếu $p\ge\sqrt{2n},$ thì $p=2$ chỉ khi $n=2.$ Do đó với mọi $n\ne 2$ thì ta có $p>\sqrt{2n},$ từ đây suy ra $a=\left[\frac{2n}{p}\right]-2\left[\frac{n}{p}\right]<2.$ Hệ quả là $a<2,$ nghĩa là $a\le 1$ (do a là số nguyên).

Bổ đề 3 được chứng minh với $n\ne 2.$ Với $n=2,$ ta có $\binom{4}{2}=2\cdot 3.$ □

Bổ đề 4. *Mọi ước số* p^r *(p nguyên tố, r là số tự nhiên) của* $\binom{2n}{n}$ *đều* $\le 2n.$ *Ta có* $\binom{2n}{n}\le(2n)^{\pi(2n)}.$

Chứng minh. Với số nguyên tố p thỏa mãn $p^r\mid\binom{2n}{n},$ lũy thừa của p trong phân tích thành thừa số nguyên tố của $\binom{2n}{n}$ là $a=\sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right]-2\left[\frac{n}{p^k}\right]\right)\ge r.$

Nếu $p^r > 2n,$ thì ta có $\left[\frac{2n}{p^k}\right]-2\left[\frac{n}{p^k}\right]=0$ với $k \geq r;$ suy ra $a=\sum_{k=1}^{r-1}\left(\left[\frac{2n}{p^k}\right]-2\left[\frac{n}{p^k}\right]\right).$

Nhưng với mọi số thực $x,\left[2x\right]-2\left[x\right]\leq 1,$ đẳng thức cuối cùng suy ra $a \leq r-1,$ mâu thuẫn với tính chất $a \geq r$. Vì vậy $p^r \leq 2n.$

Để chứng minh phần thứ hai của bổ đề ta chú ý rằng trong phân tích thành thừa số nguyên tố của $\binom{2n}{n}$ thì chỉ có các số nguyên tố $\leq 2n$ xuất hiện, ta có $\binom{2n}{n} \leq (2n)^{\pi(2n)}$ Điều phải chứng minh. □

Bổ đề 5. *Nếu n là số tự nhiên $>2,$ thì $\binom{2n}{n}$ không có ước số nguyên tố p nào mà $\frac{2}{3}n < p \leq n$.*

Chứng minh. Nếu $\frac{2}{3}n < p \leq n,$ thì $\frac{2n}{p}<3$ và $\frac{n}{p}\geq 1.$ Do đó $\left[\frac{2n}{p}\right]\leq 2,\left[\frac{n}{p}\right]\geq 1,$ suy ra $\left[\frac{2n}{p}\right]-2\left[\frac{n}{p}\right]=0.$ [(3)]. Với $k>1$ ta có $p^k > \frac{4}{9}n^2$ và do đó $\frac{2n}{p^k}<\frac{9}{2n}<1$ với $n>4.$ Vì vậy $\left[\frac{2n}{p}\right]-2\left[\frac{n}{p}\right]=0.$ với mọi $k>1$ và $n>4.$ Vậy ta suy ra với $n>4$ thì lũy thừa của số nguyên tố p trong $\binom{2n}{n}$ bằng 0, nghĩa là $\binom{2n}{n}$ không chia hết cho p. Suy ra bổ đề đúng với $n>4.$ Với $n=3$ hoặc $n=4$ ta có từ $\frac{2}{3}n < p \leq n$ suy ra $p=3$ và 3 không phải ước số của $\binom{6}{3}=20$ và $\binom{8}{4}=70.$ Bổ đề được chứng minh. □

Bổ đề 6. *Lúy thừa của số nguyên tố p mà $n<p<2n$ trong $\binom{2n}{n}$ là bằng 1.*

Chứng minh. Với $n<p<2n$ ta có $1<\frac{2n}{p}<2,\frac{n}{p}<1.$ Suy ra $\left[\frac{2n}{p}\right]=1,\left[\frac{n}{p}\right]=0$. Với $k\geq 2$ ta có $\frac{2n}{p^k}\leq\frac{2n}{p^2}<\frac{2}{n}.$ Suy ra với $n>1,\frac{2n}{p^k}<1$ và hệ quả $\left[\frac{2n}{p^k}\right]=0,$ suy ra $\left[\frac{n}{p^k}\right]=0.$ Vậy lũy thừa a của số nguyên tố p trong phân tích của $\binom{2n}{n}$ thành thừa số nguyên tố là bằng 1. Với $n=1$ thì $n<p<2n$ không thỏa mãn. Bổ đề được chứng minh. □

Bổ đề 7. *Với $n\geq 14$ ta có $\pi(n)\leq\frac{1}{2}n-1.$*

Chứng minh. Dễ dàng kiểm tra $\pi(14)=6=\frac{14}{2}-1.$ Suy ra Bổ đề 7 đúng với $n=14.$ Giả sử n là số tự nhiên không nhỏ hơn 15. Trong dãy $1,2,\ldots,n$ các số chẵn $4,6,8,\ldots,2\left[\frac{n}{2}\right]$ đều là hợp số. Số các số

[(3)] Thật vậy với số thực x ta có $2\left[x\right]\leq 2x,\left[2x\right]>2x-1,$ suy ra $\left[2x\right]-2\left[x\right]>-1,$ và hệ quả là vì vế trái là số nguyên nên ta có $\left[2x\right]-2\left[x\right]\geq 0.$

như vậy là $\left[\frac{n}{2}\right]-1$. Hơn nữa trong dãy $1,2,\ldots,n$ với $n\ge 15,$ có các số lẻ nhưng không nguyên tố là $1,9,15.$ Vì vậy $\pi(n)\le n-\left(\left[\frac{n}{2}\right]-1+3\right)=n-\left[\frac{n}{2}\right]-2<\frac{n}{2}-1$ (vì $\left[\frac{n}{2}\right]>\frac{n}{2}-1$). Do đó $\pi(n)<\frac{n}{2}-1$ với $n\ge 15,$ suy ra bổ đề được chứng minh. □

Bổ đề 8. *Ký hiệu R_n là tích tất cả các số nguyên tố p thỏa mãn $n<p\le 2n$. Nếu không có số nguyên tố nào như vậy thì đặt $R_n=1$. Khi đó với $n\ge 98.$*

(10) $$R_n>\frac{4^{n/3}}{2\sqrt{n}(2n)^{\sqrt{n/2}}}$$

Chứng minh. Từ định nghĩa của R_n suy ra $R_n\mid\binom{2n}{n}$. Hệ quả là $\binom{2n}{n}=Q_nR_n,$ với Q_n là số tự nhiên. Vì vậy theo Bổ đề 6 ta suy ra không có số nguyên tố p nào mà $n<p\le 2n$ lại xuất hiện trong phân tích thành thừa số nguyên tố của Q_n. Suy ra các số nguyên tố p không xuất hiện trong phân tích này đều $\le n,$ vì vậy theo Bổ đề 5 thì số đó phải $\le\frac{2}{3}n.$ Suy ra tích của tất cả các số nguyên tố phân biệt p thỏa mãn $p\mid Q_n$ là không lớn hơn tích của tất cả các số nguyên tố không vượt quá $\frac{2}{3}n$. Tích này theo Bổ đề 2 thì không vượt quá $4^{2n/3}$. Theo bổ đề 3 và $Q_n\mid\binom{2n}{n},$ lũy thừa của số nguyên tố p trong Q_n có thể lớn hơn 1 chỉ khi $p<\sqrt{2n}$. Số các số nguyên tố như vậy theo Bổ đề 7 (với $\left[\sqrt{2n}\right]$ thay thế cho n vì với $n\ge 98,$ ta có $\sqrt{2n}\ge 14$) là nhỏ hơn $\sqrt{2n}/2$. Theo Bổ đề 4 thì tích của tất cả các lũy thừa của các số nguyên tố xuất hiện trong phân tích thành thừa số nguyên tố của $\binom{2n}{n}$ là $<(2n)^{\sqrt{2n}/2}$. Ta cũng có bất đẳng thức như vậy cho tích của các lũy thừa của các số nguyên tố xuất hiện trong phân tích thành thừa số nguyên tố của Q_n. Vì vậy $Q_n<4^{2n/3}(2n)^{\sqrt{2n}/2}$. Nhưng vì $\binom{2n}{n}=Q_nR_n,$ và theo Bổ đề 1 suy ra $Q_nR_n>4^n/2\sqrt{n}$ từ đó công thức ***(10)*** được chứng minh. □

Bổ đề 9. *Với số tự nhiên $k\ge 8$ ta có $2^k>18(k+1).$*

Chứng minh. Chứng minh bằng quy nạp. Ta có $2^8=256>18\cdot 9.$ Nếu $2^k>18(k+1),$ thì $2^{k+1}=2^k+2^k>18k+18+18k+18>18k+36=18(k+2).$ □

Bổ đề 10. *Với mọi số thực $x\ge 8$ ta có $2^x>18x.$*

Chứng minh. Với mọi số thực $x\ge 8$ ta có $[x]\ge 8.$ Theo Bổ đề 9, $2^x\ge 2^{[x]}>18([x]+1)>18x,$ suy ra $2^x>18x,$. □

Bổ đề 11. *Với số tự nhiên $k\ge 6$ ta có $2^k>6(k+1).$*

Chứng minh. Theo Bổ đề 9 thì chỉ cần chứng minh Bổ đề 11 với $k=6$ và $k=7.$ Ta có $2^6=64>6\cdot 7$ và $2^7=128>6\cdot 8.$ □

Bổ đề 12. *Với số thực $x\ge 6$ ta có $2^x>6x.$*

Chứng minh tương tự Bổ đề 10.

Bổ đề 13. *Nếu n là số tự nhiên ≥ 648, thì $R_n > 2n$.*

Chứng minh. Theo Bổ đề 8 chỉ cần chứng minh nếu $n \geq 648$, thì $4^{n/3} > 4n\sqrt{n}\left(2n\right)^{\sqrt{n/2}}$. Lưu ý rằng nếu $n \geq 648$, thì $\sqrt{2n}/6 > 6$ và theo Bổ đề 12, $2^{\sqrt{2n}/6} > \sqrt{2n}$, suy ra $2^{n/3} > \left(2n\right)^{\sqrt{n/2}}$. Nhưng do $n \geq 648$, ta có $2n/9 > 8$, sử dụng Bổ đề 10 ta nhận được $2^{2n/9} > 4n$, suy ra $2^{n/3} > 4n\sqrt{4n} > 4n\sqrt{n}$. Vậy với $n \geq 648$, ta có $4^{n/3} > 4n\sqrt{n}\left(2n\right)^{\sqrt{n/2}}$. Bổ đề được chứng minh. □

Bổ đề 14. *Nếu $n \geq 648$, thì giữa n và $2n$ có ít nhất hai số nguyên tố khác nhau.*

Chứng minh. Từ định nghĩa của R_n thì nếu có nhiều nhất một số nguyên tố giữa n và $2n$, thì ta có $R_n \leq 2n$, với $n \geq 648$, mâu thuẫn với Bổ đề 13. □

Định lý 7. *Nếu n là số tự nhiên > 5, thì giữa n và $2n$ có ít nhất hai số nguyên tố khác nhau.*

Chứng minh. Với $n = 6$ định lý đúng vì giữa 6 và 12 chỉ có hai số nguyên tố là 7 và 11. Vì vậy theo Bổ đề 14, định lý được chứng minh cho các số tự nhiên n mà $7 \leq n < 648$. Để kiểm tra điều này ta không cần phải thử với các trường hợp $7, 8, \ldots, a = 647$ trực tiếp. Ta chỉ cần xác định dãy các số nguyên tố $q_0, q_1, \ldots, q_m$ mà $q_0 = 7, q_k < 2q_{k-2}$ với $k = 2, 3, \ldots, m$ và $q_{m-1} > a$. Ký hiệu n là số tự nhiên tùy ý thỏa mãn $7 \leq n \leq a$. Phần tử đầu tiên của dãy $q_0, q_1, \ldots, q_m$ là $\leq n$ và phần tử cuối là $> a \geq n$. Vì vậy tồn tại chỉ số lớn nhất k với $k < m-1$ thỏa mãn $q_k \leq n$. Ta có $k+2 \leq m, n < q_{k+1}$ và vì vậy do $q_{k+2} < 2q_k \leq 2n$, suy ra giữa n và $2n$ có ít nhất hai số nguyên tố là q_{k+1} và q_{k+2}. □

Dãy trên chính là 7,11,13,19,23,37,43,73,83,139,163,277,317,547,631,653,1259.

Hệ quả trực tiếp của Định lý 7 là

Định lý 8 (Tchebycheff). *Nếu n là số tự nhiên > 3, thì giữa n và $2n-2$ có ít nhất một số nguyên tố.*

Chứng minh. Với $n = 4$ và $m = 5$ thì định lý đúng. Nếu $n > 5$, thì theo Định lý 7, giữa n và $2n$ tồn tại ít nhất hai số nguyên tố. Nếu số lớn hơn là $q = 2n-1$, thì số kia là $< 2n-2$, vì $2n-2$, với $n > 5$, là hợp số nên ta có $n < p < 2n-2$. Nếu $q < 2n-1$, thì vì $q < 2n-1$, ta có $n < p < 2n-2$. □

Định lý 8 được đặt ra như là một giả thuyết bởi J.Bertrand vào năm 1845 và được chứng minh lần dầu bởi P.Tchebycheff vào năm 1850. Chứng minh ở trên là một biến thể của chứng minh của P.Erdos [1] được trình bày bởi L.Kalmar.

Hệ quả 1. *Nếu n là số tự nhiên > 1, thì giữa n và $2n$ có ít nhất một số nguyên tố.*

Chứng minh. Theo Định lý 8 thì hệ quả đúng với các số tự nhiên > 3. Kiểm tra trực tiếp với $n = 2$ và $n = 3$. □

Năm 1892 J.J.Sylvester [1] chứng minh mở rộng của Hệ quả 1: nếu $n > k$, thì trong dãy $n, n+1, n+2, \ldots, n+k-1$ có ít nhất một số có ước số $> k$. Hệ quả 1 nhận được với $n = k+1$. Mở rộng này được chứng minh bởi I.Schur [2] năm 1924. Chứng minh sơ cấp và ngắn hơn được trình bày bởi P.Erdos [2] năm 1934 (Erdos [12]).

Hệ quả 2. *Với mọi số tự nhiên $k > 1$ ta có $p_k < 2^k$.*

Chứng minh. Ta có $p_2 = 3 < 2^2$. Với mọi số tự nhiên k, $p_k < 2^k$, sử dụng Hệ quả 1 ta thấy giữa 2^k và 2^{k+1} có ít nhất một số nguyên tố, số này không lớn hơn p_k. Vì vậy $p_{k+1} < 2^{k+1}$ và theo quy nạp hệ quả được chứng minh. □

Hệ quả 2 mạnh hơn bất đẳng thức ***(3)*** mục 9; tuy nhiên chứng minh của nó thì phức tạp hơn.

Hệ quả 3. *Trong phân tích thành thừa số nguyên tố của* $n!$ *với* $n>1$ *tồn tại ít nhất một số nguyên tố với lũy thừa bằng 1.*

Chứng minh. Với $n=2$ thì hệ quả hiển nhiên đúng. Nếu $n=2k>1,$ với k là số tự nhiên >1 thì theo Hệ quả 1 thì tồn tại số nguyên tố p mà $k<p<2k,$ suy ra $p<n<2p$ và hệ quả là p là ước số của chỉ một trong các nhân tử của tích $1\cdot 2\cdot \ldots \cdot n.$ Mặt khác nếu p thỏa mãn $k<p<2k<n,$ suy ra $2k<2p$ và do đó $2k+1<2p,$ nghĩa là $p<n<2p,$ suy ra Hệ quả 3 được chứng minh. □

Hệ quả trực tiếp của Hệ quả 3 là

Hệ quả 4. *Với mọi số tự nhiên* $n>1$ *thì số* $n!$ *không phải lũy thừa bậc* k *với* $k>1$ *là số tự nhiên.*

Từ Định lý 7 suy ra

Định lý 9. *Với mọi số tự nhiên* $k>3$ *ta có* $p_{k+2}<2p_k.$

Chứng minh. Ký hiệu k là số tự nhiên $>3.$ Ta có $p_k>p_3=5.$ Theo Định lý 7 thì giữa p_k và $2p_k$ có ít nhất hai số nguyên tố khác nhau. Nhưng hai số nguyên tố nhỏ nhất lớn hơn p_k lại là p_{k+1} và $p_{k+2},$ vậy ta có $p_{k+2}<2p_k.$ □

Ta lưu ý rằng từ Định lý 9 cũng suy ra Định lý 7. Thật vậy giả sử Định lý 9 là đúng thì nếu ký hiệu n là số tự nhiên tùy ý >6 thì $p_4=7\le n.$ Đặt p_k là số nguyên tố lớn nhất thỏa mãn $p_k\le n.$ Ta có $k>3$ và $p_{k+1}>n.$ Vì vậy theo Định lý 9 thì $p_{k+2}<2p_k\le 2n.$ Do đó giữa n và $2n$ có ít nhất hai số nguyên tố là p_{k+1} và $p_{k+2}.$ Cuối cùng chỉ cần kiểm tra Định lý 7 với $n=6.$ Ta đã chứng minh các định lý 7 và 9 là tương đương.

Hệ quả 1. *Ta có* $p_{k+1}<2p_k$ *với mọi* $k=1,2,\ldots$

Chứng minh. Với $k=4,5,\ldots$ thì Hệ quả 1 được suy ra từ Định lý 9. Ta kiểm tra trực tiếp Hệ quả 1 với $k=1,2,3;\ p_2=3<4=2p_1,\ p_3=5<6=2p_2,\ p_4=7<10=2p_3.$ □

Hệ quả 2. *Với mọi số tự nhiên* $k>1$ *ta có* $p_{k+2}<p_k+p_{k+1}.$

Chứng minh. Với $k>3$ thì kết quả này được suy ra từ Định lý 9 với $p_{k+2}<2p_k<p_k+p_{k+1}$ (do $p_k<p_{k+1}$). Điều này cũng đúng với $k=2$ và $k=3.$ Thật vậy ta có $p_4=7<3+5=p_2+p_3$ và $p_5=11<5+7=p_3+p_4.$ □

Bài tập. *1*. Tìm số tự nhiên n là tổng của tất cả các số nguyên tố nhỏ hơn $n.$

Lời giải. Số nhỏ nhất có tính chất này là $5=2+3.$ Giả sử $n>5$ thỏa mãn. Nếu p_k là số nguyên tố lớn nhất nhỏ hơn $n,$ thì $p_k\ge 5.$ Do đó $k>2$ và $p_1+p_2+\ldots+p_k=n\le p_{k+1}.$ Do $k>2,$ từ Hệ quả 2 Định lý 9 suy ra $p_{k+1}<p_{k-1}+p_k$ nên $p_1+p_2+\ldots+p_n<p_{k-1}+p_n,$ vô lý. Vậy chỉ có 5 thỏa mãn.

2. Chứng minh rằng nếu $n>1$ và k là số tự nhiên thì $\frac{1}{n}+\frac{1}{n+1}+\ldots+\frac{1}{n+k}$ không phải số nguyên.

Chứng minh. Nếu biểu thức ở trên là nguyên thì ta có $\frac{1}{n}+\frac{1}{n+1}+\ldots+\frac{1}{n+k}\ge 1,$ mà ta lại có ước lượng $\frac{1}{n}+\frac{1}{n+1}+\ldots+\frac{1}{n+k}<\frac{k+1}{n},$ do đó $k+1>n,$ suy ra $k\ge n.$ Ký hiệu p là số nguyên tố lớn nhất $\le n+k.$ Ta có $2p>n+k;$ và theo Hệ quả 1 Định lý 8 thì giữa p và $2p$ có số nguyên tố $q,$ và do $2p\le n+k,$ ta có $p<q<n+k,$ mâu thuẫn với định nghĩa của $p.$ Vì $k\ge n,$ suy ra $n+k\ge 2n,$ và theo Hệ quả 1 thì tồn tại số nguyên tố r nằm giữa n và $2n.$ Vì vậy $r<2n\le n+k$ và từ định nghĩa của p suy ra $r\le p.$ Nhưng vì $n<r,$ ta có $n<p\le n+k<2p.$ Suy ra trong số các tổng con của tổng

$\frac{1}{n}+\frac{1}{n+1}+...+\frac{1}{n+k}$ có đúng một tổng mà mẫu số chia hết cho số nguyên tố p. Từ đây suy ra tổng này không phải số nguyên. Thật vậy, quy đồng các phân số với mẫu số chung là $n(n+1)...(n+k)$, ta thấy tất cả các tử số trừ ra một số là đều chia hết cho p, vậy tất cả các tổng riêng của chuỗi điều hòa $\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+...$ đều không phải số nguyên. □

3. Chứng minh Hệ quả 1 Định lý 8 là tương đương với mệnh đề ***T***: *mọi dãy hữu hạn các số tự nhiên liên tiếp chứa ít nhất một số nguyên tố thì cũng chứa ít nhất một số nguyên tố cùng nhau với tất cả các số còn lại trong dãy (xem thêm Zahlen* [1]).

Chứng minh. Giả sử $k,k+1,...,l$ ***(i)*** là dãy các số tự nhiên liên tiếp và p là số nguyên tố lớn nhất chứa trong dãy. Nếu $2p \le l$, thì theo Hệ quả 1 Định lý 8 tồn tại số nguyên tố q thỏa mãn $p<q<2p\le 1$, mâu thuẫn với định nghĩa p là số nguyên tố lớn nhất trong dãy ***(i)***. Vậy ta có $l<2p$. Do đó có thể thấy p nguyên tố cùng nhau với $1,2,...,l$ và suy ra nó nguyên tố cùng nhau với mọi phần tử của dãy ***(i)***. Vậy Hệ quả 1 Định lý 8 suy ra ***T***. Bây giờ giả sử ***T*** đúng. Ký hiệu $n>1$ là số tự nhiên. Xét dãy ***(ii)*** các số tự nhiên liên tiếp $2,3,...,2n$, dãy này chứa số nguyên tố 2 nên theo ***T*** thì tồn tại ít nhất một số p nguyên tố cùng nhau với các số còn lại trong dãy. Ta lưu ý p phải là số nguyên tố. Thật vậy nếu $p=ab$, với a và b là các số tự nhiên >1, thì số $a<p$ thuộc dãy ***(ii)*** và không nguyên tố cùng nhau với p. Hơn nữa nếu $p\le n$, thì $2p\le 2n$ và số $2p\ne p$ thuộc ***(ii)*** và $2p$ không nguyên tố cùng nhau với p. Vì vậy ta có $p>n$. Nhưng vì p thuộc dãy ***(ii)*** và $p\le 2n$. Hơn nữa $p\ne 2n$ vì $n>1$ và p nguyên tố. Từ đây suy ra $n<p<2n$. Ta đã chứng minh ***T*** suy ra Hệ quả 1 Định lý 8. Vậy hai mệnh đề này tương đương và ta có điều phải chứng minh. □

4. Sử dụng Hệ quả 1 Định lý 8 chứng minh rằng với mọi số tự nhiên k và $n\ge 2^k$ thì k số nhỏ nhất >1 không chia hết cho số nào trong các số $2,3,...,n$ đều là số nguyên tố.

Chứng minh. Nếu $n\ge 2^k$, thì $n^2\ge 2^k n$ và theo Hệ quả 1 Định lý 8 thì giữa hai phần tử liên tiếp của dãy $n,2n,2^3n,...,2^k n$ đều có ít nhất một số nguyên tố, giữa n và n^2 có ít nhất k số nguyên tố khác nhau. Vậy giữa n và n^2 cũng tồn tại ít nhất k số không chia hết cho bất kỳ số nào trong các số $2,3,...,n$. Mỗi số như vậy đều là số nguyên tố vì nếu l là một số như thế và $l=ab$, với a,b là các số tự nhiên >1, $a\le b$, thì ta có $a\le n$ (do l không chia hết cho bất kỳ số nào trong các số $2,3,...,n.$). Vậy ta phải có $b\ge a\ge n$, suy ra $l=ab\ge n^2$, vô lý. □

11. Định lý H.F.Scherk

Định lý 10 (H.F.Scherk). *Với mọi số tự nhiên* n *và các dấu* $+$ *và* $-$ *thích hợp ta có*

(11) $$p_{2n}=1\pm p_1\pm p_2\pm...\pm p_{2n-2}\pm p_{2n-1}$$

(12) $$p_{2n+1}=1\pm p_1\pm p_2\pm...\pm p_{2n-1}+2p_{2n}.$$

Các công thức này được tìm ra bởi H.F.Sherk [1] vào năm 1830, chứng minh của H.F.Scherk được công bố bởi S.S.Pillai [1] năm 1928. Chứng minh dưới đây được tác giả công bố năm 1952 (Sierpinski [14]). Chứng minh tương tự được trình bày bởi R.Teuffel [1] năm 1955.

Chứng minh. Ta nói dãy vô hạn $q_1,q_2...$ là có tính chất **P** nếu nó là dãy tăng các số tự nhiên, tất cả đều là số lẻ trừ ra số đầu tiên thỏa mãn

(13) $$q_1=2,q_2=3,q_3=5,q_4=7,q_5=11,q_6=13,q_7=17$$

(14) $$q_{n+1}<2q_n \quad \textit{với} \quad n=1,2,...$$

Theo Hệ quả 1 Định lý 9 thì dãy $q_n = p_n$ (với $n = 1,2,\ldots$) có tính chất **P**. Do đó để chứng minh định lý Scherk ta chỉ cần chứng minh với lựa chọn các dấu thích hợp thì các công thức ***(11),(12)*** đúng với mọi dãy có tính chất **P.**

Bổ đề. *Nếu* $q_1, q_2, \ldots$ *là dãy vô hạn có tính chất* ***P****, thì với* $n \geq 3$ *mọi số tự nhiên lẻ* $\leq q_{2n+1}$*, có dạng* $\pm q_1 \pm q_2 \pm \ldots \pm q_{2n-1} + q_{2n}$ *với các dấu* $+$ *và* $-$ *thích hợp.*

Chứng minh bổ đề. Từ ***(13)*** suy ra bổ đề đúng với $n = 3,$ vì

$$1 = -q_1 + q_2 + q_3 - q_4 - q_5 + q_6, \qquad 11 = q_1 - q_2 - q_3 - q_4 + q_5 + q_6,$$
$$3 = q_1 - q_2 - q_3 + q_4 - q_5 + q_6, \qquad 13 = q_1 - q_2 + q_3 + q_4 - q_5 + q_6,$$
$$5 = q_1 + q_2 + q_3 - q_4 - q_5 + q_6, \qquad 15 = -q_1 + q_2 + q_3 + q_4 - q_5 + q_6,$$
$$7 = -q_1 - q_2 - q_3 - q_4 + q_5 + q_6, \qquad 17 = q_1 + q_2 - q_3 - q_4 + q_5 + q_6,$$
$$9 = q_1 + q_2 - q_3 + q_4 - q_5 + q_6,$$

Ta lưu ý với $n = 2$ thì bổ đề không đúng vì không thể có $5 = \pm 2 \pm 3 \pm 5 + 7$.

Giả sử bổ đề đúng với số tự nhiên $n \geq 3$ và đặt $2k-1$ là số lẻ $\leq q_{2n+3}$.

Từ ***(14)*** ta có $q_{2n+3} < 2q_{2n+2}$ và hệ quả là $-q_{2n+2} < 2k-1-q_{2n+2} < q_{2n+2}$. Do đó chọn các dấu $+$ và $-$ thích hợp ta có $0 \leq \pm\left(2k-1-q_{2n+2}\right) < q_{2n+2}$. Theo ***(14)*** ta có $q_{2n+2} < 2q_{2n+1}$ và do đó $-q_{2n+1} \leq \pm\left(2k-1-q_{2n+2}\right) - q_{2n+1} < q_{2n+1}$. Hơn nữa chọn các dấu $+$ và $-$ thích hợp ta có

(15) $$0 \leq \pm\left\{\pm\left(2k-1-q_{2n+2}\right) - q_{2n+1}\right\} \leq q_{2n+1}.$$

Các số q_{2n+1} và q_{2n+2} đều lẻ và do đó số ở giữa bất đẳng thức ***(15)*** cũng là lẻ và $\leq q_{2n+1}$. Hệ quả là theo giả thiết quy nạp ta suy ra với lựa chọn các dấu $+$ và $-$ thích hợp ta có $2k-1 = \pm q_1 \pm q_2 \pm \ldots \pm q_{2n} \pm q_{2n+1} + q_{2n}$. Vì vậy lựa chọn các dấu $+$ và $-$ thích hợp ta có $2k-1 = \pm q_1 \pm q_2 \pm \ldots \pm q_{2n} \pm q_{2n+1} \pm q_{2n+2}$, suy ra bổ đề đúng với $n+1$ và theo quy nạp ta có điều phải chứng minh với $n \geq 3$. □

Hệ quả. *Lựa chọn các dấu* $+$ *và* $-$ *thích hợp ta có*

(16) $$q_{2n+1} = \pm q_1 \pm q_2 \pm \ldots \pm q_{2n-1} + q_{2n}.$$

Chứng minh. Vì q_{2n+1} là số lẻ nên với $n \geq 3$ công thức ***(16)*** được suy ra trực tiếp từ bổ đề. Với $n = 1$ và $n = 2$ thì tính toán trực tiếp cho thấy $q_3 = q_1 + q_2$ và $q_5 = q_1 - q_2 + q_3 + q_4$. □

Bây giờ ta chứng minh các công thức ***(11),(12).***

Chứng minh (12). Theo ***(14)*** thì với $n \geq 3$ số $q_{2n+1} - q_{2n} - 1$ là số lẻ $< q_{2n+1}$. Do đó áp dụng bổ đề, ta thấy với lựa chọn các dấu + và – thích hợp ta có $q_{2n+1} - q_{2n} - 1 = \pm q_1 \pm q_2 \pm \ldots \pm q_{2n-1} + q_{2n}$ và từ đây suy ra (với $q_i = p_i, i = 1,2,\ldots$) công thức ***(12)*** đúng. Với $n = 1$ và $n = 2$ tính toán trực tiếp ta có $q_3 = 1 - q_1 + 2q_2, q_5 = 1 - q_1 + q_2 - q_3 + 2q_4$. □

Chứng minh (11). Theo ***(14)*** ta có $q_{2n+2} < 2q_{2n+1}$ và ta thấy $q_{2n+2} - q_{2n+1} - 1$ là số lẻ > 0 và $< q_{2n+1}$. Áp dụng bổ đề ta thấy với $n \geq 3$ và lựa chọn các dấu + và - thích hợp thì

$$q_{2n+2} - q_{2n+1} - 1 = \pm q_1 \pm q_2 \pm \ldots \pm q_{2n-1} + q_{2n},$$

(17) $$q_{2n+2} = 1 \pm q_1 \pm q_2 \pm \ldots \pm q_{2n-1} + q_{2n} + q_{2n+1}.$$

Hơn nữa theo ***(13)*** ta thấy

$$q_2 = 1 + q_1, q_4 = 1 - q_1 + q_2 + q_3,$$
$$q_6 = 1 + q_1 - q_2 - q_3 + q_4 + q_5,$$

Suy ra ***(17)*** đúng với $n = 0,1$ và 2. Hệ quả là ***(17)*** đúng với $n = 0,1,2,\ldots$ do đó ($q_i = p_i, i = 1,2,\ldots$) công thức ***(11)*** đúng với $n = 1,2,3,\ldots$ Định lý Scherk được chứng minh. □

12. Định lý H.E.Richert

Bổ đề 1. *Nếu $m_1, m_2, \ldots$ là dãy vô hạn tăng các số tự nhiên thỏa mãn với số tự nhiên k nào đó bất đẳng thức*

(18) $$m_{i+1} \le 2m_i \text{ for } i > k$$

đúng, và nếu số tự nhiên $a \ge 0$ và số tự nhiên r và $s_{r-1} \ge m_{k+r}$ thỏa mãn các số

(19) $$a+1, a+2, \ldots, a+s_{r-1}$$

đều là tổng của các số khác nhau trong dãy $m_1, m_2, \ldots, m_{k+r-1}$ thì với $s_r = s_{r-1} + m_{k+r}$ các số

(20) $$a+1, \quad a+2, \quad \ldots, \quad a+s_r$$

đều là tổng của các số khác nhau trong dãy $m_1, m_2, \ldots, m_{k+r}$ và hơn nữa $s_r \ge m_{k+r+1}$.

Chứng minh. Giả sử các điều kiện trong giả thiết của bổ đề được thỏa mãn. Ký hiệu n là số tự nhiên thuộc dãy ***(20)***. Nếu $n \le a + s_{r-1}$, thì theo giả thiết n là tổng của các phần tử khác nhau của dãy $m_1, m_2, \ldots, m_{k+r-1}$. Bây giờ giả sử $n > a + s_{r-1}$ thì từ $s_{r-1} \ge m_{k+r}$ ta có $n \ge a + 1 + m_{k+r}$ do đó $n - m_{k+r} \ge a + 1$. Hơn nữa vì n là phần tử của dãy ***(20)*** nên ta có $n \le a + s_r = a + s_{r-1} + m_{k+r}$. Do đó $n - m_{k+r} \le a + s_{r-1}$. Vì vậy số $n - m_{k+r}$, là phần tử của dãy ***(19)*** và do đó nó là tổng của các phần tử khác nhau của dãy $m_1, m_2, \ldots, m_{k+r-1}$. Vậy n là tổng của các phần tử khác nhau của dãy $m_1, m_2, \ldots, m_{k+r}$. Hơn nữa theo ***(18)*** ta có $m_{k+r+1} \le 2m_{k+r}$, do đó $s_r = s_{r-1} + m_{k+r} \ge 2m_{k+r} \ge m_{k+r+1}$. □

Bổ đề 2. *Nếu $m_1, m_2, \ldots$ là dãy vô hạn các số tự nhiên thỏa mãn **(18)** đúng với số tự nhiên k và nếu tồn tại số nguyên $a \ge 0$ và số tự nhiên $s_0 \ge m_{k+1}$ thỏa mãn các số*

(21) $$a+1, a+2, \ldots, a+s_0$$

đều là tổng các phần tử khác nhau của dãy $m_1, m_2, \ldots m_k$ thì mọi số tự nhiên $> a$ cũng là tổng các phần tử khác nhau của dãy $m_1, m_2, \ldots$

Chứng minh. Giả sử điều kiện của bổ đề được thỏa mãn. Lần lượt áp dụng Bổ đề 1 với $r = 1,2,..,l$ trong đó l là số tự nhiên, ta suy ra các số

(22) $$a+1, a+2, \ldots, a+s_l$$

đều là tổng các phần tử khác nhau của dãy $m_1, m_2, \ldots m_{k+1}$. Nhưng $s_r > s_{r-1}, r = 1,2,\ldots,l,$ nên ta thấy với mọi số tự nhiên n thì đều tồn tại số tự nhiên l thỏa mãn $n \le a + s_l$. Hệ quả là mọi số tự nhiên $n > a$ đều là một trong các số của dãy ***(22)*** với l thích hợp. Các số này đều là tổng các phần tử khác nhau của dãy $m_1, m_2, \ldots$ Bổ đề được chứng minh. □

Bây giờ đặt $m_i = p_i$ với $i = 1,2,\ldots$ Theo Hệ quả 1 Định lý 9 thì các điều kiện trong Bổ đề 2 được thỏa mãn với $a = 6, s_0 = 13, k = 5;$ bởi vì $13 = p_6$ và các số 7,8,...19 đều là tổng của các số nguyên tố phân biệt $\le p_5$. Thật vậy

$$7 = 2+5, 8 = 3+5, 9 = 2+7, 10 = 3+7, 11 = 11,$$

$$12=5+7,13=2+11,14=3+11,\ 15=2+5+7,$$
$$16=5+11,17=2+3+5+7,18=7+11,19=3+5+11.$$

Rõ ràng ta có thể loại ra các tổng chỉ có một hạng tử: số 11 không phải tổng của hai hay nhiều hợn các số nguyên tố. Từ Bổ đề 2 ta có hệ quả

Định lý 11. *Mọi số tự nhiên* >6 *đều là tổng của các số nguyên tố khác nhau* (Richert [1],[2]).

Giả sử $m_i = p_{i+1}$. Các điều kiện của Bổ đề 2 được thỏa mãn với $a=9, s_0=19, k=6,$ từ $19=p_8=m,$ nên $s_0=m_{6+1}$ và hơn nữa mỗi số $10,11,...28$ đều là tổng của các số nguyên tố lẻ $\le m_6=19.$ Thật vậy

$$10=3+7,11=11.12=5+7,13=13,14=3+11,\ 15=3+5+7,$$
$$16=5+11,17=17,18=5+13,19=3+5+11,\ 20=7+13,21=3+5+13,22=5+17,$$
$$23=3+7+13,24=11+13,25=5+7+13,26=3+5+7+11,28=3+5+7+13.$$

Định lý 12. *Mọi số tự nhiên* ≥ 10 *đều là tổng của các số nguyên tố lẻ khác nhau.*

Nếu ta bổ sung số 2 như là một hạng tử thì ta có

Định lý 13. *Mọi số tự nhiên* ≥ 12 *đều là tổng của hai hoặc nhiều hơn các số nguyên tố khác nhau.*

Dễ dàng thấy 11 không phải tổng của hai hay nhiều hơn các số nguyên tố khác nhau. Số 17 không phải tổng của hai hoặc ba số nguyên tố khác nhau (nhưng $17=2+3+5+7$). Ta có thể chứng minh một cách sơ cấp rằng tồn tại vô hạn số lẻ không là tổng của ít hơn ba số nguyên tố.

Sau đây là bốn định lý được trình bày bởi R. Dressier, A.Makowski và T.Parker [1]: *Mọi số tự nhiên >1969 đều là tổng của các số nguyên tố khác nhau có dạng* $12k+1.$ *Mọi số tự nhiên >1349 đều là tổng của các số nguyên tố khác nhau có dạng* $12k+5.$ *Mọi số tự nhiên >1387 đều là tổng của các số nguyên tố khác nhau có dạng* $12k+7.$ *Mọi số tự nhiên >1475 đều là tổng của các số nguyên tố khác nhau có dạng* $12k+11.$ Các chặn dưới là không thể thay bằng các số nhỏ hơn.

Một số kết quả có liên quan có thể xem trong J.L.Brown Jr, [2].

13. Giả thuyết về các số nguyên tố

Vài năm trước tôi (Sierpinski) có đặt ra giả thuyết P sau đây

Giả thuyết P. *Nếu các số* $1,2,3,...,n^2$ *với* $n>1$ *được xếp thành* n *dòng, mỗi dòng chứa* n *số*

(23)
$$\begin{array}{llllll} 1, & 2, & 3, & ..., & n \\ n+1, & n+2, & n+3, & ..., & 2n \\ 2n+1, & 2n+2, & 2n+3, & ..., & 3n \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (n-1)n+1, & (n-1)n+2, & & ..., & n^2 \end{array}$$

thì mỗi một dòng chứa ít nhất một số nguyên tố (Schinzel et Sierpinski [3]).

Dòng thứ nhất của bảng ***(23)*** chứa số 2 $(n>1)$. Mệnh đề nói rằng dòng thứ hai chứa số nguyên tố với $n>1$ là hệ quả 1 của Định lý 8. Từ các bất đẳng thức của J.B.Rosser và L.Schoenfeld (mục 15) thì với $n>e^k$ thì k dòng đầu tiên chứa số nguyên tố. Sử dụng các bảng của Lander và Parkin [3] và [1],[4] có thể kiểm tra giả thuyết P đúng với $1<n\le 21\cdot 10^5.$ Do hai dòng cuối của bảng đều chứa các số $(n-1)^2, (n-1)^2+1,...,n^2,$ nên giả thuyết P suy ra rằng giữa hai bình phương liên tiếp các số tự nhiên có ít nhất hai số nguyên tố. Hơn nữa trong mọi khoảng mà điểm kết thúc là lập phương của hai số tự nhiên liên tiếp đều có hai bình phương của hai số tự nhiên liên tiếp. Mệnh đề cuối cùng chưa được chứng minh nhưng theo kết quả của A.E.Ingham vào năm 1937 thì số các số nguyên tố nằm giữa n^3 và $(n+1)^3$ tiến tới vô cùng theo n.

Hệ quả trực tiếp của giả thuyết P là giữa hai số tam giác có ít nhất một số nguyên tố. Nghĩa là nếu ta xếp các số tự nhiên thành tam giác vuông mà dòng thứ n chứa n số tự nhiên liên tiếp. tức là

1
2, 3
4, 5, 6
7, 8, 9, 10
11, 12, 13, 14, 15
. . . . . .

thì trừ ra dòng đầu tiên các dòng còn lại đều chứa số nguyên tố. Giả thuyết này chưa có câu trả lời.

Năm 1932 R.Haussner [1] đặt ra giả thuyết rằng với mọi số tự nhiên k, *thì giữa hai bội số liên tiếp của số nguyên tố* p_k *đều nhỏ hơn* p_{k+1}^2 *tồn tại ít nhất một số nguyên tố.* Giả thuyết này được kiểm chứng bởi Haussner với các số nguyên tố $p_k < 100$. Giả thuyết P cho số nguyên tố n là hệ quả trực tiếp của giả thuyết của Haussner.

L.Skula đã lưu ý rằng từ giả thuyết P suy ra với mọi số tự nhiên $n > 1$ thì các hàng thứ $n+1$ và hàng $n+2$ đều chứa ít nhất một số nguyên tố. Từ giả thuyết **P** với $n+1$ thì giữa các số $n^2-1, n^2, ..., n(n+1)$ có ít nhất một số nguyên tố và với $n > 2$ thì hai phần tử đầu tiên của dãy đều là hợp số và có ít nhất một số nguyên tố nằm trong các số $n^2-1, n^2, ..., n(n+1)$. Điều này cũng đúng với $n = 2$. Từ giả thuyết **P** với $n+1$ thì giữa các số $n^2+n+1, n^2+n+2, ..., (n+1)^2$ có ít nhất một số nguyên tố, vì vậy có ít nhất một số nguyên tố nằm giữa $n^2+n-1, n^2+n, ..., n^2+2n$ vì $(n+1)^2$ là hợp số. A.Schinzel đã đặt ra giả thuyết rằng nếu n *là số tự nhiên* > 1 *và* k *là số tự nhiên nhỏ hơn* n *và nguyên tố cùng nhau với* n, *thì trong cột thứ* k *của bảng* ***(23)*** *có ít nhất một số nguyên tố* (Schinzel và Sierpinski [3]). Nói cách khác nếu k và n là các số tự nhiên nguyên tố cùng nhau và $k < n$, thì trong các số $k, k+n, k+2n, ..., k+(n-1)n$ luôn có ít nhất một số nguyên tố. Theo bảng của Wagstaff [2] thì điều này đúng tới $n \le 500000$.

Năm 1947 Yu.V.Linnik đã chứng minh sự tồn tại của hằng số C thỏa mãn nếu $(k, n) = 1$ và $1 \le k < n$ thì số nguyên tố nhỏ nhất trong cấp số cộng $k, k+n, k+2n, ...$ nhỏ hơn n^C. J.R.Chen [13] đã chứng minh rằng bằng việc thay thế n^C bởi An^C với giá trị A thích hợp ta có thể chọn $C = 17$. (S.Graham [1]). Gần đây Chen đưa ra kết quả mới với $C = 14$.

A.Schinzel [13] đã đặt ra một giả thuyết mạnh hơn giả thuyết **P.** Theo đó nếu x là số thực ≥ 117 thì giữa x và $x+\sqrt{x}$ có ít nhất một số nguyên tố. Giả thuyết này (ký hiệu là $\mathbf{P_1}$) được kiểm tra bởi các bảng của Lander và Parkin và bảng của Brent với $117 \le x \le 4,44 \cdot 10^{12}$. Legendre là người đặt ra giả thuyết nói rằng với x đủ lớn thì có ít nhất một số nguyên tố nằm giữa x và $x+\sqrt{x}$.

Bây giờ ta chứng minh giả thuyết **P** với $n \ge 117$ được suy ra từ giả thuyết $\mathbf{P_1}$. Ký hiệu n là số nguyên ≥ 117 và k là số tự nhiên nhỏ hơn n. Ta có $kn \ge 117$ và do đó theo giả thuyết $\mathbf{P_1}$ tồn tại số nguyên tố p mà $kn < p < kn + \sqrt{kn}$. Nhưng vì $k < n$, ta có $\sqrt{kn} < n$; do đó tồn tại ít nhất một số nguyên tố trong dãy $kn+1, kn+2, ..., (k+1)n$. Do điều này đúng với mọi số tự nhiên $k < n$, ta thấy với $n \ge 117$ thì mỗi hàng của bảng ***(23)*** từ dòng thứ hai có ít nhất một số nguyên tố. Vậy giả thuyết **P** với $n \ge 117$ được suy ra từ giả thuyết $\mathbf{P_1}$. Với $n < 117$ giả thuyết **P** được kiểm tra trực tiếp.

A.Schinzel [13] nhận thấy có thể làm mạnh hơn giả thuyết $\mathbf{P_1}$ thành: với mỗi số thực $x \ge 8$ thì giữa x và $x+(\log x)^2$ có ít nhất một số nguyên tố. Sử dụng các bảng của Lander, Parkin và bảng của Brent có thể kiểm tra giả thuyết này với mọi $x < 4,44 \cdot 10^{12}$. Nếu ta đặt $x = p_n$ với $n > 4$ thì ta có bất đẳng thức $p_{n+1} - p_n < (\log p_n)^2$ với mọi $n > 4$. H.Cramer [1] đã đặt ra giả thuyết $\lim (p_{n+1} - p_n) / (\log p_n)^2 = 1$.

Dưới đây là một giả thuyết khác về hiệu của hai số nguyên tố liên tiếp được đưa ra bởi N.L.Gilbreath vào năm 1958. Ta lập bảng các số tự nhiên theo cách sau: dòng thứ nhất viết hiệu các số nguyên tố liên tiếp, nghĩa là các số $p_{n+1}-p_n, n=1,2,\ldots$, dòng thứ hai ta viết giá trị tuyệt đối của hiệu của các số liền nhau trong dòng thứ nhất. Trong các dòng tiếp theo ta lại viết tiếp như vậy. Giả thuyết của Gilbreath nói rằng các số đầu tiên của mỗi dòng đều là 1. Dưới đây là 10 dòng đầu tiên

1, 2, 2, 4, 2, 4, 2, 4, 6, 2
1, 0, 2, 2, 2, 2, 2, 2, 4
1, 2, 0, 0, 0, 0, 0, 2
1, 2, 0, 0, 0, 0, 2
1, 2, 0, 0, 0, 2
1, 2, 0, 0, 2
1, 2, 0, 2
1, 2, 2
1, 0
1

Giả thuyết của Gilbreath được kiểm tra cho 63418 dòng đầu tiên với máy tính SWAC. Giả thuyết này vẫn chưa được chứng minh (Killgrove và Ralston [1]).

14. Bất đẳng thức của hàm $\pi(x)$

Bây giờ ta xét các hệ quả của Bổ đề 9 mục 10. Do R_n ký hiệu tích của các số nguyên tố p mà $n<p<2n$ và số các số nguyên tố như vậy là $\pi(2n)-\pi(n)$ (và theo Hệ quả 1 Định lý 8 mục 10 thì với mọi số tự nhiên n tồn tại ít nhất một số nguyên tố p như thế). Hơn nữa các số nguyên tố đó đều nhỏ hơn $2n$, suy ra $R_n \le (2n)^{\pi(2n)-\pi(n)}$.

Từ công thức ***(10)*** mục 10 suy ra với các số tự nhiên $n \ge 98$ ta có $(2n)^{\pi(2n)-\pi(n)} > \dfrac{4^{n/3}}{2\sqrt{n}(2n)^{\sqrt{n/2}}}$

Lấy logarithm hai vế ta suy ra với $n \ge 98$ thì

(24) $$\pi(2n)-\pi(n) > \frac{n}{3\log 2n}\left(\log 4 - \frac{3\log 4n}{2n} - \frac{3\log 2n}{\sqrt{2n}}\right)$$

Nhưng ta đã biết $\lim\limits_{x\to x}\dfrac{\log x}{x}=0;$ do đó $\lim\limits_{n\to x}\left(\pi(2n)-\pi(n)\right)=+\infty$. Từ đây suy ra với mọi số tự nhiên k thì đều tồn tại số tự nhiên m_k mà với mọi $n \ge m_k$ thì đều tồn tại ít nhất k số nguyên tố nằm giữa n và $2n$. Hơn nữa vì $\log x/x$ (với $x > e.$) là hàm giảm theo x, ta có với $n \ge 2500$

$$\frac{3\log 4n}{2n}+\frac{3\log 2n}{\sqrt{2n}} = 6\left(\frac{\log 4n}{4n}+\frac{\log\sqrt{2n}}{\sqrt{2n}}\right)$$
$$\le 6\left(\frac{\log 4\cdot 2500}{4\cdot 2500}+\frac{\log\sqrt{2\cdot 2500}}{\sqrt{2\cdot 2500}}\right) < 0,37;$$

Vì vậy

(25) $$\log 4 - \frac{3\log 4n}{2n} - \frac{3\log 2n}{\sqrt{2n}} > 1,38-0,37 > 1.$$

Theo ***(24)*** thì công thức ***(25)*** cho thấy bất đẳng thức Finsler

(26) $$\pi(2n)-\pi(n) > \frac{n}{3\log 2n}.$$

đúng với mọi số tự nhiên $n>1$. Bây giờ ta chú ý rằng với mọi số tự nhiên n thì ta có $\binom{2n}{n}<4^n$ (áp dụng trực tiếp công thức nhị thức suy ra $(1+1)^{2n}>\binom{2n}{n}$). Do $R_n \mid \binom{2n}{n}$ nên ta thấy $R_n<4^n$ và từ định nghĩa của R_n có thể suy ra $R_n \ge n^{\pi(2n)-\pi(n)}$. Từ đó $n^{\pi(2n)-\pi(n)}<4^n$ và do đó $\pi(2n)-\pi(n)<\dfrac{\pi\log 4}{\log n}<\dfrac{7n}{5\log n}$ vì $\log 4<\dfrac{7}{5}$. Sử dụng ***(26)*** ta có (Finsler [1] và Trost [3], Satz 32)

(27) $$\frac{n}{3\log 2n}<\pi(2n)-\pi(n)<\frac{7n}{5\log n} \text{ với mọi } n>1$$

Từ ***(27)*** suy ra $\pi(2n)>\dfrac{n}{3\log 2n}$ với $n>1$ và với $n\ge 4$ ta có $n>n/2\ge[n/2]\ge n/2-1>n/4$ và do $\log\left(2\left[n/2\right]\right)\le\log n$, ta có $\pi(n)\ge\left(2\left[\dfrac{n}{2}\right]\right)>\dfrac{[n/2]}{3\log 2[n/2]}>\dfrac{n}{12\log n}$ với mọi $n\ge 4$,

(28) $$\pi(n)>\frac{n}{12\log n} \text{ với mọi } n>1$$

Dễ dàng kiểm tra bất đẳng thức đúng với n = 2 và n = 3. Ta sẽ chứng minh

(29) $$\pi(2^k)<\frac{2^{k+1}}{k\log 2}$$

Có thể thấy công thức ***(29)*** đúng với các số tự nhiên $k\le 6$ vì $\log 2<1$. Giả sử nó đúng với số tự nhiên $k\ge 6$. Theo ***(27)*** (với 2^k thay thế vị trí của n) và ***(29)*** ta có $\pi\left(2^{k+1}\right)<\pi\left(2^k\right)+\dfrac{7\cdot 2^k}{5k\log 2}<\dfrac{2^{k+1}}{k\log 2}\left(1+\dfrac{7}{10}\right)$. Nhưng với $k\ge 6$ ta có $(k+1)\left(1+\dfrac{7}{10}\right)<2k$, $\pi\left(2^{k+1}\right)<\dfrac{2^{k+2}}{(k+1)\log 2}$ và theo quy nạp bất đẳng thức (29) đúng.

Ký hiệu n là số tự nhiên >1. Tồn tại số tự nhiên k thỏa mãn $2^k\le n<2^{k+1}$, suy ra $(k+1)\log 2>\log n$. Vì vậy theo ***(29)*** ta có $\pi(n)\le\pi\left(2^{k+1}\right)<\dfrac{2^{k+1}}{(k+1)\log 2}<\dfrac{4n}{\log n}$. Từ đây ta suy ra

(30) $$\pi(n)<\frac{4n}{\log n} \text{ với mọi số tự nhiên } n>1$$

Thay n bởi p_n trong ***(28)*** và ***(30)*** và do $\pi(p_n)=n$ ta có $\dfrac{p_n}{12\log p_n}<n<\dfrac{4p_n}{\log p_n}$; suy ra vì $p_n>n$ (với $n=1,2,\ldots$).

Ta có $p_n>\dfrac{n}{4}\log p_n>\dfrac{n\log n}{4}$ và $p_n<12n\log p_n$. suy ra $\log p_n<\log 12+\log n+\log\log p_n$.

Nhưng theo Hệ quả 2 Định lý 8 mục 10 ta thấy $p_n<2^n$, suy ra $\log p_n<n\log 2$ và $\log\log p_n<\log n+\log\log 2$. Do $\log 2<1$, với $n\ge 12$ và ta có $n>12\log 2$ do đó $\log n>\log 12+\log\log 2$. Vì vậy với $n\ge 12$, ta có $\log p_n<2\log n+\log 12+\log\log 2<3\log n$. Hệ quả là $p_n<36n\log n$ với mọi $n\ge 12$ và cũng vậy với $2\le n<12$. Ta có kết luận

(31) $$\frac{n\log n}{4} < p_n < 36n\log n \text{ với mọi } n>1.$$

Từ công thức ***(28)*** ta có hệ quả sau: *với mọi số tự nhiên s thì đều tồn tại số tự nhiên có thể biểu diễn như là tổng của hai số nguyên tố theo nhiều hơn s cách.*

Chứng minh. Giả sử rằng với số tự nhiên s mà không tồn tại số tự nhiên nào có thể biểu diễn dưới dạng tổng của hai số nguyên tố nhiều hơn s cách. Ký hiệu n là số tự nhiên >1. Xét tất cả các cặp (p,q) với p,q là các số nguyên tố mà không có số nào lớn hơn n. Số các cặp như vậy là $\left[\pi(n)\right]^2$. Ta chia tập các cặp số (p,q) thành các lớp theo cách (p,q) thuộc lớp k nếu $p+q=k$. Do $p\le n$ và $q\le n$ nên ta có $k\le 2n$. Theo giả thiết với số cho trước $k\le 2n$ thì trong lớp thứ k tồn tại nhiều nhất s cặp khác nhau. Do số các lớp là nhỏ hơn $2n$, số các cặp (p,q) là nhỏ hơn $2ns$. Hệ quả là $\left[\pi(n)\right]^2 < 2ns$ và theo công thức ***(28)*** ta có $\left[\pi(n)\right]^2 > n^2/12^2(\log n)^2$, suy ra $2\cdot 12^2 s(\log n)^2 > n$.

Nhưng $e^x > x^3/3!$ với mọi $x\ge 0$, thay $x=\log n$, ta có $6n > (\log n)^3$. Vì vậy $12^3 s(\log n)^2 > (\log n)^3$ với $n>1$ suy ra $\log n < 12^3 s$ với mọi $n>1$, mà với n đủ lớn thì điều này không đúng. Hệ quả là từ giả thiết ban đầu suy ra mâu thuẫn. Vậy hệ quả được chứng minh. Có một giả thuyết được đặt ra là số các cách phân tích một số chẵn n thành tổng của hai số nguyên tố sẽ tiến tới vô cùng theo n. □

Ghi chú. Các số có thể biểu diễn thành tổng của hai số nguyên tố nhiều hơn một cách phải là chẵn với lưu ý là ta không tính các biểu diễn sai khác một hoán vị. Thật vậy nếu số lẻ n là tổng của hai số nguyên tố thì một trong hai số đó phải chẵn nghĩa là bằng 2 suy ra ta chỉ có nhiều nhất một biểu diễn. Thay đổi một chút chứng minh Bổ đề 1 ta có thể chứng minh với mọi số tự nhiên s thì đều tồn tại số tự nhiên có thể biểu diễn thành tổng của ba bình phương các số nguyên tố với nhiều hơn s cách. P.Erdos [4] đã chứng minh với mọi số tự nhiên s thì đều tồn tại số tự nhiên có thể biểu diễn thành tổng (tương ứng, hiệu) của các bình phương của hai số nguyên tố theo nhiều hơn s cách. Từ ***(30)*** suy ra $\lim\limits_{n\to\infty}\frac{\pi(n)}{n}=0$. Mà $\log n+\log\log n-\log 4<\log p_n<\log n+\log\log n+\log 36$ nên

(32) $$\lim_{n\to\infty}\frac{\log p_n}{n}=1$$

Bây giờ ta suy ra một số hệ quả từ bất đẳng thức ***(31)***. Theo ***(31)*** ta có $\frac{1}{p_k}>\frac{1}{36k\log k}$ với $k=2,3,\ldots,$ từ đây suy ra với số tự nhiên $n>2$ thì $\sum\limits_{k=2}^{n}\frac{1}{p_k}>\frac{1}{36}\sum\limits_{k=2}^{n}\frac{1}{k\log k}$.

Nhưng $\log(1+x)<x$ với $0<x<1$, suy ra với $k=2,3,\ldots,$ $\log(k+1)-\log k=\log\left(1+\frac{1}{k}\right)<\frac{1}{k}$, từ đó $\frac{\log(k+1)}{\log k}<1+\frac{1}{k\log k}$ và $\log\log(k+1)-\log\log k=\log\frac{\log(k+1)}{\log k}<\log\left(1+\frac{1}{k\log k}\right)<\frac{1}{k\log k}$. Vì vậy $\frac{1}{k\log k}>\log\log(k+1)-\log\log k$ với $k=2,3,\ldots,n$. Suy ra với số tự nhiên $n>2$ ta đều có $\sum\limits_{k=2}^{n}\frac{1}{k\log k}>\log\log(n+1)-\log\log 2>\log\log(n+1)$ ($\log\log 2<0$). Vậy $\sum\limits_{k=2}^{n}\frac{1}{p_k}>\frac{1}{36}\log\log(n+1)$.

Suy ra chuỗi tổng nghịch đảo các số nguyên tố liên tiếp, tức là chuỗi $\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\ldots,$ phân kỳ.

15. Định lý số nguyên tố và các hệ quả

Từ các công thức ***(28)*** và ***(30)*** mục 14 suy ra tồn tại các số dương ($a=\frac{1}{12}, b=4$) thỏa mãn $a<\pi(n):\frac{n}{\log n}<b$ với mọi số tự nhiên $n>1.$ Năm 1896 J.Hadamard và Poussin đã chứng minh

(33) $$\lim_{x\to\infty}\left(\pi(x):\frac{x}{\log x}\right)=1.$$

Ngày nay với phương pháp mới được đặt ra bởi A.Selberg [1] và P.Erdos [9], công thức này (được biết dưới tên Định lý số nguyên tố) được chứng minh một cách sơ cấp hơn (mặc dù vẫn rất phức tạp). Ta không trình bày chứng minh đó ở đây [(4)].

Nếu $\pi(n):\frac{n}{\log n}=h(n),$ thì $h(10^3)=1.159,$ $h(10^4)=1.132,$ $h(10^5)=1.104,$ $h(10^6)=1.084,$ $h(10^7)=1.071,$ $h(10^8)=1.061,$ $h(10^9)=1.053,$ $h(10^{10})=1.048.$ Xấp xỉ tốt hơn của hàm $\pi(x)$ được thu bởi hàm $\int_0^x\frac{dt}{\log t}$. J.E.Littlewood đã chứng minh hiệu $\pi(x)-\int_0^x\frac{dt}{\log t}$ nhận vô hạn giá trị dương và vô hạn giá trị âm khi x nhận tất cả các giá trị tự nhiên. Chứng minh định lý này và các định lý được đề cập trong chương này với phương pháp giải tích có thể xem trong cuốn sách của K.Prachar [1].

Trong công thức ***(33)*** đặt $x=p_n$ thì $\pi(p_n)=n$ và ta có $\lim_{n\to\infty}\frac{n\log p_n}{p_n}=1$ khi đó theo ***(32)***

(34) $$\lim_{n\to\infty}\frac{p_n}{n\log n}=1$$

Từ đây suy ra ta có thể xấp xỉ p_n bởi $n\log n,$ với n đủ lớn. Từ ***(34)*** suy ra ngay $\lim_{n\to\infty}\frac{p_{n+1}}{p_n}=1.$

J.B.Rosser [1] đã chứng minh rằng với mọi số tự nhiên n thì ta có bất đẳng thức $p_n>n\log n$. Các thông tin nhiều hơn về hàm $\pi(n)$ được suy ra từ ***(33)*** được cho bởi định lý J.B.Rosser và L.Schoenfield [1] nói rằng

(35) $$\frac{n}{\log n-\frac{1}{2}}<\pi(n)<\frac{n}{\log n-\frac{3}{2}}$$

với mọi số tự nhiên $n\geq 67.$ Rõ ràng công thức ***(33)*** suy ra từ ***(35)***. Nhưng ngay cả từ bất đẳng thức ***(35)*** ta cũng không quyết định được nhiều tính chất đơn giản của hàm $\pi(n).$ Một ví dụ là định lý của E.Landau (xem Landau [3] tập 1 trang 215-216) nói rằng $\pi(2n)<2\pi(n)$ đúng với giá trị đủ lớn của $n,$ nghĩa là có nhiều số nguyên tố trong khoảng $0<x\leq n$ hơn là trong khoảng $n<x\leq 2n,$ với n đủ lớn. Rosser và Schoenfeld [2] đã chỉ ra rằng chỉ cần giả thiết $n\geq 11.$ Một câu hỏi được đặt ra là với các số tự nhiên $x>1$ và $y>1$ nào thì bất đẳng thức sau đúng

(36) $$\pi(x+y)\leq\pi(x)+\pi(y)$$

Từ bất đẳng thức này suy ra ngay $\pi(2n)\leq 2\pi(n)$ đúng với mọi số tự nhiên $n.$

[(4)] Xem Trost [3], chương 7: *Elementarer Beweis des Primzahlsatces*, trang 66-73: xem LeVeque [1], tập 11 trang 229-263, chương 7: *The prime number theorem*.

Bất đẳng thức ***(36)*** được chứng minh bởi A.Schinzel [13] với $\min(x,y)\le 146,$ và bởi J.L.Selfridge với lớp rộng hơn (chưa công bố) và được kiểm tra bởi S.L.Segal [1] với $x+y\le 100000.$ Tuy nhiên D.Hensley và I.Richards [1] đã chứng minh rằng ***(36)*** là không tương thích với giả thuyết H. Sử dụng phương pháp này gần đây T.Vehka [1] đã chứng minh sự không tương tích xuất hiện với $\min(x,y)=11763.$

Tiếp tục với hàm $\pi(x)$ ta lưu ý rằng hàm số xác định số các số nguyên dương $\le x$ có đúng k ước số nguyên tố (tương ứng k ước số tự nhiên) với k và x là các số tự nhiên đã được nghiên cứu và công thức mô tả dáng điệu của nó đã được tìm ra (Sathe [1], tương ứng LeVeque [1]).

Bây giờ với hai số thực a và b thỏa mãn $0<a<b.$ Ta có $\lim_{x\to\infty}\frac{\log ax}{\log bx}=1,$ theo ***(33)*** ta có $\lim_{x\to\infty}\frac{\pi(bx)}{\pi(ax)}=\frac{b}{a}.$ Từ đó vì $0<a<b,\ \pi(bx)>\pi(ax),$ với n đủ lớn. Từ đây suy ra mệnh đề sau: *nếu a và b là hai số thực dương và $a<b,$ thì với số thực đủ lớn x sẽ có ít nhất một số nguyên tố nằm giữa ax và bx.* Đặc biệt nếu $a=1$ và $b=1+\varepsilon$ với ε là số thực dương tùy ý thì suy ra có ít nhất một số nguyên tố nằm giữa n và $n(1+\varepsilon)$ với n đủ lớn. Giả sử $c_1,c_2,\ldots,c_m$ là dãy hữu hạn các chữ số tùy ý. Ký hiệu a là một số với các chữ số là của nó $c_1,c_2,\ldots,c_m$. Áp dụng hệ quả suy ra từ công thức ***(33)*** ta có $\pi(an)<(\pi(a+1)n)$ đúng với giá trị đủ lớn của $n.$ Hệ quả là tồn tại số tự nhiên s thỏa mãn $\pi(a\cdot 10^s)<\pi((a+1)\cdot 10^s).$ Vì vậy tồn tại số nguyên tố p mà $a\cdot 10^s<p<(a+1)\cdot 10^s.$ Vì vậy m chữ số đầu tiên của p trùng với các chữ số tương ứng của $a.$ Nghĩa là m chữ số đầu tiên của p là $c_1,c_2,\ldots,c_m.$ Từ đây ta có một hệ quả khác của công thức ***(33)*** là: *với dãy hữu hạn $c_1,c_2,\ldots,c_m$ các chữ số tùy ý thì tồn tại số nguyên tố mà m chữ số đầu tiên của nó là $c_1,c_2,\ldots,c_m$* [5]

Ký hiệu x là số thực >0. Với số tự nhiên đủ lớn n ta có $nx>2$ do đó $\pi(nx)\ge 1$. Từ ***(34)*** suy ra

(37) $$\lim_{n\to\infty}\frac{p_{\pi(nx)}}{\pi(nx)\log\pi(nx)}=1$$

Nhưng từ ***(33)*** ta có

(38) $$\lim_{n\to\infty}\frac{\pi(nx)\log\pi(nx)}{nx}=1$$

Suy ra $\lim_{n\to x}(\log\pi(nx)+\log\log nx-\log nx)=0,$ vậy

(39) $$\lim_{n\to\infty}\frac{\log\pi(nx)}{\log(nx)}=1$$

Từ các công thức ***(37)***, ***(38)*** và ***(39)*** ta suy ra $\lim_{n\to\infty}\frac{P_{\pi(nx)}}{nx}=1$. Vậy ta đã chứng minh công thức ***(33)*** suy ra với mọi số thực $x>0$ thì đều tồn tại dãy vô hạn các số nguyên tố $q_1,q_2,\ldots$ thỏa mãn $\lim_{n\to\infty}\frac{q_n}{n}=x$. Tính chất này được phát hiện bởi H.Steinhaus. Cuối cùng nếu a và b là các số thực tùy ý thỏa mãn $a<b$ thì từ hệ quả của công thức ***(33)*** suy ra nếu q là số nguyên tố đủ lớn thì tồn tại số nguyên tố p thỏa mãn $aq<p<bq,$ từ đây suy ra $a<p/q<b.$ Điều này chứng tỏ tập hợp các tỷ số p/q, p và q là các số nguyên tố, là trù mật trong tập các số thực dương.

([5]) Xem Sierpinski [10] và Trost [3] trang 42 định lý 20, xem Sierpinski [25]. Định lý mạnh hơn đã được chứng minh.

CHƯƠNG 4

SỐ CÁC ƯỚC SỐ VÀ TỔNG CỦA CHÚNG

1. Số các ước số

Số các ước số của một số tự nhiên cho trước n được ký hiệu là $d(n)$. Để lập bảng các giá trị của hàm số $d(n)$ ta có thể sử dụng phương pháp dưới đây. Phương pháp này được biến đổi từ phương pháp sàng Eratosthenes. Đầu tiên để tính các giá trị $d(n)$ với $n \le a$ ta viết các số $1, 2, \ldots, a$ và đánh dấu chúng. Sau đó ta đánh dấu tất cả các số chia hết cho 2, sau đó là các số chia hết cho 3 và cứ như vậy. Cuối cùng ta đánh dấu số a. Số các ước số của số n chính là số dấu mà nó được gạch dưới (Harris [1]). Chẳng hạn với $a = 20$ ta có

$$\underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, \underline{7}, \underline{8}, \underline{9}, \underline{10}, \underline{11}, \underline{12}, \underline{13}, \underline{14}, \underline{15}, \underline{16}, \underline{17}, \underline{18}, \underline{19}, \underline{20}.$$

Vì vậy ta có

$$d(1) = 1,\ d(2) = 2,\ d(3) = 2,\ d(4) = 3,\ d(5) = 2,\ d(6) = 4,$$
$$d(7) = 2,\ d(8) = 4,\ d(9) = 3,\ d(10) = 4,\ d(11) = 2,\ d(12) = 6,$$
$$d(13) = 2,\ d(14) = 4,\ d(15) = 4,\ d(16) = 5,\ d(17) = 2,\ d(18) = 6,$$
$$d(19) = 2,\ d(20) = 6.$$

Với số tự nhiên n lớn hơn 1 xét phân tích thành thừa số nguyên tố của n là

(1) $$n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$$

Giả sử d là ước số của n. Khi đó mọi ước số của d cũng là ước số của n, do đó phân tích thành thừa số nguyên tố của d cũng có dạng ***(1)***. Hơn nữa số mũ của các lũy thừa của biểu diễn đó là nhỏ hơn các lũy thừa tương ứng trong ***(1)***. Nghĩa là mọi ước số d của n có thể viết dưới dạng

(2) $$d = q_1^{\lambda_1} q_2^{\lambda_2} \ldots q_k^{\lambda_k},$$

Với $\lambda_i \ (i = 1, 2, \ldots, k)$ là các số nguyên thỏa mãn các bất đẳng thức

(3) $$0 \le \lambda_i \le x_i \quad \textbf{\textit{với}} \quad i = 1, 2, \ldots, k$$

Mặt khác mọi số tự nhiên có thể biểu diễn ở dạng ***(2)*** với các số λ_i thỏa mãn ***(3)*** đều là ước số tự nhiên của n. vì theo ***(3)*** thì $n/d = q_1^{\alpha_1 - \lambda_1} q_2^{\alpha_2 - \lambda_2} \ldots q_k^{\alpha_k - \lambda_k}$ là số nguyên.

Cuối cùng các bộ số nguyên phân biệt

(4) $$\lambda_1, \lambda_2, \ldots, \lambda_k$$

xác định các số khác nhau trong ***(2)***. Ta có định lý

Định lý 1. *Nếu n là số tự nhiên mà phân tích thành thừa số nguyên tố của nó được viết dưới dạng **(1)** thì với tất cả các bộ số phân biệt gồm k số nguyên trong **(4)** thỏa mãn **(3)** ta xác định được tất cả các ước số của n cho bởi **(2)**. Hơn nữa mỗi bộ số đó ứng với đúng một ước số của n.*

Hệ quả là số các ước số của số tự nhiên n có biểu diễn thành thừa số nguyên tố có dạng ***(1)*** bằng với số các bộ số nguyên ***(4)*** thỏa mãn các bất đẳng thức ***(3)***. Số bộ số như vậy có thể tính một cách đơn giản. Thật vậy số nguyên λ_i thỏa mãn ***(3)*** khi và chỉ khi λ_i thuộc dãy $0, 1, 2, \ldots, \alpha_i$. Vì vậy với $i = 1, 2, \ldots, k$ cho trước thì λ_i nhận $\alpha_i + 1$ giá trị phân biệt. Suy ra

Định lý 2. *Số $d(n)$ các ước số của số tự nhiên n có biểu diễn thành thừa số nguyên tố **(1)** là*

(5) $$d(n) = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_k + 1).$$

Chẳng hạn tính $d(60)$. Ta có $60=2^2\cdot 3\cdot 5$. Do đó theo ***(5)*** ta có $d(60)=(2+1)(1+1)(1+1)=12$. Tương tự vì $100=2^2\cdot 5^2$, suy ra $d(100)=(2+1)(2+1)=9$.

Từ ***(5)*** suy ra với mọi số tự nhiên $s>1$ có vô hạn các số tự nhiên mà có đúng s ước số. Thật vậy nếu $n=p^{s-1}$, với p là số nguyên tố thì $d(n)=d\left(p^{s-1}\right)=s$. Rõ ràng đẳng thức $d(n)=1$ suy ra $n=1$. Công thức ***(5)*** chứng tỏ $d(n)=2$ chỉ khi $k=1$ và $\alpha_1=1$, nghĩa là n là số nguyên tố. Các nghiệm của phương trình $d(n)=2$ đều là số nguyên tố. Vậy với hợp số n ta có $d(n)\geq 3$. Từ ***(5)*** suy ra $d(n)$ là số lẻ khi và chỉ khi tất cả các số x_i với $i=1,2,\ldots,k$ đều chẵn, nghĩa là n là bình phương đúng.

Bài tập. *1.* Chứng minh rằng với mọi số tự nhiên n thì $d(n)\leq 2\sqrt{n}$.

Điều này là hiển nhiên vì trong hai ước số đối nhau của n thì có một số không vượt quá $\sqrt{n}$.

2. Tìm tất cả các số tự nhiên có đúng 10 ước số.

Lời giải. Nếu $d(n)=10$, thì theo ***(5)*** ta có $(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_k+1)=10$. Có thể giả sử $\alpha_1\leq\alpha_2\leq\ldots\leq\alpha_k$. Vì có hai cách để biểu diễn 10 thành tích của hai số tự nhiên >1 theo thứ tự không giảm nên $10=2\cdot 5$ và $10=10$, nên hoặc $k=2,\alpha_1=1,\alpha_2=4$, hoặc $k=1,\alpha_1=9$. Suy ra các số tự nhiên có 10 ước số có dạng pq^4 với $p,q\neq p$ là các số nguyên tố tùy ý hoặc có dạng p^9, với p là số nguyên tố tùy ý. □

3. Tìm số tự nhiên n nhỏ nhất mà $d(n)=10$.

Lời giải. Theo bài tập 2 thì các số $2^9, 2\cdot 3^4$, và $3\cdot 2^4$ (số cuối cùng là nhỏ nhất) là các số tự nhiên nhỏ nhất n mà $d(n)=10$. Vậy $n=3\cdot 2^4=48$. □

Ghi chú. Với hai số nguyên tố p,q cho trước, $q>p$, thì số tự nhiên nhỏ nhất có đúng pq ước số là $2^{q-1}\cdot 3^{p-1}$.

4. Chứng minh rằng nếu n là số tự nhiên >1 thì trong dãy vô hạn $n, d(n), d\left(d(n)\right), ddd(n),\ldots$ tất cả các phần tử của dãy sẽ bằng 2 kể từ một vị trí nào đó. Chứng minh rằng vị trí này có thể tùy ý.

Lưu ý rằng nếu n là số tự nhiên lớn hơn 2 thì $d(n)<n$, và $d(2)=2$. Mặt khác $d\left(2^{n-1}\right)=n$.

5. Chứng minh rằng với mọi số tự nhiên m thì tập hợp các số tự nhiên n mà số ước số của n chia hết cho m chứa một cấp số cộng vô hạn.

Chứng minh. Ta lưu ý rằng các số $2^m t+2^{m-1}\left(t=1,2,\ldots\right)$ tạo thành cấp số cộng vô hạn và thuộc về tập xác định như đề bài bởi m. Thật vậy, lũy thừa của 2 trong phân tích thành thừa số nguyên tố của $n=2^m t+2^{m-1}$ là $m-1$. Vì vậy theo ***(1)*** ta có $m\mid d(n)$. □

Ghi chú. Hệ quả trực tiếp của định lý trên là với mọi số tự nhiên m thì tập hợp các số tự nhiên n mà $m\mid d(n)$ có chặn dưới trù mật. Nghĩa là tồn tại số dương a mà số $S_m(x)$ các số tự nhiên $n\leq x$ mà $m\mid d(n)$ là lớn hơn ax với mọi x đủ lớn. E.Coben [1] đã chứng minh rằng với mọi số tự nhiên m thì giới hạn $\lim\limits_{x\to x}\dfrac{S_m(x)}{x}$ tồn tại và là một số dương.

Năm 1940 bảng $d(n)$ với $n \le 10000$ đã được trình bày (Glaisher [2]). Dựa vào bảng này ta tìm thấy $d(n) = d(n+1) = d(n+2) = d(n+3) = 8$ đúng với $n = 3655, 4503, 5943, 6853, 8393, 9367.$

J.Mycielski đã chỉ ra với $n = 40311$ ta có $d(n) = d(n+1) = d(n+2) = d(n+3) = d(n+4).$

Chứng minh nhận xét này suy ra ngay từ $40311 = 3^3 \cdot 1493, 40312 = 2^3 \cdot 5039, 40313 = 7 \cdot 13 \cdot 443,$ $40314 = 2 \cdot 3 \cdot 6719, 40315 = 5 \cdot 11 \cdot 733.$ Tình huống tương tự cũng xảy ra với $n = 99655.$

Câu hỏi đặt ra là có thể có bao nhiêu giá trị liên tiếp $d(n)$ bằng nhau (Erdos và Mirsky [1]).

Ta có $d(2) = d(3), d(14) = d(15), d(33) = d(34) = d(35) = 4, d(242) = d(243) = d(244) = d(245) = 6.$

D.R.Heath-Brown [1] đã chứng minh sự tồn tại vô hạn n mà $d(n) = d(n+1).$ Ta chưa biết có tồn tại dãy vô hạn tăng các số tự nhiên $n_k \, (k = 1, 2, \ldots)$ mà $\lim_{k \to \infty} d(n_{k+1} + 1) / d(n_k) = 2$ hay không. Ta cũng chưa biết các số $d(n+1)/d(n)$ có tạo thành tập trù mật trong tập các số thực dương hay không. Tuy nhiên P.Erdos đã chứng minh rằng tập hợp đó trù mật trong một khoảng không tầm thường (Erdos [14] ghi chú (1)). Với $n \le 10000$ ta có $d(n) \le 64$ và giá trị lớn nhất $d(n) = 64$ nhận được chỉ với $n = 7560$ và $9240.$ A.Schinzel [2] đã chứng minh rằng với mọi số tự nhiên h và m tồn tại số tự nhiên $n > h$ thỏa mãn $d(n) / d(n \pm 1) > m$ với $i = 1, 2, \ldots, h.$

2. Các tổng $d(1) + d(2) + \ldots + d(n)$

Với số thực $x \ge 1$ ký hiệu $T(x)$ là tổng

(6) $$T(x) = \sum_{k=1}^{[x]} d(k) = d(1) + d(2) + \ldots + d([x]).$$

Để tính tổng này đầu tiên ta chứng minh rằng với số tự nhiên k cho trước thì $d(k)$ là số các nghiệm tự nhiên của phương trình

(7) $$mn = k$$

Thật vậy nếu số tự nhiên n là ước số của $k,$ thì $m = k/n$ là số tự nhiên và cặp m, n là nghiệm tự nhiên của ***(7)***. Ngược lại nếu cặp các số tự nhiên m, n thỏa mãn ***(7)*** thì n là ước số của $k.$ Vậy mỗi ước số tự nhiên của k tương ứng với đúng một nghiệm của phương tình ***(7)***. Suy ra số $d(k)$ bằng với số các nghiệm tự nhiên của ***(7)***. Hệ quả là từ ***(6)*** suy ra $T(x)$ chính là số nghiệm tự nhiên của bất đẳng thức $mn \le [x].$ Bất đẳng thức này tương đương với

(8) $$mn \le x.$$

Tất cả các nghiệm tự nhiên của ***(8)*** được chia thành các lớp trong đó nghiệm m, n được gọi là thuộc lớp n. Ký hiệu k_n là số nghiệm thuộc lớp n thì rõ ràng

(9) $$T(x) = k_1 + k_2 + k_3 + \ldots$$

Bây giờ ta tính số các nghiệm thuộc lớp n.

Với n cho trước thì m chỉ có thể nhận các giá trị tự nhiên thỏa mãn ***(8)***, tức là $m \le \frac{x}{n}.$ Do đó m chỉ có thể là $1, 2, \ldots, \left[\frac{x}{n}\right]$, có $\left[\frac{x}{n}\right]$ số như vậy suy ra $k_n = \left[\frac{x}{n}\right],$ và từ ***(9)*** ta có

(10) $$T(x)=\left[\frac{x}{1}\right]+\left[\frac{x}{2}\right]+\left[\frac{x}{3}\right]+...$$

Vế phải không phải là tổng vô hạn vì chỉ có $[x]$ phần tử đầu tiên của nó là khác 0.

Vì vậy ***(10)*** có thể viết thành

(11) $$T(x)=\sum_{k=1}^{[x]}\left[\frac{x}{k}\right].$$

Các tính toán $T(x)$ dựa theo ***(11)*** chỉ thuận tiện khi ta muốn tìm các giá trị liên tiếp của $d(k)$, nhưng nói chung là không tốt với x lớn. Chẳng hạn để tính $T(100)$ ta cần cộng lần lượt hơn một trăm số. Ta sẽ tìm một công thức thuận tiên hơn cho $T(x)$. Đầu tiên ta chia lớp các nghiệm tự nhiên của ***(8)*** thành hai lớp mà lớp đầu tiên chứa các nghiệm với $n\le\sqrt{x}$ và lớp kia chứa các nghiệm còn lại, nghĩa là $n>\sqrt{x}$. Ta tính số các nghiệm trong mỗi lớp. Nếu n nhận giá trị tự nhiên $\le\sqrt{x}$ và nếu m,n là nghiệm tự nhiên của ***(8)*** nghĩa là nếu m là số tự nhiên thỏa mãn $m\le x/n$, thì m,n thuộc lớp thứ nhất. Do đó với mọi số tự nhiên $n\le\sqrt{x}$ số các nghiệm của lớp thứ nhất là $\left[\frac{x}{n}\right]$. Do n nhận các giá trị $1,2,...,\left[\sqrt{x}\right]$, nên số nghiệm thuộc lớp thứ nhất là $\sum_{n=1}^{[\sqrt{x}]}\left[\frac{x}{n}\right]$. Ta tính số nghiệm thuộc lớp thứ hai. Nghĩa là số các cặp số tự nhiên m,n thỏa mãn $mn\le x$ và $n>\sqrt{x}$, hay

(12) $$\sqrt{x}<n\le\frac{x}{m}.$$

Nếu $m>\sqrt{x}$, thì $x/m<\sqrt{x}$ và các bất đẳng thức ***(12)*** không thỏa mãn với mọi n. Theo đó ký hiệu m là số tự nhiên cố định $\le\sqrt{x}$. Để tìm tất cả các giá trị dương của n mà ***(12)*** thỏa mãn thì ta chỉ cần loại ra khỏi các số tự nhiên $n\le\frac{x}{m}$ (có $\left[\frac{x}{m}\right]$ số như vậy) các số n không thỏa mãn $\sqrt{x}<n$, nghĩa là số các chỉ số n mà $n\le\sqrt{x}$ (có $\left[\sqrt{x}\right]$ số như vậy). Vậy $\left[\frac{x}{m}\right]-\left[\sqrt{x}\right]$ là số các cặp m,n với $m\le\sqrt{x}$ thỏa mãn ***(12)***. Nhưng m chỉ nhận các giá trị $1,2,...,[x]$, nên số các nghiệm thuộc lớp thứ hai là $\sum_{m=1}^{[\sqrt{x}]}\left(\left[\frac{x}{m}\right]-\left[\sqrt{x}\right]\right)=\sum_{m=1}^{[\sqrt{x}]}\left[\frac{x}{m}\right]-\sum_{m=1}^{[\sqrt{x}]}\left[\sqrt{x}\right]$. Hạng tử thứ hai trong vế phải bằng với $\left[\sqrt{x}\right]^2$ vì nó là tổng của $\left[\sqrt{x}\right]$ hạng tử và mỗi hạng tử đều bằng $\left[\sqrt{x}\right]$. Do đó số nghiệm trong lớp thứ hai là $\sum_{m=1}^{[\sqrt{x}]}\left[\frac{x}{m}\right]-\left[\sqrt{x}\right]^2$. Vì vậy $\sum_{n=1}^{[\sqrt{x}]}\left[\frac{x}{n}\right]+\sum_{m=1}^{[\sqrt{x}]}\left[\frac{x}{m}\right]-\left[\sqrt{x}\right]^2$ là số nghiệm tự nhiên của ***(8)***, tức là giá trị của $T(x)$. Ta có $\sum_{m=1}^{[\sqrt{x}]}\left[\frac{x}{m}\right]=\sum_{n=1}^{[\sqrt{x}]}\left[\frac{x}{n}\right]$ vì cả hai tổng đều bằng $\left[\frac{x}{1}\right]+\left[\frac{x}{2}\right]+...\left[\frac{x}{\left[\sqrt{x}\right]}\right]$; vì vậy

(13) $$T(x)=2\sum_{n=1}^{[\sqrt{x}]}\left[\frac{x}{n}\right]-\left[\sqrt{x}\right]^2.$$

Công thức này được tìm ra bởi Lejeune Dirichlet. Ta tính $T(100)$ như sau

$$T(100)=2\sum_{n=1}^{10}\left[\frac{100}{n}\right]-10^2=2(100+50+33+25+20+$$
$$+16+14+12+11+10)-100=2\cdot 291-100=482.$$

Tương tự ta tính được $T(200)=1098,\ T(500)=3190,\ T(1000)=7069.$ Với các tính toán dài hơn ta tìm được $T(5000)=43376,\ T(10000)=93668.$ Từ ***(11)*** ta có thể nhận được một xấp xỉ trung bình cho hàm $d(n)$. Trong vế phải của ***(11)*** ta thay $\left[\frac{x}{k}\right]$ bởi $\frac{x}{k}$, khi đó các sai số trong mỗi hạng tử là nhỏ hơn 1 và vì vậy sai số của cả tổng là nhỏ hơn số hạng tử, nghĩa là nhỏ hơn $\left[x\right]\le x.$ Do đó $T(x)$ được xấp xỉ bởI $\sum_{n=1}^{[x]}\frac{x}{n}$, với sai số nhỏ hơn $x.$ Với các giá trị là số tự nhiên $x=k$ ta có

(14) $$\frac{d(1)+d(2)+\ldots+d(k)}{k}\approx\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{k},$$

với sai số nhỏ hơn 1. Do vế phải của ***(14)*** tăng tới vô hạn theo $k,$ nên tỷ số giữa vế trái và vế phải tiến tới 1. Ta đã biết tổng $\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{k}$ có thể xấp xỉ bởi $\log k,$ với sai số nhỏ hơn 1 với $k>1.$ Do đó $\log k$ là xấp xỉ của vế trái ***(14)***. Hiệu $\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{k}-\log k$ tiến tới giới hạn là hằng số *Euler* $C=0.57721566\ldots$ (ta chưa biết số này có phải là số vô tỷ hay không). Từ đây kết hợp với công thức ***(13)*** ta tìm được xấp xỉ $x\log x+(2C-1)x$ của $T(x)$ với sai số nhỏ hơn bội số hữu hạn của $\sqrt{x}.$ G.Voronoi đã chứng minh rằng sai số này là không lớn hơn bội số hữu hạn của $\sqrt[3]{x}\log x.$ Một số tác giả khác đã tìm ra đánh giá chính xác của sai số này (Kolesnik [1]).

3. Các chuỗi với các hệ số $d(n)$

Trong giải tích, các hàm $d(n)$ xuất hiện như là hệ số của các chuỗi vô hạn.

Chẳng hạn xét các chuỗi Lambert (hội tụ với $|x|<1$) $\sum_{k=1}^{\infty}\frac{x^k}{1-x^k}=\frac{x}{1-x}+\frac{x^2}{1-x^2}+\frac{x^3}{1-x^3}+\ldots$

Khai triển mỗi hạng tử của chuỗi thành chuỗi lũy thừa $\frac{x^k}{1-x^k}=x^k+x^{2k}+x^{3k}+\ldots$ ta nhận được chuỗi lặp $\sum_{k=1}^{\infty}\sum_{l=1}^{\infty}x^{kl}$ mà với mọi số tự nhiên n thì lũy thừa x^n xuất hiện với số lần đúng bằng số nghiệm tự nhiên của phương trình $kl=n,$ nghĩa là $d(n)$ lần.

Vì vậy với $|x|<1$ ta có $\sum_{k=1}^{\infty}\frac{x^k}{1-x^k}=\sum_{n=1}^{\infty}d(n)x^n$.

Ta thấy $d(n)$ là hệ số của x^n trong biểu diễn của chuỗi Lambert thành chuỗi lũy thừa.

Hàm $d(n)$ cũng là hệ số trong biểu diễn của các hàm ξ.

Với $s>1$ ta xét chuỗi vô hạn $\zeta(s)=\sum_{k=1}^{\infty}\frac{1}{k^s}=\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\ldots$ (chuỗi này hội tụ với $s>1$).

Bây giờ ta áp dụng *tích Dirichlet* cho $\zeta(s)\zeta(s)$. Tích Dirichlet được cho như sau: với hai chuỗi $a_1+a_2+...$ và $b_1+b_2+...,$ ta nhân $(a_1+a_2+...)$ với $(b_1+b_2+...,)$ và nhóm các tích a_kb_l với các bộ chỉ số có tích bằng nhau, nghĩa là $(a_1+a_2+...)(b_1+b_2+...)=a_1b_1+(a_1b_2+a_2b_1)+(a_1b_3+a_3b_1)+(a_1b_4+a_2b_2+a_4b_1)+(a_1b_5+a_5b_1)+(a_1b_6+a_2b_3+a_3b_2+a_6b_1)+(a_1b_7+a_7b_1)+...$ Từ đây ta có

(15) $$(\zeta(s))^2=\sum_{n=1}^{\infty}\frac{d(n)}{n^s}$$

4. Tổng các ước số

Tổng các ước số tự nhiên của số tự nhiên n ký hiệu là $\sigma(n)$. Từ Định lý 1 suy ra nếu ***(1)*** là phân tích thành thừa số nguyên tố của $n,$ thì

(16) $$\sigma(n)=\sum q_1^{\lambda_1}q_2^{\lambda_2}...q_k^{\lambda_k},$$

Trong đó các tổng lấy trên mọi bộ k số nguyên ***(4)*** thỏa mãn ***(3)***. Nhưng mỗi hạng tử của ***(16)*** đều xuất hiện trong khai triển tích $\left(1+q_1+q_1^2+...+q_1^{\alpha_1}\right)\left(1+q_2+q_2^2+...q_2^{\alpha_2}\right)...\left(1+q_k+q_k^2+...+q_k^{\alpha_k}\right)$ và hơn nữa xuất hiện đúng một lần. Vì vậy

Định lý 3. *Tổng $\sigma(n)$ các ước số tự nhiên của số tự nhiên $n=q_1^{\alpha_1}q_2^{\alpha_2}...q_k^{\alpha_k}$ là*

(17) $$\sigma(n)=\frac{q_1^{\alpha_1+1}-1}{q_1-1}\cdot\frac{q_2^{\alpha_2+1}-1}{q_2-1}...\frac{q_k^{\alpha_k+1}-1}{q_k-1}.$$

Đặc biệt $\sigma(100)=\frac{2^3-1}{2-1}\cdot\frac{5^3-1}{5-1}=7\cdot31=217.$ Từ Định lý 3 suy ra với các số tự nhiên nguyên tố cùng nhau a,b ta có $\sigma(ab)=\sigma(a)\sigma(b).$ Mặt khác nếu $(a,b)>1,$ thì $\sigma(ab)<\sigma(a)\sigma(b).$

Sử dụng Định lý 3 ta tính được $\sigma(1)=1,\sigma(2)=3,\sigma(3)=4,\sigma(4)=7,\sigma(5)=6,\sigma(6)=12,\sigma(7)=8,$ $\sigma(8)=15,\sigma(9)=13,\sigma(10)=18.$ Với $n>1$ thì $\sigma(n)>n.$ Suy ra $\sigma(n)>5$ với $n>4.$ Với $n\le4$ thì $\sigma(n)$ nhận các giá trị $1,3,4$ và $7.$ Không tồn tại n mà $\sigma(n)=5.$

Định lý 4. *Tồn tại vô hạn số tự nhiên không phải giá trị $\sigma(x)$ với mọi số tự nhiên $x.$*

Chứng minh. Với n là số tự nhiên >9 xét số tự nhiên k mà

(18) $$\frac{n}{3}-1<k\le\frac{n}{2}$$

Số các số k như vậy là lớn hơn $n/2-n/3=n/6.$ Theo ***(18)*** ta có

(19) $$2k\le n \text{ } \textbf{và} \text{ } 3k+3>n,$$

Và vì $n>9,$ ta có $3k>6,$ suy ra $k\ge3.$ Vì vậy $2k$ có ít nhất 4 ước số phân biệt là $1,2,k,2k.$ Do đó $\sigma(2k)\ge1+2+k+2k,$ và theo ***(19)*** suy ra $\sigma(2k)>n.$ Do số các số tự nhiên k mà thỏa mãn ***(18)***,***(19)*** và do đó $\sigma(2k)>n$ là nhiều hơn $n/6,$ nên trong các số $\sigma(1),\sigma(2),...,\sigma(n)$ có nhiều hơn $n/6$ số lớn hơn $n.$ Vì vậy trong dãy $1,2,...,n$ có nhiều hơn $n/6$ số tự nhiên không là giá trị của hàm $\sigma(x)$ với $x\le n.$ Các số này cũng không thể là giá trị $\sigma(x)$ với $x>n.$ vì các số này $\le n$ mà $\sigma(x)\ge1+x>n$ với $x>n$. Do đó với mọi các số tự nhiên $n>9$ có nhiều hơn $n/6$ số tự nhiên trong dãy $1,2,...,n$ không là giá trị của $\sigma(x)$ với mọi số tự nhiên $x.$ □

Vậy tồn tại vô hạn số tự nhiên m mà phương trình $\sigma(x)=m$ là không có nghiệm tự nhiên $x.$

Có thể chứng mỉnh ằng tất cả các số $m=3^k\,(k>1)$ đều có tính chất này (Sierpinski [27]). Có đúng 59 số $m\le 100$ như vậy. Đó là 2, 5, 9, 10, 11, 17, 19, 21, 22, 23, 25, 26, 27, 29, 33, 34, 35, 37, 41, 43, 45, 46, 47, 49, 50, 51, 52, 53, 55, 58, 59, 61, 64, 65, 66, 67, 69, 70, 71, 73, 75, 76, 77, 79, 81, 82, 83, 85, 86, 87, 88, 89, 92, 94, 95, 97, 99, 100.

Trong các số $m\le 100$ có đúng 25 số mà phương trình $\sigma(x)=m$ có duy nhất nghiệm. Đó là $m=$ 1,3,4,6,7,8,13,14,15,20,28,30,36,40,44,57,62,63,68,74,78,91,93. Một câu hỏi đặt ra là có phải tồn tại vô hạn các số tự nhiên m mà phương trình $\sigma(x)=m$ có duy nhất nghiệm hay không.

Chứng minh dưới đây cho ta kết quả tổng quát hơn. P.Erdos [14] (trang 12) đã chứng minh rằng với mọi số k cho trước tồn tại m mà phương trình $\sigma(x)=m$ có đúng k nghiệm thì tồn tại vô hạn các số m như vậy. Tuy nhiên tồn tại vô hạn số tự nhiên m mà phương trình $\sigma(x)=m$ có nhiều hơn 1 nghiệm. Chẳng hạn với các số $m=3\left(5^k-1\right)$, $k=1,2,\ldots$, thì ta có $\sigma(6)=\sigma(11)=12$ và $\left(6,5^{k-1}\right)=\left(11,5^{k-1}\right)=1$, nên $\sigma\left(6\cdot 5^{k-1}\right)=\sigma\left(11\cdot 5^{k-1}\right)=3\left(5^k-1\right).$

Dễ dàng chứng minh tồn tại vô hạn các số tự nhiên m mà phương trình $\sigma(x)=m$ có nhiều hơn 2 nghiệm. Chẳng hạn với các số $2\left(13^k-1\right)$, với $k=1,2,\ldots$ thì ta có $\sigma\left(14\cdot 13^{k-1}\right)=\sigma\left(15\cdot 13^{k-1}\right)=$ $\sigma\left(23\cdot 13^{k-1}\right)=2\left(13^k-1\right).$

Ta vẫn chưa biết có phải với mọi số tự nhiên k tồn tại số tự nhiên m_k mà phương trình $\sigma(x)=m_k$ có đúng k nghiệm tự nhiên x hay không. Kết luận này cũng được suy ra từ giả thuyết H (Schinzel [13]). Có thể chứng minh rằng nếu m_k là số nhỏ nhất mà $\sigma(x)=m_k$ có đúng k nghiệm thì

$m_1=1, m_2=12, m_3=24, m_4=96, m_5=72, m_6=168, m_7=240,\ m_8=432,$
$m_9=360, m_{10}=504, m_{11}=576, m_{12}=1512, m_{13}=1080, m_{14}=1008, m_{15}=720, m_{16}=2304, m_{17}=3600,$
$m_{18}=5376, m_{19}=2160, m_{20}=1440.$

Phương trình $\sigma(x)=m$ có đúng 3 nghiệm tự nhiên với 6 trường hợp của $m\le 100,$ đó là các số 24,42,48,60,84,90. Với $m\le 100$ phương trình $\sigma(x)=m$ có đúng 4 nghiệm chỉ khi $m=96.$ Cũng vậy với $m\le 100$ thì phương trình có đúng 5 nghiệm chỉ khi $m=72$. Không tồn tại $m\le 100$ mà phương trình có nhiều hơn 5 nghiệm tự nhiên. Tuy nhiên H.J. Kanold [2] đã chứng minh với mọi số tự nhiên k thì tồn tại số tự nhiên m mà phương trình $\sigma(x)=m$ có $\ge k$ nghiệm tự nhiên x.

Phương trình $\sigma(n)=\sigma(n+1)$ có đúng 9 nghiệm $n<10000.$ Đó là $n=$ 14, 206, 957, 1334, 1364, 1634, 2685, 2974, 4364 (Makowski [4]). Có đúng 113 nghiệm $n\le 10^7$ (Hunsucker, Nebb và Stream [1], Guy và Shanks [1]). Ta chưa biết có tồn tại vô hạn nghiệm như vậy hay không.

A.Makowski đã đặt ra câu hỏi có phải với mọi số nguyên k thì tồn tại số tự nhiên n mà $\sigma(n+1)-\sigma(n)=k$ và tổng quát hơn với mọi số tự nhiên m và k nguyên tồn tại số tự nhiên n mà $\sigma(n+m)-\sigma(n)=k.$

Các kết quả với $m\le 5$ đã được trình bày bởi Mientka và Vogt [1]. Nếu n và $n+2$ là các số nguyên tố sinh đôi thì $\sigma(n+2)=\sigma(n)+2$. Phương trình này cũng đúng với $n=434$ mà 434 và 436 không phải số nguyên tố. Tình huống tương tự xảy ra với $n=8575$ và $n=8825.$

Dựa vào giả thuyết Catalan (đã chỉnh sửa bởi Dickson [3]) thì nếu $f(n)=\sigma(n)-n$ thì với số tự nhiên $n>1$ dãy vô hạn $n, f(n), ff(n), fff(n)$ hoặc là dãy tuần hoàn hoặc là dãy dừng tại phần tử 1. Kết quả này đúng với mọi $n\le 275$ (Devitt [1]). Theo L.Alaoglu và P.Erdos [2] thì giả thuyết này không những khó chứng minh mà còn khó để kiểm tra trong các trường hợp đặc biệt. Chẳng hạn

với $n=276$. Với $n=12496=2^4\cdot 11\cdot 71$ thì tất cả các số $n, f(n), ff(n), fff(n), ffff(n)$ là phân biệt nhưng $fffff(n)=n$. Với $n=12$ ta có $f(12)=16, f(16)=15, f(15)=9, f(9)=4, f(4)=3, f(3)=1,$ chứng tỏ dãy dừng. Đối với số nguyên tố n thì $f(n)=1.$ Với $n=100$ ta có $f(100)=117, f(117)=65,$ $f(65)=19, f(19)=1.$ Với $n=6,$ thì $f(n)=n$ nên dãy tuần hoàn chu kỳ một phần tử. Với $n=95$ ta có $f(95)=25, f(25)=6, f(6)=6$ và dãy tuần hoàn từ phần tử thứ 4 với chu kỳ một phần tử. Với $n=220$ ta có $f(220)=284, f(284)=220=n,$ và do đó dãy tuần hoàn ngay từ phần tử đầu tiên với chu kỳ hai phần tử. Trong một bản thảo chưa công bố P.Poulet [3] đã thông báo rằng với $n=936$ thì dãy 936,1794,2238,2250,...,74,40,50,43,1 chứa 189 phần tử, số lớn nhất là 33289162091526.

Một câu hỏi được đặt ra là có phải tồn tại dãy dài tùy ý mà dừng tại 1 và có phải tồn tại vô hạn số tự nhiên n mà dãy trên là tuần hoàn. Câu trả lời cho câu hỏi này là khẳng định nếu giả thuyết nói rằng mọi số chẵn lớn 6 đều là tổng của hai số nguyên tố phân biệt là đúng. Thật vậy, giả sử giả thuyết đúng và ký hiệu $2k-1$ là số lẻ tùy ý >7. Khi đó $2k-2>6$ và theo giả thuyết tồn tại hai số nguyên tố lẻ phân biệt p và q, mà $2k-2=p+q$. Vì vậy $f(pq)=\sigma(pq)-pq=1+p+q=2k-1.$ Vì p,q là các số nguyên tố lẻ phân biệt, giả sử $p>q,$ và do đó $p\ge q+2$ với $q\ge 3.$ Vì vậy $pq\ge 3p=2p+p\ge 2p+1+2>p+q+1=2k-1$ do đó $pq>2k-1.$ Vậy với mọi số lẻ $n>7$ tồn tại số lẻ $m>n$ mà $f(m)=n.$ Đặt $m=g(n).$ Tồn tại dãy vô hạn tăng $g(n), gg(n),...$ Nếu với số tự nhiên k đặt $n=g^k(11)$ ta nhận được dãy $n=g^k(11), f(n)=g^{k-1}(11),...f^k(n)=11, f(11)=1.$ Do đó ta nhận được dãy giảm $n, f(n), ff(n),...$ chứa $k+2$ phần tử và phần tử cuối cùng bằng 1. Với số tự nhiên k đặt $n=g^k(25),$ ta có dãy tuần hoàn $n=g^k(25), f(n)=g^{k-1}(25),...f^k(n)=25, f(25)=6, f(6)=6,6,...$ với $k+1$ phần tử giảm trong chu kỳ tuần hoàn.

Một câu hỏi khác được đặt ra là có phải tồn tại vô hạn các số tự nhiên phân biệt mà dãy $n, f(n), ff(n),...$ là tuần hoàn mà không có phần tử nào xuất hiện trước chu kỳ tuần hoàn. Ta mới chỉ tìm ra các chu kỳ có độ dài là 1,2,4,5 và 28 như vậy (H.Cohen [1]).

Ta vừa chứng minh từ giả thuyết nói rằng mọi số tự nhiên chẵn >6 là tổng của hai số nguyên tố phân biệt suy ra mọi số tự nhiên lẻ >7 là phần tử của dãy $f(n)(n=1,2,...)$. Hơn nữa $f(3)=1, f(4)=3, f(8)=7.$ Mặt khác dễ dàng chứng minh 5 không xuất hiện trong dãy $f(n)(n=1,2,...)$. Thật vậy nếu với số tự nhiên n ta có $f(n)=\sigma(n)-n=5$ thì n là hợp số (bởi vì $\sigma(1)-1=0$ và với số nguyên tố $n, \sigma(n)-n=1$). Do đó $n=ab,$ với $1<a\le b<n.$ Khi đó vì $1, b$ và n là các ước số phân biệt của n ta có $\sigma(n)\ge 1+b+n,$ suy ra $5=\sigma(n)-n\ge 1+b>b,$ và $b>5.$ Suy ra $n=ab$ với $1<a\le b\le 4.$ Nhưng điều này là vô lý vì không có các số tự nhiên a,b có tính chất trên mà $\sigma(n)=n+5.$

Nếu không sử dụng giả thuyết nói rằng mọi số tự nhiên >6 là tổng của hai số nguyên tố phân biệt thì ta chưa chứng minh được mọi số lẻ khác 5 là có dạng $\sigma(n)-n(n=1,2,...)$. P.Erdos [17] đã chứng minh tồn tại vô hạn số tự nhiên không thuộc dãy này.

Có thể chứng minh tính chất $m\,|\,\sigma(mn-1)$ đúng với mọi số tự nhiên n khi và chỉ khi $m=3,4,6,8,12$ hoặc 24 (Gupta [1]).

Ta chưa biết có tồn tại vô hạn số tự nhiên n mà $\sigma(n)$ là bình phương hay không. Từ giả thuyết H (Chương 3 mục 8) suy ra câu trả lời khẳng định. Thật vậy đặt $f(x)=2x^2-1$ thì đa thức $f(x)$ là bất khả quy và vì $f(0)=-1$ nên nó thỏa mãn điều kiện C trong Chương 3. Do đó theo giả thuyết H

suy ra tồn tại vô hạn số tự nhiên x mà $p=2x^2-1$ là số nguyên tố >7. Với các số này ta có $\sigma(7p)=8(p+1)=(4x)^2$. Suy ra $\sigma(7p)$ là bình phương đúng.

Ta biết một số nghiệm tự nhiên của phương trình $\sigma(x^2)=y^2$ chẳng hạn $x=7, y=20.$ Ta cũng biết một số nghiệm tự nhiên của phương trình $\sigma(x^2)=y^3$ chẳng hạn $x=2\cdot 3\cdot 11\cdot 653, y=7\cdot 13\cdot 19.$

Bài tập. ***1.*** Chứng minh rằng $\sigma(n)=n+1$ khi và chỉ khi n là số nguyên tố.

Chứng minh. Nếu p là số nguyên tố thì nó có 2 ước số là p và 1. Do đó $\sigma(p)=p+1.$ Mặt khác nếu n là hợp số nghĩa là $n=ab,$ với các số tự nhiên a và $b>1$ thì n có ít nhất ba ước số tự nhiên phân biệt là $1, a$ và n. Do đó $\sigma(n)\geq 1+a+n>n+1.$ Cuối cùng nếu $n=1,$ thì $\sigma(n)=1<n+1.$ □

2. Chứng minh với mọi số tự nhiên m tồn tại các số tự nhiên x, y mà $x-y\geq m$ và $\sigma(x^2)=\sigma(y^2)$.

Chứng minh. Xét số tự nhiên n tùy ý $>m$ mà $(n,10)=1.$ Với $x=5n, y=4n$ ta có $x-y=n>m$ và $\sigma(x^2)=\sigma(y^2)=31\sigma(n^2).$ □

3. Tìm tất cả các nghiệm tự nhiên mà tổng các ước số của nó là lẻ.

Lời giải. Giả sử n là số tự nhiên mà $\sigma(n)$ lẻ. Đặt $n=2^{\alpha}k,$ với k lẻ và α là số nguyên không âm. Ta có $\sigma(n)=(2^{\alpha+1}-1)\sigma(k)$ và do đó $\sigma(k)$ lẻ. Vì k lẻ nên các ước số của nó là lẻ. Mà tổng các ước số của nó $\sigma(k)$ lẻ nên $d(k)$ là số các ước số của nó cũng lẻ. Vì vậy theo mục 1 suy ra k là bình phương đúng, nghĩa là $k=m^2$. Vì vậy $n=2^{\alpha}m^2$. Nếu α chẵn nghĩa là $\alpha=2\beta,$ thì $n=(2^{\beta}m)^2$. Nếu α lẻ thì $\alpha=2\beta+1$ và do đó $n=2(2^{\beta}m)^2$ nên hoặc $n=l^2$ hoặc $n=2l^2,$ với l là số tự nhiên. Mặt khác nếu $n=l^2$ hoặc $n=2l^2,$ với l là số tự nhiên, $n=2^{\alpha}q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_k^{\alpha_k}$ là phân tích thành thừa số nguyên tố của n với $q_1, q_2, \ldots, q_k$ là các số nguyên tố lẻ. Ta có $\sigma(n)=(2^{2\alpha+1}-1)\sigma(q_1^{2\alpha_1})\ldots\sigma(q_k^{2\alpha_k})$ hoặc $\sigma(n)=(2^{2\alpha+2}-1)\sigma(q_1^{2\alpha_1})\ldots\sigma(q_k^{2\alpha_k}).$ Nhưng vì $\sigma(q_i^{2\alpha_i})=1+q_i+q_i^2+\ldots q_i^{2\alpha_i},$ là tổng của lẻ hạng tử lẻ nên $\sigma(n)$ lẻ. Do đó $\sigma(n)$ là lẻ khi và chỉ khi n là bình phương đúng hoặc hai lần một bình phương đúng. □

4. Chứng minh rằng nếu n là hợp số thì $\sigma(n)>n+\sqrt{n}.$

Chứng minh. Hợp số n có ước số d thỏa mãn $1<d<n.$ Vì vậy $1<n/d<n$. Nếu $d\leq\sqrt{n},$ thì $d/n\geq\sqrt{n}.$ Nhưng vì n/d cũng là ước số của n (không nhất thiết khác d) và $1<n/d<n.$ nên $\sigma(n)\geq n+\sqrt{n}+1,$ suy ra $\sigma(n)>n+\sqrt{n}.$ Điều phải chứng minh. □

Ghi chú. Ta có hệ quả $\lim\limits_{n\to x}(\sigma(p_n+1)-\sigma(p_n))=+\infty$ và $\lim\limits_{n\to x}(\sigma(p_n)-\sigma(p_n-1))=-\infty$.

5. Chứng minh với số tự nhiên $k>1$ phương trình $\sigma(n)=n+k$ có số nghiệm là hữu hạn dương.

Chứng minh. Nếu $\sigma(n)=n+k$ với k là số tự nhiên >1 thì n là hợp số và theo bài tập 4 thì $\sigma(n)>n+\sqrt{n}.$ suy ra $n<k^2$. Đặc biệt phương trình $\sigma(n)=n+2$ vô nghiệm và phương trình $\sigma(n)=n+3$ có duy nhất nghiệm $n=4.$ □

6. Chứng minh rằng $\lim\limits_{n\to x}\dfrac{\sigma(n!)}{n!}=+\infty$.

Chứng minh. Dễ dàng chứng minh $\sigma(m)/m$ là tổng của các nghịch đảo các ước số của m. vì $n!$ nhận tất cả các số tự nhiên $\le n$ làm ước số nên $\frac{\sigma(n!)}{n!} \ge \frac{1}{1}+\frac{1}{2}+...+\frac{1}{n}$. Nhưng $\lim\limits_{n\to x}\left(\frac{1}{1}+\frac{1}{2}+...+\frac{1}{n}\right)=+\infty$, suy ra $\lim\limits_{n\to x}\frac{\sigma(n!)}{n!}=\infty$. □

7. L.Alaoglu và P.Erdos [1] gọi các số tự nhiên n là rất phong phú *(superabundant)* nếu $\sigma(n)/n > \sigma(k)/k$ với mọi $k<n$. Chứng minh rằng tồn tại vô hạn số như vậy.

Chứng minh. Đặt $u_n=\sigma(n)/n$ với $n=1,2,...$ từ bài tập 6 suy ra dãy $u_1,u_2,...$ không có chặn trên. Vì vậy để chứng minh bài toán ta chỉ cần chứng minh định lý tổng quát hơn: *mọi dãy vô hạn các số thực không có chặn trên chứa vô hạn các phần tử lớn hơn tất cả các phần tử đứng trước nó.*

Thật vậy giả sử dãy $u_1,u_2,...$ không có chặn trên khi đó ta có $\lim\limits_{n\to\infty}\max(u_1,u_2...,u_n)=+\infty$ và với mỗi số tự nhiên m tồn tại số tự nhiên $l>m$ mà $a_l=\max(u_1,u_2,...,u_l)>\max(u_1,u_2,...,u_m)$. Trong dãy $u_1,u_2,...,u_l$ tồn tại các phần tử không bằng a_l. Gọi u_n là phần tử đầu tiên như vậy. Khi đó ta có $n>m, n\le l$ và $u_n>u_k$ với $k<n$. Ta đã chứng minh với mọi số tự nhiên $>m$ thì tồn tại số tự nhiên $n>m$ mà $u_n>u_k$ với mọi $k<n$. Điều phải chứng minh. □

8. A.K.Srinivasan [1] gọi các số tự nhiên n là số cơ sở *(practical number)* nếu mọi số tự nhiên $\le n$ là tổng các ước số khác nhau của n. Chứng minh với số tự nhiên $n>1$ thì $2^{n-1}(2^n-1)$ là số cơ sở.

Chứng minh. Nếu k là số tự nhiên $\le 2^n-1$, thì ta đã biết k là tổng các số khác nhau trong dãy $1,2,2^2,...,2^{n-1}$. Mặt khác nếu $2^n-1<k\le 2^{n-1}(2^n-1)$, thì $k=(2^n-1)t+r$, với t là số tự nhiên $\le 2^{n-1}$ và $0\le r<2^n-1$, do đó t và r là các tổng các phần tử khác nhau trong dãy $1,2,2^2,...,2^{n-1}$. Điều phải chứng minh. □

Điều kiện cần và đủ để một số tự nhiên n là số cơ sở có trong Sierpinski [16]. Stewart [2], Margenstern [1]. Số 10 không phải số cơ sở 100 và 1000 là số cơ sở.

9. Tìm số tự nhiên m mà phương trình $\sigma(x)=m$ có nhiều hơn 1000 nghiệm.

Lời giải. Ta sử dụng phương pháp được đưa ra bởi S.Mazur. Giả sử ta đã tìm được s bộ ba các số nguyên tố $p_i,q_i,r_i\ (i=1,2,...,s)$, mà tất cả $3s$ số này đều phân biệt và hơn nữa

(20) $$(p_i+1)(q_i+1)=r_i+1,\ i=1,2,...,s.$$

Đặt

(21) $$a_i^{(0)}=p_iq_i,\quad a_i^{(1)}=r_i,\quad i=1,2,...,s.$$

Với mọi dãy $\alpha_1,\alpha_2,...,\alpha_s$ chứa s số bằng 0 hoặc 1 ta đặt

(22) $$n_{\alpha_1,\alpha_2,...,\alpha_s}=a_1^{(\alpha_1)}a_2^{(\alpha_2)}...a_s^{(\alpha_s)}.$$

Vì các số $p_i,q_i,r_i\ (i=1,2,...,s)$, là các số nguyên tố phân biệt, các điều kiện ***(21)*** và ***(22)*** suy ra

(23) $$\sigma\left(n_{\alpha_1,\alpha_2,...,\alpha_s}\right)=\sigma\left(a_1^{(\alpha_1)}\right)\sigma\left(a_2^{(\alpha_2)}\right)...\sigma\left(a_s^{(\alpha_s)}\right).$$

Theo ***(21)*** ta có $\sigma\left(a_i^{(0)}\right)=(p_i+1)(q_i+1)$, $\sigma\left(a_i^{(1)}\right)=r_i+1$, $i=1,2,...,s$, và theo ***(20)*** thì $\sigma\left(a_i^{(0)}\right)=\sigma\left(a_i^{(1)}\right)=\sigma(r_i)$, với $i=1,2,...,s$, do đó $\sigma\left(a_i^{(\alpha_i)}\right)=\sigma(r_i)$, $i=1,2,...,s$, vì vậy ta thấy công thức ***(23)*** suy ra $\sigma\left(n_{\alpha_1,\alpha_2,...\alpha_s}\right)=\sigma(r_1)\sigma(r_2)...\sigma(r_s)=\sigma(r_1r_2...r_s)$ với tất cả 2^s dãy $\alpha_1,\alpha_2,...\alpha_s$.

Các số $n_{\alpha_1,\alpha_2,...,\alpha_s}$, có 2^s số như vậy, đều phân biệt vì theo ***(21)*** và ***(22)*** thì phân tích thành thừa số nguyên tố của chúng là phân biệt. Do đó ta nhận được 2^s số tự nhiên phân biệt có chung tổng các ước số. Do đó để tìm chẳng hạn 1024 số có tổng các ước số bằng nhau ta chỉ cần tìm 10 bộ ba các số nguyên tố $p_i, q_i, r_i\ (i=1,2,...,10)$ mà 30 số đó là khác nhau và thỏa mãn ***(20)***. Dễ dàng kiểm tra các bộ ba sau đây thỏa mãn các điều kiện cần thiết

2,3,11;5,7,47;13,17,251;19,23,479;29,41,1259;31,83,2687;
43,71,3167;59,61,3719;53,101,5507;83,97,8231.

Suy ra với $m=12\cdot48\cdot252\cdot480\cdot1260\cdot2688\cdot3168\cdot3720\cdot5508\cdot8232$ thì phương trình $\sigma(x)=m$ có ít nhất 1024 nghiệm tự nhiên x. □

5. Các số hoàn hảo

Tồn tại vô hạn số tự nhiên n mà tổng các ước số của n (không tính n) là nhỏ hơn n. Chẳng hạn các số như vậy là các số nguyên tố và lũy thừa của chúng. Cũng tồn tại vô hạn các số tự nhiên n mà tổng tương ứng lớn hơn n. Chẳng hạn các số có dạng $n=2^k\cdot3$, với $k=2,3,...$ Tuy nhiên ta chưa biết có tồn tại vô hạn các số tự nhiên n mà tổng các ước số của n (không tính n) bằng n hay không. Các số có tính chất này được gọi là các số hoàn hảo. Có 30 số hoàn hảo đã được tìm ra. Tất cả chúng đều là số chẵn và ta chưa biết có tồn tại số hoàn hảo lẻ hay không. Ta đã chứng minh được nếu một số hoàn hảo lẻ là tồn tại thì nó phải lớn hơn 10^{50} (Buxton và Elmore [1] đã chỉ ra nó còn phải lớn hơn 10^{200}) và có ít nhất 8 ước số nguyên tố phân biệt (Hagis [1],[2]). Số hoàn hảo lớn nhất đã được biết là số $2^{216090}\left(2^{216091}-1\right)$. Số này có 130100 chữ số. Số hoàn hảo nhỏ nhất là $6=1+2+3$ và số tiếp theo là $28=1+2+4+7+14$. Tổng các ước số của n (không tính n) rõ ràng là $\sigma(n)-n$. Do đó một số tự nhiên là hoàn hảo khi và chỉ khi

(24) $$\sigma(n)=2n.$$

Định lý 5. *Một số chẵn là số hoàn hảo khi và chỉ khi nó có dạng* $2^{s-1}\left(2^s-1\right)$, *với* s *là số tự nhiên và* 2^s-1 *là số nguyên tố.*

Chứng minh. Gọi n là số hoàn hảo chẵn. Khi đó $n=2^{s-1}l$, với $s>1$ và l là số lẻ. Vì vậy $\sigma(n)=\left(2^s-1\right)\sigma(l)$ và theo ***(24)*** thì $\left(2^s-1\right)\sigma(l)=2^sl$. Vì $\left(2^s-1,2^s\right)=1$, suy ra $\sigma(l)=2^sq$, với q là số tự nhiên. Vì vậy $(2^s-1)q=l$ với $\sigma(l)=2^sq$, suy ra $\sigma(l)=l+q$. Nhưng vì $\left(2^s-1\right)q=l$, ta có $q\mid l$ và $q<l$ (vì $s>1$) do đó số l có ít nhất hai ước số tự nhiên phân biệt là q và l. Công thức $\sigma(l)=l+q$ chứng tỏ nó không có nghiệm khác nữa. Hệ quả là $q=1$ và l là số nguyên tố. Nhưng $l=\left(2^s-1\right)q=2^s-1$. Do đó $n=2^{s-1}l=2^{s-1}\left(2^s-1\right)$, và vì vậy 2^s-1 là số nguyên tố. Điều kiện cần được chứng minh. Để chứng minh điều kiện đủ giả sử 2^s-1 là số nguyên tố lẻ. Hơn nữa đặt $n=2^{s-1}\left(2^s-1\right)$. Ta có $\sigma(n)=\left(2^s-1\right)\sigma\left(2^s-1\right)=\left(2^s-1\right)2^s$ vì 2^s-1 là số nguyên tố. Do đó $\sigma(n)=2n$, suy ra n là số hoàn hảo. Điều kiện đủ được chứng minh. □

Dễ dàng chứng minh nếu 2^s-1 là số nguyên tố thì s cũng là số nguyên tố. Thật vậy nếu $s=ab,$ với a và b là các số tự nhiên >1 thì $2^s-1=\left(2^a-1\right)\left(1+2^a+2^{2a}+...+2^{(b-1)a}\right),$ mà $a\geq 2,$ nên vì $2^a-1\geq 2^2-1\geq 3,$ suy ra 2^s-1 là hợp số. Định lý 5 suy ra hệ quả sau đây

Hệ quả. *Mọi số hoàn hảo chẵn cho bởi công thức* $2^{p-1}\left(2^p-1\right),$ *với* p *và* 2^p-1 *là các số nguyên tố.*

Các số hoàn hảo được nghiên cứu bởi Euclid, người đã đề ra phương pháp sau để tìm những số như vậy: *ta tính các tổng các lũy thừa liên tiếp* $1+2+4+8+16+32+...$. *Nếu tổng trở thành một số nguyên tố thì ta nhân nó với hạng tử cuối cùng và nhận được một số hoàn hảo*.

Sử dụng Định lý 5 ta thấy phương pháp của Euclid thực sự đã cho biết mọi số hoàn hảo chẵn.

Bây giờ ta tính một số số hoàn hảo chẵn. Đầu tiên ta xét p lần lượt là các số nguyên tố tiếp theo tính từ 2 và kiểm tra xem 2^p-1 có phải số nguyên tố hay không. Ta thấy với $p=2,3,5,7$ thì $2^p-1=3,7,31,127$ là các số nguyên tố. Do đó 4 số hoàn hảo đầu tiên là $2\left(2^2-1\right)=6, 2^2\left(2^3-1\right)=28, 2^4\left(2^5-1\right)=496, 2^8\left(2^7-1\right)=8128.$ với $p=11$ thì $2^{11}-1=23\cdot 89$ là hợp số do đó ta không có số hoàn hảo tương ứng.

Từ Định lý 5 suy ra việc tìm tất cả các số hoàn hảo chẵn tương đương với việc tìm tất cả các số *Mersenne* (là các số nguyên tố có dạng 2^s-1). Ta sẽ nghiên cứu bài toán này trong chương 10.

Ký hiệu $V(x), x$ là số thực, là số các số hoàn hảo $\leq x$.

B.Hornfeck và E.Wirsing [1] đã chứng minh $\lim\limits_{x\to\infty}\dfrac{\log V(x)}{\log x}=0$ và E.Wirsing [1] đã chứng minh tồn tại số tự nhiên A mà $V(x)<Ae^{A(\log x)/\log\log x}$.

Ta không biết có tồn tại vô hạn số tự nhiên n mà $n\,|\,\sigma(n),$ hoặc có tồn tại số tự nhiên lẻ có tính chất này hay không. Ta đã chứng minh được không tồn tại số tự nhiên lẻ n như thế với $n<10^{50}$ (Beck và Najar [1]).

Số tự nhiên n thỏa mãn $\sigma(n)=mn,$ với m là số tự nhiên >1 được gọi là số hoàn hảo P_m. Các số này được nghiên cứu bởi Mersenns, Fermat, Descartes, Legendre và một số người khác. Các số hoàn hảo P_2 là số hoàn hảo thông thường. P.Poulet [1] (trang 9-27) đã tìm ra 334 số hoàn hảo P_m với $m\leq 8.$ Năm 1953 B.Franqui và M.Garcia [1] đã tìm ra 63 số nữa (Franqui và M.Garcia [2], A.L.Brown [1],[2]). Các số P_3 được nghiên cứu bởi R.Steurwald [1].

P.Cattaneo [1] gọi một số là giả hoàn hảo nếu nó bằng tổng các ước số tự nhiên không tầm thường của nó, nghĩa là các ước số khác 1 và chính nó. Theo đó số giả hoàn hảo là các số tự nhiên n mà $\sigma(n)=2n+1.$ Ta chưa biết có tồn tại các số như vậy hay không. P.Hagis Jr. và G.Cohen [1] đã chứng minh nếu tồn tại các số như vậy thì chúng đều lớn hơn 10^{35} và có ít nhất 7 ước số nguyên tố phân biệt.

Tuy nhiên dễ dàng chứng minh tồn tại vô hạn số tự nhiên n mà $\sigma(n)=2n-1.$ Chẳng hạn các số $2^k, k=0,1,2,...$ có tính chất này. A.Makowski [5] đã nghiên cứu nghiệm tự nhiên của phương trình $\sigma(n)=2n+2$. Ông ta lưu ý rằng nếu 2^k-3 là số nguyên tố thì $n=2^{k-1}\left(2^k-3\right)$ là nghiệm cần tìm. Các số 2^k-3 là nguyên tố với các giá trị $k<24: k=2,3,4,5,6,9,10,12,14,20,22.$ Phương trình này còn có các nghiệm khác chẳng hạn $n=650.$

Phương trình tổng quát $\sigma(n)=kn+a$ được nghiên cứu bởi C.Pomerance [1] và A.Makowski [9].

Bài tập. ***1.*** Chứng minh rằng tồn tại vô hạn số tự nhiên lẻ n mà $\sigma(n) > 2n$.

Chứng minh. Các số $n = 945m,$ với m là số tự nhiên không chia hết cho 2,3,5,7, thỏa mãn điều kiện vì $945 = 3^3 \cdot 5 \cdot 7, (m, 945) = 1$ do đó $\sigma(n) = \sigma(945)\sigma(m) \geq \sigma(945)m = 1920m > 2n.$ Vì m không chia hết cho 2 nên n là số lẻ. Có thể chứng minh 945 là số tự nhiên lẻ nhỏ nhất mà $\sigma(n) > 2n$. □

2. Tìm tất cả các số tự nhiên n mà n là tích của tất cả các ước số tự nhiên của n trừ ra n.

Lời giải. Ký hiệu Q_n là tích tất cả các nghiệm tự nhiên của n. Ta tìm các số tự nhiên n mà $Q_n / n = n,$, nghĩa là với n ta có $Q_n = n^2$. Nếu $d_1, d_2, ...d_s$ là tất cả các ước số tự nhiên của n (có $s = d(n)$ số như vậy) thì các số $n/d_1, n/d_2, ...n/d_s$ cũng là các ước số tự nhiên của n. Suy ra $Q_n = d_1, d_2, ..., d_s = n^s / Q_n,$ và do đó $Q_n = n^{s/2} = n^{d(n)/2}$. Vì $Q_n = n^2,$ ta có $n^2 = n^{d(n)/2},$ suy ra $d(n) = 4,$ điều ngược lại cũng đúng, nghĩa là nếu $d(n) = 4,$ thì $Q_n = n^2$, do đó một số tự nhiên n bằng tích các ước số của nó trừ ra n khi và chỉ khi nó có đúng 4 ước số tự nhiên.

Từ công thức tính số ước số của một số tự nhiên cho bởi công thức ***(5)*** với ***(1)*** là phân tích thành thừa số nguyên tố của n ta có $(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1) = 4$. Do các số mũ $\alpha_1, \alpha_2, ..., \alpha_k$ là các số tự nhiên suy ra $k \leq 2,$ nghĩa là $k = 1$ hoặc $k = 2$. Nếu $k = 1$ thì $\alpha_1 + 1 = 4,$ suy ra $\alpha_1 = 3$ và n là lập phương một số nguyên tố. Nếu $k = 2$ thì $\alpha_1 = \alpha_2 = 1$ và n là tích của hai số nguyên tố. Vậy mọi số tự nhiên cần tìm là các lập phương nguyên tố và tích của hai số nguyên tố phân biệt.

Các số như vậy nhỏ hơn 30 là 6,8,10,14,15,21,22,26,27. □

3. Chứng minh các định lý Descartes sau (thư Descartes gửi Mersenne ngày 15 tháng 11/ 1638).

1. *Nếu n là số hoàn hảo P_3 và không chia hết cho 3 thì $3n$ là số hoàn hảo P_4.*
2. *Nếu n chia hết cho 3 nhưng không chia hết cho 5 và 9 và hơn nữa nó là số hoàn hảo P_3 thì $45n$ là số hoàn hảo P_4.*
3. *Nếu n không chia hết cho 3 và $3n$ là số hoàn hảo P_{4k} thì n là số hoàn hảo P_{3k}.*

Chứng minh. *1.* Nếu n là số hoàn hảo P_3 thì $\sigma(n) = 3n$ và nếu n không chia hết cho 3 thì $\sigma(3n) = \sigma(3)\sigma(n) = 4 \cdot 3n$ và hệ quả là $3n$ là số hoàn hảo P_4.

2. Nếu n là số hoàn hảo P_3 và $n = 3k,$ với k không chia hết cho 3 và 5 thì $\sigma(45n) = \sigma(3^3 \cdot 5k) = \sigma(3^3)\sigma(5)\sigma(k) = 40 \cdot 6 \cdot \sigma(k)$. Nhưng vì $n = 3k$ và k không chia hết cho 3 nên ta có $\sigma(n) = \sigma(3)\sigma(k) = 4\sigma(k)$. Hệ quả là $\sigma(45n) = 60 \cdot 4\sigma(k) = 60\sigma(n)$. Vì vậy do n là số hoàn hảo P_3 nên $\sigma(n) = 3n$ và ta có $\sigma(45n) = 180n = 4 \cdot 45n,$ chứng tỏ $45n$ là số hoàn hảo P_4.

3. Nếu n không chia hết cho 3 và $3n$ là số hoàn hảo P_{4k} thì $\sigma(3n) = 4k \cdot 3n,$ suy ra $\sigma(3n) = \sigma(3)\sigma(n) = 4\sigma(n)$ và do đó $\sigma(n) = 3kn,$ chứng tỏ n là số hoàn hảo P_{3k}. □

4. Chứng minh rằng 120 và 672 là các số hoàn hảo P_3. Số $2^5 \cdot 3^3 \cdot 5 \cdot 7$ là số hoàn hảo P_4 và $2^7 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11^2 \cdot 17 \cdot 19$ là số hoàn hảo P_5.

Lời giải. Ta có các phân tích thành thừa số nguyên tố $120 = 2^3 \cdot 3 \cdot 5$ và $672 = 2^5 \cdot 3^3 \cdot 7$. Có thể chứng minh 120 là số hoàn hảo P_3 nhỏ nhất.

5. Chứng minh rằng nếu $\sigma(n) = 5n,$ thì n có nhiều hơn 5 ước số nguyên tố phân biệt.

Chứng minh. Giả sử ***(1)*** là phân tích thành thừa số nguyên tố của n. Khi đó theo ***(17)*** ta có

$$\sigma(n)<\frac{q_1^{\alpha_1+1}q_2^{\alpha_2+1}...q_k^{\alpha_k+1}}{(q_1-1)(q_2-1)...(q_k-1)}=\frac{q_1}{q_1-1}\cdot\frac{q_2}{q_2-1}\cdot...\cdot\frac{q_k}{q_k-1}\cdot n.$$

Nếu $k\le 5,$ thì ta có $\sigma(n)\le\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{5}{4}\cdot\frac{7}{6}\cdot\frac{11}{10}n=\frac{77}{16}n<5n$ mâu thuẫn với $\sigma(n)=5n.$ □

6. Định lý Mersenne: *nếu* n *không chia hết cho 5 và là số hoàn hảo* P_5 *thì* $5n$ *là số hoàn hảo* P_6.

6. Các số bạn bè

Hai số tự nhiên gọi là số bạn bè nếu mỗi số bằng tổng tất cả các ước số của số kia trừ ra chính số đó. Dễ dàng thấy hai số tự nhiên n,m là các số bạn bè khi và chỉ khi $\sigma(m)=\sigma(n)=m+n.$ ***(1)***

Cặp số bạn bè đầu tiên là 220 và 284 được tìm ra bởi Pythagoras. Cặp $2^4\cdot 23\cdot 47$ và $2^4.1151$ được tìm ra bởi Fermat ***(2)***. Cặp $2^7\cdot 191\cdot 383$ và $2^7\cdot 73727$ tìm ra bởi Decartes. Euler đã tìm ra 59 cặp số như vậy, trong đó có các cặp $2^3\cdot 17\cdot 79$, $2^3\cdot 23\cdot 59$ và $2^3\cdot 19\cdot 41$, $2^5\cdot 199$. E.J.Lee và J.S.Madachy [1] đã trình bày một danh sách 1107 cặp số bạn bè tìm được qua 25 thiên niên kỷ. Danh sách được hoàn thiện tới 10^8. Hơn 5000 cặp số bè bạn được xây dựng bởi W.Borho, H.Hoffman và H.J.J te Riele (te Riele [1],[2]). Ta biết tồn tại cặp số bạn bè cùng lẻ chẳng hạn $3^3\cdot 5\cdot 7\cdot 11, 3\cdot 5\cdot 7\cdot 139.$ Nhưng ta chưa biết có tồn tại cặp số bạn bè khác tính chẵn lẻ hay không. Ta cũng chưa biết có tồn tại vô hạn cặp số bạn bè hay không. Định nghĩa của cặp số bạn bè được mở rộng cho bộ *k* số bạn bè. Định nghĩa này được trình bày bởi L.E.Dickson, người đã gọi bộ *k* số tự nhiên $n_1,n_2,...n_k$ là bộ *k* số bạn bè nếu $\sigma(n_1)=\sigma(n_2)=...=\sigma(n_k)=n_1+n_2+...+n_k$ (Dickson [2], Mason [1]).

A.Makowski [4] đã tìm ra bộ ba số bạn bè $2^2\cdot 3^2\cdot 5\cdot 11, 2^5\cdot 3^2\cdot 7, 2^2\cdot 3^2\cdot 71$ và $2^3\cdot 3\cdot 5\cdot 13, 2^2\cdot 3\cdot 5\cdot 29, 2^2\cdot 3\cdot 5\cdot 29$ (trong bộ số thứ hai có 2 số bằng nhau). Tồn tại bộ ba mà cả ba số là bằng nhau chẳng hạn $n_1=n_2=n_3=120.$

Định nghĩa khác của bộ *k* số bạn bè được cho bởi B.F.Yanney [1]: bộ *k* số tự nhiên $n_1,n_2,...n_k$ gọi là bộ *k số bạn bè nếu* $n_1+n_2+...+n_k+\sigma(n_i)=\sigma(n_1)+\sigma(n_2)+...+\sigma(n_k)$ với $i=1,2,...,k$. Điều kiện này tương đương với điều kiện $n_1+n_2+...+n_k=(k-1)\sigma(n_i)$ với $i=1,2,...,k$.

Với $k=2$ các định nghĩa đều quy về trường hợp định nghĩa cặp các số bạn bè. Với $k>2,$ các định nghĩa này không trùng nhau. Chẳng hạn một bộ ba số bạn bè theo định nghĩa của Yanney là 308,455,581. Ta có $308=2^2\cdot 7\cdot 11, 455=5\cdot 7\cdot 13, 581=7\cdot 83,$ do đó $\sigma(n_1)=\sigma(n_2)=\sigma(n_3)=672$ và $n_1+n_2+n_3=1344=2\cdot 672.$

Ta chưa biết có các số nguyên tố cùng nhau nào là số bạn bè hay không. H.J.Kanold [1] đã chứng minh nếu cặp số bạn bè m_1,m_2 thỏa mãn m_1,m_2 nguyên tố cùng nhau thì mỗi số đều lớn hơn 10^{23} và số m_1m_2 có nhiều hơn 20 ước số nguyên tố phân biệt. P.Erdos [13] đã chứng minh rằng nếu $A(x)$ là số các cặp số bạn bè $\le x,$ thì $\lim_{x\to\infty}A(x)/x=0.$ C.Pomrance [2] đã chứng minh rằng nếu $A(x)$ là số các cặp số bạn bè $\le x,$ thì với x đủ lớn $A(x)<x\exp\left(-(\log x)^{1/3}\right).$

7. Tổng $\sigma(1)+\sigma(2)+...+\sigma(n)$

Trong mục này ta xét công thức tổng

---

(1) Ghi chú của ban biên tập. hầu hết các tác giả đều giả thiết $n\ne m.$

(2) Theo W.Borcho [1] thì các số này đã được tìm ra bởi Ibn Al Banna (1256-1321).

(25) $$S(x)=\sigma(1)+\sigma(2)+...+\sigma([x]),$$

với x là số thực ≥ 1. Giả sử n là số tự nhiên. Số n là phần tử của tổng $\sigma(k)$ khi và chỉ khi n là ước số của k. Do đó để tính số các hạng tử $\sigma(k)$ xuất hiện trong tổng $S(x)$ mà n xuất hiện như là một hạng tử thì chỉ cần tính số các số $k \leq x$ mà chia hết cho n. Nhưng các số k như vậy có dạng $k=nl \leq x$, với l là số tự nhiên mà $l \leq x/n$. Rõ ràng có [x/n] số như vậy. Do đó số tự nhiên n là hạng tử của tổng $\sigma(k)$ ứng với [x/n] số tự nhiên phân biệt $k \leq x$. Từ đây suy ra

(26) $$S(x)=\sum_{n=1}^{[x]} n\left[\frac{x}{n}\right].$$

Có một phương pháp khác để tính ***(25)***. Số $\sigma(k)$ có thể xét như là tổng các số tự nhiên n thỏa mãn phương trình $mn=k$, với m là số tự nhiên. Do đó ***(25)*** là tổng các số n mà tồn tại các số tự nhiên m thỏa mãn $mn \leq x$. Như thế với các số cố định m và n thuộc $1,2,3,...,\left[\frac{x}{m}\right]$, thì tổng của chúng bằng $1+2+...+\left[\frac{x}{m}\right]=\frac{1}{2}\left[\frac{x}{m}\right]^2+\frac{1}{2}\left[\frac{x}{m}\right]$. Hệ quả là nếu ta cho m nhận mọi giá trị dương mà $mn \leq x$ thì tổng tất cả các số n, nghĩa là $S(x)$, bằng với

(27) $$S(x)=\frac{1}{2}\sum_{m=1}^{[x]}\left[\frac{x}{m}\right]^2+\frac{1}{2}\sum_{m=1}^{[x]}\left[\frac{x}{m}\right].$$

So sánh ***(26)*** và ***(27)*** ta nhận được $\sum_{n=1}^{[x]} n\left[\frac{x}{n}\right]=\frac{1}{2}\sum_{m=1}^{[x]}\left[\frac{x}{m}\right]^2+\frac{1}{2}\sum_{m=1}^{[x]}\left[\frac{x}{m}\right]$. Rõ ràng công thức này có thể viết lại dưới dạng $\sum_{n=1}^{[x]}\left[\frac{x}{n}\right]^2=\sum_{n=1}^{[x]}(2n-1)\left[\frac{x}{n}\right]$. Tuy nhiên các công thức ***(26)*** và ***(27)*** đều không ứng dụng được để tính các giá trị của tổng $S(x)$ với số cho trước x. Công thức thích hợp hơn được tìm ra theo cách tương tự công thức ***(13)***

(28) $$S(x)=\frac{1}{2}\left(\sum_{n=1}^{[\sqrt{x}]}\left[\frac{x}{n}\right]^2+\sum_{n=1}^{[\sqrt{x}]}(2n-1)\left[\frac{x}{n}\right]-\left[\sqrt{x}\right]^3-\left[\sqrt{x}\right]^2\right).$$

Chẳng hạn sử dụng công thức này ta tính được $S(100)=8249$. Bây giờ nếu trong ***(28)*** ta bỏ đi ký hiệu [] và thay tổng $\sum_{n=1}^{[\sqrt{x}]} 1/n^2$ bởi tổng của chuỗi vô hạn $\sum_{n=1}^{\infty} 1/n^2=\pi^2/6$, sau mỗi lần tính thì sai số giảm, thì ta nhận được $\pi^2x^2/12$ là xấp xỉ của tổng $S(x)$, với sai số không lớn hơn $Ax\sqrt{x}$, với A là hằng số dương độc lập với x.

8. Các chuỗi với hệ số $\sigma(n)$

Hàm $\sigma(n)$ (tương tự $d(n)$; mục 3) xuất hiện như là hệ số của các chuỗi vô hạn. Ta có chuỗi lặp

(29) $$\sum_{k=1}^{\infty}\sum_{l=1}^{\infty} kx^{kl}$$

hội tụ tuyệt đối với $|x|<1$. Để rút gọn chuỗi này thành chuỗi lũy thừa thì với số cố định n ta nhóm các hạng tử mà x^n xuất hiện. Khi đó các hệ số của các hạng tử trong nhóm thứ n là nhân tử của tích $n=kl$. Do đó ***(29)*** trở thành tổng $\sum_{n=1}^{\infty}\sigma(n)x^n$.

Mặt khác vì $\sum_{l=1}^{\infty}kx^{kl}=kx^k\big/\left(1-x^k\right)$, ta thấy ***(29)*** bằng với tổng $\sum_{l=1}^{\infty}kx^{kl}=kx^k/(1-x^k)$.

Vì vậy ta nhận được công thức $\sum_{k=1}^{\infty}\frac{kx^k}{1-x^k}=\sum_{n=1}^{x}\sigma(n)x^n,\quad |x|<1.$

Vì ***(29)*** hội tụ tuyệt đối với $|x|<1$, ta có thể hoán vị các phần tử của chuỗi, áp dụng đẳng thức $\sum_{k=1}^{\infty}kx^{kl}=x^l\big/\left(1-x^l\right)^2$ với $|x|<1$, ta nhận được công thức $\sum_{l=1}^{\infty}\frac{x^l}{\left(1-x^l\right)^2}=\sum_{n=1}^{x}\sigma(n)x^n,\quad |x|<1.$

Trong mục 3 ta đã giới thiệu tích Dirichlet của hai chuỗi vô hạn $a_1+a_2+\ldots$ và $b_1+b_2+\ldots$.

Ta sử dụng tích đó với $a_k=1\big/k^{s-1}, b_1=1\big/l^s, k$ và l là các số tự nhiên và s là số thực >2. Ta có $a_kb_l=\frac{1}{k^{s-1}}\cdot\frac{1}{l^s}=\frac{k}{(kl)^s}$. Bây giờ nhóm các tích a_kb_1 mà kl bằng số tự nhiên cho trước n, ta thấy các tử số bằng với các ước số tự nhiên k của n; tổng của chúng là $\sigma(n)\big/n^s$. Vì vậy $\zeta(s-1)\zeta(s)=\sum_{n=1}^{\infty}\frac{\sigma(n)}{n^s}$ với $s>2$.

9. Tổng của các hạng tử xác định bởi các ước số tự nhiên của một số tự nhiên n

Xét $f(n)$ là hàm tùy ý xác định với mọi số tự nhiên n. Nếu $d_1,d_2,\ldots d_s$ là tất cả các ước số tự nhiên của n thì tổng $f(d_1)+f(d_2)+\ldots+f(d_s)$ ký hiệu bởi $\sum_{d/n}f(d)$ là tổng các hạng tử $f(d)$ với d nhận mọi giá trị là các ước số tự nhiên của n. Chẳng hạn $\sum_{d|n}1=d(n),\quad \sum_{d|n}d=\sigma(n)$ nhưng $\sum_{d|n}\frac{n}{d}=\sigma(n)$. Với hàm $f(n)$ cho trước ta đặt $F(n)=\sum_{d|n}f(d)$. Ta sẽ tính tổng $\sum_{n=1}^{[x]}F(x)=\sum_{n=1}^{[x]}\sum_{d|n}f(d)$ với số thực $x\geq 1$. Tổng ở vế phải bao gồm các hạng tử $f(k)$, với k là số tự nhiên $\leq x$. Với số tự nhiên cho trước $k\leq x$ thì hạng tử $f(k)$ xuất hiện trong tổng $\sum_{d|n}f(d)$ khi và chỉ khi k là ước số của n. Rõ ràng nó xuất hiện nhiều nhất một lần. Số các số tự nhiên $n\leq x$ như vậy là $\left[\frac{x}{k}\right]$. Từ đó số hạng tử $f(k)$ trong tổng lặp là $\left[\frac{x}{k}\right]$ suy ra

(30) $$\sum_{n=1}^{[x]}F(n)=\sum_{k=1}^{[x]}f(k)\left[\frac{x}{k}\right]$$

Đặc biệt nếu $f(n)=n^s$ với s là số nguyên cố định thì $F(n)$ là tổng các lũy thừa bậc s của các ước số tự nhiên của số tự nhiên n. Tổng này thường được ký hiệu là $\sigma_s(n)$. Công thức ***(30)*** suy ra

$\sum_{n=1}^{[x]}\sigma_s(n)=\sum_{k=1}^{[x]}k^s\left[\frac{x}{k}\right]$. Ta có ngay $\sigma_0(n)=d(n),\sigma_1(n)=\sigma(n)$ với $n=1,2,\ldots$ và ta thấy các công thức ***(11)*** và ***(26)*** là các trường hợp riêng của công thức này.

10. Hàm Mobius

Hàm Mobius là các hàm số học $\mu(n)$ xác định bởi các điều kiện

1^0. $\mu(1)=1$

2^0. $\mu(n)=1$ nếu số tự nhiên n chia hết cho bình phương một số tự nhiên >1

3^0. $\mu(n)=(-1)^k$ nếu số tự nhiên n là tích của k số nguyên tố phân biệt

Theo đó $\mu(1)=1,\mu(2)=\mu(3)=-1,\mu(4)=0,\mu(5)=-1,\mu(6)=1,\mu(7)=-1,\ \mu(8)=\mu(9)=0,\mu(10)=1$

Ta trình bày một tính chất của hàm $\mu(n)$: với n là số tự nhiên >1 mà phân tích thành thừa số nguyên tố của nó cho bởi ***(1)*** thì với s là số nguyên cho trước xét tích

(31) $$(1-q_1^s)(1-q_2^s)\ldots(1-q_k^s),$$

Khai triển của tích ***(31)*** chứa hạng tử 1 và các số $\pm d^s$ với d là ước số của n là tích các ước nguyên tố khác nhau. Các dấu + và – của mỗi số tương ứng với việc trong tích đó có chẵn hay lẻ thừa số nguyên tố. Theo tính chất 3^0 ta thấy các hệ số $\pm$ của d^s là bằng $\mu(d)$. Chú ý $\mu(1)\cdot 1^s=1$ và giả thiết d bằng 1 hoặc là tích các số nguyên tố phân biệt (tương đương với việc n không có ước số là bình phương một số tự nhiên >1) thì theo tính chất 2^0 ta thấy tích ***(31)*** bằng tổng $\sum_{d|n}\mu(d)d^s$. Nghĩa là $(1-q_1^s)(1-q_2^s\ldots)(1-q_k^s=)=\sum_{d|n}\mu(d).d^s$, suy ra với $s=0$ ta có

(32) $$\sum_{d|n}\mu(d)=0$$

với mọi số tự nhiên $n>1$. Rõ ràng với $n=1$, ta có $\sum_{d|1}\mu(d)=\mu(1)=1$. Ta thấy nếu $F(n)=\sum_{d|n}\mu(d)$ thì $F(1)=1$ và $F(n)=0$ với các số tự nhiên $n>1$. Hệ quả là ***(30)*** suy ra

(33) $$\sum_{k=1}^{[x]}\mu(k)\left[\frac{x}{k}\right]=1 \text{ với } x\geq 1.$$

Các bất đẳng thức $0\leq t-[t]<1$ đúng với mọi số thực t và vì $|\mu(k)|\leq 1$ với các số tự nhiên k ta thấy $\left|\mu(k)\left[\frac{x}{k}\right]-\mu(k)\frac{x}{k}\right|\leq 1$ với mọi số thực $x\geq 1$ và k là số tự nhiên. Từ đây suy ra nếu ta bỏ đi các ký hiệu [] trong các hạng tử của ***(33)*** thì sai số nhận được là nhỏ hơn 1 và hạng tử thứ nhất đúng bằng với $x-[x]$. Mà có tất cả $[x]-1$ hạng tử trừ ra hạng tử đầu tiên nên ta có $\left|\sum_{k=1}^{[x]}\mu(k)\left[\frac{x}{k}\right]-x\sum_{k=1}^{x}\frac{\mu(k)}{k}\right|<x-[x]+[x]-1=x-1$ suy ra theo ***(33)*** thì $\left|1-x\sum_{k=1}^{x}\frac{\mu(k)}{k}\right|<x-1$ suy ra $\left|x\sum_{k=1}^{[x]}\mu(k)/k\right|\leq x$ do đó $\left|\sum_{k=1}^{[x]}\mu(k)/k\right|\leq 1$. Chứng tỏ mỗi tổng riêng của chuỗi vô hạn

(34) $$\frac{\mu(1)}{1}+\frac{\mu(2)}{2}+\frac{\mu(3)}{3}+\ldots$$

có giá trị ≤ 1. H. von Mangoldt vào năm 1897 đã chứng minh tổng ***(34)*** bằng 0. Euler đã đặt ra giả thuyết này vào năm 1748. Bây giờ ta áp dụng tích Dirichlet cho các chuỗi $\sum_{k=1}^{\infty}\frac{\mu(k)}{k^s}$ và $\sum_{l=1}^{\infty}\frac{1}{l^s}$ với s là số tự nhiên >1. Do $\mu(1)=1$ và từ công thức ***(32)*** ta nhận được $\sum_{k=1}^{\infty}\frac{\mu(k)}{k^s}.\sum_{l=1}^{\infty}\frac{1}{l^s}=1$ nghĩa là công thức $\sum_{k=1}^{\infty}\frac{\mu(k)}{k^s}=\frac{1}{\zeta(s)}$ với s là số thực >1. Đặc biệt $\xi(2)=\pi^2/6$, đẳng thức cuối cùng suy ra $\sum_{k=1}^{\infty}\frac{\mu(k)}{k^2}=\frac{6}{\pi^2}$. Trong mối liên hệ này ta thấy dễ dàng chứng minh đẳng thức $\sum_{k=1}^{\infty}\frac{\mu^2(k)}{k^s}=\frac{\xi(s)}{\xi(2s)}$ với s là số thực >1. Rút gọn chuỗi lặp $\sum_{k=1}^{\infty}\sum_{l=1}^{\infty}\mu(k)x^{kl}$ thành chuỗi lũy thừa bằng phương pháp tương tự như đối với chuỗi ***(29)***, với $|x|<1$ ta nhận được công thức $\sum_{n=1}^{\infty}\frac{\mu(n)x^n}{1-x^n}=x$.

Định lý 6. *Với mọi hàm số học* $F(n)$ *tồn tại duy nhất một hàm số học* $f(n)$ *mà với mọi số tự nhiên* n *ta có*

(35) $$F(n)=\sum_{d|n}f(d)$$

Chứng minh. Nếu với $n=1,2,\ldots,$ công thức ***(35)*** đúng thì dãy vô hạn các đẳng thức sau là đúng

(36)
$$\begin{aligned}
F(1) &= f(1),\\
F(2) &= f(1)+f(2),\\
F(3) &= f(1)+f(3),\\
F(4) &= f(1)+f(2)+f(4),\\
F(5) &= f(1)+f(5),\\
F(6) &= f(1)+f(2)+f(3)+f(6)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Đẳng thức đầu tiên cho $f(1)=F(1)$. Do đó $f(2)$ có thể tính dựa vào đẳng thức thứ hai. Khi đó vì $f(1)$ và $f(2)$ đã được tính nên $f(3)$ tính được dựa vào đẳng thức thứ ba và cứ như vậy. Đẳng thức thứ n cho giá trị của $f(n)$ dựa vào các giá trị $f(k)$ với $k<n$ đã được tính. Do đó tồn tại hàm thỏa mãn ***(35)*** suy ra tồn tại duy nhất một hàm như vậy. Mặt khác dễ thấy từ các tính toán giá trị $f(1), f(2), \ldots$ từ ***(36)*** ta nhận được hàm $f(n)$ thỏa mãn ***(36)*** và do đó thỏa mãn ***(35)***. Định lý được chứng minh. □

Các phương trình ***(36)*** cho ta cách tính $f(n)$ dựa vào $F(1),F(2),\ldots,F(n)$.

Công thức tổng quát hơn là

(37) $$f(n)=\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)$$

Hoặc có thể viết dưới dạng

(38) $$f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)$$

Hoặc

(39) $$f(n)=\sum_{kl=n}\mu(k)F(l),$$

Trong đó tổng được lấy với mọi cặp k,l các số tự nhiên mà $kl=n$. Để chứng minh các công thức này chỉ cần chứng minh hàm xác định bởi ***(39)*** thỏa mãn ***(35)*** với mọi số tự nhiên *n*. Thật vậy từ ***(39)*** suy ra $\sum_{d|n} f(d)=\sum_{d|n}\sum_{kl=d}\mu(k)F(l)=\sum_{lk|n}\mu(k)F(l) =\sum_{l|n}F(l)\sum_{k|n/l}\mu(k)=F(n)$ vì theo tính chất của μ ta có $\sum_{k|n/l}\mu(k)$ là khác 0 (do đó bằng 1) chỉ khi $n/l=1$ nghĩa là $l=n$. Đặc biệt với $F(1)=1$ và $F(n)=0, n=2,3,\ldots,$ Định lý 6 suy ra tồn tại duy nhất hàm f, gọi là hàm Mobius, $\mu(n)=f(n),$ mà $f(1)=1,\ \sum_{d|n} f(d)=0$ với $n=2,3,\ldots$

11. Hàm Liouville $\lambda(n)$

Hàm Liouville là hàm số học xác định bởi các điều kiện

$1^0.\ \lambda(1)=1$

$2^0.\ \lambda(n)=(-1)^{\alpha_1+\alpha_2+\ldots+\alpha_k}$ nếu n có phân tích thành thừa số nguyên tố dạng ***(1)***

Ta có $\lambda(1)=1,\lambda(2)=\lambda(3)=-1,\lambda(4)=1,\lambda(5)=-1,\lambda(6)=1,\lambda(7)=\lambda(8)=-1,\lambda(9)=\lambda(10)=1.$

Giả sử với số tự nhiên $n>1$ có phân tích thành thừa số nguyên tố dạng ***(1)***.

Xét tích $\prod_{t=1}^{k}\left(1-q_i^s+q_i^{2s}-q_i^{3s}+\ldots+(-1)^{\alpha_i}q_i^{\alpha_i s}\right)$ với s là số nguyên tùy ý. Khai triển tích ta nhận được tổng đại số của các hạng tử $\left(q_1^{\lambda_1}q_2^{\lambda_2}\ldots q_k^{\lambda_k}\right)^s$ với hệ số tương ứng $(-1)^{\lambda_1+\ldots+\lambda_2}=\lambda\left(q_1^{\lambda_1}q_2^{\lambda_2}\ldots q_k^{\lambda_k}\right)$ trong đó tổng lấy trên tập mọi các ước số $d=q_1^{\lambda_1}q_2^{\lambda_2}\ldots q_k^{\lambda_k}$ của n. Hệ quả là tích bằng $\sum_{d|n}\lambda(d)d^s$.

Mặt khác ta có công thức tổng chuỗi lũy thừa $1-q_i^s+q_i^{2s}-q_i^{3s}+\ldots+(-1)^{\alpha_i}q_i^{\alpha_i s}=\frac{1+(-1)^{\alpha_i}q_i^{(\alpha_i+1)s}}{1+q_i^s}$ và sử dụng công thức này cho các nhân tử của tích ta có $\prod_{i=1}^{k}\frac{1+(-1)^{\alpha_i}q_i^{(\alpha_i+1)s}}{1+q_i^s}=\sum_{d|n}\lambda(d)d^s$. Đặc biệt với $s=0$

(40) $$\frac{1+(-1)^{\alpha_1}}{2}\cdot\frac{1+(-1)^{\alpha_2}}{2}\cdot\frac{1+(-1)^{\alpha_k}}{2}=\sum_{d|n}\lambda(d).$$

Số $\frac{1+(-1)^{\alpha}}{2}$ bằng 0 hoặc 1 tùy thuộc α lẻ hay chẵn. Do vế trái của ***(40)*** khác 0 (do đó bằng 1) khi và chỉ khi tất cả các lũy thừa $\alpha_1,\alpha_2,\ldots\alpha_k,$ là chẵn, nghĩa là n là bình phương một số tự nhiên. Ta có định lý

Định lý 7. *Tổng* $\sum_{d|n}\lambda(d)$ *bằng 0 trong trường hợp* n *là bình phương một số tự nhiên hoặc bằng 1.*

Trong chứng minh Định lý 7 ta đã giả sử $n>1$ nhưng định lý vẫn đúng với $n=1$ vì $\lambda(1)=1$. Đặt $F(n)=\sum_{d|n}\lambda(d)$ hệ quả là $F(n)=1$ đúng với mọi n là bình phương một số tự nhiên và $F(n)=0$ trong các trường hợp khác. Theo ***(30)*** (với $f(n)=\lambda(k)$) ta nhận được $\sum_{k=1}^{[x]}\lambda(k)\left[\frac{x}{k}\right]=\sum_{n=1}^{[x]}F(n)$

với mọi $x \geq 1$. Tổng trong vế phải chứa số các hạng tử bằng 1 đúng bằng số các tự nhiên $\leq x$ mà là bình phương. Do đó tổng này bằng $\left[\sqrt{x}\right]$. Vì vậy $\sum_{k=1}^{[x]} \lambda(k)\left[\frac{x}{k}\right] = \left[\sqrt{x}\right]$ với $x \geq 1$.

CHƯƠNG 5

ĐỒNG DƯ

1. Đồng dư và các tính chất

Giả sử a và b là các số nguyên. Ta nói rằng *a đồng dư với b theo modulo m* nếu hiệu của a và b chia hết cho m. Sử dụng ký hiệu được đề xuất bởi Gauss ta viết

(1) $$a \equiv b \pmod{m}$$

Công thức ***(1)*** tương đương với $m \mid a-b$

Rõ ràng nếu hai số nguyên là đồng dư modulo m thì chúng có cùng số dư khi chia cho m.

Ký hiệu đồng dư $\equiv$ được sử dụng khá giống ký hiệu $=$

Ta liệt kê dưới đây một số mối liên hệ giữa các đồng dư thức và các đẳng thức

I. *Tính phản xạ:* mọi số nguyên là đồng dư với chính nó theo mọi modulo, nghĩa là $a \equiv a \pmod{m}$ với mọi số nguyên a và mọi số tự nhiên m vì rõ ràng $a-a=0$ chia hết cho mọi số tự nhiên m.

II. *Tính đối xứng:* đồng dư thức ***(1)*** tương đương với đồng dư thức $b \equiv a \pmod{m}$ vì rõ ràng các số a – b và b – a cùng chia hết hoặc cùng không chia hết cho *m*

III. *Tính kết hợp:* nếu $a \equiv b \pmod{m}$ và $b \equiv c \pmod{m}$ thì $a \equiv c \pmod{m}$ vì ta có đẳng thức $a-c=(a-b)+(b-c)$ và lưu ý tổng của hai số chia hết cho m là một số chia hết cho m.

Ta có một số tính chất khác của đồng dư sau đây.

Ta chứng minh hai đồng dư thức với cùng modulo có thể cộng hoặc trừ tương ứng các vế. Thật vậy giả sử

(2) $$a \equiv b \pmod{m} \text{ và } c \equiv d \pmod{m}.$$

Để chứng minh $a+c \equiv b+d \pmod{m}$ và $a-c \equiv b-d \pmod{m}$ ta lưu ý các đẳng thức $(a+c)-(b+d)=(a-b)+(c-d)$ và $(a-c)-(b-d)=(a-b)-(c-d)$. Tương tự sử dụng đẳng thức $ac-bd=(a-b)c+(c-d)b,$ ta chứng minh được từ ***(2)*** suy ra đồng dư thức $ac \equiv bd \pmod{m}$. *Hệ quả là ta có thể nhân theo vế hai đồng dư thức với cùng modulo.*

Các định lý về các tính chất cộng, trừ, nhân các đồng dư thức ở trên có thể mở rộng cho hữu hạn các đồng dư thức.

Định lý về phép cộng các đồng dư thức chứng tỏ ta có thể chuyển vế đối dấu mọi hạng tử trong một đồng dư thức bởi vì phép toán này tương đương với việc trừ các hạng tử trong cả hai vế.

Từ tính chất phép nhân các đồng dư thức chứng tỏ có thể nhân một đồng dư thức với mọi số nguyên tùy ý và do đó ta có thể lũy thừa cả hai vế của đồng dư thức với số mũ bất kỳ.

Tuy nhiên ta không thể chia một đồng dư thức cho một đồng dư thức khác (ngay cả khi thương số là các số nguyên). Chẳng hạn $48 \equiv 18 \pmod{10}$ và $12 \equiv 2 \pmod{10}$ nhưng không có $4 \equiv 9 \pmod{10}$.

Do một ước số của ước số của một số nguyên cũng là ước số của số nguyên đó nên nếu $d \mid m$ thì đồng dư thức $a \equiv b \pmod{m}$ chứng tỏ $a \equiv b \pmod{d}$.

Tính kết hợp của các đồng dư thức cùng với tính chất cộng và nhân các đồng dư thức chứng tỏ trong đồng dư thức cho trước ta có thể thay mọi hạng tử hoặc nhân tử bởi các số đồng dư với nó.

Quy tắc này không đúng với các lũy thừa. Chẳng hạn đồng thức thức $2^6 \equiv 4(\mathrm{mod}\,5)$ không thể thay thế bởi đồng dư thức $2^1 \equiv 4(\mathrm{mod}\,5)$ mặc dù $6 \equiv 1(\mathrm{mod}\,5)$.

Giả sử $f(x) = A_0x^n + A_1x^{n-1} + ... + A_{n-1} + A_n$ là đa thức bậc n với hệ số nguyên. Ký hiệu m là số tự nhiên và a, b là các số nguyên thỏa mãn $a \equiv b(\mathrm{mod}\,\mathrm{m})$. Từ định lý về các lũy thừa tự nhiên và tính chất nhân các đồng dư thức suy ra

$$A_0a^n \equiv A_0b^n (\mathrm{mod}\,m),$$
$$A_1a^{n-1} \equiv A_1b^{n-1} (\mathrm{mod}\,m),$$
$$...$$
$$A_{n-1}a \equiv A_{n-1}b(\mathrm{mod}\,m),$$
$$A_n \equiv A_n (\mathrm{mod}\,m).$$

Cộng lại ta có $A_0a^n + A_1a^{n-1} + ... + A_{n-1}a + A_n \equiv A_0b^n + A_1b^{n-1} + ... + A_{n-1}b + A_n (\mathrm{mod}\,m)$. Nghĩa là $f(a) \equiv f(b)(\mathrm{mod}\,m)$. Ta đã chứng minh được

Định lý 1. *Nếu $f(x)$ là đa thức một biến x với hệ số nguyên thì đồng dư thức $a \equiv b(mod\ m)$ suy ra đồng dư thức $f(a) \equiv f(b)(\mathrm{mod}\,m)$.*

Định lý 1 cho ta quy tắc cho biết một số có chia hết cho 9,7,11,13,27,37 hay không.

Ký hiệu N là số tự nhiên. Biểu diễn của N trong hệ thập phân được cho bởi biểu diễn có dạng $N = c_1 10^{n-1} + c_2 10^{n-2} + ... + c_{n-1}10 + c_n$. Đặt

(3) $$f(x) = c_1x^{n-1} + c_2x^{n-2} + ... + c_{n-1}x + c_n$$

Khi đó $f(x)$ là đa thức hệ số nguyên và

(4) $$f(10) = N$$

Theo Định lý 1 thì vì $10 \equiv 1(\mathrm{mod}\,9)$ ta có

(5) $$f(10) \equiv f(1)(\mathrm{mod}\,9).$$

Nhưng $f(1) = c_1 + c_2 + ... + c_n$ và hệ quả là theo ***(4)*** và ***(5)*** thì $N \equiv c_1 + c_2 + ... + c_n (\mathrm{mod}\,9)$ chứng tỏ mọi số tự nhiên N sai khác tổng các chữ số của nó trong hệ cơ số 10 một bội số của 9. Do đó N *chia hết cho 9 khi và chỉ khi tổng các chữ số của nó chia hết cho 9.* Tổng quát hơn nếu ký hiệu S_N là tổng các chữ số của N (trong hệ thập phân) thì với các số tự nhiên N và N' ta có $N \equiv s_N (\mathrm{mod}\,9)$, $N' \equiv s_{N'} (\mathrm{mod}\ 9)$ suy ra $NN' \equiv s_N s_{N'} (\mathrm{mod}\ 9)$. Vì $NN' \equiv s_{NN'} (\mathrm{mod}\ 9)$ nên $s_{NN'} \equiv s_N s_{N'} (\mathrm{mod}\ 9)$.

Từ ***(3)*** và đồng dư thức $10 \equiv -1(\mathrm{mod}\ 11)$, Định lý 1 suy ra $f(10) \equiv f(-1)(\mathrm{mod}\ 11)$, do đó theo ***(4)*** và ***(3)*** ta có $(-1)^{n-1} N \equiv c_1 - c_2 + c_3 - c_4 + ...(\mathrm{mod}11)$. Từ đây ta nhận được quy tắc về tính chia hết cho 11. Bây giờ ta tìm các quy tắc về tính chia hết cho 7 hoặc 13.

Ký hiệu $(c_1, c_2, ..., c_n)_{10}$ là số trong hệ thập phân có các chữ số là $c_1, c_2, ..., c_n$ (ký hiệu này là cần thiết để phân biệt với tích các chữ số $c_1, c_2, ..., c_n$). Mọi số tự nhiên đều có dạng $N = (c_{n-2}c_{n-1}c_n)_{10} + (c_{n-5}c_{n-4}c_{n-3})_{10}.1000 + (c_{n-8}c_{n-7}c_{n-6})_{10}.1000^2 + ...$ Vì $1000 \equiv -1(\mathrm{mod}\ 7)$ và

$1000 \equiv -1 (\mathrm{mod}\, 13)$ nên ta có $N \equiv (c_{n-2}c_{n-1}c_n)_{10} - (c_{n-5}c_{n-6}c_{n-7})_{10} + (c_{n-8}c_{n-7}c_{n-6})_{10} - ... (\mathrm{mod}\, 7)$ và đồng dư thức tương tự cũng nhận được khi thay modulo 7 bởi modulo 13.

Các đồng dư thức này cũng cho ta biết quy tắc về tính chia hết cho 7 hoặc 13. Chẳng hạn ta có $N = 8589879056 \equiv 56 - 879 + 589 - 8$ theo cả modulo 7 và modulo 13. Vì số trong vế phải các đồng dư thức này (bằng -242) là không chia hết cho cả 7 lẫn 13 nên N không chia hết cho cả 7 lẫn 13.

Các quy tắc với 27 và 37 được dựa trên tính chất $100 \equiv 1$ theo $\mathrm{mod}\, 27$ và $\mathrm{mod}\, 37$. Từ đây ta nhận được các quy tắc tương tự với các trường hợp ở trên. Chẳng hạn ta có $N = 24540509 \equiv 509 + 540 + 24$ theo $\mathrm{mod}\, 27$ và $\mathrm{mod}\, 37$. Số trong vế phải là 1073 có thể viết thành $1073 \equiv 73 + 1$ theo $\mathrm{mod}\, 27$ và $\mathrm{mod}\, 37$. Số 74 chia hết cho 37 nhưng không chia hết cho 27 và do đó số N cũng chia hết cho 37 nhưng không chia hết cho 27.

Bài tập. ***1***. Tìm hai chữ số tận cùng của số 2^{1000}.

Lời giải. Ta có $2^{10} = 1024 \equiv 24 (\mathrm{mod}\, 100)$ vì vậy $2^{20} \equiv 24^2 \equiv 76 (\mathrm{mod}\, 100)$. Nhưng $76^2 \equiv 76 (\mathrm{mod}\, 100)$ suy ra theo quy nạp $76^k \equiv 76 (\mathrm{mod}\, 100)$, $k = 1, 2, ...$ Do đó $2^{1000} = 2^{20.50} \equiv 76^{50} \equiv 76 (\mathrm{mod}\, 100)$. Vậy hai chữ số tận cùng của 2^{1000} là 7 và 6.

2. Chứng minh rằng ít nhất một trong sáu đồng dư thức sau là đúng (Erdos [10]): 1) $x \equiv 0 (\mathrm{mod}\, 2)$, 2) $x \equiv 0 (\mathrm{mod}\, 3)$, 3) $x \equiv 1 (\mathrm{mod}\, 4)$, 4) $x \equiv 3 (\mathrm{mod}\, 8)$, 5) $x \equiv 7 (\mathrm{mod}\, 12)$, 6) $x \equiv 23 (\mathrm{mod}\, 24)$ với số nguyên x bất kỳ.

Chứng minh. Nếu số nguyên x không thỏa mãn cả 1) và 2) thì nó không chia hết cho 2 và 3 do đó có dạng $24t +$ r với t là số nguyên và r là một trong các số 1,5,7,11,13,17,19,23. Khi đó dễ dàng kiểm tra số $x = 24t + r$ thỏa mãn các đồng dư thức 3),3),5),4),3),3),4),6) tương ứng. □

Ghi chú. P.Erdos [10] đã đặt ra bài toán sau đây: cho trước số tự nhiên n, có tồn tại hay không tập hợp hữu hạn các đồng dư thức với modulo phân biệt lớn hơn n mà mọi số nguyên thỏa mãn ít nhất một trong số chúng? H.Davenport [2] đặt ra giả thuyết rằng câu trả lời là khẳng định nhưng sẽ không có một lời giải đơn giản. P.Erdos đã tự chứng minh giả thuyết này trong trường hợp $n = 2$ bằng cách sử dụng một số đồng dư thức với modulo là ước số của 120. D.Swift đã cho lời giải với $n = 3$ bằng cách sử dụng các đồng dư thức với modulo là ước số của 2880. Giả thuyết đã được chứng minh với mọi $n < 20$ (Choi [1]).

3. Tìm hai chữ số tận cùng của số 9^{9^9}.

Lời giải. Theo modulo 100 thì $9^2 \equiv 81, 9^4 \equiv 81^2 \equiv 61, 9^8 \equiv 61^2 \equiv 21, 9^9 \equiv 21.9 \equiv 89, 9^{10} \equiv 89.9 \equiv 1.$ Ta có $9^9 \equiv 9 (\mathrm{mod}\ 10)$ suy ra $9^9 = 10k + 9$ với k là số tự nhiên. Vì vậy từ $9^{10} \equiv 1 (\mathrm{mod}\, 100)$ suy ra $9^{9^9} = 9^{10k+9} \equiv 9^9 \equiv 89 (\mathrm{mod}\ 100)$ chứng tỏ chữ số tận cùng của 9^{9^9} là 9 và chữ số liền trước đó là 8.

4. Tìm hai chữ số tận cùng của số 9^{9^9}.

Lời giải. Từ bài tập 3 suy ra $9^{9^9} \equiv 9 (\mathrm{mod}\ 10)$ do đó $9^{9^9} = 10t + 9$ với t là số tự nhiên. Suy ra $9^{9^9} = 9^{10t+9} \equiv 9^9 \equiv 89 (\mathrm{mod}\ 100)$. Vì vậy hai chữ số tận cùng của 9^{9^9} là hai chữ số tận cùng của 9^{9^9}.

Ghi chú. Theo W.Lietzmann ([1] trang 118) thì số các chữ số của số này lớn hơn một phần tư của một triệu. Gauss đã gọi số này là số lớn vô hạn.

2. Nghiệm của các đồng dư thức và hệ thặng dư đầy đủ

Ký hiệu $f(x)$ là đa thức bậc n với hệ số nguyên và m là modulo cho trước. Tất cả các số a mà $f(a) \equiv 0 (\mathrm{mod}\, m)$ được gọi là nghiệm của đồng dư thức

(6) $$f(x)\equiv 0(\mathrm{mod}\, m)$$

Từ Định lý 1 suy ra nếu a là nghiệm của đồng dư thức ***(6)*** thì mọi số đồng dư với a theo modulo m cũng là nghiệm của ***(6)***. Do đó có thể coi lớp tất cả các số có cùng đồng dư là một nghiệm đơn của đồng dư thức. Nghiệm đơn này có thể được chọn bởi mọi số trong đó.

Mọi số nguyên là đồng dư theo modulo m với một trong các số thuộc dãy

(7) $$0,1,2,\ \ldots,m-1.$$

Thật vậy, ký hiệu a là số nguyên cho trước và $r=a-m\left[\dfrac{a}{m}\right]$. Số r đồng dư với a theo modulo m.

Vì $t-1<[t]\le t$ với mọi số thực t nên ta có $\dfrac{a}{m}-1<\left[\dfrac{a}{m}\right]\le\dfrac{a}{m}$, suy ra $0\le r<m$. Vì vậy r thuộc dãy ***(7)*** và do đó mọi số tự nhiên a là đồng dư theo modulo m với ít nhất một trong các phần tử thuộc dãy ***(7).*** Mặt khác, các phần tử thuộc ***(7)*** là các đồng dư phân biệt modulo m nên mọi số nguyên a đồng dư với đúng một phần tử thuộc ***(7)***. Số này gọi là số dư của a theo modulo m.

Tất cả các số nguyên có cùng số dư r modulo m đều có dạng $mk + r$ với k là số nguyên.

Để giải đồng dư thức ***(6)*** ($f(x)$ là đa thức hệ số nguyên) ta chỉ cần tìm các số trong dãy ***(7)*** là nghiệm của đồng dư thức đó. Vậy ***(6)*** có thể được giải sau hữu hạn phép thử. Do đó về lý thuyết ta có thể tìm mọi nghiệm của ***(6)*** (*f (x)* là đa thức hệ số nguyên) hoặc chứng minh *f (x)* vô nghiệm.

Ví dụ. ***1***. Giải đồng dư thức

(8) $$x^5-3x^2+2\equiv 0(\mathrm{mod}\, 7).$$

Ta sẽ tìm xem trong các số 0,1,2,3,4,5,6 thì số nào thỏa mãn ***(8)***. Lần lượt thế 0 và 1 vào ***(8)*** ta thấy 1 là nghiệm và 0 không phải nghiệm của ***(8)***. Tương tự 2 không phải nghiệm. Ta có $3^2\equiv 2(\mathrm{mod}\, 7)$ suy ra $3^4\equiv 4(\mathrm{mod}\, 7)$ và $3^5\equiv 12\equiv 5(\mathrm{mod}\, 7)$. Do đó $3^5-3.3^2+2\equiv 5-3.2+2\equiv 1(\mathrm{mod}\, 7)$ và vì vậy 3 không phải nghiệm. Với 4 ta có $4k\equiv -3(\mathrm{mod}\, 7)$ suy ra $4^5\equiv -3^5\equiv -5(\mathrm{mod}\, 7)$ và do đó $4^5-3.4^2+2\equiv -5-3.2+2\equiv 3(\mathrm{mod}\, 7)$ nên 4 không phải nghiệm của ***(8)***. Ta có $5\equiv -2(\mathrm{mod}\, 7)$ suy ra $5^5\equiv -2^5\equiv 3(\mathrm{mod}\, 7)$ và $5^5-3.5^2+2\equiv 3-3.4+2\equiv 0(\mathrm{mod}\, 7)$ do đó 5 là nghiệm. Ta có $6\equiv -1(\mathrm{mod}\, 7)$ suy ra $6^5-3.6^2+2\equiv -1-3+2\equiv 5(\mathrm{mod}\, 7)$ nên 6 không phải nghiệm. Vậy đồng dư thức ***(8)*** có hai nghiệm là 1 và 5. Do đó các số nguyên x thỏa mãn ***(8)*** đều có dạng $7k+1$ hoặc $7k+5$ với k là số nguyên tùy ý.

2. Giải đồng dư thức

(9) $$x^2+x\equiv 0(\mathrm{mod}\, 2)$$

Ta chỉ cần kiểm tra xem ***(9)*** có đúng với 0 hoặc 1 hay không. Cả hai trường hợp đều thỏa mãn suy ra mọi số nguyên x đều là nghiệm của ***(9)***. Kết quả này cũng được suy ra từ tính chất x^2 và x có cùng tính chẵn lẻ và do đó tổng của chúng luôn chẵn. Ta nói đồng dư thức đúng với mọi số nguyên.

Đây là một ví dụ cho thấy một đồng dư thức có thể luôn đúng cho dù các hệ số không phải bội số của modulo. Một ví dụ khác là đồng dư thức $x^3-x\equiv 0(\mathrm{mod}\, 3)$. Thật vậy $x^3-x=(x-1)x(x-1)$ là tích của ba số nguyên liên tiếp nên trong đó có một số chia hết cho 3 và vì vậy tích của chúng chia hết cho 3. Ta có $x^3-x\equiv 0(\mathrm{mod}\, 3)$ với mọi số nguyên x.

3. Do ***(9)*** luôn đúng nên đồng dư thức $x^2+x+1\equiv 0\pmod 2$ không có nghiệm. Tương tự đồng dư thức $x^2\equiv 3\pmod 8$ cũng không có nghiệm nguyên x vì bình phương một số lẻ chia 8 dư 1 và bình phương một số chẵn chia 8 dư 0 hoặc 4.

Kí hiệu m là modulo cho trước, k là số tự nhiên cho trước $<m$ và $a_1,a_2,\ldots,a_k$ là các số nguyên không âm $<m$. Câu hỏi đặt ra là khi nào thì đồng dư thức $f(x)\equiv 0\pmod m$ ($f(x)$ là đa thức hệ số nguyên) có tất cả các nghiệm là $a_1,a_2,\ldots,a_k$ (và các đồng dư của chúng modulo m).

Nếu m là số nguyên tố thì rõ ràng hàm cần tìm là $f(x)=(x-a_1)(x-a_2)\ldots(x-a_k)$.

Nếu $m=4$ và $a_1,a_2,\ldots,a_k$, $k\le 4$, là các số nguyên không âm cho trước <4 thì các nghiệm của đồng dư $(x-a_1)(x-a_2)\ldots(x-a_k)\equiv 0\pmod 4$ là các số $a_1,a_2,\ldots,a_k$ (và các đồng dư của chúng theo mobulo 4). Tuy nhiên M.Chojnacka Pniewska [1] đã chứng minh rằng không tồn tại đa thức $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ mà $f(x)\equiv 0\pmod 6$ thỏa mãn với 2 và 3 nhưng không thỏa mãn với mọi số nguyên <6 khác. Thật vậy, giả sử $f(x)$ có tính chất đó. Khi đó $f(2)\equiv f(3)\equiv 0\pmod 6$ suy ra $3f(2)-3f(3)\equiv 0\pmod 6$. Ta có $3.2^k\equiv 2.3^k\equiv 0\pmod 6$ với mọi $k=1,2,\ldots$ nên $3f(2)\equiv 3a_n\pmod 6$ và $2f(3)\equiv 2a_n\pmod 6$. Do đó $3f(2)-2f(3)\equiv a_n\pmod 6$ suy ra $a_n\equiv 0\pmod 6$ nên $f(0)\equiv 0\pmod 6$. Ta đã chứng minh đồng dư thức $f(x)\equiv 0\pmod 6$ có nghiệm $x=0$, mâu thuẫn với giả thiết 2 và 3 là tất cả các nghiệm.

Có thể chứng minh rằng (Sierpinski [15]) nếu m là hợp số $\ne 4$ thì tồn tại hai số nguyên a và b không có cùng số dư khi chia cho m và nếu $f(x)$ là đa thức hệ số nguyên thì đồng dư thức $f(a)\equiv f(b)\equiv 0\pmod m$ kéo theo đồng dư thức $f(0)\equiv 0\pmod m$. Từ đây suy ra nếu m là hợp số $\ne 4$ thì tồn tại đa thức bậc hai $f(x)=x^2+a_1x+a_2$ với hệ số nguyên mà đồng dư thức $f(x)\equiv 0\pmod m$ có nhiều hơn hai nghiệm.

Đây là một tính huống khá giống nhau giữa lý thuyết các đồng dư thức và lý thuyết các phương trình Diophante tuyến tính một biến. Thật vậy, số nguyên x thỏa mãn đồng dư thức ***(6)*** khi và chỉ khi tồn tại số nguyên y thỏa mãn $f(x)=my$. Vì vậy đồng dư thức $f(x)\equiv 0\pmod m$ tương đương với phương trình Diophante $f(x)-my=0$.

Với những lập luận tương tự ta chứng minh được một đồng dư thức mà vế trái là một đa thức nhiều biến hệ số nguyên và vế phải là một số cho trước là giải được về lý thuyết. Chẳng hạn đối với đồng dư thức $f(x,y)\equiv 0\pmod m$ với $f(x)$ là đa thức với các biến x,y thì chỉ cần tìm xem trong m^2 bộ số x,y với x và y nhận mọi giá trị $0,1,\ldots,m-1$ thì bộ số nào thỏa mãn đồng dư thức đó. Các phép thử này có thể làm đơn giản hơn dựa vào nhận xét nếu $a\equiv c\pmod m$ và $b\equiv d\pmod m$ thì $f(a,b)\equiv f(c,d)\pmod m$. Một ví dụ đơn giản là xét đồng dư thức $x^4+y^4\equiv 1\pmod 5$. Tất cả các nghiệm của phương trình này là $(x,y)=(0,1),(0,2)(0,3),(0,4),(1,0),(2,0),(3,0),(4,0)$. Vì vậy trong mọi nghiệm của nó có đúng một số chia hết cho 5. Đồng dư thức $x^3+y^3+z^3\equiv 4\pmod 9$ vô nghiệm vì lập phương của một số nguyên thì đồng dư với $0,1,-1$ theo modulo 9 và do đó tổng của ba lập phương không thể đồng dư với 4.

3. Nghiệm của đa thức và nghiệm của đồng dư thức

Nếu phương trình $f(x,y)=0$ với $f(x,y)$ là đa thức hệ số nguyên có các nghiệm nguyên x,y thì rõ ràng với mọi số tự nhiên m đều tồn tại các số nguyên x,y mà số $f(x,y)$ chia hết cho m, nghĩa là đồng dư thức $f(x,y)\equiv 0(\mathrm{mod}\, m)$ có nghiệm tự nhiên m. Vì vậy nếu tồn tại modulo m mà đồng dư thức $f(x,y)\equiv 0(\mathrm{mod}\, m)$ không có nghiệm nguyên thì phương trình $f(x,y)=0$ cũng không có nghiệm nguyên.

Ví dụ với mọi số tự nhiên n thì phương trình $x^2+1-3y^n=0$ không có nghiệm nguyên vì $x^2+1-3y^n\equiv 0(\mathrm{mod}\, 3)$ không có nghiệm. Thật vậy, vì một bình phương của số nguyên thì chia 3 dư 0 hoặc 1, do đó vế trái của đồng dư thức chia 3 dư 1 hoặc 2.

Tuy nhiên nếu phương trình $f(x,y)=0$ không có nghiệm với $f(x,y)$ là đa thức hệ số nguyên thì không suy ra tồn tại modulo m mà đồng dư thức $f(x,y)\equiv 0(\mathrm{mod}\, m)$ vô nghiệm. Chẳng hạn phương trình $(2x-1)(3y-1)=0$ không có nghiệm nguyên nhưng đồng dư thức $(2x-1)(3y-1)\equiv 0(\mathrm{mod}\, m)$ lại có nghiệm với mọi số tự nhiên m. Thật vậy, mọi số tự nhiên m đều có thể biểu diễn được dưới dạng $m=2^{k-1}(2x-1)$ với k,x là các số tự nhiên. Số $2^{2k-1}+1$ chia hết cho $2+1=3$ và do đó tồn tại số tự nhiên y thỏa mãn $2^{2k-1}+1=3y$. Do đó $(2x-1)(3y-1)=2^{k+2}m$ và từ đây suy ra đồng dư thức ở trên là giải được. Dễ dàng chứng minh kết luận tổng quát và chặt hơn: *nếu a_1,a_2 là các số tự nhiên mà $(a_1,a_2)=1, b_1,b_2$ là các số nguyên tùy ý thì đồng dư thức $(a_1x+b_1)(a_2y+b_2)\equiv 0(\mathrm{mod}\, m)$ là giải được với mọi số tự nhiên m* (Skolem [1]).

Dễ dàng chứng minh phương trình $2x^2-219y^2=1$ không có nghiệm nguyên x,y bởi vì đồng dư thức $2x^2-219y^2\equiv 1(\mathrm{mod}\, 3)$ là không giải được (thật vậy, nếu x là số nguyên, x^2 chia 3 dư 0 hoặc 1 và do đó vì $219=3\cdot 73$, số $2x^2-219y^2$ chia 3 dư 0 hoặc 2).

Khó hơn một chút để chứng minh phương trình $2x^2-219y^2=-1$ không có nghiệm nguyên. T.Nagell [7] đã suy ra kết luận này bằng cách sử dụng một định lý tổng quát hơn với chứng minh rất khó. Tuy nhiên đồng dư thức $2x^2-219y^2\equiv -1(\mathrm{mod}\, m)$ (tài liệu đã dẫn trang 62) là giải được với mọi số tự nhiên m.

Ta trình bày chứng minh trực tiếp phương trình $2x^2-219y^2=-1$ là không có nghiệm nguyên x,y. Giả sử phản chứng phương trình này có nghiệm nguyên. Khi đó các số x,y đều khác 0. Ta giả sử các số này đều dương. Hơn nữa giả sử x,y được chọn với y nhỏ nhất có thể. Đặt $x_1=|293x-3066y|$, $y_1=-28x+293y$. Khi đó $2x_1^2-219y_1^2=2x^2-219y^2$. Hệ quả là x_1,y_1 thỏa mãn phương trình. Ta không thể có $x_1=0$ và do đó x_1 là số tự nhiên. Ta cũng không thể có $y_1\le 0$ vì nếu ngược lại thì $x\ge\frac{293}{28}y$ suy ra $x^2\ge\frac{85849}{784}y^2$ và do đó $2x^2-219y^2\ge\frac{y^2}{392}$ nên $-1\ge\frac{y^2}{392}$, vô lý. Vậy x_1,y_1 là các số tự nhiên. Theo giả thiết thì $y\le y_1$ nên $-28x+293y\ge y$ suy ra $x\le\frac{292}{28}y=\frac{73}{7}y$ vì vậy $x^2\le\frac{539}{49}y^2$ và $2x^2-219y^2\le\frac{-73}{49}y^2\le-\frac{73}{49}<-1$, mâu thuẫn với giả thiết x,y là nghiệm của phương trình. Vậy phương trình không có nghiệm nguyên x,y.

Bây giờ ta chứng minh rằng đồng dư thức $2x^2-219y^2\equiv -1(\mathrm{mod}\, m)$ là giải được với mọi số tự nhiên m. Với m là số tự nhiên đặt $m=m_1.m_2$ với $m_1=11^\alpha$ (α nguyên ≥ 0) và $(m_2,11)=1$. Đặt

$x_1 = 5.13^{\varphi(m_1)-1}, y_1 = 13^{\varphi(m_1-1)}$. Vì $(13, m_1) = 1$ nên theo định lý Euler (Chương 6) thì $13^{\varphi(m_1)} \equiv 1 (\mathrm{mod}\, m_1)$. Do đó $13^2 \left(2x_1^2 - 219y_1^2\right) = 2 \cdot 25 \cdot 13^{2\varphi(m_1)} \equiv 2 \cdot 25 - 219 \equiv -13^2 (\mathrm{mod}\, m_1)$ suy ra vì $(13, m_1) = 1$ ta có $2x_1^2 - 219y_1^2 \equiv -1 (\mathrm{mod}\, m_1)$. Đặt $x_2 = 7.11^{\varphi(m_2)-1}, y_2 = 11^{\varphi(m_2)-1}$. Vì $(11, m_2) = 1$ nên $11^{\varphi(m_2)} \equiv 1 (\mathrm{mod}\, m_2)$ vậy $11^2 \left(2x_2^2 - 219y_2^2\right) = 2.49.11^{2\varphi(m_2)} - 219.11^{2\varphi(m_2)} \equiv 2.49 - 219 \equiv -11^2 (\mathrm{mod}\, m_2)$ và do đó vì $(11, m_2) = 1$ ta nhận được $2x_2^2 - 219y_2^2 \equiv (\mathrm{mod}\, m_2)$. Bây giờ vì $(m_1, m_2) = 1$ nên theo định lý số dư Trung Hoa (Chương 1 mục 12) suy ra tồn tại các số nguyên x, y thỏa mãn

$$x \equiv x_1 (\mathrm{mod}\, m_1),\ x \equiv x_2 (\mathrm{mod}\, m_2)$$
$$y \equiv y_1 (\mathrm{mod}\, m_1), y \equiv y_2 (\mathrm{mod}\, m_2)$$

Vì vậy $2x^2 - 219y^2 \equiv 2x_1^2 - 219y_1^2 \equiv -1 (\mathrm{mod}\, m_1)$ và $2x^2 - 219y^2 \equiv 2x_2^2 - 219y_2^2 \equiv -1 (\mathrm{mod}\, m_2)$ do đó vì $(m_1, m_2) = 1$ và $m = m_1 m_2, 2x^2 - 219y^2 \equiv -1 (\mathrm{mod}\, m)$ chứng tỏ đồng dư thức ở trên là giải được với mọi số tự nhiên m.

Bây giờ ta giải một đồng dư thức khác mà vế trái không có dạng đa thức. Xét

(*) $$2^x \equiv x^2 (\mathrm{mod}\, 3).$$

Vì $2^2 \equiv 1 (\mathrm{mod}\, 3)$ ta có $2^{x+2k} \equiv 2^x (\mathrm{mod}\, 3)$ với mọi số nguyên không âm x và $k = 0, 1, 2, \ldots$ Vì $(x + 3l)^2 \equiv x^2 (\mathrm{mod}\, 3)$ với mọi số nguyên x, l nên ta thấy nếu x là nghiệm của đồng dư thức ***(*)*** thì $x + 6t,\ t = 0, 1, 2, \ldots,$ cũng là các nghiệm của ***(*)***. Trong các số 0,1,2,3,4,5 thì chỉ có 2 và 4 là nghiệm của đồng dư thức ***(*)***. Vậy mọi nghiệm của đồng dư thức là $2 + 6t$ hoặc $4 + 6t$ với $t = 0, 1, 2, \ldots$.

Ghi chú. Các số đồng dư với nghiệm của ***(*)*** theo modulo của đồng dư thức có thể không phải nghiệm của ***(*)*** chẳng hạn số 5.

4. Đồng dư thức bậc một

Đặt

(10) $$ax \equiv b (\mathrm{mod}\, m),$$

với m là modulo cho trước và a, b là các số nguyên cho trước. Ta đã biết trong mục 2 thì đồng dư thức ***(10)*** tương đương với phương trình Diophante

(11) $$ax - my = b$$

Từ Định lý 15 Chương 1 thì phương trình ***(11)*** có nghiệm nguyên x, y khi và chỉ khi $(a, m) | b$. Do đó đây cũng là điều kiện cần và đủ đối với tính giải được của đồng dư thức ***(10)***.

Giả sử các điều kiện được thỏa mãn ta sẽ tìm phương pháp tính tất cả các nghiệm của ***(10)*** và tính số nghiệm đó.

Đặt $d = (a, m)$ thì số b/d nguyên. Với x_0 là nghiệm của đồng dư thức ***(10)*** và x là nghiệm tùy ý của nó thì ta có $ax_0 \equiv b (\mathrm{mod}\, m)$ và theo ***(10)*** thì ta có $a(x - x_0) \equiv 0 (\mathrm{mod}\, m)$. Do đó $m | a(x - x_0)$ suy ra $\frac{m}{d} | \frac{a}{d}(x - x_0)$. Nhưng vì $d = (a, m)$ nên $\left(\frac{m}{d}, \frac{a}{d}\right) = 1$ do đó $\frac{m}{d}$ là ước số của $x - x_0$ suy ra $x = x_0 + \frac{m}{d}t$ với t là số nguyên.

Ngược lại, xét số nguyên tùy ý t và nghiệm tùy ý x_0 của đồng dư thức ***(10)*** và đặt $x = x_0 + \frac{m}{d}t$ ta nhận được nghiệm của đồng dư thức ***(10)*** vì $ax = ax_0 + \frac{a}{d}tm \equiv ax_0 \equiv b \pmod m$.

Bây giờ cho t lần lượt nhận các giá trị $0,1,2,\ldots,d-1$. Ta chứng minh các số

(12) $$x_t = x_0 + \frac{m}{d}t$$

là phân biệt modulo m.

Thật vậy, nếu $x_t \equiv x_u \pmod m$ thì theo ***(12)*** ta có $x_0 + \frac{m}{d}t \equiv x_0 + \frac{m}{d}u \pmod m$ và do đó $\frac{m}{d}(t-u) = mz$ với z là số nguyên, suy ra $t-u = dz$, vô lý vì t,u là các số phân biệt trong dãy $0,1,2,\ldots,d-1$.

Cuối cùng ta chứng minh rằng mỗi nghiệm của đồng dư thức ***(10)*** đồng dư theo modulo m với một trong các nghiệm $x_0, x_1, \ldots, x_{d-1}$ (xác định trong ***(12)***). Thật vậy, nếu x là nghiệm của đồng dư thức ***(10)*** thì với số nguyên t ta có $x = x_0 + \frac{m}{d}t$. Đặt r là số dư nhận được khi chia t cho d.

Khi đó r là một trong các số $0,1,2,\ldots,d-1$. Ta có $t = f + du$ với u là số nguyên.

Vì vậy $x = x_0 + \frac{m}{d}t = x_0 + \frac{m}{d}(r+du) = x_0 + \frac{m}{d}r + mu = x_r + mu$, suy ra $x \equiv x_r \pmod m$, điều phải chứng minh.

Từ các kết quả này ta có

Định lý 2. *Đồng dư thức bậc một $ax \equiv b \pmod m$ là giải được khi và chỉ khi b chia hết cho ước số chung lớn nhất d của hệ số a của x và modulo m. Nếu điều kiện này được thỏa mãn thì đồng dư thức có đúng d nghiệm phân biệt theo modulo m.*

Nếu a và m nguyên tố cùng nhau thì $d = 1$. Ta có hệ quả

Hệ quả. *Nếu hệ số của x nguyên tố cùng nhau với modulo m thì đồng dư thức bậc một $ax \equiv b \pmod m$ có đúng một nghiệm.*

Nếu đồng dư thức $ax \equiv b \pmod m$ là giải được và $(a,m) = d > 1$ thì đồng dư thức $\frac{a}{d}x \equiv \frac{b}{d} \left(\mod \frac{m}{d} \right)$ nhận được từ đồng dư thức ban đầu với $\left(\frac{a}{d}, \frac{m}{d} \right) = 1$ cũng giải được. Do đó để giải các đồng dư thức bậc một (trong trường hợp đồng dư thức là giải được) ta có thể giả sử hệ số của biến số và modulo là nguyên tố cùng nhau. C.Sardi [1] đã trình bày một phương pháp để giải các đồng dư thức như vậy. Xét $ax \equiv b \pmod m$ với $a > 1$ và $(a,m) = 1$. Hơn nữa đặt $a_1 = m - a\left[\frac{m}{a} \right]$ thì $0 < a_1 < a$ vì m không chia hết cho a. Nhân cả hai vế với $-\left[\frac{m}{a} \right]$ ta nhận được $a_1 x \equiv -b\left[\frac{m}{a} \right] \pmod m$, nghĩa là đồng dư thức với $a_1 < a$. Quá trình này lặp lại và ta nhận được $a_n = 1$, nghĩa là đồng dư thức $x \equiv c \pmod m$ với nghiệm duy nhất $x = c$.

5. Định lý Wilson và định lý Fermat nhỏ

Ký hiệu p là số nguyên tố lẻ và D là số nguyên không chia hết cho p.

Các cặp số m,n thuộc dãy

(13) $\qquad 1,2,3,\ldots,p-1$

được gọi là đối tích khi và chỉ khi đồng dư thức sau thỏa mãn

(14) $\qquad mn \equiv D \pmod p$

Từ định nghĩa này suy ra nếu m là số đối tích với n thì n đối tích với m.

Ta sẽ chứng minh với mỗi số thuộc dãy ***(13)*** thì tồn tại đúng một số đối tích với nó. Xét m là số thuộc dãy ***(13)***. Điều kiện cần và đủ để x thuộc dãy ***(13)*** là đối tích của m là $mx \equiv D \pmod m$. Từ đồng dư thức $mx \equiv D \pmod p$ (với m là số thuộc dãy ***(13)***) và theo hệ quả của Định lý 2 thì đồng dư thức cuối cùng có đúng một nghiệm. Do đó trong dãy $0,1,2,3,\ldots,p-1$ có đúng một số thỏa mãn đồng dư thức này. Số này khác 0 vì D không chia hết cho p. Suy ra trong dãy ***(13)*** có đúng một số thỏa mãn đồng dư thức ở trên.

Có thể xảy ra trường hợp các số đối tích là bằng nhau. Khi đó ***(14)*** trở thành $m^2 \equiv d \pmod p$. Điều này chỉ có thể xảy ra nếu tồn tại bình phương đồng dư với D theo modulo p. Khi đó D được gọi là thặng dư bậc hai modulo p. Trong trường hợp ngược lại, nghĩa là không có bình phương nào đồng dư với D theo modulo p thì ta nói D không phải thặng dư bậc hai modulo p. Nói cách khác số D không chia hết cho p được gọi là thặng dư bậc hai hay không phải thặng dư bậc hai tùy thuộc vào việc đồng dư thức $x^2 \equiv D \pmod p$ là giải được hay không. Đầu tiên ta xét trường hợp D không phải thặng dư bậc hai modulo p nguyên tố. Khí đó mỗi cặp các đối tích m,n chứa hai số phân biệt thuộc dãy ***(13)***. Do đó tất cả các số thuộc dãy ***(13)*** có thể chia thành các cặp đối tích, số các cặp như vậy là đúng bằng $(p-1)/2$. Từ ***(14)*** ta có $(p-1)/2$ đồng dư thức

$$\begin{aligned}
&m_1 n_1 \equiv D \pmod p,\\
&m_2 n_2 \equiv D \pmod p,\\
&\ldots\\
&m_{\frac{p-1}{2}} n_{\frac{p-1}{2}} \equiv D \pmod p.
\end{aligned}$$

Khi đó nhân các đồng dư thức này theo vế và lưu ý tích $m_1 n_1 m_2 n_2 \ldots m_{\frac{p-1}{2}} n_{\frac{p-1}{2}}$ chính là tích các phần tử thuộc dãy ***(13)*** sai khác nhiều nhất một hoán vị. Ta có

(15) $\qquad (p-1)! \equiv D^{\frac{1}{2}(p-1)} \pmod p.$

Bây giờ xét trường hợp D là thặng dư bậc hai modulo p. Khi đó đồng dư thức

(16) $\qquad x^2 \equiv D \pmod p$

là giải được. Ta tính số các số trong ***(13)*** mà thỏa mãn ***(16)***. Ta có thể giả sử ***(16)*** là giải được, khi đó trong dãy $0,1,2,\ldots,p-1$ có ít nhất một số k là nghiệm của ***(16)***. Không thể có $k=0$ vì theo giả thiết thì D không chia hết cho p. Do đó số k là một trong các số thuộc dãy (13) và do đó $p-k$ cũng thuộc dãy này. Số này là khác k vì p là số lẻ. Với $l = p-k$ ta có $l^2 \equiv k^2 \pmod p$ nên từ đồng dư thức $k^2 \equiv D \pmod p$ suy ra $l^2 \equiv D \pmod p$.

Vậy nếu D là thặng dư bậc hai modulo p thi trong dãy ***(13)*** có ít nhất hai số khác nhau mà cùng thỏa mãn đồng dư thức ***(16)***. Ta chứng minh có đúng hai số như vậy.

Giả sử x thuộc dãy ***(13)*** thỏa mãn đồng dư thức ***(16)***. Vì $k^2 \equiv D \pmod p$ nên ta có $x^2 \equiv k^2 \pmod p$ suy ra $p \mid x^2 - k^2 = (x-k)(x+k)$. Nhưng vì p là số nguyên tố nên $p \mid x-k$ hoặc $p \mid x+k$. Nếu $p \mid x-k$ thì vì x và k cùng thuộc dãy ***(13)*** suy ra $x = k$. Nếu $p \mid x+k$ thì vì $0 < x < p$ và $0 < k < p$ do đó $0 < x+k < 2p$ nên ta có $x+k = p$ suy ra $x = p-k = l$.

Vậy ta đã chứng minh được k và l là tất cả các số trong dãy ***(13)*** mà thỏa mãn đồng dư thức ***(16)***. Do đó: *nếu D không chia hết cho số nguyên tố lẻ p và là thặng dư bậc hai modulo p thì đồng dư thức **(16)** có đúng hai nghiệm.*

Bây giờ ta bỏ các số k và l ra khỏi dãy ***(13)***. Khi đó không có số nào trong $p-3$ số còn lại thỏa mãn đồng dư thức ***(16)*** do đó có thể chia chúng thành $(p-3)/2$ cặp đối tích. Do đó ta nhận được $(p-3)/2$ đồng dư thức

$$m_1 n_1 \equiv D \pmod p,$$
$$m_2 n_2 \equiv D \pmod p,$$
$$\dots$$
$$m_{\frac{p-3}{2}} n_{\frac{p-3}{2}} \equiv D \pmod p.$$

Vì $kl = k(p-k) \equiv k^2 \equiv D \pmod p$ nên ta có thể cộng đồng dư thức $kl \equiv -D \pmod p$ vào các đồng dư thức ở trên sau đó nhân lại. Khi đó vế trái của đồng dư thức nhận được bằng $(p-1)!$. Do đó

(17) $$(p-1) \equiv -D^{\frac{1}{2}(p-1)} \pmod p$$

Ta thấy ***(15)*** hoặc ***(17)*** đúng hay không phụ thuộc vào việc D là thặng dư bậc hai modulo p hay không. Kết hợp lại ta viết

(18) $$(p-1)! \equiv \pm D^{\frac{1}{2}(p-1)} \pmod p,$$

Các dấu – và + trong vế phải được lấy tùy thuộc D là thặng dư bậc hai modulo p hay không.

Đặc biệt với $D = 1$ ta thấy 1 là thặng dư bậc hai theo mọi modulo p nên

(19) $$(p-1)! \equiv -1 \pmod p.$$

Trong chứng minh tính chất ***(19)*** có sử dụng tới giả thiết p là số nguyên tố lẻ, nhưng kết quả vẫn đúng với $p = 2$ vì ta thấy $(2-1)! = 1 \equiv -1 \pmod 2$. Vậy ta có định lý

Định lý 3 (Wilson). *Nếu p là số nguyên tố thì $(p-1)!+1$ chia hết cho p.*

Mệnh đề ngược lại cũng đúng. Thật vậy, nếu p là số tự nhiên >1 và nếu $(p-1)!+1$ chia hết cho p thì p là số nguyên tố. Thật vậy, giả sử phản chứng p không phải số nguyên tố. Khi đó tồn tại ước số q của p mà $1 < q < p$. Số $(p-1)!+1$ chia hết cho p nên nó chia hết cho q nhưng vì $q < p, q \le p-1$ nên $q \mid (p-1)!$ suy ra $q \mid 1$, mâu thuẫn. Vậy ta có

Định lý 3ª. *Điều kiện cần và đủ để số tự nhiên $n > 1$ là số nguyên tố là $(n-1)!+1$ chia hết cho n.*

Vậy về lý thuyết thì để quyết định xem một số tự nhiên $n > 1$ có phải số nguyên tố hay không ta chỉ cần sử dụng đúng một phép chia.

Từ Định lý 3 suy ra với số nguyên tố p thì số $w_p = \{(p-1)!+1\}/p$ là số tự nhiên. C.E.Froberg [2] đã tính các số dư nhận được khi chia w_p cho p với các số nguyên tố $p < 50000$. Các số nguyên tố thỏa mãn $p^2 \mid (p-1)!+1$ được gọi là các số nguyên tố Wilson. Từ bảng cho bởi Froberg thì trong các số nguyên tố $p < 50000$ chỉ có ba số nguyên tố Wilson là 5,13 và 563.

Từ Định lý 3[a] và lưu ý với $n > 2$ thì $(n-1)! = (n-2)!(n-1) \equiv -(n-2)! \pmod n$ ta có

Định lý 3[b] (Leibniz). *Số tự nhiên $n > 1$ là số nguyên tố khi và chỉ khi $(n-2)! \equiv 1 \pmod n$.(0!=1)*

Có thể chứng minh số tự nhiên $p > 1$ là số nguyên tố khi và chỉ khi tồn tại số tự nhiên $n < p$ mà $(n-1)!(p-n)! \equiv (-1)^n \pmod p$ (Dickson [7] tập 1 trang 64).

Rõ ràng nếu n là số tự nhiên thỏa mãn $n \mid (n-1)!$ thì n là hợp số. Dễ dàng chứng minh nếu n là hợp số $\neq 4$ thì $n \mid (n-1)!$. Thật vậy, nếu n là hợp số thì tồn tại các số tự nhiên a và b mà $n = ab, 1 < a < b, 1 < b < n$. Nếu $a \neq b$ thì a và b là các nhân tử phân biệt của tích $(n-1)!$ và do đó $n = ab$ là ước số của $(n-1)!$. Nếu $a = b$ thì $n = a^2$ và vì n là hợp số $\neq 4$ nên $a > 2$. Vì vậy $n = a^2 \neq 2a$ và do đó a và $2a$ là các nhân tử phân biệt của tích $(n-1)!$. Vậy $(n-1)!$ chia hết cho $2a^2$ và do đó cũng chia hết cho $a^2 = n$. Với $n = 4$ thì ta có $(n-1)! = 3! = 6 \equiv 2 \pmod 4$.

Từ Định lý 3 suy ra tồn tại hữu hạn các số tự nhiên n mà $n!+1$ là hợp số. Chẳng hạn các số $n = p-1$ với p là số nguyên tố > 3. Khi đó $(p-1)! > 2(p-1) = p + (p-2) > p$. A.Schinzel [14] đã chứng minh với mọi số hữu tỷ $c \neq 0$ thì luôn tồn tại vô hạn hợp số nguyên có dạng $cn!+1$. Tuy nhiên ta chưa biết có tồn tại vô hạn các số nguyên tố có dạng $n!+1$ hay không? Với $n < 546$ thì các số nguyên tố có dạng này nhận được với $n = 1, 2, 3, 11, 27, 37, 41, 73, 77, 116, 154, 320, 340, 399, 427$ (Buhler, Crandall và Penk [1]).

Ta cũng chưa biết có tồn tại vô hạn các số tự nhiên k mà các số $P_k = p_1 p_2 \ldots p_k + 1$ nguyên tố hay không? Câu hỏi tương tự với P_k là hợp số. Ta đã biết một số số nguyên tố có dạng P_k là $P_1 = 3$, $P_2 = 7$, $P_4 = 211$, $P_5 = 2311$, nhưng các số sau đây $P_6 = 59 \cdot 509$, $P_7 = 19 \cdot 97 \cdot 277$, $P_8 = 347 \cdot 27953$, $P_9 = 317 \cdot 703763$, $P_{10} = 331 \cdot 571 \cdot 34231$ không phải số nguyên tố. Với k nằm giữa 10 và 442 thì P_k là số nguyên tố chỉ với $k = 11, 75, 171, 172, 284$ (Buhler, Crandall và Penk [1]). Từ Định lý 3^b suy ra tồn tại vô hạn số tự nhiên n mà $n!-1$ là hợp số. Chẳng hạn với các số $n = p-2$ với p là số nguyên tố > 5. Ta chưa biết có tồn tại vô hạn các số nguyên tố dạng này hay không. Nếu $n < 546$, thì $n!-1$ là số nguyên tố chỉ với $n =$ 3, 4, 6, 7, 12, 14, 30, 32, 33, 94, 166, 324, 379, 427 (Buhler, Crandall và Penk [1]).

Từ các công thức ***(15)***, ***(17)*** và Định lý 3 suy ra

Định lý 4. *Nếu số nguyên D không chia hết cho số nguyên tố lẻ p thì*

$$D^{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod p, \qquad \textbf{(20)}$$

Trong đó các dấu + hoặc– được lấy tùy thuộc D có phải là thặng dư bậc hai modulo p hay không.

Bình phương hai vế của ***(20)*** ta nhận được

Định lý 5. *Nếu số nguyên D không chia hết cho số nguyên tố p thì*

$$D^{p-1} \equiv 1 \pmod p \qquad \textbf{(21)}$$

Đây là định lý nhỏ Fermat. Định lý này được Fermat phát biểu (không kèm theo chứng minh) vào năm 1640. Lời giải đầu tiên được trình bày bởi L.Euler năm 1736.

Chứng minh ở trên của công thức ***(20)*** không đúng khi $p=2$ nhưng ta có thể thấy ***(21)*** vẫn đúng vì với D không chia hết cho $p=2$ nên nó là số lẻ và do đó $D\equiv 1(\mathrm{mod}\,2)$.

Đặc biệt từ Định lý 5 suy ra nếu p là số nguyên tố lẻ thì $2^{p-1}-1$ chia hết cho p. Các nghiên cứu xem khi nào thì $2^{p-1}-1$ chia hết cho p^2 đã được tiến hành. Với $p<6\cdot 10^9$ thì chỉ có hai số được tìm ra là $p=1093, p=3511$ (Brillhart, Tonascia và Weinberger [1] và Lehmer [9]).

Ứng dụng đơn giản của Định lý 5 cho phép tính tất cả các nghiệm của đồng dư thức $ax\equiv b(\mathrm{mod}\,p)$ với p là số nguyên tố và a không chia hết cho p. Thật vậy, $x=a^{p-2}b$ là nghiệm vì theo Định lý 5 ta có $a^{p-1}\equiv 1(\mathrm{mod}\,p)$ suy ra $ax=a^{p-1}b\equiv b(\mathrm{mod}\,p)$.

Hệ quả trực tiếp của Định lý 5 là

Định lý 5^a**.** *Nếu p là số nguyên tố thì với mọi số nguyên a ta có $p\mid a^p-a$.*

Ngược lại, Định lý 5 được suy ra từ Định lý 5^a. Thật vậy, nếu a là số nguyên không chia hết cho số nguyên tố p thì từ $p\mid a^p-a=a(a^{p-1})-1$ suy ra $a^{p-1}\equiv 1\ (\mathrm{mod}\,p)$.

Các định lý Wilson và Fermat được kết hợp thành định lý duy nhất có dạng sau đây (Moser [4])

Định lý 6. *Nếu p là số nguyên tố và a là số nguyên thì*

(22) $$p\mid a^p+(p-1)!a$$

Thật vậy, từ Định lý 3 suy ra $(p-1)!\equiv -1(\mathrm{mod}\,p)$ và do đó $a^p+(p-1)!a\equiv a^p-a(\mathrm{mod}\,p)$. Theo Định lý 5^a suy ra $a^p-a\equiv 0(\mathrm{mod}\,p)$ nên ***(22)*** được kéo theo.

Mặt khác, nếu Định lý 6 đúng thì với $a=1$ từ công thức ***(22)*** có thể suy ra Định lý 3. Vì vậy với mọi số nguyên a mà đồng dư thức $a^p+(p-1)!a\equiv a^p-a(\mathrm{mod}\,p)$ được thỏa mãn thì từ ***(22)*** có thể suy ra $a^p-a\equiv 0(\mathrm{mod}\,p)$. Do đó Định lý 5^a đúng và nó tương đương với định lý Fermat nhỏ.

Dễ dàng chứng minh dạng chung của định lý Fermat nhỏ và định lý Wilson tương đương với

Định lý 6^a**.** *Nếu p là số nguyên tố và a là số nguyên thì* $p\mid (p-1)!a^p+a$

Trong mối liên hệ này các tác giả Dickson [7] tập 1 trang 84-86 và T.Szele [1] đã chứng minh dạng tổng quát sau đây của Định lý 5^a, dạng tổng quát này được đặt ra bởi J.A.Serret năm 1855: *với mọi số tự nhiên m và số nguyên a thì số* $\sum_{d\mid m}\mu(d)a^{d\mid m}$ *chia hết cho m.*

Vì vậy, với mọi số nguyên a và hai số nguyên tố phân biệt p và q ta có $pq\mid a^{pq}-a^p-a^q+a$.

Ta có một hệ quả khác của Định lý 5

Định lý 7. *Tồn tại vô hạn số nguyên tố có dạng $4k+1$ với k là số tự nhiên.*

Chứng minh. Xét n là số tự nhiên tùy ý >1 và đặt

(23) $$N=(n!)^2+1$$

Số N lẻ và >1. Ký hiệu p là ước số nguyên tố nhỏ nhất của N. Theo ***(23)*** thì $p>n$. Do p lẻ nên nó có dạng $4k+1$ hoặc $4k+3$. Theo ***(23)*** ta có $(n!)^2\equiv -1(\mathrm{mod}\,p)$ và lũy thừa cả hai vế lên

$(p-1)/2$ lần ta có $(n!)^{p-1} \equiv (-1)^{(p-1)/2} \pmod p$. Nhưng $n!$ không chia hết cho p và theo Định lý 5, ta có $(n!)^{p-1} \equiv 1 \pmod p$ suy ra

(24) $$(-1)^{\frac{1}{2}(p-1)} \equiv 1 \pmod p$$

Không thể có $p = 4k+3$ vì nếu như vậy thì từ ***(24)*** suy ra $(-1)^{\frac{1}{2}(p-1)} = (-1)^{2k+1} = -1 \equiv 1 \pmod p$ do đó $p \mid 2$, vô lý. Vậy p phải có dạng $4k+1$.

Do đó ta đã chứng minh được với mọi số tự nhiên $n > 1$ thì luôn tồn tại số nguyên tố $p > n$ có dạng $4k+1$. Các ước số nguyên tố của số cho bởi ***(23)*** thỏa mãn tính chất này. Định lý 7 được chứng minh.

Ta cũng chứng minh được có vô hạn các số nguyên tố có dạng $4k+3$. Thật vậy, ký hiệu n là số tự nhiên tùy ý > 3 và đặt

(25) $$N_1 = n! - 1$$

thì N_1 là số lẻ > 1 và vì thế các ước số nguyên tố của nó đều lẻ. Nếu tất cả các ước số của nó đều có dạng $4k+1$ thì N_1 cũng có dạng $4k+1$. Nhưng điều này không đúng với $n > 3$. Vậy với mọi số tự nhiên $n > 3$ thì tồn tại số nguyên tố $p > n$ có dạng 4*k* + 3. Vì vậy

Định lý 7^a**.** *Tồn tại vô hạn số nguyên tố có dạng* $4k+3$ *với* k *là số tự nhiên.*

Với số thực cho trước $x > 1$ ký hiệu $\pi_1(x)$ là số các số nguyên tố $\le x$ có dạng $4k+1$ và $\pi_3(x)$ là số các số nguyên tố $\le x$ có dạng $4k+3$. Đặt $\Delta(x) = \pi_3(x) - \pi_1(x)$. Năm 1914 J.E.Littlewood đã chứng minh rằng tồn tại vô hạn số tự nhiên n mà $\Delta(n) > 0$ và tồn tại vô hạn số n mà $\Delta(n) < 0$. Tuy nhiên tới tận năm 1957 thì ta vẫn chưa tìm được số n nào mà $\Delta(n) < 0$. Sử dụng máy tính điện tử EDSAC, J. Leech [1] đã tính các số $\Delta(n)$ với $n \le 3000000$ và chứng minh được số tự nhiên nhỏ nhất n mà $\Delta(n) < 0$ là $n = 26861$. Với số n đó ta có $\pi_1(n) = 1473$, $\pi_3(n) = 1472$ và $\Delta(n) = -1$. Ta tính được $\Delta(623681) = -8$, $\Delta(627859) = \Delta(627860) = \ldots = \Delta(627900) = 0$, $\Delta(2951071) = 256$.

Từ Định lý 5 suy ra nếu p là số nguyên tố thì $a^{p-1} \equiv 1 \pmod p$ với $a = 1, 2, \ldots p-1$. Cộng $p-1$ đồng dư thức ta có $1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv p-1 \pmod p$. Vì vậy $p \mid 1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} + 1$ với mọi số nguyên tố p. G.Giuga [1] đã đặt ra giả thuyết rằng tính chất này không đúng với các hợp số. Giả thuyết này được E.Bedocchi [1] *(1)* chứng minh với $p \le 10^{1700}$.

Định lý sau đây là hệ quả của Định lý 3.

Định lý 8. *Nếu* p *là số nguyên tố có dạng* $4k+1$ *với* k *là số tự nhiên thì*

(26) $$p \left| \left[\left(\frac{p-1}{2} \right)! \right]^2 + 1 \right.$$

Chứng minh. Từ $\frac{1}{2}(p-1) = 2k$ suy ra

$$1 \cdot 2 \cdot 3 \ldots \tfrac{1}{2}(p-1) = (-1)(-2)\ldots\left(-\frac{p-1}{2}\right) \equiv (p-1)(p-2)\ldots\frac{p+1}{2} \pmod p;$$

(1) Xem phụ lục mục bổ sung cho các chứng minh

Do đó $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv 1\cdot 2\ldots\frac{p-1}{2}.\frac{p+1}{2}\ldots(p-1)\equiv(p-1)!\equiv -1(\mathrm{mod}\, p)$ và suy ra ***(26)***.

Dựa theo Định lý 8 ta chứng minh

Định lý 9 (Fermat). *Mọi số nguyên tố p có dạng* $4k+1$ *đều là tổng của hai bình phương.*

Chứng minh. Giả sử p là số nguyên tố có dạng $4k+1$ và $a=\left(\frac{p-1}{2}\right)!$. Theo Định lý 8 ta có $p\,|\,a^2+1$ do đó a nguyên tố cùng nhau với p. Theo định lý Thue (Chương 1 mục 13) thì tồn tại hai số tự nhiên $x,y\le\sqrt{p}$ mà với cách chọn các dấu + và – thích hợp thì $ax\pm y$ chia hết cho p. Vì vậy suy ra số $a^2x^2-y^2=(ax-y)(ax+y)$ chia hết cho p. Do đó $a^2x^2-y^2=(ax-y)(ax+y)$ chia hết cho p và $a^2x^2+x^2=(a^2+1)x^2$ chia hết cho p (vì $p\,|\,a^2+1$). Hệ quả là số $x^2+y^2=a^2x^2+x^2-(a^2x^2-y^2)$ chia hết cho p. Nhưng vì x,y là các số tự nhiên $\le\sqrt{p}$ nên chúng đều $<\sqrt{p}$ vì p là số nguyên tố và không phải bình phương một số tự nhiên. Do đó x^2+y^2 là số tự nhiên >1 và $<2p$ và hơn nữa nó chia hết cho p do đó nó bằng p, nghĩa là $p=x^2+y^2$. Chứng tỏ p là tổng của hai bình phương các số tự nhiên. □

Các số có dạng $4k+3$ (không nhất thiết nguyên tố) không thể biểu diễn được thành tổng của hai bình phương vì một bình phương chia 4 dư 0 hoặc 1, do đó tổng hai bình phương chia 4 dư 0,1 hoặc 2. Chứng tỏ trong các số nguyên tố thì chỉ có $2=1^2+1^2$ và các có dạng $4k+1$ là tổng của hai bình phương các số tự nhiên.

H.Davenport [2] (trang 120-122) đã trình bày bốn cách phân tích số nguyên tố có dạng $4k+1$ thành tổng hai bình phương. Các cách đó được cho bởi Legendre (1808), Gauss (1825), Serret (1848) và Jacobsthal (1906). Cách xây dựng đơn giản nhất (không kèm theo chứng minh) thuộc về Gauss. Nếu $p=4k+1$ là số nguyên tố ta lấy các số nguyên x,y mà $x\equiv(2k)!/2(k!)^2(\mathrm{mod}\, p)$ và $y\equiv(2k)!x(\mathrm{mod}\, p)$ với $|x|<\frac{1}{2}p,\ |y|<\frac{1}{2}p$. Khi đó $p=x^2+y^2$. Các chứng minh được trình bày bởi Cauchy và Jacobsthal đều không đơn giản. Các tính toán các số x,y là không dễ. Chẳng hạn với $p=29$ thì $x\equiv 14!/2\cdot(7!)^2=1716\equiv 5(\mathrm{mod}\,29)$, $y\equiv 14!x\equiv 14!\cdot 5\equiv 2(\mathrm{mod}\,29)$ suy ra $x=5,y=2$.

Ta không biết có tồn tại vô hạn số nguyên tố p mà $p=x^2+(x+1)^2$ với x là số tự nhiên hay không. Câu trả lời khẳng định được suy ra từ giả thuyết H (Chương 3 mục 8). Chẳng hạn ta có $5=1^2+2^2$, $13=2^2+3^2$, $41=4^2+5^2$, $61=5^2+6^2$, $113=7^2+8^2$, $181=9^2+10^2$, $313=12^2+13^2$, $421=14^2+15^2$, $613=17^2+18^2$, $761=19^2+20^2$.

Giả thuyết nói rằng tồn tại vô hạn số nguyên tố mà mỗi số đều là tổng của hai bình phương liên tiếp là tương đương với giả thuyết nói rằng tồn tại vô hạn số nguyên tố p mà $2p=a^2+1$ với a là số tự nhiên. Thật vậy, giả sử $p=x^2+(x+1)^2$ với x là số tự nhiên thì $2p=(2x+1)^2+1$. Ngược lại nếu $2p=a^2+1$ với a là số tự nhiên thì với $p>2$ số a lẻ >1 và do đó $a=2x+1$ với x là số tự nhiên. Suy ra $2p=(2x+1)^2+1$ nghĩa là $p=x^2+(x+1)^2$.

Từ giả thuyết H suy ra tồn tại vô hạn số nguyên tố p mà $p=a^2+b^2$ với a và b là các số nguyên tố. Chẳng hạn $13=2^2+3^2, 29=2^2+5^2, 53=2^2+7^2, 173=2^2+13^2, 293=2^2+17^2, 1373=2^2+37^2$.

Cũng từ giả thuyết H suy ra tồn tại vô hạn các số nguyên tố là tổng của ba bình phương liên tiếp các số tự nhiên. Chẳng hạn $29=2^2+3^2+4^2, 149=6^2+7^2+8^2, 509=12^2+13^2+14^2$, $677=14^2+15^2+16^2$, $1877=24^2+25^2+26^2$. Trong mối liên hệ này ta lưu ý rằng giả thuyết H suy

ra tồn tại vô hạn số nguyên tố mà mỗi số đều là tổng ba bình phương các số nguyên tố lẻ phân biệt. Chẳng hạn $83=3^2+5^2+7^2, 179=3^2+7^2+11^2, 419=3^2+11^2+17^2, 563=3^2+5^2+23^2$. Dễ dàng chứng minh trong các bình phương này luôn phải có số 3^2.

Một hệ quả khác có thể suy ra từ giả thuyết H là với mọi số tự nhiên n thì luôn tồn tại vô hạn số tự nhiên x mà x^2+n^2 là các số nguyên tố.

Có thể chứng minh rằng với mọi số tự nhiên n thì luôn tồn tại số nguyên tố p thỏa mãn $p=a^2+b^2$ với $a>n$ và $b>n$ (Chương 3 mục 7).

Nếu một số nguyên tố là tổng của hai hoặc bốn bình phương các số nguyên tố phân biệt thì một trong các số nguyên tố đó phải bằng 2. Nếu một số nguyên tố là tổng của ba bình phương các số nguyên tố phân biệt thì một trong các số đó bằng 3. Tuy nhiên từ giả thuyết H suy ra với mọi số tự nhiên n thì tồn tại số nguyên tố $q>p_{n+3}$ mà số $p={p_n}^2+p_{n+1}^2+p_{n+2}^2+p_{n+3}^2+q^2$ nguyên tố. Chẳng hạn $373=3^2+5^2+7^2+11^2+13^2, 653=5^2+7^2+11^2+13^2+17^2, 1997=7^2+11^2+13^2+17^2+37^2$.

Bây giờ ta chứng minh nếu phép phân tích một số nguyên tố thành tổng của hai bình phương tự nhiên là tồn tại thì biểu diễn đó là duy nhất sai khác các hoán vị. Ta chứng minh mệnh đề tổng quát sau đây

Định lý 10. *Giả sử a và b là các số tự nhiên thì nếu tồn tại biểu diễn của số nguyên tố p dưới dạng $p=ax^2+by^2$ với x, y là các số tự nhiên thì biểu diễn này là duy nhất (không tính hoán vị x và y nếu $a=b=1$).*

Chứng minh. Giả sử với số nguyên tố p

(27) $$p=ax^2+by^2=ax_1^2+by_1^2$$

Với x, y, x_1, y_1 là các số tự nhiên. Rõ ràng $(x,y)=(x_1,y_1)=1$. Từ ***(27)*** ta có

$$p^2=(axx_1+byy_1)^2+ab(xy_1-yx_1)^2=(axx_1-byy_1)^2+ab(xy_1+yx_1)^2$$

Nhưng $(axx_1+byy_1)(xy_1+yx_1)=(ax^2+by^2)x_1y_1+(ax_1^2+by_1^2)xy=p(x_1y_1+xy)$. Do đó ít nhất một trong các nhân tử ở vế trái phải chia hết cho p. Nếu $p \mid axx_1+byy_1$ thì từ công thức thứ nhất của p^2 suy ra $xy_1-yx_1=0$. Do đó $x/y=x_1/y_1$ mà $(x,y)=(x_1,y_1)=1$ suy ra $x=x_1$, $y=y_1$. Nếu $p \mid xy_1+yx_1$ thì từ công thức thứ hai của p^2 suy ra $p^2 \geq abp^2$. Điều này chỉ có thể khi $a=b=1$. Nhưng $xx_1-yy_1=0$ nên $x/y=y_1/x_1$ mà $(x,y)=(x_1,y_1)=1$ suy ra $x=y_1$, $y=x_1$. Vậy các phân tích $p=x^2+y^2$ và $p=x_1^2+y_1^2$ chỉ sai khác thứ tự các hạng tử. Định lý 10 được chứng minh. □

Hệ quả trực tiếp của Định lý 10 là nếu một số tự nhiên có hai (hoặc nhiều hơn) biểu diễn thành dạng ax^2+by^2 với x, y là các số tự nhiên thì nó phải là hợp số. Mệnh đề ngược lại không đúng. Chẳng hạn số 14 có duy nhất một biểu diễn có dạng $14=2x^2+3y^2$ với x, y là các số tự nhiên $(x=1, y=2)$ và số 15 là hợp số nhưng không có biểu diễn nào dưới dạng $15=2x^2+3y^2$ với x, y là các số nguyên. Số 18 có biểu diễn duy nhất dưới dạng $18=x^2+y^2$ với x, y là các số tự nhiên với $x=y=3$. Các số 25 và 45 có biểu diễn duy nhất không tính các hoán vị có dạng x^2+y^2 với x, y là các số tự nhiên, đó là $25=3^2+4^2$, $45=3^2+6^2$.

Tuy nhiên ta có định lý sau đây

Định lý 11. *Số tự nhiên có dạng $4k+1>1$ là số nguyên tố khi và chỉ khi nó có đúng một biểu diễn (không tính các hoán vị) dưới dạng tổng của hai bình phương các số nguyên ≥ 0 và trong biểu diễn đó các bình phương là nguyên tố cùng nhau.*

Chứng minh. Giả sử số $p=4k+1$ nguyên tố. Thế thì theo Định lý 9 và 10, số p có đúng một biểu diễn (không tính các hoán vị) dưới dạng $p=x^2+y^2$ với x,y là các số tự nhiên. Rõ ràng trong biểu diễn này thì x,y là các số nguyên tố cùng nhau. Vì nếu ngược lại $(x,y)=d>1$ thì $d^2 \mid p$ vô lý. Vậy ta đã chứng minh được điều kiện cần. Để chứng minh điều kiện đủ ta chứng minh bổ đề sau đây

Bổ đề. *Nếu hai số tự nhiên có dạng $4k+1$ với $k>0$ đều là tổng của hai bình phương các số nguyên thì tích của chúng không thỏa mãn các điều kiện của Định lý 11.*

Chứng minh bổ đề. Giả sử $m=a^2+b^2$, $n=c^2+d^2$ với a,b,c,d là các số nguyên. Ta có

(28) $$mn=(ac+bd)^2+(ad-bc)^2=(ac-bd)^2+(ad+bc)^2$$

Giả sử hai biểu diễn mới nhận được này của số mn chỉ sai khác thứ tự các hạng tử. Thế thì $ac+bd=ad+bc$ hoặc $ac+bd=|ac-bd|$. Trong trường hợp thứ nhất ta có $a(c-d)=b(c-d)$ nhưng $c\neq d$ vì nếu $c=d$ thì $n=2c^2$ mâu thuẫn với việc n là số lẻ, nên $a=b$. Nhưng điều này là không thể vì m là số lẻ. Trong trường hợp còn lại, nghĩa là $ac+bd=|ac-bd|$ ta có $ac+bd=ac-bd$ hoặc $ac+bd=bd-ac$. Trong trường hợp thứ nhất thì $bd=0$ và do đó $b=0$ hoặc $d=0$. Nếu $b=0$ thì $m=a^2$ với $a>1$ và $mn=(ac)^2+(ad)^2$ với ac và ad có ước số chung >1 và do đó mn không thỏa mãn các điều kiện đặt ra trong Định lý 11. Trong trường hợp thứ hai ta có $ac=0$ và do đó $a=0$ hoặc $c=0$, chứng minh tương tự trường hợp trước suy ra mn không thỏa mãn các điều kiện đặt ra trong Định lý 11. Vì vậy chỉ cần xét trường hợp phân tích ***(28)*** không chỉ sai khác thứ tự các hạng tử. Trong trường hợp này rõ ràng mn không thỏa mãn các điều kiện trong Định lý 11. Bổ đề được chứng minh. □

Ta chứng minh điều kiện đủ. Giả sử phản chứng rằng $s=4k+1>1$ thỏa mãn các điều kiện trong Định lý 11 và không phải số nguyên tố. Gọi p là ước số nguyên tố tùy ý của s. Rõ ràng p là số lẻ. Nếu p bằng $4t+3$ thì vì giả thiết $s=a^2+b^2$ với $(a,b)=1$ ta có $a^2\equiv -b^2 \pmod p$ từ đây lũy thừa cả hai vế lên số mũ $\frac{1}{2}(p-1)=(2t+1)$ thì theo Định lý 5 ta có $1\equiv -1 \pmod p$, nghĩa là $2 \mid p$, điều này là không thể. Vì vậy p phải có dạng $4t+1$ và do đó theo Định lý 9, p là tổng của hai bình phương các số tự nhiên. Do đó mỗi ước số nguyên tố của s đều là tổng hai bình phương các số nguyên nên theo ***(28)*** các ước số của s cũng có tính chất này. Nếu số s là hợp số thì nó là tích của các số tự nhiên $n,m>1$ mà mỗi số là tổng bình phương hai số nguyên có dạng $4t+1$ (vì các ước số nguyên tố của nó đều có dạng này) nên theo bổ đề thì số $s=mn$ không thỏa mãn các điều kiện trong Định lý 11, mâu thuẫn với giả thiết. Định lý 11 được chứng minh. □

Áp dụng Định lý 11 ta thấy để kiểm tra xem một số tự nhiên cho trước n có dạng $4k+1$ có phải là số nguyên tố hay không thì ta xét dãy $n-0^2$, $n-1^2$, ..., $n-\left(\left[\sqrt{n}\right]\right)^2$ và kiểm tra xem có số nào là bình phương hay không.

Sử dụng Định lý 11 theo cách này thì vào năm 1960 T.Kulikowski, với sự trợ giúp của máy tính EMC tại Warsaw Polytechnic, đã chỉ ra số $2^{39}-7$ là nguyên tố vì nó chỉ có duy nhất một biểu diễn thành tổng hai bình phương các số nguyên là $2^{39}-7=64045^2+738684^2$ và các số nguyên này là nguyên tố cùng nhau. Các số 2^n-7, $n=4,5,\ldots 38$, đều là hợp số. Bài toán tìm số nguyên tố có dạng 2^n-7 được đặt ra bởi P.Erdos vào năm 1956.

Bài tập. ***1***. Chứng minh rằng các số tự nhiên $n>1$ và $n+2$ tạo thành một cặp số nguyên tố sinh đôi khi và chỉ khi đồng dư thức

(29) $$4\big((n-1)!+1\big)+n\equiv 0\big(\bmod n(n+2)\big)$$

đúng (Clement [1], với $n>3$ xem Coblyn [1]).

Chứng minh. Giả sử n và $n+2$ đều là số nguyên tố. Theo Định lý 3 thì $(n-1)!+1\equiv 0(\mathrm{mod}\, n)$ và $(n+1)!+1\equiv 0(\mathrm{mod}\, n+2)$. Nhưng vì $n\equiv -2(\mathrm{mod}\, n+2)$ và $n+1\equiv -1(\mathrm{mod}\, n+2)$ nên suy ra ta có $(n+1)!\equiv (n-1)!2(\mathrm{mod}\, n+2)$. Suy ra vế trái của ***(29)*** chia hết cho n do đó

$$4\big((n-1)!+1\big)+n\equiv (n+1)!2+2+n+2=2\big((n+1)!+1\big)+n+2\equiv 0(\mathrm{mod}\, n+2)$$

Vì vậy vế trái của ***(29)*** cũng chia hết cho $n+2$. Nhưng các số n, $n+2$ là các số nguyên tố phân biệt nên vế trái của ***(29)*** chia hết cho $n(n+2)$ và do đó ***(29)*** được thỏa mãn.

Bây giờ giả sử với số tự nhiên $n>1$ thì đồng dư thức ***(29)*** đúng. Nếu n chẵn nghĩa là $n=2k$ với k là số tự nhiên thì khi đó $n-1\le k$ suy ra $k\,|\,(n-1)!$ và $2k\,|\,(n-1)!4$. Hệ quả là $(n-1)!4\equiv 0(\mathrm{mod}\, n)$ mà theo ***(29)*** suy ra $4\equiv 0(\mathrm{mod}\, n)$ và $2k\,|\,4$, suy ra $k\,|\,2$ nên $k=1$ hoặc $k=2$ do đó $n=2$ hoặc $n=4$. Nhưng đồng dư thức ***(29)*** không đúng với $n=2$ và $n=4$. Vì vậy ***(29)*** kéo theo $(n-1)!+1\equiv 0(\mathrm{mod}\, n)$ và theo Định lý 3^a thì n là số nguyên tố. Cuối cùng với số tự nhiên n thì đồng dư thức $4\big((n-1)!+1\big)+n\equiv 2\big((n+1)!+1\big)(\mathrm{mod}\, n+2)$ đúng, suy ra từ ***(29)***, sử dụng tính chất $n+2$ lẻ, ta có $(n-1)!+1\equiv 0(\mathrm{mod}\, n+2)$. Vì vậy sử dụng Định lý 3^a ta có $n+2$ là số nguyên tố. Vậy n, $n+2$ là cặp số nguyên tố sinh đôi. □

2. Chứng minh rằng nếu $n=a^2+b^2=c^2+d^2$ với a,b,c,d là các số tự nhiên thỏa mãn $a\ge b,\ c\ge d,\ a>c,\ (a,b)=(c,d)=1,$ thì số

(30) $$\sigma=\frac{ac+bd}{(ac+bd,ab+cd)}$$

là ước số của n thỏa mãn $1<\delta<n$.

Chứng minh. Nếu $n=a^2+b^2=c^2+d^2$ thì

(31) $$\begin{cases} n^2=(ac+bd)^2+(ad-bc)^2=(ad+bc)^2+(ac-bd)^2 \\ (ac+bd)(ad+bc)=n(ab+cd)\end{cases}$$

Vì vậy $n\,|\,(ac+bd)(ad+bc)$. Nếu $n\,|\,ac+bd$ thì theo ***(31)*** ta có $ad-bc=0$ suy ra $a/b=c/d$, mà $(a,b)=(c,d)=1,$ suy ra $a=c$, và $(a,b)=(c,d)=1$ suy ra $a=d$, mâu thuẫn với giả thiết $a>c\ge d$. Các số $n_1=ac+bd$ và $n_2=ad+bc$ đều không chia hết cho n, vì từ tính chất $n\,|\,n_1\ n_2$ bài tập 2 Chương 1 mục 6 và công thức ***(31)*** suy ra δ là ước số của số n và $1<\sigma<n$.

3. Chứng minh định lý sau đây của Liouville [1]: *nếu p là số nguyên tố >5 thì số $(p-1)!+1$ không phải lũy thừa bậc k của p với mọi số tự nhiên k.*

Chứng minh. Như đã chứng minh ở trên, nếu số tự nhiên n là hợp số $\ne 4$ thì $n\,|\,(n-1)!$. Do đó nếu p là số nguyên tố >5 thì $p-1\,|\,(p-2)!$ suy ra $(p-1)^2\,|\,(p-1)!$. Mặt khác áp dụng công thức nhị thức cho $\big(1+(p-1)\big)^k=p^k$ với k là số tự nhiên thì $(p-1)^2\,|\,1+k(p-1)-p^k$. Nếu $(p-1)!+1=p^k$ thì $(p-1)^2\,|\,k(p-1)-(p-1)!$, theo công thức $(p-1)^2\,|\,(p-1)!$ suy ra $(p-1)^2\,|\,k(p-1)$ và do đó $p-1\,|\,k$ suy ra $k\ge p-1$ nên $(p-1)!+1=p^k\ge p^{p-1}$, vô lý vì $(p-1)\le (p-1)^{p-2}$.

4. Chứng minh rằng nếu p là số nguyên tố >5 thì số $(p-1)!+1$ có ít nhất hai ước số nguyên tố phân biệt.

Chứng minh. Theo Định lý 3 thì số $(p-1)!+1$ có ít nhất một ước số nguyên tố p. Theo bài tập 3 thì số này không phải lũy thừa bậc k của p với mọi số tự nhiên k do đó nó phải có ước số nguyên tố khác. □

5. Chứng minh định lý Lerch [1] nói rằng nếu p là số nguyên tố lẻ thì

$$1^{p-1}+2^{p-1}+\ldots+(p-1)^{p-1}\equiv p+(p-1)!\pmod{p^2}$$

Chứng minh. Với p là số nguyên tố lẻ thì theo Định lý 3 số $\dfrac{(p-1)!+1}{p}$ nguyên. Gọi r là số dư nhận được khi chia số này cho p thì ta có $\dfrac{(p-1)!+1}{p}\equiv r\pmod{p}$. Vì vậy $(p-1)!\equiv pr-1\pmod{p^2}$.

Theo Định lý 5 với $a=1,2,\ldots p-1$ thì số $\dfrac{a^{p-1}-1}{p}$ nguyên, gọi r_a là số dư nhận được khi chia số đó cho p thì $\dfrac{a^{p-1}-1}{p}\equiv r_\alpha \pmod{p}$. Do đó

(32) $$a^{p-1}\equiv pr_a+1\pmod{p^2}$$

Suy ra

$$((p-1)!)^{p-1}=1^{p-1}.2^{p-1}\ldots(p-1)^{p-1}\equiv(pr_1+1)(pr_2+1)\ldots(pr_{p-1}+1)\equiv 1+p(r_1+r_2+\ldots+r_{p-1})\pmod{p^2}$$

Nhưng vì $(p-1)!\equiv pr-1\pmod{p^2}$ suy ra

$$((p-1)!)^{p-1}\equiv(pr-1)^{p-1}\equiv 1-(p-1)\,pr\equiv 1+pr\pmod{p^2}$$

So sánh với công thức của $((p-1)!)^{p-1}$ ta có $p(r_1+r_2+\ldots+r_{p-1})\equiv pr\pmod{p^2}$ suy ra theo ***(32)***

$$\begin{aligned}1^{p-1}+2^{p-1}+\ldots+(p-1)^{p-1}&\equiv p(r_1+r_2+\ldots+r_{p-1})+p-1\\&\equiv pr+p-1\equiv(p-1)!+p\pmod{p^2}\end{aligned}$$

6. Chứng minh rằng mọi số nguyên tố $p>5$ đều là ước số của số $n_p=111\ldots1$ được biểu diễn trong hệ thập phân với $p-1$ chữ số 1.

Chứng minh. Xét số nguyên tố $p>5$. Khi đó $(10,p)=1$ và $9n_p=10^{p-1}-1$. Theo Định lý 5 thì $10^{p-1}\equiv 1\pmod{p}$ suy ra $p\mid 9n_p$. Nhưng vì $(p,9)=1$ (với p là số nguyên tố >5) ta có $p\mid n_p$. □

7. Chứng minh rằng nếu p là số nguyên tố và c là số nguyên thì tồn tại vô hạn số tự nhiên x thỏa mãn dãy vô hạn các đồng dư thức sau

(*) $$x=c\pmod{p},\quad x^x\equiv c\pmod{p},\quad x^{x^x}\equiv c\pmod{p},\ldots$$

Chứng minh. Với p là số nguyên tố và c là số nguyên cho trước thì vì $(p,p-1)=1$ suy ra tồn tại vô hạn số tự nhiên $x>1$ mà $x\equiv c\pmod{p}$ và $x\equiv 1\pmod{p-1}$. Vì vậy $x^k\equiv 1\pmod{p-1}$ với $k=1,2,\ldots$ Do đó $x^k=1+(p-1)l_k$ mà $x>1$ nên l_k là số tự nhiên. Vì vậy $x^{x^x}=x\left(x^{l_k}\right)^{p-1}\pmod{p}$.

Nếu $p \mid c$ thì $x \equiv 0 \pmod p$ và rõ ràng x thỏa mãn các đồng dư thức ***(*)***. Nếu c không chia hết cho p thì $(c, p) = 1$ và vì $(x, p) = 1$ nên $\left(x^{l_k}, p\right) = 1$. Vậy theo Định lý 5 suy ra $\left(x^{l_k}\right)^{p-1} \equiv 1 \pmod p$ do đó $x^{x^x} \equiv x \equiv c \pmod p$ với mọi $k = 1, 2, \ldots$ Thế $1, x, x^x, x^{x^x}, \ldots$ cho k ta nhận được ***(*)***. □

Các đồng dư thức dạng ***(*)*** cũng được nghiên cứu với các modulo tùy ý (Schinzel và Sierpinski [4]).

8. Tìm tất cả các số tự nhiên mà mỗi số có đúng một biểu diễn dưới dạng tổng hai bình phương các số tự nhiên nguyên tố cùng nhau (không xét các biểu diễn sai khác hoán vị)

Lời giải. Ta sẽ chứng minh rằng các số cần tìm là các lũy thừa tự nhiên của các số nguyên tố có dạng $4k + 1$.

Bổ đề 1. *Nếu p là số nguyên tố có dạng $4t + 1$ thì với $k = 1, 2, \ldots$, số p^k có đúng một biểu diễn thành tổng hai bình phương các số tự nhiên nguyên tố cùng nhau.*

Chứng minh bổ đề 1. Theo Định lý 11 thì bổ đề đúng với $k = 1$. Xét k là số tự nhiên tùy ý và giả sử bổ đề đúng với k. Khi đó tồn tại các số tự nhiên c và d thỏa mãn $(c, d) = 1$ và $p^k = c^2 + d^2$. Từ Định lý 11 suy ra tồn tại các số tự nhiên a, b mà $(a, b) = 1$ và $p = a^2 + b^2$. Vì vậy

$$\textbf{(33)} \quad p^{k+1} = \left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2$$

Nếu mỗi số $ad - bc$ và $ac - bd$ đều chia hết cho p thì $ad \equiv bc \pmod p$ và $ac \equiv bd \pmod p$ và suy ra $a^2cd \equiv b^2cd \pmod p$ do đó $p \mid cd(a^2 - b^2)$. Nhưng vì $p^k = c^2 + d^2$ và $(c, d) = 1$ nên cả hai số c và d đều không chia hết cho p. Hệ quả là từ $p \mid a^2 - b^2$ và $p \mid a^2 + b^2$ suy ra $p \mid a$ và vì $p = a^2 + b^2$ nên $p \mid b$, mâu thuẫn với giả thiết $(a, b) = 1$. Vì vậy ít nhất một trong các số $ad - bc$ và $ac - bd$ không chia hết cho p. Nếu đó là số $ad - bc$ thì theo ***(33)*** số $ac + bd$ cũng không chia hết cho p. Khi đó các số $ac + bd$ và $ad - bc$ nguyên tố cùng nhau vì theo ***(33)*** thì các ước số chung của chúng phải là ước số của p^{k+1} nhưng p không phải ước số của bất kỳ số nào trong chúng. Tương tự nếu $ac - bd$ không chia hết cho p thì các số $ad + bc$ và $ac - bd$ nguyên tố cùng nhau. Vì vậy trong mọi trường hợp thì công thức ***(33)*** cho ta biểu diễn của p^{k+1} thành tổng hai bình phương các số tự nhiên nguyên tố cùng nhau. Vậy theo quy nạp chứng tỏ với mọi $k = 1, 2, \ldots$ thì số p^k là tổng hai bình phương các số tự nhiên nguyên tố cùng nhau.

Bây giờ giả sử với số tự nhiên k thì số p^k có hai biểu diễn phân biệt thành tổng hai bình phương các số tự nhiên nguyên tố cùng nhau. Đặt $p^k = a^2 + b^2 = c^2 + d^2$ với $(a, b) = (c, d) = 1$ và $a \geq b, c \geq d, a > c$. Ta có

$$\textbf{(34)} \qquad p^{2k} = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2$$

$$\text{và } (ac + bd)(ad + bc) = (ab + cd)\, p^k.$$

Do đó ít nhất một trong các số $ac + bd$ và $ad + bc$ chia hết cho p. Nếu cả hai số đều chia hết cho p thì theo ***(34)*** ta có $ad \equiv bc \pmod p$ và $ac \equiv bd \pmod p$ suy ra $p \mid cd\left(a^2 - b^2\right)$ và từ $p^k = c^2 + d^2$ và $(c, d) = 1$ suy ra $p \mid a^2 - b^2$ mà $p \mid a^2 + b^2$ suy ra $p \mid 2a^2$ mà p là số lẻ nên suy ra $p \mid a$. Nhưng khi đó vì $p \mid a^2 + b^2$ ta có $p \mid b$, mâu thuẫn với $(a, b) = 1$. Vì vậy có đúng một trong các số $ac + bd$ và $ad + bc$ chia hết cho p. Nhưng tích của chúng là bội số của p^k nên số chia hết cho p phải chia hết cho p^k. Nếu $p^k \mid ac + bd$ thì theo ***(34)*** suy ra $ad - bc = 0$ do đó $a / b = c / d$ mà

$(a,b)=(c,d)=1$ suy ra $a=c$, mâu thuẫn với giả thiết. Nếu $p^k \mid ad+bc$ thì theo ***(34)*** ta có $ac-bd=0$ và suy ra $a/b=d/c$ mà $(a,b)=(c,d)=1$ suy ra $a=d$, mâu thuẫn với $a>c\geq d$. Bổ đề 1 được chứng. □

Để chứng minh định lý ta chỉ cần chứng minh rằng nếu số tự nhiên lẻ nào đó có biểu diễn duy nhất (không tính các hoán vị) thành tổng bình phương hai số tự nhiên nguyên tố cùng nhau thì số đó là lũy thừa tự nhiên của một số nguyên tố có dạng $4k+1$.

Bổ đề 2. *Nếu m và n là các số tự nhiên lẻ nguyên tố cùng nhau và mỗi số đều có thể biểu diễn thành tổng bình phương hai số tự nhiên nguyên tố cùng nhau thì tích của chúng có ít nhất hai cách biểu diễn thành tổng bình phương hai số tự nhiên nguyên tố cùng nhau (không tính các hoán vị).*

Chứng minh bổ đề 2. Giả sử m và n là các số tự nhiên lẻ nguyên tố cùng nhau và a,b,c,d là các số tự nhiên thỏa mãn $(a,b)=(c,d)=1, m=a^2+b^2, n=c^2+d^2$. Giả sử $a\geq b, c\geq d$ ta có

(35) $$mn=(ac+bd)^2+(ad-bc)^2=(ad+bc)^2+(ac-bd)^2$$

và

(36) $$(ac+bd)(ad+bc)=cdm+abn$$

Các biểu diễn mn thành tổng các bình phương cho bởi ***(35)*** là phân biệt bởi vì nếu $ac+bd=ad-bc$ thì ta có $(a-b)(c-d)=0$ và do đó $a=b$ hoặc $c=d$, điều này là không thể vì các số m và n lẻ và nếu $ac+bd=ac-bd$ (số $ac-bd\geq 0$ vì $a\geq b, c\geq d$) thì ta có $ac=0$, vô lý. Vậy để chứng minh Bổ đề 2 ta chỉ cần chứng minh $(ac+bd, ad-bc)=1$ và $(ad+bc, ac-bd)=1$. Nếu $(ac+bd, ad-bc)>1$ thì các số $ac+bd$ và $ad-bc$ có ước số nguyên tố chung p. Vì vậy theo ***(35)*** thì $p \mid mn$ và do đó $p \mid m$ hoặc $p \mid n$. Nếu $p \mid m$ thì theo ***(36)*** ta có $p \mid abn$ mà $p \mid m$ và $(m,n)=1$ suy ra $p \mid ab$, do đó $p \mid a$ hoặc $p \mid b$ mà $p \mid m=a^2+b^2$ suy ra $p \mid a$ và $p \mid b$, mâu thuẫn với giả thiết $(a,b)=1$. Nếu $p \mid n$ thì theo ***(36)*** ta có $p \mid cdm$ mà $(m,n)=1$ suy ra $p \mid cd$ mà $p \mid c^2+d^2$ và $(c,d)=1$ suy ra mâu thuẫn. Bổ đề 2 được chứng minh. □

Bây giờ giả sử số lẻ n có biểu diễn duy nhất thành tổng hai bình phương các số tự nhiên nguyên tố cùng nhau. Giả sử $n=a^2+b^2$ là biểu diễn duy nhất đó và p là ước số nguyên tố của n. Khi đó p là số lẻ. Nếu $p=4k+3$ thì lũy thừa cả hai vế của đồng dư thức $a^2\equiv -b^2 \pmod p$ lên $\frac{1}{2}(p-1)=(2k+1)$ lần thì ta có $a^{p-1}\equiv -b^{p-1} \pmod p$ nhưng $(a,b)=1$ và $(a,p)=(b,p)=1$, sử dụng Định lý 5 ta có $a^{p-1}\equiv -b^{p-1}\equiv 1 \pmod p$. Vì vậy $1\equiv -1 \pmod p$ suy ra $p \mid 2$, vô lý. Vậy mọi ước số nguyên tố của n đều có dạng $4k+1$. Do đó phân tích thành thừa số nguyên tố của n là $n=q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_k^{\alpha_k}$ với $\alpha_1,\alpha_2,\ldots,\alpha_k$ và k là các số tự nhiên và các số nguyên tố $q_i\ (i=1,2,\ldots,k)$ đều có dạng $4t+1$. Nếu $k=1$ thì không còn gì để chứng minh. Giả sử $k>1$. Khi đó các số $q_1^{\alpha_1}, q_2^{\alpha_2}, \ldots q_k^{\alpha_k}$ là đôi một nguyên tố cùng nhau. Từ Bổ đề 1 suy ra mỗi số đó đều là tổng hai bình phương các số tự nhiên nguyên tố cùng nhau. Nên theo Bổ đề 2 suy ra số $q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_{k-1}^{\alpha_{k-1}}$ cũng là tổng hai bình phương các số tự nhiên nguyên tố cùng nhau. Vì $(q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_{k-1}^{\alpha_{k-1}}, q_k^{\alpha_k})=1$ nên số $q_1^{\alpha_1}\cdot q_2^{\alpha_2}\cdot\ldots q_k^{\alpha_k}=n$ có ít nhất hai biểu diễn phân biệt thành tổng hai bình phương các số tự nhiên nguyên tố cùng nhau, mâu thuẫn với giả thiết. Vậy ta có $k=1$ và định lý được chứng minh (Sierpinski [29]). □

6. Các số idonei

Ta sử dụng tên gọi này cho các số d có tính chất sau đây: nếu số lẻ $n>1$ có biểu diễn duy nhất (không tính các hoán vị) dưới dạng x^2+y^2d với x, y là các số nguyên không âm và các hạng tử là nguyên tố cùng nhau thì n là số nguyên tố *(1)*.

Từ Định lý 11 suy ra 1 thuộc lớp các số này. Euler đã tìm ra 65 số như vậy: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848.

Các số d đã được nghiên cứu tới $5\cdot10^{10}$ (Weinberger [1]) nhưng ta vẫn chưa tìm được số idonei nào lớn hơn 1848. Vào năm 1934 S.Chowla [1] đã chứng minh rằng số các số idonei là hữu hạn, sau đó Schowla cùng với W.E.Briggs đã chứng minh rằng có nhiều nhất một số như vậy lớn hơn 10^{65} mà không có ước số chính phương (Chowla và Briggs [1]). Cuối cùng P.Weinberger [1] đã thay 10^{65} bởi 1365. Các số idonei mà có ước số chính phương thì hoặc là nhỏ hơn 100 hoặc có dạng $4d$ với d là số idonei chẵn không có ước số chính phương (Grube [1] hoặc Grosswald [1]). Các thông tin khác về các số idonei có thể tìm trong các bài báo của I.G.Melnikov [1] và J.Steinig [1].

7. Các số giả nguyên tố và giả nguyên tố tuyệt đối

Từ Định lý 5^{α} ta có nếu n là số nguyên tố thì $n\,|\,2^n-2$. Các nhà toán học Trung Hoa 25 thế kỷ trước cho rằng mệnh đề ngược lại cũng đúng. Mệnh đề này đúng với các số tự nhiên $n\le300$ *(2)*. Số 341 là hợp số (bằng $11\cdot31$) và $341\,|\,2^{341}-2$. Thật vậy vì 11 và 31 là các số nguyên tố lẻ nên theo Định lý 5 ta có $2^{10}\equiv1(\mathrm{mod}11)$ và rõ ràng $2^{10}\equiv1(\mathrm{mod}31)$. Vì vậy $2^{341}\equiv2\cdot2^{340}\equiv2(\mathrm{mod}11)$ và $2^{341}\equiv2(\mathrm{mod}31)$. Do đó $2^{341}-2$ chia hết cho 11 và 31, nên nó chia hết cho tích $11\cdot31=341$.

Các hợp số n mà $n\,|\,2^n-2$ được gọi là các số giả nguyên tố.

Tất cả các số giả nguyên tố ≤2000 là: $341=11\cdot31$, $561=3\cdot11\cdot17$, $645=3\cdot5\cdot43$, $1105=5\cdot13\cdot17$, $1387=19\cdot73$, $1729=7\cdot13\cdot19$, $1905=3\cdot5\cdot127$. P.Poulet [2] đã lập bảng tất cả các số giả nguyên tố lẻ nhỏ hơn 10^8 và C.Pomerance, J.L.Selfridge và S.S.Wagstaff Jr. [1] đã nâng lên thành $25\cdot10^9$.

Định lý 12. *Tồn tại vô hạn các số giả nguyên tố* *(1)*

Bổ đề. *Nếu n là số giả nguyên tố lẻ thì số $m=2^n-1$ cũng là số giả nguyên tố tố lẻ. Rõ ràng $m>n$.*

Chứng minh bổ đề. Giả sử n là số giả nguyên tố thì n là hợp số và do đó nó có ước số q mà $1<q<n$. Ta có $1<2^q-1<2^n-1=m$. Từ đây suy ra m là hợp số lẻ vì n lẻ. Do đó vì n là số giả nguyên tố nên $\left(2^n-2\right)/n$ là số nguyên. Ta thấy số $\left(2^n-2\right)/n$ chẵn. Từ đây suy ra $2n\,|\,2^n-2$ do đó $n\,|\,2^{n-1}-1$. Hệ quả là với số nguyên k ta có $2^{n-1}-1=kn$. Vì vậy $2^{m-1}=2^{2^n-2}=2^{2kn}$ và do đó $2^{m-1}-1=\left(2^n\right)^{2k}-1$ suy ra $2^n-1\,|\,2^{m-1}-1$ nên $m\,|\,2^m-2$, nghĩa là m là số giả nguyên tố. Rõ ràng $m>n$ vì $n>2$ (n là hợp số) nên ta có $2^n>n+1$ và do đó $m>n$. Bổ đề được chứng minh.

Định lý 12 là hệ quả trực tiếp của bổ đề với lưu ý tồn tại các số giả nguyên tố lẻ, ví dụ $n=341$.

Ký hiệu $P(x)$ là số các số giả nguyên tố nhỏ hơn x ta có ước lượng sau đây bởi C.Pomerance [3],[4]: $\exp(\log x)^{5/14}<P(x)<x\exp\left(-\dfrac{\log x\log\log\log x}{2\log\log x}\right)$ với x đủ lớn.

---

(1) Một số định nghĩa khác được trình bày bởi rất nhiều tác giả nhưng nói chung là không chính xác. Định nghĩa chính xác đầu tiên được trình bày bởi F.Grube [1] tương đối phức tạp. Theo đó các số này được gọi là số Euler.

(2) Lưu ý rằng vào các năm 1680-81 Leibniz đã chứng minh rằng 2^n-2 không chia hết cho n trừ khi n là số nguyên tố. Tuy nhiên chứng minh đó là sai (Dickson [7] tập 1 trang 64).

(1) Cipolla [1], D.H.Lehmer [3], Sierpinski [6].

Tới tận năm 1950 các số giả nguyên tố lẻ mới được biết tới. D.H.Lehmer là người đầu tiên tìm các số giả nguyên tố chẵn. Đó là số $n = 161038$. Không dễ để tìm được số này, nhưng để chứng minh nó là số giả nguyên tố thì khá đơn giản và sơ cấp. Tính toán trực tiếp ta có

$$n = 2\cdot 73\cdot 1103,\ n-1 = 3^2\cdot 29\cdot 617,\ 2^9-1 = 7\cdot 73,\ 2^{29}-1 = 233\cdot 1103\cdot 2089$$

Vì $9 | n-1$ và $29 | n-1$ suy ra $2^9-1 | 2^{n-1}-1$ và $2^{29}-1 | 2^{n-1}-1$. Lưu ý rằng $73 | 2^9-1$ và $1103 | 2^{29}-1$ suy ra 2^n-2 chia hết cho 73 và 1103. Nhưng đây là số chẵn nên nó chia hết cho 2, vì vậy $n | 2^n-2$. Suy ra *n* là số giả nguyên tố.

N.G.W.H Beeger [1] đã chứng minh rằng tồn tại vô hạn số giả nguyên tố chẵn, sau đó A.Rotkiewicz [2] đã chứng minh với các số tự nhiên bất kỳ a và b thì luôn tồn tại vô hạn số giả nguyên tố chẵn n thỏa mãn $n | a^n b - ab^n$. Suy ra với mọi số tự nhiên lẻ a thì tồn tại vô hạn số tự nhiên chẵn *n* mà $n | a^n - a$. (A.Rotkiewicz [7] đã chứng minh với các số tự nhiên a,b tùy ý và số nguyên tố p thì luôn tồn tại vô hạn số n chia hết cho p mà $p | a^n b - ab^n$). A.Rotkiewicz [5],[6] đã chứng minh tồn tại vô hạn số giả nguyên tố có dạng $ax+b\left(x = 0,1,2,\ldots\right)$ với a,b là các số nguyên tố cùng nhau, $a > 0$ (Rotkiewicz [8]).

Các số giả nguyên tố còn được gọi là các số Poulet vì Poulet đã lập bảng các số đó. Các số có mọi ước số d thỏa mãn $d | 2^a - 2$ được gọi là các số siêu-Poulet (Duparc [2]). Ví dụ $n = 2047$. Thật vậy ta có $2047 = 2^{11}-1 = 23\cdot 89$ suy ra theo Định lý 5^8 thì $11 | 2^{11}-2$ suy ra $2^{11}-2 | 2^{2^{11}-1}-2$ và chứng tỏ 2047 là số giả nguyên tố. Các ước số tự nhiên của 2047 là $1, 23, 89$ và 2047. Theo Định lý 5^a $23 | 2^{23}-2$ và $89 | 2^{89}-2$ suy ra 2047 là số siêu-Poulet. Tồn tại các số Poulet nhưng không phải siêu-Poulet. Chẳng hạn $561 = 3\cdot 11\cdot 17$. Thật vậy, 560 chia hết cho $2, 10$ và 16 nên theo Định lý 5 suy ra $3 | 2^2-1 | 2^{560}-1, 11 | 2^{10}-1 | 2^{560}-1 | 17 | 2^{16}-1 | 2^{560}-1$. Vì vậy $561 = 3.11.17 | 2^{560}-1 | 2^{561}-2$ suy ra 561 là số Poulet. Tuy nhiên ước số 33 của 561 thì không phải ước số của $2^{33}-2$ vì $2^{33}-2$ không chia hết cho 11. Vì vậy 561 không phải số siêu-Poulet.

Từ Định lý 5^a suy ra các số Poulet là tích của hai số nguyên tố phân biệt thì đều là số siêu-Poulet. Câu hỏi được đặt ra là có tồn tại vô hạn cặp số nguyên tố phân biệt *p, q* mà $pq | 2^{pq}-2$ hay không. Câu trả lời cho câu hỏi này là khẳng định và được suy ra từ định lý tổng quát hơn của A.Rotkiewicz [1]: *cho trước ba số tự nhiên tùy ý a,b,s. Khi đó tồn tại vô hạn số tự nhiên n là tích của s số nguyên tố phân biệt thỏa mãn $n | a^{n-1}-b^{n-1}$.*

Định lý này suy ra với các số tự nhiên tùy ý a và s thì tồn tại vô hạn số tự nhiên n là tích của các số nguyên tố và $n | a^n - a$ (với s = 2 xem Schinzel [9], D.H.Lehmer [3], Erdor [8]). Từ đây suy ra tồn tại vô hạn số siêu-Poulet.

Mặt khác có thể chứng minh tồn tại vô hạn số Poulet mà không phải siêu-Poulet (bài tập 1)

Hợp số *n* được gọi là số giả nguyên tố tuyệt đối nếu với mọi số nguyên a thì $a^n - a$ chia hết cho n.

Số giả nguyên tố tuyệt đối là số giả nguyên tố, nhưng điều ngược lại không đúng. Chẳng hạn ta có 341 là số giả nguyên tố nhưng nó không phải số giả nguyên tố tuyệt đối vì $11^{341}-11$ không chia hết cho 341 vì ta có $11^2 \equiv -3 (\mathrm{mod}\, 31)$ suy ra $11^{10} \equiv (-3)^5 \equiv 11^{30} \equiv 1 (\mathrm{mod}\, 31)$, $11^{341} \equiv 11^{11} \equiv -1 (\mathrm{mod}\, 31)$. Nhưng vì $11^{30} \equiv 1 (\mathrm{mod}\, 31)$, $11^{341} \equiv 11^{11} \equiv -7 (\mathrm{mod}\, 31)$ suy ra $11^{341}-11 \equiv -18 (\mathrm{mod}\, 31)$..

Dễ dàng chứng minh rằng nếu *n* là tích của *k* số nguyên tố phân biệt $q_1, q_2, \ldots q_k$ với *k* là số tự nhiên >1 và nếu $q_i - 1 | n-1$, $i = 1,2,\ldots,k$ thì *n* là số giả nguyên tố tuyệt đối. Thật vậy từ Định lý 5 suy ra

nếu $i=1,2...k$ và số nguyên a không chia hết cho q_i thì $q_i \mid a^{q_i-1}-1$ mà $q_i-1 \mid n-1$, $q_i \mid a^{n-1}-1$ và ta có $q_i \mid a^n-a$. Tính chất cuối cùng đúng với $q_i \mid a$.

Vì vậy $561=3\cdot 11\cdot 17$ là số giả nguyên tố tuyệt đối vì 560 chia hết cho 2,10 và 16. Có thể chứng minh 561 là số giả nguyên tố tuyệt đối nhỏ nhất.

Dễ thấy với mọi số tự nhiên *m* thì với $n=(6m+1)(12m+1)(18m+1)$ số $n-1$ chia hết cho 36*m* nên suy ra nó chia hết cho 6*m*,12*m* và 18*m*. Vì vậy nếu các số 6*m*+1,12*m*+1 và 18*m*+1 đều là số nguyên tố thì $n=(6m+1)(12m+1)(18m+1)$ là số giả nguyên tố tuyệt đối (Chernick [1]).

Ta không biết có tồn tại vô hạn số giả nguyên tố tuyệt đối hay không. Tuy nhiên từ giả thuyết H (Chương 3 mục 8) suy ra tồn tại vô hạn số tự nhiên *m* mà các số 6*m* + 1,12*m* +1 và 18*m* +1 đều là số nguyên tố. Vì vậy từ giả thuyết H suy ra tồn tại vô hạn số giả nguyên tố tuyệt đối.

Các số $6m+1$, $12m+1$ và $18m+1$ đều là các số nguyên tố với $m=1$, 6, 35, 45, 51. Suy ra các số $1729=7\cdot 13\cdot 19$, $294409=37\cdot 73\cdot \le 109$, $211\cdot 421\cdot 621$, $271\cdot 541\cdot 811$, $307\cdot 613\cdot 919$ đều là các số giả nguyên tố tuyệt đối. Dưới đây là một số số giả nguyên tố tuyệt đối khác

$5\cdot 29\cdot 73$, $5\cdot 17\cdot 29\cdot 113$, $5\cdot 17\cdot 29\cdot 113\cdot 337$, $5\cdot 17\cdot 29\cdot 113\cdot 337\cdot 673$, $5\cdot 17\cdot 29\cdot 113\cdot 337\cdot 673\cdot 2689$,
$7\cdot 23\cdot 41$, $7\cdot 31\cdot 73$, $7\cdot 73\cdot 101$, $7\cdot 13\cdot 31$, $7\cdot 13\cdot 31\cdot 61\cdot 181$, $7\cdot 13\cdot 31\cdot 61\cdot 181\cdot 541$, $7\cdot 13\cdot 31\cdot 61\cdot 181\cdot 541\cdot 2161$,
$13\cdot 37\cdot 61\cdot 181\cdot 541\cdot 2161$, $13\cdot 37\cdot 61$, $13\cdot 37\cdot 91$, $13\cdot 37\cdot 241$, $13\cdot 61\cdot 397$, $13\cdot 97\cdot 421$, $43\cdot 3361\cdot 3907$

Nếu *n* là số giả nguyên tố tuyệt đối thì $n \mid 2^n-2$ và $n \mid 3^n-3$. Ta chưa chứng minh được có tồn tại vô hạn các hợp số n mà $n \mid 2^n-2$ và $n \mid 3^n-3$ hay không?

Nếu *n* là số giả nguyên tố tuyệt đối và a là số nguyên nguyên tố cùng nhau với n thì vì $a^n-n=a(a^{n-1}-1)$ chia hết cho *n* nên $a^{n-1}-1$ chia hết cho n. Hợp số *n* thỏa mãn $n \mid a^{n-1}-1$ với $(a,n)=1$ được gọi là các số Carmichael. Carmichael là người đầu tiên lưu ý sự tồn tại các số như vậy vào năm 1909. Ta thấy mọi số giả nguyên tố tuyệt đối đều là số Carmichael. Điều ngược lại cũng đúng vì có thể chứng minh số tự nhiên *n* là số Carmichael khi và chỉ khi $n=q_1q_2...q_k$ với $k\ge 3$ và $q_1,q_2,...,q_k$ là các số nguyên tố lẻ phân biệt thỏa mãn $q_i-1 \mid n-1, i=1,2...,k$ (Carmichael [2],[3], Sispanov [1], Dupare [1], Knodel [1], Sierpinski [12] trang 186-188). Ước lượng tốt nhất về số các số Carmichael nhỏ hơn một số cho trước được trình bày bởi Pomerance [3].

Có tồn tại các số tự nhiên $n>2$ mà với mọi số nguyên $a, n \mid a^{n-2}-a$. Chẳng hạn *n* =195. Vì $195=3\cdot 5\cdot 13$ nên ta chỉ cần chứng minh với mọi số nguyên a thì số $a^{193}-a$ chia hết cho 3,5 và 13. Gọi p là một trong các số 3,5, 13. Khi đó $p-1 \mid 192$ vì $192=4.48$. Nếu $p \mid a$ thì $p \mid a^{193}-a$. Nếu p không chia hết cho a thì theo Định lý 5, $p \mid a^{p-1}-1$ và vì $p-1 \mid 192$, $p \mid a^{192}-1$ suy ra $p \mid a^{193}-a$. Do đó $p \mid a^{193}-a$ với mọi số nguyên a và p=3,5,13. Vì vậy $195 \mid a^{193}-a$ với mọi số nguyên a.

Tương tự vì $399=3\cdot 7\cdot 19, 18 \mid 396, 1023=3\cdot 11\cdot 31, 30 \mid 1020$ nên ta chứng minh được với mọi số nguyên a thì $399 \mid a^{397}-a, 1023 \mid a^{1021}-a$.

Nếu *n* là số tự nhiên >3 thỏa mãn $n \mid a^{n-2}-a$ với mọi số nguyên a thì với $(a,n)=1$ ta có $n \mid a^{p-3}-1$. Số $n>3$ mà $n \mid a^{n-3}-1$ với $(a,n)=1$ được D.C Morrow [1] gọi là các D-số. Ta chứng minh rằng mọi số có dạng *n* = 3p với p là số nguyên tố ≥ 3 đều là các D-số. Nếu $p=3$ nghĩa là $n=9$ thì ta thấy $9 \mid a^6-1$ với mọi a mà $(a,9)=1$. Giả sử p là số nguyên tố >3 và a là số nguyên thỏa mãn $(a,3p)=1$. Khi đó $(a,p)=1$ và theo Định lý 5, $p \mid a^{p-1}-1$ suy ra $p \mid a^{3p-3}-1$. Nhưng vì $(a,3p)=1$ nên số a không chia hết cho 3 và số $p-1$ chẵn (vì p là số nguyên tố lẻ) do đó

$3 | a^{3(p-1)} - 1$. Chứng tỏ số $a^{3p-3} - 1$ chia hết cho p và 3 mà vì $(p,3) = 1$ nên số đó chia hết cho 3p. Suy ra $3p | a^{3p-3} - 1$ với mọi a thỏa mãn $(a,3p) = 1$ và do đó 3p là D-số.

A.Makowski [7] đã chứng minh định lý tổng quát hơn nói rằng với mọi số tự nhiên $k \geq 2$ thì luôn tồn tại vô hạn hợp số *n* mà với mọi số nguyên a thỏa mãn $(a,n) = 1$ thì $n | a^{n-k} - 1$ (chứng minh định lý này có trong Chương 6 mục 5).

Bài tập. ***1.*** Chứng minh rằng không tồn tại số siêu-Poulet chẵn.

Chứng minh. Giả sử phản chứng rằng 2*n* là một số siêu-Poulet. Khi đó $2n | 2^{2n} - 2$ suy ra $n | 2^{2n} - 1$ và chứng tỏ *n* là số lẻ. Vì 2*n* là số siêu-Poulet nên $n | 2^n - 2$ suy ra vì *n* lẻ nên ta có $n | 2^{n-1} - 1$. Do đó vì $n | 2^{n-1} - 1$ nên $n | 2^{2n-1} - 2^{n-1} = 2^{n-1}(2^n - 1)$. Lại vì *n* lẻ nên ta có $n | 2^{n-1} - 1$ và so sánh với $n | 2^n - 2$ chứng tỏ $n = 1$, điều này là vô lý vì $2n$ là hợp số.

Ta đã đề cập tới định lý Beeger nói rằng tồn tại vô hạn số Poulet chẵn.

Bài tập 1 suy ra các số này không phải số siêu-Poulet.

2. Chứng minh rằng $n = 2 \cdot 73 \cdot 1103 \cdot 2089$ là số giả nguyên tố. (S.Maciag)

Chứng minh. Ta có *n* = 2089*m* với *m* là số giả nguyên tố và $9 | m-1, 29 | m-1$. Vì vậy $n-1 = (m-1)2089 + 2088$. Do $2088 = 2^3.3^2.29$ mà $9 | m-1$ và $29 | m-1$ nên suy ra $9 | n-1$ và $29 | n-1$. Vì vậy từ $2^9 - 1 = 7.73$ và $2^{29} - 1 = 233.1103.2089$ suy ra $73 | 2^{n-1} - 1, 1103 | 2^{n-1} - 1$ và vì $2089 | 2^{29} - 1, 2089 | 2^{n-1} - 1$. Bây giờ dựa vào phân tích thành thừa số nguyên tố của *n* suy ra $n | 2^n - 2$.

3. Chứng minh rằng tồn tại vô hạn số Mersenne là số Poulet.

Tính chất này suy ra trực tiếp từ bổ đề trong chứng minh Định lý 12 và tính chất tồn tại các số Poulet lẻ (chẳng hạn 341).

Tuy nhiên ta không biết có tồn tại vô hạn số Mersenne là số siêu-Poulet hay không.

4. Chứng minh rằng $n | 2^n - 1$ không đúng với mọi số tự nhiên $n > 1$.

Chứng minh. Giả sử phản chứng rằng *n* là số tự nhiên lớn hơn 1 và thỏa mãn $n | 2^n - 1$. Gọi p là ước số nguyên tố nhỏ nhất của *n* và σ là số nhỏ nhất mà $p | 2^\sigma - 1$. Vì p >1 suy ra $\sigma > 1$. Hơn nữa từ $p | 2^n - 1$ suy ra $\sigma | n$. Nếu *n* chia cho σ dư r với $0 < r < \sigma$ thì *n*=$k\sigma$ +r suy ra $2^n - 1 = 2^{k\sigma} 2^r - 1$. Nhưng vì $p | 2^r - 1$ nên ta có $2^\sigma \equiv 1 (\mathrm{mod}\, p)$ và suy ra $2^n - 1 \equiv \tau - 1 (\mathrm{mod}\, p)$ mà vì $p | 2^n - 1$ suy ra $p | 2^r - 1$và ta có mâu thuẫn với định nghĩa của σ. Từ định lý Fermat nhỏ suy ra $p | 2^{p-1} - 1$ và ta có $p | 2^r - 1$ (vì *n* lẻ và do đó p lẻ). Vì vậy từ định nghĩa của σ suy ra $\sigma \leq p - 1$ nên $1 < \sigma < p$, mâu thuẫn với định nghĩa của p.

Ghi chú. Dễ dàng chứng minh rằng tồn tại vô hạn số tự nhiên *n* thỏa mãn $n | 2^n + 1$ chẳng hạn các số $n = 3^k$ với *k*=0,1, 2, ... Không khó để chứng minh tồn tại vô hạn các số tự nhiên *n* mà $n | 2^n + 2$. Thật vậy, ta thấy tính chất này đúng với *n* = 2 và nếu *n* là số tự nhiên chẵn thỏa mãn $n | 2^n + 2$ và $n - 1 | 2^n + 1$ thì các số $m = 2^n + 2$ thỏa mãn $m | 2^m + 2$ và $m - 1 | 2^m + 1$. Vì vậy ta nhận được các số *n*=2,6,66, ...

Có thể chứng minh không tồn tại số tự nhiên $n > 1$ mà $n | 2^{n-1} + 1$.

5. Chứng minh rằng tồn tại vô hạn hợp số n thỏa mãn $n | a^{n-1} - a$ với mọi số nguyên a.

Gợi ý. Chỉ cần đặt n=2p với p là số nguyên tố lẻ.

8. Định lý Lagrange

Định lý 13 (Lagrange). *Nếu n là số tự nhiên và f(x) là đa thức bậc n biến x với các hệ số nguyên, và nếu hệ số của x^n không chia hết cho p thì đồng dư thức $f(x)\equiv 0(\mathrm{mod}\, p)$ có nhiều nhất n nghiệm.*

Chứng minh. Từ hệ quả của Định lý 2 suy ra Định lý 13 đúng với n=1. Ký hiệu n là số tự nhiên tùy ý >1 và giả sử Định lý 13 đúng với đa thức bậc $n-1$. Giả sử $f(x)=a_o x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ là đa thức hệ số nguyên thỏa mãn a_o không chia hết cho số nguyên tố p và giả sử đồng dư thức

(37) $$f(x)\equiv 0(\mathrm{mod}\, p)$$

có nhiều hơn n nghiệm. Khi đó tồn tại $n+1$ số $x_1, x_2, \ldots, x_{n+1}$ là các nghiệm phân biệt của đồng dư thức ***(37)***. Đặc biệt $f(x_1)=0(\mathrm{mod}\, p)$. Ta có

$$f(x)-f(x_1)=a_0\left(x^n-x_1^n\right)+a_1\left(x^{n-1}-x_1^{n-1}\right)+\ldots+a_{n-1}(x-x_1).$$

Nhưng vì $x^k-x_1^k=(x-x_1)\left(x^{k-1}+x^{k-2}x_1+\ldots+x_1^{k-1}\right)$, suy ra

(38) $$f(x)-f(x_1)=(x-x_1)g(x),$$

với $g(x)$ là đa thức bậc $n-1$ với biến số x và các hệ số nguyên. Hơn nữa hệ số của x^{n-1} là a_0 và theo giả thiết thì hệ số này không chia hết cho p. Vì vậy theo ***(38)*** và lưu ý $f(x_1)\equiv 0(\mathrm{mod}\, p)$, đồng dư thức ***(37)*** tương đương với đồng dư thức

(39) $$(x-x_1)g(x)\equiv 0(\mathrm{mod}\, p).$$

Do đó các số $x_1, x_2, \ldots, x_{n+1}$ là nghiệm của đồng dư thức ***(39)***. Với $i=2,3,\ldots,n+1$ ta có $p\,|\,(x_i-x_1)g(x_i)$ mà $x_1, x_2, \ldots, x_{n+1}$ là các nghiệm phân biệt của ***(37)*** suy ra $p\,|\,g(x_i)$ với $i=2,3,\ldots,n+1$. Chứng tỏ đồng dư thức $g(x)\equiv 0(\mathrm{mod}\, p)$ có ít nhất n nghiệm phân biệt, mâu thuẫn với giả thiết Định lý 13 đúng với các đa thức bậc $n-1$.

Do đó ta kết luận đồng dư thức ***(37)*** có không quá n nghiệm, và theo quy nạp suy ra Định lý 13.

Trong Định lý 13 thì giả thiết modulo p nguyên tố là cần thiết. Chẳng hạn đồng dư thức $x^2-1\equiv 0(\mathrm{mod}\, 8)$ có bốn nghiệm 1,3,5,7. Tương tự đồng dư thức $x^2+3x+2\equiv 0(\mathrm{mod}\, 6)$ có bốn nghiệm 1,2,4,5 trong khi hệ số của lũy thừa cao nhất là nguyên tố cùng nhau với modulo.

Có thể chứng minh nếu m là hợp số thì chỉ khi $m=4$ thì định lý sau đây đúng: *nếu $f(x)$ là đa thức bậc n với hệ số nguyên mà hệ số của lũy thừa cao nhất nguyên tố cùng nhau với m thì đồng dư thức $f(x)\equiv 0(\mathrm{mod}\, m)$ có nhiều nhất n nghiệm phân biệt* (Sierpinski [12] trang 180-181)

Hệ quả. *Nếu đồng dư thức bậc n với hệ số nguyên và modulo nguyên tố p có nhiều hơn n nghiệm thì tất cả các hệ số của nó đều chia hết cho p.*

Chứng minh. Giả sử ***(37)*** là đồng dư thức thỏa mãn các điều kiện trên và đặt

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$$

Giả sử trong các số $a_0, a_1, \ldots a_n$ có số không chia hết cho p khi đó gọi a_m là số đầu tiên trong dãy $a_0, a_1, \ldots a_n$ mà không chia hết cho p. Khi đó với mọi số nguyên x ta có

$$f(x)\equiv a_mx^{n-m}+a_{m+1}x^{n-m-1}+\ldots+a_{n-1}x+a_n\,(\mathrm{mod}\, p)$$

Nếu $n=m$ thì $f(x)\equiv a_n \pmod p$ và vì đồng dư thức ***(37)*** có nhiều hơn n nghiệm nên tồn tại số nguyên x thỏa mãn $f(x)\equiv 0 \pmod p$ suy ra $a_n \equiv 0 \pmod p$. Do đó $m<n$. Hệ quả là đa thức $a_m x^{n-m}+...+=a_{n-1}x+a_n$ thỏa mãn các điều kiện của Định lý 13 do đó nó có nhiều nhất $n-m\le n$ nghiệm phân biệt, mâu thuẫn với giả thiết. Hệ quả được chứng minh.

Nếu tất cả các hệ số của đồng dư thức là chia hết cho modulo thì hiển nhiên đồng dư thức đúng. Tuy nhiên điều ngược lại không đúng. Chẳng hạn đồng dư thức $x^2+x\equiv 0 \pmod 2$ luôn đúng.

Tương tự theo Định lý 5^a thì đồng dư thức $x^{17}-x\equiv 0 \pmod{17}$ luôn đúng.

Ứng dụng đơn giản của Định lý 5^a suy ra mọi đồng dư thức với modulo nguyên tố p là tương đương với một đồng dư thức bậc không lớn hơn p. Thật vậy, theo Định lý 5^a thì với số nguyên x ta có $x^p \equiv x \pmod p$, $x^{p+1}\equiv x^2 \pmod p$ và cứ như vậy. Chứng tỏ mọi lũy thừa bậc $\ge p$ của biến x có thể thay bởi một lũy thừa bậc $\le p-1$ của x.

Định lý 14. *Nếu $m=ab$ với a,b là các số tự nhiên nguyên tố cùng nhau thì số các nghiệm của đồng dư thức*

(40) $$f(x)\equiv 0 \pmod m$$

với $f(x)$ *là đa thức biến x hệ số nguyên là bằng với tích các nghiệm của các đồng dư thức*

(41) $$f(x)\equiv 0 \pmod a$$

và số nghiệm của đồng dư thức

(42) $$f(x)\equiv 0 \pmod b$$

Chứng minh. Nếu x là nghiệm của đồng dư thức ***(40)*** thì nó là nghiệm của các đồng dư thức ***(41)*** và ***(42)*** bởi vì nếu $m \mid f(x)$ thì $a \mid f(x)$ và $b \mid f(x)$. Vì vậy mỗi nghiệm của đồng dư thức ***(40)*** tương ứng với một cặp (u,v), u là nghiệm của đồng dư thức ***(41)*** và v là nghiệm của đồng dư thức ***(42)***. Cụ thể hơn u là số dư nhận được khi chia x cho a, v là số dư nhận được khi chia x cho b.

Dễ thấy các cặp u,v phân biệt tương ứng với các nghiệm phân biệt của đồng dư thức ***(40)***. Thật vậy nếu hai nghiệm phân biệt x,y cùng tương ứng với cặp (u,v) thì $x\equiv y \pmod a$ và $x\equiv y \pmod b$ mà $(a,b)=1$ suy ra $m=ab \mid x-y$ và do đó $x\equiv y \pmod m$, mâu thuẫn với giả thiết các nghiệm x,y phân biệt.

Bây giờ giả sử u là nghiệm của đồng dư thức ***(41)*** và v là nghiệm của đồng dư thức ***(42)*** thì vì $(a,b)=1$, theo định lý số dư Trung Hoa (Chương 1 mục 12) suy ra tồn tại số nguyên x thỏa mãn $x\equiv u \pmod a$ và $x\equiv v \pmod b$. Suy ra (theo Định lý 1) $f(x)\equiv f(u) \pmod a$ và $f(x)\equiv f(v) \pmod b$. Nhưng vì $f(u)\equiv 0 \pmod a$ và $f(v)\equiv 0 \pmod b$ nên $f(x)\equiv 0 \pmod a$ và $f(x)\equiv 0 \pmod b$.

Hệ quả là vì $(a,b)=1$ và $ab=m$ ta có $f(x)\equiv 0 \pmod m$.

Vậy ta đã chứng minh được mỗi cặp (u,v) với u là nghiệm của đồng dư thức ***(41)*** và v là nghiệm của đồng dư thức ***(42)*** tương ứng với đúng một nghiệm của đồng dư thức ***(40)***.

Từ quan hệ một-một này suy ra số nghiệm của đồng dư thức ***(40)*** đúng bằng số các cặp (u,v) với u là nghiệm của đồng dư thức ***(41)*** và v là nghiệm của đồng dư thức ***(42)***.

Định lý 14 được chứng minh.

Hệ quả. *Nếu* $m = q_1^{\alpha_1} q_2^{\alpha_2} ... q_k^{\alpha_k}$ *là phân tích thành thừa số nguyên tố của số nguyên* m *thì số nghiệm của đồng dư thức* ***(40)*** *đúng bằng với tích các số nghiệm của k đồng dư thức sau đây*

$$f(x) \equiv 0 \left(\mathrm{mod}\, q_1^{\alpha_1}\right), \quad f(x) \equiv 0 \left(\mathrm{mod}\, q_2^{\alpha_2}\right), \quad ..., \quad f(x) \equiv 0 \left(\mathrm{mod}\, q_k^{\alpha_k}\right)$$

Từ đây ta có một phương pháp để quy việc tính các nghiệm của đồng dư thức modulo m tùy ý về việc tìm các nghiệm của các đồng dư thức với modulo là lũy thừa của các số nguyên tố.

Bài tập. Chứng minh rằng với mọi số tự nhiên *n* thì luôn tồn tại modulo m mà đồng dư thức $x^2 \equiv 1 (\mathrm{mod}\, m)$ có nhiều hơn n nghiệm.

Chứng minh. Nếu p là số nguyên tố lẻ thì đồng dư thức $x^2 \equiv 1 (\mathrm{mod}\, p)$ có đúng hai nghiệm là 1 và $p - 1$ (xem mục 5). Từ hệ quả của Định lý 14 suy ra đồng dư thức $x^2 \equiv 1 (\mathrm{mod}\, p_2 p_{3....} p_{s+1})$ có đúng 2^s nghiệm. Vì vậy ta chỉ cần chọn số tự nhiên s mà $2^s > n$. Chẳng hạn đồng dư thức $x^2 \equiv 1 (\mathrm{mod} 105)$ có tám nghiệm vì $105 = p_2 p_3 p_4$. Các nghiệm này là 1, 29, 34, 41, 64, 71, 76, 104.

9. Đồng dư thức bậc hai

Xét đồng dư thức bậc hai

(43) $$ax^2 + bx + c \equiv 0 (\mathrm{mod}\, m)$$

với m là số tự nhiên cho trước và a, b, c là các số nguyên. Giả sử $a \neq 0 (\mathrm{mod}\, m)$ vì nếu ngược lại, tức là $a \equiv 0 (\mathrm{mod}\, m)$, thì ***(43)*** trở thành đồng dư thức bậc nhỏ hơn hai. Vì $m \mid ax^2 + bx + c$ tương đương với $4am \mid 4a\left(ax^2 + bx + c\right)$ nên đồng dư thức ***(43)*** tương đương với đồng dư thức

(44) $$4a\left(ax^2 + bx + c\right) \equiv 0 (\mathrm{mod}\, 4am)$$

Đặt $D = b^2 - 4ac$ thì từ đẳng thức $4a\left(ax^2 + bc + c\right) = (2ax + b)^2 - \left(b^2 - 4ac\right)$ suy ra đồng dư thức ***(44)*** có thể viết lại dưới dạng

(45) $$(2ax + b)^2 \equiv D (\mathrm{mod}\, 4am)$$

Gọi *x* là nghiệm của đồng dư thức ***(43)*** và đặt $z = 2ax + b$. Khi đó theo ***(45)*** thì z là nghiệm của đồng dư thức trùng phương sau

(46) $$z^2 \equiv D (\mathrm{mod}\, 4am)$$

Vì vậy mỗi nghiệm x của các đồng dư thức ***(43)*** tương ứng với nghiệm của đồng dư thức ***(46)***.

Để chứng minh điều ngược lại cũng đúng, nghĩa là với nghiệm cho trước z của đồng dư thức ***(46)*** ta tìm tất cả các nghiệm x của ***(43)*** tương ứng với z. Ta sẽ giải đồng dư thức $2ax + b \equiv z (\mathrm{mod}\, 4am)$. Đồng dư thức này là giải được khi $(2a, 4am) \mid z - b$, nghĩa là $2a \mid z - b$. Vì vậy ta kết luận rằng nghiệm của đồng dư thức bậc hai có thể quy về các nghiệm của một đồng dư thức bậc một và một đồng dư thức trùng phương dạng ***(46)***. Theo ghi chú của Định lý 14 thì nghiệm của đồng dư thức ***(46)*** được quy về nghiệm của các đồng dư thức

(47) $$z^2 \equiv D \left(\mathrm{mod}\, p^{\alpha}\right)$$

với p là số nguyên tố và α là số tự nhiên.

Ta sẽ giải đồng dư thức ***(47).*** Đầu tiên giả sử $p \mid D$. Khi đó $D = p^{\mu} D_1$ với μ là số tự nhiên và D_1 không chia hết cho p. Nếu $\mu \geq \alpha$ thì $D \equiv 0 \left(\mathrm{mod}\, p^{\alpha}\right)$ và do đó ***(47)*** trở thành $z^2 \equiv 0 \left(\mathrm{mod}\, p^{\alpha}\right)$.

Đồng dư thức này có thể giải một cách đơn giản. Nếu $\mu < \alpha$ thì đồng dư thức ***(47)*** tương đương với phương trình

(48) $$z^2 = p^\mu \left(D_1 + tp^{\alpha-\mu} \right)$$

với t là số nguyên tùy ý và $D_1 + tp^{\alpha-\mu}$ không chia hết cho p (vì D_1 không chia hết cho p). Vì vậy μ là lũy thừa cao nhất của p mà p^μ là ước số của z^2. Do đó μ chẵn. Ta có $\mu = 2\lambda$ với λ là số tự nhiên. Vì vậy $z = p^\lambda z_1$ và do đó theo ***(48)*** thì $z_1^2 = D_1 + tp^{\alpha-\mu}$. Từ đây suy ra $z_1^2 \equiv D_1 (\mathrm{mod}\, p^{\alpha-\mu})$. Vì vậy nghiệm của đồng dư thức ***(47)*** có thể quy về nghiệm của đồng dư thức với cùng dạng trong đó vế phải không chia hết cho p. Ta giả sử trong đồng dư thức ***(47)*** thì $D \not\equiv 0 (\mathrm{mod}\, p)$. Nếu z thỏa mãn đồng dư thức này thì nó thỏa mãn đồng dư thức $z^2 \not\equiv D (\mathrm{mod}\, p)$, chứng tỏ D là thặng dư bậc hai modulo p. Từ đây suy ra điều kiện cần để đồng dư thức ***(47)*** giải được (D không chia hết cho p) là D là thặng dư bậc hai modulo p. Ta chứng minh điều kiện này cũng là điều kiện đủ. Thật vậy, ta chỉ cần chứng minh rằng nếu đồng dư thức

(49) $$z^2 \equiv D \left(\mathrm{mod}\, p^{\alpha-1} \right)$$

với α là số tự nhiên >1 là giải được thì đồng dư thức ***(47)*** cũng giải được. Xét riêng hai trường hợp p là số nguyên tố lẻ và $p = 2$. Trong trường hợp thứ nhất p lẻ thì gọi y là số nguyên thỏa mãn ***(49)***. Khi đó

(50) $$y^2 \equiv D \left(\mathrm{mod}\, p^{\alpha-1} \right)$$

Vì vậy suy ra

(51) $$M = \frac{y^2 - D}{p^{\alpha-1}}$$

là số nguyên. Ký hiệu x là nghiệm của đồng dư thức

(52) $$2xy + M \equiv 0 (\mathrm{mod}\, p)$$

Vì D không chia hết cho p, y không chia hết cho p, suy ra vì p lẻ nên $2y$ không chia hết cho p do đó đồng dư thức ***(25)*** là giải được. Đặt $z = y + p^{\alpha-1}$ khi đó $z^2 = y^2 + 2p^{\alpha-1}xy + p^{2\alpha-2}x^2$.

Theo ***(51)*** thì $y^2 = D + Mp^{\alpha-1}$ suy ra đồng dư thức sau đúng

(53) $$z^2 = D + \left(2xy + M \right) p^{\alpha-1} + x^2 p^{2\alpha-2}$$

Theo ***(52)*** thì số $2xy + M$ chia hết cho p. Vì $2\alpha - 2 = \alpha + (\alpha - 2) \geq \alpha$ (do $\alpha > 1$), $p^\alpha \mid p^{2\alpha-2}$. Do đó theo ***(53)*** thì z thỏa mãn đồng dư thức ***(47)***. Điều kiện đủ được chứng minh.

Ta có kết quả sau đây

Định lý 15. *Đồng dư thức **(47)**, với p là số nguyên tố lẻ, α là số tự nhiên và D là số nguyên không chia hết cho p, là giải được khi và chỉ khi D là thặng dư bậc hai modulo p.*

Ta chứng minh với các điều kiện trong Định lý 15 thì đồng dư thức ***(47)*** có đúng hai nghiệm.

Nếu z là nghiệm của đồng dư thức ***(47)*** thì rõ ràng $z_1 = -z$ là nghiệm của đồng dư thức đó. Hơn nữa z và z_1 không đồng dư với nhau modulo p^α vì nếu ngược lại thì ta có $p^\alpha \mid 2z$, mà p lẻ nên $p^\alpha \mid z$ và do đó $p \mid D$, mâu thuẫn với giả thiết. Vậy ta thấy tồn tại ít nhất hai nghiệm phân biệt của đồng dư thức ***(47)*** là z và z_1. Ta sẽ chứng minh chúng là tất cả các nghiệm của ***(47)***. Giả sử t là nghiệm của đồng dư thức ***(47)*** thì $t^2 \equiv D \left(\mathrm{mod}\, p^\alpha \right)$ mà $z^2 \equiv D \left(\mathrm{mod}\, p^\alpha \right)$ suy ra $t^2 \equiv z^2 \left(\mathrm{mod}\, p^\alpha \right)$.

Vì vậy $p^\alpha \mid (t-z)(t+z)$. Nếu các số $t-z$ và $t+z$ đều chia hết cho p thì $p \mid 2z$ mà p lẻ nên $p \mid z$ và do đó $p \mid D$, mâu thuẫn với giả thiết. Vậy một trong các số t − z và t + z là không chia hết cho p. Nếu t+z không chia hết cho p thì từ $p^\alpha \mid t-z$ suy ra $t \equiv -z \pmod{p^\alpha}$, nếu t − z không chia hết cho p thì $p^\alpha \mid t+z$ suy ra $t \equiv -z \pmod{p^\alpha}$. Vậy mỗi nghiệm của đồng dư thức ***(47)*** đồng dư modulo với z hoặc $-z$. Chứng tỏ ***(47)*** có đúng hai nghiệm.

Bây giờ đặt $p = 2$. Khi đó với $\alpha = 1$ thì từ công thức ***(47)*** suy ra $z^2 \equiv D \pmod 2$ với D không chia hết cho 2, tức là D lẻ. Hệ quả trực tiếp là đồng dư thức này có đúng một nghiệm là z = 1.

Với $\alpha = 2$ thì đồng dư thức có dạng $z^2 \equiv D \pmod 4$. Nhưng bình phương của một số nguyên là đồng dư với 0 hoặc 1 modulo 4 mà D lẻ nên đồng dư thức là giải được chỉ trong trường hợp D có dạng $4k+1$. Khi đó đồng dư thức có đúng hai nghiệm là $z = 1$ và $z = 3$.

Với $\alpha = 3$ thì đồng dư thức có dạng $z^2 \equiv D \pmod 8$. Vì D lẻ nên z lẻ suy ra vì bình phương của một số lẻ là $\equiv 1 \pmod 8$ nên đồng dư thức ban đầu là giải được chỉ khi D có dạng $8k+1$. Trong trường hợp đó thì đồng dư thức có bốn nghiệm là 1,3,5,7.

Với $\alpha > 3$ ta xét đồng dư thức

(54) $$z^2 \equiv D \pmod{2^\alpha} \text{ với } \alpha > 3$$

Ta thấy từ đồng dư thức ***(54)*** suy ra đồng dư thức $z^2 \equiv D \pmod 8$. Đồng dư thức này giải được chỉ khi D = $8k+1$. Ta chứng minh rằng đây cũng là điều kiện đủ cho tính giải được của ***(54)***. Giả sử D = $8k+1$ và đồng dư thức

(55) $$z^2 \equiv D \pmod{2^{\alpha-1}}$$

là giải được (điều này đúng với $\alpha = 4$). Khi đó tồn tại số nguyên *y* thỏa mãn $y^2 \equiv D \pmod{2^{\alpha-1}}$ và vì D lẻ nên *y* lẻ. Đặt

(56) $$M = \frac{y^2 - D}{2^{\alpha-1}}$$

Khi đó M nguyên. Hơn nữa gọi x là nghiệm của đồng dư thức bậc một biến x

(57) $$xy + M \equiv 0 \pmod 2$$

Đồng dư thức này giải được vì hệ số y của biến x và modulo 2 là nguyên tố cùng nhau.

Đặt $z = y + x2^{\alpha-2}$. Theo ***(56)*** ta có

(58) $$z^2 = y^2 + xy2^{\alpha-1} + x^2 2^{2\alpha-4} = D + (xy + M)2^{\alpha-1} + x^2 2^{2\alpha-4}$$

Nhưng theo ***(57)*** thì $xy + M$ chẵn suy ra $(xy+M)2^{\alpha-1} \equiv 0 \pmod{2^\alpha}$ và vì $2\alpha - 4 = \alpha + (\alpha - 4) \geq \alpha$ (đúng vì $\alpha \geq 4$) nên $x^2 2^{2\alpha-4}$ chia hết cho 2^α. Hệ quả là $x^2 2^{2\alpha-4} \equiv 0 \pmod{2^\alpha}$. Vì vậy từ ***(58)*** suy ra ***(54)*** và như thế chứng tỏ với mọi $\alpha > 3$ thì tính giải được của ***(55)*** suy ra tính giải được của ***(54)***. Nhưng ta đã giả sử $D = 8k+1$ nên đồng dư thức $z^2 \equiv D \pmod{2^3}$ giải được và do đó theo quy nạp (với $D = 8k+1$) thì đồng dư thức ***(54)*** là giải được với mọi số tự nhiên $\alpha \geq 3$. Ta có định lý

Định lý 16. *Đồng dư thức* $z^2 \equiv D \pmod{2^\alpha}$, *với* D *lẻ và* α *là số tự nhiên, là giải được khi và chỉ khi* D *có dạng* $2k+1,\ 4k+1$ *hoặc* $8k+1$ *tương ứng với* $\alpha = 1,\ \alpha = 2$ *hoặc* $\alpha > 2$.

Ta sẽ chứng minh với $\alpha \geq 3$ thì đồng dư thức ***(54)*** (với $D = 8k+1$) có đúng bốn nghiệm.

Ta đã chứng minh (với các giả thiết ở trên) đồng dư thức này có ít nhất một nghiệm. Ký hiệu nghiệm này là z_0. Giả sử z là nghiệm bất kỳ của đồng dư thức ***(54)***. Ta có $z_0^2 \equiv D \pmod{2^\alpha}$ và suy ra theo ***(54)*** thì $2^\alpha \mid (z-z_0)(z+z_0)$. Vì D lẻ nên z và z_0 cùng lẻ và suy ra $z-z_0$ và $z+z_0$ chẵn. Các số này không cùng chia hết cho 4 vì nếu ngược lại thì $2 \mid z$, vô lý. Vậy một trong các số đó không chia hết cho 4. Nếu $z-z_0$ không chia hết cho 4 thì $\frac{1}{2}(z-z_0)$ lẻ. Nhưng vì $2^{\alpha-1} \mid \frac{1}{2}(z-z_0)(z+z_0)$ nên $2^{\alpha-1} \mid z+z_0$ và do đó $z = -z_0 + 2^{\alpha-1}t$ với t là số nguyên. Nếu t chẵn thì $z \equiv -z_0 \pmod{2^\alpha}$. Nếu t lẻ thì $z \equiv -z_0 + 2^{\alpha-1} \pmod{2^\alpha}$. Bây giờ ta xét trường hợp còn lại, nghĩa là $z+z_0$ không chia hết cho 4. Khi đó số $\frac{1}{2}(z+z_0)$ lẻ và do đó vì $2^{\alpha-1} \mid (z-z_o)\frac{1}{2}(z+z_o)$ ta suy ra $2^{\alpha-1} \mid z-z_o$ và do đó $z = z_0 + 2^{\alpha-1}u$ với u là số nguyên. Nếu u chẵn thì $z \equiv z_0 \pmod{2^\alpha}$. Nếu u lẻ thì $z \equiv z_0 + 2^{\alpha-1} \pmod{2^\alpha}$. Vậy ta đã chứng minh được mọi nghiệm z của đồng dư thức ***(54)*** đều phải thỏa mãn một trong các đồng dư thức sau

(59)
$$z \equiv -z_0 \pmod{2^\alpha},\ z \equiv -z_0 + 2^{\alpha-1} \pmod{2^\alpha}$$
$$z \equiv z_0 \pmod{2^\alpha},\quad z \equiv z_0 + 2^{\alpha-1} \pmod{2^\alpha}$$

Chứng tỏ số các nghiệm của đồng dư thức này là không lớn hơn bốn. Mặt khác dễ dàng kiểm tra rằng các số được cho bởi các đồng dư thức ***(59)*** đều thỏa mãn đồng dư thức ***(54)*** (nếu nó đúng với z_0) và vì $\alpha \geq 3$ nên các số đó đôi một khác nhau modulo 2^α. Vậy chúng là các nghiệm phân biệt của đồng dư thức ***(54)***.

Ta có định lý sau đây

Định lý 17. *Đồng dư thức $z^2 \equiv D \pmod{m}$, với D là số nguyên và $(D,m)=1$, là giải được khi và chỉ khi (i) D là thặng dư bậc hai với mọi modulo là ước số nguyên tố lẻ của m và (ii) D có dạng $4k+1$ trong trường hợp m chia hết cho 4 nhưng không chia hết cho 8 và có dạng $8k+1$ nếu m chia hết cho 8. Số các nghiệm của đồng dư thức này là $2^{\lambda+\mu}$ với λ là số các ước số nguyên tố lẻ của m và $\mu = 0$ trong trường hợp m không chia hết cho 4 và $\mu = 1$ nếu m chia hết cho 4 nhưng không chia hết cho 8 và cuối cùng $\mu = 2$ với m chia hết cho 8.*

CHƯƠNG 6

HÀM CHỈ EULER VÀ ĐỊNH LÝ EULER

1. Hàm chỉ Euler

Với mọi số tự nhiên n thì số các số tự nhiên $\le n$ và nguyên tố cùng nhau với n được ký hiệu là $\varphi(n)$. Hàm số $\varphi(n)$ được gọi là hàm chỉ Euler (Euler là nhà toán học đầu tiên nghiên cứu về các tính chất của hàm số này vào năm 1760). Ký hiệu $\varphi(n)$ được đề xuất bởi Gauss vào năm 1801 do đó đôi khi hàm số này cũng được gọi là hàm Gauss.

Từ định nghĩa ta có ngay

$$\varphi(1)=1,\ \varphi(2)=1,\ \varphi(3)=2,\ \varphi(4)=2,\ \varphi(5)=4,\ \varphi(6)=2,\ \varphi(7)=6,\ \varphi(8)=4,\ \varphi(9)=6,\ \varphi(10)=4$$

Nếu n là số nguyên tố thì mọi số tự nhiên nhỏ hơn n đều nguyên tố cùng nhau với n do đó

(1) $$\varphi(n)=n-1$$

Nếu số tự nhiên n là hợp số, nghĩa là nó có ước số d thỏa mãn $1<\mathrm{d}<n$, khi đó trong các số 1, 2, …n có ít nhất hai số là n và d không nguyên tố cùng nhau với n do đó $\varphi(n)\le n-2$. Với $n=1$ ta có $\varphi(n)=n>n-1$. Vậy ***(1)*** đúng khi và chỉ khi n là số nguyên tố.

Từ đây suy ra tính chất: *số tự nhiên $n>1$ là số nguyên tố khi và chỉ khi với mọi số tự nhiên $a<n$ thì* $a^{n-1}\equiv 1(\mathrm{mod}\, n)$.

Thật vậy, từ đồng dư thức này suy ra $(a,n)=1$ và do đó nếu nó đúng với mọi $a<n$ thì $\varphi(n)=n-1$ và do đó n là số nguyên tố. Điều kiện đủ được chứng minh. Điều kiện cần được suy ra từ định lý Fermat nhỏ (Định lý 5 Chương 5).

Dễ dàng tính giá trị $\varphi(n)$ với mọi lũy thừa các số nguyên tố $n=p^k$, k là số tự nhiên.

Tất cả những số trong dãy $1, 2, \ldots, p^k$ mà không nguyên tố cùng nhau với p^k là các số chia hết cho p tức là các số có dạng pt với t là số tự nhiên bất kỳ thỏa mãn $pt\le p^k$, nghĩa là $t\le p^{k-1}$. Rõ ràng có đúng p^{k-1} số như thế. Vì vậy trong dãy $1, 2, \ldots, p^k$ có đúng p^{k-1} số không nguyên tố cùng nhau với p^k và suy ra $\varphi(p^k)=p^k-p^{k-1}$.

Định lý 1. *Nếu p là số nguyên tố và k là số tự nhiên thì* $\varphi(p^k)=p^{k-1}(p-1)$.

Để tính $\varphi(n)$ với n là số tự nhiên tùy ý ta chứng minh bổ đề sau

Bổ đề. *Với m là số tự nhiên và l là số tự nhiên nguyên tố cùng nhau với m, r là số nguyên tùy ý thì khi chia các số*

(2) *r, l+r, 2l+r, ..., (m – 1) l+r*

cho m ta sẽ nhận được dãy các số dư

(3) *0, 1, 2, ...,m – 1*

Chứng minh. Giả sử với các số nguyên *k* và h với $0\le k<h<m$ ta có các số kl + r và hl + r có cùng số dư khi chia cho *m*. Khi đó hiệu $(h-k)l$ chia hết cho *m* suy ra vì $(l,m)=1$, $m\mid h-k$, vô lý vì

$0 < h - k < m$. Vì vậy khi chia các số trong ***(2)*** cho m ta nhận được các số dư khác nhau. Mà có tất cả m số trong ***(2)*** nên dãy các số dư nhận được chính là ***(3)***. Bổ đề được chứng minh.

Định lý 2. *Nếu l và m là các số tự nhiên nguyên tố cùng nhau thì*

(4) $$\varphi(lm) = \varphi(l)\varphi(m)$$

Chứng minh. Vì $\varphi(1) = 1$ nên Định lý 2 đúng nếu ít nhất một trong các số l, m bằng 1. Giả sử $l > 1$ và $m > 1$. Ta đã biết $\varphi(lm)$ là số các số trong bảng

$$\begin{array}{rrcrcr} 1, & 2, & \ldots, & r, & \ldots, & l \\ l+1, & l+2, & \ldots, & l+r, & \ldots, & 2l \\ 2l+1, & 2l+2, & \ldots, & 2l+r, & \ldots, & 3l \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ (m-1)l+1, & (m-1)l+2, & \ldots, & (m-1)l+r, & \ldots, & ml \end{array}$$

mà nguyên tố cùng nhau với lm, nghĩa là số các số trong bảng mà nguyên tố cùng nhau với cả l và m. Với r là số tự nhiên cho trước $\le l$ ta xét cột thứ r trong bảng. Nếu $(r,l) = 1$ thì tất cả các số trong cột này đều nguyên tố cùng nhau với l. Nếu $(r,l) > 1$ thì không có số nào trong cột là nguyên tố cùng nhau với l. Số các số tự nhiên r $< l$ mà $(r,l) = 1$ là $\varphi(l)$. Đây cũng là số các cột mà mọi phần tử trong cột đều nguyên tố cùng nhau với l. Xét một trong các cột như vậy, giả sử đó là cột thứ r. Theo bổ đề thì các số dư nhận được khi chia các số trong cột cho m chính là các số $0,1,\ldots,m-1$ và suy ra số các số trong cột mà nguyên tố cùng nhau với m chính là $\varphi(m)$. Suy ra trong $\varphi(l)$ cột như vậy thì mỗi cột có $\varphi(m)$ số nguyên tố cùng nhau với m. Vậy tổng số các số trong bảng mà nguyên tố với cả m và l là $\varphi(l)\,\varphi(m)$ và như vậy định lý được chứng minh.

Từ Định lý 2, theo quy nạp, ta có hệ quả

Hệ quả. *Nếu $m_1, m_2, \ldots, m_k$ là các số tự nhiên đôi một nguyên tố cùng nhau thì*

$$\varphi(m_1 m_{2\ldots} m_k) = \varphi(m_1)\varphi(m_2)\ldots\varphi(m_k)$$

Với số tự nhiên $n > 1$ có phân tích thành thừa số nguyên tố là $n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ thì áp dụng công thức vừa chứng minh với các số $m_1 = q_i^{\alpha_i}, i = 1,2,\ldots,k$ ta có $\varphi(n) = \varphi\left(q_1^{\alpha_1}\right)\varphi\left(q_2^{\alpha_2}\right)\ldots\varphi\left(q_k^{\alpha_k}\right)$.

Nhưng theo Định lý 1 thì $\varphi\left(q_i^{\alpha_i}\right) = q_i^{\alpha_i - 1}\left(q_i - 1\right)$ với i = 1, 2, $\ldots k$, ta có định lý sau đây

Định lý 3. *Với số tự nhiên $n > 1$ có phân tích thành thừa số nguyên tố là $n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ thì*

(5) $$\varphi(n) = q_1^{\alpha_1 - 1}(q_1 - 1)\, q_2^{\alpha_2 - 1}(q_2 - 1)\ldots q_k^{\alpha_k - 1}(q_k - 1)$$

Công thức này có thể viết lại thành

(6) $$\varphi(n) = n\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\ldots\left(1 - \frac{1}{q_k}\right)$$

Từ Định lý 3 dễ thấy nếu $(a,b) \ne 1$ thì $\varphi(ab) > \varphi(a)\varphi(b)$ và nếu $m \mid n$ thì $\varphi(m) \mid \varphi(n)$.

Định lý 4. *Ta có* $\lim_{n\to\infty}\varphi(n)=+\infty$.

Chứng minh (J. Browkin). Chỉ cần chứng minh rằng $\varphi(n)\geq\frac{1}{2}\sqrt{n}$ với mọi số tự nhiên n. Rõ ràng bất đẳng thức đúng với $n=1$. Giả sử $n>1$ và $2^{\alpha_0}q_1^{\alpha_1}q_2^{\alpha_2}...q_k^{\alpha_k}$ là phân tích thành thừa số nguyên tố của n với α_0 là số nguyên không âm và $\alpha_1,\alpha_2,...\alpha_k$ là các số tự nhiên. Với số tự nhiên tùy ý $a>2$ ta có $a-1>\sqrt{a}$ và với mọi số tự nhiên b thì $b-\frac{1}{2}\geq 2b$. Vì vậy theo Định lý 3 ta có

$$\begin{aligned}\varphi(n)&\geq 2^{\alpha_0-1}q_1^{\alpha_1-1}q_2^{\alpha_2-1}...q_k^{\alpha_k-1}(q_1-1)(q_2-1)...(q_k-1)\\&\geq 2^{\alpha_0-1}q_1^{\alpha_1-\frac{1}{2}}q_2^{\alpha_2-\frac{1}{2}}...q_k^{\alpha_k-\frac{1}{2}}\geq 2^{\alpha_0-1}q_1^{\frac{1}{2}\alpha_1}q_2^{\frac{1}{2}\alpha_2}...q_k^{\frac{1}{2}\alpha_k}\\&\geq\frac{1}{2}\sqrt{n}\end{aligned}$$

Trong mối liên hệ với Định lý 4 ta lưu ý rằng tồn tại vô hạn số tự nhiên n mà $\varphi(n)>\varphi(n+1)$.

Để chứng minh tính chất này ta chứng minh

Định lý 5. *Nếu n là hợp số tự nhiên thì*

(7) $$\varphi(n)\leq n-\sqrt{n}$$

Chứng minh. Ký hiệu n là hợp số và p_1 là ước số nguyên tố nhỏ nhất của nó. Ta đã biết $p_1\leq\sqrt{n}$ do đó theo công thức ***(6)*** thì $\varphi(n)\leq n\left(1-\frac{1}{p_1}\right)\leq n-\frac{n}{\sqrt{n}}$ suy ra ***(7)*** đúng. Bây giờ giả sử n là số nguyên tố >7. Khi đó $n+1$ là hợp số và $n+1\geq 9$. Vậy $\sqrt{n+1}\geq 3$ và theo ***(7)*** thì $\varphi(n+1)\leq n+1-\sqrt{n+1}\leq n-2$. Nhưng vì $\varphi(n)=n-1$ nên $\varphi(n)>\varphi(n+1)$. Bất đẳng thức đúng với mọi số nguyên tố $n>7$. Nó cũng đúng với $n=5$ và $n=7$. Do đó nó đúng với vô hạn số tự nhiên n.

Đẳng thức $\varphi(n)=\varphi(n+1)$ với n là số tự nhiên được nghiên cứu bởi nhiều tác giả (Klee [2], Moser [1], Lal, Gillard [1], Yorigana [1], Baillie [1],[2]). Tất cả các nghiệm $n\leq 10000$ của phương trình này là $n=1, 3, 15, 104, 164, 194, 255, 495, 584, 975, 2204, 2625, 2834, 3255, 3705, 5186, 5187$. Số tự nhiên n nhỏ nhất mà $\varphi(n)=\varphi(n+1)=\varphi(n+2)$ là 5186. Dễ thấy 5186 thỏa mãn tính chất này vì ta có các phân tích thành thừa số nguyên tố $5186=2.2593$, $5187=3.7.13.19$, $5188=2^2.1297$ và $2592=2.6.12.18=2.1296$.

Ta chưa biết có tồn tại các số tự nhiên n mà $\varphi(n)=\varphi(n+1)$ hay không. Với $n\leq 2\cdot 10^8$ thì có 391 số như vậy và trong đó chỉ có $n=1586$ thỏa mãn $\varphi(n)=\varphi(n+1)=\varphi(n+2)$. Với phương trình $\varphi(n+2)=\varphi(n)$ thì ta biết có 7998 nghiệm $n\leq 4\cdot 10^6$. Với $n\leq 100$ thì $n=4,7,8,10,26,32,70,74$. Phương trình $\varphi(n+3)=\varphi(n)$ chỉ có hai nghiệm $n=3$ và $n=5$ với $n\leq 10^6$.

Dễ dàng chứng minh với mọi số tự nhiên cho trước *k* thì phương trình $\varphi(n+k)=\varphi(n)$ có ít nhất một nghiệm tự nhiên *n* (bài tập 11). Từ giả thuyết H (Chương 3 mục 8) thì tồn tại vô hạn nghiệm tự nhiên của phương trình trên với k chẵn (Schinzel và Sierpinski [3] trang 195). A.Schinzel và Adrzej

Wakulicz [1] đã chứng minh rằng với mọi số tự nhiên $k \le 2\cdot 10^{58}$ thì phương trình $\varphi(n+k)=\varphi(n)$ có ít nhất hai nghiệm tự nhiên *n* (Shinzel [8]).

Nếu một trong hai số n và $n+2$ là nguyên tố thì $\varphi(n+2)=\varphi(n)+2$. Phương trình này cũng đúng với một số hợp số chẳng hạn $n=12,14,20,44$. Moser [1] đã chứng minh rằng không tồn tại hợp số lẻ $n<10000$ thỏa mãn phương trình này. Từ đây đặt ra giả thuyết nói rằng không tồn tại số lẻ n nào ngoại trừ các cặp số nguyên tố sinh đôi $n, n+2$ mà $\varphi(n+2)=\varphi(n)+2$. Trong mối liên hệ này A.Makowski [4] đã đặt câu hỏi còn tồn tại hợp số tự nhiên n mà $\varphi(n+2)=\varphi(n)+2$ và $\sigma(n+2)=\sigma(n)+2$ hay không.

Nếu n là số nguyên tố thì $\varphi(n)=n-1$ do đó $\varphi(n)\mid n-1$. Ta chưa biết có tồn tại vô hạn các hợp số n mà $\varphi(n)\mid n-1$ hay không. D.H.Lehmer [1] đã đặt ra giả thuyết không tồn tại những số như vậy. G.L.Cohen và P.Hagis Jr. [1] đã chứng minh nếu tồn tại các số như vậy thì các số đó có ít nhất 14 ước số nguyên tố phân biệt. Mặt khác dễ dàng tìm được các số tự nhiên n mà $\varphi(n)\mid n$. Tất cả các số có tính chất này là $n=2^\alpha$, $\alpha=0,1,2,\ldots$ và $n=2^\alpha 3^\beta$ với α,β là các số tự nhiên (Sierpinski [26], 196-197).

Từ ***(5)*** suy ra nếu $n=2^\alpha$ với α là số tự nhiên >1 thì $\varphi(n)=2^{\alpha-1}$. Do đó $2\mid\varphi(2^\alpha)$ với $\alpha=2,3,\ldots$. Tuy nhiên nếu *n* có ước số nguyên tố lẻ p thì $p-1$ chẵn và do đó theo ***(5)*** thì $p-1\mid\varphi(n)$ và do đó $2\mid\varphi(n)$. Vì mọi số tự nhiên >2 hoặc là lũy thừa bậc k của 2 với $k>1$ hoặc có ước số nguyên tố lẻ nên suy ra với mọi số tự nhiên $n>2$ thì $2\mid\varphi(n)$.

Do $\varphi(1)=\varphi(2)=1$ suy ra phương trình $\varphi(x)=m$, m lẻ, là giải được chỉ khi $m=1$. Vì vậy tồn tại vô hạn số tự nhiên (lẻ) m mà phương trình $\varphi(x)=m$ không có nghiệm tự nhiên x.

Mặt khác có thể chứng minh tồn tại vô hạn số tự nhiên chẵn m mà phương trình $\varphi(x)=m$ không có nghiệm tự nhiên x. Ta chứng minh tính chất này bằng cách chứng minh phương trình đó không có nghiệm khi $m=2\cdot 5^{2k}$ với $k=1,2,\ldots$. Từ ***(5)*** suy ra nếu $\varphi(n)=2\cdot 5^{2k}$ với k là số tự nhiên thì n có đúng một ước số nguyên tố vì nếu q_1 và q_2 là các ước số nguyên tố phân biệt của n thì theo ***(5)*** suy ra $(q_1-1)(q_2-1)\mid\varphi(n)=2.5^{2k}$ và do đó $4\mid\varphi(n)$, vô lý. Vì vậy $n=2^\alpha p^\beta$ với α là số nguyên ≥ 0 và β là số tự nhiên. Hơn nữa $\alpha\le 1$ vì nếu ngược lại thì với $\alpha\ge 2$, $2^{\alpha-1}(p-1)\mid\varphi(n)$ và do đó $4\mid\varphi(n)$, vô lý. Nếu $\alpha=0$ ta có $n=p^\beta$ và nếu $\alpha=1, n=2p^\beta$ thì $\varphi(n)=p^{\beta-1}(p-1)=2\cdot 5^{2k}$. Nếu $\beta>1$, p = 5 và do đó $p-1=4$, vô lý. Vậy $\beta=1$ suy ra $p=2.5^{2k}+1$, vô lý vì số $5^{2k}=(5^k)^2$ đồng dư 1 modulo 3, suy ra $3\mid p$ và do đó $p=3$, điều này không đúng. Vậy phương trình $\varphi(n)=2\cdot 5^{2k}$, với $k=1,2,\ldots$ không có nghiệm tự nhiên.

Sử dụng phương pháp tương tự, định lý mạnh hơn sau đây được chứng minh bởi A.Schinzel [6].

Định lý chỉ ra với mọi số tự nhiên s thì tồn tại số tự nhiên m chia hết cho s và phương trình $\varphi(n)=m$ không có nghiệm tự nhiên *n.*. Định lý này là hệ quả trực tiếp của kết quả được trình bày bởi S.S.Pillai [2] theo một cách khác: *nếu* $g(x)$ *ký hiệu số các số tự nhiên* $m\le x$ *mà phương trình* $\varphi(n)=m$ *là giải được thì* $\lim\limits_{x\to\infty}\dfrac{g(x)}{x}=0$.

Thật vậy, H.Maier và C.Pomerance [1] đã chứng minh tồn tại số thực $C = 0,81781465$ mà với mọi $\varepsilon > 0$ và $x > x_0(\varepsilon)$ thì

$$\frac{x}{\log x}\exp\left((C-\varepsilon)(\log\log\log x)^2\right) < g(x)$$
$$< \frac{x}{\log x}\exp\left((C+\varepsilon)(\log\log\log x)^2\right)$$

Từ Định lý 4 suy ra với mọi số tự nhiên m thì số các nghiệm tự nhiên của phương trình $\varphi(n) = m$ là hữu hạn. Ngược lại, Định lý 4 là hệ quả trực tiếp của tính chất này. Từ định lý của Pillai suy ra

Định lý 6. *Với mọi số tự nhiên s thì luôn tồn tại số tự nhiên m mà phương trình $\varphi(n) = m$ có nhiều hơn s nghiệm tự nhiên n phân biệt.*

Chứng minh. Ta trình bày một chứng minh sơ cấp thuộc về A.Schinzel [5].

Ký hiệu s là số tự nhiên và $m = (p_1 - 1)(p_2 - 1)\ldots(p_s - 1)$ với p_i là số nguyên tố thứ i. Ta sẽ chứng minh các số $x_1, x_2, \ldots, x_{s+1}$ với $x_i = p_1\ldots p_{i-1}(p_i - 1)p_{i+1}\ldots p_s$, $i = 1, 2, \ldots, s$ và $x_{i+1} = p_1 p_2 \ldots p_s$ là nghiệm của phương trình $\varphi(n) = m$.

Thật vậy, với i là một trong các số $1, 2, \ldots, s$ thì số $p_i - 1$ không chia hết cho mọi số nguyên tố $> p_i$ và do đó $p_i - 1 = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_{i-1}^{\gamma_{i-1}}$ với $\gamma_1, \gamma_2, \ldots, \gamma_{i-1}$ là các số nguyên không âm. Vì vậy $x_i = p_1^{\gamma_1+1} p_2^{\gamma_2+1} \ldots p_{i-1}^{\gamma_{i-1}+1} p_{i+1} p_{i+2} \ldots p_s$ nên $\varphi(x_i) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_{i-1}^{\gamma_{i-1}} (p_1 - 1)(p_2 - 1)\ldots(p_{i-1} - 1)(p_{i+1} - 1)\ldots(p_s - 1)$ suy ra theo định nghĩa của m thì $\varphi(x_i) = m$ với $i = 1, 2, \ldots, s$. Ta thấy các số $x_1, x_2, \ldots, x_{s+1}$ là các số nguyên dương phân biệt. Định lý được chứng minh.

Tồn tại dãy vô hạn tăng các số tự nhiên $m_k\ (k = 1, 2, \ldots)$ mà số nghiệm của phương trình $\varphi(n) = m_k$ với mọi $k = 1, 2, \ldots$ là lớn hơn m_k^c với c là hằng số dương (P.Erdos [3]). P.Erdos đã đặt ra giả thuyết với mọi $\varepsilon > 0$ thì hằng số này có thể chọn là $1 - \varepsilon$. A.Balog [1] đã chứng minh điều này đúng với $\varepsilon = \frac{7}{20}$.

Câu hỏi đặt ra là có phải với mọi số tự nhiên s thì đều tồn tại số tự nhiên m mà phương trình $\varphi(n) = m$ có đúng s nghiệm tự nhiên hay không. Ta chưa biết câu trả lời ngay cả khi $s = 1$. Thật vậy, ta chưa biết số tự nhiên m nào mà phương trình $\varphi(n) = m$ có đúng một nghiệm. Giả thuyết Carmichael [5] nói rằng không tồn tại số tự nhiên *m* như vậy. P.Masai và A.Valette [1] đã chứng minh không tồn tại số $m \le 10^{10000}$ nào như vậy. Tuy nhiên có thể chứng minh tồn tại vô hạn số tự nhiên m mà phương trình $\varphi(n) = m$ có đúng hai (hoặc ba) nghiệm tự nhiên *n* (bài tập 12).

Với mọi số tự nhiên s > 1 ký hiệu m_s là số tự nhiên nhỏ nhất m mà phương trình $\varphi(n) = m$ có đúng s nghiệm tự nhiên (nếu số m_s tồn tại). Ta tính được

$$m_2 = 1, m_3 = 2, m_4 =, m_5 = 8, m_6 = 12, m_7 = 32, m_8 = 36, m_9 = 40, m_{10} = 24, m_{11} = 48, m_{12} = 160$$
$$m_{13} = 396, m_{14} = 2268, m_{15} = 704$$

Ta đặt ra giả thuyết rằng với mọi số tự nhiên $s > 1$ thì tồn tại vô hạn số tự nhiên m mà phương trình $\varphi(n) = m$ có đúng s nghiệm tự nhiên *n*. Tính chất này được suy ra từ giả thuyết H (Schinzel

[13]). Khó khăn duy nhất trong chứng minh nằm ở việc chứng tỏ sự tồn tại của các số m_s vì P.Erdos [14] đã chứng minh nếu với số tự nhiên s cho trước mà tồn tại số tự nhiên m mà phương trình $\varphi(n)=m$ có đúng s nghiệm tự nhiên n thì có vô hạn số tự nhiên m có tính chất này.

Ta chưa biết có tồn tại vô hạn các số tự nhiên không có dạng $n-\varphi(n)$ với n là số tự nhiên hay không. Có thể chứng minh các số 10, 26, 34 và 50 đều không có dạng này. Ta không biết có tồn tại số lẻ có dạng này hay không. Câu trả lời là khẳng định nếu ta chứng minh được mọi số chẵn lớn hơn 6 đều là tổng của hai số nguyên tố phân biệt.

Bài tập. ***1.*** Chứng minh công thức N.C.Scholomiti [1] $\varphi(n)=\sum_{k=1}^{n-1}\left[\frac{1}{(n,k)}\right]$ với mọi số tự nhiên $n>1$.

Chứng minh. Lưu ý nếu $n>1, k<n$ và $(n,k)>1$ thì $\left[\frac{1}{(n,k)}\right]=1$. Mặt khác nếu $(n,k)>1$ thì $\left[\frac{1}{(n,k)}\right]=0$. Do đó vế phải của công thức bằng với số các số tự nhiên $<n$ nguyên tố cùng nhau với $n>1$ và do đó bằng $\varphi(n)$.

2. Tìm các số tự nhiên n mà $\varphi(n)$ không chia hết cho 4.

Lời giải. Các số đó là 1, 2, 4 và p^α và $2p^\alpha$ với p là số nguyên tố có dạng $4t+3$. Chứng minh là hiển nhiên (Carmichael [1], Klee [1]).

3. Chứng minh tồn tại vô hạn cặp số tự nhiên $x, y, y>x,$ mà $d(x)=d(y)$, $\varphi(x)=\varphi(y)$, $\sigma(x)=\sigma(y)$.

Chứng minh. Các cặp số $x=3^k.568$, $y=3^k.638$ với $k=0,1,2,\ldots$ đều thỏa mãn (Jankowska [1]).

4. Chứng minh rằng tồn tại vô hạn các bộ số x, y, z mà $x<y<z$ và

$$d(x)=d(y)=d(z),\ \varphi(x)=\varphi(y)=\varphi(z),\ \sigma(x)=\sigma(y)=\sigma(z)$$

Chứng minh. Đặt

$$x=5^k\cdot 2^3\cdot 3^3\cdot 71\cdot 113,\quad y=5^k\cdot 2^3\cdot 3\cdot 29\cdot 37\cdot 71$$
$$z=5^k\cdot 2\cdot 3^3\cdot 11\cdot 29\cdot 113$$

P.Erdos [15] đã chứng minh rằng với mọi số tự nhiên s thì đều tồn tại s số tự nhiên phân biệt $a_1, a_2, \ldots, a_s$ thỏa mãn $d(a_i)=d(a_j)$, $\varphi(a_i)=\varphi(a_j)$, $\sigma(a_i)=\sigma(a_j)$ với mọi $1\le i\le j\le s$. Từ giả thuyết Erdos [16] thì suy ra các số $a_1, a_2, \ldots a_s$ có thể chọn đôi một nguyên tố cùng nhau.

5. Chứng minh rằng với mọi số tự nhiên m thì tồn tại số tự nhiên n mà $\varphi(n)-\varphi(n-1)>m$ và $\varphi(n)-\varphi(n+1)>m$.

Chứng minh. Với p là số nguyên tố có dạng $4k+3$ và lớn hơn $2m+3$. thì ta có $\varphi(p)=4k+2, \varphi(p-1)=\varphi(4k+2)=\varphi(2k+1)\le 2k+1$. Do đó $\varphi(p)-\varphi(p-1)\ge 2k+1>m$. Ta cũng có $p+1=4(k+1)=2^\alpha l$ với $\alpha\ge 2$ và l là số lẻ. Vì vậy $\varphi(p+1)=2^{\alpha-1}\varphi(l)\le 2^{\alpha-1}l=\frac{1}{2}(p+1)$ và do đó $\varphi(p)-\varphi(p+1)\ge p-1-\frac{1}{2}(p+1)=\frac{1}{2}(p-3)>m$.

Lưu ý rằng: *tồn tại số tự nhiên* $n>1$ *mà* $\varphi(n-1)/\varphi(n)>m$ *và* $\varphi(n+1)/\varphi(n)>m$ *và tương tự tồn tại số tự nhiên* $n>1$ *mà* $\varphi(n)/\varphi(n-1)>m$ *và* $\varphi(n)/\varphi(n+1)>m$ (Schinzel và Sierpinski [1]).

Có thể chứng minh (Erdos và Schinzel [1]) với hai số tự nhiên m và $k>1$ thì tồn tại số tự nhiên n thỏa mãn $\dfrac{\varphi(n+i)}{\varphi(n+i-1)}>m$ với $i=1,2,...,k$ và số tự nhiên n thỏa mãn $\dfrac{\varphi(n+i-1)}{\varphi(n+i)}>m$ với $i=1,2,...,k$.

6. Chứng minh rằng với các số tự nhiên a,b tùy ý thì tồn tại vô hạn các cặp số tự nhiên x,y mà $\varphi(x):\varphi(y)=a:b$.

Chứng minh. Với a và b là hai số tự nhiên cho trước. Không giảm tổng quát giả sử các số này nguyên tố cùng nhau. Ký hiệu c là số tự nhiên nguyên tố cùng nhau với ab (có vô hạn số như vậy chẳng hạn các số $kab+1$ với $k=1,2,...$). Đặt $x=a^2bc,\ y=ab^2c$. Vì các số a,b,c đôi một nguyên tố cùng nhau nên $\varphi(x)=\varphi(a^2)\varphi(b)\varphi(c)$ và $\varphi(y)=\varphi(a)\varphi(b^2)\varphi(c)$. Từ Định lý 3 suy ra với mọi số tự nhiên n ta có $\varphi(n^2)=n\varphi(n)$ và suy ra $\varphi(a^2)=a\varphi(a)$, $\varphi(b^2)=b\varphi(b)$ nên $\varphi(x):\varphi(y)=a:b$.

Từ giả thuyết H suy ra sự tồn tại vô hạn các số nguyên tố x,y thỏa mãn $\varphi(x):\varphi(y)=a:b$ với các cặp số cho trước a,b (Schinzel và Sierpinski [3] trang 192).

7. Chứng minh rằng nếu n là số tự nhiên >1 thì tồn tại vô hạn số tự nhiên m mà $\varphi(m)/m=\varphi(n)/n$.

Chứng minh. Số n là số tự nhiên >1 có ước số nguyên tố p do đó $n=p^\alpha n_1$ với α là số tự nhiên và $(n_1,p)=1$. Vì vậy $\dfrac{\varphi(n)}{n}=\dfrac{p^{\alpha-1}(p-1)\varphi(n_1)}{p^\alpha n_1}=\dfrac{p-1}{p}\dfrac{\varphi(n_1)}{n_1}$. Đặt $m=p^\alpha n_1$ với β là số tự nhiên. Lập luận tương tự ta có $\dfrac{\varphi(m)}{m}=\dfrac{p-1}{p}=\dfrac{\varphi(n_1)}{n_1}$ do đó $\dfrac{\varphi(m)}{m}=\dfrac{\varphi(n)}{n}$ và suy ra điều phải chứng minh.

Có thể chứng minh các số $\varphi(n)/n, n=1,2,...$ tạo thành một tập hợp trù mật trong khoảng $(0,1)$. Mặt khác tồn tại tập hợp trù mật trong khoảng $(0,1)$ chứa các số hữu tỷ mà không có dạng $\varphi(n/n)$ (Schoenberg [1], Sierpinski [26] trang 210). K.Zarankiewicz đã đặt ra câu hỏi có phải tập hợp các số $\varphi(n+1)/\varphi(n), n=1,2,...$ là trù mật trong tập hợp các số thực hay không. A.Schinzel [3] đã chứng minh câu trả lời là khẳng định (Erdos và Schinzel [1]).

8. Tim tất cả các nghiệm tự nhiên của phương trình $\varphi(n)=\varphi(2n)$.

Lời giải. Đó là các số lẻ.

9. Tìm tất cả các nghiệm tự nhiên của phương trình $\varphi(2n)=\varphi(3n)$.

Lời giải. Đó là các số tự nhiên chẵn không chia hết cho 3.

10. Tìm tất cả các nghiệm tự nhiên của phương trình $\varphi(3n)=\varphi(4n)$.

Lời giải. Đó là các số không chia hết cho 2 hoặc không chia hết cho 3.

11. Chứng minh rằng với mọi số tự nhiên k thì tồn tại ít nhất một số tự nhiên n mà $\varphi(n+k)=\varphi(n)$.

Chứng minh. Nếu k là số lẻ thì mệnh đề đúng vì $\varphi(2k)=\varphi(k)$ và ta đặt $n=k$. Giả sử k chẵn và ký hiệu p là số nguyên tố nhỏ nhất không phải ước số của k. Khi đó mỗi số nguyên tố $<p$ đều là ước số

của k. Vì vậy $\varphi\big((p-1)k\big)=(p-1)\varphi(k)$ (điều này suy ra từ Định lý 3 vì nếu *m* là số tự nhiên mà mọi ước số nguyên tố của nó đều là ước số nguyên tố của k thì $\varphi(mk)=m\varphi(k)$ mà $(p,k)=1$ suy ra $\varphi(pk)=\varphi(p)\varphi(k)=(p-1)\varphi(k)=\varphi\big((p-1)k\big)$. Do đó đặt $n=(p-1)k$ ta có $\varphi(n+k)=\varphi(n)$, điều phải chứng minh (Sierpinski [18] trang 184).

Ta chứng minh được với mọi số tự nhiên m thì luôn tồn tại số tự nhiên k mà phương trình $\varphi(n+k)=\varphi(n)$ có nhiều hơn m nghiệm tự nhiên n (tài liệu đã dẫn trang 184-185).

12. Chứng minh rằng tồn tại vô hạn số tự nhiên m mà phương trình $\varphi(n)=m$ có đúng hai nghiệm tự nhiên n.

Chứng minh. Các số $m=2\cdot 3^{6k+1}$ với $k=1,2,\ldots$ thỏa mãn. Thật vậy, giả sử n là số tự nhiên thỏa mãn $\varphi(n)=2\cdot 3^{6k+1}$. Rõ ràng n không phải lũy thừa của 2 (vì $\varphi\left(2^{\alpha}\right)=2^{\alpha-1}$) nên nó có ước số nguyên tố lẻ p và hơn nữa nó không có nhiều hơn một ước số như vậy vì $\varphi(n)$ không chia hết cho 4.

Nếu $p=3$ thì $n=3^{\beta}$ hoặc $n=2^{\alpha}3^{\beta}$ với α,β là các số tự nhiên. Khi đó vì $\varphi(n)=2\cdot 3^{6k+1}$ suy ra $2.3^{\beta-1}=2.3^{6k+1}$ hoặc $2^{\alpha}.3^{\beta-1}=2.3^{6k+1}$ và do đó $\alpha=1$ và $\beta-1=6k+1$. Vì thế $n=3^{6k+2}$ hoặc $n=2.3^{6k+2}$ và trong mọi trường hợp ta có $\varphi(n)=2\cdot 3^{6k+1}=m$.

Nếu $p\neq 3$ thì $p>3$ và do đó n không chia hết cho p^2 vì nếu ngược lại thì $p\,|\,\varphi(n)=2\cdot 3^{6k+1}$ mâu thuẫn vì $p>3$. Vì vậy $n=p$ hoặc $n=2^{\alpha}p$ với α là số tự nhiên. Vì vậy từ $\varphi(n)=2\cdot 3^{6k+1}$ suy ra ta có $p-1=2\cdot 3^{6k+1}$ hoặc $2^{\alpha-1}(p-1)=2\cdot 3^{6k+1}$. Mà p − 1 chẵn suy ra $\alpha=1$ và trong mọi trường hợp thì $p=2\cdot 3^{6k+1}+1$, vô lý vì với $k\geq 1$ ta có $p>7$ và theo định lý Fermat nhỏ thì $3^6\equiv 1(\mathrm{mod}\,7)$ suy ra $p=2.3^{6k+1}+1\equiv 2.3+1\equiv 0(\mathrm{mod}\,7)$, do đó $p\,|\,7$. Vì vậy phương trình $\varphi(n)=2\cdot 3^{6k+1}$ với *k* là số tự nhiên có đúng hai nghiệm là $n=3^{6k+2}$ và $n=2\cdot 3^{6k+2}$.

Phương trình $\varphi(n)=2\cdot 3$ có bốn nghiệm là $n=7,9,14,18$ và phương trình $\varphi(n)=2\cdot 3^2$ cũng có bốn nghiệm là $n=19,27,38,54$.

Ghi chú. A.Schinzel [6] đã tìm ra vô hạn số tự nhiên m mà phương trình $\varphi(n)=m$ có đúng ba nghiệm tự nhiên. Đó là các số $m=7^{12k+1}\cdot 12$ với $k=0,1,2,\ldots$. Khi đó $\varphi(n)=m$ với $n=7^{12k+2}.3$, $7^{12k+2}.4$ và $7^{12k+2}.6$. Để chứng minh đây là tất cả các nghiệm bằng cách sơ cấp thì tương đối dài.

13. Tìm tất cả các nghiệm tự nhiên của phương trình $\varphi(n)=2^{10}$.

Lời giải. Giả sử n là số chẵn và $n=2^{\alpha}q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_{k-1}^{\alpha_{k-1}}$ với $q_1,q_2,\ldots q_{k-1}$ là các số nguyên tố lẻ là phân tích thành thừa số nguyên tố của n.

Đặt $q_1<q_2<\ldots<q_{k-1}$ (có thể bỏ qua trường hợp $k=1$, nghĩa là $n=2^{\alpha}$). Vì $\varphi(n)=2^{10}$ nên $2^{\alpha-1}q_1^{\alpha_1-1}q_2^{\alpha_2-1}\ldots q_{k-1}^{\alpha_{k-1}-1}=(q_1-1)(q_2-1)\ldots(q_{k-1}-1)=2^{10}$ suy ra $\alpha_1=\alpha_2=\ldots=\alpha_{k-1}=1$ và $q_i=2^{\beta}+1$, $i=1,2,\ldots,k-1$ và β_i với $i=1,2,..,k-1$ là các số tự nhiên và $\alpha-1+\beta_1+\beta_2+\ldots+\beta_{k-1}=10$ do đó $\beta_i\leq 10$ với $i=1,2,\ldots,k-1$.

Các số nguyên tố lẻ có dạng $2^{\beta}+1,\beta\leq 10$ là các số $2^{\beta}+1$ với $\beta=1,2,4,8$. Vì thế $k\leq 5$.

Nếu $k=1$ thì nếu $n=2^{\alpha}$ ta có $\alpha-1=10$ suy ra $\alpha=11$ và hệ quả là $n=2^{11}=2048$.

Nếu $k=2$ thì $\alpha-1+\beta_1=10$ và với $\beta_1=1,2,4,8$ ta có $\alpha=10,9,7,3$ tương ứng. Do đó các giá trị của n là $2^{10}.3=3072$, $2^9.5=2560$, $2^7.17=2176$ hoặc $2^3.257=2056$.

Nếu $k=3$ thì $\alpha-1+\beta_1+\beta_2=10$. Vì vậy β_1 không thể >2 vì nếu như vậy thì β_1 lớn hơn hoặc bằng 4. Nhưng $\beta_1<\beta_2$ (với $q_1<q_2$) ta có $\beta_2>4$ do đó $\beta_2\geq 8$ và $\beta_1+\beta_2\geq 12$, vô lý. Vì vậy β_1 bằng 1 hoặc 2. Nếu $\beta_1=1$ thì $\alpha+\beta_2=10$ và $\beta_2>\beta_1=1$ do đó $\beta_2=2,4,8$ suy ra $\alpha=8,6,2$ và do đó $n=2^8.3.5, 2^6.3.17, 2^2.3.257$. Nếu $\beta_1=2$ thì $\alpha+\beta_2=9$, $\beta_2=4$ hoặc 8 suy ra $\alpha=5$ hoặc 1 và do đó $n=2^5.5.17$ hoặc $2.5.257$.

Nếu $k=4$ thì $\alpha-1+\beta_1+\beta_2+\beta_3=10$. Vì $\beta_1<\beta_2<\beta_3$ (suy ra từ $q_1<q_2<q_3$) và β_1,β_2,β_3 chỉ có thể là $1,2,4,8$ nên $\beta_1=1,\beta_2=2,\beta_3=4$ chứng tỏ $\alpha=4$ và do đó $n=2^4.3.5.17$.

Cuối cùng ta thấy không thể có $k=5$ vì nếu $k=5$ suy ra $\beta_1=1,\beta_2=2,\beta_3=4,\beta_4=8$ mâu thuẫn với đẳng thức $\alpha-1+\beta_1+\beta_2+\beta_3=10.$

Bây giờ giả sử n lẻ thì $n=q_1^{\alpha_1}q_2^{\alpha_2}...q_{k-1}^{\alpha_{k-1}}$ với $q_1,q_2,...,q_{k-1}$ là các số nguyên tố lẻ $q_1<q_2<...<q_{k-1}$. Theo giả thiết thì $q_1^{\alpha_1-1}q_2^{\alpha_2-1}...q_{k-1}^{\alpha_{k-1}-1}(q_1-1)(q_2-1)...(q_{k-1})-1=2^{10}$ nên $\alpha_1=\alpha_2=...=\alpha_{l-1}=1$ và $q_i=2^{\beta_i}+1$ với $i=1,2,...,k-1$. Hơn nữa $\beta_1+\beta_2+...\beta_{k-1}=10$.

Nếu $k=2$ thì $\beta_1=10$, vô lý. Nếu $k=3$ thì $\beta_1+\beta_2=10$ suy ra $\beta_1=2,\beta_2=8$ và do đó $n=5\cdot 257$.

Nếu $k=4$ thì $\beta_1+\beta_2+\beta_3=10$, vô lý vì β_1,β_2,β_3 là các số phân biệt thuộc dãy 1,2,4,8.

Tương tự không thể có $k\geq 5$. Vậy phương trình $\varphi(n)=2^{10}$ có đúng 12 nghiệm tự nhiên là

$$n=2^{11},2^{10}\cdot 3,2^9\cdot 5,2^7\cdot 17,2^3\cdot 257,2^8\cdot 3\cdot 5,2^6\cdot 3\cdot 17,2^2\cdot 3\cdot 257,2^5\cdot 5\cdot 17,5\cdot 257,2\cdot 5\cdot 257,2^3\cdot 3\cdot 5\cdot 17.$$

Ghi chú. Có thể chứng minh với $0\leq m\leq 31$ (m là số nguyên) thì phương trình $\varphi(n)=2^m$ có đúng $m+2$ nghiệm tự nhiên n. Với $31<m<2^{20}$ thì phương trình luôn có đúng 32 nghiệm. Chứng minh dựa trên tính chất các số $2^{2^n}+1$ $(5\leq n\leq 20)$ đều là hợp số *(1)*

14. Chứng minh rằng tồn tại vô hạn số tự nhiên m mà phương trình $\varphi(n)=m$ có ít nhất một nghiệm tự nhiên và mọi nghiệm của nó đều là số chẵn.

Chứng minh. Đặt $m=2^{32+2^s}$ với $s=6,7,...$. Nếu tồn tại số tự nhiên lẻ n thỏa mãn $\varphi(n)=m$ thì n là tích của các ước số nguyên tố khác nhau và có dạng $F_h=2^{2^k}+1$ vì nếu p là số nguyên tố và $p\mid n$ thì $p-1\mid\varphi(n)=m$ suy ra $p-1$ là lũy thừa cả 2 và do đó $p=F_k$. Giả sử đó là các số $F_{h_1},F_{h_2},...,F_{h_k}$. Khi đó $2^{h_1}+2^{h_2}+...+2^{h_k}=2^5+2^s$ với $h_1,h_2,...,h_k$ là các số tự nhiên phân biệt. Số 2^5+2^s với $s>5$ chỉ có một biểu diễn thành tổng các lũy thừa phân biệt của 2 nên một trong các số $F_{h_1},F_{h_2},...,F_{h_k}$ bằng F_5, vô lý vì F_5 là hợp số. Vậy phương trình $\varphi(n)=m$ không có nghiệm lẻ. Nếu n chẵn thì ta có $\varphi\left(2^{33+2^8}\right)=m$. □

(1) Carmichael [1] đã trình bày chứng minh với $m<2^{10}$. Với $2^{10}\leq m\leq 2^{20}$ thì chứng minh tương tự.

15. Chứng minh nếu $p>2$ và $2p+1$ là các số nguyên tố thì với $n=4p$ ta có $\varphi(n+2)=\varphi(n)+2$.

Chứng minh. Nếu các số $p>2$ và $2p+1$ là các số nguyên tố thì $\varphi(4p)=\varphi(4)\varphi(p)=2(p-1)$ và $\varphi(4p+2)=\varphi(2(2p+1))=\varphi(2p+1)=2p$ suy ra $\varphi(4p=2)=\varphi(4p)+2$. □

Ghi chú. Từ giả thuyết H (Chương 3 mục 8) suy ra tồn tại vô hạn cặp số nguyên tố sinh đôi. Tương tự, từ giả thuyết H cũng suy ra tồn tại vô hạn số nguyên tố p mà số $2p+1$ cũng là số nguyên tố. Do đó giả thuyết H suy ra tồn tại vô hạn số tự nhiên lẻ và vô hạn số tự nhiên chẵn n mà $\varphi(n+2)=\varphi(n)+2$.

2. Các tính chất của hàm chỉ Euler

Bây giờ với số tự nhiên cho trước n ta sẽ tính số các số tự nhiên $\le n$ mà ước số chung lớn nhất của chúng với n là bằng d với $d\mid n$.

Ước số chung lớn nhất của $m\le n$ và n là d khi và chỉ khi $m=kd$ với k là số tự nhiên $\le n/d$. Hệ quả là số các số tự nhiên $m\le n$ thỏa mãn điều kiện $(m,n)=d$ là bằng với số các số tự nhiên $\le n/d$ mà nguyên tố cùng nhau với n/d, tức là bằng với $\varphi(n/d)$.

Vì vậy ta thấy trong dãy $1,2,...,n$ thì với mọi ước số tự nhiên d của số tự nhiên n luôn có đúng $\varphi(n/d)$ số tự nhiên m mà $(m,n)=d$.

Giả sử $d_1,d_2,...,d_s$ là tất cả các ước số tự nhiên của số tự nhiên n. Các số $1,2,...,n$ có thể chia thành s lớp theo quy tắc số m thuộc lớp i khi và chỉ khi $(n,m)=d_i$. Số các phần tử của lớp i là $\varphi\left(\frac{n}{d_i}\right)$.

Hơn nữa vì số các số trong dãy $1,2,...,n$ là bằng n nên $\varphi\left(\frac{n}{d_1}\right)+\varphi\left(\frac{n}{d_2}\right)+..+\varphi\left(\frac{n}{d_s}\right)=n$. Nhưng nếu d_1 nhận mọi giá trị là ước số của n thì $\frac{n}{d_i}$ cũng nhận mọi giá trị là ước số của n. Vì vậy $\varphi(d_1)+\varphi(d_2)+...+\varphi(d_s)=n$, nghĩa là

(8) $$\sum_{d\mid n}\varphi(d)=n$$

Vậy ta đã chứng minh được

Định lý 7. *Tổng các giá trị của hàm chỉ Euler ứng với mọi ước số của n là bằng n.*

Sử dụng tích Dirichlet (Chương 4 mục 3) cho các chuỗi $a_1+a_2+...$ và $b_1+b_2+...,$ với số thực $s>2$, $a_n=\varphi(n)/n^s$, $b_n 1/n^s\ (n=1,2,...)$ ta nhận được từ ***(8)***

$$c_n=\sum_{d\mid n}a_d b_{\frac{n}{d}}=\sum_{d\mid n}\frac{\varphi(d)}{d^s}.\frac{d^s}{n^s}=\frac{1}{n}\sum_{d\mid n}\varphi(d)=\frac{n}{n^s}=\frac{1}{n^{s-1}}$$

Vì vậy $\sum_{n=1}^{x}c_n=\xi(s-1)$ và do đó $\sum_{n=1}^{x}\frac{\varphi(n)}{n}=\frac{\xi(s-1)}{\xi(s)}$ với $s>2$.

Sử dụng ***(8)*** có thể chứng minh đẳng thức Liouville $\sum_{n=1}^{\infty}\frac{\varphi(n)x^n}{1-x^n}=\frac{x}{(1-x)^2}$ với $|x|<1$.

Từ Định lý 6 mục 10 Chương 4 thì hàm chỉ Euler là hàm số duy nhất thỏa mãn Định lý 7.

Công thức ***(8)*** và công thức ***(37)*** cho ta công thức

(9) $$\varphi(n) = n\sum_{d|n}\frac{\mu(d)}{d}$$

đúng với mọi số tự nhiên n. Công thức này có thể viết lại dưới dạng

(10) $$\varphi(n) = \sum_{kl=n} l\mu(k)$$

với tổng lấy trên mọi cặp số tự nhiên k và l mà $kl = n$. Với $x \geq 1$ thì từ công thức ***(10)*** suy ra

(11) $$\sum_{n=1}^{[x]}\varphi(n) = \sum_{kl\leq x} l\mu(k)$$

với $\sum_{kl\leq x}$ là tổng tính trên mọi cặp số tự nhiên k,l mà $kl \leq x$. Nhưng $\sum_{kl\leq x} l\mu(k) = \sum_{k=1}^{[x]}\left(\mu(k)\sum_{l=1}^{[x/k]} l\right)$ và từ $\sum_{i=1}^{[x/k]} l = \frac{1}{2}\left[\frac{x}{k}\right]\left(\left[\frac{x}{k}\right]+1\right)$ theo công thức ***(33)*** Chương 4, công thức ***(11)*** suy ra

(12) $$\sum_{n=1}^{[x]}\varphi(n) = \frac{1}{2} + \frac{1}{2}\sum_{k=1}^{[x]}\left(\mu(k)\left[\frac{x}{k}\right]^2\right)$$

Công thức này có thể sử dụng để tính tổng các giá trị liên tiếp của hàm φ và tìm xấp xỉ cho tổng đó. Sử dụng công thức $\sum_{k=1}^{\infty}\frac{\mu(k)}{k^2} = \frac{6}{\pi^2}$ đã được chứng minh trong Chương 4 mục 10 ta có thể thấy tỷ số của $\sum_{n=1}^{[x]}\varphi(n)$ và $3x^2/\pi^2$ tiến tới 1 khi x tăng vô hạn.

Dạng tổng quát của hàm số $\varphi(n)$ là hàm số $\varphi_k(n)$ được xác định với các cặp số tự nhiên k,n là số các dãy $a_1, a_2, \ldots a_k$ chứa k số tự nhiên $\leq n$ mà $(a_1, a_2, \ldots a_k, n) = 1$.

Dễ dàng chứng minh được định lý C.Jordan [1] (trang 95-97) nói rằng nếu $n = q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_s^{\alpha_s}$ là phân tích thành thừa số nguyên tố của n thì $\varphi_k(n) = n^k\left(1-\frac{1}{q_1^k}\right)\left(1-\frac{1}{q_2^k}\right)\ldots\left(1-\frac{1}{q_s^k}\right)$ và $\sum_{d|n}\varphi_k(d) = n^k$.

Một dạng tổng quát khác của hàm φ là hàm $\phi_k(n)$ được cho bởi V.L.Klee, Jr. [3]. Hàm số này được xác định (với các số tự nhiên k và n) là số các số h xuất hiện trong dãy $1, 2, \ldots, n$ mà (h,n) không chia hết cho lũy thừa bậc k bất kỳ lớn hơn 1.

Dễ dàng chứng minh nếu $n = q_1^{\alpha_1}q_1^{\alpha_2}\ldots q_s^{\alpha_s}$ là phân tích thành thừa số nguyên tố của n thì $\Phi_k(n) = \prod_{\alpha_i<k} q_i^{\alpha_i}\prod_{a_i\geq k} q_i^{\alpha_i-k}\left(q_i^k-1\right)$. Ta cũng có $\Phi_k(n) = n\prod_{\substack{q^k|n\\ qprime}}\left(1-q^{-k}\right)$ và $\sum_{d|n}\Phi_k\left(d^k\right) = n^k$.

3. Định lý Euler

Cho trước số tự nhiên $m > 1$ và đặt

(13) $r_1, r_2, ..., r_{\varphi(m)}$

là dãy các số tự nhiên nguyên tố cùng nhau với m và nhỏ hơn m. Ký hiệu a là số nguyên tùy ý nguyên tố cùng nhau với m. Ký hiệu Q_k là số dư nhận được khi chia số ar_k cho $m\left(k=1,2,...,\varphi(m)\right)$. Ta có

(14) $Q_k \equiv ar_k \pmod m$ với $k=1,2,...,\varphi(m)$.

và

(15) $Q_k = ar_k + mt_k$,

với $t_k \left(k=1,2,...,\varphi(m)\right)$ là các số nguyên.

Ta sẽ chứng minh các số

(16) $Q_1, Q_2, ..., Q_{\varphi(m)}$

và các số ***(13)*** là trùng nhau chỉ sai khác một hoán vị. Ta chỉ cần chứng minh

(i) các phần tử của dãy ***(16)*** là các số tự nhiên nguyên tố cùng nhau với m và nhỏ hơn m,
(ii) các phần tử của ***(16)*** là phân biệt.

Đặt $d_k = (Q_k, m)$. Theo ***(15)*** thì $ar_k = Q_k - mt_k$ suy ra $d_k \mid m$. Nhưng vì $(a,m)=(r_k,m)=1, (ar_k,m)=1$ mà $d_k \mid m$ và $d_k \mid ar_k$ suy ra $d_k = 1$, nghĩa là $(Q_k, m)=1$. Mặt khác, số Q_k là số dư nhận được khi chia một số cho m nên $0 \le Q_k < m$. Hơn nữa vì $(Q_k, m)=1$ và $m>1$ nên Q_k khác 0. Vì vậy mọi phần tử của dãy ***(16)*** đều thỏa mãn tính chất ***(i)***.

Bây giờ giả sử với hai chỉ số phân biệt i và j trong dãy $1,2,...,\varphi(m)$ thì $Q_i = Q_j$. Khi đó theo ***(14)*** ta có $ar_i \equiv ar_j \pmod m$ và do đó $m \mid a(r_i - r_j)$ nên vì $(a,m)=1$ ta có $m \mid r_i - r_j$, vô lý vì r_i và r_j là hai phần tử phân biệt của ***(13)*** (với $i \ne j$) là các số tự nhiên phân biệt $\le m$. Vì vậy ta đã chứng minh được các phần tử của dãy ***(16)*** đều có tính chất ***(ii)***.

Từ đây suy ra các phần tử của dãy ***(16)*** và các phần tử của dãy ***(13)*** là đồng nhất sai khác một thứ tự. Do đó $Q_1 Q_2 ... Q_{\varphi(m)} = r_1 r_2 ... r_{\varphi(m)}$. Ký hiệu P là giá trị chung của các tích số này. Số P nguyên tố cùng nhau với m vì các nhân tử của nó nguyên tố cùng nhau với m. Nhân các đồng dư thức nhận được từ ***(14)*** bằng cách thay $1,2,...,\varphi(m)$ cho k ta nhận được $Q_1 Q_2 ... Q_{\varphi(m)} \equiv a^{\varphi(m)} r_1 r_2 ... r_{\varphi(m)} \pmod m$, nghĩa là $P \equiv a^{\varphi(m)} P \pmod m$. Điều này tương đương với $m \mid P\left(a^{\varphi(m)} - 1\right)$ suy ra vì $(P,m)=1$ ta có $m \mid a^{\varphi(m)} - 1$.

Vậy ta đã chứng minh được

Định lý 8 (Euler). *Với mọi số nguyên a nguyên tố cùng nhau với số tự nhiên m thì $a^{\varphi(m)} \equiv 1 \pmod m$.*

Nếu p là số nguyên tố thì $\varphi(p) = p-1$ do đó định lý Euler là tổng quát của định lý Fermat nhỏ (Chương 5 mục 5).

Định lý 8^a (Redei). *Với mọi số tự nhiên $m>1$ và a nguyên ta có (Szele [1] ghi chú 2)*

(17) $m \mid a^m - a^{m-\varphi(m)}$.

Chứng minh. Đặt $m = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k}$ là phân tích thành thừa số nguyên tố của m. Ký hiệu i là một trong các số $1, 2, \dots, k$. Nếu $(a, q_i) = 1$ thì theo Định lý 8 ta có $q_i^{\alpha_i} \mid a^{\varphi\left(q_i^{\alpha_i}\right)} - 1$ và từ Định lý 3 suy ra $\varphi\left(q_i^{\alpha_i}\right) \mid \varphi(m)$ và ta có $q_i^{\alpha_i} \mid a^{\varphi(m)} - 1$. Nếu α và $q \geq 2$ là các số tự nhiên thì theo quy nạp ta có $q^{\alpha - 1} \geq \alpha$. Mặt khác với $i = 1, 2, \dots, k$, ta có $q_i^{\alpha_i - 1} \mid m$ và $q_i^{\alpha_i - 1} \mid \varphi(m)$ suy ra $q_i^{\alpha_i - 1} \mid m - \varphi(m)$. Hơn nữa $m - \varphi(m)$ dương với m lớn hơn 1, nên từ tính chất cuối cùng suy ra $m - \varphi(m) \geq q_i^{\alpha_i - 1} \geq \alpha_i$. Vì vậy nếu $(a, q_i) > 1$ thì với $q_i \mid a$ ta có $q_i^{\alpha_i} \mid q_i^{m - \varphi(m)} \mid a^{m - \varphi(m)}$.

Vậy với mọi số nguyên a thì $q_i^{\alpha_i} \mid a^{m - \varphi(m)} \left(a^{\varphi(m)} - 1\right)$ với mọi $i = 1, 2, 3, \dots, k$. Nghĩa là $q_i^{\alpha_i} \mid a^m - a^{m - \varphi(m)}$ suy ra theo phân tích thành thừa số nguyên tố của a thì công thức ***(17)*** đúng. Định lý 8^a được chứng minh. □

Định lý Euler là hệ quả của Định lý 8^a. Thật vậy, theo Định lý 8^a thì với mọi số tự nhiên $m > 1$ và mọi số nguyên a ta có $m \mid a^{m - \varphi(m)} \left(a^{\varphi(m)} - 1\right)$. Do đó vì $(a, m) = 1$ nên $\left(a^{m - \varphi(m)}, m\right) = 1$ suy ra $m \mid a^{\varphi(m)} - 1$.

Bài tập. ***1.*** Chứng minh rằng từ một cấp số cộng vô hạn các số nguyên thì có thể chọn ra một chuỗi lũy thừa.

Chứng minh. Giả sử ta có cấp số cộng vô hạn các số nguyên

(18) $\qquad a, a + r, a + 2r, \dots$

Nếu $r = 0$ thì không có gì để chứng minh vì dãy ***(18)*** lập thành một cấp số nhân.

Nếu $r < 0$ thì bài toán được quy về trường hợp $r > 0$ bằng cách đổi dấu tất cả các phần tử của dãy.

Vậy chỉ cần xét trường hợp r là số tự nhiên. Hơn nữa có thể giả sử $(a, r) = 1$ vì nếu $d = (a, r) > 1$ thì ta có $a = da'$, $r = dr'$ với $(a', r') = 1$ và do đó chỉ cần chứng minh với cấp số cộng $a', a' + r', a' + 2r', \dots$.

Bây giờ xét $r > 0$, khi đó từ phần tử nào đó dãy ***(18)*** sẽ gồm toàn số lớn hơn 1. Vì vậy ta có thể giả sử $a > 1$. Vì $(a, r) = 1$ nên theo Định lý 8 thì $a^{\varphi(r)} \equiv 1 (\mathrm{mod}\, r)$. Vì vậy với các số tự nhiên $n, a^{n\varphi(r)} \equiv (\mathrm{mod}\, r)$ và do đó số $k_n = \left(aa^{n\varphi(r)} - a\right) / r$ nguyên với mọi $n = 1, 2, \dots$. Nhưng $a + k_n r = a\left(a^{\varphi(r)}\right)^n$ với $n = 1, 2, \dots,$ và do đó vì $a > 0$, $0 \leq k_1 < k_2 < \dots$ và các số $a + k_n r \left(n = 1, 2, \dots\right)$ tạo thành một cấp số nhân. □

Bài toán ta vừa chứng minh suy ra trong mọi cấp số cộng vô hạn thì có vô hạn các phần tử có chung ước số nguyên tố (Polya và Szego [1] trang 344). Một hệ quả khác của bài toán này là mọi cấp số cộng vô hạn các phần tử hữu tỷ thì tồn tại các phần tử lập thành một cấp số nhân số vạn.

2. Chứng minh rằng nếu m, a, r là các số tự nhiên với $(a, r) = 1$ và Z là tập hợp vô hạn các phần tử của cấp số cộng $a + kr \, (k = 1, 2, \dots)$ thì cấp số này chứa các phần tử là tích của nhiều hơn m phần tử phân biệt trong Z.

Chứng minh. Lấy ra $s = m\varphi(r) + 1$ số phân biệt trong tập Z và ký hiệu các số đó là $t_1, t_2, \dots, t_s$. Các số này là phần tử của cấp số cộng $a + kr \left(k = 1, 2, \dots\right)$ nên chúng đồng dư với s $a (\mathrm{mod}\, r)$. Do đó $t_1 t_2 \dots t_s \equiv a^s \equiv a \cdot a^{m\varphi(r)} (\mathrm{mod}\, r)$ mà $(a, r) = 1$ nên theo Định lý 8 suy ra $a^{\varphi(r)} \equiv 1 (\mathrm{mod}\, r)$. Vì vậy

$t_1 t_2 ... t_s \equiv a \pmod r$ và hệ quả là số $t_1 t_2 ... t_s$ là phần tử của cấp số cộng $a + kr \left(k = 1, 2, ...\right)$. Hơn nữa $s = m\varphi\left(r\right) + 1 > m$ và do đó ta có điều phải chứng minh. □

3. Chứng minh rằng mọi số tự nhiên không chia hết cho 2 hoặc 5 đều là ước số của số tự nhiên nào đó với các chữ số (trong hệ thập phân) đều bằng 1.

Chứng minh. Nếu $\left(n, 10\right) = 1$ thì $\left(9n, 10\right) = 1$ và vì vậy theo Định lý 8 thì $10^{\varphi(9n)} \equiv 1 \pmod{9n}$. Do đó $10^{\varphi(9n)} - 1 = 9nk$ với k là số tự nhiên. Vì vậy $nk = \left(10^{\varphi(9n)} - 1\right)/9$ và do đó các chữ số trong hệ thập phân của số này đều bằng 1. □

4. Chứng minh rằng mọi số tự nhiên đều có bội số với các chữ số trong hệ thập phân đều bằng 1 hoặc 0 và các chữ số 1 đứng liền trước các chữ số 0.

Chứng minh. Mọi số tự nhiên đều biểu diễn được dưới dạng $n = n_1 2^\alpha 5^\beta$ với $\left(n_1, 10\right) = 1$. Theo bài tập 3 thì n_1 là ước số của số m mà các chữ số của nó trong hệ thập phân đều bằng 1. Mặt khác $2^\alpha 5^\beta \mid 10^\gamma$ với $\gamma = \max\left(\alpha, \beta\right)$ nên $n \mid m \cdot 10^\gamma$. □

5. Tìm tất cả các nghiệm tự nhiên của đồng dư thức $x^x \equiv 3 \pmod{10}$.

Lời giải. Nếu số tự nhiên x thỏa mãn đồng dư thức trên thì vì $\left(3, 10\right) = 1$ ta có $\left(x, 10\right) = 1$. Hệ quả là $\left(x + 20k, 10\right) = 1$ với $k = 0, 1, 2, ...$ Vì vậy theo Định lý 8 thì với $\varphi\left(10\right) = 4$ ta có $\left(x + 20k\right)^4 \equiv 1 \pmod{10}$ do đó $\left(x + 20k\right)^{20k} \equiv 1 \pmod{10}$. Mặt khác đồng dư thức $\left(x + 20k\right)^x \equiv x^x \pmod{10}$ đúng với mọi số tự nhiên x. Do đó nhân hai đồng dư thức cuối cùng theo vế suy ra $\left(x + 20k\right)^{x + 20k} \equiv x^x \pmod{10}$ với mọi $k = 0, 1, 2, ...$. Nếu số tự nhiên x thỏa mãn đồng dư thức $x^x \equiv 3 \pmod{10}$ thì mọi phần tử của cấp số cộng $x + 20k \left(k = 0, 1, 2, ...\right)$ là thỏa mãn tính chất này. Dễ thấy trong các số nguyên x mà $0 \le x < 20$ chỉ có 7 và 13 thỏa mãn đồng dư thức đó nên tất cả các nghiệm tự nhiên của đồng dư thức $x^x \equiv 3 \pmod{10}$ là $7 + 20k$ và $13 + 20k$ với $k = 0, 1, 2, ...$

4. Các số với số mũ cho trước theo một modulo cho trước

Từ Định lý 8 suy ra nếu a là số nguyên nguyên tố cùng nhau với số tự nhiên m thì đồng dư thức

(19) $$a^x \equiv 1 \pmod m$$

có vô hạn nghiệm tự nhiên x chẳng hạn dãy vô hạn các số $x = k\varphi\left(m\right)$ với $k = 1, 2, ...$ đều là nghiệm. Mặt khác đồng dư thức ***(19)*** có nghiệm tự nhiên chỉ khi $\left(a, m\right) = 1$.

Nếu $x = \delta$ là nghiệm tự nhiên nhỏ nhất của đồng dư thức ***(19)*** thì ta nói số này có số mũ δ theo modulo m.

Rõ ràng nếu hai số đồng dư theo modulo m thì chúng có cùng số mũ modulo m vì với $a \equiv b \pmod m$ và với x ta có ***(19)*** thì $b^x \equiv 1 \pmod m$ vì từ $a \equiv b \pmod m$ suy ra $a^x \equiv b^x \pmod m$ với mọi $x = 1, 2, ...$

Định lý 9. *Nếu $\left(a, m\right) = 1$ thì mọi nghiệm của đồng dư thức **(19)** đều chia hết cho số mũ δ của a theo modulo m.*

Chứng minh. Giả sử phản chứng rằng tồn tại nghiệm x đồng dư thức ***(19)*** mà không chia hết cho δ. Nghĩa là x chia δ dư r. Theo đó $x = k\delta + r$ với k là số nguyên không âm. Theo ***(19)*** ta có

(20) $$a^{k\delta+r} \equiv 1(\mathrm{mod}\, m) \text{ hay } \left(a^{\delta}\right)^{k} a^{r} \equiv 1(\mathrm{mod}\, m).$$

Theo định nghĩa của δ thì đồng dư thức $a^{\delta} \equiv 1(\mathrm{mod}\, m)$ đúng. Vì vậy theo ***(20)*** thì $a^{r} \equiv (\mathrm{mod}\, m)$. Vì vậy từ giả thiết suy ra tồn tại nghiệm r của đồng dư thức ***(19)*** nhỏ hơn δ, nhưng điều này mâu thuẫn với định nghĩa của δ. Định lý được chứng minh. □

Theo Định lý 8 thì $\varphi(m)$ là nghiệm của đồng dư thức ***(19)***. Định lý 9 suy ra

Hệ quả. *Số mũ của một số nguyên tố với m theo modulo m là ước số của $\varphi(m)$.*

Đặc biệt nếu tồn tại các số nguyên tố cùng nhau với m và có số mũ là $\varphi(m)$ theo modulo m (cũng tức là các số có số mũ lớn nhất theo modulo m) thì các số đó được gọi là căn nguyên thủy của m.

Ví dụ 3 là căn nguyên thủy của 10 vì $3^1 \equiv 3, 3^2 \equiv 9, 3^3 \equiv 7, 3^4 \equiv 1(\mathrm{mod}10)$ và $\varphi(10) = 4$. Tuy nhiên 10 không phải là căn nguyên thủy của 3 vì $10 \equiv 1(\mathrm{mod}\, 3)$ chứng tỏ 10 có số mũ là 1 theo modulo 3 và $\varphi(3) = 2$. Số 7 là căn nguyên thủy của 10 vì $7^1 \equiv 7, 7^2 \equiv 9, 7^3 \equiv 3, 7^4 \equiv 1(\mathrm{mod}10)$ và 10 cũng là căn nguyên thủy của 7 vì $10 \equiv 3, 10^2 \equiv 2, 10^3 \equiv 6, 10^4 \equiv 4, 10^5 \equiv 5, 10^6 \equiv 1(\mathrm{mod}\, 7)$ và $\varphi(7) = 6$.

Từ Định lý 8 suy ra với mọi số tự nhiên m thì đều tồn tại số tự nhiên nhỏ nhất $\lambda(m)$ mà $m \mid a^{\lambda(m)} - 1$ với $(a, m) = 1$ (các số này là cần thiết khi xác định các hàm Liouville trong Chương 4 mục 11). Số $\lambda(m)$ được gọi là lũy thừa phổ quát *(universal exponent)* nhỏ nhất modulo m. Theo Định lý 8 thì $\lambda(m) \le \varphi(m)$ với mọi số tự nhiên m. Ta có $\lambda(2) = 1, \lambda(2^2) = 2, \lambda(2^{\alpha}) = 2^{\alpha-2}, \alpha = 3, 4, \ldots$. Nếu $m = 2^{\alpha} q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}$, $2 < q_1 < q_2 < \ldots < q_s$ là phân tích thành thừa số nguyên tố của m thì $\lambda(m) = \left[\lambda(2^{\alpha_0}), \varphi(q_1^{\alpha_1}), \ldots, \varphi(q_s^{\alpha_s})\right]$ và với mọi số tự nhiên m thì luôn tồn tại số tự nhiên có số mũ $\lambda(m)$ theo modulo m (Ore [1] trang 292-293).

Trong *Mathematical Tables và Aids to Computation 4 (1950)* trang 29-30, S.Whitten [1] đã tính được $\lambda(n)$ với $n \le 1200$. Dưới đây là bằng $\lambda(m)$ với $m < 100$.

	0	1	2	3	4	5	6	7	8	9
			1	2	2	4	2	6	2	6
1	4	10	2	12	6	4	4	16	6	18
2	4	6	10	22	2	20	12	18	6	28
3	4	30	8	10	16	12	6	36	18	12
4	4	40	6	42	10	12	22	46	4	42
5	20	16	12	52	18	20	6	18	28	58
6	4	60	30	6	16	12	10	66	16	22
7	12	70	6	72	36	20	18	30	12	78
8	4	54	40	82	6	16	42	28	10	88
9	12	12	22	30	46	36	8	96	42	30

Có thể chứng minh $\lambda(m)=\varphi(m)$ chỉ khi $m=1,2,4,p^{\alpha}$ và $2p^{\alpha}$ với p là số nguyên tố lẻ và α là số tự nhiên. Một báo cáo khác gần đây đã chỉ ra sự tồn tại dãy tăng vô hạn các số tự nhiên $n_k\,(k=1,2,\ldots)$ mà $\lim\limits_{k=\infty}\lambda(n_k)/\varphi(n_k)=0$. Chẳng hạn dãy $n_k=p_1\,p_2\ldots p_k\,(k=1,2,\ldots)$. Có thể chứng minh m là hợp số Carmichael (và do đó là số giả nguyên tố tuyệt đối) khi và chỉ khi $\lambda(m)\,|\,m-1$ (Carmichael [2] trang 237 công thức ***(18)***).

Carmichael đã thông báo (tài liệu đã dẫn trang 236) phương trình $\lambda(n)=2$ có đúng sáu nghiệm $n=2,4,6,8,12,24,$ và phương trình $\lambda(n)=4$ có đúng 12 nghiệm mà nghiệm nhỏ nhất là $n=5$ và nghiệm lớn nhất là $n=240$. Phương trình $\lambda(n)=12$ có 84 nghiệm mà nghiệm nhỏ nhất là $n=13$ và nghiệm lớn nhất là $n=65520$. Ta có $\lambda(100)=20$. Với $n<100$ thì đẳng thức $\lambda(n+1)=\lambda(n)$ đúng chỉ với $n=3,15$ và 90.

Với mọi số tự nhiên s thì đều tồn tại số tự nhiên m_s mà phương tình $\lambda(n)=m_s$ có nhiều hơn s nghiệm tự nhiên n. Theo Định lý 11 (sẽ được chứng minh trong mục tiếp theo) thì với mọi số tự nhiên s đều tồn tại số tự nhiên k mà $p=2^sk+1$ là số nguyên tố. Với $j=0,1,2,\ldots,s,s+1$ ta có $\lambda\left(2^j\left(2^sk+1\right)\right)=2^sk$ do đó đặt $m_s=2^sk$ ta nhận được tính chất ở trên.

Dễ dàng chứng minh với mọi số tự nhiên $n>2$ thì các số $\lambda(n)$ đều chẵn. Tồn tại vô hạn số chẵn không phải giá trị của hàm $\lambda(n)$. Có thể chứng minh các số $2\cdot7^k$ với $k=1,2,\ldots,$ đều có tính chất này (Sierpinski [26] trang 191-192).

Định lý 10. *Nếu p là số nguyên tố >2 thì mọi ước số tự nhiên của số 2^p-1 đều có dạng $2kp+1$ với k là số nguyên.*

Chứng minh. Do tích của hai (hoặc nhiều hơn) các số có dạng $2kp+1$ thì cũng có dạng này và vì 1 có dạng đó (với $k=0$) nên chỉ cần chứng minh mọi ước số nguyên tố q của số 2^p-1 đều có dạng $2kp+1$. Nếu $q\,|\,2^p-1$ thì $2^p\equiv1\left(\mathrm{mod}\,q\right)$ và do đó theo Định lý 9 thì $\delta\,|\,p$ với δ là số mũ của 2 theo modulo q. Ta không thể có $\delta=1$ vì nếu vậy thì $2\equiv1\left(\mathrm{mod}\,q\right)$ và $q\,|\,1$, vô lý. Do đó vì $\delta\,|\,p$ và p là số nguyên tố suy ra $\delta=p$. Mặt khác hệ quả của Định lý 9 suy ra $\delta\,|\,\varphi(q)$, nghĩa là $\delta\,|\,q-1$. Vì vậy $p\,|\,q-1$ và vì q là ước số của một số lẻ và $(p,2)=1$ (vì p là số nguyên tố >2) nên suy ra $2p\,|\,q-1$, nghĩa là $q-1=2kp$ do đó $q=2kp+1$ với k là số nguyên. Định lý được chứng minh. □

Ta lưu ý trong Định lý 10 thì giả thiết p là số nguyên tố >2 là cần thiết. Các ước số 3,5 và 15 của 2^4-1 không có dạng $8k+1$ và ước số $7=2^3-1$ của $2^{15}-1$ không có dạng $30k+1$.

Bài tập. ***1.*** Chứng minh định lý Fermat sau đây: *nếu p là số nguyên tố >3 thì mọi ước số tự nhiên >1 của số $\left(2^p+1\right)/3$ đều có dạng $2kp+1$ với k là số tự nhiên.*

Chứng minh. Số $\left(2^p+1\right)/3$ là số tự nhiên vì với số lẻ $p, 2+1\,|\,2^p+1$. Ký hiệu d là ước số >1 của $\left(2^p+1\right)/3$ và q là ước số nguyên tố của d. Nếu $q=3$ thì $2^q+1\equiv0\left(\mathrm{mod}\,9\right)$ suy ra $2^{2p}\equiv1\left(\mathrm{mod}\,9\right)$ và theo Định lý 9 thì số $2p$ chia hết cho số mũ của 2 theo modulo 9. Nhưng ta lại dễ dàng tính được $\delta=6$ và do đó $6\,|\,2p$ suy ra $3\,|\,p$, mâu thuẫn với giả thiết $p>3$. Vì vậy cần phải có $q\neq3$. Vì

$2^p+1=0\pmod q$ ta có $2^{2p}\equiv 1\pmod q$. Ký hiệu δ là số mũ của 2 theo modulo q. Ta không thể có $\delta=1$ hoặc $\delta=2$ vì $q\neq 3$. Vậy $\delta>2$. Nhưng theo Định lý 9 thì $\delta\mid 2p$ và vì $2^{q-1}\equiv 1\pmod q$, $\delta\mid q-1$. Do đó các số $2p$ và $q-1$ có ước số chung $\delta>2$ và suy ra p và $q-1$ có ước số chung >1. Nhưng vì p là số nguyên tố nên suy ra $p\mid q-1$ và do đó $q=pt+1$ với t là số nguyên và vì p,q đều lẻ nên t chẵn. Do đó $q=2kp+1$ với k là số tự nhiên và vì thế mỗi ước số của d đều có dạng $2kp+1$. Hệ quả là d cũng có dạng $2kp+1$. Định lý được chứng minh. □

2. Chứng minh rằng nếu a,b và n là các số tự nhiên thỏa mãn $a>b, n>1$ thì mỗi ước số nguyên tố của số a^n-b^n sẽ có dạng $nk+1$ với k là số nguyên hoặc là ước số của $a^{n_1}-b^{n_1}$ với $n_1\mid n$ và $n_1<n$.

Chứng minh. Đặt $(a,b)=d$. Vì $a>b$ nên $a=a_1d,\ b=b_1d$ với $(a_1,b_1)=1$ và $a_1>b_1$. Giả sử p là ước số nguyên tố của số a^n-b^n. Khi đó $p\mid a^n-b^n=d^n\left(a_1^n-b_1^n\right)$. Nếu $p\mid d^n$ thì $p\mid d$ và vì vậy $p\mid a-b$. Định lý được chứng minh. Giả sử $p\mid a_1^n+b_1^n$ khi đó vì $(a_1,b_1)=1$ nên ta có $(a_1,p)=(b_1,p)=1$. Gọi p là ước số nguyên thủy của $a_1^\delta-b_1^\delta$ (nghĩa là $p\mid a_1^\delta-b_1^\delta$ và ta không có $p\mid a_1^m-b_1^m$ với mọi $0<m<\delta$). Lưu ý rằng $\delta\mid n$. Thật vậy, giả sử n không chia hết cho δ. Khi đó $n=k\delta+r$ với k là số nguyên ≥ 0 và $0<r<\delta$. Nhưng $p\mid a_1^\delta-b_1^\delta$ và do đó $p\mid a_1^{k\delta}-b_1^{k\delta}$. Do $a_1^{k\delta+r}-b_1^{k\delta+r}=\left(a_1^{k\delta}-b_1^{k\delta}\right)a_1^r+b_1^{k\delta}\left(a_1^r-b_1^r\right)$ suy ra $p\mid b_1^{k\delta}\left(a_1^r-b_1^r\right)$ mà $(b_1,p)=1$ suy ra $p\mid a_1^r-b_1^r$ với $0<r<\delta$, mâu thuẫn với giả thiết p là ước số nguyên thủy của $a_1^\delta-b_1^\delta$.

Nếu $\delta<n$ thì $\delta\mid n$ và $p\mid a_1^{n_1}-b_1^{n_1}\mid a^{n_1}-b^{n_1}$ với $n_1=\delta,\ n_1\mid n$ và $n_1<n$. Đặt $\delta=n$ khi đó theo định lý Fermat nhỏ thì $p\mid a_1^{p-1}-1,\ p\mid b_1^{p-1}-1$ suy ra $p\mid a_1^{p-1}-b_1^{p-1}$. Hệ quả là $n=\delta\mid p-1$ và do đó p có dạng $nk+1$. □

3. Chứng minh rằng nếu a,b,n là các số tự nhiên mà $a>b, n>1$ thì mọi ước số nguyên tố của a^n+b^n hoặc là có dạng $2nk+1$ với k là số nguyên nào đó; hoặc là ước số của số $a^{n_1}+b^{n_1}$ với n_1 là thương số nhận được khi chia n cho một số lẻ lớn hơn 1 nào đó.

Chứng minh. Tương tự như bài tập trước.

5. Sự tồn tại vô hạn các số nguyên tố trong cấp số cộng $nk+1$

Định lý 11. *Nếu p là số nguyên tố và s là số tự nhiên thì tồn tại vô hạn số nguyên tố có dạng $2p^sk+1$ với k là số tự nhiên.*

Chứng minh. Giả sử p nguyên tố và s là số tự nhiên. Đặt $a=2^{p^{s-1}}$. Giả sử q là ước số nguyên tố tùy ý của số $a^{p-1}+a^{p-2}+....a+1$. Nếu a đồng dư với $1\pmod q$ thì $q\mid a^{p-1}+a^{p-2}+...+a+1\equiv p\pmod q$ do đó $q\mid p$ mà p và q là các số nguyên tố suy ra $q=p$ và do đó $a^p\equiv 1\pmod p$ nên $2^{p^s}\equiv 1\pmod p$. Nhưng theo Định lý 5^a Chương 5 thì suy ra $2^p\equiv 2\pmod p$ nên theo quy nạp thì $2^{p^s}\equiv 2\pmod p$ và suy ra 1 đồng dư với $2\pmod p$ do đó $p\mid 1$, vô lý.

Vậy $a\not\equiv 1\pmod q$, nghĩa là $2^{p^{s-1}}\not\equiv 1\pmod q$. Ký hiệu δ là số mũ của 2 theo modulo q. Vì $q\mid a^p-1$, nghĩa là $2^{p^s}\equiv 1\pmod q$ nên $\delta\mid p^s$ và vì $s^{p^{s-1}}\not\equiv 1\pmod q$ nên không thể có $\delta\mid p^{s-1}$. Vậy δ bằng p^s. Theo hệ quả của Định lý 9 ta có $\delta\mid\varphi(q)$, nghĩa là $p^s\mid q-1$. Vì $2^{p^s}\equiv 1\pmod q$ nên q lẻ và do đó $p-1$

chẵn. Nếu p là số nguyên tố >2 thì $(p,2)=1$ và do đó vì $p^s \mid q-1$ suy ra $2p^s \mid q-1$ chứng tỏ $q=2p^sk+1$ với số tự nhiên k nào đó. Nếu $p=2$ thì $2^s \mid q-1$ suy ra $q=2^sk+1$ với k là số tự nhiên.

Vậy nếu p lẻ thì tồn tại ít nhất một số nguyên tố có dạng $2p^sk+1$. Nếu $p=2$ thì tồn tại ít nhất một số nguyên tố có dạng 2^sk+1. Vì s tùy ý nên Định lý 11 được chứng minh. □

Chứng minh định lý tổng quát hơn sau đây là khó hơn

Định lý 11^a**.** *Với mọi số tự nhiên n thì tồn tại vô hạn số nguyên tố có dạng $nk+1$ với k là số tự nhiên.*

Chứng minh (theo A.Rotkiewicz [4], xem thêm Estermann [2]). Đầu tiên ta lưu ý rằng để chứng minh định lý thì chỉ cần chứng minh rằng với mọi số tự nhiên n thì tồn tại ít nhất một số nguyên tố có dạng $nk+1$ với k là số tự nhiên vì khi đó với hai số tự nhiên n,m thì tồn tại ít nhất một số nguyên tố có dạng $nmt+1$ với t là số tự nhiên và số nguyên tố này $>m$ và có dạng $nk+1$ với k là số tự nhiên.

Không giảm tổng quát có thể giả sử $n>2$ vì trong dãy tất cả các số lẻ thì tồn tại vô hạn số nguyên tố.

Đặt $n=q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_s^{\alpha_s}$ là phân tích thành thừa số nguyên tố của n với $q_1<q_2<\ldots.<q_s$. Giả sử với mọi ước số nguyên tố p của a^n-1 thì n có số mũ $<n$ theo modulo p. Đặt

(21) $$P_n=\prod_{d\mid n}\left(n^d-1\right)^{\mu(n/d)},$$

với μ là hàm Mobius (Chương 4 mục 10). Ta biểu diễn các nhân tử n^d-1 thành tích các ước số nguyên tố của nó. Khi đó tích ***(21)*** trở thành tích của các ước số nguyên tố và số mũ của chúng đều nguyên (dương, âm hoặc bằng 0). Xét p là một trong các ước số nguyên tố đó. Khi đó tồn tại số tự nhiên $d\mid n$ thỏa mãn $p\mid n^d-1$. Vì $d\mid n$ nên $p\mid n^n-1$ và $(n,p)=1$. Ký hiệu δ là số mũ của n theo modulo p. Từ giả thiết suy ra $\delta<n$. Hệ quả trực tiếp của Định lý 9 là trong các số n^d-1 với $d\mid n$ thì tất cả các số chia hết cho p là các số mà $\delta\mid d$, nghĩa là $d=\delta k$ với k là số tự nhiên thỏa mãn $\delta k\mid n$ do đó $k\mid\frac{n}{\delta}$. Vì $p\mid n^n-1$ nên ta có $\delta\mid n$ và suy ra n/δ là số tự nhiên >1 (vì $\delta<n$).

Gọi λ là lũy thừa lớn nhất mà p^λ là ước số của $n^\delta-1$. Ta có $p^\lambda\mid n^\delta-1$ và không có $p^{\lambda+1}\mid n^\delta-1$. Nếu với số tự nhiên $k\mid n/\delta$ ta có $p^{\lambda+1}\mid n^{k\delta}-1$ thì vì $\frac{n^{\delta k}-1}{n^\delta-1}=\left(\left(n^\delta\right)^{k-1}-1\right)+\left(\left(n^\delta\right)^{k-2}-1\right)+\ldots+\left(n^\delta-1\right)+k$, $p\mid k$, vô lý, vì $k\mid n$ và $(n,p)=1$. Do đó với mọi số tự nhiên $k\mid n/\delta,\lambda$ là lũy thừa lớn nhất mà $p^\lambda\mid n^{\delta k}-1$. Từ đây suy ra trong phân tích ***(21)*** thì số mũ của số nguyên tố p là $\sum_{k\mid\frac{n}{\delta}}\lambda\mu\left(\frac{n}{\delta k}\right)$. Nhưng vì n/δ là số tự nhiên >1, theo công thức ***(32)*** Chương 4 mục 10 ta có $\sum_{k\mid\frac{n}{\delta}}\mu\left(\frac{n}{\delta k}\right)=\sum_{k\mid\frac{n}{\delta}}\mu(k)=0$. Vì tính chất này đúng với mọi ước số nguyên tố p của số ***(21)*** nên $P_n=1$. Nhưng theo ***(21)*** ta có

(22) $$P_n=\prod_{d\mid n}\left(n^{n/d}-1\right)^{\mu(d)}=\prod_{d\mid q_1q_2\ldots q_s}\left(n^{n/d}-1\right)^{\mu(d)}$$

vì $\mu(d)=0$ với mọi số d chia hết cho bình phương một số tự nhiên >1.

Đặt $b = n^{q_1^{\alpha_1-1} q_2^{\alpha_2-1} \ldots q_s^{\alpha_s-1}}$ ta có $b \geq n > 2$ và $b^{q_1 q_2 \ldots q_s} = n^n$ vì vậy theo ***(22)*** thì $P_n = \prod_{d \mid q_1 q_2 \ldots q_s} \left(b^{q_1 q_2 \ldots q_s / d} - 1\right)^{\mu(d)}$.

Ta thấy P_n là thương của hai đa thức biến b với hệ số nguyên. Bây giờ ta tìm lũy thừa nhỏ nhất của b trong cả tử số và mẫu số của thương số. Ta xét hai trường hợp: s là số chẵn và s lẻ. Trong trường hợp thứ nhất thì lũy thừa tự nhiên nhỏ nhất của b trong tử số nhận được với $d = q_1 q_2 \ldots q_s$. Do đó số mũ trong lũy thừa này bằng 1 và tử số chia cho b^2 có số dư là $b-1$ hoặc $b^2 - b + 1$. Trong mẫu số thì vì $q_1 < q_2 < \ldots < q_s$ nên lũy thừa nhỏ nhất nhận được với $d = q_2 q_3 \ldots q_s$. Do đó số mũ trong lũy thừa này là q_1. Tử số chia b^2 dư 1 hoặc $b^2 - 1$. Nhưng vì $P_n = 1$ suy ra mâu thuẫn vì nếu $b > 2$ thì các số $b-1$ và $b^2 - b + 1$ là khác 1 và $b^2 - 1$. Nếu s lẻ thì lũy thừa nhỏ nhất của b đạt được trong tử số là với $d = q_2 q_3 \ldots q_s$ và trong mẫu số là với $d = q_1 q_2 \ldots q_s$ và ta lại thu được mâu thuẫn.

Vậy từ giả thiết với mọi ước số nguyên tố p của $n^n - 1$ thì số n có số mũ nhỏ hơn n theo modulo p dẫn tới mâu thuẫn. Vậy $n^n - 1$ có ít nhất một ước số nguyên tố p mà n có số mũ n theo modulo p. Nhưng $(n, p) = 1$ và theo định lý Fermat nhỏ thì $p \mid n^{p-1} - 1$ suy ra theo Định lý 9 ta có $n \mid p - 1$, nghĩa là $p = nk + 1$ với k là số tự nhiên. Vậy ta đã chứng minh với mọi số tự nhiên $n > 1$ thì tồn tại ít nhất một số nguyên tố có dạng $nk + 1$ với k là số tự nhiên, suy ra Định lý 11^a được chứng minh, □

Sử dụng Định lý 11^a ta chứng minh được định lý A.Makowski (Chương 5 mục 7): *với mọi số tự nhiên* $k \geq 2$ *thì tồn tại vô hạn hợp số tự nhiên* n *mà* $n \mid a^{n-k} - 1$ *với mọi số nguyên* a *mà* $(a, n) = 1$.

Chứng minh. Đặt $k = q_1^{\alpha_1} q_2^{\alpha} \ldots q_s^{\alpha_s}$ với $q_1 < q_2 < \ldots < q_s$ là phân tích thành thừa số nguyên tố của số tự nhiên $k \geq 2$. Theo Định lý 11^a thì tồn tại vô hạn số nguyên tố $p > k$ có dạng $(q_1 - 1)(q_2 - 1)\ldots(q_s - 1)t + 1$ với t là số tự nhiên. Ta sẽ chứng minh nếu p là một số như vậy thì số $n = kp$ là hợp số thỏa mãn các điều kiện trong đề bài. Thật vậy, ta có

$$\begin{aligned} n - k = k(p-1) &= q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s} (q_1 - 1)(q_2 - 1)\ldots(q_s - 1)t \\ &= q_1 q_2 \ldots q_s \varphi(k) t, \end{aligned}$$

Sử dụng định lý Euler và định lý Fermat nhỏ suy ra với $(a, n) = 1$ thì $a^{n-k} - 1$ chia hết cho k và p và do đó chia hết cho $kp = n$. □

Ta có một ứng dụng khác của Định lý 11^a.

Ta gọi dãy $p, p+2, p+6$ mà các phần tử đều là số nguyên tố là bộ ba nguyên tố loại một và dãy $p, p+4, p+6$ mà các phần tử đều là số nguyên tố là bộ ba nguyên tố loại hai. Ta chứng minh nếu từ tập hợp tất cả các số nguyên tố ta bỏ đi các số nguyên tố thuộc vào các bộ ba nguyên tố loại một hoặc loại hai thì vẫn còn lại vô hạn số nguyên tố trong dãy

Thật vậy, từ Định lý 11^a suy ra tồn tại vô hạn số nguyên tố q có dạng $q = 15k + 1$ với k là số tự nhiên. Hiển nhiên với mọi số q thì $3 \mid q+2, 5 \mid q+4, 3 \mid q-4, 5 \mid q-6$. Vì vậy do $q > 15$ nên ta thấy các số $q+2, q+4, q-4$ và $q-6$ đều là hợp số. Vậy q không thể thuộc bộ ba nguyên tố loại một hoặc loại hai. Thật vậy, nếu q là một trong các số đó, nghĩa là $q = p$ hoặc $q = p+2$ hoặc $q = p+6$ và các số $p, p+2, p+6$ là nguyên tố thì trong trường hợp đầu tiên số $p + 2 = q + 2$ là hợp số và trong trường hợp thứ hai số $p + 6 = q + 4$ là hợp số và trong trường hợp thứ ba thì số $p = q - 6$ là hợp số. Vậy cả ba

trường hợp đều không xảy ra. Tương tự nếu $p, p+4, p+6$ là nguyên tố thì nếu $p=q, p+4=q+4$ là hợp số, nếu $q=p+4$ thì $p+6=q+2$ là hợp số và nếu $q=p+6$ thì $p=q-6$ là hợp số.

6. Sự tồn tại căn nguyên thủy của số nguyên tố

Ký hiệu p là số nguyên tố cho trước. Theo hệ quả của Định lý 9 thì các phần tử của dãy

(23) $1,2,3,\ldots,p-1$

đều có số mũ (theo $(\mathrm{mod}\, p)$) là ước số của $\varphi(p)=p-1$. Với mỗi ước số tự nhiên δ của $p-1$ ký hiệu $\Psi(\delta)$ là số các phần tử trong dãy ***(23)*** có số mũ δ theo modulo p. Vì mỗi phần tử của dãy ***(23)*** là nguyên tố cùng nhau với p nên chúng có số mũ δ là ước số của $p-1$. Hệ quả là $\sum_{\delta|p-1}\Psi(\delta)=p-1.$

Từ Định lý 7 ta có $\sum_{\delta|p-1}\varphi(\delta)=p-1$ suy ra

(24) $$\sum_{\delta|p-1}\left(\varphi(\delta)-\Psi(\delta)\right)=0.$$

Ta sẽ chứng minh $\Psi(\delta)\le\varphi(\delta)$ với $\delta\mid p-1$. Rõ ràng điều này đúng với $\Psi(\delta)=0$. Giả sử $\Psi(\delta)>0$, nghĩa là dãy ***(23)*** chứa ít nhất một số a có số mũ δ theo modulo p. Khi đó ta có $a^{\delta}\equiv 1(\mathrm{mod}\, p)$. Hệ quả là a là một trong các nghiệm của đồng dư thức

(25) $$x^{\delta}-1\equiv 0(\mathrm{mod}\, p).$$

Giả sử

(26) $r_1, r_2, \ldots, r_{\delta}$

là các số dư nhận được khi chia các số $a^k\ (k=1,2,\ldots,\delta)$ cho p. Các số ***(26)*** là phân biệt vì nếu ngược lại thì nếu $r_k=r_{k+1}$ với k,l là các số tự nhiên và $k+l\le\delta$ thì $p\mid a^{k+l}-a^k=a^k\left(a^l-1\right)$ suy ra vì $(a,p)=1$ ta có $p\mid a^l-1$, nghĩa là $a^l\equiv 1(\mathrm{mod}\, p)$, vô lý vì a có số mũ δ theo modulo p và l là số tự nhiên nhỏ hơn δ (thật vậy, $k+l\le\delta$ và $k\ge 1$ suy ra $l<\delta$). Theo định nghĩa ***(26)*** với $k=1,2,\ldots,\delta$ thì ta có $r_k\equiv a^k(\mathrm{mod}\, p)$. Vì vậy từ $a^{\delta}\equiv 1(\mathrm{mod}\, p)$ suy ra $r_k^{\delta}\equiv\left(a^{\delta}\right)^k\equiv 1(\mathrm{mod}\, p)$, chứng tỏ ***(26)*** là các nghiệm của đồng dư thức ***(25)***. Đồng dư thức ***(25)*** có bậc δ và thỏa mãn các điều kiện của định lý Lagrange (Định lý 13 mục 8 Chương 5) nên nó không có nghiệm nào ngoài các nghiệm cho bởi ***(26)***.

Mặt khác mọi số x có số mũ δ theo modulo p đều thỏa mãn đồng dư thức ***(25)*** do đó nó là một trong các số ***(26)***. Ta cần tìm r_k có số mũ δ theo modulo p. Ta chứng minh đó là số r_k với $(k,\delta)=1$.

Giả sử $(k,\delta)=1$. Khi đó r_k là nghiệm của đồng dư thức ***(25)*** và có số mũ $\delta'\le\delta$ theo modulo p. Vì vậy $r_k^{\delta'}\equiv 1(\mathrm{mod}\, p)$. Nhưng $r_k\equiv a^k(\mathrm{mod}\, p)$ suy ra $a^{k\delta'}\equiv 1(\mathrm{mod}\, p)$. Ta thấy $k\delta'$ là một trong các nghiệm của đồng dư thức $a^x\equiv 1(\mathrm{mod}\, p)$. Vậy theo Định lý 9 thì $\delta\mid k\delta'$ mà theo giả thiết $(k,\delta)=1$ suy ra $\delta\mid\delta'$ và vì $\delta'\le\delta$ chứng tỏ $\delta'=\delta$. Vậy nếu $(k,\delta)=1$ thì r_k có số mũ δ theo modulo p.

Bây giờ giả sử $(k,\delta)=d>1$. Đặt $k=k_1 d,\ \delta=\delta_1 d$ với $\delta_1<\delta$ thì $k\delta_1=k_1 d\delta_1=k_1\delta$. Hệ quả là $r_k^{\delta_1}\equiv a^{k\delta_1}\equiv a^{k_1\delta}\equiv\left(a^{\delta}\right)^{k_1}\equiv 1(\mathrm{mod}\, p)$. Điều này chứng tỏ $r_k^{\delta_1}\equiv 1(\mathrm{mod}\, p)$ với $\delta_1<\delta$ và do đó số r_k không có số mũ δ theo modulo p.

Vậy ta đã chứng minh $(k,\delta)=1$ là điều kiện cần và đủ để r_k có sỗ mũ δ theo modulo p. Nói cách khác tất cả các số các số r_k trong dãy ***(26)*** mà có số mũ δ theo modulo p là các số mà có chỉ số k nguyên tố cùng nhau với δ. Số các số như vậy là $\varphi(\delta)$. Vì vậy (với ước số tự nhiên cho trước δ của số $p-1$) nếu $\psi(\delta)>0$ thì $\psi(\delta)=\varphi(\delta)$. Từ đây suy ra mọi hạng tử của ***(24)*** là không âm, mà tổng của chúng là bằng 0 nên tất cả các hạng tử đều bằng 0.

Do đó $\psi(\delta)=\varphi(\delta)$ với $\delta\,|\,p-1$.

Ta đã chứng minh được

Định lý 12. *Giả sử p là số nguyên tố và δ là ước số tự nhiên của $p-1$. Khi đó tồn tại đúng $\varphi(\delta)$ số phân biệt trong dãy $1,2,\ldots,p-1$ mà có số mũ δ theo modulo p.*

Trong trường hợp riêng quan trọng $\delta=p-1$ ta có

Hệ quả. *Mọi số nguyên tố p có đúng $\varphi(p-1)$ căn nguyên thủy trong dãy $1,2,\ldots,p-1$.*

Từ chứng minh của định lý suy ra nếu g là căn nguyên thủy của số nguyên tố p thì tất cả các căn nguyên thủy của p thuộc dãy ***(23)*** có thể tìm được trong các số dư nhận được khi chia các số trong dãy $g,g^2,g^3,\ldots,g^{p-1}$ với số mũ nguyên tố cùng nhau với $p-1$ cho p.

Ký hiệu $\gamma(p)$ là căn nguyên thủy nhỏ nhất của số nguyên tố p. Bảng dưới đây cho các giá trị của hàm $\gamma(p)$ với các số nguyên tố lẻ $p<100$

p	3	5	7	11	13	17	19	23	29	31	37	41
$\gamma(p)$	2	2	3	2	2	3	2	5	2	3	2	6

p	43	47	53	59	61	67	71	73	79	83	89	97
$\gamma(p)$	3	5	2	2	2	2	7	5	3	2	3	5

Ta chứng minh được $\overline{\lim}\,\gamma(p)=\infty$ (Pillai [7]) và hơn nữa với vô hạn số $p,\gamma(p)>c\log p$ (Turan [1]). Mặt khác, ta chưa biết có tồn tại vô hạn các số nguyên tố mà 2 là căn nguyên thủy của nó hay không. E.Artin đã đặt ra giả thuyết nói rằng mọi số nguyên $g\neq -1$ không là bình phương đều là căn nguyên thủy của vô hạn số nguyên tố (Hasse [1] trang 68). Kết quả này có thể suy ra từ giả thuyết H (Schinzel và Sierpinski [3] trang 199-201).

Bảng ở trên cho thấy $\gamma(p)\le 7$ với mọi số nguyên tố $p<100$. Với $p<191$ ta cũng có $\gamma(p)<7$. Nhưng $\gamma(191)=19$. Nếu $p<409$ thi $\gamma(p)\le 19$ nhưng $\gamma(409)=21$. Với các số nguyên tố $p<3361$ ta có $\gamma(p)\le 21$ nhưng $\gamma(3361)=22$. Với $p<5711$ ta có $\gamma(p)\le 22$ nhưng $\gamma(5711)=29$. Nếu p là số nguyên tố <5881 thì $\gamma(p)\le 29$ nhưng $\gamma(5881)=31$ (Wertheim [1] trang 406-409).

Nếu g là căn nguyên thủy của số nguyên tố p thì các số $g^0, g^1, g^2, \ldots, g^{p-1}$ chia cho p cho các số dư phân biệt và mỗi số đều khác 0. Hệ quả là số các số dư như vậy bằng với số các số $g^0, g^1, g^2, \ldots, g^{p-1}$, nghĩa là bằng $p-1$. Do đó với mọi số $x = g^0, g^1, \ldots, g^{p-1}$ thì tồn tại y trong dãy $0,1,2,\ldots,p-2$ mà $g^y \equiv x \pmod p$.

Ta tìm tất cả các số tự nhiên $m>1$ có căn nguyên thủy. Ta có định lý: *số tự nhiên $m>1$ có căn nguyên thủy khi và chỉ khi nó là một trong các số $2, 4, p^\alpha, 2p^\alpha$ với p là số nguyên tố lẻ và α là số tự nhiên.*

Số các căn nguyên thủy của m có dạng này là $\varphi(\varphi(m))$ (Sierpinski [12] trang 193).

Litver và Yudina [1] đã kiểm tra với mọi số nguyên tố $p \le 10^6$ ngoại trừ $p = 40487$ thì $\gamma(p)$ là căn nguyên thủy của p^α với mọi α.

Từ định lý về sự tồn tại của các căn nguyên thủy của các số nguyên tố lẻ ta tìm tất cả các số tự nhiên m mà từ $a \equiv b \pmod m$ và $c \equiv d \pmod m$ suy ra $a^c \equiv b^d \pmod m$ với mọi a,b,c,d nguyên dương.

Để đơn giản ta gọi các tính chất ở trên là tính chất P. Giả sử số tự nhiên m có tính chất P. Ký hiệu a là số tự nhiên cho trước. Do $m \mid a-a$ và $m \mid (m+1)-1$ ta có $m \mid a^{m+1}-a$, nghĩa là $m \mid a(a^m-1)$. Mặt khác giả sử m là số mà với mọi số nguyên a ta có $m \mid a(a^m-1)$. Lấy a,b,c,d là các số nguyên thỏa mãn $m \mid a-b$ và $m \mid c-d$. Nếu $c=d$ thì vì $m \mid a-b$ ta có $m \mid a^c - b^d$. Giả sử $c \ne d$. Đổi vai trò (nếu cần thiết) của c và d, ta giả sử $c>d$. Khi đó vì $m \mid c-d$, $c = d+mk$ với k là số tự nhiên thì ta có $a \mid a^d$ và $a^m - 1 \mid a^{mk}-1$. Hơn nữa, vì $m \mid a(m^a-1)$ suy ra $m \mid a^d(a^{mk}-1) = a^c - a^d$. Nhưng vì $m \mid a-b$ nên ta có $m \mid a^d - b^d$ mà theo công thức $m \mid a^c - a^d$ suy ra $m \mid a^c - b^d$. Ta thấy số m có tính chất P. Vậy điều kiện cần và điều kiện đủ để một số m có tính chất P là với mọi số nguyên $a, m \mid a(a^m-1)$.

Bây giờ ta tìm tất cả các số m có tính chất P. Hiển nhiên 1 và 2 đều có tính chất P. Giả sử m là số tự nhiên >2. Nếu m chia hết cho bình phương số nguyên tố p thì với $a=p$ ta có $p^2 \mid p(p^m-1)$, vô lý vì $(p, p^m-1)=1$. Hệ quả là m phải là tích của các nhân tử là các số nguyên tố phân biệt mà tất cả đều lớn hơn 2. Tích này chứa số nguyên tố lẻ p. Ký hiệu g là căn nguyên thủy của số nguyên tố p. Vì $p \mid m \mid g(g^m-1)$ và $(p,g)=1$ suy ra $p \mid g^m-1$. Nhưng do g có số mũ $p-1$ theo modulo p nên ta có $p-1 \mid m$. Do đó m chẵn và là tích của ít nhất hai số nguyên tố phân biệt là 2 và p. Nếu m là tích của đúng hai số nguyên tố thì $m=2p$. Vì $p-1 \mid m$ và $(p-1,p)=1$ ta có $p-1 \mid 2$ nên vì $p \ge 3$ (p là số nguyên tố lẻ) ta suy ra $p=3$ và do đó $m = 2 \cdot 3 = 6$. Số 6 có tính chất P bởi vì với mọi số nguyên a ta có $6 \mid (a-1)a(a+1) = a(a^2-1)$ và $a^2-1 \mid a^6-1$ suy ra $6 \mid a(a^6-1)$.

Bây giờ giả sử m là tích của ba số nguyên tố phân biệt, nghĩa là $m = 2p_1p_2$ với $2 < p_1 < p_2$. Ta đã biết $p_1 - 1 \mid m$ suy ra $p_1 - 1 \mid 2p_1p_2$. Nhưng $p_1 - 1 > 1$ (vì $p_1 > 2$) và $p_1 - 1 < p_1 < p_2$. Số nguyên tố p_2 không chia hết cho $p_1 - 1$ do đó $p_1 - 1 \mid 2p_1$ suy ra tương tự trường hợp trên ta có $p_1 = 3$ và do đó $m = 6p_2$. Do $p_2 - 1 \mid m = 6p_2$ và $(p_2-1, p_2) = 1$ suy ra $p_2 - 1 \mid 6$ mà $p_2 > p_1$, nghĩa là $p_2 > 3$ và do đó $p_2 - 1 > 2$ suy ra $p_2 - 1 = 3$ hoặc $p_2 - 1 = 6$. Nhưng $p_2 - 1 = 3$ là không thể xảy ra vì p_2 là số nguyên tố do đó ta phải có $p_2 - 1 = 6$. Suy ra $p_2 = 7$ và do đó $m = 2 \cdot 3 \cdot 7 = 42$. Có thể kiểm tra trực tiếp số 42 có tính chất

P. Thật vậy, $6 \mid a\left(a^6-1\right)$ với mọi số nguyên a suy ra $6 \mid a\left(a^{42}-1\right)$. Nếu a không chia hết cho 7 thì theo định lý Fermat nhỏ ta có $7 \mid a^6-1$ và lại suy ra $7 \mid a\left(a^{42}-1\right)$. Vì vậy với mọi số nguyên a thì từ $6 \mid a\left(a^{42}-1\right)$ và $7 \mid a\left(a^{42}-1\right)$ và lưu ý $(6,7)=1$ suy ra $42 \mid a\left(a^{42}-1\right)$ suy ra 42 có tính chất P.

Hơn nữa giả sử m là tích của bốn số nguyên tố. Tức là $m=2 p_1 p_2 p_3$ với $2<p_1<p_2<p_3$. Khi đó ta có $p_1-1 \mid 2$ suy ra $p_1=3$, tương tự $p_2-1 \mid 2 p_1=6$ suy ra $p_2=7$ và $p_3-1 \mid 2 p_1 p_2=42$. Do đó vì $p_3>p_2=7$ ta có $p_3-1=7,14,21$ hoặc 42 mà vì p_3 nguyên tố suy ra $p_3-1=42$, nghĩa là $p_3=43$ suy ra $m=1806$. Dễ thấy số 1806 có tính chất P vì ta đã chứng minh $42 \mid a\left(a^{42}-1\right)$ với mọi số nguyên a nên suy ra $42 \mid a\left(a^{1806}-1\right)$. Nếu a chia hết cho 43 thì ta có $43 \mid a\left(a^{1806}-1\right)$. Nếu a không chia hết cho 43 thì tính chất trên là hệ quả của định lý Fermat nhỏ vì $43 \mid a^{42}-1$ suy ra $43 \mid a^{1806}-1$. Do $42 \mid a\left(a^{1806}-1\right)$ và $43 \mid a\left(a^{1806}-1\right)$ đúng với mọi số nguyên a và lưu ý $(42,43)=1$ và $1806=42 \cdot 43$ suy ra $1806 \mid a\left(a^{1806}-1\right)$. Vậy 1806 có tính chất P.

Cuối cùng giả sử m là tích của nhiều hơn bốn số nguyên tố. Khí đó $m=2 p_1 p_2 \ldots p_k$ với $k \geq 4,2<p_1<p_2<\ldots<p_k$. Ở trên ta đã thấy $p_1=3, p_2=7, p_3=43$. Hơn nữa $p_4-1 \mid m$ suy ra $p_4-1 \mid 2 p_1 p_2 p_3$, nghĩa là $p_4-1 \mid 1806$. Mặt khác $p_4-1>p_3-1=42$ và hơn nữa p_4-1 chẵn. Các ước số của số $1806=2 \cdot 3 \cdot 7 \cdot 43$ không lớn hơn 42 là các số 86, 258, 602, 1806. Do đó p_4 phải là một trong các số 87,259,603 hoặc 1807 nhưng các số này đều không phải số nguyên tố vì ta có $87=3 \cdot 29,\ 259=7 \cdot 37,\ 603=3^2 \cdot 67,\ 1807=13 \cdot 139$. Vì vậy giả thiết m là tích của nhiều hơn bốn số nguyên tố dẫn tới mâu thuẫn.

Vậy ta đã chứng minh được định lý J.Dyer Bennet [1] nói rằng các số 1,2,6,42,1806 là tất cả các số có tính chất P. Do đó chúng là tất cả các modulo m mà các đồng dư thức $a \equiv b(\bmod m)$ và $c \equiv d(\bmod m)$ suy ra $a^c=b^d(\bmod m)$ với mọi số nguyên dương a, b, c, d.

Dễ thấy các số m có tính chất P là những số không có ước số chính phương mà $\lambda(m) \mid m$ với $\lambda(m)$ là lũy thừa phổ quát nhỏ nhất theo modulo m (mục 4).

Bài tập. Chứng minh rằng 2 không phải căn nguyên thủy của mọi số nguyên tố có dạng $2^{2^n}+1$ với n là số tự nhiên >1.

Chứng minh. Nếu p là số nguyên tố và $p=2^{2^n}+1$ thì $2^{2^{n+1}} \equiv 1(\bmod p)$. Nhưng $p-1=2^{2^n}>2^{n+1}$ với $n>1$ vì dễ dàng chứng minh bằng quy nạp $2^n>n+1$ với $n=2,3,\ldots$ Do đó 2 có số mũ $<p-1$ theo modulo p và không phải căn nguyên thủy của p. □

7. Thặng dư bậc n của một số nguyên tố theo modulo p

Nếu p là số nguyên tố, n là số tự nhiên >1 thì số nguyên a được gọi là thặng dư bậc n theo modulo p nếu tồn tại số nguyên x thỏa mãn $x^n \equiv a(\bmod p)$.

Rõ ràng số 0 là thặng dư bậc n với mọi modulo p nguyên tố và n là số nguyên tùy ý.

Do đó ta giả thiết các thặng dư bậc n ở đây đều khác 0.

Từ quan điểm lý thuyết thì tồn tại phương pháp quyết định xem một số tự nhiên $a \neq 0$ có là thặng dư bậc n theo modulo p hay không. Thật vậy, chỉ cần kiểm tra xem có tồn tại số x trong dãy $1,2,\ldots,p-1$ mà thỏa mãn $x^n \equiv a \pmod p$ hay không.

Trong mối liên hệ này ta có

Định lý 13 (Euler). *Số nguyên a không chia hết cho số nguyên tố p là thặng dư bậc n theo modulo p nguyên tố khi và chỉ khi*

(27) $$a^{(p-1)/d} \equiv 1 \pmod p \textbf{ với } d = (p-1, n)$$

Chứng minh. Giả sử số nguyên a không chia hết cho số nguyên tố p và là thặng dư bậc n theo modulo p. Khi đó tồn tại số nguyên x không chia hết cho p thỏa mãn $a \equiv x^n \pmod p$. Vì vậy

(28) $$a^{(p-1)/d} = \left(x^n\right)^{(p-1)/d} \equiv \left(x^{p-1}\right)^{n/d}.$$

Vì $d \mid n$ và theo định lý Fermat nhỏ $x^{p-1} \equiv 1 \pmod p$, từ ***(28)*** suy ra ***(27)***. Điều kiện cần được chứng minh. Bây giờ giả sử công thức ***(27)*** đúng. Ký hiệu g là căn nguyên thủy của p. Trong mục 6 ta đã biết tồn tại số nguyên h mà $0 \le h \le p-2$ và $a \equiv g^h \pmod p$, theo ***(27)*** suy ra $g^{h(p-1)/d} \equiv 1 \pmod p$.

Vì g là căn nguyên thủy của số nguyên tố p, từ tính chất cuối cùng ở trên suy ra $p-1 \mid \dfrac{h(p-1)}{d}$ nên $d \mid h$ và do đó $h = kd$ với k là số nguyên không âm.

Theo định nghĩa thì $d = (p-1, n)$ và theo Định lý 16 Chương 1 suy ra tồn tại hai số tự nhiên u, v thỏa mãn $d = nu - (p-1)v$ suy ra $kd = knu - k(p-1)v$. Theo định lý Fermat nhỏ thì $g^{k(p-1)v} \equiv 1 \pmod p$. Vì vậy sử dụng $a \equiv g^h \equiv g^{kd \pmod p}$ ta tìm được $a \equiv a g^{k(p-1)v} \equiv g^{kd + k(p-1)v} \equiv g^{knu} \equiv \left(g^{ku}\right)^n \pmod p$ chứng tỏ a là thặng dư bậc n theo modulo p. Điều kiện đủ được chứng minh. □

Nếu a là thặng dư bậc n theo modulo p thì rõ ràng mọi số đồng dư với $a \pmod p$ cũng là thặng dư bậc n theo modulo p. Do đó thặng dư bậc n theo modulo p có thể được hiểu là lớp các số đồng dư với một thặng dư bậc n theo modulo p.

Định lý 14. *Nếu p là số nguyên tố, n là số tự nhiên và $d = (n, p-1)$ thì số các thặng dư bậc n phân biệt theo modulo p (tính cả 0) là $(p-1)/d + 1$.*

Chứng minh. Ký hiệu g là căn nguyên thủy của p. Ký hiệu $d = (p-1, n)$, $n = dm, p-1 = ds$ với m, s là các số tự nhiên và $(m, s) = 1$. Ký hiệu k, l là hai số trong dãy $1, 2, \ldots, s$ mà $k > l$. Nếu $g^{kn} \equiv g^{\ln} \pmod p$ thì $p \mid g^{kn} - g^{\ln} = g^{\ln}\left(g^{(k-l)n} - 1\right)$ do đó $(p, g) = 1, g^{(k-l)n} \equiv 1 \pmod p$. Vì vậy do g là căn nguyên thủy của số nguyên tố p nên $p-1 \mid (k-l)n$ mà $n = dm,\ p-1 = ds$ suy ra $s \mid (k-l)m$ do đó vì $(m, s) = 1,\ s \mid k-l$, vô lý vì k và l là hai số phân biệt trong dãy $1, 2, \ldots, s$. Vậy ta suy ra các số $g^n, g^{2n}, \ldots, g^{sn}$ có các số dư khác nhau khi chia cho p. Hơn nữa các số đó đều là thặng dư bậc n theo modulo p (vì đồng dư thức $x^n \equiv g^{kn} \pmod p$ có nghiệm $x = g^k$). Do đó tồn tại ít nhất s thặng dư bậc n phân biệt theo modulo p. Các thặng dư này đều khác 0.

Bây giờ ký hiệu a là thặng dư bậc n tùy ý theo modulo p và khác 0. Khi đó tồn tại số nguyên x (không chia hết cho p) thỏa mãn $x^n \equiv a \pmod p$. Ta đã biết trong dãy $0,1,...,p-2$ tồn tại số y mà $x \equiv g^y \pmod p$ suy ra $a \equiv g^{ny} \pmod p$. Ký hiệu r là số dư nhận được khi chia y cho x. Ta có $y = ks + r$ với k là số nguyên không âm và $0 \le r < s$. Vì vậy $ny = nks + nr$. Nhưng vì $n = dm,\ p-1 = ds$ nên $ns = (p-1)m$. Hệ quả là $ny = k(p-1)m + nr$ suy ra $a \equiv g^{ny} \equiv g^{nr} \pmod p$ và chứng tỏ không có thặng dư bậc n theo modulo p khác 0 nào ngoài các thặng dư $1, g^n, g^{2n}, ... g^{(s-1)n}$. Từ $sn = (p-1)m$, thặng dư 1 có thể thay bởi g^{sn}. Vậy ta đã chứng minh với số nguyên tố p cho trước thì tồn tại đúng $\dfrac{p-1}{(n, p-1)} + 1$ thặng dư bậc n phân biệt theo modulo p. □

Hệ quả trực tiếp của Định lý 14 là với số tự nhiên cho trước n thì mọi số nguyên đều là thặng dư bậc n theo modulo nguyên tố p cho trước khi và chỉ khi n nguyên tố cùng nhau với $p-1$.

Theo đó khi $n = 3$ thì mọi số nguyên đều là thặng dư bậc ba theo modulo p nguyên tố khi và chỉ khi p không có dạng $3k+1$ với k là số tự nhiên, nghĩa là p là 2,3 hoặc có dạng $3k+2$ với k tự nhiên.

Dễ dàng chứng minh rằng tồn tại vô hạn số nguyên tố có dạng $3k+2$.

Thật vậy, ký hiệu n là số tự nhiên tùy ý và đặt $N = 6n!-1$. Rõ ràng N là số tự nhiên >1. Dễ thấy mọi ước số của N đều có dạng $6k+1$ hoặc $6k-1$. Không phải tất cả các ước số của N đều có dạng $6k+1$ vì nếu như vậy thì tích của chúng cũng có dạng như vậy, điều này không đúng vì N không có dạng đó. Hệ quả là N có ít nhất một ước số nguyên tố $p = 6k-1$ với k là số tự nhiên. Do $p \mid N = 6n!-1$ suy ra $p > n$. Vì vậy do n tùy ý nên tồn tại số nguyên tố lớn tùy ý có dạng $6k-1 = 3(2(k-1)+1)+2$. Điều phải chứng minh.

Có thể chứng minh rằng nếu n là số nguyên tố và m là số tự nhiên >1 thì mọi số nguyên đều là thặng dư bậc n theo modulo m khi và chỉ khi m là tích của các số nguyên tố phân biệt mà không có số nào có dạng $nk+1$ (với k là số tự nhiên) (Sierpinski [9]).

Bài tập. Chứng minh rằng nếu p là số nguyên tố, n là số tự nhiên và $d = (p-1, n)$ thì thặng dư bậc n theo modulo p nguyên tố trùng với thặng dư bậc d theo modulo p.

Chứng minh. Vì $d = (p-1, n)$ nên ta có $d \mid p-1$ và do đó $d = (p-1, d)$ và theo Định lý 13 thì điều kiện cần và đủ để một số nguyên a không chia hết cho p là thặng dư bậc n theo modulo p là trùng với điều kiện để a là thặng dư bậc d theo modulo p. Do đó tập hợp các thặng dư bậc n và thặng dư bậc d là trùng nhau.

Đặc biệt, nếu p là số nguyên tố có dạng $4k+3$ với $k = 0,1,2,...,$ thì (vì $2 = (p-1, 4)$) các thặng dư bậc hai theo modulo p trùng với các thặng dư bậc bốn theo modulo p. □

8. Các tính chất và ứng dụng của hàm chỉ số

Trong mục 4 ta đã định nghĩa căn nguyên thủy của số tự nhiên m là số nguyên g có số mũ $\varphi(m)$ theo modulo m. Từ đó suy ra các số $g^0, g^1, ..., g^{\varphi(m)-1}$ là không đồng dư $\pmod m$. Vì số các số trong dãy này là $\varphi(m)$ tức là đúng bằng với số các số nguyên tố cùng nhau với m trong dãy $1,2,...,m,$ nên với mọi số nguyên x nguyên tố cùng nhau với m thì tồn tại đúng một số y trong dãy

$0,1,2,\ldots,\varphi(m)-1$ mà $g^y \equiv x \pmod m$. Ta nói y là chỉ số của x theo căn nguyên thủy g và ký hiệu là $ind_\theta x$, hoặc nếu không có gì gây nhầm lẫn thì ký hiệu đơn giản là $\text{ind}\, x$. Ta gọi g là cơ sở của chỉ số.

Cố định số tự nhiên $m>1$ có căn nguyên thủy g và xét hàm chỉ số $\text{ind}\, x$ với số nguyên x nguyên tố cùng nhau với m. Ta chứng minh các tính chất sau đây của hàm chỉ số

I. *Chỉ số của các số nguyên đồng dư* $\pmod m$ *và nguyên tố cùng nhau với* m *là bằng nhau.*

Thật vậy, nếu $a \equiv b \pmod m$ và $g^{inda} \equiv a \pmod m$ thì $g^{inda} \equiv b \pmod m$. Nhưng vì $(b,m)=1$ nên đồng dư thức $g^x \equiv b \pmod m$ có đúng một nghiệm trong các số $0,1,\ldots,\varphi(m)-1$ và đó là $ind\, b$ suy ra $ind\, a = ind\, b$. Vì vậy trong bảng các giá trị của $ind\, x$ chỉ xuất hiện các số x nhỏ hơn modulo và nguyên tố cùng nhau với modulo.

II. *Chỉ số của tích là đồng dư* $\pmod{\varphi(m)}$ *với tổng các chỉ số của các nhân tử, nghĩa là*

(29) $$ind\,(ab) \equiv ind\, a + ind\, b \pmod{\varphi(m)}.$$

Thật vậy, theo định nghĩa của chỉ số ta có $g^{ind\, a} \equiv a \pmod m$, $g^{ind\, b} \equiv b \pmod m$ với các số a và b nguyên tố cùng nhau với m. Vì vậy nhân hai đồng dư thức cuối cùng ta nhận được $g^{ind\, a + ind\, b} \equiv ab \pmod m$. Nhưng vì $g^{ind(ab)} \equiv ab \pmod m$ ta suy ra

(30) $$g^{ind\{ab)} \equiv g^{ind\, a + ind\, b} \pmod m.$$

Giả sử với mọi số nguyên không âm μ, v thì đồng dư thức $g^\mu \equiv g^v \pmod m$ đúng. Nếu $\mu \geq v$ thì $m \mid g^v\left(g^{\mu - v} - 1\right)$ mà $(g,m)=1$ suy ra $g^{\mu - v} = 1 \pmod m$. Số g là căn nguyên thủy của m có số mũ $\varphi(m)$ theo modulo m. Vì vậy theo Định lý 9 suy ra $\varphi(m) \mid \mu - v$.

Tính chất cuối cùng cũng đúng với $\mu \leq v$. Vì vậy từ ***(30)*** ta có đồng dư thức ***(29)***.

Tính chất này được mở rộng cho hữu hạn nhân tử. Vì vậy

III. *Chỉ số của lũy thừa bậc* n *(*n *là số tự nhiên) là đồng dư* $\pmod{\varphi(m)}$ *với tích của* n *với chỉ số của cơ sở. Ta có* $ind\ a^n \equiv n\ ind\ a \pmod{\varphi(m)}$.

Bây giờ ta trình bày quan hệ giữa các chỉ số lấy với các căn nguyên thủy khác nhau của một số cố định m. Theo định nghĩa của chỉ số ta có $a \equiv g^{ind_g a} \pmod m$. Vì vậy sử dụng các tính chất ***I*** và ***II*** ta có

$$ind_\gamma a \equiv ind_g a \cdot ind_\gamma g \pmod{\varphi(m)}$$

với γ là căn nguyên thủy của m. Do đó để đổi cơ sở của chỉ số thì ta chỉ cần nhân mỗi số với một số cố định (gọi là chỉ số của chỉ số cũ đối với cơ sở mới) và tính đồng dư theo modulo $\varphi(m)$ của tích.

Định lý 15. *Để một số a không chia hết cho* p *là thặng dư bậc hai của một số nguyên tố lẻ* p *thì điều kiện cần và đủ là* $ind\ a$ *chẵn.*

Chứng minh. Giả sử $ind_g a = 2k$ với k là số nguyên không âm. Ta có $g^{2k} \equiv a \pmod p$ chứng tỏ đồng dư thức $x^2 \equiv a \pmod p$ có nghiệm $x = g^k$. Do đó a là thặng dư bậc hai modulo p.

Trong dãy $1,2,\ldots,p-1$ có $\frac{1}{2}(p-1)$ số có chỉ số chẵn vì các chỉ số của các số trong dãy trùng với các số $0,1,2,\ldots,p-2$ (sai khác một thứ tự) mà trong đó có đúng $\frac{1}{2}(p-1)$ số chẵn. Các số đó đều là thặng dư bậc hai của p. Nhưng theo Định lý 14 với $d=(2,p-1)=2$ thì chỉ có $\frac{1}{2}(p-1)$ thặng dư bậc hai trong dãy $1,2,\ldots,p-1$. Vậy không có số nào có chỉ số lẻ mà là thặng dư bậc hai theo modulo p nguyên tố. Định lý được chứng minh. □

Hệ quả trực tiếp của Định lý 15 là không tồn tại căn nguyên thủy của số nguyên tố lẻ p lại là thặng dư bậc hai của p.

Ta lưu ý rằng mệnh đề tương tự với thặng dư bậc n với n lớn hơn 2 là không đúng. Chẳng hạn, trong các chỉ số theo modulo 5 thì có hai số là 0 và 3 là chia hết cho 3 và các số 1,2,3,4 đều là thặng dư bậc ba modulo 5 vì $1\equiv 1^3 \pmod 5, 2\equiv 3^3 \pmod 5, 3\equiv 2^3 \pmod 5, 4\equiv 4^3 \pmod 5$. Với modulo 7 thì các số $1\equiv 1^4 \pmod 7, 2\equiv 2^4 \pmod 7, 4\equiv 3^4 \pmod 7$ là thặng dư bậc bốn với chỉ số theo modulo 7 lại là 0 hoặc 4 đều chia hết cho 4.

Các chỉ số được sử dụng để giải các đồng dư thức.

Xét số nguyên tố p và các số a, b không chia hết cho p. Xét đồng dư thức $ax\equiv b \pmod p$.

Từ các tính chất ***I*** và ***II*** ta có $ind\ a+ind\ x\equiv ind\ b \pmod{p-1}$ suy ra $ind\ x\equiv ind\ b-ind\ a \pmod{p-1}$.

Số $ind\ x$ là số dư nhận được khi chia hiệu $ind\ b-ind\ a$ cho $p-1$. Vì vậy khi biết giá trị $ind\ x$ ta tính x theo $x\equiv g^{ind\ x} \pmod p$. Trong thực hành phương pháp này yêu cầu sử dụng bảng các chỉ số.

Đặt a là số nguyên không chia hết cho p và n là lũy thừa tự nhiên. Xét đồng dư thức $x^n\equiv a \pmod p$.

Theo ***I*** và ***III*** thì đồng dư thức này tương đương với $n\ ind\ x\equiv ind\ a \pmod{p-1}$ vì vậy bài toán giải đồng dư thức được quy về bài toán giải đồng dư thức tuyến tính.

Xét đồng dư thức $a^x\equiv b \pmod p$ với a, b là các số nguyên không chia hết cho số nguyên tố p. Khi đó đồng dư thức này tương đương với đồng dư thức tuyến tính $x\ ind\ a\equiv ind\ b \pmod{p-1}$.

Ví dụ. Ta trình bày bảng các chỉ số $\pmod{13}$. Đầu tiên ta tính các căn nguyên thủy của 13. Ta bắt đầu với số 2. Ta tính thặng dư $\pmod{13}$ của các lũy thừa liên tiếp của 2. Rõ ràng chỉ cần tính 2^n với số mũ tự nhiên n. Nếu r_k là số dư nhận được khi chia 2^k cho 13 thì số dư nhận được khi chia 2^{k+1} cho 13 là $2r_k$. Theo cách này ta tìm được $2\equiv 2$, $2^2\equiv 4$, $2^3\equiv 8$, $2^4\equiv 3$, $2^5\equiv 6$, $2^6\equiv 12$, $2^7\equiv 11$, $2^8\equiv 9$, $2^9\equiv 5$, $2^{10}\equiv 10$, $2^{11}\equiv 7$, $2^{12}\equiv 1 \pmod{13}$. Vậy 2 là căn nguyên thủy của 13. Ta có bảng các số x tương ứng với chỉ số của nó là $ind_2\ x=k$ (với $k=0,1,\ldots,11$) như sau

$\text{ind}_2\ x$	0	1	2	3	4	5	6	7	8	9	10	11
x	1	2	4	8	3	6	12	11	9	5	10	7

Sử dụng bảng này ta có bảng các chỉ số ứng với $x=1,2,\ldots,12$ như sau

x	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_2\, x$	0	1	4	2	9	5	11	3	8	10	7	6

Với $6x \equiv 5 \pmod{13}$ ta có $ind\ 6 + ind\ x \equiv ind\ 5 \pmod{12}$ suy ra $ind\ x \equiv ind\ 5 - ind\ 6 \pmod{12}$. Kiểm tra trong bảng thứ hai ta có $ind\ 5 = 9$ và $ind\ 6 = 5$ vì vậy $x \equiv 9 - 5 \equiv 4 \pmod{12}$ và do đó $ind\ x = 4$ và sử dụng bảng thứ nhất suy ra $x = 3$.

Xét đồng dư thức $x^8 \equiv 3 \pmod{13}$. Ta có $8\ ind\ x \equiv ind\ 3 \pmod{12}$. Mặt khác, sử dụng các bảng ở trên ta có $ind\ 3 = 4$ suy ra nếu đặt $ind\ x = y$ thì ta nhận được đồng dư thức $8y \equiv 4 \pmod{12}$. Đồng dư thức này tương đương với $12 | 8y - 4$ do đó $3 | 2y - 1$, nghĩa là $2y \equiv 1 \pmod{3}$. Vì vậy $4y \equiv 2 \pmod{3}$. Nhưng vì $4 \equiv 1 \pmod{3}$, $y \equiv 2 \pmod{3}$ và do đó $y = 2 + 3k$ với k là số nguyên. Các số có dạng này mà thuộc dãy $0,1,2,\ldots,11$ là các số 2,5,8 và 11. Hệ quả là chúng là các giá trị của $y = ind\ x$. Sử dụng bảng thứ nhất ta tính được x bằng 4,6,9 và 7. Vì vậy đồng dư thức ban đầu có đúng bốn nghiệm là 4,6,7,9.

Cuối cùng xét đồng dư thức $6^x \equiv 7 \pmod{13}$. Ta có $x\ ind\ 6 \equiv ind\ 7 \pmod{12}$. Kiểm tra trong bảng thứ hai ta có $ind\ 6 = 5$, $ind\ 7 = 11$. Vì vậy đồng dư thức trở thành $5x \equiv 11 \pmod{12}$, điều này chỉ đúng với $x = 7$ với các số x thuộc dãy 0,1,...,11. Vậy đồng dư thức ban đầu có nghiệm $7 + 12k$ với $k = 0,1,2,\ldots$.

Bài tập. ***1.*** Chứng minh rằng với mọi số nguyên tố lẻ p nguyên tố với mọi căn nguyên thủy của p thì

$$ind\,(-1) = ind\,(p-1) = \frac{1}{2}(p-1)$$

Chứng minh. Theo định lý Fermat nhỏ thì với mọi căn nguyên thủy g của số nguyên tố lẻ p thì $p \mid g^{p-1} - 1 = \left(g^{\frac{1}{2}(p-1)} - 1\right)\left(g^{\frac{1}{2}(p-1)} + 1\right)$. Nhưng vì $p \mid g^{\frac{1}{2}(p-1)} - 1$ là không thể vì g là căn nguyên thủy của p nên $p \mid g^{\frac{1}{2}(p-1)} + 1$, nghĩa là $g^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$ chứng tỏ $ind\,(-1) = \frac{1}{2}(p-1)$. □

2. Chứng minh rằng điều kiện cần và đủ để số nguyên g nguyên tố cùng nhau với số nguyên tố lẻ p là căn nguyên thủy của p là $g^{(p-1)/q} \not\equiv 1 \pmod{p}$ với mọi ước số nguyên tố q của $p-1$.

Chứng minh. Nếu với số nguyên tố q mà $q \mid p-1$ và $g^{(p-1)/q} = 1 \pmod{p}$ thì q có số mũ $\le (p-1)/q < p-1$ và do đó g không phải căn nguyên thủy của p. Điều kiện cần được chứng minh.

Mặt khác, giả sử số nguyên g nguyên tố cùng nhau với p không phải căn nguyên thủy của p. Khi đó lũy thừa δ của g theo modulo p là $< p-1$. Do δ là ước số của $p = 1$ nên $(p-1)/\delta$ là số tự nhiên > 1 và do đó nó có ước số nguyên tố q. Vậy ta có $q \mid (p-1)/\delta$ suy ra $\delta \mid (p-1)/q$ và vì $p \mid g^{\delta} - 1$ (g có số mũ δ theo modulo p) nên $p \mid g^{(p-1)/q} - 1$, nghĩa là $g^{(p-1)/q} = 1 \pmod{p}$.

Điều kiện đủ được chứng minh. □

CHƯƠNG 7

BIỂU DIỄN HỆ CƠ SỐ TÙY Ý

1. Biểu diễn của số tự nhiên trong cơ số tùy ý

Xét g là số tự nhiên >1. Biểu diễn cơ số g của số tự nhiên N được cho bởi công thức

(1) $$N = c_m g^m + c_{m-1} g^{m-1} + \ldots + c_1 g + c_0$$

Trong đó m là số nguyên ≥ 0 và $c_n \left(n = 0,1,2,\ldots,m\right)$ là các số nguyên thỏa mãn tính chất

(2) $$0 \leq c_n \leq g-1 \quad \text{với} \quad n = 0,1,\ldots,m \quad \text{và} \quad c_m \neq 0.$$

Mỗi số thuộc dãy

(3) $$0,1,2,\ldots,g-1$$

được gọi là các chữ số và công thức ***(1)*** có thể viết thành $N = \left(\gamma_m \gamma_{m-1} \ldots \gamma_1 \gamma_0\right)_g$, với γ_n là chữ số ký hiệu cho c_n. Nếu $g \leq 10$ các số 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 được dùng làm ký hiệu cho các chữ số trong ***(3)***. Ví dụ

$$N = \left(10010\right)_2 \text{ nghĩa là } N = 1\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2 + 0 = 18,$$
$$N = \left(5603\right)_7 \text{ nghĩa là } N = 5\cdot 7^3 + 6\cdot 7^2 + 0\cdot 7 + 3 = 2012.$$

Định lý 1. *Mọi số tự nhiên đều được biểu diễn duy nhất trong cơ số g (g là số tự nhiên >1) nghĩa là có thể biểu diễn dưới dạng **(1)** trong đó các số nguyên $c_n \left(n = 0,1,\ldots,m\right)$ thỏa mãn các bất đẳng thức **(2)**.*

Chứng minh. Giả sử số tự nhiên N có thể biểu diễn như trong ***(1)*** với $c_n \left(n = 0,1,\ldots m\right)$ nguyên thỏa mãn ***(2)***. Ký hiệu n là một trong các số $0,1,2,\ldots,m-1$. Từ ***(1)*** ta có

(4) $$\frac{N}{g^n} = c_m g^{m-n} + c_{m-1} g^{m-n-1} + \ldots + c_n + \frac{c_{n-1}}{g} + \frac{c_{n-2}}{g^2} + \ldots + \frac{c_0}{g^n}.$$

Nhưng theo ***(2)*** thì $0 \leq \frac{c_{n-1}}{g} + \frac{c_{n-2}}{g^2} + \ldots + \frac{c_0}{g^n} \leq \frac{g-1}{g} + \frac{g-1}{g^2} + \ldots + \frac{g-1}{g^n} = 1 - \frac{1}{g^n}$. Vì vậy từ ***(4)*** ta suy ra $\left[\frac{N}{g^n} =\right] = c_m g^{m-n} + c_{m-1} g^{m-n-1} + c_{n+1} g + c_n$ và tương tự $\left[\frac{N}{g^{n+1}}\right] = c_m g^{m-n-1} + c_{m-1} g^{m-n-2} + \ldots + c_{n+1}$. Các công thức này suy ra

(5) $$c_n = \left[\frac{N}{g^n}\right] - g\left[\frac{N}{g^{n+1}}\right] \text{ với mọi } n = 0,1,\ldots,m.$$

Từ ***(1)*** và ***(2)*** ta cũng có

$$g^m \leq N \leq \left(g-1\right)\left(g^m + g^{m-1} + \ldots + g + 1\right) = g^{m+1} - 1 < g^{m+1}$$

suy ra $m\log g \leq \log N < \left(m+1\right)\log g$ và vì vậy $m \leq \frac{\log N}{\log g} < m+1$. Do đó

(6) $$m = \left[\frac{\log N}{\log g}\right].$$

Các công thức ***(6)*** và ***(5)*** chứng tỏ rằng nếu N được biểu diễn dưới dạng ***(1)*** và điều kiện ***(2)*** được thỏa mãn thì các số m và $c_n\left(n=0,1,...,m\right)$ xác định duy nhất theo N. Điều này chứng tỏ với số tự nhiên cho trước N (với số tự nhiên xác định $g>1$) tồn tại nhiều nhất một biểu diễn dạng ***(1)*** thỏa mãn ***(2)***. Vì vậy để chứng minh định lý ta chỉ cần chỉ ra rằng với mọi số tự nhiên N và $g>1$ tồn tại ít nhất một biểu diễn dạng ***(1)*** thỏa mãn ***(2)***. Gọi N_1 và c_0 là thương số và số dư nhận được khia chia N cho g. Ta có $N=c_0+gN_1$. Thay N bằng N_1 ta tìm được thương số N_2 và phần dư c_1 từ phép chia N_1 cho g. Tiếp tục như vậy với N_2 và cứ như thế. Rõ ràng tất cả các thương số lần lượt thu được sẽ giảm bởi vì $N_{n+1}\le N_n/g$. Do các số này đều là các số nguyên không âm nên với $k\ge 1$ nào đó ta phải có $N_k=0$. Ký hiệu m là chỉ số lớn nhất mà $N_m\ne 0$. Ta có dãy đẳng thức

$$N=c_0+gN_1,\ N_1=c_1+gN_2,\ ...,\ N_{m-1}=c_{m-1}=gN_m,\ N_m=c_m.$$

Vì vậy ta thu được biểu diễn của N có dạng $N=c_0+c_1g+c_2g^2+...+c_mg^m$ trong đó $c_m\ne 0$ bởi vì $N_m\ne 0$ và $c_n\left(n=0,1,...,m\right)$ là các phần dư thu được khi chia cho g nên nó thỏa mãn ***(2)***. □

Vậy ta đã chứng minh được Định lý 1 và ta cũng có ngay thuật toán tìm biểu diễn của N trong cơ số g như sau: ta chia N cho g và ký hiệu phần dư là c_0 và thương số là N_1, sau đó ta chia N_1 cho g và ký hiệu phần dư là c_1 và thương số là N_2. Tiếp tục quá trình này cho tới khi nhận được thương số $N_{m+1}=0$. Khi đó ta thu được biểu diễn của N theo dạng (1). Trường hợp riêng khi $g=2$ thì chỉ có hai chữ số là 0 và 1. Từ Định lý 1 ta có hệ quả sau đây

Hệ quả. *Các số tự nhiên có thể biểu diễn duy nhất dưới dạng tổng các bình phương lũy thừa phân biệt của 2.*

Ví dụ: $100=2^6+2^5+2^2$, $29=2^4+2^3+2^2+2^0$, $M_n=2^n-1=2^{n-1}+2^{n-2}+...+2+2^0$.

Bài tập. ***1.*** Tìm tất cả các chữ số trong biểu diễn cơ số 2 của 12 số nguyên tố đầu tiên.

Lời giải. 10, 11, 101, 111, 1011, 1101, 10001, 10011, 10111, 11101, 11111, 100101.

2. Chứng minh rằng với mọi số tự nhiên m tồn tại số nguyên tố mà biểu diễn của nó trong cơ số 2 thỏa mãn chữ số cuối cùng của nó là 1 và m chữ số liền trước đó là 0.

Lời giải. Theo Định lý 11 Chương 6, với số tự nhiên m tồn tại số nguyên tố p có dạng $m^{m+1}k+1$, k tự nhiên. Biểu diễn của số nguyên tố này trong cơ số 2 có chữ số cuối cùng là 1 và m chữ số liền trước bằng 0. □

Ghi chú. Tồn tại những số nguyên tố mà biểu diễn cơ số 2 của chúng gồm toàn chữ số 1. Có 30 số như thế đã được tìm ra, số lớn nhất có 216091 chữ số 1 trong hệ cơ số 2. Ta chưa biết có tồn tại vô hạn các số như vậy hay không. Rõ ràng những số nguyên tố như vậy đều có dạng 2^n-1. Mặt khác có những số nguyên tố mà trong biểu diễn hệ cơ số 2 của chúng thì chỉ có chữ số đầu và chữ số cuối bằng 1 còn lại tất cả đều là 0. Ví dụ các số 11, 101, 10001, 100000001 và 10000000000000001. Ta chưa biết ngoài các số này ra thì có số nguyên tố nào như vậy hay không. Tất cả các số như vậy đều có dạng $2^{2^n}+1$.

3. Chứng minh với số tự nhiên bất kỳ $s>1$ tồn tại ít nhất 2 số nguyên tố mà biểu diễn cơ số 2 có đúng s chữ số.

Chứng minh. Với $s=2$ và $s=3$ kết quả được suy ra từ bài tập 1. Nếu $s\ge 4$ thì $2^{s-1}>5$ và theo Định lý 7 Chương 3 suy ra giữa 2^{n-1} và 2^s tồn tại ít nhất hai số nguyên tố. Mặt khác nếu n là số tự nhiên mà $2^{s-1}\le n<2^s$ thì n có đúng s chữ số trong hệ cơ số 2. □

4. Chứng minh rằng chữ số cuối cùng trong biểu diễn cơ số 12 của số chính phương là một bình phương đúng.

Chứng minh. Nếu chữ số cuối cùng của số tự nhiên là $0,1,\ldots,11$ thì chữ số cuối cùng trong hệ cơ số 12 của bình phương của nó là $0,1,4,9,4,1,0,1,4,9,4,1,$ tương ứng. □

Ghi chú. Tất cả các cơ số có tính chất trên là 2, 3, 4, 5, 8, 12, 16 (xem Muller [1]).

5. Chứng minh rằng tồn tại vô hạn số tự nhiên n không chia hết cho 10 và thỏa mãn số n' nhận được từ n bằng cách đảo ngược thứ tự các chữ số thập phân của nó là ước số của n và $n:n'>1$.

Chứng minh. Các số $9899\ldots9901=9\cdot1099\ldots9989$ và $8799\ldots9912=4\cdot2199\ldots9978$ trong đó số chữ số 9 ở giữa là tùy ý và bằng nhau ở cả hai vế có tính chất đó. Có thể chứng minh số nhỏ nhất >9 có tính chất trên là $8712=4\cdot2178$ và các số ở trên là tất cả các số có tính chất như vậy (xem Subba Rao [1]). Vấn đề khi nào thì tồn tại các số như vậy được đặt ra bởi D.R.Kaprekar. □

6. Chứng minh rằng mọi số tự nhiên có thể biểu diễn duy nhất dưới dạng

(*) $$n=a_1\cdot1!+a_2\cdot2!+\ldots+a_m\cdot m!,$$

với m là số tự nhiên, $a_m\neq0$ và $a_j\ (j=1,2,\ldots,m)$ là các số nguyên thỏa mãn $0\le a_j\le j$ với $j=1,2,\ldots,m$.

Chứng minh. Giả sử số tự nhiên n có hai biểu diễn dạng ***(*)***. Ta có

$$a_1\cdot1!+a_2\cdot2!+\ldots+a_m\cdot m!=a_1'\cdot1!+a_2'\cdot2!+\ldots+a_m'\cdot m!.$$

Ký hiệu k là số tự nhiên lớn nhất thỏa mãn $a_k\neq a_k'$, nghĩa là $a_k'>a_k$ suy ra $a_k'-a_k\ge1$, vì vậy

$$k!\le a_k'\cdot k!-a_k\cdot k!=a_1\cdot1!+\ldots+a_{k-1}(k-1)!-a_1'\cdot1!-\ldots-a_{k-1}'(k-1)!$$

$$\le1\cdot1!+2\cdot2!+\ldots+(k-1)(k-1)!=k!-1<k!,$$

Vô lý. Xét s là số tự nhiên. Xác định tất cả các biểu diễn dạng ***(*)*** với $m\le s$ và $0\le a_j\le j$ với $j=1,2,\ldots,m$. Số các biểu diễn như vậy là $(1+1)(2+1)\ldots(s+1)=(s+1)!$. Vì vậy số các biểu diễn (bỏ qua trường hợp $n=0$) là $(s+1)!-1$. Ở trên ta đã chứng minh các biểu diễn ***(*)*** khác nhau sẽ cho các số n khác nhau. Mặt khác mọi biểu diễn dạng ***(*)*** với $m\le s$ cho ta số tự nhiên $\le1\cdot1!+2\cdot2!+\ldots+m\cdot m!=(m+1)!-1\le(s+1)!-1$. Vì vậy hiển nhiên mọi số tự nhiên $\le(s+1)!-1$ có thể biểu diễn dưới dạng ***(*)*** như là n ở trên với $m\le s$. □

7. Với các số tự nhiên g và s cố định đặt $f(n)$ là tổng các lũy thừa bậc *s của các chữ số trong hệ cơ số* g của số tự nhiên n. Chứng minh rằng dãy vô hạn

(i) $$n,\ f(n),\ ff(n),\ fff(n),\ldots$$

tuần hoàn.

Chứng minh. Rõ ràng ta chỉ cần chứng minh trong dãy trên có hai phần tử bằng nhau. Xét số tự nhiên $n=a_0+a_1g+\ldots+a_{k-1}g^{k-1}$ là biểu diễn của n trong hệ cơ số g. Ta có $f(n)=a_0^s+a_1^s+\ldots+a_{k-1}^s\le k(g-1)^s<kg^s$. Nhưng g^k/k tiến tới vô cùng theo k do đó với k đủ lớn ta có $g^k/k>g^{s+1}$. Vì vậy $kg^s<g^{k-1}\le n$. Từ đây ta suy ra với n đủ lớn, ký hiệu là $n>m$, ta có $f(n)<n$. Vậy với mọi số $x>m$ thì tồn tại $k(x)$ mà $fff\ldots.f(x)<m$ (f được tính $k(x)$ lần). Do đó trong dãy ban đầu có vô hạn phần tử không vượt quá m. Suy ra tồn tại hai phần tử bằng nhau. □

Ghi chú. Với $g=10$ và $s=2$, Porges [1] đã chứng minh dãy ***(i)*** tuần hoàn sẽ chứa một phần tử bằng 1 hoặc 8 phần tử 4,16, 37, 58, 89, 145, 42, 20. Ví dụ với $n=3$ ta có dãy 3, 9, 81, 65, 61, 37, 58, …, 16, 37, …. Nếu $n=5$ ta có dãy 5, 25, 29, 85, 89,145, …, 58, 89, …. Nếu $n=7$ ta có dãy 7, 49, 97, 130, 10, 1, 1, 1, … Tổng quát hóa kết quả của Porges được trình bày bởi B.M.Stewart [1]. Trường

hợp $g=10$ và $s=3$ được giải quyết bởi K.Iseki [1], người đã chứng minh rằng có 9 vòng lặp như vậy. Đó là: một phần tử trong các trường hợp 1, 153, 370, 371, 407; hai phần tử với cặp 136 và 244 hoặc 919 và 1459; ba phần tử với các bộ ba 55, 250, 133, hoặc 160, 217, 252 (xem Iseki [2]). K.Chikawa, K.Iseki và T.Kusakabe [1] đã chứng minh rằng trong trường hợp $g=10$, $s=4$ thì có 6 vòng lặp như vậy. Đó là: một phần tử thuộc 1, 1634, 8208, 9474; hai phần tử 2178, 6514; bảy phần tử 13139, 6725, 4338, 4514, 1138, 4179, 9219 (Chikawa, Iseki, Kusakabe và Shibamura [1] tìm ra tất cả các vòng lặp với $g=10$, $s=5$, Avanesov, Gusev [1] giải quyết các trường hợp $g=10, s=6$ hoặc 7, Takada [1] giải quyết trường hợp $g=10, s=8$, Iseki và Takada [1] với $g=10$, $s=9$ và cuối cùng Avanesov, Gusev [2] giải quyết trường hợp $g=10$, $s=10$ hoặc 11).

8. Chứng minh vòng lặp của dãy ***(i)*** có thể dài tùy ý.

Chứng minh. Với số tự nhiên n tùy ý tồn tại số tự nhiên $m>n$ thỏa mãn $f(m)=n$. Thật vậy với mọi số tự nhiên s thì tổng các lũy thừa bậc s của các chữ số của nó trong hệ cơ số g của $m=\dfrac{g^n-1}{g-1}$ là n và hơn nữa nếu $n>1$ ta có $m>n$. Nếu $n=1$ ta đặt $m=g$. □

9. Tính bảng tổng và tích các chữ số trong hệ cơ số 7.

Lời giải.

	1	2	3	4	5	6
1	2	3	4	5	6	10
2	3	4	5	6	10	11
3	4	5	6	10	11	12
4	5	6	10	11	12	13
5	6	10	11	12	13	14
6	10	11	12	13	14	15

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	11	13	15
3	3	6	12	15	21	24
4	4	11	15	22	26	33
5	5	13	21	26	34	42
6	6	15	24	33	42	51

2. Biểu diễn trong hệ cơ số âm

Định lý 2. *Nếu g là số nguyên <-1 thì mọi số nguyên $N\neq 0$ có thể biểu diễn duy nhất dưới dạng* ***(1)*** *trong đó $c_n\,(n=0,1,\ldots,m)$ nguyên thỏa mãn*

(7) $$0\le c_n<|g| \quad \textit{với} \quad n=0,1,\ldots,m \quad \textit{và} \quad c_m\neq 0.$$

Định lý này được Z.Pawlak và Andrzej Wakulicz [1] tìm ra bằng cách sử dụng máy tính điện tử.

Chứng minh. Xét số nguyên $g<-1$ và $x=N$ là số nguyên tùy ý. Ký hiệu c_0 là phần dư khi chia x cho $|g|$. Ta có $0\le c_0<|g|$ và $x=c_0+gx_1$ trong đó x_1 nguyên. Vì vậy $gx_1=x-c_0$ và do đó $|gx_1|\le|x|+c_0\le|x|+|g|-1$ trong đó $|x_1|\le(|x|+|g|-1)/|g|$.

Nếu $(|x|+|g|-1)/|g|\ge|x|$ thì $|x|+|g|-1\ge|g||x|$, nghĩa là $|g|-1\ge(|g|-1)|x|$ suy ra vì $|g|>1$ ta có $|x|\le 1$ do đó $x=0,1$ hoặc -1. Nếu $x=0$ hoặc $x=1$ thì $x=c_0$. Nếu $x=-1$ thì $x=|g|-1+g=c_0+g$ suy ra $c_0=|g|-1$. Vì vậy chỉ cần xét trường hợp $(|x|+|g|-1)/|g|<|x|$. Ta có $|x_1|<|x|$ và có thể áp dụng thủ tục vừa sử dụng với x cho x_1.

Tiếp tục quá trình này và sau hữu hạn bước ta nhận được biểu diễn của N trong dạng ***(1)*** với $c_n\,(n=0,1,\ldots,m)$ nguyên thỏa mãn ***(7)***.

Tiếp theo để chứng minh biểu diễn của N trong dạng ***(1)*** thỏa mãn ***(7)*** là duy nhất, ta chỉ cần nhận xét N chia cho $|g|$ có phần dư c_0, $(N-c_0)/g$ chia cho $|g|$ có phần dư c_1 và cứ thế suy ra $c_0,c_1,c_2,\ldots$ xác định duy nhất theo N vì vậy biểu diễn này là duy nhất.

Định lý 2 được chứng minh.

Ví dụ. $-1=(11)_{-2}$, $10=(11110)_{-2}$, $-10=(1010)_{-2}$, $16=(10000)_{-2}$, $-16=(110000)_{-2}$, $25=(1101001)_{-2}$, $-25=(111011)_{-2}$, $100=(110100100)_{-2}=(10201)_{-3}$.

3. Phân số vô hạn trong hệ cơ số cho trước

Xét số tự nhiên $g>1$ và số thực x. Đặt $x_1=x-[x]$. Ta có $0\le x_1\le 1$. Hơn nữa với $x_2=gx_1-[gx_1]$ thì $0\le x_2<1$. Tiếp tục ta xác định x_3 bởi $gx_2-[gx_2]$ và cứ như vậy ta thu được dãy vô hạn $x_n\,(n=1,2,\ldots)$ định nghĩa bởi các điều kiện

(8) $\qquad x_1=x-[x],\quad x_{n+1}=gx_n-[gx_n]\qquad$ với $\qquad n=1,2,\ldots$

Các công thức này suy ra

(9) $\qquad 0\le x_n<1\qquad$ với $\qquad n=1,2,\ldots$

Đặt

(10) $\qquad c_n=[gx_n]\qquad$ với $\qquad n=1,2,\ldots$

Theo ***(9)*** ta có $0\le gx_n<g$ vì vậy theo ***(10)*** $0\le c_m<g$ và do đó

(11) $\qquad 0\le c_n\le g-1\qquad$ với $\qquad n=1,2,\ldots$

Từ ***(8)*** và ***(11)*** suy ra $x=[x]+x_1$, $x_1=\dfrac{c_1+x_2}{g}$, $x_2=\dfrac{c_2+x_3}{g}$, ..., $x_n=\dfrac{c_n+x_{n+1}}{g}$. Vì vậy với $n=1,2,\ldots$,

(12) $\qquad x=[x]+\dfrac{c_1}{g}+\dfrac{c_2}{g^2}+\ldots+\dfrac{c_n}{g^n}+\dfrac{x_{n+1}}{g^n}.$

Theo ***(9)*** thì $0\le\dfrac{x_{n+1}}{g^n}<\dfrac{1}{g^n}$ và từ $g\ge 2, g^n$ tăng vô hạn theo n, ta suy ra $\lim\limits_{n\to\infty}\dfrac{x_{n+1}}{g^n}=0$. Vì theo ***(12)*** ta nhận được khai triển của x thành chuỗi vô hạn

(13) $\qquad x=[x]+\dfrac{c_1}{g}+\dfrac{c_2}{g^2}+\dfrac{c_3}{g^3}+\ldots$

trong đó theo ***(11)*** các số c_n là các chữ số trong hệ cơ số g.

Vì vậy ta đã chứng minh mọi số thực x có ít nhất một biểu diễn có dạng ***(13)*** với mọi hệ cơ số $g>1$ trong đó c_n là các chữ số trong hệ cơ số g.

Giả sử rằng số thực x được biểu diễn trong dạng ***(13)*** với c_n là các số nguyên thỏa mãn ***(11)*** thì với mọi $n=1,2,\ldots$ đặt

(14) $\qquad r_n=[x]+\dfrac{c_1}{g}+\dfrac{c_2}{g^2}+\ldots+\dfrac{c_n}{g^n}.$

Ta có $x-r_n=\dfrac{c_{n+1}}{g^{n+1}}+\dfrac{c_{n+2}}{g^{n+2}}+\ldots$ suy ra ra theo ***(11)***, $0\le x-r_n\le\dfrac{g-1}{g^{n+1}}+\dfrac{g-1}{g^{n+2}}+\ldots=\dfrac{1}{g^n}$.

Biểu thức $x-r_n=1/g^n$ dương chỉ trong trường hợp $c_{n+1}=c_n=\ldots=g-1$ nghĩa là tất cả các chữ số trong biểu diễn đều bằng $g-1$ với n xác định. Vậy $x=r_n+1/g^n$ và theo ***(14)*** suy ra x là thương số của một số nguyên và một lũy thừa của g. Nếu m là số tự nhiên nhỏ nhất mà $c_n=g-1$ với $n\ge m$ thì nếu $m=1$ thì theo ***(13)*** ta có $x=[x]+1$, vô lý. Nếu $m>1$ thì $c_{m-1}\ne g-1$ suy ra theo

(11) thì $c_{m-1} < g-1$ nghĩa là $c_{m-1} \le g-2$ suy ra $c'_{m-1} = c_{m-1}+1$ cũng là chữ số trong hệ cơ số g. Hệ quả là ta có biểu diễn khác với ***(13)***

$$x = [x] + \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_{m-2}}{g^{m-2}} + \frac{c'_{m-1}}{g^{m-1}} + \frac{0}{g^m} + \frac{0}{g^{m+1}} + \ldots,$$

Dễ dàng chứng minh điều ngược lại. Nếu x là thương số của một số nguyên và một lũy thừa của g thì x có hai biểu diễn dạng ***(13)*** với c_n là các số nguyên thỏa mãn ***(11)***. Trong đó có một biểu diễn mà chỉ có hữu hạn số c_n khác 0. Trong biểu diễn còn lại thì tất cả các hệ số này bằng $g-1$.

Nếu số thực x không là thương số của một số nguyên và một lũy thừa của g thì $0 \le x - r_n < \frac{1}{g^n}$ với $n = 1, 2, \ldots,$ vì vậy $0 \le g^n x - g^n r_n < 0$. Suy ra từ ***(14)*** số $g^n r_n$ nguyên. Ta có $g^n r_n = \left[g^n x \right]$. Điều này cũng đúng với $n = 0$ từ định nghĩa $r_0 = [x]$. Ta có

(15) $$g^n r_n = \left[g^n x \right] \quad \text{và} \quad g^{n-1} r_{n-1} = \left[g^{n-1} x \right] \quad \text{với} \quad n = 1, 2, \ldots$$

Nhưng theo ***(14)*** thì $r_n - r_{n-1} = \frac{c_n}{g^n}$ với mọi $n = 1, 2, \ldots,$ vậy $c_n = g^n r_n - g g^{n-1} r_{n-1}$ và theo ***(15)*** suy ra

(16) $$c_n = \left[g^n x \right] - g \left[g^{n-1} x \right], \qquad n = 1, 2, \ldots$$

Chứng tỏ mọi số thực x không là thương số của một số nguyên và một lũy thừa của g có đúng một biểu diễn dạng ***(13)*** trong đó c_n là các số nguyên thỏa mãn ***(11)***. Biểu diễn này ký hiệu bởi

(17) $$x = [x] + (0, c_1 c_2 c_3 \ldots)_g .$$

Công thức ***(16)*** cho ta cách tính chữ số thứ n khá đơn giản. Tuy nhiên không dễ để tính toán các giá trị ở vế phải của nó. Ví dụ với $g = 10$ công thức ***(16)*** cho chữ số thứ 1000 của $\sqrt{2}$ là $c_{1000} = \left[10^{1000} \sqrt{2} \right] - 10 \left[10^{999} \sqrt{2} \right]$.

Ta đã chứng minh rằng để thu được biểu diễn dạng ***(17)*** của một số thực tùy ý ta có thể áp dụng thuật toán: $x_1 = x - [x]$, $c_1 = [g x_1]$, $x_2 = g x_1 - c_1$, $c_2 = [g x_2]$, $x_3 = g x_2 - c_2$, ..., $x_n = g x_{n-1} - c_{n-1}$, $c_n = [g x_n], \ldots$.

Ta cũng đã chứng minh rằng biểu diễn ***(13)*** là hữu hạn (nghĩa là tất cả các chữ số trong biểu diễn đều bằng 0 trừ ra một số hữu hạn) nếu và chỉ nếu x là thương số của một số nguyên và một lũy thừa của g.

Dễ dàng chứng minh điều kiện này tương đương với việc nói rằng x là số hữu tỷ có dạng biểu diễn phân số tối giản với mẫu số là tích của các số nguyên tố mà mỗi số đều là ước số của g.

Điều kiện cần là hiển nhiên.

Mặt khác nếu $x = l/m$ với l là số nguyên và m là số tự nhiên thỏa mãn mọi ước số nguyên tố của m là ước của g thì nếu $g = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}$ là phân tích thành các thừa số nguyên tố của g ta có $m = q_1^{\lambda_1} q_2^{\lambda_2} \ldots q_s^{\lambda_s}$ với $\lambda_1, \lambda_2, \ldots \lambda_s$ là các số nguyên không âm. Với số tự nhiên k thỏa mãn $k\alpha_i \ge \lambda_i$ với mọi $i = 1, 2, \ldots, s$. Thì $m \mid g^k$ do đó $g^k = hm$ với h là số tự nhiên. Vì vậy $x = l/m = hl/g^k$ suy ra điều kiện đủ.

Vì vậy nếu số thực x không phải số hữu tỷ mà biểu diễn dạng phân số tối giản của nó có mẫu số là tích của các ước số nguyên tố đều là ước của g thì x có đúng một biểu diễn dạng ***(13)*** với

$c_n\,(n=1,2,\ldots)$ là các chữ số trong hệ cơ số g. Hơn nữa biểu diễn này là vô hạn và có vô hạn chữ số khác $g-1$. Biểu diễn này thu được bằng thuật toán ở trên.

Thuật toán để tìm biểu diễn của số thực x vẫn có hiệu lực trong trường hợp g là số thực >1. Khi đó các công thức ***(8), (9), (10)*** và ***(12)*** vẫn đúng. Mệnh đề về các số c_n cũng vẫn đúng nhưng cần thêm điều kiện $0\le c_n<g$ và c_n nguyên. Ví dụ với $g=\sqrt{2}$, $x=\sqrt{2}$ thì biểu diễn cho bởi thuật toán là $\sqrt{2}=1+\dfrac{1}{\left(\sqrt{2}\right)^3}+\dfrac{1}{\left(\sqrt{2}\right)^9}+\dfrac{1}{\left(\sqrt{2}\right)^{12}}+\dfrac{1}{\left(\sqrt{2}\right)^{21}}+\ldots$ Tuy nhiên $\sqrt{2}$ còn có biểu diễn khác $\sqrt{2}=\dfrac{1}{\sqrt{2}}+\dfrac{1}{\left(\sqrt{2}\right)^3}+\dfrac{1}{\left(\sqrt{2}\right)^5}+\dfrac{1}{\left(\sqrt{2}\right)^7}+\ldots$ Với $g=\sqrt{2}$ và $x=\left(2\sqrt{2}+1\right)/4$ ta có hai biểu diễn có dạng ***(13)*** là $\dfrac{2\sqrt{2}+1}{4}=\dfrac{1}{\sqrt{2}}+\dfrac{1}{\left(\sqrt{2}\right)^6}+\dfrac{1}{\left(\sqrt{2}\right)^8}+\ldots=\dfrac{1}{\sqrt{2}}+\dfrac{1}{\left(\sqrt{2}\right)^4}+\ldots$, trong đó đẳng thức sau được cho bởi thuật toán ở trên. Ta cũng có

$$\begin{aligned}\frac{1}{2}+\frac{\sqrt{2}}{4}&=\frac{1}{\left(\sqrt{2}\right)^4}+\frac{1}{\left(\sqrt{2}\right)^5}+\frac{1}{\left(\sqrt{2}\right)^6}+\ldots\\&=\frac{1}{\left(\sqrt{2}\right)^2}+\frac{1}{\left(\sqrt{2}\right)^5}+\frac{1}{\left(\sqrt{2}\right)^7}+\ldots\end{aligned}$$

Với biểu diễn thứ hai cho bởi thuật toán trên. Xem Gelfond [1].

4. Biểu diễn của các số hữu tỷ

Xét số hữu tỷ x có dạng phân số tối giản l/m và giả sử biểu diễn của x có dạng ***(13)*** với $c_n\,(n=1,2,\ldots)$ là các chữ số trong hệ cơ số nguyên $g>1$. Đặt $x_n\,(n=1,2,\ldots)$ là các số định nghĩa bởi ***(8).*** Khi đó các công thức ***(9)***, ***(10)*** đúng. Theo ***(8)*** ta có $mx_1=l-[x]$. Từ đó mx_1 là số tự nhiên và từ ***(8)*** ta có $mx_{n+1}=gmx_n-m\left[gx_n\right]$ với mọi $n=1,2,\ldots,$ từ đó theo quy nạp ta suy ra mọi số mx_n đều nguyên và hơn nữa theo ***(9)*** thì chúng thỏa mãn các bất đẳng thức $0\le mx_n<m$ với $n=1,2,\ldots$ Nếu với n nào đó ta có $x_n=0$ thì theo ***(8)*** ta có $x_j=0$ với mọi $j\ge n$. Vì vậy theo ***(10)*** thì $c_j=0$ với $j\ge n$ và biểu diễn ***(13)*** của x là hữu hạn. Hơn nữa giả sử $x_n\ne 0$ với mọi $n=1,2,\ldots$ ta có $0<mx_n<m$ với $n=1,2,\ldots$ và do đó các số $mx_1,mx_2,\ldots,mx_m$ chỉ có thể nhận $m-1$ giá trị phân biệt $1,2,\ldots,m-1$. Từ đây suy ra tồn tại các số tự nhiên h và s thỏa mãn $h+s\le m$ và $mx_h=mx_{h+s}$, mà theo ***(8)*** suy ra $x_n=x_{n+s}$ với $n>h$ do đó theo ***(10)*** thì $c_n=c_{n+s}$ với $n\ge h$. Suy ra dãy vô hạn các chữ số của ***(17)*** là tuần hoàn. Ta có định lý sau đây

Định lý 3. *Biểu diễn của số hữu tỷ trong dạng* ***(13)*** *với* g *là số tự nhiên lớn hơn 1 sẽ tuần hoàn. Số các chữ số đứng trước vòng lặp nhỏ hơn mẫu số của số ban đầu.*

Xét dãy vô hạn tùy ý $c_1,c_2,\ldots,$ với $c_n\,(n=1,2,\ldots)$ là các chữ số trong hệ cơ số g. Thế thì c_n thỏa mãn ***(11)***, vì vậy suy ra chuỗi vô hạn ***(13)*** hội tụ và tổng x của chúng là số thực. Từ Định lý 3 suy ra nếu dãy $c_1,c_2,\ldots$ không tuần hoàn thì x là số vô tỷ. Để chứng minh điều ngược lại ta chỉ cần chứng minh nếu dãy các chữ số $c_1,c_2,\ldots$ tuần hoàn thì số ***(17)*** hữu tỷ. Giả sử dãy $c_1,c_2,\ldots$ là tuần hoàn. Nghĩa là với số tự nhiên s và h nào đó ta có $c_{n+s}=c_n$ và do đó $n\ge h$. Suy ra

$$\frac{c_1}{g}+\frac{c_2}{g^2}+\ldots$$
$$=\frac{c_1}{g}+\frac{c_2}{g^2}+\frac{c_{h-1}}{g^{h-1}}+\frac{c_h}{g^h}+\frac{c_{h+1}}{g^{h+1}}+\ldots+\frac{c_{h+s-1}}{g^{h+s-1}}+\frac{c_h}{g^{h+s}}+\frac{c_{h+1}}{g^{h+s+1}}+\ldots+\frac{c_{h+s-1}}{g^{h+2s-1}}+\ldots$$
$$=\frac{c_1}{g}+\frac{c_2}{g^2}+\ldots+\frac{c_{h-1}}{g^{h-1}}+\left(\frac{c_h}{g^h}+\frac{c_{h+1}}{g^{h+1}}+\ldots+\frac{c_{h+s-1}}{g^{h+s-1}}\right)\times\left(1+\frac{1}{g^s}+\frac{1}{g^{2s}}+\ldots\right)$$
$$=\frac{c_1}{g}+\frac{c_2}{g^2}+\ldots+\frac{c_{h-1}}{g^{h-1}}+\left(\frac{c_h}{g^h}+\frac{c_{h+1}}{g^{h+1}}+\ldots+\frac{c_{h+s-1}}{g^{h+s-1}}\right)\frac{g^s}{g^s-1}$$
$$=\frac{c_1g^{h+s-2}+c_2g^{h+s-3}+\ldots+c_{h-1}g^s+c_hg^{s-1}+\ldots+c_{h+s-1}}{g^{h-1}\left(g^s-1\right)}-\frac{c_1g^{h-1}+c_2g^{h-2}+\ldots+c_{h-1}}{g^{h-1}\left(g^s-1\right)}$$
$$=\frac{\left(c_1c_2\ldots c_{h+s-1}\right)_g}{g^{h-1}\left(g^s-1\right)}-\frac{\left(c_1c_2\ldots c_{h-1}\right)_g}{g^{h-1}\left(g^s-1\right)}$$

Vì vậy ta thấy tổng của chuỗi trên là số hữu tỷ $\frac{\left(c_1c_2\ldots c_{h+s-1}\right)_g-\left(c_1c_2\ldots c_{h-1}\right)_g}{g^{h-1}\left(g^s-1\right)}$. Tuy nhiên phân số này chưa chắc đã tối giản.

Công thức cho ta quy tắc rút gọn các biểu diễn tuần hoàn trong hệ cơ số $g>1$. Ta có

Định lý 3^a**.** *Với hệ cơ số tự nhiên* $g>1$ *cho trước, các số có biểu diễn dạng* ***(13)*** *thỏa mãn dãy các chữ số của nó là tuần hoàn đều là số hữu tỷ (biểu diễn hữu hạn được coi như tuần hoàn với chu kỳ bằng* 0 *hoặc* $g-1$*).*

Hệ quả của Định lý 3^a là nếu x có biểu diễn không tuần hoàn trong hệ cơ số g thì x là số vô tỷ. Từ nhận xét này ta có thể chứng minh số $a=0.1234567891011121314\ldots$ (các số 1,2,3, ... được viết cạnh nhau) là số vô tỷ. Để chứng minh điều này chỉ cần chú ý rằng trong biểu diễn của a sẽ xuất hiện số $10^n\left(n=1,2,\ldots\right)$ với n tùy ý, do đó nó chứa dãy số 0 dài vô hạn, do đó không thể tuần hoàn chu kỳ hữu hạn được.

Bài tập. ***1.*** Biểu diễn số $\frac{1}{99^2}$ dưới dạng thập phân

Lời giải. $\frac{1}{99^2}=0.\dot{0}\dot{0}\dot{0}\dot{1}\dot{0}\dot{2}\dot{0}\dot{3}\ldots\dot{0}\dot{8}\dot{0}\dot{9}\dot{1}\dot{0}\dot{1}\dot{1}\dot{1}\dot{2}\ldots\dot{9}\dot{6}\dot{9}\dot{7}\dot{9}\dot{9}$ trong đó các dấu chấm phía trên các chữ số chỉ ra vòng lặp. Vòng lặp bắt đầu từ ngay sau dấu phẩy thập phân và thu được bằng việc viết liên tiếp các số từ 0 tới 99 trừ ra số 98. Tổng quát hơn J.W.L.Glaisher [1] đã đưa ra công thức $\frac{1}{\left(g-1\right)^2}=(0.\dot{0}\dot{1}\dot{2}\dot{3}\ldots\overline{\dot{g-3}}\,\overline{\dot{g-1}})_g$ với g là số tự nhiên >2.

2. Sử dụng $e=2.718281828\ldots$ hãy biểu diễn e trong cơ số 2 chính xác tới 24 chữ số.

Lời giải. $e=(10.10110111111000010101000 1\ldots)_2$. Biểu diễn này được đưa ra bởi G.Peano trong [1] trang 154. Trong đó ta có $e=\left(!.,!.!!.!!!!!!....!.!.!....!\right)_2$.

3. Sử dụng $\pi=3.14159265\ldots$ hãy biểu diễn π trong cơ số 2 chính xác tới 24 chữ số.

Lời giải. $\pi=\left(11.001001000011111101101010\ldots\right)_2$ (xem G.Peano [1] trang 177).

4. Chứng minh rằng trong mọi biểu diễn thập phân vô hạn tồn tại dãy dài tùy ý các chữ số xuất hiện vô hạn lần.

Chứng minh. Ký hiệu 0. $c_1 c_2 c_3 \ldots$ là biểu diễn thập phân vô hạn và m là số tự nhiên. Xét các khối có m chữ số xuất hiện trong dãy $c_1 c_2 \ldots$, nghĩa là các dãy

(18) $$c_{km+1}, c_{km+2}, \ldots, c_{km+m} \quad \text{với} \quad k = 0,1,\ldots$$

Ta chia tất cả các dãy như vậy thành hai lớp với tính chất hai dãy thuộc cùng một lớp nếu và chỉ nếu các phần tử của dãy này đều tương ứng bằng các phần tử của dãy kia. Rõ ràng số các lớp các dãy chưa m phần tử không vượt quá 10^m do đó hữu hạn. Nhưng mặt khác tồn tại vô hạn dãy có dạng ***(18)*** suy ra ít nhất một dãy xuất hiện vô hạn lần. □

Ghi chú. Trong trường hợp riêng của định lý trên ta chú ý rằng trong mọi biểu diễn thập phân vô hạn ít nhất có một chữ số xuất hiện vô hạn lần. Hơn nữa nếu đó là một số vô tỷ thì có ít nhất hai chữ số xuất hiện vô hạn lần. Tuy nhiên ta không biết với $\sqrt{2}$ và π thì hai chữ số đó là bao nhiêu. L.E.J.Brouwer đã lưu ý rằng ta không biết dãy 0123456789 có xuất hiện trong biểu diễn thập phân của π hay không. Biểu diễn thập phân tới chữ số thứ 100000 của e và π được trình bày lần lượt bởi Shanks và Wrench trong [2] và [1]. Số π được tính chính xác tới chữ số thứ 1000000 bởi Gilloud và Bourger [1] và tới 4196239 trong Tamura và Kanada [1].

5. Chứng minh rằng số $(cc\ldots c)_{10}$ với các chữ số trong hệ cơ số 10 là c trong đó $c = 2$, $c = 5$ hoặc $c = 6$ không có dạng m^n, với m và n là các số tự nhiên > 1.

Chứng minh. Các số 2, 5, 6 không chia hết cho bất kỳ bình phương nào > 1. Vì vậy chúng không có dạng m^n với các số tự nhiên m, $n > 1$. Các số có chữ số tận cùng là 22, 55, 66 lần lượt không chia hết cho các số 4, 25 và 4 suy ra chúng không có dạng m^n với các số tự nhiên m, $n > 1$. Một số > 4 với các chữ số trong biểu diễn thập phân đều bằng 4 thì chia hết cho 4 nhưng không chia hết cho 8. Do đó không thể là lũy thừa bậc n của một số tự nhiên m với $n \geq 3$. Nếu $44\ldots4 = m^2$ thì số $111\ldots1$ là bình phương đúng, nhưng điều này là không thể vì hai chữ số tận cùng của bình phương không thể là 11. □

Ghi chú. R.Oblath [1] đã chỉ ra rằng nếu các số 33…3, 77…7, 88…8, 99…9 lớn hơn 10 thì chúng không có dạng m^n với m, n là các số tự nhiên > 1. Ta chưa biết 11…1 có thể có dạng đó không (xem Shorey và Tijdeman [1]).

6. Biểu diễn $\frac{1}{10}$ trong hệ cơ số 2 và 3.

Lời giải. $\frac{1}{10} = \left(0.00\dot{0}\dot{1}\dot{1}\right)_2 = \left(0.\dot{0}\dot{0}\dot{2}\dot{2}\right)_3$.

7. Biểu diễn $\frac{1}{61}$ trong hệ cơ số 10.

Lời giải. $\frac{1}{61} = \left(0.\dot{0}\dot{1}\dot{6}\dot{3}\dot{9}\dot{3}\dot{4}\dot{4}\dot{2}\dot{6}\dot{2}\dot{2}\dot{9}\dot{5}\dot{0}\dot{8}\dot{1}\dot{9}\dot{6}\dot{7}\dot{2}\dot{1}\dot{3}\dot{1}\dot{1}\dot{4}\dot{7}\dot{5}\dot{4}\dot{0}\dot{9}\dot{8}\dot{3}\dot{6}\dot{0}\dot{6}\dot{5}\dot{5}\dot{7}\dot{3}\dot{7}\dot{7}\dot{0}\dot{4}\dot{9}\dot{1}\dot{8}\dot{0}\dot{3}\dot{2}\dot{7}\dot{8}\dot{6}\dot{8}\dot{8}\dot{5}\dot{2}\dot{4}\dot{5}\dot{9}\right)_{10}$.

Ghi chú. Có thể chứng minh rằng vòng lặp của $1/97$ chứa 96 chữ số và của $1/1913$ chứa 1912 chữ số. Ta với điều kiện nào của số tự nhiên $n > 2$ thì biểu diễn thập phân của nó tuần hoàn và có vòng lặp chứa $n-1$ chữ số. Trong lớp này còn có các số $n = 313, 1021, 1873, 2137, 3221, 3313$. Có thể chứng minh các số nguyên tố nhận 10 làm căn nguyên thủy thì có tính chất này.

5. Số chuẩn tắc và số chuẩn tắc tuyệt đối

Xét số tự nhiên $g > 1$. Ta viết số thực $x : x = [x] + (0.c_1 c_2 c_3 \ldots)_g$ là biểu diễn trong hệ cơ số g. Với mọi chữ số c (trong hệ cơ số g) và với mọi số tự nhiên n ta ký hiệu $l(c, n)$ là số các chữ số của

dãy $c_1, c_2, ..., c_n$ bằng c. Nếu $\lim_n \frac{l(c,n)}{n} = \frac{1}{g}$ với g giá trị của c thì số x được gọi là chuẩn tắc trong cơ số g. Ví dụ số $\frac{1234567890}{9999999999}$ là chuẩn tắc cơ số 10, số $\frac{1}{10}$ chuẩn tắc cơ số 2 nhưng không chuẩn tắc cơ số 3. Nếu x là chuẩn tắc cơ số 10 thì $x/2$ chưa chắc đã là chuẩn tắc. Ví dụ $x = 0.\dot{1}3\dot{5}7\dot{9}8\dot{2}0\dot{4}6$ là chuẩn tắc nhưng $x/2 = 0.\dot{0}6\dot{7}8\dot{9}9\dot{1}0\dot{2}3$ thì không.

Số chuẩn tắc trong mọi hệ cơ số được gọi là số chuẩn tắc tuyệt đối. Sự tồn tại của các số chuẩn tắc tuyệt đối được chứng minh bởi E.Borel [1]. Chứng minh này sử dụng lý thuyết độ đo và chỉ thuần túy chỉ ra sự tồn tại mà không đề xuất một phương pháp nào để xây dựng những số đó.

Ví dụ hữu ích đầu tiên về các số chuẩn tắc tuyệt đối được đưa ra năm 1916 (Sierpinski [5], H.Lebesgue [1]). Như đã được chứng minh bởi Borel thì hầu hết (theo nghĩa của lý thuyết độ đo) các số thực là số chuẩn tắc tuyệt đối.

Tuy nhiên với hầu hết các số thực quen thuộc thì ta lại không biết chúng có phải là số chuẩn tắc hay không. Ví dụ, ta không biết các số $\sqrt{2}$, π, e là chuẩn tắc trong hệ cơ số 10 hay không. Vì vậy mặc dù Borel đã chỉ ra hầu hết các số thực đều là số chuẩn tắc tuyệt đối nhưng không dễ dàng để xây dựng những số như thế.

D.G.Champernowne [1] vào năm 1933 đã chứng minh rằng số a (ở mục 4 ta đã chứng minh số này là vô tỷ) là chuẩn tắc cơ số 10. Champarnowne cũng đặt ra giả thuyết rằng số 0.2357111317..., (tất cả các số nguyên tố được đặt liên tiếp sau dấu phẩy thập phân) là chuẩn tắc cơ số 10. Giả thuyết này và định lý tổng quát hơn được chứng minh bởi A.H.Copeland và P.Erdos [1]. Các tính chất khác của số chuẩn tắc được nghiên cứu bởi W.M. Schmidt [1].

6. Phân số thập phân trong cơ số biến thiên

Xét $g_1, g_2, ...$ là dãy vô hạn các số tự nhiên >1, x là số thực. Xét dãy vô hạn $c_1, c_2, ...$ và $x_1, x_2, ...$ như sau

(19) $c_0 = [x],\ x_1 = x - c_0,\ c_1 = [g_1 x_1],\ x_2 = g_1 x_1 - c_1,$

$$c_2 = [g_2 x_2], ...,\ c_n = [g_n x_n],\ x_{n+1} = g_n x_n - c_n, \qquad n = 1, 2, ...$$

Rõ ràng $0 \le x_n <$ và $0 \le c_n \le g_n - 1$ với mọi $n = 1, 2, ...$

So sánh ***(19)*** và thuật toán trong mục 3 ta thấy chữ số c_1 là chữ số trong hệ cơ số g_1, c_2 là chữ số trong hệ cơ số g_2 và cứ như thế. Từ ***(19)*** ta có

(20) $$x = c_0 + \frac{c_1}{g_1} + \frac{c_2}{g_1 g_2} + \frac{c_3}{g_1 g_2 g_3} + ... + \frac{c_n}{g_1 g_2 ... g_n} + \frac{x_{n+1}}{g_1 g_2 ... g_n}.$$

với $n = 1, 2, ...$ ta có $g_n \ge 2$ và $0 \le x_{n-1} < 1$, hạng tử cuối cùng trong ***(20)*** không âm và nhỏ hơn $1/2^n$ suy ra nó tiến tới 0 khi n tiến tới vô cùng. Suy ra ta có biểu diễn của x thành chuỗi vô hạn

(21) $$x = c_0 + \frac{c_1}{g_1} + \frac{c_2}{g_1 g_2} + \frac{c_3}{g_1 g_2 g_3} + ...$$

Nếu $g_1 = g_2 = ... = g$ ta nhận lại biểu diễn nguyên thủy của x trong hệ cơ số g. Đặt $g_n = n + 1$, $n = 1, 2, ...$ thì ***(21)*** trở thành

(22) $$x = c_0 + \frac{c_1}{2!} + \frac{c_2}{3!} + \frac{c_3}{4!} + ...,$$

với $c_0, c_n\ (n = 1, 2, ...)$ là các số nguyên và

(23) $0 \le c_n < n \qquad (n = 1,2,\ldots)$

Rõ ràng nếu x là số hữu tỷ thì thuật toán ***(19)*** dẫn tới biểu diễn hữu hạn của ***(22)*** trong đó $c_n\,(n = 1,2,\ldots)$ thỏa mãn bất đẳng thức ***(23)***. Tuy nhiên mọi số hữu tỷ cũng có biểu diễn vô hạn thuộc dạng ***(22)*** vì

$$c_0 + \frac{c_1}{2!} + \frac{c_2}{3!} + \ldots + \frac{c_{n-1}}{n!} + \frac{c_n}{(n+1)!}$$

$$= c_0 + \frac{c_1}{2!} + \ldots + \frac{c_{n-1}}{n!} + \frac{c_n - 1}{(n+1)!} + \frac{n+1}{(n+2)!} + \frac{n+2}{(n+3)!} + \frac{n+3}{(n+4)!} + \ldots$$

Biểu diễn dạng ***(21)*** được nghiên cứu trong E.Strauss [1] và G.Cantor [1], biểu diễn ***(22)*** được nghiên cứu trong C.Stephanos [1] và G.Faber [1].

Ta hãy xem xét thêm một số khai triển khác các số thực thành chuỗi vô hạn.

Xét số thực dương x. Ký hiệu k_1 là số tự nhiên nhỏ nhất thỏa mãn $k_1 x > 1$. Đặt $k_1 x = 1 + x_1$ và ta có $x_1 > 0$. Ta tiếp tục quá trình này với x_1, nghĩa là ta tìm số tự nhiên nhỏ nhất k_2 thỏa mãn $k_2 x_1 > 1$ và đặt $k_2 x_1 = 1 + x_2$ và cứ như vậy. Khai triển này của x là chuỗi vô hạn có dạng $x = \frac{1}{k_1} + \frac{1}{k_1 k_2} + \frac{1}{k_1 k_2 k_3} + \ldots$, với $k_n\,(n = 1,2,\ldots)$ là các số tự nhiên và $k_{n+1} \ge k_n$ với $n = 1,2,\ldots$.

Có thể chứng minh rằng mỗi số thực dương có duy nhất một biểu diễn dạng này và điều kiện cần và đủ để số x là vô tỷ là $\lim\limits_{n\to\infty} k_n = +\infty$ (Sierpinski [3]).

Khai triển nhận được của số e là $e = \frac{1}{1} + \frac{1}{1\cdot 1} + \frac{1}{1\cdot 1\cdot 2} + \frac{1}{1\cdot 1\cdot 2\cdot 3} + \ldots$.

Xét a là số tự nhiên > 2. Sử dụng đẳng thức $\frac{a - \sqrt{a^2-4}}{2} = \frac{1}{2} + \frac{a^2 - 2 - \sqrt{(a^2-2)^2 - 4}}{2a}$ suy ra với $a_1 = a$, $a_{n+1} = a_n^2 - 2\,(n = 1,2,\ldots)$ ta có

(24) $$\frac{a - \sqrt{a^2-4}}{2} = \frac{1}{a_1} + \frac{1}{a_1 a_2} + \frac{1}{a_1 a_2 a_3} + \ldots$$

Chuỗi này hội tụ rất nhanh vì bằng quy nạp ta có $a_n > 2^{2^{n-1}}$, $n = 1,2,\ldots$

Đặt biệt với $a = 3$ ta có $a_1 = 3$, $a_2 = 7$, $a_3 = 47$, $a_4 = 2207$, $a_5 = 4870847$ và cứ thế.

Vì vậy $\frac{3 - \sqrt{5}}{2} = \frac{1}{3} + \frac{1}{3\cdot 7} + \frac{1}{3\cdot 7\cdot 47} + \frac{1}{3\cdot 7\cdot 47\cdot 2207} + \ldots$

Khai triển này được gọi là chuỗi Pell (E.Lucas [2] trang 331).

Nếu a chẵn, $a = 2b$, $b > 1$ thì từ ***(24)*** ta có khai triển $b - \sqrt{b^2-1} = \frac{1}{2b_1} + \frac{1}{2b_1 2b_2} + \frac{1}{2b_1 2b_2 2b_3} + \ldots$

với $b_1 = b$ và $b_{n+1} = 2b_n^2 - 1$ với $n = 1,2,\ldots$

Ta có khai triển thành tích vô hạn sau đây $\sqrt{\frac{b+1}{b-1}} = \left(1 + \frac{1}{b_1}\right)\left(1 + \frac{1}{b_2}\right)\left(1 + \frac{1}{b_3}\right)\ldots$

Một số trường hợp riêng của khai triển này (ví dụ $b = 2$, $b = 3$ và một vài trường hợp khác) được trình bày bởi G.Cantor [2] năm 1869.

Bây giờ đặt x_0 là số vô tỷ thỏa mãn $0 < x_0 < 1$. Xét a_1 là số tự nhiên lớn nhất thỏa mãn $x_0 < \frac{1}{a_1}$. Đặt $x_1 = \frac{1}{a_1} - x_0$. Ta có $0 < x_1 < 1$. Ta tiếp tục quá trình này với x_1 và tìm được số tự nhiên lớn nhất a_2 thỏa mãn $x_1 < \frac{1}{a_2}$. Đặt $x_2 = \frac{1}{a_2} - x_1$ và tiếp tục như vậy. Ta thu được dãy vô hạn các số tự nhiên $a_1, a_2 \ldots$ và dãy vô hạn các số vô tỷ $x_1, x_2, \ldots$ thỏa mãn $0 < x_n < 1$ với $n = 0,1,2,\ldots$ và $x_n = \frac{1}{a_n} - x_{n-1}$ với $n = 1,2,\ldots$ Hơn nữa $\frac{1}{a_n + 1} < x_{n-1} < \frac{1}{a_n}$ với $n = 1,2,\ldots$ Vì vậy $-x_{n-1} < -\frac{1}{a_n + 1}$ do đó $\frac{1}{a_{n+1} + 1} < x_n < \frac{1}{a_n} - x_{n-1} < \frac{1}{a_n} - \frac{1}{a_n + 1} = \frac{1}{a_n (a_n + 1)}$. Suy ra $a_{n+1} + 1 > a_n (a_n + 1)$ và vì thế $a_{n+1} \geq a_n (a_n + 1)$ với $n = 1,2,\ldots$ Từ đây bằng quy nạp ta suy ra $a_{n+2} > 2^{2^n}$ với $n = 1,2,\ldots$ Số a_n tăng nhanh chóng tới vô hạn theo n. Từ định nghĩa của a_n và $x_n \, (n = 1,2,\ldots)$ suy ra

(25) $$x_0 = \frac{1}{a_1} - \frac{1}{a_2} + \frac{1}{a_3} - \ldots + \frac{(-1)^{n-1}}{a_n} + (-1)^n x_n .$$

Do $0 < x_n < \frac{1}{a_{n+1}}$ mà $\lim_{n \to \infty} a_{n+1} = +\infty$ suy ra $\lim_{n \to \infty} x_n = 0$. Vì vậy công thức ***(25)*** cho ta khai triển của số vô tỷ x_0 thành chuỗi hội tụ rất nhanh

(26) $$x_0 = \frac{1}{a_1} - \frac{1}{a_2} + \frac{1}{a_3} - \frac{1}{a_4} + \ldots$$

Trong đó $a_n \, (n = 1,2,\ldots)$ là các số tự nhiên thỏa mãn bất đẳng thức

(27) $$a_{n+1} \geq a_n (a_n + 1) \quad \text{với} \quad n = 1,2,\ldots$$

Ta đã chứng minh rằng mọi số vô tỷ $x_0, 0 < x_0 < 1$ đều biểu diễn được ở dạng ***(26)***. Có thể chứng minh mọi số vô tỷ nằm giữa 0 và 1 có đúng một biểu diễn dạng này và số thực x_0 có thể biểu diễn ở dạng ***(26)*** với $a_n \, (n = 1,2,\ldots)$ là các số tự nhiên thỏa mãn ***(27)*** sẽ là số vô tỷ (Sierpinski [4]).

CHƯƠNG 8

LIÊN PHÂN SỐ

1. Liên phân số và sự hội tụ của chúng

Các liên phân số đơn (hoặc gọn hơn là liên phân số) đã được xác định khi nghiên cứu thuật toán Euclid mục 9 Chương 1. Ở đây ta trình bày một phương pháp biểu diễn các số hữu tỷ như là các liên phân số đơn. Xét liên phân số đơn dạng tổng quát

(1) $$a_0+\frac{1|}{|a_1}+\frac{1|}{|a_2}+\ldots+\frac{1|}{|a_n},$$

với n là số tự nhiên cho trước, a_0 là số thực và $a_1,a_2,\ldots,a_n$ là các số dương. Số

(2) $$R_k=a_0+\frac{1|}{|a_1}+\frac{1|}{|a_2}+\ldots+\frac{1|}{|a_k},$$

với $k=1,2,\ldots,n$, được gọi là hội tụ thứ k của liên phân số ***(1)***. Suy ra hội thứ thứ 0 là $R_0=a_0$. Từ công thức ***(2)*** suy ra hội tụ thứ k R_k của liên phân số là một hàm $k+1$ biến $a_0,a_1,\ldots,a_k$ và với $k<n$ nếu thay số a_k bởi số $a_k+\frac{1}{a_{k+1}}$ thì hội tụ R_k trở thành hội tụ R_{k+1}. Đặt

(3)
$$\begin{aligned}
&P_0=a_0, && Q_0=1,\\
&P_1=a_0a_1+1, && Q_1=a_1,\\
&P_k=P_{k-1}a_k+P_{k-2}, && Q_k=Q_{k-1}a_k+Q_{k-2}
\end{aligned}$$

với $k=2,3,\ldots,n$. Bằng quy nạp ta chứng minh được P_k là hàm số của các biến $a_0,a_1,\ldots,a_k,Q_k$ là hàm số của $a_1,a_2,\ldots,a_k$. Hơn nữa P_k và Q_k là các đa thức hệ số nguyên với các biến ban đầu. Kiểm tra trực tiếp ta có

$$\frac{P_0}{Q_0}=\frac{a_0}{1}=R_0,\qquad \frac{P_1}{Q_1}=\frac{a_0a_1+1}{a_1}=a_0+\frac{1}{a_1}=R_1.$$

Ta chứng minh với mọi số dương $a_1,a_2,\ldots,a_n$ thì

(4) $$P_k/Q_k=R_k,\ k=0,1,2,\ldots,n,$$

Ở trên ta thấy đẳng thức này đúng với $k=0$ và $k=1$. Với $k=2$ đẳng thức cũng đúng từ ***(3)***; ta có

$$\frac{P_2}{Q_2}=\frac{P_1a_2+P_0}{Q_1a_2+Q_0}=\frac{(a_0a_1+1)a_2+a_0}{a_1a_2+1}=a_0+\frac{1}{a_1+\frac{1}{a_2}}=R_2.$$

Giả sử ***(4)*** đúng với $k=m$, $2\le m<n$. Suy ra với mọi số dương $a_1,a_2,\ldots,a_m$ ta có $R_m=P_m/Q_m$. Theo ***(3)*** thì đẳng thức

(5) $$R_m=\frac{P_{m-1}a_m+P_{m-2}}{Q_{m-1}a_m+Q_{m-1}}$$

đúng với mọi số dương $a_1,a_2,\ldots,a_m$. Đẳng thức ***(5)*** vẫn đúng nếu a_m thay bởi $a_m+\frac{1}{a_{m+1}}$ trong cả hai vế (vì $a_{m+1}>0$). Khi đó R_m trở thành R_{m+1} và do trong vế phải của đẳng thức thì các hàm số $P_{m-1},P_{m-2},Q_{m-1},Q_{m-2}$ không phụ thuộc a_m, ta có

$$R_{m+1}=\frac{P_{m-1}\left(a_m+\dfrac{1}{a_{m+1}}\right)+P_{m-2}}{Q_{m-1}\left(a_m+\dfrac{1}{a_{m+1}}\right)+Q_{m-2}}=\frac{\left(P_{m-1}a_m+P_{m-2}\right)a_{m+1}+P_{m-1}}{\left(Q_{m-1}a_m+Q_{m-2}\right)a_{m+1}+Q_{m-1}}.$$

Do đó theo ***(3)*** ta có $R_{m+1}=\dfrac{P_m a_{m+1}+P_{m-1}}{Q_m a_{m+1}+Q_{m-1}}=\dfrac{P_{m+1}}{Q_{m+1}}$, suy ra ***(4)*** đúng với $k=m+1.$

Theo quy nạp thì nó đúng với mọi $k=0,1,2,...,n$.

Viết $\Delta_k=P_{k-1}Q_k-Q_{k-1}P_k$, $k=1,2,...,m$. Ta có $\Delta_1=P_0Q_1-Q_0P_1=a_0a_1-(a_0a_1+1)=-1$. Nhưng theo ***(3)*** ta có $\Delta_k=P_{k-1}(Q_{k-1}a_k+Q_{k-2})-Q_{k-1}(P_{k-1}a_k+P_{k-2})=P_{k-1}Q_{k-2}-Q_{k-1}P_{k-2}=-\Delta_{k-1}$ với $k=2,3,...,n$, suy ra $\Delta_k=(-1)^k$ với $k=1,2,...,n$. Ta đã chứng minh được

(6) $$\Delta_k=P_{k-1}Q_k-Q_{k-1}P_k=(-1)^k \text{ với } k=1,2,...,n.$$

2. Biểu diễn một số vô tỷ thành liên phân số

Giả sử x là một số vô tỷ. Đặt $a_0=[x]$. Vì x là số vô tỷ nên $0<x-a_0<1$ suy ra $x_1=1/(x-a_0)$ là số vô tỷ >1. Đặt $a_1=[x_1]$. Rõ ràng $[x_1]$ là số tự nhiên và lập luận tương tự như trên suy ra số $x_2=1/(x_1-a_1)$ là số vô tỷ >1. Tiếp tục quá trình này ta nhận được dãy vô hạn $x_1,x_2,...$ các số vô tỷ lớn hơn 1 và dãy các số tự nhiên $a_n=[x_n]$ thỏa mãn $x_n=1/(x_{n-1}-a_{n-1})$, $n=1,2,...;$ $x_0=x$.

Ta có $x_{n-1}=a_{n-1}+\dfrac{1}{x_n}$, $n=1,2,...$ Dãy đẳng thức $x=a_0+\dfrac{1}{x_1}$, $x_1=a_1+\dfrac{1}{x_2}$, ..., $x_{n-1}=a_{n-1}+\dfrac{1}{x_n}$ suy ra

(7) $$x=a_0+\frac{1|}{|a_1}+\frac{1|}{|a_2}+...+\frac{1|}{|a_{n-1}}+\frac{1|}{|x_n}.$$

Đặt

(8) $$R_n=a_0+\frac{1|}{|a_1}+\frac{1|}{|a_2}+...+\frac{1|}{|a_n}.$$

So sánh ***(7)*** và ***(8)*** ta thấy nếu a_n trong ***(8)*** được thay bởi x_n, R_n trở thành x. P_k và Q_k được định nghĩa theo ***(3)***, với a_0 tùy ý và các số dương $a_1,a_2,...,a_n$ thì ta có $R_n=\dfrac{P_n}{Q_n}=\dfrac{P_{n-1}a_n+P_{n-2}}{Q_{n-1}a_n+Q_{n-2}}$.

Hơn nữa vì P_{n-1}, P_{n-2}, Q_{n-1} và Q_{n-2} không phụ thuộc a_n, thay a_n bởi x_n trong cả hai vế đẳng thức trên ta nhận được

(9) $$x=\frac{P_{n-1}x_n+P_{n-2}}{Q_{n-1}x_n+Q_{n-2}}.$$

Công thức này đúng với mọi số tự nhiên $n>1$ vì vậy thay n bởi $n+1$, ta có $x=\dfrac{P_n x_{n+1}+P_{n-1}}{Q_n x_{n+1}+Q_{n-1}}$, suy ra theo ***(6)*** thì

(10) $$x-R_n=\frac{P_n x_{n+1}+P_{n-1}}{Q_n x_{n+1}+Q_{n-1}}-\frac{P_n}{Q_n}=\frac{(-1)^n}{(Q_n x_{n+1}+Q_{n-1})Q_n}.$$

Từ đẳng thức này và bất đẳng thức $x_{n+1}>a_{n+1}$ suy ra

(11) $$\left|x-R_n\right|<\frac{1}{\left(Q_n\,a_{n+1}+Q_{n-1}\right)Q_n}=\frac{1}{Q_{n+1}\,Q_n}$$

Ta sẽ chứng minh $Q_k\geq k$ với mọi $k=1,2,\ldots$ Hiển nhiên điều này đúng với $k=1$ vì $Q_1=a_1$ là số tự nhiên. Nếu với số tự nhiên k bất đẳng thức $Q_k\geq k$ là đúng thì theo ***(3)***, $Q_k\left(k=0,1,2,\ldots\right)$ là số tự nhiên và ta có $Q_{k+1}=Q_k\,a_{k+1}+Q_{k-1}\geq Q_k+1\geq k+1$. Vì vậy theo quy nạp bất đẳng thức $Q_k\geq k$ đúng với mọi $k=1,2,\ldots$ Theo ***(11)*** ta có $\left|x-R_n\right|<\frac{1}{n\left(n+1\right)}$ với $n=1,2,\ldots$. Vì vậy $x=\lim\limits_{n\to\infty}R_n$.

Ta nói x được biểu diễn bởi liên phân số vô hạn

(12) $$x=a_0+\frac{1|}{|\,a_1}+\frac{1|}{|\,a_2}+\frac{1|}{|\,a_3}+\ldots$$

Vậy ta đã chứng minh mọi số vô tỷ x có thể biểu diễn như là một liên phân số đơn vô hạn, biểu diễn này nhận được dựa vào thuật toán nêu trên. Do $a_{n+1}=\left[x_{n+1}\right]>x_{n+1}-1$ và vì vậy $x_{n+1}<a_{n+1}+1$. Từ công thức ***(10)*** suy ra

(13) $$\begin{aligned}\left|x-R_n\right|&=\frac{1}{\left(Q_n\,x_{n+1}+Q_{n-1}\right)Q_n}>\frac{1}{\left(Q_n\left(a_{n+1}+1\right)+Q_{n-1}\right)Q_n}\\&=\frac{1}{Q_n\left(Q_{n+1}+Q_n\right)}.\end{aligned}$$

Nhưng do $a_{n+2}\geq 1$, thay n bởi $n+1$ trong ***(11)*** ta nhận được

(14) $$\left|x-R_{n+1}\right|<\frac{1}{\left(Q_{n+1}+Q_n\right)Q_{n+1}}.$$

Áp dụng tính chất $Q_{n+1}=Q_n\,a_n+Q_{n-1}>Q_n$ cho ***(13)*** và ***(14)*** suy ra

(15) $$\left|x-R_{n+1}\right|<\left|x-R_n\right|,\text{ với mọi }\quad n=1,2,3,\ldots$$

Nghĩa là với mọi hội tụ liên tiếp của x, thì hội tụ thứ hai sẽ cho xấp xỉ tốt hơn hội tụ trước. Công thức ***(10)*** chứng tỏ $x-R_n$ là số dương với n chẵn và là số âm với n lẻ. Nghĩa là các hội tụ chẵn thì nhỏ hơn x, trong khi đó hội tụ lẻ thì lớn hơn x. Kết hợp với bất đẳng thức ***(15)*** suy ra các hội tụ chẵn lập thành dãy tăng nghiêm ngặt và tiến tới x, trong khi dãy hội tụ lẻ giảm nghiêm ngặt.

Bây giờ ký hiệu a_0 là số nguyên tùy ý và $a_1,a_2,\ldots$ là dãy vô hạn các số tự nhiên tùy ý. Sử dụng lập luận ở trên với một số thay đổi ta kết luận nếu các số R_k xác định bởi ***(2),*** thì với mọi số tự nhiên $n,m>n$, ta có $\left|R_m-R_n\right|<\frac{1}{n\left(n+1\right)}$. Suy ra dãy vô hạn $R_n\left(n=1,2,\ldots\right)$ hội tụ, nghĩa là tồn tại giới hạn $x=\lim\limits_{n\to\infty}R_n$. Ta xét công thức ***(12)***. Vì vậy mọi liên phân số vô hạn ***(12)*** (với $a_1,a_2,\ldots$ là các số tự nhiên) đều biểu diễn một số thực. Bây giờ giả sử ***(12)*** ta viết

(16) $$x_n=a_n+\frac{1|}{|\,a_{n+1}}+\frac{1|}{|\,a_{n+2}}+\ldots\quad\text{với}\quad n=0,1,2,\ldots,$$

với $x_0=x$. Đặt

(17) $$R_k^{(n)}=a_n+\frac{1|}{|\,a_{n+1}}+\ldots+\frac{1|}{|\,a_{n+k}}\quad\text{với}\quad k=1,2,\ldots$$

Thế thì

(18) $\lim_{k\to\infty} R_{k+1}^{(n)} = x_n$ và $\lim_{k\to\infty} R_k^{(n+1)} = x_{n+1}$.

Nhưng rõ ràng $R_{k+1}^{(n)} = a_n + \dfrac{1}{R_k^{(n+1)}}$ suy ra theo ***(18)***

(19) $x_n = a_n + \dfrac{1}{x_{n+1}}$ với $n = 0,1,2,\ldots$

Ta cũng có $R_{k+2}^{(n)} = a_n + \dfrac{1}{R_{k+1}^{(n+1)}} = a_n + \dfrac{1}{a_{n+1} + \dfrac{1}{R_k^{(n+2)}}}$, nhưng vì $R_k^{(n+2)} \geq a_{n+2}$ nên $R_{k+2}^{(n)} \geq a_n + \dfrac{1}{a_{n+1} + \dfrac{1}{a_{n+2}}}$,

suy ra vì $\lim_{k\to\infty} R_{k+2}^{(n)} = x_n$, ta kết luận $x_n \geq a_n + \dfrac{1}{a_{n+1} + \dfrac{1}{a_{n+2}}}$. Hệ quả là $x_n > a_n$ với mọi $n = 0,1,2,\ldots$ Vì vậy $x_{n+1} > a_{n+1}$ và do đó $x_{n+1} > 1$ với $n = 1,2,\ldots$

Mặt khác theo ***(19)*** ta có $x_n < a_n + 1$. Vì vậy $a_n < x_n < a_n + 1$ với $n = 0,1,2,\ldots,$ suy ra $a_n = [x_n]$ với $n = 0,1,2,\ldots$ Từ đây theo ***(19)*** chứng tỏ nếu ***(12)*** là biểu diễn tùy ý của x thành liên phân số thì $x_1 = \dfrac{1}{x - a_0}$, $x_{n+1} = \dfrac{1}{x_n - a_n}$ với $n = 1,2,\ldots,$ và

(20) $a_n = [x_n]$ với $n = 0,1,2,\ldots$

Suy ra mọi số vô tỷ chỉ có thể biểu diễn một cách duy nhất thành liên phân số.

Bây giờ ta chứng minh mọi liên phân số vô hạn đều biểu diễn một số vô tỷ. Thật vậy ta giả sử số hữu tỷ $x = l/m$ (với $(l,m) = 1$) được biểu diễn ở dạng ***(12)***.

Ta thấy từ ***(12)*** suy ra ***(20)***. Do đó $a_0 = \left[\dfrac{l}{m}\right]$, $x_1 = \dfrac{1}{\dfrac{l}{m} - \left[\dfrac{l}{m}\right]} = \dfrac{m}{l - m\left[\dfrac{l}{m}\right]}$. Nhưng $\left[\dfrac{l}{m}\right] > \dfrac{l}{m} - 1$, suy ra $l - m\left[\dfrac{1}{m}\right] < l - m\left(\dfrac{l}{m} - 1\right) = m$. Hệ quả là nếu $x_1 = l_1/m_1$, l_1/m_1 là phân số tối giản thì $m_1 < m$. Vì vậy suy ra mẫu số của các số hữu tỷ $x_0, x_1, x_2, \ldots$ lập thành dãy giảm nghiêm ngặt, vô lý. Từ đây ta kết luận rằng số hữu tỷ không thể biểu diễn thành liên phân số vô hạn.

Ta có định lý sau đây

Định lý 1. *Mọi số vô tỷ có thể biểu diễn duy nhất thành một liên phân số vô hạn có dạng* ***(12)*** *(với a_0 là số nguyên và $a_1, a_2, \ldots$ là các số tự nhiên cho bởi công thức* ***(20)****). Ngược lại mọi liên phân số vô hạn đều biểu diễn một số vô tỷ.*

Với số vô tỷ với lũy thừa bậc 2 thì các biểu diễn thành liên phân số cũng được tính (ta sẽ thảo luận kỹ hơn trong mục 4). Rất ít số vô tỷ được chỉ rõ liên phân số của nó. Số e là một ví dụ. Ta đã có

$$e = 2 + \frac{1|}{|1} + \frac{1|}{|2} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|4} + \frac{1|}{|1} + \ldots + \frac{1|}{|1} + \frac{1|}{|2k} + \frac{1|}{|1} + \ldots$$

và

$$\frac{e^2 - 1}{e^2 + 1} = \frac{1|}{|1} + \frac{1|}{|3} + \frac{1|}{|5} + \frac{1|}{|7} + \ldots$$

Quy luật của dãy $a_0, a_1, a_2, \ldots$ trong liên phân số biểu diễn e^2 cũng được biết. Đó là dãy $7, 2, 1, 1, 3, 18, 5, 1, 1, 6, 30, \ldots, 2+3k, 1, 1, 3+3k, 18+12k, \ldots$

Không có quy luật tương tự cho số π. Trong trường hợp này G.Lochs [1] đã tính các số a_k với $k = 0,1,\ldots 968$. Số lớn nhất là $a_{431} = 20776$; tất cả các số ≤ 34 đều xuất hiện trong dãy và số 1 xuất hiện 393 lần. Sau đây là danh sách của 30 số đầu tiên: 3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, 1, 84, 2, 1, 1, 15, 3, 13, 1, 4. R.W.Gasper Jr. [1] đã tính a_k với $k \le 204103$. Số lớn nhất là $a_{156381} = 179136$.

Dễ dàng tìm điều kiện cần và đủ của số không nguyên x mà liên phân số biểu diễn x bắt đầu với a_1 bằng với số tự nhiên cho trước m. Thật vậy ta có $a_1 = [x_1] = \left[\dfrac{1}{x - a_0}\right]$; suy ra $a_1 = m$ khi và chỉ khi $m \le 1/(x - a_0) < m+1$, nghĩa là $a_0 + \dfrac{1}{m+1} < x \le a_0 + \dfrac{1}{m}$. Đặc biệt điều kiện để số x với $0 < x < 1$ có tham số đầu tiên trong biểu diễn dạng liên phân số bằng m là $\dfrac{1}{m+1} < x \le \dfrac{1}{m}$. Hệ quả là x phải thuộc khoảng có độ dài $1/m - 1/(m+1) = 1/(m(m+1))$.

Từ đây ta suy ra xác suất để phần tử đầu tiên bằng m là $1/(m(m+1))$. Từ đó với $m = 1$ thì xác suất này là $\dfrac{1}{2}$, với $m = 2$ xác suất là $\dfrac{1}{6}$, với $m = 3$ xác suất chỉ còn $\dfrac{1}{12}$, và cứ như vậy. Ta thấy xác suất này giảm dần khi m tiến tới vô cùng. Dễ dàng chứng minh xác suất mà phần tử đầu tiên > 10 là $\dfrac{1}{11}$. Đây là lý do vì sao phần tử đầu tiên a_1 thường là các chữ số nhỏ.

Phép tính toán các xác suất để phần tử thứ hai bằng một số tự nhiên cho trước m là khó hơn. Lưu ý rằng xác suất để chữ số thứ k trong biểu diễn liên phân số của một số thực trong hệ thập phân bằng với chữ số c là $\dfrac{1}{10}$ với mọi k và mọi chữ số c.

Sử dụng lý thuyết độ đo có thể chứng minh xác suất để giữa các phần tử của biểu diễn một số vô tỷ thành liên phân số đơn có hữu hạn (hoặc không có) phần tử nào bằng 1 là 0 (xem Hausdorff [1] trang 426). Tương tự xác suất để giữa các phần tử đó chỉ có hữu hạn số phân biệt cũng bằng 0.

3. Luật xấp xỉ tốt nhất

Bây giờ ta chứng minh định lý cho biết tầm quan trọng của liên phân số trong việc tìm xấp xỉ tốt nhất của các số vô tỷ. Cho trước số vô tỷ x và biểu diễn của nó dưới dạng liên phân số ***(12).*** Đặt r/s là số hữu tỷ xấp xỉ x tốt hơn hội tự thứ n R_n của x. Nói cách khác giả sử

(21) $$\left|x - \frac{r}{s}\right| < |x - R_n|.$$

Theo ***(15)*** ta có $|x - R_n| < |x - R_{n-1}|$, suy ra theo ***(21)*** ta có

(22) $$\left|x - \frac{r}{s}\right| < |x - R_{n-1}|$$

Nhưng ta đã biết x nằm giữa R_{n-1} và R_n. Vì vậy các bất đẳng thức ***(21)*** và ***(22)*** chứng minh rằng r/s cũng nằm giữa R_{n-1} và R_n. Vì vậy ta có

(23) $$\left|\frac{r}{s}-R_{n-1}\right|<\left|R_{n-1}-R_n\right|.$$

Nhưng từ ***(4)*** và ***(6)*** thì $\left|R_{n-1}-R_n\right|=\left|\frac{P_{n-1}}{Q_{n-1}}-\frac{P_n}{Q_n}\right|=\frac{\left|P_{n-1}Q_n-Q_{n-1}P_n\right|}{Q_{n-1}Q_n}=\frac{1}{Q_{n-1}Q_n}$, theo ***(23)*** suy ra

(24) $$\frac{\left|rQ_{n-1}-sP_{n-1}\right|}{sQ_{n-1}}<\frac{1}{Q_{n-1}Q_n}.$$

Số $rQ_{n-1}-sP_{n-1}$ là số nguyên khác 0 vì nếu ngược lại thì $r/s=R_{n-1}$, mâu thuẫn với ***(22)***. Vì vậy ta có $\left|rQ_{n-1}-sP_{n-1}\right|>1$; kết hợp với ***(24)*** suy ra $s>Q_n$. Ta đã chứng minh được

Định lý 2. *Giả sử số hữu tỷ r/s, r là số nguyên và s là số tự nhiên, là một xấp xỉ tốt hơn hội tụ thứ n $R_n\left(n\geq 1\right)$ của số vô tỷ x. Thế thì mẫu số s là lớn hơn mẫu số của hội tụ R_n.*

Định lý này được gọi là luật xấp xỉ tốt nhất.

Ví dụ, biểu diễn π thành liên phân số đơn ta thấy hội tụ thứ 2 của nó là $\frac{22}{7}$ vì vậy tỷ số $\frac{22}{7}$ xấp xỉ π tốt hơn mọi phân số có mẫu số ≤ 7. Tương tự xấp xỉ thứ 3 của nó là 355/113 suy ra đây là xấp xỉ của π tốt hơn mọi xấp xỉ hữu tỷ khác có mẫu số ≤ 113.

4. Liên phân số biểu diễn các căn bậc hai

Ký hiệu D là số tự nhiên không phải bình phương đúng của một số tự nhiên. Ta sử dụng thuật toán trình bày trong mục 2 và nhận được biểu diễn thành liên phân số của số vô tỷ $x=\sqrt{D}$. Ta có

(25) $$a_0=\left[\sqrt{D}\right],\ \sqrt{D}=a_0+\frac{1}{x_1};$$

Suy ra $x_1=\frac{1}{\sqrt{D}-a_0}=\frac{\sqrt{D}+a_0}{D-a_0^2}=\frac{\sqrt{D}+b_1}{c_1}$, ở đây $b_1=a_0,\ c_1=D-a_0^2$ và $c_1>0$ (bởi vì $a_0=\left[\sqrt{D}\right]<\sqrt{D}$, và D không phải bình phương đúng). Vì vậy

(26) $$D-b_1^2=c_1.$$

Hơn nữa ta có $a_1=\left[x_1\right]$ và $x_1=a_1+\frac{1}{x_2}$, suy ra theo ***(26)***

$$x_2=\frac{1}{x_1-a_1}=\frac{1}{\frac{\sqrt{D}+b_1}{c_1}-a_1}=\frac{c_1}{\sqrt{D}+b_1-a_1c_1}=\frac{c_1\left(\sqrt{D}+a_1c_1-b_1\right)}{D-\left(a_1c_1-b_1\right)^2}$$

$$=\frac{c_1\left(\sqrt{D}+a_1c_1-b_1\right)}{D-b_1^2-a_1^2c_1^2+2a_1b_1c_1}=\frac{\sqrt{D}+a_1c_1-b_1}{1-a_1^2c_1+2a_1b_1}=\frac{\sqrt{D}+b_2}{c_2}$$

Với $b_2=a_1c_1-b_1$ và $c_2=1-a_1^2c_1+2a_1b_1$. Với số tự nhiên $n>1$ ta viết

(27) $$b_{n+1}=a_nc_n-b_n,\ c_{n+1}=c_{n-1}-a_n^2c_n+2a_nb_n.$$

Ta sẽ chứng minh với $n>1$ thì đẳng thức sau là đúng

(28) $$D-b_n^2=c_{n-1}c_n$$

Thật vậy

$$D-b_2^2 = D-\left(a_1 c_1 - b_1\right)^2 = D-b_1^2 - a_1^2 c_1^2 + 2a_1 b_1 c_1$$
$$= c_1 - a_1^2 c_1^2 + 2a_1 b_1 c_1 = c_1\left(1-a_1^2 c_1 + 2a_1 b_1\right) = a_1 c_2.$$

Nếu với số tự nhiên $n>1$ ta có $D-b_n^2 = c_{n-1} c_n$ thì theo ***(27)*** ta có

$$D-b_{n+1}^2 = D-\left(a_n c_n - b_n\right)^2 = D-b_n^2 - a_n^2 c_n^2 + 2a_n b_n c_n$$
$$= c_{n-1} c_n - a_n^2 c_n^2 + 2a_n b_n c_n = c_n\left(c_{n-1} - a_n^2 c_n + 2a_n b_n\right) = c_n c_{n+1},$$

và theo quy nạp suy ra ***(28)***.

Giả thiết của D suy ra theo ***(28)*** thì $c_n \neq 0$ với mọi $n=1,2,\ldots$ Ta chứng minh

(29) $$x_n = \frac{\sqrt{D}+b_n}{c_n} \quad \text{với} \quad n=1,2,,,,$$

Ta đã chứng minh ***(29)*** đúng với $n=1$ và $n=2$. Giả sử nó đúng với $n>1$.

Khi đó theo ***(27)*** và ***(28)*** ta có

$$x_{n+1} = \frac{1}{x_n - a_n} = \frac{1}{\frac{\sqrt{D}+b_n}{c_n} - a_n} = \frac{c_n}{\sqrt{D}+b_n-a_n c_n} = \frac{c_n\left(\sqrt{D}+a_n c_n - b_n\right)}{D-\left(a_n c_n - b_n\right)^2} = \frac{\sqrt{D}+b_{n+1}}{c_{n+1}}$$

và công thức ***(29)*** đúng theo quy nạp. Ta đã biết c_1 là số tự nhiên, do đó vì $b_1 = a_0 = \left[\sqrt{D}\right] < \sqrt{D}$ và vì vậy $0<\sqrt{D}-b_1<1$, ta có $0<\left(\sqrt{D}-b_1\right)/c_1<1$ và vì $x_1>1$, ta có $\left(\sqrt{D}+b_1\right)/c_1>1$.

Vậy ta thấy $0<\frac{\sqrt{D}-b_1}{c_1}<1<\frac{\sqrt{D}+b_1}{c_1}$.

Bây giờ ta chứng minh công thức trên đúng với mọi số tự nhiên n, nghĩa là

(30) $$0<\frac{\sqrt{D}-b_n}{c_n}<1<\frac{\sqrt{D}+b_n}{c_n}$$

Công thức này đúng với $n=1$.

Giả sử nó đúng với số tự nhiên tùy ý n. Theo ***(29)*** ta có $\frac{\sqrt{D}+b_{n+1}}{a_{n+1}} = x_{n+1} > 1$. Từ ***(27)*** và ***(28)*** ta có

$$\frac{\sqrt{D}-b_{n+1}}{c_{n+1}} = \frac{D-b_{n+1}^2}{c_{n+1}\left(\sqrt{D}+b_{n+1}\right)} = \frac{c_n}{\sqrt{D}+b_{n+1}} = \frac{c_n}{\sqrt{D}+a_n c_n - b_n} = \frac{1}{\frac{\sqrt{D}-b_n}{c_n}+a_n},$$

nên $0<\frac{\sqrt{D}-b_{n+1}}{c_{n+1}}<1$, và vì ***(30)*** ta có $\frac{\sqrt{D}-b_n}{c_n}+a_n > a_n \geq 1$.

Vậy bất đẳng thức ***(30)*** đúng theo quy nạp.

Nếu $c_n<0$ với số tự nhiên n, thì theo ***(30)*** ta có $\sqrt{D}-b_n<0$ và $\sqrt{D}+b_n<0$, suy ra $2\sqrt{D}<0$, vô lý. Vì vậy $c_n>0$ với mọi $n=1,2,\ldots$. Hệ quả là $\sqrt{D}-b_n<c_n<\sqrt{D}+b_n$, vì vậy $\sqrt{D}-b_n<\sqrt{D}+b_n$ và do đó $b_n>0$ với $n=1,2,\ldots$. Hệ quả là từ ***(30)*** suy ra $b_n<\sqrt{D}$ và $c_n<\sqrt{D}+b_n<2\sqrt{D}$. Từ đây ta

suy ra số bộ các số tự nhiên b_n và c_n là nhỏ hơn $2D$. Vì vậy giữa các phần tử của dãy vô hạn ***(29)*** với $n=1,2,...$ chỉ có hữu hạn số phân biệt và mỗi số đó là nhỏ hơn $2D$. Suy ra giữa các số $x_1, x_2, ..., x_{2D}$ có ít nhất hai số bằng nhau. Hệ quả là tồn tại k và $s<2D$ thỏa mãn

(31) $$x_k = x_{k+s};$$

Từ $x_{n+1}=\dfrac{1}{x_n-\lfloor x_n\rfloor}$ với $n=1,2,...,$ ***(31)*** suy ra $x_{k+1}=x_{k+s+1}$ và tổng quát hơn $x_n=x_{n+s}$ với $n\ge k$.

Vì vậy dãy vô hạn $x_1, x_2, ...$ và dãy $a_1, a_{2,...}$ ($a_n=\lfloor x_n\rfloor$, $n=1,2,...$) đều là dãy tuần hoàn.

(32) $$x'_n=\frac{\sqrt{D}-b_n}{c_n} \quad \text{với} \quad n=1,2,...$$

Từ ***(29)*** suy ra nếu ta đổi dấu của $\sqrt{D}$, số x'_n trở thành $-x'_n$ và hệ quả là đẳng thức $x_n=a_n+1/x_{n+1}$ trở thành $-x'_n=a_n-1/x'_{n+1}$, đẳng thức này được viết lại thành $1/x'_{n+1}=a_n+x'_n$.

Từ ***(32)***, ***(30)*** và $0<x'_n<1$, ta có

(33) $$a_n=\left\lfloor\frac{1}{x'_{n+1}}\right\rfloor \quad x'_n=\frac{\sqrt{D}-b_n}{c_n} \quad \text{với} \quad n=1,2,...$$

Hơn nữa từ ***(31)*** suy ra $x'_k=x'_{k+s}$, ta có theo ***(33)*** với $k>1$ thì $a_{k-1}=\left\lfloor\dfrac{1}{x'_k}\right\rfloor=\left\lfloor\dfrac{1}{x'_{k+s}}\right\rfloor=a_{k+s-1}$.

Do $x_n=a_n+1/x_{n+1}$ và ***(31)*** suy ra $x_{k-1}=x_{k+s-1}$. Lặp lại lập luận này với $k>2$, ta nhận được $x_{k-2}=x_{k+s-2}$ và cứ như thế. Từ đây suy ra dãy $x_1, x_2, ...$ và do đó dãy $a_1, a_2, ...$ đều là các dãy tuần hoàn ngay từ phần tử đầu tiên (nghĩa là tại a_1 chứ không phải a_0). Vậy

(34) $$x_{n+s}=x_n \quad \text{và} \quad a_{n+s}=a_n \quad \text{với} \quad n=1,2,...$$

Dãy các công thức $$x_1=a_1+\frac{1}{x_2}, x_2=a_2+\frac{1}{x_3}, ..., x_s=a_s+\frac{1}{x_{s+1}}=a_s+\frac{1}{x_1}$$

$$\text{và } -x'_1=a_1-\frac{1}{x'_2}, -x'_2=a_2-\frac{1}{x'_3}, ..., -x'_s=a_s-\frac{1}{x'_{s+1}}=a_s-\frac{1}{x'_1}$$

hoặc tương đương $$\frac{1}{x'_2}=a_1+\frac{1}{\left(\dfrac{1}{x'_1}\right)}, \frac{1}{x'_3}=a_2+\frac{1}{\left(\dfrac{1}{x'_2}\right)}, ..., \frac{1}{x'_1}=a_s+\frac{1}{\left(\dfrac{1}{x'_s}\right)}$$

là hệ quả trực tiếp của công thức

(35)
$$x_1=a_1+\frac{1|}{|a_2}+...+\frac{1|}{|a_s}+\frac{1|}{|x_1},$$
$$\frac{1}{x'_1}=a_s+\frac{1|}{|a_{s-1}}+...+\frac{1|}{|a_1}+\frac{1|}{|\left(\dfrac{1}{x'_1}\right)}.$$

Nhưng theo ***(25)***, $\sqrt{D}=a_0+1/x_1$ và $-\sqrt{D}=a_0-1/x_1'$, suy ra $\sqrt{D}=-a_0+1/x_1'$. Vì vậy từ công thức ***(35)*** suy ra $\sqrt{D}=a_0+\dfrac{1|}{|a_1}+\dfrac{1|}{|a_2}+...+\dfrac{1|}{|a_s}+\dfrac{1|}{|x_1}$, $\sqrt{D}=a_s-a_0+\dfrac{1|}{|a_{s-1}}+\dfrac{1|}{|a_{s-2}}+...+\dfrac{1|}{|a_1}+\dfrac{1|}{|\left(\dfrac{1}{x_1'}\right)}$.

Vì $x_1>1$, $1/x_1'>1$, suy ra

(36) $$a_s=2\left[\sqrt{D}\right], a_1=a_{s-1},\ a_2=a_{s-2},...,a_{s-1}=a_1.$$

Vậy ta thấy dãy $a_1,a_2,...,a_{s-1}$ là đối xứng. Ta có định lý sau đây

Định lý 3. *Nếu D là số tự nhiên không phải bình phương đúng thì trong biểu diễn thành dạng liên phân số* $\sqrt{D}=a_0+\dfrac{1|}{|a_1}+\dfrac{1|}{|a_2}+...$, *dãy* $a_1,a_{2,...}$ *là tuần hoàn. Hơn nữa nếu chu kỳ tuần hoàn bắt đầu ngay từ* a_1 *và chứa* s *phần tử* $a_1,a_2,...,a_s$, *thì* $s<2D$, $a_s=2\left[\sqrt{D}\right]$ *và dãy* $a_1,a_2,...,a_{s-1}$ *đối xứng.*

Biểu diễn liên phân số của $\sqrt{D}$ thường được viết là $\sqrt{D}=\left(a_0;\overline{a_1,a_2,...,a_s}\right)$, dấu gạch ngang trên đầu chỉ ra đó là chu kỳ tuần hoàn. Tuy nhiên không phải chỉ các căn bậc hai của các số tự nhiên không phải bình phương đúng mới có tính chất như trên. Có thể chứng minh rằng lớp các số vô tỷ dương cũng có các tính chất trên thì trùng với lớp các căn bậc hai của các số hữu tỷ lớn hơn 1.

Ví dụ có thể kiểm tra $\sqrt{\dfrac{13}{2}}=\left(2;\overline{1,1,4}\right)$, $\sqrt{\dfrac{5}{3}}=\left(1;\overline{3,2}\right)$, $\sqrt{\dfrac{26}{5}}=\left(2;\overline{3,1,1,3,4}\right)$.

Các căn bậc hai vô tỷ không có tính chất trên chẳng hạn là $\dfrac{1+\sqrt{13}}{4}=\left(0;\overline{1,6,1,1}\right)$, $\dfrac{2+\sqrt{19}}{5}=\left(0;\overline{1,3,1,2,8,2}\right)$, $\dfrac{1+\sqrt{365}}{14}=\left(1;\overline{2,3,2}\right)$, $\sqrt{\dfrac{1}{2}}=\left(0;\overline{1,2}\right)$, $\dfrac{1+\sqrt{17}}{2}=\left(2;\overline{1,1,2}\right)$.

Bây giờ ta trình bày phương pháp tính các liên phân số của $\sqrt{D}$. Đầu tiên ta có

Bổ đề. *Nếu* k *là số tự nhiên và* x *là số thực thì*

(37) $$\left[\frac{x}{k}\right]=\left[\frac{[x]}{k}\right].$$

Chứng minh. Vì $[x]\le x$, ta có $\dfrac{[x]}{k}\le\dfrac{x}{k}$, do đó $\left[\dfrac{[x]}{k}\right]\le\left[\dfrac{x}{k}\right]$. Để chứng minh chiều ngược lại ta sử dụng bất đẳng thức $t-[t]<1$ với $t=\dfrac{[x]}{k}$. Ta có $\dfrac{[x]}{k}-\left[\dfrac{[x]}{k}\right]<1$, suy ra $[x]<k\left[\dfrac{[x]}{k}\right]+k$ và hệ quả là các số ở cả hai vế đều là số nguyên, $[x]\le k\left[\dfrac{[x]}{k}\right]+k-1$. Do $x<[x]+1$, suy ra $x<k\left[\dfrac{[x]}{k}\right]+k$ và vì $\left[\dfrac{x}{k}\right]<\left[\dfrac{[x]}{k}\right]+1$, suy ra $\left[\dfrac{x}{k}\right]\le\left[\dfrac{[x]}{k}\right]$, ta có điều phải chứng minh. □

Theo bổ đề và sử dụng ***(29)*** ta có $a_n=[x_n]=\left[\dfrac{\sqrt{D}+b_n}{c_n}\right]=\left[\dfrac{[\sqrt{D}]+b_n}{c_n}\right]=\left[\dfrac{a_0+b_n}{c_n}\right]$, nghĩa là

(38) $$a_n=\left[\frac{a_0+b_n}{c_n}\right] \text{ với } n=1,2,...$$

Vậy theo ***(27)*** và ***(28)***, ta nhận được thuật toán sau đây để tính liên phân số $\sqrt{D}$.

Đặt $a_0=\left[\sqrt{D}\right]$, $b_1=a_0$, $c_1=D-a_0^2$ *và ta lần lượt tìm các số* a_{n-1}, b_n, *và* c_n *bằng cách sử dụng* $a_{n-1}=\left[\frac{a_0+b_{n-1}}{c_{n-1}}\right]$, $b_n=a_{n-1}c_{n-1}-b_{n-1}, c_n=\frac{D-b_n^2}{c_{n-1}}$. *Ta xét dãy* $(a_2,c_2),(b_3,c_3),(b_4,c_4)$,... *và tìm chỉ số nhỏ nhất* s *mà* $b_{s+1}=b_1$ *và* $c_{s+1}=c_1$; *khi đó biểu diễn của* $\sqrt{D}$ *thành dạng liên phân số chính là* $\sqrt{D}=\left(a_0;\overline{a_1,a_2,...,a_s}\right)$. *Ta nhận được kết quả này sau một số hữu hạn phép tính hữu tỷ.*

Ghi chú. Vì chu kỳ khi bỏ ra phần tử cuối cùng mà ta đã biết là bằng $2\left[\sqrt{D}\right]$ là một dãy đối xứng, nên để tính chu kỳ ta chỉ cần tính các phần tử thuộc nửa đầu của dãy. Lưu ý này rất quan trọng trong thực hành. Có thể chứng minh rằng nếu s là số phần tử của chu kỳ là chẵn thì số $\frac{1}{2}s$ bằng với chỉ số k đầu tiên mà $b_{k+1}=b_k$; nếu s lẻ thì $\frac{1}{2}(s-1)$ là chỉ số k đầu tiên mà $c_{k+1}=c_k$ (T.Mulr, xem Perron [1] trang 91).

Ví dụ. Tính biểu diễn của $\sqrt{a^2-2}$ với a là số tự nhiên ≥ 3. Vì $(a-1)^2=a^2-2a+1<a^2-2<a^2$ do đó $a_0=\left[\sqrt{a^2-2}\right]=a-1$ nên $b_1=a_0=a-1$, $c_1=D-a_0^2=a^2-2-(a-1)^2=2a-3$ suy ra $a_1=\left[\frac{a_0+b_1}{c_1}\right]=\left[\frac{2a-2}{2a-3}\right]=\left[1+\frac{1}{2a-3}\right]=1$ (vì $a\geq 3$, ta có $2a-3\geq 3$).

Vậy $b_2=a_1c_1-b_1=2a-3-(a-1)=a-2$, $c_2=\frac{D-b_2^2}{c_1}=\frac{a^2-2-(a-2)^2}{2a-3}=\frac{4a-6}{2a-3}=2$,

$a_2=\left[\frac{a_0+b_2}{a_2}\right]=\left[\frac{a-1+a-2}{2}\right]=\left[a-\frac{3}{2}\right]=a-2$, suy ra $b_3=a_2c_2-b_2=(a-2)2-(a-2)=a-2$,

$c_3=\frac{D-b_3^2}{c_2}=\frac{a^2-2-(a-2)^2}{2}=\frac{4a-6}{2}=2a-3$, $a_3=\left[\frac{a_0+b_3}{c_3}\right]=\left[\frac{a-1+a-2}{2a-3}\right]=1$, suy ra

$b_4=a_3c_3-b_3=2a-3-(a-2)=a-1$, $c_4=\frac{D-b_4^2}{c_3}=\frac{a^2-2-(a-1)^2}{2a-3}=1$,

$a_4=\left[\frac{a_0+b_4}{c_4}\right]=\frac{a-1+a-1}{1}=2a-2$. vì vậy $b_5=a_4c_4-b_4=2a-2-(a-1)=a-1=b_1$,

$c_5=\frac{D-b_5^2}{c_4}=\frac{a^2-2-(a-1)^2}{1}=2a-3=c_1$. Vậy $b_5=b_1$ và $c_5=c_1$, suy ra $s=4$.

Vậy biểu diễn nhận được là

(39) $$\sqrt{a^2-2}=\left(a-1;\overline{1,a-2,1,2a-2}\right) \text{ với mọi số tự nhiên } a\geq 3.$$

Lưu ý rằng a_1 và a_3 (tổng quát hơn là a_n, n lẻ) không phụ thuộc vào a.

Công thức ***(39)*** không đúng với $a=2$. Thật vậy $\sqrt{2}=1+\dfrac{1}{1+\sqrt{2}}$ và do đó $\sqrt{2}=\left(1,\overline{2}\right)$. Thay 3,4,5 vào ***(39)*** ta nhận được các công thức $\sqrt{7}=\left(2;\overline{1,1,1,4}\right)$, $\sqrt{14}=\left(3;\overline{1,2,1,6}\right)$, $\sqrt{23}=\left(4;\overline{1,3,1,8}\right)$. Các biểu diễn sau đây tìm được bằng cách tương tự: $\sqrt{a^2+1}=\left(a;\overline{a,2a}\right)$ với mọi số tự nhiên a;

$$\sqrt{a^2-1}=\left(a-1;\overline{1,2a-2}\right),\ \sqrt{a^2-a}=\left(a-1;\overline{2,2a-2}\right) \text{ với } a=2,3,\ldots;$$

$$\sqrt{a^2+4}=\left(a;\overline{\frac{1}{2}(a-1),1,1,\frac{1}{2}(a-1),2a}\right) \text{ với mọi số lẻ } a>1;$$

$$\sqrt{a^2-4}=\left(a-1;1,\frac{1}{2}(a-3),2,\frac{1}{2}(a-3),1,2a-2\right) \text{với mọi số lẻ } a>3;$$

$$\sqrt{4a^2+4}=\left(2a;\overline{a,4a}\right) \text{ với mọi số tự nhiên } a;$$

$$\sqrt{(na)^2+a}=\left(na;\overline{2n,2an}\right),\sqrt{(na)^2+2a}=\left(na;\overline{n,2na}\right) \text{ với mọi số tự nhiên } a,n;$$

$$\sqrt{\left(na^2\right)^2-a}=\left(na-1;\overline{1,2n-2,1,2(na-1)}\right) \text{với mọi số tự nhiên } a \text{ và } n>1.$$

Bây giờ ta tìm tất cả các số tự nhiên D mà biểu diễn liên phân số của $\sqrt{D}$ chỉ chứa đúng một phần tử trong chu kỳ tuần hoàn. Từ tính chất ***(36)*** ta có $\sqrt{D}=\left(a;\overline{2a}\right)$, suy ra $\sqrt{D}=a+\dfrac{1}{a+\sqrt{D}}$, và do đó $D=a^2+1$. Vậy căn bậc hai $\sqrt{D}$ của một số tự nhiên chỉ có biểu diễn liên phân số với chu kỳ tuần hoàn gồm 1 phần tử khi và chỉ khi $D=a^2+1$, với a là số tự nhiên.

Dễ dàng tìm tất cả các số tự nhiên D mà biểu diễn của $\sqrt{D}$ thành liên phân số có chu kỳ tuần hoàn chứa đúng hai phần tử. Thật vậy theo ***(36)*** ta có $\sqrt{D}=\left(a;\overline{b,2a}\right)$ với $b\neq 2a$. Vì vậy $\sqrt{D}=a+\dfrac{1|}{|b}+\dfrac{1|}{|a+\sqrt{D}}$ và hệ quả là $D=a^2+\dfrac{2a}{b}$. Suy ra $2a=kb$, với k là số tự nhiên >1 vì $b\neq 2a$. Vì vậy ta kết luận rằng tất cả những số có căn bậc hai biểu diễn thành liên phân số đơn tuần hoàn chu kỳ hai phần tử đều có dạng $D=a^2+k$, với k là ước số lớn hơn 1 của 2a.

Bây giờ ta tìm tất cả các số tự nhiên mà biểu diễn liên phân số căn bậc hai của nó có 3 phần tử trong chu kỳ tuần hoàn. Giả sử D là số như vậy. Khi đó $\sqrt{D}=\left(a_0;\overline{a_1,a_2,2a_0}\right)$. Theo Định lý 3 thì dãy a_1,a_2 đối xứng. Ta có $a_1=a_2$ và hơn nữa $a_1\neq 2a_0$ vì nếu ngược lại thì chu kỳ của liên phân số của $\sqrt{D}$ chỉ chứa 1 phần tử. Suy ra công thức sau là đúng

(40) $$\sqrt{D}=a_0+\frac{1|}{|a_1}+\frac{1|}{|a_1}+\frac{1|}{|a_0+\sqrt{D}}$$

Lưu ý $\sqrt{D}$ là số vô tỷ nên đẳng thức trên tương đương với

(41) $$D=a_0^2+\frac{2a_0a_1+1}{a_1^2+1}.$$

Đây là tất cả các nghiệm cần tìm.

Ta sẽ chứng minh rằng số tự nhiên D có dạng ***(41)*** nếu và chỉ nếu a_1 là số chẵn và

(42) $a_0=\left(a_1^2+1\right)k+\dfrac{1}{2}a_1,$ với $k=1,2,\ldots$

Điều kiện đủ là đúng. Nếu a_1 là số chẵn thì công thức ***(42)*** đúng, do đó a_0 là số tự nhiên thỏa mãn $2a_0>a_1$ và $2a_0\,a_1+1=2\left(a_1^2+1\right)a_1\,k+a_1^2+1=\left(a_1^2+1\right)\left(2a_1\,k+1\right)$, suy ra số D có dạng ***(41)*** là số tự nhiên. Mặt khác nếu với số tự nhiên a_0 nào đó mà $a_1\neq 2a_0$ và số D có dạng ***(41)*** là số tự nhiên thì vì $2a_0\,a_1+1$ lẻ nên số a_1^2+1 (và các ước số của nó) cũng lẻ, do đó a_1 chẵn và vì D có dạng ***(41)*** là nguyên suy ra $\dfrac{2a_0\,a_1+1}{a_1^2+1}-1=\dfrac{\left(a_0-a_1/2\right)2a_1}{a_1^2+1}$ nguyên, số a_1^2+1 là ước của $\left(a_0-a_1/2\right)2a_1$. Nhưng $\left(2a_1,a_1^2+1\right)=1$ (vì a_1 chẵn); do đó $a_0-a_1/2$ chia hết cho a_1^2+1 và ta có $a_0-a_1/2=\left(a_1^2+1\right)k$ với số nguyên k nào đó. Suy ra công thức ***(42)*** đúng. Nhưng vì $2a_0\neq a_1$, ta phải có $k>0$ và do đó k là số tự nhiên. Điều kiện cần được chứng minh.

Định lý 4. *Tất cả các số tự nhiên D có biểu diễn liên phân số của $\sqrt{D}$ có chu kỳ tuần hoàn gồm ba phần tử được cho bởi công thức $D=\left(\left(a_1^2+1\right)k+a_1/2\right)^2+2a_1k+1$, với a_1 là số tự nhiên chẵn, $k=1,2,\ldots$ Khi đó $\sqrt{D}=\left(a_0;\overline{a_1,a_1,2a_0}\right)$.(Tổng quát của định lý này đối với trường hợp chu kỳ tuần hoàn gồm số lượng phần tử tùy ý có thể xem trong Perron [1] trang 88, Satz 3,17, tài liệu đã dẫn trang 89-90, xem thêm Drittes Beispiel đối với trường hợp $k=3$.)*

Không khó để chứng minh $D=\left(\left(a_1^2-1\right)k+a_1/2\right)^2+\left(2a_1k+1\right)^2$. Đặc biệt từ Định lý 4 suy ra mọi số tự nhiên D mà biểu diễn liên phân số của $\sqrt{D}$ có chu kỳ chứa 3 phần tử và 2 phần tử đầu tiên đều bằng 2 là các số $D=\left(5k+1\right)^2+4k+1$, với $k=1,2,\ldots$ Sử dụng Định lý 4 dễ dàng kiểm tra trong các số $D\leq 1000$ tồn tại đúng 7 số thỏa mãn $\sqrt{D}$ có thể biểu diễn thành liên phân số chu kỳ tuần hoàn gồm 3 phần tử. Đó là $41,130,269,370,458,697,986.$

Định lý 5. *Nếu s là số tự nhiên >1, $a_1,a_2,\ldots,a_{s-1}$ là phần đối xứng trong chu kỳ của biểu diễn dạng liên phân số của $\sqrt{D_0},D_0$ là số tự nhiên, thì tồn tại vô hạn số tự nhiên D mà $a_1,a_2,\ldots,a_{s-1}$ là phần đối xứng trong chu kỳ của liên phân số $\sqrt{D}$ (xem Kraitchik [1] trang 57-58).*

Chứng minh. Nếu $\sqrt{D_0}=a_0+\dfrac{1|}{|a_1}+\dfrac{1|}{|a_2}+\ldots+\dfrac{1\ |}{|a_{s-1}}+\dfrac{1\quad|}{|a_o+\sqrt{D}}$, thì nếu ký hiệu P_k/Q_k là hội tụ thứ k của $\dfrac{1|}{|a_1}+\dfrac{1|}{|a_2}+\ldots+\dfrac{1\ |}{|a_{s-1}}$ ta có $\sqrt{D_0}=a_0+\dfrac{P_{s-1}\left(a_0+\sqrt{D_0}\right)+P_{s-2}}{Q_{s-1}\left(a_0+\sqrt{D_0}\right)+Q_{s-2}}$ suy ra vì $\sqrt{D_0}$ là số vô tỷ nên $Q_{s-2}=P_{s-1}$ và $Q_{s-1}D_0=a_0\left(Q_{s-1}a_0+Q_{s-2}\right)+P_{s-1}a_0+P_{s-2}$ suy ra $D_0=a_0^2+\dfrac{a_0\left(Q_{s-2}+P_{s-1}\right)+P_{s-2}}{Q_{s-1}}$.

Đặt $a=a_0+Q_{s-1}k$ với $k=1,2,3,\ldots$ thì

$$\begin{aligned}\frac{a\left(Q_{s-2}+P_{s-1}\right)+P_{s-2}}{Q_{s-1}}&=\frac{a_0\left(Q_{s-2}+P_{s-1}\right)+P_{s-2}}{Q_{s-1}}+\left(Q_{s-2}+P_{s-1}\right)k\\&=D_0-a_0^2+\left(Q_{s-2}+P_{s-1}\right)k\end{aligned}$$

là số tự nhiên và $\leq 2a+1$. Lưu ý rằng $\dfrac{Q_{s-2}+P_{s-1}}{Q_{s-1}}<\dfrac{2Q_{s-1}}{Q_{s-1}}=2$ và $\dfrac{P_{s-2}}{Q_{s-1}}<1.$

Suy ra $D=a^2+\dfrac{a\left(Q_{s-2}+P_{s-1}\right)+P_{s-2}}{Q_{s-1}}$ là số tự nhiên và $\left[\sqrt{D}\right]=a$.

Hơn nữa $Q_{s-2}=P_{s-1}$ $\sqrt{D}=a+\dfrac{P_{s-1}\left(a+\sqrt{D}\right)+P_{s-2}}{Q_{s-1}\left(a+\sqrt{D}\right)+Q_{s-2}}$ nên $\sqrt{D}=a+\dfrac{1|}{|a_1}+\dfrac{1|}{|a_2}+\ldots+\dfrac{1|}{|a_{s-1}}+\dfrac{1|}{|a+\sqrt{D}}$.

Suy ra số

$$D=\left(a_0+Q_{s-1}k\right)^2+D_0-a_0^2+\left(Q_{s-2}+P_{s-1}\right)k$$
$$=Q_{s-1}^2k^2+\left(2a_0Q_{s-1}+Q_{s-2}+P_{s-1}\right)k+D_0$$

với $k=1,2,\ldots.,$ thỏa mãn điều kiện định lý. Điều phải chứng minh. □

Định lý 6. *Với mọi số tự nhiên s, tồn tại vô hạn số tự nhiên D mà biểu diễn $\sqrt{D}$ dưới dạng liên phân số có chu kỳ chứa đúng s phần tử.*

Bổ đề. *Nếu n là số tự nhiên >1 và $a_1,a_2,\ldots,a_n$ là dãy đối xứng các số tự nhiên và hơn nữa nếu P_k/Q_k ký hiệu hội tụ thứ k của liên phân số $\dfrac{1|}{|a_1}+\dfrac{1|}{|a_2}+\ldots+\dfrac{1|}{|a_n}$ thì $P_n=Q_{n-1}$.*

Chứng minh bổ đề. Theo ***(3)*** thì $Q_n=Q_{n-1}a_n+Q_{n-2}$, $Q_{n-1}=Q_{n-2}a_{n-1}+Q_{n-3},\ldots,$ $Q_2=a_2a_1+1, Q_1=a_1$. Vì vậy $\dfrac{Q_n}{Q_{n-1}}=a_n+\dfrac{1|}{|a_{n-1}}+\dfrac{1|}{|a_{n-2}}+\ldots+\dfrac{1|}{|a_2}+\dfrac{1|}{|a_1}$. Nhưng vì dãy $a_1,a_2,\ldots,a_n$ đối xứng suy ra $\dfrac{Q_n}{Q_{n-1}}=a_1+\dfrac{1|}{|a_2}+\ldots++\dfrac{1|}{|a_n}$ và do đó $\dfrac{Q_{n-1}}{Q_n}=\dfrac{1|}{|a_1}+\dfrac{1|}{|a_2}+\ldots+\dfrac{1|}{|a_n}=\dfrac{P_n}{Q_n}$ suy ra $P_n=Q_{n-1}$. Điều phải chứng minh. □

Ghi chú. Nếu ký hiệu 1 là Q_0 thì bổ đề cũng đúng với $n=1$.

Chứng minh định lý 6. Cho trước hai số tự nhiên k,n và đặt $a_1,a_2,\ldots,a_n$ là dãy các phần tử đều bằng $2k$. Từ bổ đề ta có $P_n=Q_{n-1}$. Với số nguyên $t\geq 0$ ký hiệu $y_t=Q_nt+k+\dfrac{1|}{|2k}+\dfrac{1|}{|2k}+\ldots+\dfrac{1|}{|2k}+\dfrac{1\quad|}{|Q_nt+k+y}$.

Vì $Q_{n-1}=P_n$, ta có $y_t-Q_nt-k=\dfrac{P_n\left(Q_nt+k+y_t\right)+P_{n-1}}{Q_n\left(Q_nt+k+y_t\right)+P_n}$.

Do đó $Q_n\left(y_t^2-\left(Q_nt+k\right)^2\right)=2P_n\left(Q_nt+k\right)+P_{n-1}$.

Đặc biệt vớI $t=0$ ta nhận được $Q_n\left(y_0^2-k^2\right)=2P_nk+P_{n-1}$.

Mặt khác, theo định nghĩa của $y_t, y_0=\left(k;\overline{2k}\right)=\sqrt{k^2+1}$. Hệ quả là $Q_n=2P_nk+P_{n-1}$ và do đó $y_t^2=\left(Q_nt+k\right)^2+2P_nt+1,$ suy ra $y_t=\sqrt{\left(Q_nt+k\right)^2+2P_nt+1}$. Vì vậy với số tự nhiên k và số nguyên $t\geq 0$ thì biểu diễn liên phân số của căn bậc hai của $D=\left(Q_nt+k\right)^2+2P_nt+1$ có chu kỳ chứa đúng $n+1$ phần tử và mỗi phần tử đều bằng $2k$. Lưu ý chu kỳ $\left(k;\overline{2k}\right)=\sqrt{k^2+1}$ chỉ có duy nhất một phần tử. Suy ra Định lý 6 được chứng minh. □

Ví dụ với $k=1$ và $n=1,2,3,4,5,6$ ta có với $t=0,1,2,\ldots,$ tương ứng (xem Kraitchik [1] trang 57)

$$\sqrt{(2t+1)^2+2t+1} = (2t+1;\overline{2, 4t+2}),$$
$$\sqrt{(5t+1)^2+4t+1} = (5t+1;\overline{2, 2, 10t+2}),$$
$$\sqrt{(12t+1)^2+10t+1} = (12t+1;\overline{2, 2, 2, 24t+2}),$$
$$\sqrt{(29t+1)^2+24t+1} = (29t+1;\overline{2, 2, 2, 2, 58t+2}),$$
$$\sqrt{(70t+1)^2+58t+1} = (70t+1;\overline{2, 2, 2, 2, 2, 140t+2}),$$
$$\sqrt{(169t+1)^2+140t+1} = (169t+1;\overline{2, 2, 2, 2, 2, 2, 338t+2}).$$

Vì vậy với $t=1$, ta có

$$\sqrt{12} = (3;\overline{2, 6}), \quad \sqrt{41} = (6;\overline{2, 2, 12}),$$
$$\sqrt{180} = (13;\overline{2, 2, 2, 26}), \quad \sqrt{925} = (30;\overline{2, 2, 2, 2, 60}).$$

Dễ dàng chứng minh với mọi số n có dạng $3k$ hoặc $3k+1$ tồn tại vô hạn số tự nhiên D thỏa mãn biểu diễn của $\sqrt{D}$ thành liên phân số có chu kỳ chứa $n+1$ phần tử mà n phần tử đầu tiên đều bằng 1 (Sierpinski [26] trang 300).

Ví dụ ta có với $t=1,2,\ldots$ thì $\sqrt{(89t-44)^2+110t-54} = \left(89t-44;\overline{1,1,1,1,1,1,1,1,1,178t-88}\right)$.

Vì vậy với $t=1$ thì $\sqrt{2081} = \left(45;\overline{1,1,1,1,1,1,1,1,1,90}\right)$.

W.Patz [1] đã lập bảng biểu diễn thành liên phân số của tất cả các số vô tỷ $\sqrt{D}$, với $D<10000$. Từ bảng đó cho thấy trong 100 số tự nhiên đầu tiên thì chu kỳ dài nhất là

$$\sqrt{94} = \left(9;\overline{1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18}\right),$$

Chu kỳ này chứa 16 phần tử.

Số $\sqrt{919}$ có chu kỳ 60 phần tử

$$\sqrt{919} = (30;\overline{3, 5, 1, 2, 1, 2, 1, 1, 1, 2, 3, 1, 19, 2, 3, 1, 1, 4, 9, 1,}$$
$$\overline{7, 1, 3, 6, 2, 11, 1, 1, 1, 29, 1, 1, 1, 11, 2, 6, 3, 1, 7, 1,}$$
$$\overline{9, 4, 1, 1, 3, 2, 19, 1, 3, 2, 1, 1, 1, 2, 1, 2, 1, 5, 3, 60)}$$

(Kraitchik [1] trang 57 tính toán sai số thành 62).

Số $\sqrt{991}$ có chu kỳ 60 phần tử

$$\sqrt{991} = (31;\overline{2, 12, 10, 2, 2, 2, 1, 1, 2, 6, 1, 1, 1, 1, 3, 1, 8, 4, 1, 2, 1,}$$
$$\overline{2, 3, 1, 4, 1, 20, 6, 4, 31, 4, 6, 20, 1, 4, 1, 3, 2, 1, 2,}$$
$$\overline{1, 4, 8, 1, 3, 1, 1, 1, 1, 6, 1, 1, 2, 2, 2, 10, 12, 2, 62}).$$

Dễ thấy $\sqrt{1000} = \left(31;\overline{1,1,1,1,1,6,2,2,15,2,2,15,2,2,6,1,1,1,1,1,62}\right)$.

Mọi nghiệm vô tỷ của đa thức bậc hai với hệ số nguyên gọi là số vô tỷ bậc hai. Nếu x là số thực thỏa mãn phương trình $Ax^2+Bx+C=0$, với A,B,C là các số nguyên thì ta đã biết $D=B^2-4AC>0$ và D không là bình phương đúng. Ta có $x=\left(-B\pm\sqrt{D}\right)/2A$.

Định lý Lagrange sau đây được chứng minh với một số thay đổi từ chứng minh Định lý 3*: biểu diễn liên phân số của một số vô tỷ bậc hai thực là tuần hoàn. Ngược lại mọi liên phân số tuần hoàn biểu diễn một số vô tỷ bậc hai thực (Lagrange, Kraïtchik [1] trang 9-13).*

Ví dụ. Ta có $\frac{1}{2}\left(\sqrt{5}+1\right)=\left(1;\overline{1}\right)$. Kết quả này suy ra từ $\frac{1}{2}\left(\sqrt{5}+1\right)=1+1/\left(\frac{1}{2}\left(\sqrt{5}+1\right)\right)$.

Bài tập. ***1.*** Chứng minh rằng mọi số thực là tổng của hai số mà mỗi số đều có biểu diễn liên phân số với thương số đầu tiên = 1.

Chứng minh. Trong mục 3 ta thấy phần tử đầu tiên của liên phân số = 1 khi và chỉ khi $t-[t]\ge\frac{1}{2}$ (vì nếu $t-[t]=1/2$ thì suy ra $t=[t]+\frac{1|}{|1}+\frac{1|}{|1}$). Với số thực x ta đặt $u=\frac{1}{2}\left(x-[x]\right)+\frac{1}{2}$, $v=[x]-1+u$. Khi đó $x=u+v$ và vì $0\le x-[x]<1$ ta có $\frac{1}{2}\le u<1$ suy ra $[v]=[x]-1$, và do đó $v-[v]=u\ge\frac{1}{2}$. Từ các bất đẳng thức này ta suy ra điều phải chứng minh. □

Ghi chú. M.Hall, Jr. [1] đã chứng minh rằng mỗi số thực là tổng của hai số mà mỗi số đều có biểu diễn liên phân số với phần tử đầu tiên không lớn hơn 4. Tuy nhiên ngay cả khi x đã tính được chính xác tới $1/10^{100}$ thì một cách tổng quát ta vẫn chưa tìm được phần tử đầu tiên trong biểu diễn liên phân số của nó. Thật vậy vì ta mới chỉ biết $0<x<1/10^{100}$ nên ta chỉ có thể kết luận $1/x>10^{100}$ nghĩa là phần tử đầu tiên là $\ge 10^{100}$.

2. Chứng minh rằng không tồn tại số tự nhiên D mà $\sqrt{D}$ có thể biểu diễn thành liên phân số với chu kỳ tuần hoàn chứa 6 phần tử mà 5 phần tử đầu tiên bằng 1.

Chứng minh. Giả sử $\sqrt{D}=a_0+\frac{1|}{|1}+\frac{1|}{|1}+\frac{1|}{|1}+\frac{1|}{|1}+\frac{1|}{|1}+\frac{1}{|a_0+\sqrt{D}}$. Ký hiệu P_n/Q_n là hội tụ thứ n của liên phân số $\frac{1|}{|1}+\frac{1|}{|1}+\ldots$. Ta có $\sqrt{D}-a_0=\frac{P_5\left(a_0+\sqrt{D}\right)+P_4}{Q_5\left(a_0+\sqrt{D}\right)+Q_4}=\frac{5\left(a_0+\sqrt{D}\right)+3}{8\left(a_0+\sqrt{D}\right)+5}$ nên $D=a_0^2+\frac{10a_8+3}{8}$, vô lý vì số lẻ $10a_0+3$ không chia hết cho 8. □

3. Ký hiệu $f(s)$ là số tự nhiên nhỏ nhất D mà chu kỳ của liên phân số $\sqrt{D}$ chứa s phần tử. Tính giá trị của $f(s)$ với $s\le 10$

Lời giải.

$f(1)=2,\sqrt{2}=(1;\overline{2});\ f(2)=3,\sqrt{3}=(1;\overline{1,2});\ f(3)=41,\sqrt{41}=(6;\overline{2,2,12});$
$f(4)=7,\sqrt{7}=(2;\overline{1,1,1,4});\ f(5)=13,\sqrt{13}=(3;\overline{1,1,1,1,6});\ f(6)=19,\sqrt{19}=(4;\overline{2,1,3,1,2,8});\ f(7)=58,\sqrt{58}=(7;\overline{1,1,1,1,1,1,14});\ f(8)=31,\sqrt{31}=(5;\overline{1,1,3,5,3,1,1,10});\ f(9)=106,\sqrt{106}=(10;\overline{3,2,1,1,1,1,2,3,20});\ f(10)=43,\sqrt{43}=(6;\overline{1,1,3,1,5,1,3,1,1,12}).$

5. Sử dụng liên phân số $\sqrt{D}$ để giải các phương trình $x^2-Dy^2=1$ và $x^2-Dy^2=-1$

Giả sử D là số tự nhiên không phải bình phương đúng. Đặt $\sqrt{D}=\left(a_0;\overline{a_1,a_2,\ldots,a_s}\right)$ và P_k/Q_k là hội tụ thứ k. Ta có $\sqrt{D}=a_0+\frac{1|}{|a_1}+\frac{1|}{|a}+\ldots+\frac{1|}{|a_{s-1}}+\frac{1}{|a_s-a_0+\sqrt{D}}$ vì vậy

$$\sqrt{D}=P_{s-1}\left(a_s-a_0+\sqrt{D}\right)+P_{s-2}Q_{s-1}\left(a_s-a_0+\sqrt{D}\right)+Q_{s-2}$$

và tổng quát hơn vì $a_0=a_s-a_0$, $\sqrt{D}=\frac{P_{ks-1}(\sqrt{D}+a_0)+P_{ks-2}}{Q_{ks-1}(\sqrt{D}+a_0)+Q_{ks-2}}$ với $k=1,2,3,\ldots$, mà $\sqrt{D}$ là số vô tỷ nên $a_0Q_{ks-1}-P_{ks-1}=-Q_{ks-2}$ và $DQ_{ks-1}-a_0P_{ks-1}=P_{ks-2}$. Nhân đẳng thức thứ nhất với $-P_{ks-1}$ và đẳng thức thứ hai với $-Q_{ks-1}$ sau đó cộng lại và sử dụng ***(6)*** ta suy ra

$$P_{ks-1}^2-DQ_{ks-1}^2=Q_{ks-2}-P_{ks-1}-P_{ks-2}Q_{ks-1}=(-1)^{ks}.$$

Nếu s lẻ thì suy ra

(43) $P_{ks-1}^2-DQ_{ks-1}^2$ bằng -1 với k lẻ và bằng 1 với k chẵn

Nếu s chẵn thì

(44) $P_{ks-1}^2-DQ_{ks-1}^2=1$ với mọi $k=1,2,3,...$

Vì vậy ta thấy các hội tụ của liên phân số của $\sqrt{D}$ là nghiệm tự nhiên của $x^2-Dy^2=1.$

Ta chứng minh điều ngược lại cũng đúng, nghĩa là mọi nghiệm tự nhiên của phương trình trên cho ta tử số và mẫu số của hội tụ của liên phân số $\sqrt{D}$.

Thật vậy giả sử t và u là nghiệm tự nhiên của $x^2-Dy^2=1.$ Ta có $t>u$. Đặt

(45) $$\frac{t}{u}=\frac{1|}{|b_1}+\frac{1|}{|b_2}+...+\frac{1\ |}{|b_{k-1}}$$

là biểu diễn của số t/u thành liên phân số ta có k chẵn. Biểu diễn như vậy là tồn tại vì nếu $k-1$ chẵn thì với $b_{k-1}>1$ số $b_{k-1}-1+\frac{1|}{|1}$ có thể thay thế vị trí của b_{k-1}, và với $b_{k-1}=1$ thì số $b_{k-2}+1$ có thể thay thế vị trí của $b_{k-2}+\frac{1\ |}{|b_{k-1}}$.

Ký hiệu t'/u' là hội tụ cuối cùng của liên phân số ***(45)***. Thế thì

(45ª) $$\frac{t'}{u'}=b_0+\frac{1\ |}{|b_1}+\frac{1\ |}{|b_2}+...+\frac{1\ |}{|b_{k-2}}$$

Ta có $u'<u$. Với $k=2$ ta có $t'/u'=b_0$) vì k chẵn sử dụng ***(6)*** ta có $tu'-ut'=1.$

Bây giờ trừ cả hai vế của dẳng thức cuối cùng cho $t^2-Du^2=1,$ ta nhận được

(46) $$t(u'-t)=u(t'-Du)$$

Theo ***(45)*** ta có $0<t/u-b_0\le 1$, suy ra

(47) $$0<t-b_0u\le u$$

Do t và u nguyên tố cùng nhau (vì $t^2-Du^2=1$) suy ra với số nguyên l thì các đẳng thức sau là đúng

(48) $$u'-t=lu,\quad t'-Du=lt$$

Vì vậy

(49) $$u'-(t-b_0u)=(l+b_0)u$$

Từ các bất đẳng thức $0<u'<u$ và ***(47)*** ta suy ra $|u'-(t-b_0u)|<u$, và theo ***(49)*** ta có $l+b_0=0$, do đó $l=-b_0$, vì vậy theo ***(48)*** thì $u'=t-b_0u,\quad t'=Du-b_0t,$ và hệ quả là

(50) $$\frac{t(b_0+\sqrt{D})+t'}{u(b_0+\sqrt{D})+u'}=\frac{t\sqrt{D}+Du}{t+u\sqrt{D}}=\sqrt{D};$$

Nhưng theo ***(45)*** và ***(45$^{\alpha}$)*** thì vế trái của ***(50)*** trở thành $b_0+\dfrac{1|}{b_1}+\dfrac{1|}{|b_2}+\ldots+\dfrac{1\ |}{|b_{k-1}}+\dfrac{1\quad|}{|b_0+\sqrt{D}}$; do đó theo ***(50)*** thì ta có liên phân số $\sqrt{D}=\left(b_0;\overline{b_1,b_2,\ldots,b_{k-1},2b_0}\right)$, hội tụ thứ $k-1$ của nó là ***(45)***. Ở trên ta đã chỉ ra số k bằng với số các phần tử trong chu kỳ của liên phân số $\sqrt{D}$. Chu kỳ này không nhất thiết là nhỏ nhất. Ký hiệu s là chu kỳ nhỏ nhất của liên phân số. Rõ ràng $s\,|\,k$ và do đó $k=sn$, với n là số tự nhiên. Với mọi nghiệm tự nhiên của phương trình $x^2-Dy^2=1$ là t và u, thì phân số t/u là hội tụ của liên phân số $\sqrt{D}$; đúng hơn nó là hội tụ thứ $ns-1$ với s là số các phần tử của chu kỳ ngắn nhất của liên phân số và n là số tự nhiên. Ở trên ta đã chứng minh (công thức ***(44)***) nếu s là số chẵn thì mọi hội tụ thứ $ns-1$ $(n=1,2,\ldots)$ đều là nghiệm tự nhiên của $x^2-Dy^2=1$. Ta có định lý sau đây

Định lý 7. *Nếu chu kỳ của liên phân số $\sqrt{D}$ chứa s chẵn phần tử thì tử số và mẫu số của hội tụ thứ $ns-1$ với $n=1,2,\ldots$, tạo thành nghiệm tự nhiên của phương trình $x^2-Dy^2=1$. Hơn nữa tất cả các nghiệm đều có thể nhận được theo cách này.*

Từ đây ta thấy nghiệm nhỏ nhất của phương trình cho bởi hội tụ thứ $s-1$. Nếu s lẻ thì công thức ***(43)*** chứng tỏ tử số và mẫu số của hội tụ thứ $ns-1$ tạo thành nghiệm của $x^2-Dy^2=1$ chỉ khi n chẵn. Vì vậy ta có

Định lý 8. *Nếu chu kỳ của liên phân số $\sqrt{D}$ chứa lẻ phần tử thì tử số và mẫu số của hội tụ $2ns-1$, $n=1,2,\ldots$ tạo thành nghiệm tự nhiên của $x^2-Dy^2=1$. Hơn nữa mọi nghiệm là nhận được theo cách này.*

Vì vậy nghiệm nhỏ nhất được cho bởi hội tụ thứ $2ns-1$. Biểu diễn của $\sqrt{991}$ thành liên phân số được trình bày ở trên. Ta thấy chu kỳ của nó gồm 60 phần tử. Sử dụng biểu diễn này và Định lý 7 có thể tính được nghiệm tự nhiên nhỏ nhất của phương trình $x^2-991y^2=1$ (Chương 2 mục 15). Nghiệm này là x có 30 chữ số và y có 29 chữ số. Bây giờ ta chuyển sang phương trình

(51) $$x^2-Dy^2=-1$$

Giả sử $D=a^2+1$, với a là số tự nhiên >1. Như ta đã biết ta có $\sqrt{a^2+1}=\left(a;\overline{2a}\right)$. Vì vậy nếu P_k/Q_k là hội tụ thứ k của $\left(a;\overline{2a}\right)$, thì theo ***(43)***, với $s=1$, ta có

$$P_{k-1}^2-DQ_{k-1}^2=-1,\qquad k=1,3,5,\ldots$$

Vì vậy nghiệm tự nhiên nhỏ nhất của phương trình là số $t=P_0=a,\ u=Q_0=1$. Với các nghiệm tự nhiên khác của ***(51)*** là t,u ta có $u>1$. Nếu $D\neq a^2+1,a$ là số tự nhiên thì nếu t và u là nghiệm tự nhiên của phương trình ***(51)*** thì ta có $u>1$ vì nếu u=1 ta có $t^2-D=-1$ suy ra $D=t^2+1$, mâu thuẫn với giả thuyết của D. Vì vậy ta có thể giả sử t và u là nghiệm tự nhiên của ***(51)*** với $u>1$. Ký hiệu ***(45)*** là liên phân số của t/u, thì k lẻ. Ta xét t'/u' theo ***(45$^{\alpha}$)***. Vì k lẻ ta có $tu'-ut'=-1$, suy ra vì $t^2-Du^2=-1$, ta nhận lại ***(46)***. Lập luận tương tự được sử dụng chứng tỏ ***(45)*** là hội tụ thứ $k-1$ của liên phân số $\sqrt{D}$ và $k=sn$, trong đó s là số các phần tử (nhỏ nhất) trong chu kỳ của liên phân số $\sqrt{D}$ và n là số tự nhiên. Nhưng nếu s chẵn thì theo ***(44)*** ta thấy không có hội tụ thứ $sn-1$ nào cho ta nghiệm của ***(51)***. Nếu ngược lại là s lẻ thì theo ***(43)*** hội tụ thứ $sn-1$ cho nghiệm của ***(51)*** với n lẻ. Vậy ta có định lý

Định lý 9. *Nếu chu kỳ của liên phân số $\sqrt{D}$ có s phần tử và s chẵn thì phương trình **(51)** không có nghiệm tự nhiên. Nếu s lẻ thì tử số và mẫu số của các hội tụ thứ $((2n-1)s-1), n=1,2,\ldots$ tạo thành nghiệm tự nhiên của **(51)**. Hơn nữa tất cả các nghiệm là nhận được theo cách này.*

Ví dụ. *1*. Đặt $D = 2$. Vì $D = \left(1; \overline{2}\right)$, ta có $s = 1$ và do đó theo Định lý 7 suy ra tử số và mẫu số của hội tụ thứ $2n-1, n = 1, 2, \ldots$ tạo thành nghiệm tự nhiên của $x^2 - 2y^2 = 1$ và hơn nữa mọi nghiệm là nhận được theo cách này. Hội tụ đầu tiên là $1 + \frac{1}{2} = \frac{3}{2}$ cho nghiệm tự nhiên nhỏ nhất $x = 3, y = 2$. Theo Định lý 9 thì tử số và mẫu số của mọi hội tụ thứ $2n-2$. $n = 1, 2, \ldots,$ tạo thành nghiệm tự nhiên của phương trình $x^2 - 2y^2 = -1$ và mọi nghiệm nhận được theo cách này. Hội tụ thứ 0 là $1/1$ cho nghiệm tự nhiên nhỏ nhất của phương trình.

2. Đặt $D = 3$. Khi đó $\sqrt{3} = \left(1; \overline{1, 2}\right)$. Ta có $s = 2,$ và theo Định lý 7 thì tử số và mẫu số của hội tụ thứ $2n-1,$ $n = 1, 2, \ldots$ tạo thành nghiệm của phương trình $x^2 - 3y^2 = 1$ và tất cả các nghiệm nhận dược theo cách này. Nghiệm tự nhiên nhỏ nhất được cho bởi hội tụ đầu tiên, nghĩa là $1 + \frac{1}{1} = \frac{3}{2}$, suy ra $x = 3, y = 2$. Tuy nhiên theo Định lý 9 thì phương trình $x^2 - 3y^2 = -1$ không có nghiệm tự nhiên.

3. Đặt $D = 13$. Khi đó $\sqrt{13} = \left(3; \overline{1, 1, 1, 1, 6}\right)$. Ta có $s = 5$ và theo Định lý 8 thì tử số và mẫu số của mọi hội tụ thứ $10n-1,$ $n = 1, 2, \ldots,$ cho nghiệm của phương trình $x^2 - 13y^2 = 1,$ và tất cả các nghiệm nhận được theo cách này. Nghiệm tự nhiên nhỏ nhất cho bởi hội tụ thứ 9, nghĩa là số $3 + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|6} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} = \frac{649}{180}$ suy ra $x = 649, y = 180$. Từ Định lý 9 suy ra tử số và mẫu số của mọi hội tụ thứ $10n-6,$ $n = 1, 2, \ldots,$ đều là nghiệm của phương trình $x^2 - 13y^2 = -1$ và tất cả các nghiệm nhận được theo cách này. Nghiệm tự nhiên nhỏ nhất cho bởi hội tụ thứ 4, nghĩa là số $3 + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} = \frac{18}{5}$ suy ra $x = 18, y = 5$.

Không khó để tìm tất cả các nghiệm tự nhiên nhỏ nhất của phương trình $x^2 - Dy^2 = -1$ bằng cách sử dụng biểu diễn liên phân số của $\sqrt{D}$ với $D < 100$. Bảng các nghiệm với $D \le 1003$ được cho bởi Legendre [1]. Đây là bảng các nghiệm tự nhiên nhỏ nhất của phương trình $x^2 - Dy^2 = 1$ với $D \le 40$

D	x	y
2	3	2
3	2	1
5	9	4
6	5	2
7	8	3
8	3	1
10	19	6
11	10	3
12	7	2
13	649	180
14	15	4

D	x	y
15	4	1
17	33	8
18	17	4
19	170	39
20	9	2
21	55	12
22	197	42
23	24	5
24	5	1
26	51	10
27	26	5

D	x	y
28	127	24
29	4901	1820
30	11	2
31	1520	273
32	17	3
33	23	4
34	35	6
35	6	1
37	73	12
38	37	6
39	25	4
40	19	3

Từ Định lý 8 suy ra phương trình $x^2 - Dy^2 = -1$ là có nghiệm tự nhiên với $D \le 100$ chỉ khi D nhận các giá trị $2, 5, 10, 13, 17, 26, 29, 37, 41, 50, 53, 58, 61, 65, 73, 74, 82, 85, 89, 97.$

6. Liên phân số dạng phức

Ta nghiên cứu các phân số có dạng

(52) $$a_0 + \frac{b_1|}{|a_1} + \frac{b_2|}{|a_2} + \ldots + \frac{b_n|}{|a_n}$$

với $a_0, a_1, \ldots, a_n, b_1, b_2, \ldots, b_n$ các các số thực hoặc phức tùy ý. Ta cần có điều kiện sau để các biểu thức là có nghĩa

$$a_n \neq 0, \quad a_{n-1} + \frac{b_n}{a_n} \neq 0, \quad a_{n-2} + \frac{b_{n-2}|}{|a_{n-2}} + \frac{b_n}{a_n} \neq 0, \ldots, \quad a_1 + \frac{b_2}{a_2} + \ldots + \frac{b_n}{a_n} \neq 0.$$

Ta thấy một số (hoặc tất cả) các số $a_1, a_2, \ldots, a_{n-1}$ có thể bằng 0.

Ví dụ liên phân số $\frac{1|}{|0} + \frac{1|}{|0} + \ldots + \frac{1|}{|0} + \frac{1|}{|2} = 2.$

Có thể chứng minh liên phân số

(53) $$R_n = a_0 + \frac{b_1|}{|a_1} + \frac{b_2|}{|a_2} + \ldots + \frac{b_n|}{|a_n}$$

được định nghĩa tốt nếu các số P_k và $Q_k \left(k = 0,1,\ldots,n\right)$ được cho bởi công thức truy hồi

$$P_0 = a_0,\ Q_0 = 1,\ P_1 = a_0 a_1 + b_1,\ Q_1 = a_1,$$
$$P_k = P_{k-1} a_k + P_{k-2} b_k,\ Q_k = Q_{k-1} a_k + Q_{k-2} b_k,\ k = 2,3,\ldots,n,$$

Thế thì $R_n = \frac{P_n}{Q_n}$ và $P_{k-1} Q_k - Q_{k-1} P_k = (-1)^k b_1 b_2 \ldots b_k$ với $k = 1,2,\ldots,n.$

Lưu ý rằng nếu liên phân số ***(52)*** được định nghĩa tốt thì các hội tụ riêng của nó có thể không có tính chất đó. Ví dụ liên phân số $\frac{1|}{|1} + \frac{-1|}{|\ 1} + \frac{1|}{|1} = 2$ nhưng các tổng riêng $\frac{1|}{|1} + \frac{-1|}{|\ 1}$ không xác định.

Nếu các dãy $a_0, a_1, a_2, \ldots$ và $b_1, b_2, \ldots$ đều là dãy vô hạn và nếu dãy các số ***(53)*** hội tụ tới giới hạn là x, thì x được gọi là giới hạn của liên phân số vô hạn

(54) $$x = a_0 + \frac{b_1|}{|a_1} + \frac{b_2|}{|a_2} + \ldots$$

Các liên phân số như vậy được trình bày bởi các công thức của Brouncker cho $\pi/4$ vào năm 1655.

Ta có $$\frac{\pi}{4} = \frac{1|}{|1} + \frac{1^2|}{|\ 2} + \frac{3^2|}{|\ 2} + \frac{5^2|}{|\ 2} + \ldots$$

và $$\log 2 = \frac{1|}{|1} + \frac{1^2|}{|1} + \frac{2^2|}{|1} + \frac{3^2|}{|1} + \ldots$$

Công thức thứ nhất được suy ra từ công thức

$$\frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \ldots + \frac{(-1)^{n-1}}{2n-1} = \frac{1|}{|1} + \frac{1^2|}{|2} + \frac{3^2|}{|2} + \frac{5^2|}{|2} \ldots + \frac{(2n-3)^2|}{|2}$$

và công thức quen thuộc của Leibniz cho $\pi/4$.

Công thức sau cho bởi công thức

$$\frac{1}{1} - \frac{1}{2} + \frac{1}{3} - \ldots + \frac{(-1)^{n-1}}{n} = \frac{1|}{|1} + \frac{1^2|}{|1} + \frac{2^2|}{|1} + \frac{3^2|}{|1} + \ldots \frac{(n-1)^2|}{|\quad 1}$$

với mọi số tự nhiên n (Sierpinski [7] phần 2 trang 140).

Bây giờ ta chuyển sang nghiên cứu một số trường hợp đặc biệt của liên phân số có dạng ***(54)***.

Với số thực x_0 thì ký hiệu $G(x_0)$ là số nguyên nhỏ nhất $> x_0$. Ta có $x_0 < G(x_0) \le x_0 + 1$, do đó $0 < G(x_0) - x_0 \le 1$ và hệ quả là $x_1 = \dfrac{1}{G(x_0) - x_0} \ge 1$. Vì vậy $G(x_1) \ge 2$. Lặp lại thủ tục này với x_1 thay cho x_0 và cứ như vậy. Vì vậy nếu $x_n = \dfrac{1}{G(x_{n-1}) - x_{n-1}}$ với $n = 1, 2, \ldots$, ta có $x_n \ge 1$ và $G(x_n) \ge 2, n = 1, 2, \ldots$ Hơn nữa $x_0 = G(x_0) + \dfrac{-1\ |}{|\ G(x_1)} + \dfrac{-1\ |}{|\ G(x_2)} + \ldots + \dfrac{-1\ |}{|\ G(x_{n-1})} + \dfrac{-1|}{|\ x_n}$.

Từ đây suy ra liên phân số vô hạn của x_0

(55) $$x_0 = G(x_0) + \frac{-1\ |}{|\ G(x_1)} + \frac{-1\ |}{|\ G(x_2)} + \frac{-1\ |}{|\ G(x_2)} + \ldots$$

Vì vậy ta đã thấy mọi số thực x đều có thể biểu diễn thành liên phân số vô hạn

$$x = a_0 - \frac{1|}{|\ a_1} - \frac{1|}{|\ a_2} - \frac{1|}{|\ a_3} - \ldots,$$

với a_0 là số nguyên và a_n là các số tự nhiên ≥ 2. Có thể chứng minh rằng mọi số thực có đúng một biểu diễn như vậy. Đặc biệt ta có $1 = 2 - \dfrac{1|}{|\ 2} - \dfrac{1|}{|\ 2} - \dfrac{1|}{|\ 2} - \ldots$

Với mọi số hữu tỷ thì trong biểu diễn dạng ***(55)*** của chúng ta có $G(x_n) = 2$ với n đủ lớn.

Công thức $\sqrt{2} = 2 - \dfrac{1|}{|\ 2} - \dfrac{1\ |}{|\ 2 + \sqrt{2}}$ cho ta biểu diễn của $\sqrt{2}$ thành liên phân số với chu kỳ gồm 2 phần tử $\sqrt{2} = 2 - \dfrac{1|}{|\ 2} - \dfrac{1|}{|\ 4} - \dfrac{1|}{|\ 2} - \dfrac{1|}{|\ 4} - \ldots$.

Một dạng biểu diễn khác của số thực x thành liên phân số nhận được với a_0 là số nguyên gần x nhất và x_1 là số cho bởi công thức $x = a_0 \pm 1/x_1$ với các dấu $+$ và $-$ được chọn tùy thuộc $x > a_0$ hay $x < a_0$. Với x_1 xác định ta định nghĩa a_1 và x_2 tương tự như vậy và cứ như thế (Hurwitz [1]).

Biểu diễn dạng này của $\sqrt{2}$ trùng với biểu diễn liên phân số đơn $\sqrt{2}$. Với $\sqrt{3}$ ta có $\sqrt{3} = 2 - \dfrac{1|}{|\ 4} - \dfrac{1|}{|\ 4} - \ldots$ nghĩa là biểu diễn vẫn có dạng ***(55)***. Với $\sqrt{5}$ ta nhận lại biểu diễn liên phân số đơn của $\sqrt{5}$. Với $\sqrt{7}$ ta có $\sqrt{7} = 3 - \dfrac{1|}{|\ 3} - \dfrac{1|}{|\ 6} - \dfrac{1|}{|\ 3} - \ldots$, nghĩa là có dạng ***(55)***. Nhưng với $\sqrt{13}$ ta có $\sqrt{13} = 4 - \dfrac{1|}{|\ 3} - \dfrac{1|}{|\ 2} + \dfrac{1|}{|\ 7} - \dfrac{1|}{|\ 3} - \dfrac{1|}{|\ 2} + \dfrac{1|}{|\ 7} - \ldots$, biểu diễn này không có dạng ***(55)*** và cũng không phải liên phân số đơn.

Để kết thúc chương này ta xét liên phân số

$$a_0 + \cfrac{a_1 + \cfrac{a_2 + \ldots}{b_2}}{b_1} = a_0 + \frac{|\ a_1}{b_1|} + \frac{|\ a_2}{b_2|} + \ldots = a_0 + \frac{a_1}{b_1} + \frac{a_2}{b_1 b_2} + \frac{a_3}{b_1 b_2 b_3} + \ldots.$$

Ký hiệu $b_1, b_2, \ldots$ là dãy vô hạn các số tự nhiên mà trong đó có vô hạn phần tử khác 1. Ký hiệu x_0 là số thực và đặt $a_0 = [x_0], a_1 = [b_1(x_0 - a_0)]$. Rõ ràng a_1 là số nguyên $< b_1$. Đặt $x_1 = b_1(x_0 - a_0) - a_1$.

Ta có $0 \le x_1 < 1$. Trong trường hợp tổng quát giả sử với số tự nhiên $n > 1$ ta có số x_{n-1}; khi đó đặt $a_n = \left[b_n x_{n-1}\right]$ và $x_n = b_n x_{n-1} - a_n$. Vì vậy dãy $a_1, a_2, \ldots$ được định nghĩa bằng quy nạp và các phần tử của nó là các số nguyên không âm thỏa mãn $a_n < b_n$, cũng vậy dãy $x_1, x_2, \ldots$ là dãy các số thực với $0 \le x_n < 1$, với mọi $n = 1, 2, \ldots$.

Ta nhận được

(56) $$x_0 = a_0 + \frac{a_1}{b_1} + \frac{a_2}{b_1 b_2} + \ldots + \frac{a_n}{b_1 b_2 \ldots b_n} + \frac{x_n}{b_1 b_2 \ldots b_n}$$

Theo giả thiết các số $b_1, b_2, \ldots$ đều là số tự nhiên và có vô hạn số trong các số đó là ≥ 2. Vì vậy tích $b_1 b_2 \ldots b_n$ tăng tới vô hạn theo n. Hơn nữa vì $0 \le x_n < 1$, công thức ***(56)*** cho biểu diễn của x_0 thành chuỗi vô hạn

(57) $$x_0 = a_0 + \frac{a_1}{b_1} + \frac{a_2}{b_1 b_2} + \frac{a_3}{b_1 b_2 b_3} + \ldots,$$

Nghĩa là liên phân số vô hạn

(58) $$x_0 = a_0 + \frac{|a_1}{b_1|} + \frac{|a_2}{b_2|} + \ldots$$

Từ đây ta có định lý: *với mọi dãy vô hạn các số tự nhiên $b_1, b_2, \ldots$ mà vô hạn các phần tử trong đó là khác 1 thì mọi số thực x_0 đều có thể biểu diễn thành liên phân số có dạng **(58)** với $a_0 = \left[x_0\right]$, $a_n \left(n = 1, 2, \ldots\right)$ là các số nguyên $0 \le a_n < b_n$ với $n = 1, 2, \ldots$*. Dễ thấy biểu diễn dạng ***(57)*** trùng với biểu diễn thập phân với cơ số biến thiên trong Chương 7 mục 6.

CHƯƠNG 9

KÝ HIỆU LEGENDRE VÀ KÝ HIỆU JACOBI

1. Ký hiệu Legendre $\left(\frac{D}{p}\right)$ và các tính chất

Giả sử p là một số nguyên tố lẻ và D là số nguyên không chia hết cho p, ký hiệu Legendre $\left(\frac{D}{p}\right)$ nhận giá trị bằng 1 nếu D là thặng dư bậc hai modulo p và nhận giá trị bằng -1 trong trường hợp ngược lại. Theo Định lý 4 Chương 5 ta có

(1) $$\left(\frac{D}{p}\right) \equiv D^{\frac{1}{2}(p-1)} \pmod{p}$$

Suy ra $\left(\frac{D}{p}\right)$ bằng 1 nếu và chỉ nếu $D^{(p-1)/2}$ chia p dư 1. Theo Định lý 15 Chương 6 ta có

(2) $$\left(\frac{D}{p}\right) = (-1)^{ind\, D},$$

trong đó chỉ số *ind D* được lấy tương ứng theo căn nguyên thủy của p. Nếu D và D' là các số tự nhiên không chia hết cho p thì từ ***(1)*** suy ra các tính chất sau

I. *Nếu* $D \equiv D' \pmod{p}$ *thì* $\left(\frac{D}{p}\right) = \left(\frac{D'}{p}\right)$

Từ ***(2)*** suy ra nếu D và D' là các số nguyên không chia hết cho p thì

(3) $$\left(\frac{DD'}{p}\right) = (-1)^{idcDD'} \text{ và } \left(\frac{D}{p}\right)\left(\frac{D'}{p}\right) = (-1)^{idc\, D + idc\, D'}$$

Nhưng theo tính chất II của các chỉ số (Chương 6 mục 8) ta có $\text{ind}\, DD' \equiv ind\, D + ind\, D' \pmod{p-1}$.

Do p là số nguyên tố lẻ ta có $\text{ind}\, DD' \equiv ind\, D + ind\, D' \pmod{2}$, suy ra $(-1)^{ind\, DD'} = (-1)^{ind\, D + ind\, D'}$.

Từ đó theo ***(3)*** ta có $\left(\frac{DD'}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{D'}{p}\right)$. Vậy ta đã chứng minh

II. *Nếu* D *và* D' *là các số nguyên không chia hết cho* p *thì* $\left(\frac{DD'}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{D'}{p}\right)$.

Bây giờ ta chứng minh (Sierpinski [2]) nếu $\left\{\frac{D}{p}\right\}$ là số thực định nghĩa bởi số nguyên tố lẻ p và mọi số nguyên D không chia hết cho p thì nó khác 0 với ít nhất một giá trị của D và khác 1 với ít nhất một giá trị của D. Hơn nữa nó cũng thỏa mãn các điều kiện

1'. *Nếu* $D \equiv D' \pmod{p}$ *thì* $\left\{\frac{D}{p}\right\} = \left\{\frac{D'}{p}\right\}$

2'. $\left\{\frac{DD'}{p}\right\} = \left\{\frac{D}{p}\right\}\left\{\frac{D'}{p}\right\}$ *với mọi* D *và* D' *không chia hết cho p*

Khi đó với mọi số nguyên D không chia hết cho p ta có

(4) $$\left\{\frac{D}{p}\right\}=\left(\frac{D}{p}\right).$$

Giả sử g là căn nguyên thủy của p.

Với mọi số nguyên D không chia hết cho p ta có $D=g^{ind\,D}\pmod p$.

Theo các tính chất **1',2'** của $\left\{\frac{D}{p}\right\}$ ta có

(5) $$\left\{\frac{D}{p}\right\}=\left\{\frac{g^{ind\,D}}{p}\right\}=\left\{\frac{g}{p}\right\}^{ind\,D}$$

Đặt $\left\{\frac{g}{p}\right\}=a$. Do $g^{p-1}\equiv 1\pmod p$, theo **1',2'** ta có $a^{p-1}=\left\{\frac{g}{p}\right\}^{p-1}=\left\{\frac{g^{p-1}}{p}\right\}=\left\{\frac{1}{p}\right\}$, nhưng theo **2'** thì $\left\{\frac{1}{p}\right\}^2=\left\{\frac{1}{p}\right\}$ suy ra $\left\{\frac{1}{p}\right\}=0$ hoặc $\left\{\frac{1}{p}\right\}=1$. Ta không thể có $\left\{\frac{1}{p}\right\}=0$ vì nếu như vậy thì theo **2'** (với $D'=1$) ta sẽ có $\left\{\frac{D}{p}\right\}=\left\{\frac{D}{p}\right\}\left\{\frac{1}{p}\right\}=0$ mâu thuẫn với giả thiết $\left\{\frac{D}{p}\right\}$ không đồng nhất 0 (nếu D không chia hết cho p). Vì vậy $\left\{\frac{1}{p}\right\}=1$ và do đó $a^{p-1}=1$. Nhưng $a=\left\{\frac{g}{p}\right\}$ là số thực và phương trình $x^{p-1}=1$, p lẻ, có ít nhất hai nghiệm là 1 và -1. Suy ra $a=1$ hoặc $a=-1$. Nếu $a=1$ thì theo ***(5)*** với mọi số nguyên D không chia hết cho p ta có $\left\{\frac{D}{p}\right\}=1$, mâu thuẫn với giả thiết $\left\{\frac{D}{p}\right\}$ không đồng nhất 1 (D không chia hết cho p). Từ đó ta phải có $a=-1$ suy ra theo ***(5)*** thì $\left\{\frac{D}{p}\right\}=(-1)^{ind\,D}$. Bởi vậy từ ***(2)*** ta có $\left\{\frac{D}{p}\right\}=\left(\frac{D}{p}\right)$. Định lý được chứng minh.

Từ đó ta thấy mọi tính chất của ký hiệu Legendre có thể nhận được từ ***I, II*** và nhận xét $\left\{\frac{D}{p}\right\}$ không đồng nhất 1 hoặc 0 với mọi số nguyên tố lẻ p.

Từ công thức ***(1)*** suy ra

III. $$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}$$

Để có thêm một số tính chất của ký hiệu Legendre ta chứng minh kết quả sau

Bổ đề Gauss. $\left(\frac{D}{p}\right)=(-1)^{\lambda}$ *với* λ *là số các dư modulo* p *xuất hiện trong dãy*

(6) $$D,2D,3D,\ldots,\frac{1}{2}(p-1)D$$

mà không vượt quá $p/2$.

Chứng minh. Với $k=1,2,\ldots,(p-1)/2$, ký hiệu r_k là số dư của kD khi chia cho p. Đặt $Q_k=r_k$ nếu $r_k<p/2$ và $Q_k=p-r_k$ nếu $r_k>p/2$. Không xảy ra trường hợp $r_r=p/2$ vì p là số nguyên tố lẻ.

Do D không chia hết cho p và trong dãy ***(6)*** thì các hệ số của D là số tự nhiên $\le (p-1)/2$ nên các tổng và hiệu của các phần tử trong dãy ***(6)*** đều không chia hết cho p. Vì vậy dễ thấy tổng và hiệu của các phần tử của dãy sau cũng thế

(7) $$\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_{\frac{p-1}{2}}$$

Nhưng theo định nghĩa của $\mathcal{Q}_k$ thì chúng đều lớn hơn 0 và nhỏ hơn $(p-1)/2$ (vì $\mathcal{Q}_k = r_k < p/2$ nên $2\mathcal{Q}_k < p$, nghĩa là $2\mathcal{Q}_k \le p-1$ hoặc $\mathcal{Q}_k = p - r_k$ và $r_k > p/2$ lại suy ra $\mathcal{Q}_k < p/2$). Từ đó ta suy ra các phần tử của ***(7)*** chính là các số $1, 2, \ldots, (p-1)/2$. Vì vậy

(8) $$\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_{\frac{p-1}{2}} = \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!\ D^{p-1} \pmod p$$

Các đồng dư thức được suy ra từ định lý Fermat nhỏ $D^{p-1} \equiv 1 \pmod p$.

Ký hiệu λ_k bằng 0 hoặc 1 nếu như $r_k < p/2$ hoặc $r_k > p/2$ tương ứng.

Theo định nghĩa của $\mathcal{Q}_k$ ta có

(9) $$\mathcal{Q}_k \equiv (-1)^{\lambda_k} r_k \pmod p$$

Nhưng theo định nghĩa của r_k, $r_k \equiv kD \pmod p$. Vì vậy theo ***(9)*** ta có

(10) $$\mathcal{Q}_1 \mathcal{Q}_2 \cdots \mathcal{Q}_{\frac{p-1}{2}} \equiv (-1)^{\lambda_1 + \lambda_2 + \ldots + \lambda_{(p-1)/2}} \pmod p$$

Các công thức ***(8)*** và ***(9)*** kết hợp với việc $\left(\frac{p-1}{2}\right)! D^{(p-1)/2}$ không chia hết cho p suy ra

(11) $$D^{\frac{p-1}{2}} \equiv (-1)^{\lambda_1 + \lambda_2 + \ldots + \lambda_{(p-1)/2}} \pmod p$$

Nhưng theo định nghĩa của λ_k thì số $\lambda = \lambda_1 + \lambda_2 + \ldots + \lambda_{(p-1)/2}$ chính là số các phần dư $> \frac{p}{2}$ nhận được khi chia các số trong dãy ***(6)*** lần lượt cho p. Mặt khác, vế trái của ***(11)*** đồng dư với $\left(\frac{D}{p}\right) \pmod D$. Từ đó ***(11)*** trở thành đồng dư thức $\left(\frac{D}{p}\right) \equiv (-1)^{\lambda} \pmod p$.

Bây giờ để chứng minh $\left(\frac{D}{p}\right) = (-1)^{\lambda}$ ta chỉ cần để ý $\left(\frac{D}{p}\right)$ bằng 1 hoặc -1 và p là số nguyên tố lẻ ≥ 3. Bổ đề được chứng minh. □

Các số λ_k xác định như trên thỏa mãn $(-1)^{\lambda_k} = (-1)^{[2kD/p]}$. Thật vậy, nếu $r_k < p/2$ thì $\lambda_k = 0$ và mặt khác theo định nghĩa của r_k suy ra với số nguyên t_k ta có $kD = pt_k + r_k$. Từ đó $2kD/p = 2t_k + 2r_k/p$ và do $0 < 2r_k < p, [2kD/p] = 2t_k$ ta có $(-1)^{\lambda_k} = (-1)^{[2kD/p]}$. Nếu $r_k > p/2$ thì $1 < 2r_k/p < 2$ (vì $r_k < p$) suy ra $[2r_k/p] = 1$ và $[2kD/p] = 2t_k + 1$. Nếu $r_k > p/2$ ta có $\lambda_k = 1$ suy ra công thức $(-1)^{\lambda_k} = (-1)^{[2kD/p]}$. Vì công thức ở trên đúng với mọi $k = 1, 2, \ldots, (p-1)/2$ ta có $(-1)^{\lambda} = (-1)^{\lambda_1 + \lambda_2 + \ldots + \lambda_{(p-1)/2}} = (-1)^{\sum_{k=1}^{(p-1)/2} [2kD/p]}$. Do đó bổ đề Gauss dẫn tới

Hệ quả. $\left(\frac{D}{p}\right)=(-1)^{\sum_{k=1}^{(p-1)/2}[2kD/p]}$

Đặc biệt nếu $D=2$. Từ hệ quả ta có

(12) $$\left(\frac{2}{p}\right)=(-1)^{\lambda} \text{ với } \lambda=\sum_{k=1}^{(p-1)/2}[4k/p]$$

Nếu $1\le k<p/4$ thì $0<4k/p<1$ và do đó $[4k/p]=0$. Đẳng thức $k=p/4$ không thể có vì p lẻ. Với $[p/4]<k\le(p-1)/2$ ta có $1<4k/p\le 2(p-1)/p<2$; hệ quả là $[4k/p]=1$. Từ đây ta suy ra trong các hạng tử của λ trong công thức ***(12)*** có $(p-1)2-[p/4]$ hạng tử bằng 1, các hạng tử còn lại bằng 0. Hệ quả là $\lambda=(p-1)/2-[p/4]$. Nhưng với p lẻ ta có $\frac{p-1}{2}=\left[\frac{p}{4}\right]\equiv\frac{p^2-1}{8}(\bmod 2)$. Thật vậy mọi số p lẻ đều có dạng $8k+1,8k+3,8k+5,8k+7$, với k là số tự nhiên.

Viết $f(p)=\frac{p-1}{2}-\left[\frac{p}{4}\right]$ và $g(p)=\frac{p^2-1}{8}$ thì ta có

$$\begin{aligned}
f(8k+1)&=4k-2k=2k,\\
f(8k+3)&=4k+1-2k=2k+1\\
f(8k+5)&=4k+2-(2k+1)=2k+1,\\
f(8k+7)&=4k+3-(2k+1)=2k+2,\\
g(8k+1)&=k(8k+2),\\
g(8k+3)&=(4k+1)(2k+1),\\
g(8k+5)&=(2k+1)(4k+3),\\
g(8k+7)&=(4k+3)(2k+2),
\end{aligned}$$

Suy ra trong mọi trường hợp $f(p)\equiv g(p)(\bmod 2)$.

Từ đó $\lambda\equiv\frac{p^2-1}{8}(\bmod 2)$ và vì vậy theo ***(12)*** suy ra

IV. $$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$$

Vậy 2 là thặng dư bậc hai của mọi số nguyên tố p có dạng $8k\pm1$ và không là thặng dư bậc hai của mọi số nguyên tố p có dạng $8k\pm3$ (với k là số nguyên).

Áp dụng tính chất ***IV*** để chứng minh định lý sau

Định lý 1. *Tồn tại vô hạn số nguyên tố có dạng* $8k-1$, *với* $k=1,2,\ldots$

Chứng minh. Xét n là số tự nhiên >1. Số $N=2(n!)^2-1$ là lớn hơn 1 và có ít nhất một ước số nguyên tố lẻ p không có dạng $8k+1$. Vì nếu ngược lại thì tất cả các ước số nguyên tố của N đều có dạng $8k+1$ do đó số N tự nó cũng có dạng đó, nhưng N có dạng $8k-1$, mâu thuẫn.

Ta có $p\mid N$, nghĩa là $2(n!)^2\equiv 1^2(\bmod p)$ suy ra $2(n!)^2$ là thặng dư bậc hai theo modulo p.

Vì vậy $\left(\frac{2(n!)^2}{p}\right)=1$, suy ra theo tính chất ***II*** ta có $\left(\frac{2(n!)^2}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{n!}{p}\right)^2=\left(\frac{2}{p}\right)$ nên $\left(\frac{2}{p}\right)=1$ và theo ***IV*** thì p có dạng $8k\pm1$. Nhưng từ định nghĩa của p suy ra nó có dạng $8k-1$. Mà $p\mid N=2(n!)^2-1$ suy ra $p>n$. Từ đó ta thấy với mọi số tự nhiên $n>1$ tồn tại số nguyên tố p lớn hơn n có dạng $8k-1$. Định lý được chứng minh. □

Định lý 2. *Tồn tại vô hạn số nguyên tố có dạng* $8k+3$*, với* $k=0,1,2,\ldots$

Chứng minh. Giả sử n là số tự nhiên >1. Đặt $a=p_2p_3\ldots p_n$. Do a lẻ nên bình phương của nó là a^2 có dạng $8t+1$. Số $N=a^2+2$ có dạng $8t+3$. Nếu mọi ước số nguyên tố của N đều có dạng $8t\pm1$ thì N cũng có dạng đó, vô lý. Vậy số lẻ N có ước số nguyên tố lẻ p không có dạng $8k\pm1$ suy ra p có dạng $8k+3$ hoặc $8k+5$. Giả sử $p=8k+5$. Từ $p\mid N=a^2+2$ suy ra $a^2\equiv-2\pmod p$ và do đó $\left(\frac{-2}{p}\right)=1$. Nhưng theo ***II, III, IV*** thì $\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=(-1)^{(p-1)/2}(-1)^{(p^2-1)/8}$. Do $p=8k+5$ suy ra số $\frac{1}{2}(p-1)$ chẵn và $\frac{1}{8}(p^2-1)$ lẻ do vậy $\left(\frac{-2}{p}\right)=-1$, mâu thuẫn. Vậy p có dạng $8k+3$. Mà $p\mid a^2+2, a=p_2p_3\ldots p_n$ nên $p>p_n$. Do n được chọn lớn tùy ý nên ta có điều phải chứng minh. □

Định lý 3. *Tồn tại vô hạn số nguyên tố có dạng* $8k+5$*, với* $k=0,1,2,\ldots$

Chứng minh. Xét số tự nhiên $n>1$ và đặt $a=p_2p_3\ldots p_n$. Do a là số lẻ, số $N=a^2+4$ có dạng $8k+5$. Nếu tất cả các ước của nó có dạng $8t\pm1$ thì N cũng có dạng đó, vô lý. Vậy N có ước nguyên tố lẻ p có dạng $8k+3$ hoặc $8k+5$. Nếu $p=8k+3$ thì vì $p\mid N=a^2+4$ suy ra $a^2\equiv-4\pmod p$ và do đó $\left(\frac{-4}{p}\right)=1$. Theo ***II, III*** thì $\left(\frac{-4}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^2=(-1)^{(p-1)/2}$. Từ đó vì $p=8k+3$ ta có $\left(\frac{-4}{p}\right)=-1$, mâu thuẫn. Vậy p có dạng $8k+5$. Nhưng vì $p\mid a^2+4$ và $a=p_2p_3\ldots p_n$ suy ra $p>p_n$. Vì n có thể chọn tùy ý nên Định lý 3 được chứng minh. □

2. Luật tương hỗ bậc hai

Cho hai số nguyên tố lẻ phân biệt p và q.

Xét các cặp số (kq,lp) với $k=1,2,\ldots,(p-1)/2, l=1,2,\ldots,(q-1)/2$. Số các cặp này là $\frac{p-1}{2}\cdot\frac{q-1}{2}$.

Với mọi cặp ta có $kq\neq lp$ vì nếu $kq=lp$ ta có $p\mid kq$, suy ra, vì $(p,q)=1, p\mid k$, vô lý vì $k\le(p-1)/2$. Ta chia tất cả các cặp này thành hai lớp, lớp thứ nhất chứa các cặp mà $kq<lp$, lớp còn lại chứa các cặp mà $kq>lp$. Ta tính số các cặp trong mỗi lớp.

Cho trước số l trong dãy $1,2,\ldots,(q-1)/2$. Nếu cặp (kq,lp) thuộc lớp thứ nhất thì $k<lp/q$. Do lp/q không nguyên và vì $\frac{lp}{q}\le\frac{(q-1)p}{2q}\le\frac{p}{2}$, suy ra $\left[\frac{lp}{q}\right]<\frac{p}{2}$, ta có $2\left[\frac{lp}{q}\right]<p$, nghĩa là $2\left[\frac{lp}{q}\right]\le p-1$ suy ra $\left[\frac{lp}{q}\right]\le\frac{p-1}{2}$. Từ đó với số cho trước $l, l\le\frac{1}{2}(q-1)$, k có thể nhận các giá trị

$1,2,\ldots,\left[\frac{lp}{q}\right]$, suy ra số cặp thuộc lớp thứ nhất là $\sum_{l=1}^{(q-1)/2}\left[\frac{lp}{q}\right]$. Tương tự số cặp thuộc lớp thứ hai là $\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]$. Do số cặp trong cả hai lớp là $\frac{p-1}{2}\cdot\frac{q-1}{2}$ suy ra

(13) $$\frac{p-1}{2}\cdot\frac{q-1}{2}=\sum_{l=1}^{(q-1)/2}\left[\frac{lp}{q}\right]+\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]$$

Từ bổ đề Gauss và các tính chất ***I, II*** ta có

$$\left(\frac{2q}{p}\right)=\left(\frac{2(p+q)}{p}\right)=\left(\frac{2^2\frac{q+p}{2}}{p}\right)=\left(\frac{(q+p)/2}{p}\right)$$

$$=(-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{k(p+q)}{p}\right]}=(-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]+\sum_{k=1}^{(p-1)/2}k}=(-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]+\frac{p^2-1}{8}}$$

Đẳng thức cuối cùng suy ra từ đẳng thức $\sum_{k=1}^{(p-1)/2}k=\frac{1}{8}(p^2-1)$.

Vì q lẻ nên từ ***II, IV*** ta có $\left(\frac{2q}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{q}{p}\right)=\left(\frac{q}{p}\right)(-1)^{\frac{p^2-1}{8}}$, kết hợp với công thức ở trên của $\left(\frac{2q}{p}\right)$ suy ra $\left(\frac{q}{p}\right)=(-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]}$. Từ ***(13)*** hai công thức này suy ra

V. $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

đúng với mọi cặp số nguyên tố lẻ phân biệt p và q. Công thức này được gọi là luật tương hỗ bậc hai. Số $\frac{p-1}{2}\cdot\frac{q-1}{2}$ là lẻ nếu và chỉ nếu mỗi số p và q đều có dạng $4k+3$ vì vậy đẳng thức ***V*** suy ra nếu hai số nguyên tố lẻ phân biệt p và q có dạng $4k+3$ thì $\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)$ và nếu trong hai số có số có dạng $4k+1$ thì $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$. Gauss đã tự mình đưa ra 7 lời giải cho định lý này. Bảng 45 lời giải được trình bày từ năm 1796 tới năm 1897 được tổng hợp bởi P.Bachmann trong [2] trang 203. Số lời giải cho luật tương hỗ này ngày một tăng. Ta áp dụng tính chất ***V*** cho định lý sau.

Định lý 4. *Tồn tại vô hạn số nguyên tố có dạng* $5k-1$ *với* k *là số tự nhiên.*

Chứng minh. Xét n là số tự nhiên tùy ý >1. Đặt $N=5(n!)^2-1$. Rõ ràng N là số lẻ >1 và không có dạng $5t+1$, do đó nó có ít nhất một ước số nguyên tố lẻ p (khác 5) và không có dạng $5t+1$. Ta có $p>n$. Do $p\mid N$, suy ra $5(n!)^2\equiv 1(\mathrm{mod}\,p)$ vì thế $\left(\frac{5}{p}\right)=1$. Theo ***V*** ta có $\left(\frac{p}{5}\right)=1$. Số nguyên tố p khác 5 phải có dạng $5k\pm1$ hoặc $5k\pm2$. Nếu $p=5k\pm2$ thì theo ***I,II*** ta có $\left(\frac{p}{5}\right)=\left(\frac{\pm2}{5}\right)=\left(\frac{\pm1}{5}\right)\left(\frac{2}{5}\right)$. Nhưng từ ***III*** thì $\left(\frac{\pm1}{5}\right)=1$ và theo ***IV*** thì $\left(\frac{2}{5}\right)=-1$ ta suy ra $\left(\frac{p}{5}\right)=-1$

mâu thuẫn. Vì vậy p có dạng $5k\pm1$ do đó theo giả thiết suy ra nó có dạng $5k-1$. Vì vậy với mọi số tự nhiên n tồn tại số nguyên tố $p>n$ có dạng $5k-1$. Điều phải chứng minh. □

Nếu $p=5k-1$ (k là số tự nhiên) là số nguyên tố thì k chẵn (nếu ngược lại thì p chẵn và >2). Vì vậy $k=2t$, với t là số tự nhiên và $p=10t-1$. Từ Định lý 4 suy ra tồn tại vô hạn số nguyên tố có dạng $10t-1$ với t là số tự nhiên. Hay nói cách khác tồn tại vô hạn số nguyên tố có chữ số tận cùng là 9. Dễ dàng kiểm tra rằng tồn tại vô hạn số nguyên tố có dạng $5k\pm2$ với k là số tự nhiên. Thật vậy, xét số tự nhiên tùy ý $n>2$. Đặt $N=p_2p_3\ldots p_n-2$. Thì N là số lẻ >1 mà không chia hết cho 5. Nếu tất cả các ước số nguyên tố của nó đều có dạng $5k\pm1$ thì số N cũng có dạng đó, vô lý. Vậy tồn tại ít nhất một ước số nguyên tố p của N khác 5 và không có dạng $5k\pm1$. Do đó p có dạng $5k\pm2$. Nhưng do $p>p_n$ ta suy ra điều phải chứng minh. Chứng minh trong cấp số cộng tồn tại vô hạn số nguyên tố có dạng $5k+2$ và $5k-2$ không khó. Lời giải ở trên thực ra đạt được kết quả mạnh hơn, vì k phải là số lẻ nên thực ra ta đã chứng minh rằng tồn tại vô hạn số nguyên tó có chữ số tận cùng là 7 và 3.

Định lý 5. *Mọi số nguyên tố p có dạng $6k+1$ đều có dạng $p=3x^2+y^2$ với các số tự nhiên x,y.*

Chứng minh. Giả sử p là số nguyên tố có dạng $6k+1$. Theo tính chất ***V*** của ký hiệu Legendre suy ra $\left(\frac{3}{p}\right)=(-1)^{(p-1)/2}\left(\frac{p}{3}\right)$. Từ ***I*** ta có $\left(\frac{p}{3}\right)=\left(\frac{1}{3}\right)=1$. Kết hợp hai đẳng thức này ta có

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{1}{2}(p-1)}\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)=1,$$

Suy ra -3 là thặng dư bậc hai modulo p. Suy ra tồn số nguyên a thỏa mãn $a^2+3\equiv0\pmod p$. Từ định lý Thue (Chương 1 mục 13) suy ra tồn tại các số tự nhiên $x,y\le\sqrt{p}$ mà với cách chọn dấu phù hợp thì $ax\pm y$ chia hết cho p. Vậy ta có $p\mid3x^2+y^2$. Nhưng do $p\mid a^2+3$ nên $p\mid a^2x^2+3x^2$, ta có $p\mid3x^2+y^2$. Lại có $x\le\sqrt{p}$ và $y\le\sqrt{p}$. Hệ quả là bởi vì p là số nguyên tố nên ta có $x^2<p$ và $y^2<p$, dẫn tới $3x^2+y^2<4p$. Do $p\mid3x^2+y^2$ ta có $3x^2+y^2=pt$ với t là số tự nhiên <4. Nếu $t=3$ thì $3\mid y$ và do đó $y=3z$ trong đó z là số tự nhiên.Vậy $p=x^2+3z^2$. Nếu $t=2$ thì các số x,y cùng tính chẵn lẻ. Trong cả hai trường hợp thì $2p=3x^2+y^2$ đều chia hết cho 4 suy ra $2\mid p$, vô lý. Nếu $t=1$ ta có $p=3x^2+y^2$. Điều phải chứng minh. □

Dễ dàng chứng minh rằng nếu số nguyên tố p có dạng $p=3x^2+y^2$ với x,y là các số tự nhiên thì p có dạng $p=6k+1$ với k là số tự nhiên. Từ Định lý 10 Chương 5 suy ra mọi số nguyên tố có dạng $6k+1$ có đúng một biểu diễn dạng $3x^2+y^2$ với x và y là các số tự nhiên. B.Van der Pol và P.Speziali [1] đã tính mọi biểu diễn dạng $3x^2+y^2$ của các số nguyên tố có dạng $6k+1$ không vượt quá 10000. Đặc biệt ta có

$$\begin{aligned}
&7=3\cdot1^2+2^2, &&13=3\cdot2^2+1^2, &&19=3\cdot1^2+4^2, &&31=3\cdot3^2+2^2\\
&37=3\cdot2^2+5^2, &&43=3\cdot3^2+4^2, &&61=3\cdot2^2+7^2, &&67=3\cdot1^2+8^2,\\
&73=3\cdot4^2+5^2, &&79=3\cdot5^2+2^2, &&97=3\cdot4^2+7^2.
\end{aligned}$$

A.Makowski đã lưu ý rằng từ Định lý 5 suy ra hệ quả: *với mọi số nguyên tố p có dạng $6k+1$ thì số $2p^4$ là tổng của ba trùng phương.* Tính chất này suy trực tiếp từ Định lý 5 và đồng nhất thức

$$2\left(3x^2+y^2\right)^4=\left(3x^2+2xy-y^2\right)^4+\left(3x^2-2xy-y^2\right)^4+\left(4xy\right)^4$$

và lưu ý rằng với $p=3x^2+y^2$ ta có $3x^2\pm2xy-y^2=p-2y^2\pm2xy$. Vế phải khác 0 vì $p=6k+1$ lẻ.

Ta chú ý đẳng thức

$$2\left(3x^2+y^2\right)^2=\left(3x^2+2xy-y^2\right)^2+\left(3x^2-2xy-y^2\right)^2+\left(4xy\right)^2.$$

Do đó với $x=1, y=2$ ta có

$$2\cdot 7^4=3^4+5^4+8^4, \qquad 2\cdot 7^2=3^2+5^2+8^2$$

Và với $x=2, y=1$ ta có

$$2\cdot 13^4=15^4+7^4+8^4, \qquad 2\cdot 13^2=15^2+7^2+8^2$$

Ta cũng có hai đẳng thức

$$2\left(3x^2+y^2\right)^2=\left(x+y\right)^4+\left(x-y\right)^4+\left(2x\right)^4,$$
$$2\left(3x^2+y^2\right)^2=\left(x+y\right)^2+\left(x-y\right)^2+\left(2x\right)^2,$$

từ đây suy ra với mọi số nguyên tố p *có dạng* $6k+1$ *thì số* $2p^2$ *là tổng của ba trùng phương. Ví dụ* với $x=1,\ y=2$ ta có

$$2\cdot 7^2=3^4+1^4+2^4, \qquad 2\cdot 7=3^2+1^2+2^2$$

Và với $x=2, y=1$ ta có

$$2\cdot 13^2=3^4+1^4+4^4, \qquad 2\cdot 13=3^2+1^2+4^2$$

3. Tính toán ký hiệu Legendre

Ta tính toán các ký hiệu Legendre dựa vào 5 tính chất được suy trực tiếp từ định nghĩa của nó và lưu ý rằng giá trị của các ký hiệu này bằng 1 hoặc -1. Với số nguyên tố lẻ cho trước p và D là số nguyên không chia hết cho p. Đặt r là phần dư của D khi chia cho p. Suy ra $0<r<p$ và theo I, $\left(\frac{D}{p}\right)=\left(\frac{r}{p}\right)$. Ký hiệu a^2 là bình phương lớn nhất là ước số của r. Ta có $r=ka^2$ với $k=1$ hoặc k là tích của các số nguyên tố khác nhau, nghĩa là $k=q_1q_2...q_s$ với $q_1<q_2...<q_s$. Hơn nữa vì $r<p$, ta có $q_s<p$. Từ ***II*** ta có $\left(\frac{D}{p}\right)=\left(\frac{ka^2}{p}\right)=\left(\frac{k}{p}\right)\left(\frac{a^2}{p}\right)=\left(\frac{k}{p}\right)\left(\frac{a}{p}\right)^2=\left(\frac{k}{p}\right)$. Số này bằng $\left(\frac{1}{p}\right)=1$ hoặc bằng $\left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)...\left(\frac{q_s}{p}\right)$. Nếu $q_1=2$ thì $\left(\frac{q_1}{p}\right)$ được tính dựa vào tính chất ***IV***. Nếu $q_1>2$ thì giá trị của $\left(\frac{q}{p}\right)$ với q và p là các số nguyên tố lẻ và $q<p$ được tính dựa vào tính chất ***V*** vì ta có $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. Bởi vậy việc tính toán các ký hiệu Legendre $\left(\frac{D}{p}\right)$ quy về việc tính các ký hiệu $\left(\frac{D'}{p}\right)$ với q là số nguyên tố lẻ nhỏ hơn p. Do đó sau một số hữu hạn phép rút gọn ta có thể tính được giá trị của ký hiệu $\left(\frac{D}{p}\right)$. Quá trình này có bất tiện vì phải sử dụng tới phép phân tích thành thừa số nguyên tố. Để tránh vấn đề này Jacobi đã đưa ra một ký hiệu tổng quát hơn. Ta sẽ tìm hiểu kỹ hơn trong mục tiếp theo.

4. Ký hiệu Jacobi và các tính chất

Jacobi định nghĩa ký hiệu $\left(\frac{D}{P}\right)$ cho các số lẻ $P>1$ và số nguyên D nguyên tố cùng nhau với P như sau: *nếu* $P=q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_s^{\alpha_s}$ *là phân tích thành thừa số nguyên tố của* P *(các thừa số đều lẻ) thì*

(14) $$\left(\frac{D}{P}\right)=\left(\frac{D}{q_1}\right)^{\alpha_1}\left(\frac{D}{q_2}\right)^{\alpha_2}\ldots\left(\frac{D}{q_s}\right)^{\alpha_s},$$

trong đó vế phải là các ký hiệu Legendre. Từ đây suy ra ngay nếu P là số nguyên tố thì ký hiệu Jacobi trùng với ký hiệu Legendre. Tuy nhiên các quy tắc về thặng dư bậc hai của ký hiệu Jacobi không suy trực tiếp từ ký hiệu Legendre. Lý do là từ đẳng thức $\left(\frac{D}{P}\right)=-1$ suy ra D không phải thặng dư bậc hai của P bởi vì ít nhất một trong các nhân tử $\left(\frac{D}{q_i}\right)$ trong vế phải của ***(14)*** phải bằng -1, suy ra đồng dư thức $x^2\equiv D\pmod{q_i}$ là không có nghiệm do đó đồng dư thức $x^2\equiv D\pmod{P}$ cũng không có nghiệm, đẳng thức $\left(\frac{D}{P}\right)=+1$ không suy ra rằng D là thặng dư bậc hai của P, ví dụ $\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=(-1)(-1)=1$ và đồng dư thức $x^2\equiv 2\pmod{15}$ là không giải được vì phương trình $x^2\equiv 2\pmod 3$ vô nghiệm. Ký hiệu Jacobi cũng có 5 tính chất tương tự ký hiệu Legendre. Trước khi chứng minh chúng ta lưu ý ***(14)*** có thể viết thành dạng

(15) $$\left(\frac{D}{P}\right)=\left(\frac{D}{q_1}\right)\left(\frac{D}{q_2}\right)\ldots\left(\frac{D}{q_s}\right),$$

trong đó $P=q_1q_2\ldots q_s$ và các số nguyên tố $q_1,q_2,\ldots,q_s$ không nhất thiết phân biệt.

Tính chất I. *Nếu* $D\equiv D'\pmod P$ *thì* $\left(\frac{D}{P}\right)=\left(\frac{D'}{P}\right)$.

Chứng minh. Theo ***(15)*** ta có

(16) $$\left(\frac{D}{P}\right)=\left(\frac{D}{q_1}\right)\left(\frac{D}{q_2}\right)\ldots\left(\frac{D}{q_s}\right),\quad \left(\frac{D'}{P}\right)=\left(\frac{D'}{q_1}\right)\ldots\left(\frac{D'}{q_s}\right),$$

Nếu $D\equiv D'\pmod P$ thì suy ra $D\equiv D'\pmod{q_i}$ với mọi $i=1,2,\ldots,s$. Do đó theo tính chất ***I*** của các ký hiệu Legendre thì $\left(\frac{D}{q_i}\right)=\left(\frac{D'}{q_i}\right)$ với $i=1,2,\ldots,s$, suy ra theo ***(16)*** thì $\left(\frac{D}{P}\right)=\left(\frac{D'}{P}\right)$. □

Tính chất II. $\left(\frac{DD'}{P}\right)=\left(\frac{D}{P}\right)\left(\frac{D'}{P}\right)$ *với mọi số nguyên* D *và* D' *không chia hết cho* P.

Sử dụng tính chất ***II*** của ký hiệu Legendre, công thức ***(16)*** và $\left(\frac{DD'}{P}\right)=\left(\frac{DD'}{q_1}\right)\left(\frac{DD'}{q_2}\right)\ldots\left(\frac{DD'}{q_s}\right)$.

Hệ quả trực tiếp của tính chất ***II*** là $\left(\frac{1}{P}\right)=1$.

Tính chất III. $\left(\frac{-1}{P}\right)=(-1)^{(P-1)/2}$.

Chứng minh. Theo ***(15)*** và tính chất ***III*** của các ký hiệu Legendre ta có

(17) $$\left(\frac{-1}{P}\right)=\left(\frac{-1}{q_1}\right)\left(\frac{-1}{q_2}\right)\ldots\left(\frac{-1}{q_s}\right)=(-1)^{\frac{q_1-1}{2}+\frac{q_2-1}{2}+\ldots+\frac{q_s-1}{2}}$$

Ta có $P=q_1q_2\ldots q_s=\big((q_1-1)+1\big)\big((q_2-1)+1\big)\ldots\big((q_s-1)+1\big)$. Tất cả các số $q_1-1,q_2-1,\ldots,q_s-1$ đều chẵn, do đó tích của hai trong số chúng đều chia hết cho 4.

Vì vậy $P=4k+1+(q_1-1)+(q_2-1)+\ldots+(q_s-1)$, và do $\frac{P-1}{2}=2k+\frac{q_1-1}{2}+\frac{q_2-1}{2}+\ldots+\frac{q_s-1}{2}$. Suy ra $(-1)^{\frac{P-1}{2}}=(-1)^{\frac{q_1-1}{2}+\frac{q_2-1}{2}+\ldots+\frac{q_s-1}{2}}$. Theo ***(17)***, ta có tính chất ***III***. □

Tính chất IV. $\left(\frac{2}{P}\right)=(-1)^{(P^2-1)/8}$.

Chứng minh. Theo ***(15)*** và tính chất ***IV*** của các ký hiệu Legendre ta có

(18) $$\left(\frac{2}{P}\right)=\left(\frac{2}{q_1}\right)\left(\frac{2}{q_2}\right)\ldots\left(\frac{2}{q_s}\right)=(-1)^{\frac{q_1^2-1}{8}+\frac{q_2^2-1}{8}+\ldots+\frac{q_s^2-1}{8}}$$

Do bình phương lẻ luôn có dạng $8k+1$, đẳng thức $P^2=\big((q_1^2-1)+1\big)\big((q_2^2-1)+1\big)\ldots\big((q_s^2-1)+1\big)$ chứng tỏ mọi hiệu $q_1^2-1,q_2^2-1,\ldots,q_s^2-1$ đều chia hết cho 8. Suy ra tích của hai trong số chúng đều chia hết cho 64.

Vì vậy $P^2=64k+1+(q_1^2-1)+(q_2^2-1)+\ldots+(q_s^2-1)$ và vì $\frac{P^2-1}{8}=8k+\frac{q_1^2-1}{8}+\frac{q_2^2-1}{8}+\ldots+\frac{q_s^2-1}{8}$ suy ra $(-1)^{\frac{P^2-1}{8}}=(-1)^{\frac{q_1^2-1}{8}+\frac{q_2^2-1}{8}+\ldots+\frac{q_s^2-1}{8}}$. Theo ***(18)*** suy ra tính chất ***IV***. □

Tính chất V. $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$ *với mọi cặp số lẻ nguyên tố cùng nhau* $P,Q>1$.

Chứng minh. Đặt $Q=r_1r_2\ldots r_t$ trong đó $r_1,r_2,\ldots,r_t$ không cần là các số nguyên tố lẻ phân biệt. Theo ***(15)***, tính chất ***II*** và tính chất ***V*** của ký hiệu Legendre ta có

(19) $$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=\prod_{i=1}^{s}\prod_{j=1}^{t}\left(\frac{q_i}{r_j}\right)\left(\frac{r_j}{q_i}\right)=(-1)^{\sum_{i=1}^{s}\sum_{j=1}^{t}\frac{q_i-1}{2}\cdot\frac{r_j-1}{2}}$$

Nhưng

(20) $$\sum_{i=1}^{s}\sum_{j=1}^{t}\frac{q_i-1}{2}\cdot\frac{r_j-1}{2}=\sum_{i=1}^{s}\frac{q_i-1}{2}\cdot\sum_{j=1}^{t}\frac{r_j-1}{2}$$

Để ý rằng trong chứng minh tính chất ***III*** thì ta có $\sum_{i=1}^{s}\frac{q_i-1}{2}\cdot\sum_{j=1}^{t}\frac{r_j-1}{2}=\frac{P-1}{2}\cdot\frac{Q-1}{2}+2h$. Kết hợp với ***(19), (20)*** suy ra tính chất ***V***. □

5. Luật Eisenstein

Các tính chất ở trên của ký hiệu Jacobi được sử dụng để dẫn tới luật Eisenstein mà theo đó giá trị của các ký hiệu Jacobi có thể được tính (và do đó các ký hiệu Legendre cũng vậy) mà không cần sử dụng tới các phân tích thành thừa số nguyên tố.

Đầu tiên ta chú ý rằng việc tính giá trị của $\left(\frac{D}{P}\right)$ với P là số lẻ >1 và D nguyên tố cùng nhau với P có thể rút gọn thành việc tính các giá trị $\left(\frac{Q}{P}\right)$ với Q là số tự nhiên lẻ.

Thật vậy nếu 2^β (với β là số nguyên ≥ 0) là lũy thừa bậc cao nhất của 2 là ước số của D thì $D=(-1)^\alpha 2^\beta Q$ trong đó $\alpha=0$ hoặc 1, Q là số tự nhiên lẻ. Rõ ràng để tính Q ta không cần biết phân tích thành thừa số nguyên tố của D mà chỉ cần chia D liên tục cho 2. Theo các tính chất của ký hiệu Jacobi và theo công thức của D ta có $\left(\frac{D}{P}\right)=(-1)^{\frac{P-1}{2}\alpha+\frac{P^2-1}{8}\beta}\left(\frac{Q}{P}\right)$. Vì vậy chỉ cần tính $\left(\frac{Q}{P}\right)$ với Q,P là các số lẻ nguyên tố cùng nhau.

Ký hiệu R là phần dư của Q khi chia cho P. Khi đó R là một trong dãy $1,2,\ldots,P-1$. Số $P-R$ cũng thuộc về dãy này. Vì vậy với số nguyên t ta có $Q=Pt+R$ và $Q=P(t+1)-(P-R)$. Do tổng của R và $P-R$ lẻ nên một trong hai số đó là lẻ và số còn lại chẵn. Ký hiệu số lẻ là P_1. Nếu $P_1=R$ thì $Q=Pt+P_1$. Nếu $P_1=P-R$ thì $Q=P(t+1)-P_1$. Trong cả hai trường hợp ta có $Q=Pk+\varepsilon_1 P_1$ với k là số nguyên và ε_1 bằng 1 hoặc -1.

Ta chú ý rằng k là số chẵn vì nếu ngược lại thì số $Q\pm P_1$ lẻ, vô lý vì các số Q và P_1 đều lẻ. Suy ra $k=2k_1$ với k_1 nguyên. Ta có $Q=2k_1P+\varepsilon_1P_1$. Nếu $P_1\neq 1$ thì ta có thể lập lại lập luận trên với P và P_1 suy ra $P=2k_2P_1+\varepsilon_2P_2$ với k_2 nguyên và $\varepsilon_2=\pm 1, P_2$ là số tự nhiên. Nếu $P_2\neq 1$ thì theo trường hợp trên $P_1=2k_3P_2+\varepsilon_3P_3$ và lại tiếp tục như thế.

Dãy các số $P,P_1,P_2,\ldots$ giảm nghiêm ngặt vì $P_1\leq P-1,\ P_2\leq P_1-1,\ldots$ Do đó dãy các bất đẳng thức của các số $P,P_1,P_2,\ldots$ không thể kéo dài vô hạn vì số các số lẻ $<P$ là hữu hạn. Vì vậy ta suy ra bất đẳng thức cuối cùng $P_{n-2}=2k_nP_{n-1}+\varepsilon_nP_n$ với P_n phải bằng 1 vì nếu ngược lại thì bất đẳng thức tiếp theo sẽ nhận được. Vậy ta có dãy đẳng thức

$$Q=2k_1P+\varepsilon_1P_1,\ P=2k_2P_1,\ P_1=2k_3P_2+\varepsilon_3P_3,\ \ldots$$

(21) $$P_{n-3}=2k_{n-1}P_{n-2}+\varepsilon_{n-1}P_{n-1},\ P_{n-2}=2k_nP_{n-1}+\varepsilon_nP_n,$$

với $P_n=1$. Đẳng thức đầu tiên trong ***(21)*** theo tính chất ***I, II*** của ký hiệu Jacobi suy ra

(22) $$\left(\frac{Q}{P}\right)=\left(\frac{\varepsilon_1}{P}\right)\left(\frac{P_1}{P}\right)$$

Nếu $\varepsilon_1=1$ thì $\left(\frac{\varepsilon_1}{P}\right)=1=(-1)^{\frac{P-1}{2}\cdot\frac{1-1}{2}}=(-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}}$; Nếu $\varepsilon_1=-1$ thì $\left(\frac{\varepsilon_1}{P}\right)=(-1)^{\frac{P-1}{2}}=(-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}}$.

Trong mọi trường hợp ta đều có $\left(\frac{\varepsilon_1}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}}$.

Từ tính chất ***V*** của ký hiệu Jacobi và nhận xét bình phương của ký hiệu Jacobi luôn bằng 1 ta có $\left(\frac{P_1}{P}\right)=\left(\frac{P}{P_1}\right)\cdot(-1)^{\frac{P-1}{2}\cdot\frac{P_1-1}{2}}$ suy ra theo ***(22)*** thì $\left(\frac{Q}{P}\right)=\left(\frac{P}{P_1}\right)\cdot(-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}+\frac{P-1}{2}\cdot\frac{P_1-1}{2}}$.

Nhưng vì $\varepsilon_1^2=1$ ta có

$$\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}+\frac{P-1}{2}\cdot\frac{P_1-1}{2}=\frac{P-1}{2}\cdot\frac{P_1-\varepsilon_1}{2}=\frac{P-1}{2}\cdot\frac{\varepsilon_1P_1-\varepsilon_1^2}{2\varepsilon_1}$$

$$=\frac{P-1}{2}\cdot\frac{\varepsilon_1P_1-1}{2\varepsilon_1}$$

Hiển nhiên $(-1)^{a/\varepsilon_1}=(-1)^a$ với $\varepsilon_1=\pm1$ do đó $(-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}+\frac{P-1}{2}\cdot\frac{\varepsilon_1P_1-1}{2}}=(-1)^{\frac{P-1}{2}\cdot\frac{\varepsilon_1P_1-1}{2}}$; vậy ta có công thức $\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{\varepsilon_1P_1-1}{2}}\left(\frac{P}{P_1}\right)$. Tương tự từ đẳng thức thứ hai trong ***(20)*** suy ra công thức $\left(\frac{P}{P_1}\right)=(-1)^{\frac{P_1-1}{2}\cdot\frac{\varepsilon_2P_2-1}{2}}\left(\frac{P_1}{P_2}\right)$ và cứ tiếp tục như thế. Đẳng thức áp chót cho ta công thức $\left(\frac{P_{n-3}}{P_{n-2}}\right)=(-1)^{\frac{P_{n-2}-1}{2}\cdot\frac{\varepsilon_{n-1}P_{n-1}-1}{2}}\left(\frac{P_{n-2}}{P_{n-1}}\right)$. Đẳng thức cuối cùng với $P_n=1$ suy ra $\left(\frac{\varepsilon_n}{P_{n-1}}\right)=(-1)^{\frac{P_{n-1}-1}{2}\cdot\frac{\varepsilon_n-1}{2}}$. Vậy ta thu được $\left(\frac{P_{n-3}}{P_{n-2}}\right)=(-1)^{\frac{P_{n-1}-1}{2}\cdot\frac{\varepsilon_nP_n-1}{2}}$.

Bây giờ kết hợp các công thức thu được cho $\left(\frac{Q}{P}\right),\left(\frac{P}{P_1}\right),\ldots,\left(\frac{P_{n-2}}{P_{n-1}}\right)$ ta có công thức

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{\varepsilon_1P_1-1}{2}+\frac{P_1-1}{2}\cdot\frac{\varepsilon_2P_2-1}{2}+\ldots+\frac{P_{n-1}-1}{2}\cdot\frac{\varepsilon_nP_n-1}{2}}$$

Giá trị của vế phải của đẳng thức phụ thuộc vào số các hạng tử lẻ của số mũ. Tích $\frac{P-1}{2}\cdot\frac{\varepsilon_1P_1-1}{2}$ lẻ nếu và chỉ nếu mỗi số P và ε_1P_1 đều có dạng $4t+3$. Vậy ta có thể viết

(23) $$\left(\frac{Q}{P}\right)=(-1)^m,$$

trong đó m là số các cặp P_{i-1},ε_iP_i ($i=1,2,\ldots,n$, và $P_0=P$) mà cả P_{i-1} và ε_iP_i đều có dạng $4t+3$.

Luật Eisenstein. *Để tính* $\left(\frac{Q}{P}\right)$ *ta sử dụng đẳng thức* ***(21)*** *và tìm m là số tất cả các cặp* P_{i-1} *và* ε_iP_i *mà* P_{i-1} *và* ε_iP_i *đều có dạng* $4t+3$, *sau đó ta thay m vào* ***(23)***.

Sử dụng luật này ta có thể tính các ký hiệu Jacobi mà không cần sử dụng tới các phân tích thành thừa số nguyên tố.

Ví dụ. ***1.*** Sử dụng luật Eisenstein để tính $\left(\frac{641}{257}\right)$. Đẳng thức ***(21)*** là

$$641=2\cdot257+127,\quad 257=2\cdot127+3,\quad 127=42\cdot3+1$$

Trong các cặp $257,127;127,3;3,1,$ chỉ có 2 cặp mà cả hai đều có dạng $4t+3$.

Vì vậy $m=1$ do đó $\left(\frac{641}{257}\right)=-1$ suy ra 641 không phải thặng dư bậc hai modulo 257.

2. Tính $\left(\frac{65537}{274177}\right)$. Ta có

$$65537 = 0 \cdot 274177 + 65537,\ 274177 = 4 \cdot 65537 + 12029,\ \ 65537 = 6 \cdot 12029 - 6637,$$
$$12029 = 2 \cdot 6637 - 1245,\ 6637 = 6 \cdot 1245 - 883,\ 1245 = 2 \cdot 833 - 421,\ 833 = 2 \cdot 421 - 9,$$
$$421 = 46 \cdot 9 + 7,\ 9 = 2 \cdot 7 - 5,\ 7 = 2 \cdot 5 - 3,\ 5 = 2 \cdot 3 - 1$$

Trong các cặp $P_{i-1},\ \varepsilon_i P_i$ chỉ có $7, -5$ và $3, -1$ đều có dạng $4t + 3$.

Suy ra $m = 2$ vì vậy $\left(\frac{65537}{274177}\right) = 1$.

3. Tính $\left(\frac{-104}{997}\right)$ ta tìm được $-104 = (-1) \cdot 2^3 \cdot 13$. Do đó $\left(\frac{-104}{997}\right) = \left(\frac{-1}{997}\right)\left(\frac{2}{997}\right)\left(\frac{13}{997}\right)$. Số 997 có dạng $4t + 1$ nên $\left(\frac{-1}{997}\right) = 1$. Số 997 có dạng $8t + 5$ nên $\left(\frac{2}{997}\right) = -1$. Vì vậy $\left(\frac{-104}{997}\right) = -\left(\frac{13}{997}\right)$.

Để tính $\left(\frac{13}{997}\right)$ ta xét dãy đẳng thức $13 = 0 \cdot 997 + 13,\ \ 997 = 76 \cdot 13 + 9,\ \ \ 13 = 2 \cdot 9 - 5,\ \ 9 = 2 \cdot 5 - 1.$

Trong dãy này không có cặp $P_{i-1},\ \varepsilon_i P_i$ nào mà hai phần tử đều có dạng $4t + 3$.

Vậy $m = 0$ suy ra $\left(\frac{13}{997}\right) = 1$ và ta có $\left(\frac{-104}{997}\right) = -1$.

CHƯƠNG 10

CÁC SỐ MERSENNE VÀ CÁC SỐ FERMAT

1. Một số tính chất của các số Mersenne

Các số Mersenne $M_n = 2^n - 1$ đã được tìm hiểu trong Chương 4 mục 5. Định lý 5 Chương 5 nói rằng một số chẵn là số hoàn hảo khi và chỉ khi nó có dạng $2^{n-1}M_n$ với n là số tự nhiên và M_n là số nguyên tố Mersenne. Đây là lý do khiến các số nguyên tố Mersenne được quan tâm. Hơn nữa số nguyên tố lớn nhất được biết hiện nay cũng là số Mersenne.

Trong Chương 4 mục 5 ta đã biết nếu số Mersenne M_n là số nguyên tố thì n cũng là số nguyên tố, tuy nhiên điều ngược lại không đúng chẳng hạn $M_{11} = 23 \cdot 89$.

Dễ dàng chứng minh một số tự nhiên m là số Mersenne khi và chỉ khi $m+1$ không có ước số nguyên tố lẻ. Golomb [1] đã lưu ý rằng từ nhận xét này ta có thể xây dựng một phương pháp tìm tất cả các số Mersenne tương tự phương pháp sàng Eratosthenes. Bây giờ ta chứng minh một định lý mà trong một số trường hợp giúp ta quyết định được một số Mersenne là hợp số hay không.

Định lý 1. *Nếu q là số nguyên tố có dạng $8k+7$ thì $q \mid M_{(q-1)/2}$.*

Chứng minh. Từ công thức trong Chương 9 ta có nếu q là số nguyên tố thì $\left(\frac{2}{q}\right) \equiv 2^{(q-1)/2} \pmod q$.

Nếu q là số nguyên tố có dạng $8k+7$ thì theo tính chất 4 của ký hiệu Legendre (Chương 9 mục 1) ta có $\left(\frac{2}{q}\right) = 1$. Hệ quả là $2^{(q-1)/2} \equiv 1 \pmod q$ suy ra $q \mid 2^{(q-1)/2} - 1$. □

Bằng phép quy nạp đơn giản ta có $2^{4k+3} > 8(k+1)$. Thật vậy $2^7 > 8 \cdot 2$ và nếu $2^{4k+3} > 8(k+1)$ thì $2^{4(k+1)+3} > 2^4 \cdot 8(k+1) > 8(k+2)$. Do đó nếu $q = 8k+7 > 7$ thì $2^{(q-1)/2} - 1 > 8k+7 = q$ suy ra nếu q là số nguyên tố có dạng $8k+7 > 7$ thì $M_{(q-1)/2}$ là hợp số chia hết cho q. Ta có hệ quả

Hệ quả. *Nếu số nguyên tố $n > 3$ có dạng $4k+3$ và $q = 2n+1$ là số nguyên tố thì M_n là hợp số chia hết cho q.*

Bằng cách này ta xác định được các số Mersenne sau đây đều là hợp số, các ước số nguyên tố của chúng cũng được tìm ra cụ thể

$23 \mid M_{11}$, $47 \mid M_{23}$, $167 \mid M_{83}$, $263 \mid M_{131}$, $359 \mid M_{179}$, $383 \mid M_{191}$, $479 \mid M_{239}$, $503 \mid M_{251}$, $719 \mid M_{359}$, $839 \mid M_{419}$, $863 \mid M_{431}$, $887 \mid M_{443}$, $983 \mid M_{491}$, $1319 \mid M_{659}$, $1367 \mid M_{683}$, $1439 \mid M_{719}$, $1487 \mid M_{743}$, $1823 \mid M_{911}$, $2039 \mid M_{1019}$.

Từ giả thuyết H (Chương 3 mục 8) ta đã biết tồn tại vô hạn số nguyên tố p có dạng $4k+3$ mà $q = 2p+1$ là số nguyên tố. Vì vậy sử dụng hệ quả ở trên ta thấy giả thuyết H suy ra sự tồn tại vô hạn các số nguyên tố p mà các số M_p là hợp số (Schinzel và Sierpiniski [3] trang 198 C_9).

Từ Định lý 1 chú ý rằng với cùng phương pháp lập luận ta có thể suy ra nếu q là số nguyên tố có dạng $8k+1$ thì $q \mid M_{(q-1)/2}$. Tuy nhiên $(q-1)/2 = 4k$ không phải số nguyên tố. Chẳng hạn $17 \mid M_8$, $41 \mid M_{20}$, $89 \mid M_{44}$, $97 \mid M_{48}$.

Ta chưa biết số Mersenne nào là hợp số với chỉ số nguyên tố và không phải tích của các số nguyên tố phân biệt. Ta cũng chưa chứng minh được có tồn tại vô hạn các số Mersenne không có ước số chính phương hay không.

Định lý 2. *Nếu n là số tự nhiên >1 thì M_n không thể là lũy thừa bậc m của một số tự nhiên với m là số tự nhiên >1 (Gerono [1]).*

Chứng minh. Giả sử rằng $2^n-1=k^m$ với k và $m>1$ là các số tự nhiên. Vì $n>1$ nên k lẻ. Nếu m chẵn thì k^m có dạng $8t+1$ suy ra $k^m+1=2(4t+1)$. Nhưng vì $n>1,\ k^m+1=2^n$ chia hết cho 4 suy ra mâu thuẫn. Vậy m lẻ và $2^n=k^m+1=(k+1)\left(k^{m-1}-k^{m-2}+\ldots-k+1\right)$, nhân tử thứ hai là tổng của lẻ hạng tử lẻ nên nó là số lẻ, mà nó lại là ước của 2^n nên phải bằng 1. Do đó $2^n=k+1$ và $m=1$ mâu thuẫn với giả thiết. Định lý 2 được chứng minh. □

Định lý 2 suy ra không tồn tại số Mersenne là bình phương ngoại trừ $M_1=1^2$.

Mặt khác tồn tại các số Mersenne là số tam giác. Tuy nhiên chỉ tồn tại bốn số như vậy là $M_1=t_1,\ M_2=t_2,\ M_4=t_5,\ M_{12}=t_{90}$ (Ramanujan [1], Nagell [4],[12] và Hasse [2]).

Dễ dàng chứng minh với $|x|<\frac{1}{2}$ thì $\frac{1}{(1-x)(1-2x)}=M_1+M_2x+M_3x^2+\ldots.$

Bài tập. ***1.*** Chứng minh rằng mọi số lẻ là ước số của vô hạn các số Mersenne.

Chứng minh. Nếu m là số lẻ thì theo định lý Euler, với mọi số tự nhiên k ta có $m\,|\,M_{k\varphi(m)}$. □

2. Tìm số Mersenne nhỏ nhất chia hết cho bình phương một số tự nhiên >1.

Lời giải. Số đó là $M_6=2^6-1=63=3^2\cdot 7$ vì $M_1=1,\ M_2=3,\ \ M_3=7,\ \ M_4=15=3\cdot 5$ và $M_5=31.$

3. Tìm số Mersenne nhỏ nhất có chỉ số lẻ mà nó chia hết cho bình phương một số tự nhiên >1.

Lời giải. Đó là số $M_{21}=7\cdot 127\cdot 337$ vì

$$M_7=127,\ M_9=7\cdot 73,\ M_{11}=23\cdot 89,\ \ M_{13}=8191, M_{15}=7\cdot 31\cdot 151,$$
$$M_{17}=131071,\ M_{19}=524287$$

Ghi chú. Các số Mersenne tiếp theo sau M_{21} có chỉ số lẻ và chia hết cho bình phương một số tự nhiên >1 là M_{63} và M_{105}. Chúng đều chia hết cho 7^2 vì $M_{21}\,|\,M_{63}$ và $M_{21}\,|\,M_{105}$.

4. Chứng minh rằng nếu a và n là các số tự nhiên >1 thì nếu a^n-1 là số nguyên tố thì nó là số Mersenne.

Chứng minh. Nếu $a>2$ ta có $a-1\,|\,a^n-1$ do đó vì $n>1,\ 1<a-1<a^n-1$ suy ra a^n-1 không phải số nguyên tố. Do đó vì a^n-1 nguyên tố suy ra $a\le 2$ vì vậy $a=2$ (vì $1-1$ không phải số nguyên tố). Vậy $a^n-1=M_n$. □

5. Chứng minh rằng nếu m là số tự nhiên tùy ý, s là số các chữ số của m trong hệ thập phân thì tồn tại số Mersenne M_n mà s chữ số đầu tiên của nó trùng với s chữ số của m tương ứng.

Chứng minh suy ra ngay từ tính chất của các số 2^n (Sierpinski [11] định lý 2).

6. Chứng minh rằng với mọi số tự nhiên s thì s chữ số tận cùng của các số $M_n(1,2,\ldots)$ tạo thành dãy vô hạn tuần hoàn chu kỳ gồm $4\cdot 5^{s-1}$ phần tử.

Chứng minh suy ra từ Định lý 1 trong bài báo trích dẫn ở trên.

Rất nhiều các định lý về các ước số của M_n được tổng hợp bởi E.Storchi trong [1].

2. Định lý của E.Lucas và D.H.Lehmer

Định lý 3. *Số M_p, p là số nguyên tố lẻ, là nguyên tố khi và chỉ khi nó là ước số của phần tử thứ $p-1$ của dãy $s_1, s_2, \ldots$, với $s_1 = 4, s_k = s_{k-1}^2 - 2,\ k = 1,2,\ldots$ (Lehmer [2], Kraitchik [1] trang 141 và Trost [3])*

Chứng minh. Đặt $a = 1+\sqrt{3},\ b = 1-\sqrt{3}$. Ta có $a+b = 2,\ ab = -2,\ a-b = 2\sqrt{3}$. Xác định dãy các số tự nhiên $u_n, v_n\ (n = 1,2,\ldots)$ được cho bởi công thức bởi

$$u_n = \frac{a^n - b^n}{a-b}, \quad v_n = a^n + b^n$$

Các công thức này suy ra với mọi $n = 1,2,\ldots$ ta có

$$u_n = \binom{n}{1} + \binom{n}{3}\cdot 3 + \binom{n}{5}\cdot 3^2 + \ldots, \qquad v_n = 2\left(1 + \binom{n}{3}\cdot 3 + \binom{n}{5}\cdot 3^2 + \ldots\right)$$

Vì vậy với mọi số tự nhiên k, l ta có

(1) $$2u_{k+l} = u_k v_l + v_k u_l,$$

(2) $$(-2)^{l+1} u_{k-l} = u_l v_k - u_k v_l \quad \text{với} \quad k > l,$$

(3) $$u_{2k} = u_k v_k,$$

(4) $$v_{2k} = v_k^2 + (-2)^{k+1},$$

(5) $$v_k^2 - 12u_k^2 = (-2)^{k+2},$$

(6) $$2v_{k+l} = v_k v_l + 12u_k u_l.$$

Với số nguyên tố lẻ q ký hiệu $\omega(q)$ là số tự nhiên nhỏ nhất n thỏa mãn $q \mid u_n$ (số này là tồn tại).

Bổ đề 1. *Số nguyên tố lẻ q là ước của u_n, n là số tự nhiên, khi và chỉ khi $\omega(q) \mid n$.*

Chứng minh bổ đề 1. Cho trước số nguyên tố lẻ q. Ký hiệu S là tập tất cả các số tự nhiên n thỏa mãn $q \mid u_n$. Từ ***(1)*** và ***(2)*** nếu hai số k và l thuộc tập S thì $k+l$ cũng thuộc tập S, hơn nữa nếu $k > l$ thì $k-l$ cũng thuộc S. Do đó tập S có tính chất: tổng và hiệu (dương) của hai phần tử thuộc S cũng thuộc S.

Ký hiệu d là số tự nhiên nhỏ nhất thuộc S. Từ tính chất ở trên suy ra các số $kd, k = 1,2,\ldots,$ cũng thuộc S. Mặt khác giả sử n thuộc S và n chia d dư $r > 0$. Khi đó $n = td + r$ với t là số nguyên ≥ 0 và $r < d$. Nếu $t = 0$ thì rõ ràng là vô lý vì r nhỏ hơn d không thể bằng n và vì vậy không thuộc S theo định nghĩa của d. Hệ quả t là số tự nhiên và vì vậy td thuộc S suy ra theo tính chất của S thì số $r = n - td$ là hiệu của hai phần tử thuộc S với $n > td$ nên cũng thuộc S, điều này mâu thuẫn với định nghĩa của d. Từ đây suy ra $r = 0$, nghĩa là tập S là tập hợp các bội số dương của phần tử của nó.

Vậy nếu n thuộc S thì $\omega(q) \mid n$ và cứ như vậy. Bổ đề được chứng minh. □

Bổ đề 2. *Nếu q là số nguyên tố > 3 thì*

(7) $$q \mid u_q - 3^{(q-1)/2}$$

Và

(8) $$q \mid v_q - 2$$

Chứng minh bổ đề 2. Để chứng minh ***(7)*** ta sử dụng đẳng thức

$$u_q = \frac{1}{2\sqrt{3}}\left[\left(1+\sqrt{3}\right)^q - \left(1-\sqrt{3}\right)^q\right] = \sum_{k=0}^{(q-1)/2} \binom{q}{2k+1} 3^k$$

Trong tổng này tất cả các hệ số nhị thức chỉ trừ ra hệ số đầu tiên thì đều chia hết cho q do đó suy ra ***(8)***. □

Bổ đề 3. *Nếu với số nguyên tố $q>3$ số $\omega(q)$ tồn tại thì $\omega(q)\le q+1$.*

Chứng minh bổ đề 3. Vì $u_1=1,\ v_1=2$, theo ***(1)*** và ***(2)*** với $k=q, l=1$ ta có $2u_{q+1}=2u_q+v_q$ và $-4u_{q-1}=2u_q-v_q$ vì vậy $-8u_{q+1}u_{q-1}=4u_q^2-v_q^2$. Nhưng từ Bổ đề 2 ta có $q\mid u_q^2-3^{q-1}$ và $q\mid v_q^2-4$. Vì q là số nguyên tố >3, sử dụng định lý Fermat nhỏ ta nhận được $q\mid 3^{q-1}-1$. Vì vậy $q\mid u_q^2-1$ và do đó $q\mid 4u_q^2-v_q^2$. Hệ quả là $q\mid 8u_{q+1}u_{q-1}$ suy ra vì $q>3$ ta có hoặc $q\mid u_{q+1}$ hoặc $q\mid u_{q-1}$. Trong trường hợp thứ nhất theo Bổ đề 1 ta có $\omega(q)\le q+1$ và trong trường hợp sau ta có $\omega(q)\le q-1$. Vì vậy ta luôn có $\omega(q)\le q+1$. □

Bây giờ ta chứng minh điều kiện trong Định lý 3 cũng là điều kiện đủ.
Giả sử p là số nguyên tố lẻ và $M_p\mid s_{p-1}$. Khi đó

(9) $$M_p\mid 2^{2^{p-2}}s_{p-1}$$

Ta có $2s_1=v_2$. Với số tự nhiên n giả sử $2^{2^{n-1}}s_n=v_{2^n}$, điều này đúng với $n=1$. Do $s_{n+1}=s_n^2-2$ ta có $2^{2^n}s_{n+1}=\left(2^{2^{n-1}}s_n\right)^2-2^{2^n+1}=v_{2^n}^2-2^{2^n+1}$. Nhưng từ ***(4)*** với $k=2^n$ ta có $v_{2^{n+1}}=v_{2^n}^2-2^{2^n+1}$. Vì vậy $2^{2^n}s_{n+1}=v_{2^{n+1}}$. Công thức $2^{2^{n-1}}s_n=v_{2^n}$ được suy ra theo quy nạp. Vì vậy với $n=p-1$ ta có

(10) $$2^{2^{p-1}}s_{p-1}=v_{2^{p-1}}$$

Từ ***(10)*** và ***(9)*** ta có

(11) $$M_p\mid v_{2^{p-1}}$$

Suy ra theo ***(3)*** với $k=2^{p-1}$

(12) $$M_p\mid u_{2^p}$$

Ký hiệu q là ước số nguyên tố tùy ý của M_p. Vì p lẻ nên số $M_p=2^p-1$ không chia hết cho 3, ta có $q>3$. Do $q\mid M_p$ và công thức ***(12)*** suy ra $q\mid u_{2^p}$ do đó theo bổ đề 1 ta có $\omega(q)\mid 2^p$.

Mặt khác $\omega(q)$ không phải ước của 2^{p-1} vì nếu ngược lại thì theo Bổ đề 1 suy ra $q\mid u_{2^{p-1}}$ do đó theo ***(5)*** với $k=2^{p-1}$, p là ước số của một lũy thừa của 2, điều này không thể vì q là số nguyên tố >3. Vì vậy $\omega(q)=2^p$.

Theo Bổ đề 3 ta có $2^p\le q+1$ suy ra $M_p\le q$ và vì $q\mid M_p$ suy ra $M_p=q$ nghĩa là M_p là số nguyên tố. Vậy điều kiện trong Định lý 3 cũng là điều kiện đủ. Để chứng minh điều kiện cần ta chứng minh

Bổ đề 4. *Nếu p là số nguyên tố có dạng $12k+7$ thì $p\mid 3^{(p-1)/2}+1$.*

Chứng minh bổ đề 4. Xét số nguyên tố p có dạng $12k+7$ với số nguyên $k\ge 1$. Khi đó $p>3$ và theo tính chất 1 của ký hiệu Legendre (Chương 9 mục 1) ta có $\left(\frac{p}{3}\right)=\left(\frac{1}{3}\right)=1$. Theo tính chất 5 ký

hiệu Legendre ta có $\left(\frac{p}{3}\right)\left(\frac{3}{p}\right)=-1$ suy ra $\left(\frac{3}{p}\right)=1$. Hệ quả là $3^{(p-1)/2}\equiv -1(\mathrm{mod}\, p)$ suy ra $p\,|\,3^{(p-1)/2}+1$. □

Bây giờ ta chứng minh điều kiện trong Định lý 3 là điều kiện cần. Giả sử p là số nguyên tố >2 và $q=M_p$ là số nguyên tố. Vì $p>2$ ta có $8\,|\,2^p=q+1$. Vì vậy $q=8t+7$ với số nguyên $t\geq 0$. Ta có $q-1=2^p-2=2\left(2^{p-1}-1\right)$. Vì $p-1$ chẵn nghĩa là $p-1=2s$ với s là số tự nhiên nên ta có $2^{p-1}-1=(3+1)^s-1=3u$ với u là số nguyên. Vì vậy $3\,|\,2^{p-1}-1\,|\,q-1=8t+6$ suy ra $3\,|\,t$ nghĩa là $t=3k$ với k là số nguyên. Do đó $q=8t+7=24k+7$. Theo ***(4)*** với $k=2^{p-1}$ ta có

(13) $$v_{2^p}=v_{2^{p-1}}^2-4\cdot 2^{2^{p-1}-1}$$

Nhưng từ $q=24k+7=8\cdot 3k+7$ và theo Định lý 1 ta có $q\,|\,M_{(q-1)/2}$, nghĩa là $q\,|\,M_{2^{p-1}-1}=2^{2^{p-1}-1}-1$ suy ra theo ***(13)*** thì

(14) $$q\,|\,v_{2^p}-v_{2^{p-1}}^2+4$$

Nhưng theo ***(6)*** với $k=q,\ l=1$ và vì $q+1=2^p$ ta có $2v_{2^p}=v_qv_1+12u_qu_1=2v_q+12u_q$. Hệ quả là

(15) $$v_{2^p}=v_q+6_{u_q}=(v_q-2)+6(u_q+1)-4$$

Do $q=24k+7$ ta áp dụng Bổ đề 4 cho q do đó $q\,|\,3^{(q-1)/2}+1$ và vì vậy theo ***(7)*** ta có $q\,|\,u_q+1$ và theo ***(8)*** thì $q\,|\,v_p-2$. Vì vậy theo công thức ***(15)*** ta có $q\,|\,v_{2^p}+4$ suy ra theo ***(14)*** thì $q\,|\,v_{2^{p-1}}^2$. Vì vậy từ ***(10)*** ta có $q=M_p$ lẻ suy ra $M_p\,|\,s_{p-1}$. Định lý 3 được chứng minh. □

Dễ dàng chứng minh Định lý 3 tương đương với định lý Lucas sau đây

Định lý 3α. *Giả sử p là số nguyên tố lẻ thì* M_p *là số nguyên tố nếu và chỉ nếu* M_p *là ước số của phần tử thứ* $p-1$ *của dãy* $t_1,t_2,\ldots,$, *với* $t_1=2, t_{k+1}=2t_k^2-1$ *với* $k=1,2,\ldots$

Sự tương đương này được suy ra ngay từ việc dãy $s_k\ (k=1,2,\ldots)$ trở thành dãy $t_k\ (k=1,2,\ldots)$ nếu s_k được thay bởi $2t_k$. Do đó vì M_p lẻ nên $M_p\,|\,s_{p-1}$ tương đương với $M_p\,|\,t_{p-1}$. Chứng minh của Định lý ***3***α dựa trên các hàm lượng giác các biến phức được trình bày bởi T.Bang [1].

3. Số nguyên tố lớn nhất đã tìm được

Định lý 3 không thuận tiện khi sử dụng để nghiên cứu các số Mersenne có chỉ số lớn hơn 10. Lý do là vì các phần tử của dãy $s_k\ (k=1,2,\ldots)$ tăng rất nhanh theo k. Theo quy nạp từ định nghĩa của dãy $\left(s_1=4, s_k=s_{k-1}^2-2, k=2,3,..\right)$ ta có $s_k\geq 10^{2^{k-2}}+4$ với mọi $k=2,3,\ldots$ suy ra $s_{10}>10^{2^8}=10^{256}$ nghĩa là phần tử thứ 10 là s_{10} có hơn 250 chữ số. Số s_{100} có hơn 10^{27} chữ số. Vì vậy để sử dụng Định lý 3 để nghiên cứu xem khi nào thì số M_p (p là số nguyên tố >2) là số nguyên tố thì ta làm như sau.

Với mọi số nguyên t ký hiệu $\bar{t}$ là phần dư nhận được khi chia t cho M_p. Ta có ngay $M_p\,|\,t-\bar{t}$. Bây giờ ta xét dãy $r_k\ (k=1,2,\ldots)$ định nghĩa bởi

(16) $$r_1=4;\ r_{k+1}=\overline{r_k^2}-\overline{2}\quad \text{với}\quad k=1,2,\ldots$$

Và theo quy nạp ta chứng minh

(17) $M_p \mid s_k - r_k$ với $k = 1, 2, \ldots$

Ta thấy ***(17)*** đúng với $k = 1$. Giả sử tính chất này đúng với số tự nhiên k nào đó. Khi đó từ $M_p \mid s_k^2 - r_k^2$ suy ra $M_p \mid s_k^2 - 2 - \left(r_k^2 - 2\right)$. Vì $s_k^2 - 2 = s_{k+1}$ và vì $M_p \mid t - \bar{t}$ với $t = r_k^2 - 2$ và theo ***(16)*** thì $M_p \mid r_k^2 - 2 - r_{k+1}$ nên ta nhận được $M_p \mid s_{k+1} - r_{k+1}$. Công thức ***(17)*** được chứng minh.

Theo ***(17)*** thì công thức $M_p \mid s_{p-1}$ tương đương với $M_p \mid r_{p-1}$. Theo ***(16)*** thì để tính r_{p-1} ta có thể tính $p-2$ bình phương các số dư nhận được khi chia cho M_p, các số này không có nhiều chữ số hơn M_p, và tính số dư bởi các bình phương của chúng trừ đi 2 khi chia cho M_p.

Các máy tính điện tử hiện nay có thể tính toán theo thủ tục trên với các số nguyên tố p tới 200.000. Theo cách này số M_{293} được chỉ ra là hợp số vì nó không phải ước số của r_{293}. Ta chưa biết số nguyên tố nào là ước số của số này. Tình huống tương tự xảy ra với M_{347} (Brillhart, Lehmer, Selfridge, Tuckerman and Wagstaff [1]).

Tới tận năm 1950 số nguyên tố lớn nhất được tính là M_{127}, số này có 39 chữ số. Số này được nghiên cứu bởi E.Lucas năm 1876 và năm 1914 E.Fauquembergue đã chứng minh nó là số nguyên tố. Tháng 1 năm 1952 với sự trợ giúp của máy SWAC các số M_{521} và M_{607} đã được chứng minh là số nguyên tố. Số thứ nhất có 157 chữ số và số kia có 183 chữ số. Cùng năm đó vào tháng 7 số M_{1279} được chứng minh là số nguyên tố. Nó có 376 chữ số. Tháng 10 năm 1952 các kết quả tương tự được R.M.Robinson chứng minh cho các số M_{2203} và M_{2281}. Số đầu tiên có 664 chữ số và số kia có 687 chữ số (H.S.Uhler [2],[3]). Số nguyên tố Mersenne tiếp theo là M_{3217} được tìm ra bởi H.Riesel vào năm 1957 bằng máy BESK và năm 1962 Alexander Hurwitz tìm ra M_{4253} và M_{4423} bằng máy IBM 7090. Các tính toán khác được thực hiện bởi D.B.Gillies trên máy ILLIAC II dẫn tới các số nguyên tố M_{9683}, M_{9941} và M_{11213} vào năm 1964. Năm 1971 B.Tuckerman tìm được số Mersenne tiếp theo là M_{19937} bằng máy IBM 360/91. Các số nguyên tố M_{21701}, M_{23209} được tìm ra bởi E.Nickel và C.Noll bằng máy CDC Cyber 174 năm 1978 và 1979. Năm 1979 D.Slowinski sử dụng máy CRAY 1 tìm ra M_{44497}, năm 1983 là M_{86243}, M_{132049} và năm 1985 là số M_{216091}. Số cuối cùng là số nguyên tố lớn nhất được tính hiện nay và nó có 65050 chữ số.

Vậy 30 số nguyên tố Mersenne M_n đã được tính là

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4219, 4423,$$
$$9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 132049, 216091$$

(Brillhart, Lehmer, Selfridge, Tuckerman và Wagstaff [1]).

Với mọi $n \le 263$ phân tích thành thừa số nguyên tố của $2^n - 1$ cũng được tính. Chẳng hạn M_{101} là tích của hai số nguyên tố, số bé hơn là 7432339208719 (Brillhart et al. [1]).

Có một giả thuyết nói rằng nếu M_n là số nguyên tố thì M_{M_n} cũng là số nguyên tố. Giả thuyết này đúng với 4 số nguyên tố Mersenne đầu tiên nhưng với số thứ 5 là $M_{13} = 8191$ thì giả thuyết sai. Câu trả lời phủ định được trình bày bởi D.J.Wheeler năm 1953. Số $M_{M_{13}} = 2^{8191} - 1$ (có 2466 chữ số) là hợp số (Robinson [1] trang 844). Kết quả này có được bằng cách sử dụng định lý Lucas và Lehmer, các tính toán thực hiện bởi máy tính điện tử trong 100 giờ đồng hồ. Chưa có ước số nguyên tố nào của số này được tính. Tuy nhiên năm 1957 ta đã chứng minh được M_{17} là số nguyên tố nhưng $M_{M_{17}}$ là hợp số và nó chia hết cho $1768\left(2^{17} - 1\right) + 1$. Tương tự với M_{19} là số nguyên tố nhưng $M_{M_{19}}$ là hợp số chia hết cho $120\left(2^{19} - 1\right) + 1$.

Trong mối liên hệ này có một giả thuyết khác được đặt ra (chưa có câu trả lời): *dãy* $q_0, q_1, q_2, \ldots,$ *với* $q_0 = 2,\ q_{n+1} = 2^{q_n} - 1,\ n = 0,1,2,\ldots,$ *chỉ chứa các số nguyên tố?*

Giả thuyết này được kiểm tra với q_n mà $n \le 4$, số q_5 có hơn 1037 chữ số. Hơn nữa vì các ước số của q_5 đều có dạng $2kq_4 + 1 > 2q_4$, số q_5 không có ước số nguyên tố có ít hơn 39 chữ số. Vì vậy ta vẫn chưa biết q_5 có phải số nguyên tố hay không.

4. Ước số nguyên tố của các số Fermat

Các số Fermat $F_n = 2^{2^n} + 1 (n = 0,1,2,\ldots)$ là trường hợp đặc biệt của các số có dạng $a^n + 1$ với a là số tự nhiên > 1. Giả sử số $a^m + 1$ với số tự nhiên $m > 1$ là số nguyên tố. Nếu m có ước số lẻ $k > 1$ thì $n = kl$ suy ra $a^l + 1 | \left(a^l\right)^k + 1 = a^m + 1$ và vì $k > 1$ số $a^m + 1$ là hợp số. Hệ quả là nếu $a^m + 1$ (với m là số tự nhiên > 1) là số nguyên tố thì m là lũy thừa của 2, nghĩa là $m = 2^n$ với n là số tự nhiên. Đặc biệt nếu $2^m + 1$ (với m là số tự nhiên) là số nguyên tố thì nó phải là số Fermat. Vì vậy suy ra số tự nhiên s là số nguyên tố Fermat khi và chỉ khi s là số nguyên tố > 2 và $s - 1$ không có ước số nguyên tố lẻ. Từ đây ta có phương pháp để tìm tất cả các số Fermat là số nguyên tố. Phương pháp này là ứng dụng thứ hai của phương pháp sàng Eratosthenes (so sánh với phương pháp tìm tất cả các số Mersenne trong mục 1).

Định lý 4. *Nếu* a *là số nguyên chẵn,* n *là số tự nhiên và* p *là số nguyên tố thỏa mãn* $p | a^{2^n} + 1$ *thì* $p = 2^{n+1}k + 1$, *với* k *là số tự nhiên.*

Chứng minh. Vì $p | a^{2^n} + 1$ ta có $p | a^{2^{n+1}} - 1$; $p | a^{2^n} - 1$ là không thể vì nếu $p | 2$, thì $p = 2$, mâu thuẫn vì từ $p | a^{2^n} + 1$ suy ra $(p, a) = 1$ và a chẵn. Ký hiệu δ là lũy thừa nhỏ nhất của a mà $p | a^\delta - 1$. Vì $p | a^{2^{n+1}} - 1$ nên theo Định lý 9 chương 6 ta có $\delta | 2^{n+1}$. Không thể có $\delta | 2^n$ vì ta không có $p | a^{2^n} - 1$. Từ đây suy ra $\delta = 2^{n+1}$ và theo định lý Fermat nhỏ $p | a^{p-1} - 1$ suy ra $\delta | p - 1$ nghĩa là $2^{n+1} | p - 1$ vì vậy $p = 2^{n+1}k + 1$ với k là số tự nhiên. □

Định lý 5. *Mọi ước số* > 1 *của số* F_n *với số nguyên* $n > 1$ *đều có dạng* $2^{n+2}k + 1$ *với* k *là số tự nhiên.*

Chứng minh. Từ chứng minh của Định lý 4 (với $a = 2$) ta có nếu p là số nguyên tố và $p | F_n$ thì 2 có cấp $2^{n+1} \bmod p$. Mặt khác từ Định lý 4 suy ra p có dạng $2^{n+1}t + 1$ với t là số tự nhiên. Hệ quả là nếu $n > 1$ thì nó có dạng $8k + 1$ suy ra theo mục 1 thì $p | M_{(p-1)/2}$ nghĩa là $p | 2^{(p-1)/2} - 1$. Nhưng 2 có cấp $2^{n+1} \bmod p$ nên $2^{n+1} | (p-1)/2$ và do đó $2^{n+2} | p - 1$ suy ra $p = 2^{n+2}k + 1$ với k là số tự nhiên. Vì vậy ta thấy mọi ước số nguyên tố của $F_n (n > 1)$ đều có dạng $2^{n+2}k + 1$. Hơn nữa vì mọi ước số > 1 của F_n đều là tích các ước số nguyên tố của F_n nên bản thân F_n cũng có dạng trên (vì tích của các số có dạng $mk + 1$ thì cũng có dạng đó). Định lý 5 được chứng minh. □

Định lý 5 được sử dụng để nghiên cứu xem khi nào thì một số Fermat cho trước có phải là số nguyên tố hay không. Chẳng hạn các ước số nguyên tố của F_4 (theo Định lý 5) đều có dạng $2^6 k + 1 = 64k + 1$. Để kiểm tra F_4 có là số nguyên tố không ta có thể chia nó lần lượt cho các số nguyên tố có dạng trên mà không vượt quá $\sqrt{F_4}$ (nghĩa là nhỏ hơn 2^8). Số duy nhất thỏa mãn các điều kiện này là 193 do đó vì $F_4 = 65637$ không chia hết cho 193 nên nó là số nguyên tố.

Bây giờ xét số F_5. Theo Định lý 5 thì mọi ước số nguyên tố của số này có dạng $2^7 k + 1 = 128k + 1$. Thay $k = 1, 2, 3, 4, 5$ ta nhận được các số nguyên tố với $k = 2$ và $k = 5$. Các số này là 257 và 641.

Chia $F_5 = 2^{32}+1$ cho các số này ta thấy nó chia hết cho số thứ hai. Hệ quả là F_5 là hợp số. Cụ thể $641 | F_5$. Chứng minh sơ cấp tính chất này như sau, ta có $641 = 5^4 + 2^4 \,|\, 5^4 \cdot 2^{28} + 2^{32}$ và $641 = 5 \cdot 2^7 + 1 \,|\, 5^2 \times 2^{14} - 1 \,|\, 5^4 \cdot 2^{28} - 1$, suy ra 641 là ước số của hiệu các số $5^4 \cdot 2^{28} + 2^{32}$ và $5^4 \cdot 2^{28} - 1$ nghĩa là số $2^{32}+1 = F_5$. Ta có $F_5 = 641 \cdot 6700417$. Vì $\sqrt{6700417} < 2600$ và các ước số nguyên tố của 6700417 (là các ước số của F_5) đều có dạng $128k+1$ với $k = 5, 6, \ldots,$ nên để kiểm tra 6700417 có phải số nguyên tố hay không chỉ cần chia số này cho $128k+1$ với $5 \le k \le 20$. Tuy nhiên tất cả các phép chia này đều có số dư dương. Vì vậy 6700417 là số nguyên tố. Vậy F_5 là tích của hai số nguyên tố. Kết quả này được tìm ra bởi Euler vào năm 1732.

Các ước số nguyên tố của F_6 phải có dạng $256k+1$. Ước số đầu tiên dạng này nhận được khi $k = 1071$ và đó là 274177. Do đó F_6 là hợp số. Kết quả này được Landry tìm ra năm 1880. Có thể chứng minh F_6 cũng là tích của hai số nguyên tố giống như F_5. Các ước số nguyên tố của F_7 phải có dạng $512k+1$. Ước số đầu tiên ứng với $k = 1165031037646443$ được tìm ra bởi M.J.Morrison và J.Brillhart năm 1975 với sự hỗ trợ của máy tính IBM 360/91. Nhân tử kia cũng là số nguyên tố. Trước đó, năm 1905, J.C.Morehead đã chứng minh F_7 là hợp số bằng cách sử dụng Định lý 6 mục 5. Các ước số nguyên tố của F_8 có dạng $1024k+1$. Ước số đầu tiên có dạng này ứng với $k = 1208689024954$ được tìm ra bởi R.P.Brent năm 1980. Trước đó, năm 1908, J.C.Morehead và A.E.Western đã chứng minh F_8 là hợp số bằng cách sử dụng Định lý 6. Sau đó năm 1981 Brent và H.C.Williams đã chứng minh nó là tích của hai số nguyên tố. Số F_9 là hợp số. Western đã tìm ra vào năm 1903 số $2^{11}k+1$ với $k = 2^5 \cdot 37$ là ước số nguyên tố của F_9. Số F_{10} là hợp số được phát hiện bởi J.L.Selfridge năm 1953. Với sự hỗ trợ của máy tính điện tử SWAC ông ta đã tính được $2^{12} \cdot 11131 + 1$ là một ước số nguyên tố của nó. Một ước số nguyên tố khác của số này là $2^{14} \cdot 395937 + 1$ được tìm ra bởi J.Brillhart năm 1962 với sự hỗ trợ của máy IBM 704.

Bài toán tìm dãy các ước số có vẻ dễ dàng hơn.

Năm 1899 Cunningham tìm ra hai ước số nguyên tố của F_{11} là $2^{13} \cdot 39 + 1$ và $2^{13} \cdot 119 + 1$. Bốn ước số nguyên tố của F_{12} đã được tìm ra là: $2^{14} \cdot 7 + 1$ tìm ra bởi Pervouchine và Lucas năm 1877; các ước số $2^{16} \cdot 397 + 1$ và $2^{16} \cdot 973 + 1$ tìm ra bởi Western năm 1903; ước số $2^{14} \cdot 11613415 + 1$ tìm ra bởi Hallyburton và Brillhart năm 1975.

Số F_{13} đã được chứng minh là hợp số bởi G.A.Paxson và F_{14} bởi J.L.Selfridge và Alexander Hurwitz, nhưng chưa có ước số nguyên tố nào của các số này được tìm ra. Gần đây J.R.Hallyburton và J.Brillhart đã tìm ra ước số $2^{16} \cdot 41365885 + 1$ của F_{13}. Số F_{15} được chứng minh hợp số năm 1925 bởi Kraitchik. Ông ta tính được $2^{21} \cdot 579 + 1$ là một ước số của nó. F_{16} được chứng minh là hợp số bởi Selfridge năm 1953. Sử dụng máy SWAC ông ta tính được ước số $2^{19} \cdot 1575 + 1$ của nó.

Kết quả sau cùng này quan trọng vì nó cho câu trả lời phủ định cho giả thuyết nói rằng tất cả các phần tử của dãy $2+1,\ 2^2+1,\ 2^{2^2}+1,\ 2^{2^{2^2}}+1,\ 2^{2^{2^{2^2}}}+1,\ \ldots$ đều là số nguyên tố. Thật vậy số F_{16} (có 19729 chữ số) là phần tử thứ 5 của dãy.

Câu hỏi F_{17} có phải là hợp số hay không mới được trả lời gần đây. Năm 1980 G.B.Gostin đã chỉ ra nó chia hết cho $2^{19} \cdot 59251857 + 1$. Số F_{18} là hợp số. Năm 1903 Western tìm được ước số nguyên tố $2^{20} \cdot 13 + 1$ của nó. Số F_{19} cũng là hợp số. Năm 1962 Riesel tìm được $2^{21} \cdot 33629 + 1$ là ước số nguyên tố của nó. Ta chưa biết F_{20}, F_{22} có phải là số nguyên tố hay không. Năm 1963 Wrathall chỉ ra F_{21} là hợp số và nó chia hết cho $2^{23} \cdot 534689 + 1$. Năm 1878 Pervouchine chỉ ra F_{23} chia hết cho số nguyên tố $2^{25} \cdot 5 + 1$. Vậy ta đã biết 84 số Fermat là hợp số với

$n = 5,\ 6,\ 7,\ 8,\ 9,10,11,\ 12,13,14,\ 15,16,\ 1\ 7,\ 18,19,\ 21,\ 23,\ 25,\ 26,27,\ 29,30,\ 32,\ 36,$
$38,\ 39,\ 42,\ 52,\ 55,\ 58,\ 62,\ 63,\ 66,\ 71,\ 73,\ 75,77,\ 81,91,\ 93,\ 99,117,125,\ 144,147,150,$
$201,205,\ 207,\ 215,\ 226,228,\ 250,255,\ 267,268,275,\ 284,287,\ 298,\ 316,\ 329,\ 334,$
$398,\ 416,452,544,556,\ 637,\ 692,\ 744,\ 931,1551,1945,\ 20232089,\ 2456,\ 3310,4724,$
$6537,6835,9428,\ 9448,\ 23471$

(Keller [1], [2], [3]). Số Fermat lớn nhất là hợp số đã được tìm ra là F_{23471}. Số này có ước số nguyên tố $2^{23473}\cdot 5+1$. Số các chữ số của F_{23471} là lớn hơn 10^{7064}. Tình huống tương tự được trình bày trong mục 3 và tính chia hết cũng được thực hiện theo cách đó.

Để kiểm tra F_n có chia hết cho m hay không đầu tiên ta ký hiệu $\overline{t}$ là số dư nhận được khi chia số nguyên t cho m. Ta định nghĩa dãy $r_k\ (k=1,2,\ldots,)$ bởi điều kiện

$$r_1 = 2^2, \qquad r_{k+1} = \overline{r_k^2}, \qquad k = 1,2,\ldots$$

Dễ dàng chứng minh bằng quy nạp $m \mid 2^{2^k} - r_k$ với $k = 1,2,\ldots$. Hệ quả là để biết F_n có chia hết cho m hay không ta chỉ cần tìm xem $r_n + 1$ có chia hết cho m hay không.

Ta chưa chứng minh được tồn tại vô hạn số Fermat là hợp số, hoặc chứng minh có ít nhất một số Fermat $> F_4$ là hợp số. Các sự kiện ở trên dẫn tới giả thuyết nói rằng mọi số Fermat $> F_4$ đều là hợp số.

Sử dụng Định lý 5 suy ra các ước số nguyên tố của các số Fermat đều có dạng $k\cdot 2^m + 1$ với k, m là các số tự nhiên. Ta đã nghiên cứu vấn đề khi nào thì các số dạng này là số nguyên tố. Nếu $k = 1$ thì $2^m + 1$ là số nguyên tố khi và chỉ khi nó là số Fermat. Hệ quả là ta biết chỉ có 5 số như vậy ứng với $m = 1,2,4,8,16$. Số nhỏ nhất ở dạng này mà ta chưa biết nó có phải số nguyên tố hay không là $2^{2^{20}} + 1$. Hệ quả là ta mới chỉ biết có 4 số có dạng $2\cdot 2^m + 1$ là số nguyên tố ứng với $m = 1,3,7,15$. Tuy nhiên ta đã biết 24 số nguyên tố có dạng $3\cdot 2^m + 1$ ứng với

$$m = 1,\ 2,5,\ 6,\ 8,12,18,30,\ 36,41,\ 66,189,\ 201,209,\ 276,\ 353,$$
$$408,438,\ 534,\ 2208,\ 2816,3168,3189,3912$$

Ta mới chỉ biết có 3 số nguyên tố có dạng $4\cdot 2^m + 1$ ứng với $m = 2,6,14$. Ta đã biết 17 số nguyên tố có dạng $5\cdot 2^m + 1$ ứng với

$$m = 1,\ 3,\ 7,13,\ 15,25,\ 39,55,\ 75,85,\ 127,\ 1947,3313,4687,5947,\ 13165,23473$$

Với mọi số tự nhiên $k < 3061$ ta biết ít nhất một số tự nhiên m mà $k\cdot 2^m + 1$ là số nguyên tố. Với $k = 3061$ thì $k\cdot 2^m + 1$ là hợp số với mọi $m < 17008$ (Robinson [2], Cormackand Williams [1], Baillie, Cormackand Williams [1], Jaeschke [1], Keller [1]). Mặt khác có thể chứng minh tồn tại vô hạn các số tự nhiên k mà $k\cdot 2^m + 1$ là hợp số với $m = 1,2,\ldots$ (bài tập 3). Với $n = 39$ và $n = 207$ ta có $3\cdot 2^{n+2} + 1 \mid F_n$. Với $n = 5,\ 23,\ 73,125,1945,\ 23471$ ta có $5\cdot 2^{n+2} + 1 \mid F_n$ và do đó $5\cdot 2^{n+3} + 1 \mid F_n$ với $n = 36$ và 3310. Nếu với các số có dạng $k\cdot 2^m + 1$ đặt $k = m = n$ thì ta nhận được các số Cullen $C_n = n\cdot 2^n + 1$ (Beeger [2]). A.J.C.Cunningham và H.J.Woodall [1] đã chứng minh rằng mọi số Cullen C_n với $1 < n < 141$ đều là hợp số và có các ước số nguyên tố nhỏ. Tuy nhiên C_{141} là số nguyên tố (Robinson [2]).

Bài tập. ***1.*** Chứng minh rằng nếu m là số tự nhiên $\neq 3$ thì $2^m + 1$ không phải lũy thừa với số mũ lớn hơn 1.

Chứng minh. Đầu tiên ta chứng minh rằng nếu m là số tự nhiên $\neq 3$ thì 2^m+1 không phải bình phương một số tự nhiên. Thật vậy nếu $2^m+1 = n^2$, với n là số tự nhiên thì n lẻ và >1 hơn nữa >3 vì $n=3$ suy ra $m=3$ mâu thuẫn với giả thiết. Do đó $2^m=n^2-1=(n-1)(n+1)$ vì vậy $n-1=2^k$, $n+1=2^{m-k}$ với k là số tự nhiên nằm giữa 1 và m, $k<m-k$. Vì vậy $2^{m-k}-2^k=2$ vô lý vì $k>1$. Giả sử $m\neq 3$ và $2^m+1=n^8$ với s là số tự nhiên >2. Vì 2^m+1 không phải bình phương, s lẻ. Hệ quả $2^m=n^s-1=(n-1)\left(n^{s-1}+n^{s-2}+\ldots+n+1\right)$ vô lý vì nhân tử thứ hai là tổng của lẻ số lẻ nên nó cũng là số lẻ >1. Điều phải chứng minh. □

2. Chứng minh các số Fermat $m=2^{2^n}+1(n=0,1,2,\ldots,)$ thỏa mãn $m\mid 2^m-2$.

Chứng minh. Với mọi số nguyên $n\geq 0$ ta có $n+1\leq 2^n$ suy ra $2^{n+1}\mid 2^{2^n}$ và hệ quả là $2^{2^{n+1}}-1\mid 2^{2^{2^n}}-1$ và vì $m=2^{2^n}+1\mid 2^{2^{n+1}}-1$ suy ra $m\mid 2^{2^{2^n}}-1$ vậy hệ quả là $m\mid 2^m-2$. □

Ghi chú. Kết quả trên chứng tỏ các số Fermat là hợp số đều là số giả nguyên tố (Chương 5 mục 7). Có thể chứng minh nếu với số tự nhiên k số $m=2^k+1$ thỏa mãn $m\mid 2^m-2$ thì m là số Fermat (Jakobczyk [1] trang 122 Định lý 10).

3. Chứng minh rằng tồn tại vô hạn số tự nhiên k mà với mọi số $k\cdot 2^n+1$ đều là hợp số với mọi số tự nhiên n.

Chứng minh. Ta đã biết F_m là các số nguyên tố với $m=0,1,2,3,4$. Hơn nữa F_5 là tích của hai số nguyên tố là 641 và p với $p>F_4$. Theo định lý số dư Trung Hoa suy ra tồn tại vô hạn số tự nhiên k thỏa mãn

(18) $$k\equiv 1\left(\mathrm{mod}\left(2^{32}-1\right)641\right) \text{ và } k\equiv -1(\mathrm{mod}\, p)$$

Ta sẽ chứng minh nếu k là số tự nhiên như vậy và lớn hơn p thì tất cả các số $k\cdot 2^n+1$, $n=1,2,\ldots$ là hợp số. Giả sử $n=2^s(2t+1)$ với s là một trong các số $0,1,2,3,4$ và t là số nguyên tùy ý ≥ 0. Theo ***(18)*** ta có $k\cdot 2^n+1\equiv 2^{2^s(2t+1)}+1\left(\mathrm{mod}\, 2^{32}-1\right)$ và vì $F_s\mid 2^{32}-1$ và $F_s\mid 2^{2^s(2t+1)}+1$ suy ra số $k\cdot 2^n+1$ chia hết cho F_s và lớn hơn $p>F_s$, số này là hợp số. Đặt $n=2^5(2t+1)$ với $t=0,1,2,\ldots,$ theo ***(18)*** ta có $k\cdot 2^n+1\equiv 2^{2^5(2t+1)}+1(\mathrm{mod}\, 641)$ và vì $641\mid 2^{2^5}+1\mid 2^{2^5(2t+1)}+1$ ta suy ra số $k\cdot 2^n+1$ chia hết cho 641. Nhưng số này lớn hơn 641 nên nó là hợp số. Bây giờ xét trường hợp n chia hết cho 2^6 nghĩa là $n=2^6t$ với $t=1,2,\ldots$ Theo ***(18)*** ta có $k\cdot 2^n+1\equiv -2^{2^6t}+1(\mathrm{mod}\, p)$. Nhưng $p\mid 2^{2^5}+1\mid 2^{2^6}-1\mid 2^{2^6t}-1$ suy ra $k\cdot 2^n+1$ chia hết cho p và lớn hơn p nên nó là hợp số. Vậy $k\cdot 2^n+1$ là hợp số với mọi $n=1,2,\ldots$ (Sierpinski [28] và Aigner [1]). □

4. Tìm tất cả các số nguyên tố có dạng n^n+1 với n là số tự nhiên và không có quá 300000 chữ số.

Lời giải. Chỉ có 3 số thỏa mãn. Đó là $1^1+1=2$, $2^2+1=5$, $4^4+1=257$. Thật vậy nếu n^n+1 với n là số tự nhiên là số nguyên tố thì n không có ước số lẻ >1 và do đó $n=2^k$ với k là số tự nhiên. Nhưng khi đó $n^n+1=2^{2^k}+1$ suy ra k không có ước số lẻ >1 và do đó $k=2^s$ với s là số nguyên >0. Vì vậy $n^n+1=F_{2^s+s}$. Do đó với $s=0$ ta nhận được $F_1=5$, với $s=1$ là $F_3=257$, với $s=2$ và $s=3$ thì F_6 và F_{11} là hợp số, với $s=4$ ta nhận được $F_{20}>2^{2^{20}}>2^{10^6}$, nhưng số này có nhiều hơn 300000 chữ số (Sierpinski [20]).

5. Tìm tất cả các số nguyên tố có dạng $n^{n^n}+1$ mà không có quá 10^{616} chữ số.

Lời giải. Chỉ có hai số như vậy là $1^1+1=2,\ 2^{2^2}+1=17$. Chứng minh tương tự bài toán trên. Đầu tiên ta chứng minh nếu $n>2$ và số $n^{n^n}+1$ là nguyên tố thì $n=2^{2^s}$ với s là số tự nhiên. Khi đó $n^{n^n}+1=F_{2^{2^s+s}+s}$. Với $s=1,2$ ta nhận được các hợp số F_9, F_{66}, với $s=3$ ta nhận được F_{2053} có nhiều hơn 10^{616} chữ số. Vậy nếu không tồn tại số nguyên tố có dạng $n^{n^n}+1$ với $n>2$ thì tồn tại vô hạn số Fermat là hợp số. □

6. Chứng minh rằng trong các số $2^{2^n}+3, n=1,2,\ldots,$, có vô hạn hợp số.

Chứng minh. Ta chứng minh các số $2^{2^{2^k+1}}+3$ với $k=1,2,\ldots,$ đều là hợp số. Thật vậy ta đã biết với mọi số tự nhiên k ta đều có $2^{2k}=3l+1$ với l là số tự nhiên. Vì vậy $2^{2^{2^k+1}}+3=2^{6l+2}+3=4\left(2^3\right)^{2l}+3\equiv 4+3\equiv 0\left(\mathrm{mod}\,7\right)$. Nhưng do với mọi số tự nhiên k thì số $2^{2^{2^k+1}}+3>7$ do đó nó là hợp số. □

Bài toán hỏi rằng trong các số có dạng $2^{2^n}+3$ có vô hạn số nguyên tố vẫn là câu hỏi mở.

7. Chứng minh rằng tất cả các số $2^{2^n}+5,\ n=1,2,\ldots,$ đều là hợp số.

Chứng minh. Tất cả các số này chia hết cho 3. □

5. Điều kiện cần và đủ để một số Fermat là số nguyên tố

Định lý 5. *Số Fermat F_n với n là số tự nhiên là số nguyên tố khi và chỉ khi $F_n \mid 3^{(F_n-1)/2}+1$.*

Chứng minh. Ký hiệu n là số tự nhiên.

Giả sử $F_n \mid 3^{(F_n-1)/2}+1$ thì F_n không chia hết cho 3. Giả sử p là ước số nguyên tố (khác 3) bất kỳ của F_n. Ký hiệu δ là cấp của $3 \bmod p$. Vì $p \mid 3^{F_n-1}-1$ suy ra $\delta \mid F_n-1=2^{2^n}$. Nếu $\delta < 2^{2^n}$ thì $\delta=2^k$ với k là số nguyên không âm $<2^n$. Hệ quả là $2^k \mid 2^{2^{n-1}}=\left(F_n-1\right)/2$ do đó $\delta \mid \left(F_n-1\right)/2$ và vì vậy do $p \mid 3^\delta-1,\ p \mid 3^{(F_n-1)/2}-1$ nên vì $p \mid F_n$ ta có $p \mid 3^{(F_n-1)/2}+1$ suy ra $p \mid 2$ vậy $p=2$. Điều này là vô lý vì $p \mid F_n$ và F_n lẻ. Vậy $\delta=2^{2^n}$. Nhưng ta đã biết $\delta \mid p-1$ suy ra $p=2^{2^n}k+1$ với k là số tự nhiên. Từ đây suy ra $p \geq 2^{2^n}+1$ và vì $p \mid F_n$ nên ta có $F_n=p$ chứng tỏ F_n là số nguyên tố. Điều kiện đủ được chứng minh. Để chứng minh điều kiện cần ta chứng minh bổ đề sau đây

Bổ đề. *Nếu p là số nguyên tố có dạng $12k+5$ thì $p \mid 3^{(p-1)/2}+1$.*

Chứng minh bổ đề. Nếu p là số nguyên tố và $p=12k+5$ thì theo tính chất của ký hiệu Legendre ta có $\left(\frac{p}{3}\right)=\left(\frac{-1}{3}\right)=-1$ suy ra theo tính chất 5 của ký hiệu Legendre thì $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right)=1$ và hệ quả là $\left(\frac{3}{p}\right)=-1$ do đó $3^{(p-1)/2}\equiv -1\left(\mathrm{mod}\,p\right)$. Vậy $p \mid 3^{(p-1)/2}+1$. Điều phải chứng minh. □

Xét số tự nhiên n. Số $F_n=2^{2^n}+1$ có dạng $12k+5$ vì với mọi số tự nhiên n ta có $2^n=2m$ và dễ dàng chứng minh bằng quy nạp $4^m\equiv 4\left(\mathrm{mod}12\right)$ với mọi $m=1,2,\ldots$ và hệ quả là $F_n=4^m+5\equiv 5\left(\mathrm{mod}12\right)$ nghĩa là $F_n=12k+5$ và nếu F_n là số nguyên tố thì theo bổ đề $F_n \mid 3^{(F_n-1)/2}+1$. Định lý được chứng minh. □

Từ Định lý 5 suy ra nếu F_n là số nguyên tố thì 3 là căn nguyên thủy của F_n. Chứng minh điều này nhận được với lưu ý là 3 có cấp $F_n - 1 \bmod F_n$ được suy trực tiếp từ chứng minh Định lý 5. Áp dụng Định lý 5 ta có thủ tục hữu hiệu để kiểm tra xem một số Fermat F_n có là số nguyên tố hay không. Ký hiệu $\overline{t}$ là phần dư nhận được khi chia số nguyên t cho F_n và đặt

$$r_1 = 3, \qquad r_{k+1} = \overline{r_k^2}, \qquad k = 1, 2, \ldots$$

Bằng quy nạp ta chứng minh được $F_n \mid 3^{2^{k-1}} - r_k$ với mọi $k = 1, 2, \ldots$ Vì vậy với $k = 2^n$ ta có $F_n \mid 3^{(F_n-1)/2} - r_{2^n}$. Từ đây suy ra $3^{(F_n-1)/2} + 1$ đồng dư với $r_{2^n} + 1 \bmod F_n$.

Bằng phương pháp này ta chứng minh được các số F_7, F_8, F_{13} và F_{14} là hợp số. Số F_7 có 39 chữ số vì vậy để tìm được số $r_{2^7} + 1 = r_{128} + 1$ bằng cách áp dụng thủ tục ở trên ta cần tính vài trăm phép tính với ba mươi bình phương các số tự nhiên, mỗi số có ít hơn 39 chữ số. Hơn nữa các bình phương này cần phải đem chia cho F_7 (có 39 chữ số). Sự phức tạp của các phép tính này không phải vấn đề lớn đối với các máy tính diện tử, nhưng vào năm 1905 (nghĩa là khi Morehead tìm được kết quả này) thì lượng tính toán thủ công là vô cùng lớn.

Phương pháp tương tự cũng được áp dụng để chỉ ra F_8, F_{13} và F_{14} là hợp số.

Phương pháp trình bày ở trên không cho thêm thông tin về các ước số nguyên tố của các số được xét cũng như cách phân tích chúng thành tích của hai thừa số > 1. Đây là lý do vì sao chúng ta chưa có những phân tích thành thừa số của F_{14}.

Số Fermat tiếp theo là F_{20} có hơn 300000 chữ số, các tính toán mô tả ở trên trong trường hợp này yêu cầu hơn một triệu phép chia các số có hơn vài trăm nghìn chữ số, mỗi số đều có nhiều hơn 300000 chữ số.

Bài tập. Tìm ước số nguyên tố nhỏ nhất của $12^{2^{15}} + 1$.

Lời giải. Theo Định lý 4 thì các ước số nguyên tố của $12^{2^{15}} + 1$ đều có dạng $2^{16}k + 1$ với k là số tự nhiên. Hệ quả là $p \geq 2^{16} + 1 = F_4$. Vì F_4 là số nguyên tố nên theo Định lý 5 ta có $F_4 \mid 3^{2^{15}} + 1$. Vì vậy $3^{2^{15}} \equiv -1 \pmod{F_4}$. Nhưng theo định lý nhỏ Fermat ta có $2^{2^{16}} = 2^{F_4 - 1} \equiv 1 \pmod{F_4}$ suy ra $4^{2^{15}} \equiv 1 \pmod{F_4}$. Vì vậy $12^{2^{15}} = 3^{2^{15}} \cdot 4^{2^{15}} \equiv -1 \pmod{F_4}$ do đó $F_4 \mid 12^{2^{15}} + 1$. Vậy ta thấy F_4 là ước số nguyên tố nhỏ nhất của $12^{2^{15}} + 1$, hơn nữa số này $> F_4$ và vì vậy nó là hợp số.

Ta chưa biết có tồn tại vô hạn hợp số có dạng $12^{2^n} + 1$ với $n = 1, 2, \ldots,$ hay là trong số đó có vô hạn các số nguyên tố hay không.

CHƯƠNG 11

BIỂU DIỄN CÁC SỐ TỰ NHIÊN THÀNH TỔNG CÁC LŨY THỪA BẬC k KHÔNG ÂM

1. Tổng của hai bình phương

Định lý 1. *Số tự nhiên n là tổng của hai bình phương khi và chỉ khi trong phân tích thành thừa số nguyên tố của n thì các số nguyên tố có dạng $4k+3$ đều có số mũ lẻ.*

Bổ đề. *Mọi số nguyên tố lẻ p là ước số của tổng hai bình phương nguyên tố cùng nhau đều có dạng $4k+1$.*

Chứng minh bổ đề. Giả sử a,b là 2 số nguyên nguyên tố cùng nhau và số nguyên tố lẻ p thỏa mãn $p \mid a^2+b^2$. Thế thì $a^2 \equiv (-1)^{(p-1)/2} b^{p-1} \pmod p$; suy ra $a^{p-1} \equiv (-1)^{(p-1)/2} b^{p-1} \pmod p$. Nhưng vì $(a,b)=1$, các số a,b không chia hết cho p, suy ra theo định lý Fermat nhỏ ta có $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod p$; hệ quả là $(-1)^{(p-1)/2} \equiv 1 \pmod p$, mà $p>2$ suy ra $(-1)^{(p-1)/2}=1$ vậy $(p-1)/2$ chẵn nên p có dạng $4k+1$. □

Chứng minh định lý. Giả sử n là tổng hai bình phương

(1) $$n = a^2 + b^2$$

Xét phân tích thành thừa số nguyên tố

(2) $$n = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$$

Giả sử p là ước số nguyên tố có dạng $4k+3$ của n. Ký hiệu $d=(a,b), a=da_1, b=db_1$ với $(a_1,b_1)=1$. Theo ***(1)*** thì $d^2 \mid n$, và do đó $n=d^2 n_1$, với n_1 là số tự nhiên. Giả sử số mũ của p trong phân tích ***(2)*** là lẻ thì vì $n=d^2 n_1$ ta có $p \mid n_1 = a_1^2 + b_1^2$, mâu thuẫn với bổ đề. Ta đã chứng minh xong điều kiện cần.

Để chứng minh điều kiện đủ chú ý rằng không giảm tổng quát có thể giả sử $n>1$. Ta có $1=1^1+0^2$. Giả sử ***(2)*** là phân tích thành thừa số nguyên tố của n. Ký hiệu m là số tự nhiên nhỏ nhất mà bình phương của nó là ước số của n. Khi đó $n=m^2 k$, với k bằng 1 hoặc là tích của các số nguyên tố khác nhau mà không có số nào có dạng $4k+3$. Vì $2=1^2+1^2$ và theo Định lý 9 Chương 5 thì các số nguyên tố này là tổng của hai bình phương.

Từ đẳng thức $(a^2+b^2)(c^2+d^2) = (ab+cd)^2 + (ad-bc)^2$ suy ra tích của hai (và do đó hữu hạn) số tự nhiên mà mỗi số là tổng hai bình phương thì cũng là tổng của hai bình phương. Hệ quả là k là tổng hai bình phương. Do đó $k=u^2+v^2$, suy ra $n=m^2k=(mu)^2+(mv)^2$.

Điều kiện đủ được chứng minh. □

Một vấn đề được đặt ra là có bao nhiêu cách biểu diễn một số tự nhiên thành tổng hai bình phương như vậy. Câu trả lời có trong Chương 8 mục 9.

Hệ quả. *Số không phân tích được thành tổng hai bình phương nguyên thì cũng không phải tổng hai bình phương hữu tỷ.*

Chứng minh. Nếu n là số tự nhiên không phải tổng hai bình phương thì theo Định lý 1 suy ra trong phân tích thành thừa số nguyên tố của n có số nguyên tố p có dạng $4k+3$ với số mũ lẻ. Giả sử $n=\left(\frac{1}{m}\right)^2+\left(\frac{l_1}{m_1}\right)^2$ với m,m_1 là các số tự nhiên và l,l_1, là các số nguyên. Khi đó $(mm_1)^2 n = (lm_1)^2 + (l_1 m)^2$. Nhưng p phải có số mũ lẻ trong phân tích thành thừa số nguyên tố của

vế trái của đẳng thức và do đó theo Định lý 1 thì vế trái không thể phân tích thành tổng hai bình phương như trong vế phải. Mâu thuẫn suy ra hệ quả được chứng minh. □

E.Landau [1] đã chứng minh rằng nếu $f(x)$ ký hiệu số các số tự nhiên $\le x$ là tổng của hai bình phương thì $f(x):\dfrac{x}{\sqrt{\log x}}$ tiến tới một giới hạn dương hữu hạn khi x tăng vô hạn.

Biểu diễn $n=x^2+y^2$, với x,y là các số nguyên $0\le x\le y$, và $n\le 10000$, được trình bày bởi A.van Wijngarden [1]. Số cách phân tích n thành tổng hai bình phương với $n\le 20000$ được trình bày bởi I H.Gupta [2]. Với mọi số nguyên tố $p\le 10007401$ có dạng $4k+1$ thì bảng các phân tích như vậy trình bày bởi Kogbetlianz và Krikorian [1].

Bài tập. *1.* Tìm điều kiện cần và đủ để số hữu tỷ l/m có thể biểu diễn thành tổng bình phương hai số hữu tỷ.

Lời giải. Điều kiện cần và đủ là lm là tổng của hai bình phương nguyên.

Lưu ý nếu $\dfrac{l}{m}=\left(\dfrac{l_1}{m_1}\right)^2+\left(\dfrac{l_2}{m_2}\right)^2$ thì $lm\left(m_1m_2\right)^2=\left(mm_2l_1\right)^2+\left(mm_1l_2\right)^2$.

Mặt khác $lm=a^2+b^2$ suy ra $\dfrac{l}{m}=\left(\dfrac{a}{m}\right)^2+\left(\dfrac{b}{m}\right)^2$

Ghi chú. Từ bài tập 1 và Định lý 1 suy ra phân số tối giản l/m, với l,m là các số tự nhiên, là tổng của hai bình phương hữu tỷ khi và chỉ khi mỗi số l,m đều là tổng của hai bình phương nguyên.

2. Chứng minh rằng nếu số hữu tỷ $r\ne 0$ là tổng hai bình phương hữu tỷ thì có vô hạn cách biểu diễn số đó như là tổng hai bình phương hữu tỷ dương.

Chứng minh. Giả sử $r=a^2+b^2$, với a,b là các số hữu tỷ khác 0. Không giảm tổng quát có thể giả sử a,b dương và $a\ge b$. Với mọi số tự nhiên k ta có $r=\left(\dfrac{\left(k^2-1\right)a-2kb}{k^2+1}\right)^2+\left(\dfrac{\left(k^2-1\right)b+2ka}{k^2+1}\right)^2$ là một biểu diễn của r thành tổng hai bình phương các số hữu tỷ. Nếu $k\ge 3$, ta có $3k^2-8k=3k(k-3)+3\ge 3$, suy ra $\dfrac{k^2-1}{2k}\ge\dfrac{4}{3}>\dfrac{b}{a}$ và do đó $n=a_k^2+b_k^2$, $k=3,4,\ldots,m+2$, $a_k=\dfrac{\left(k^2-1\right)a-2kb}{k^2+1}>0$. Hơn nữa dễ dàng chứng minh dãy a_k tăng theo k. Vì vậy các số a_k là phân biệt và với $k\ge 3$ thì các số này dương. Vậy với $k\ge 3$ ta có thể biểu diễn r thành tổng hai bình phương hữu tỷ dương khác nhau. Ta thấy r có vô hạn cách biểu diễn như vậy. Bây giờ giả sử $r=a^2$, với a là số hữu tỷ. Vì $r\ne 0$, ta có thể giả sử $a>0$. Với số tự nhiên k ta có $r=\left(\dfrac{\left(k^2-1\right)a}{k^2+1}\right)^2+\left(\dfrac{2ka}{k^2+1}\right)^2$. Rõ ràng $a_k=\left(k^2-1\right)a/\left(k^2+1\right)$ tăng theo k. Hệ quả là tồn tại vô hạn biểu diễn của r thành tổng hai bình phương hữu tỷ dương. □

3. Giả sử m là số tự nhiên. Tìm số tự nhiên n có ít nhất m biểu diễn thành tổng hai bình phương tự nhiên.

Lời giải. Đặt $n=a^2$, với $a=\left(3^2+1\right)\left(4^2+1\right)\ldots\left(\left(m+2\right)^2+1\right)$. Số $a/\left(k^2+1\right)$ là tự nhiên với mọi $k=3,4,\ldots,m+2$. Hệ quả là các số $a_k=\dfrac{k^2-1}{k^2+1}a;\ n_k=\dfrac{2ka}{k^2+1}$ $(k=3,4,\ldots,m+2)$ cũng là số tự nhiên.

Nhưng ta có đẳng thức $a^2=\left(\frac{k^2-1}{k^2+1}a\right)^2+\left(\frac{2ka}{k^2+1}\right)^2$. Nếu $a_k=\frac{k^2-1}{k^2+1}a,\quad b_k=\frac{2ka}{k^2+1}$ ta có $n=a^2=a_k^2+b_k^2$ với $k=3,4,\ldots,m+2$. Nhưng ta lại có $a_k-b_k=\frac{k^2-2k-1}{k^2+1}a=\frac{\left(k^2-1\right)^2-2}{k^2+1}a>0$ với $\lambda=3,4,\ldots,m+2$ và $a_k=a-\frac{2a}{k^2+1}$ suy ra $a_3<a_4<\ldots<a_{m+2}$.

Vì vậy các biểu diễn $n=a_k^2+b_k^2, k=3,4,\ldots,m+2$, đều khác nhau và có m biểu diễn tất cả. Do đó n có tính chất yêu cầu. Cùng lúc ta đã chứng minh được với mọi số tự nhiên m thì tồn tại ít nhất m tam giác Pythagoras phân biệt có tính chất trong giả thiết.

4. Cho trước biểu diễn n thành tổng hai bình phương. Tìm biểu diễn tương tự của $2n$.

Lời giải. Nếu $n=a^2+b^2$ thì $2n=\left(a+b\right)^2+\left(a-b\right)^2$

2. Số cách biểu diễn thành tổng hai bình phương

Ta tính số cách biểu diễn một số tự nhiên thành tổng của hai bình phương. Nếu n có thể biểu diễn thành tổng của hai bình phương nghĩa là

(3) $$n=x^2+y^2$$

thì $n\geq x^2$ và $n\geq y^2$, suy ra $|x|\leq\sqrt{n},|y|\leq\sqrt{n}$. Vì vậy chỉ cần thay các giá trị của mà $|x|$ không vượt quá $\sqrt{n}$ vào ***(3)*** và thử xem khi nào $n-x^2$ là bình phương đúng. Nếu $n-x^2$ là bình phương thì đặt $y=\pm\sqrt{n-x^2}$ và ta nhận được một biểu diễn của n thành tổng hai bình phương. Nếu với mọi x thì $n-x^2$ đều không phải bình phương thì biểu diễn như vậy là không tồn tại. Ta chỉ cần xét trường hợp x dương vì dấu của x không ảnh hưởng tới giá trị $n-x^2$.

Lưu ý rằng dãy $n,n-1^2,n-2^2,n-3^2,\ldots$ có hiệu liên tiếp là $1,3,5,\ldots,$ nghĩa là dãy các số tự nhiên lẻ liên tiếp. Ví dụ với $n=10$ ta có dãy $10,9,6,1$. Phần tử thứ hai của dãy là bình phương đúng vì vậy ta có $x=\pm1,y=\pm3,$ hoặc $x=\pm3,y=\pm1$. Có tất cả 8 biểu diễn cần tìm. Đó là

$$10=1^2+3^2=1^2+(-3)^2=(-1)^2+3^2=(-1)^2+(-3)^2=3^2+1^2$$
$$=3^2+(-1)^2=(-3)^2+1^2=(-3)^2+(-1)^2.$$

Xét $n=25$. Ta có dãy $25,24,\ 21,16,9,0$. Ở đây $25,16,9,0$ là các bình phương. Vì vậy ta có 12 biểu diễn thỏa mãn.

Ký hiệu $\tau(n)$ là số tất cả các biểu diễn của số tự nhiên n thành tổng hai bình phương. Hai biểu diễn là khác nhau ngay cả khi chúng sai khác một hoán vị. Ta có

$$\tau(1)=4,\quad \tau(2)=4,\quad \tau(3)=0,\quad \tau(4)=4,\quad \tau(5)=8,$$
$$\tau(6)=0,\quad \tau(7)=0,\quad \tau(8)=4,\quad \tau(9)=4,\quad \tau(10)=8.$$

Trong mục 5 Chương 5 ta đã biết mỗi số nguyên tố có dạng $4k+1$ đều có thể biểu diễn duy nhất (sai khác một hoán vị) thành tổng của hai bình phương. Suy ra với mọi số nguyên tố p có dạng $4k+1$ thì ta có $\tau(p)=8$.

Lập luận ở trên suy ra với mọi số tự nhiên n ta có $\tau(n)\leq4\sqrt{n}$.

Bài tập 3 mục 1 suy ra không có chặn trên của $\tau(n)$.

Bây giờ ta tính tổng

(4) $$T(n)=\tau(1)+\tau(2)+\ldots+\tau(n)$$

Số $\tau(k)$ là số nghiệm nguyên của phương trình $x^2+y^2=k$ vì vậy $T(n)$ là số nghiệm của

(5) $$0<x^2+y^2\le n$$

Ta chia các nghiệm của ***(5)*** thành các lớp mà hai nghiệm thuộc cùng một lớp khi và chỉ khi các giá trị x là bằng nhau. Ta tính số nghiệm trong mỗi lớp. Nếu $x=0$ thì theo ***(5)*** y có thể nhận các giá trị nguyên mà $y^2\le n$, nghĩa là $|y|\le\sqrt{n}$. Có $2\left[\sqrt{n}\right]$ khả năng như vậy. Nếu $x=k\ne 0$ thì theo ***(5)*** ta phải có $k^2\le n$; do đó $|k|\le\sqrt{n}$ và $y^2\le n-k^2$, suy ra $|y|\le\sqrt{n-k^2}$. Có $1+2\left[\sqrt{n-k^2}\right]$ số như vậy (1 có thể thêm vào khi $y=0$). Vì k nhận mọi giá trị $\pm1,\pm2,\ldots,\pm\left[\sqrt{n}\right]$ và các dấu $\pm$ không ảnh hưởng tới giá trị của k^2, nên

$$2\left[\sqrt{n}\right]+2\sum_{k=1}^{\left[\sqrt{n}\right]}\left(1+2\left[\sqrt{n-k^2}\right]\right)=4\left[\sqrt{n}\right]+4\sum_{k=1}^{\left[\sqrt{n}\right]}\left[\sqrt{n-k^2}\right]$$

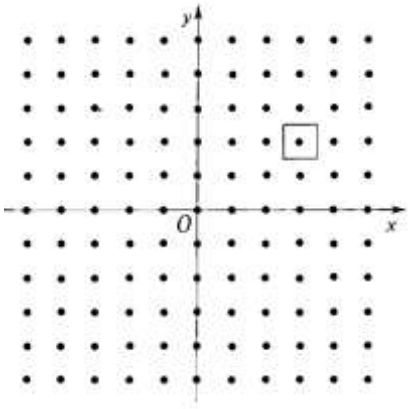
do đó

(6) $$T(n)=4\sum_{k=0}^{\left[\sqrt{n}\right]}\left[\sqrt{n-k^2}\right]$$

Vì vậy chẳng hạn với $n=100$ ta có

$$T(100)=4([\sqrt{100}]+[\sqrt{99}]+[\sqrt{96}]+[\sqrt{91}]+[\sqrt{84}]+[\sqrt{75}]+$$
$$+[\sqrt{64}]+[\sqrt{51}]+[\sqrt{36}]+[\sqrt{19}])=4(10+9+9+9+9+8+$$
$$+8+7+6+4)=316.$$

Tổng ***(4)*** có mô tả hình học khá đơn giản. Ta đã biết $1+T(n)$ là số các cặp số nguyên mà $x^2+y^2\le n$, số này bằng với số các điểm có tọa độ nguyên trong mặt phẳng (điểm nguyên) chứa trong hình tròn C với tâm là $(0,0)$ và bán kính $\sqrt{n}$. Bây giờ với mỗi điểm nguyên ta xét hình vuông nhận nó là tâm và các cạnh song song với các trục tọa độ và diện tích là 1. Diện tích P bị phủ bởi các hình vuông nhận được từ các điểm nguyên không nằm bên ngoài C bằng với số điểm đó, tức là $1+T(n)$. Hình tròn C_1 với tâm $(0,0)$ và bán kính $\sqrt{n}+\frac{1}{\sqrt{2}}$ chứa các điểm bị phủ bởi hình vuông ứng với các điểm của hình tròn C. Vì $1/\sqrt{2}$ là khoảng cách lớn nhất giữa một điểm nằm trong hình vuông diện tích 1 tới tâm của nó do đó diện tích P nhỏ hơn diện tích của hình tròn C_1. Vì vậy $P\le\pi\left(\sqrt{n}+\frac{1}{\sqrt{2}}\right)^2$.



Mặt khác diện tích của hình tròn C_2 với tâm $(0,0)$ và bán kính $\sqrt{n}-\frac{1}{\sqrt{2}}$ là nhỏ hơn P, nên $P>\pi\left(\sqrt{n}-\frac{1}{\sqrt{2}}\right)^2$. Vì vậy từ đẳng thức $P=1+T(n)$ suy ra

(7) $$\pi\left(\sqrt{n}-\frac{1}{\sqrt{2}}\right)^2-1<T(n)<\pi\left(\sqrt{n}+\frac{1}{\sqrt{2}}\right)^2-1$$

Lưu ý $\pi\sqrt{2}<5$ và với mọi số tự nhiên $n, 0<\frac{1}{2}\pi-1<1\le\sqrt{n}$. Vì vậy

$$\pi\left(\sqrt{n}+\frac{1}{\sqrt{2}}\right)^2-1=\pi n+\pi\sqrt{2}\sqrt{n}+\frac{1}{2}\pi-1<\pi n+6\sqrt{n}$$

$$\pi\left(\sqrt{n}-\frac{1}{\sqrt{2}}\right)^2-1=\pi n-\pi\sqrt{2}\sqrt{n}+\frac{1}{2}\pi-1>\pi n-6\sqrt{n}$$

Theo ***(7)*** ta có $\pi n-6\sqrt{n}<T(n)<\pi n+6\sqrt{n}$, suy ra $T(n)-\pi n|<6\sqrt{n}$ với mọi số tự nhiên n, suy ra

(8) $$\left|\frac{T(n)}{n}-\pi\right|<\frac{6}{\sqrt{n}}$$

Từ ***(8)*** và ***(4)*** suy ra $\lim\limits_{n\to\infty}\frac{\tau(1)+\tau(2)+\ldots+\tau(n)}{n}=\pi$ nghĩa là giá trị trung bình của hàm $\tau(n)$ là π. Do đó π là giá trị trung bình của số cách biểu diễn một số tự nhiên thành tổng hai bình phương. Ta có $T(100)=316$ nghĩa là một số tự nhiên không lớn hơn 100 có trung bình 3.16 cách biểu diễn thành tổng hai bình phương. Tương tự theo ***(6)*** ta tính được $T(400)=1256$ suy ra $T(400)/400=3.14$ và $T(1000)=3148$ suy ra $T(1000)/1000=3.148$. Theo ***(6)*** $T(n)$ có thể tính với mọi n (các tính toán có thể rất dài), và từ ***(8)*** ta có phương pháp tính với sai số cho trước.

Từ ***(8)*** ta có $|T(n)-\pi n|<6\sqrt{n}$ với mọi số tự nhiên n.

Năm 1906 tôi ***(Sierpinski)*** đã sử dụng phương pháp của Voronoi để chỉ ra tồn tại hằng số A thỏa mãn $|T(n)-\pi n|<A\sqrt[3]{n}$ (Sierpinski [1]). Kết quả mạnh hơn được tìm ra bởi Van der Corput và những người khác. Kết quả tốt nhất tới nay có trong Ivic [1].

Ở trên ta đã tính số điểm nguyên chứa trong hình tròn tâm $(0,0)$. Năm 1957, H.Steinhaus [1] đặt ra bài tập sau: *chứng minh rằng với mọi số tự nhiên n thì luôn tồn tại hình tròn chứa đúng n điểm nguyên.* Ta sẽ chứng minh nếu $p=\left(\sqrt{2},\frac{1}{3}\right)$ thì với mọi số tự nhiên n luôn tồn tại hình tròn C_n với tâm p chứa đúng n điểm nguyên bên trong.

Thật vậy, giả sử hai điểm (x_1,y_1) và (x_2,y_2) phân biệt và cách đều p.

Thế thì $\left(x_1-\sqrt{2}\right)^2+\left(y_1-\frac{1}{3}\right)^2=\left(x_2-\sqrt{2}\right)^2+\left(y_2-\frac{1}{3}\right)^2$.

Suy ra $2(x_2-x_1)\sqrt{2}=x_2^2+y_2^2-x_1^2-y_1^2+\frac{2}{3}(y_1-y_2)$

Vì $\sqrt{2}$ là số vô tỷ, $x_1-x_2=0$, suy ra $y_2^2-y_1^2+\frac{2}{3}(y_1-y_2)=0$, và do đó $(y_2-y_1)\left(y_2+y_1-\frac{2}{3}\right)=0$.

Nhưng $y_2+y_1-\frac{2}{3}\neq 0$ vì y_1 và y_2 là các số nguyên, hệ quả là $y_2-y_1=0$. Suy ra $x_1=x_2$ và $y_1=y_2$ mâu thuẫn với giả thiết các điểm này là phân biệt.

Ký hiệu n là số tự nhiên tùy ý. Rõ ràng mọi hình tròn C với tâm p và bán kính đủ lớn chứa nhiều hơn n điểm nguyên. Hơn nữa số điểm nguyên chứa trong C là hữu hạn. Ở trên ta đã chứng minh

khoảng cách từ p tới các điểm nguyên đều phân biệt, nên ta có thể sắp xếp các điểm nguyên nằm trong C theo dãy $p_1, p_2, \ldots, p_n, p_{n+1}, \ldots$ ứng với các khoảng cách tăng dần từ các điểm đó tới p. Ký hiệu C_n là hình tròn tâm p và bán kính bằng khoảng cách từ p_{n+1} tới p. Rõ ràng các điểm nguyên chứa trong C_n là $p_1, p_2, \ldots, p_n$. Do đó hình tròn C_n có tính chất yêu cầu. Định lý Steinhaus được chứng minh.

Có thể chứng minh không có điểm nào trong mặt phẳng với tọa độ hữu tỷ có tính chất: *với mọi số tự nhiên n thì luôn tồn tại hình tròn nhận điểm đó làm tâm và chứa đúng n điểm nguyên* (Sierpinski [19] trang 26). Mặt khác có thể chứng minh với mọi số tự nhiên n thì luôn tồn tại hình tròn có tâm có tọa độ hữu tỷ và chứa đúng n điểm nguyên bên trong. H.Steinhaus đã chứng minh rằng với mọi số tự nhiên n thì luôn tồn tại hình tròn với diện tích n chứa đúng n điểm nguyên bên trong. Tuy nhiên chứng minh điều này khá khó. Có thể chứng minh rằng với mọi số tự nhiên n thì luôn tồn tại hình vuông chứa đúng n điểm nguyên bên trong (Sierpinski [19] trang 28-30).

Với mọi số tự nhiên n thì trong không gian luôn tồn tại hình cầu chứa đúng n điểm có tọa độ nguyên. Để chứng minh điều này chỉ cần lưu ý rằng nếu u, v, w là các số hữu tỷ thỏa mãn $u\sqrt{2}+v\sqrt{3}+\mathrm{w}\sqrt{5}$ thì $u=v=\mathrm{w}=0$, và hình cầu có tâm là $\left(\sqrt{2},\sqrt{3},\sqrt{5}\right)$ với bán kính 3 chứa ít nhất một điểm nguyên. Từ hai nhận xét này chứng minh được quy về trường hợp hình tròn trên mặt phẳng. J.Browkin đã chứng minh với mọi số tự nhiên n thì luôn tồn tại hình lập phương (trong không gian ba chiều) mà chứa đúng n điểm nguyên.

A.Schinzel [7] đã chứng minh rằng *với mọi số tự nhiên n thì luôn tồn tại hình tròn mà trên biên của nó có đúng n điểm nguyên*. Cụ thể nếu n lẻ, nghĩa là $n=2k+1$, với k là số nguyên không âm thì hình tròn với tâm $\left(\frac{1}{3},0\right)$ và bán kính $5^k/3$ có tính chất yêu cầu. Nếu n chẵn, nghĩa là $n=2k$, với k là số tự nhiên thì hình tròn với tâm $\left(\frac{1}{2},0\right)$ và bán kính $5^{(k-1)/2}/2$ có tính chất yêu cầu. T.Kulikowski [1] đã chứng minh với mọi số tự nhiên n thì luôn tồn tại hình cầu trong không gian ba chiều mà trên biên của nó chứa đúng n điểm nguyên. Ông ta cũng mở rộng định lý này cho các hình cầu chiều cao.

Các điểm hữu tỷ (nghĩa là các điểm có tọa độ là các số hữu tỷ) trên biên của hình tròn cũng đã được nghiên cứu. Tồn tại đường tròn mà không chứa điểm hữu tỷ nào chẳng hạn $x^2+y^2=3$. Có các đường tròn đi qua đúng 1 điểm hữu tỷ chẳng hạn đường tròn $\left(x-\sqrt{2}\right)^2+\left(y-\sqrt{2}\right)^2=4$ chỉ đi qua duy nhất một điểm hữu tỷ là $(0,0)$. Có đường tròn đi qua đúng hai điểm hữu tỷ chẳng hạn $x^2+\left(y-\sqrt{2}\right)^2=3$ chỉ đi qua các điểm hữu tỷ $(1,0)$ và $(-1,0)$. Tổng quát hơn ta chứng minh *nếu có ba điểm hữu tỷ trên biên một hình tròn thì có vô hạn điểm hữu tỷ trên đó.* Dễ dàng chứng minh rằng nếu có ba điểm hữu tỷ trên biên hình tròn thì hình tròn đó có tâm là điểm hữu tỷ và bình phương bán kính của nó cũng là hữu tỷ. Không giảm tổng quát có thể giả sử tâm của hình tròn là $(0,0)$. Ký hiệu hình tròn là C. Không khó chứng minh được nếu đường tròn C chứa ít nhất một điểm hữu tỷ thì nó chứa vô hạn điểm hữu tỷ. Thật vậy nếu a,b là các số hữu tỷ thỏa mãn $a^2+b^2=r^2$ thì với mọi số hữu tỷ t điểm (x,y) với $x=\dfrac{2at+b\left(1-t^2\right)}{1+t^2}$, $y=\dfrac{a\left(1-t^2\right)-2bt}{1+t^2}$ là điểm hữu tỷ và $x^2+y^2=r^2$.

Vậy với một đường tròn cho trước thì chỉ có các khả năng sau: nó không chứa điểm hữu tỷ nào; hoặc chứa đúng một điểm hữu tỷ; hoặc chứa đúng hai điểm hữu tỷ; hoặc chứa vô hạn điểm hữu tỷ. Có thể chứng minh rằng trong trường hợp cuối thì tập hợp các điểm hữu tỷ trù mật trên đường tròn, nghĩa là với mọi cung của đường tròn thì đều có ít nhất một điểm hữu tỷ nào đó.

Sierpinski [21] đã chứng minh nếu r^2 là số hữu tỷ thì đường tròn C với bán kính r chứa vô hạn điểm mà khoảng cách giữa chúng đôi một là hữu tỷ. Từ đây suy ra với mọi số tự nhiên n thì luôn tồn tại đường tròn chứa n điểm mà khoảng cách đôi một giữa chúng đều là số tự nhiên.

Một hệ quả quan trọng khác là với mọi số tự nhiên n thì luôn tồn tại tập hợp n điểm mà không có ba điểm nào thuộc cùng một đường thẳng và khoảng cách đôi một giữa chúng là số tự nhiên. Định lý này lần đầu được chứng minh bởi N.H.Anning và P.Erdos. Chứng minh của họ không giống ở trên (Anning và Erdos [1], Hagwiger [1] trang 85). Các tác giả này đã chứng minh rằng nếu trong một tập vô hạn các điểm trên mặt phẳng mà khoảng cách đôi một giữa các điểm đó là nguyên thì tất cả các điểm thuộc một đường thẳng (Erdos [6] và Trost [2]).

Bài tập. Chứng minh rằng tập hợp các điểm hữu tỷ trên mặt phẳng có thể chia thành hai tập hợp, một tập có hữu hạn điểm chung với mọi đường kẻ ngang và tập kia có hữu hạn điểm chung với mọi đường kẻ dọc.

Chứng minh. Điều kiện được thỏa mãn với tập thứ nhất bao gồm tất cả các điểm có dạng $\left(\frac{l}{m},\frac{r}{s}\right)$, các phân số là tối giản và tử số nguyên, mẫu số tự nhiên, chúng thỏa mãn $|l|+m<|r|+s$. Tập thứ hai là các điểm còn lại. □

Có thể chứng minh tập hợp các điểm hữu tỷ trong không gian ba chiều có thể chia thành ba phần mà mỗi phần chỉ có giao hữu hạn với mọi đường thẳng song song với các trục tọa độ. Mệnh đề cho tập hợp tất cả các điểm trong không gian ba chiều tương đương với giả thuyết continuum (xem Sierpinski [13] và [22] trang 397).

3. Tổng của hai bình phương các số tự nhiên

Định lý 2. *Số tự nhiên n là tổng của hai bình phương các số tự nhiên khi và chỉ khi mọi ước số nguyên tố có dạng $4k+3$ của nó có lũy thừa chẵn trong phân tích thành thừa số nguyên tố của n và hoặc là 2 có lũy thừa lẻ trong phân tích đó hoặc là n có ít nhất một ước số nguyên tố có dạng $4k+1$.*

Chứng minh. Giả sử tồn tại số tự nhiên là tổng hai bình phương các số tự nhiên và có tính chất: số đó không có ước số nguyên tố có dạng $4k+1$, và trong phân tích thành thừa số nguyên tố của số đó thì 2 có lũy thừa chẵn ≥ 0. Giả sử n là số tự nhiên nhỏ nhất có các tính chất này.

Vì n là tổng hai bình phương các số tự nhiên nên theo Định lý 1 tất cả các ước số nguyên tố của n mà có dạng $4k+3$ thì có lũy thừa chẵn trong phân tích thành thừa số nguyên tố của n. Hệ quả là $n=2^{2k}m^2$ với m là số tự nhiên lẻ và số nguyên $k\geq 0$. Vì vậy ta có thể viết $2^{2k}m^2=a^2+b^2$, với a, b là các số tự nhiên.

Nếu $k>0$ thì vế trái của đẳng thức này chia hết cho 4, suy ra a, b cùng chẵn, nghĩa là $a=2a_1, b=2b_1,$ vì vậy $2^{2(k-1)}m^2=a_1^2+b_1^2<m,$ mâu thuẫn với định nghĩa của n. Do đó $k=0$ và $n=m^2=a^2+b^2>1$. Các số a,b nguyên tố cùng nhau vì nếu $(a,b)=d>1$ ta có $a=da_2, b=db_2$, với a_2, b_2 là các số tự nhiên suy ra $m=dm_1$ và $m_1^2=a_2^2+b_2^2<m^2=n$, mâu thuẫn với định nghĩa của n. Vậy $(a,b)=1$.

Nhưng vì m lẻ và >1 (không có ước số nguyên tố dạng $4k+1$), nên nó có ước số nguyên tố dạng $p=4k+3$. Suy ra $p\,|\,a^2+b^2$ nên $a^2\equiv -b^2 (\mathrm{mod}\, p)$. Lũy thừa cả hai vế lên $2k+1$ và lưu ý $2(2k+1)=p-1$, sử dụng định lý nhỏ Fermat ta nhận được $1\equiv(-1)^{2k+1}(\mathrm{mod}\, p)$, vô lý.

Vậy ta đã chứng minh được mọi số tự nhiên là tổng hai bình phương các số tự nhiên thì có tính chất là hoặc trong phân tích thành thừa số nguyên tố của nó số nguyên tố 2 có lũy thừa lẻ hoặc nó có ước số dạng $4k+1$. Kết hợp với Định lý 1 suy ra điều kiện cần đã được chứng minh.

Bây giờ ta chứng minh điều kiện đủ. Giả sử số tự nhiên n thỏa mãn các điều kiện trong định lý. Ta có hoặc $n=2m^2$ hoặc $n=2^\alpha m^2 l$, với $\alpha=0$ hoặc 1 và l là tích các ước số nguyên tố có dạng

$4k+1$. Nếu $n=2m^2$ thì $n=m^2+m^2$, và do đó nó là tổng hai bình phương các số tự nhiên. Giả sử $n=2^\alpha m^2 l$ với l là tích các số nguyên tố có dạng $4k+1$. Theo Định lý 9 Chương 5 thì mỗi một nhân tử đều là tổng của hai bình phương dương. Nhưng tích của hai số lẻ mà mỗi số là tổng của hai bình phương dương lại là tổng của hai bình phương dương. Bởi vì nếu $n_1=a^2+b^2, n_2=c^2+d^2$, với n_1,n_2 lẻ thì một trong các số a,b, giả sử là a, là lẻ và số kia chẵn, cũng vậy với c,d, giả sử c lẻ và d chẵn. Khi đó $n_1n_2=\left(a^2+b^2\right)+(c^2+d^2)=\left(ad+bc\right)^2+\left(ac-bd\right)^2$ với $ac-bd$ lẻ và do đó $\neq 0$. Vì vậy n_1n_2 là tổng của hai bình phương các số tự nhiên. Vậy l là tổng hai bình phương các số tự nhiên, nghĩa là $l=a^2+b^2$ suy ra $m^2l=\left(ma\right)^2+\left(mb\right)^2$ và $2m^2l=\left(ma+mb\right)^2+\left(ma-mb\right)^2$ và $ma-mb\neq 0$ (vì a khác b do $l=a^2+b^2$ lẻ). Vậy mọi số n là tổng hai bình phương các số tự nhiên. Điều kiện đủ được chứng minh.

Định lý 2 được chứng minh. □

Từ Định lý 2 suy ra các số n^2 là tổng của hai bình phương các số tự nhiên khi và chỉ khi n có ít nhất một ước số nguyên tố có dạng $4k+1$. Hoặc nói cách khác số tự nhiên n là cạnh huyền của một tam giác Pythagoras khi và chỉ khi n có ít nhất một ước số nguyên tố có dạng $4k+1$. Xem thêm hệ quả bài tập 3 mục 1.

Bài tập. ***1.*** Chứng minh rằng số tự nhiên n là tổng hai bình phương các số tự nhiên khác nhau khi và chỉ khi ***(i)*** các số nguyên tố có dạng $4k+3$ xuất hiện trong phân tích thành thừa số nguyên tố của n đều có lũy thừa chẵn; ***(ii)*** số n có ít nhất một ước số nguyên tố có dạng $4k+1$.

Chứng minh. Sự cần thiết của điều kiện ***(i)*** suy ra từ Định lý 1. Giả sử số tự nhiên n không thỏa mãn điều kiện ***(ii)*** nghĩa là nó không có ước số nguyên tố dạng $4k+1$. Suy ra nếu $n=a^2+b^2$ với các số tự nhiên khác nhau a,b thì với $d=\left(a,b\right)$ ta có $n=d^2\left(a_1^2+b_1^2\right)$. Với $a=da_1, d=bd_1$ và a_1,b_1 là các số nguyên tố cùng nhau và phân biệt. Số $a_1^2+b_1^2$ không có ước số nguyên tố có dạng $4k+1$ và do đó vì $\left(a_1+b_1\right)=1$ nên lập luận tương tự trong chứng minh Định lý 2 ta suy ra số $a_1^2+b_1^2$ không có ước số nguyên tố có dạng $4k+3$. Vì vậy $a_1^2+b_1^2=s^2$ với s là số tự nhiên >1 vì a_1,b_1 là các số tự nhiên khác nhau. Hệ quả là số $a_1^2+b_1^2$ chia hết cho 4 và suy ra các số a_1,b_1 đều là chẵn, mâu thuẫn vì $\left(a_1,b_1\right)=1$.

Bây giờ giả sử số tự nhiên n thỏa mãn các điều kiện ***(i), (ii)*** thì theo Định lý 2 ta có $n=a^2+b^2$ với a,b là các số tự nhiên. Nếu $a=b$ thì $n=2a^2$ và vì n thỏa mãn ***(ii)*** nên nó có ước số có dạng $4k+1$ do đó a là cạnh huyền của tam giác Pythagoras. Nghĩa là $a^2=c^2+d^2$ với c,d là các số tự nhiên. Rõ ràng $c\neq d$ vì nếu $c=d$ thì $a^2=2c^2$ mà $\sqrt{2}$ là số vô tỷ nên suy ra vô lý. Vậy $n=2a^2=\left(c+d\right)^2+\left(c-d\right)^2$ với $c-d\neq 0$ và $c+d\neq c-d$ (vì d là số tự nhiên). Hệ quả là n là tổng của hai bình phương các số tự nhiên phân biệt. Điều kiện đủ được chứng minh. □

2. Chứng minh rằng số tự nhiên n là tổng hai bình phương các số tự nhiên nguyên tố cùng nhau khi và chỉ khi n không chia hết cho 4 và cũng không chia hết cho các số tự nhiên có dạng $4k+3$.

Chứng minh. Giả sử số tự nhiên n là tổng hai bình phương các số tự nhiên nguyên tố cùng nhau, nghĩa là $n=a^2+b^2$. Nếu $n=4k$ thì các số a,b cùng chẵn, mâu thuẫn với $\left(a,b\right)=1$. Nếu n có ước số có dạng $4k+3$ thì nó có ước số nguyên tố cũng có dạng đó, mà theo chứng minh Định lý 2 thì ước số này không phải ước số của tổng hai bình phương các số tự nhiên nguyên tố cùng nhau. Vì vậy điều kiện ở trên là cần thiết.

Giả sử số tự nhiên n thỏa mãn điều kiện được đặt ra. Nếu $n=2$ thì $n=1^2+1^2$. Nếu $n\geq 2$ thì từ điều kiện suy ra n là tích của các số nguyên tố có dạng $4k+1$ hoặc là tích của 2 với các số nguyên tố có dạng $4k+1$. Trong trường hợp n lẻ và các ước số nguyên tố của n đều là tổng hai bình

phương các số tự nhiên nguyên tố cùng nhau thì theo bổ đề 2 và bài tập 8 mục 5 Chương 5 thì bằng quy nạp đơn giản ta thấy n là tổng hai bình phương các số tự nhiên nguyên tố cùng nhau. Trong trường hợp còn lại, nghĩa là nếu n là tích của 2 và các số nguyên tố có dạng $4k+1$ thì ta có $n=2\left(a^2+b^2\right)$ với a,b là hai số tự nhiên nguyên tố cùng nhau. Vì a^2+b^2 lẻ nên một trong hai số a,b có một số lẻ và số kia chẵn. Ta có $n=\left(a+b\right)^2+\left(a-b\right)^2$ với $a+b$ và $a-b$ là các số tự nhiên lẻ, hơn nữa chúng nguyên tố cùng nhau vì nếu $d\left|a+b\right.$ và $d\left|a-b\right.$ với d là số tự nhiên thì $d\left|2a\right.$ và $d\left|2b\right.$; vì d là ước số của số lẻ $a+b$ nên nó cũng lẻ. Ta có $d\mid a$ và $d\mid b$,mà $\left(a,b\right)=1$ suy ra $d=1$. Vậy $\left(a+b,a-b\right)=1$. Điều kiện đủ được chứng minh. □

4. Tổng của ba bình phương

Định lý 3. *Số tự nhiên n là tổng của 3 bình phương chỉ khi nó không có dạng $4^l\left(8k+7\right)$, các số nguyên $k,l\ \geq 0$.*

Chứng minh. Giả sử tồn tại số tự nhiên có dạng $4^l\left(8k+7\right)$, các số nguyên $k,l\ \geq 0$, là tổng ba bình phương. Ký hiệu n là số nhỏ nhất như vậy. Khi đó ta có $n=4^l\left(8k+7\right)=a^2+b^2+c^2$ với các số nguyên a,b,c. Nếu trong các số a,b,c có đúng một số lẻ thì tổng của các bình phương này có dạng $4t+1$ và khác n. Nếu hai trong số các số a,b,c là lẻ thì tổng các bình phương của chúng có dạng $4t+2$, do đó khác n. Nếu cả ba số là lẻ thì tổng các bình phương của chúng có dạng $8t+3$ và do đó khác n. Hệ quả là các số a,b,c đều chẵn. Đặt $a=2a_1,b=2b_1,c=2c_1,$ với a_1,b_1,c_1 là các số nguyên. Vậy $4^{t-1}\left(8k+7\right)=a_1^2+b_1^2+c_1^2$, mâu thuẫn với định nghĩa của n. Do đó các số tự nhiên không có dạng $4^l\left(8k+7\right)$, k,l là các số tự nhiên không âm, không thể là tổng của 3 bình phương các số nguyên. Định lý 3 được chứng minh. □

Có thể chứng minh điều kiện trong Định lý 3 cũng là điều kiện đủ để một số n là tổng của ba bình phương. Gauss là người đầu tiên chứng minh rằng mọi số tự nhiên không có dạng $4^l\left(8k+7\right)$, k và l là các số nguyên không âm, là tổng của ba bình phương các số nguyên. Lời giải gốc của Gauss đã được cải tiến bởi Lejeune Dirichlet và Landau (Landau [2] tập 1 trang 114-125). Gần đây N.C.Ankeny [1] đã trình bày một chứng minh sơ cấp cho định lý Gauss. Chứng minh này dựa trên định lý Minkowski liên quan tới các điểm nguyên chứa trong một hình lồi và định lý về cấp số cộng (Mordell [7], Wojcik [1]). Hệ quả trực tiếp của định lý Gauss là ta có thể suy ra mọi số tự nhiên có dạng $8k+3$ đều là tổng của ba bình phương các số nguyên, các số này là lẻ.

Vì vậy $8k+3=(2a+1)^2+(2b+1)^2+(2c+1)^2,$ với a,b,c là các số nguyên không âm và do đó

$$k=\frac{a(a+1)}{2}+\frac{b(b+1)}{2}+\frac{c(c+1)}{2}=t_a+t_b+t_c,$$

nên ta thấy định lý Gauss suy ra định lý sau đây: *mọi số tự nhiên đều là tổng của ba (hoặc ít hơn) các số tam giác*. Định lý này được đặt ra lần đầu bởi Fermat.

Đối với các số có dạng $8k+1$, B.Jones và G.Pall [1] đã chỉ ra chỉ trừ 1 và 25 thì tất cả đều là tổng của ba bình phương các số tự nhiên. Đối với các số dạng $8k+5$ nhỏ hơn 5.10^{10} thì chỉ có các số 5, 13, 37 và 85 là không phải tổng của ba bình phương các số tự nhiên. Không có số nào có dạng $8k+7$ là tổng của ba bình phương các số nguyên (và do đó không là tổng ba bình phương các số tự nhiên).

Số có dạng $4k$ là tổng của ba bình phương các số tự nhiên khi và chỉ khi k cũng có tính chất đó. Thật vậy nếu $4k=a^2+b^2+c^2$ với a,b,c là các số tự nhiên thì a,b,c chẵn do đó $a=2a_1,b=2b_1,c=2c_1$ với a_1,b_1,c_1 là các số tự nhiên. Vì vậy $k=a_1^2+b_1^2+c_1^2$. Ngược lại đẳng thức

cuối cùng suy ra $4k=(2a_1)^2+(2b_1)^2+(2c_1)^2$. Suy ra không có số nào có dạng $2^n, n=1,2...$ là tổng của ba bình phương các số tự nhiên. Nhưng $8.3n^2=(2n)^2+(2n)^2+(4n)^2$ và do đó có vô hạn số có dạng $8k$ là tổng bình phương của ba số tự nhiên và có vô hạn số không có tính chất đó.

Đối với các số có dạng $8k+2$, G.Pall [1] đã đặt ra giả thuyết nói rằng mọi số có dạng $2(8n+1)$ ngoại trừ 2 đều là tổng của ba bình phương các số tự nhiên. A.Schinzel [1] đã lưu ý rằng giả thuyết này là sai. Số $2(8.8+1)=130$ không phải tổng ba bình phương các số tự nhiên (bài tập 1). Không có ví dụ khác nhỏ hơn 5.10^{10} trong khi đối với các số $2(8n+5)$ thì có hai ví dụ là 10 và 58.

Các số có dạng $8k+4$ là tổng của ba bình phương các số tự nhiên khi và chỉ khi các số $2k+1$ tương ứng cũng có tính chất đó. Hệ quả là số $8(4k+3)+4=4(8k+7), k=0,1,2,..$ không phải tổng của ba bình phương các số tự nhiên. Mặt khác các số $8(4k+1)+4=4(8k+3), k=0,1,2,...$ đều là tổng của ba bình phương các số tự nhiên. Mọi số có dạng $8k+6$ đều là tổng của ba bình phương các số tự nhiên vì theo định lý Gauss thì các số đó là tổng bình phương của ba số nguyên, hơn nữa nó không phải tổng bình phương của hai số nguyên vì $8k+6=2(4k+3)$.

Từ các kết quả về các số ***idonei*** trong Chương 5 mục 6 với lý thuyết các dạng bậc hai suy ra có nhiều nhất một trong các số có dạng $8k+2$ hoặc $8k+5$ lớn hơn 130 là tổng bình phương của ba số tự nhiên (Grosswald và Calloway [1], Schinzel [10]).

Ký hiệu $\tau_3(n)$ là số các biểu diễn khác nhau một số n thành tổng của ba bình phương các số nguyên. Với $n\le 10$ ta có $\tau_3(1)=6, \tau_3(2)=12, \tau_3(3)=8,\ \tau_3(4)=6$, $\tau_3(5)=24$, $\tau_3(6)=24$, $\tau_3(7)=0$, $\tau_3(8)=12$, $\tau_3(9)=30$, $\tau_3(10)=24$. Định lý 3 suy ra với vô hạn các số n ta có $\tau_3(n)=0$.

Đối với các số $T_3(n)=\tau_3(1)+\tau_3(2)+...+\tau_3(n)$, sử dụng lập luận hình học tương tự trong mục 2 đối với tổng hai bình phương (ta thay các điểm hữu tỷ trong mặt phẳng bởi các điểm trong không gian mà có các tọa độ nguyên và xét các hình cầu và hình lập phương thay cho hình tròn và hình vuông tương ứng) ta có bất đẳng thức

$$\frac{4}{3}\pi\left(\sqrt{n}-\frac{\sqrt{3}}{2}\right)^2-1<T_3(n)<\frac{4}{3}\pi\left(\sqrt{n}+\frac{\sqrt{3}}{2}\right)^3-1$$

Từ bất đẳng thức này suy ra với mọi số tự nhiên n ta có ước lượng $\left|T_3(n)-\frac{4}{3}\pi n\sqrt{n}\right|<10n,$ suy ra

$$\lim_{n\to\infty}\frac{T_3(n)}{\frac{4}{3}\pi n\sqrt{n}}=1.$$

Ký hiệu $f(x)$ là số các số tự nhiên x có thể biểu diễn thành tổng ba bình phương. Từ định lý Gauss suy ra số $x-f(x)$ là $\le x$ và không có dạng $4^l(8k+7)$ với các số nguyên $k,l\ge 0$. Vì vậy với số nguyên không âm l ta có $8(k+1)-1\le 4^{-l}x$ và do đó $k+1\le\frac{1}{8}(4^{-l}x+1)$ số các số $k\ge 0$ là $\left[\frac{1}{8}(4^{-l}x+1)\right]$. Ta có $x-f(x)=\sum_{l=o}^{[x]}\frac{4^{-l}x+1}{8}$.

Nếu $l>\log x/\log 4$ thì $4^l>x>x/7,$ suy ra $(4^{-l}x+1)/8<1$.

Hệ quả là $x-f(x)=\sum_{l=0}^{[\log x/\log 4]}\left[\frac{4^{-l}x+1}{8}\right]$ do đó $x-f(x)=\sum_{l=0}^{[\log x/\log 4]}\frac{4^{-l}x+1}{8}-a\left(\frac{\log x}{\log 4}+1\right), 0\le a\le 1.$

Nhưng $\sum_{t=[\log x/\log 4]+1}^{\infty}4^{-l}=\frac{4}{3}.4^{-[\log x\log 4]-1}<\frac{4}{3}.4^{-\log x/\log 4}=\frac{4}{3x}.$

Từ $\sum_{l=0}^{\infty}\frac{4^{-l}x}{8}=\frac{x}{6}$ suy ra ta có $\lim_{x\to+\infty}\frac{x-f(x)}{x}=\frac{1}{6}$ và do đó $\lim_{x\to+\infty}\frac{f(x)}{x}=\frac{5}{6}.$

Công thức này được tìm ra bởi Landau năm 1908.

M.C.Charkrabarti [1] đã nghiên cứu hàm $g(x)=\frac{f(x)-\frac{5}{6}x}{\log x}$ và chứng minh được

$$\lim_{x\to+\infty}\inf g(x)=0,\ \lim_{x\to+\infty}\sup g(x)=\frac{1}{\log 8}$$

Hơn nữa các giá trị của $g(x)$ trù mật trong khoảng $\left(0,\frac{1}{\log 8}\right).$

Bài tập. ***1.*** Chứng minh rằng 130 không phải tổng ba bình phương dương.

Chứng minh. Giả sử $130=a^2+b^2+c^2$ với a,b,c là các số tự nhiên. Không giảm tổng quát có thể giả sử $a\ge b\ge c$. Suy ra $a^2+1+1\le 130\le 3a^2$. Nên $43<a^2\le 128$ và do đó $7\le a\le 11$. Nhưng $130-7^2=81=3^4, 130-8^2=66=2.3.11, 130-9^2=49=7^2, 130-10^2=30=2.3.5, 130-11^2=9=3^2$ và theo các phân tích thành thừa số nguyên tố của các số 81,66,49,30,9 thì không có số nào thỏa mãn điều kiện Định lý 2 nên chúng không là tổng của hai bình phương các số tự nhiên. Vậy 130 không phải tổng ba bình phương các số tự nhiên. □

Ghi chú. Dễ dàng chứng minh rằng 130 là số tự nhiên nhỏ nhất có dạng $2(8k+1)$ không phải tổng ba bình phương các số tự nhiên.

2. Sử dụng định lý Gauss chứng minh rằng số tự nhiên là tổng ba bình phương các số hữu tỷ khi và chỉ khi nó là tổng ba bình phương các số nguyên.

Chứng minh. Giả sử số tự nhiên n là tổng ba bình phương các số hữu tỷ thì quy đồng các số hữu tỷ đó thành các phân số có chung mẫu số, ta có thể viết $m^2n=a^2+b^2+c^2$ với a,b,c là các số nguyên. Nếu $n=4^l(8k+7)$ với k,l nguyên ≥ 0 thì đặt $m=2^r(2s+1)$, s và r là các số nguyên không âm ta có $m^2n=4^{k+r}(8t+7)$ với $k+r$ và t là các số nguyên không âm. Nhưng theo Định lý 3 thì điều này vô lý vì $m^2n=a^2+b^2+c^2$. Hệ quả là n không có dạng $4^l(8k+7)$ với các số nguyên k,l. Vì vậy theo định lý Gauss nó là tổng ba bình phương các số nguyên. Điều kiện trong bài toán cũng là điều kiện đủ. □

3. Chứng minh rằng không tồn tại các số hữu tỷ x,y,z mà $x^2+y^2+z^2+x+y+z=1.$

Chứng minh. Phương trình ở trên tương đương với

(9) $$(2x+1)^2+(2y+1)^2+(2z+1)^2=7.$$

Trong chứng minh bài tập 2 ta đã chứng minh (không sử dụng định lý Gauss) không tồn tại số có dạng $4^l(8k+7)$ với k và l là các số nguyên không âm mà có thể biểu diễn thành tổng của ba bình

phương các số hữu tỷ. Vì vậy 7 không có biểu diễn như vậy, suy ra x, y, z không thể thỏa mãn phương trình ***(9)***. □

4. Sử dụng định lý Gauss chứng minh rằng mọi số lẻ có dạng $a^2+b^2+2c^2$ với k, l là các số nguyên.

Chứng minh. Giả sử t là số nguyên không âm tùy ý. Số $4t+2$ không có dạng $4^l(8k+7)$ với k, l là các số nguyên không âm. Do đó theo định lý Gauss thì $4t+2=x^2+y^2+z^2$ với x, y, z là các số nguyên. Không thể xảy ra trường hợp tất cả các số đó đều chẵn vì vế trái đẳng thức không chia hết cho 4. Tuy nhiên số các số lẻ trong chúng là chẵn vì vế trái là chẵn, vì vậy giả sử x, y lẻ và z chẵn, nghĩa là $z=2c$. Các số $x+y$ và $x-y$ chẵn và do đó $x+y=2a, x-y=2b$ suy ra $x=a+b, y=a-b$. Vậy $4t+2=(a+b)^2+(a-b)^2+4c^2$ nên $2t+11=a^2+b^2+2c^2$ với a, b, c là các số nguyên. Điều phải chứng minh. □

5. Từ định lý Gauss suy ra mọi số tự nhiên sẽ có dạng $a^2+b^2+c^2$ hoặc $a^2+b^2+2c^2$ với a, b, c nguyên.

Chứng minh. Nếu một số tự nhiên không phải tổng của 3 bình phương thì theo định lý Gauss nó có sẽ dạng $4^l(8k+7)$ với k, l là các số nguyên không âm nào đó. Nhưng theo bài tập 4 thì ta lại có $8k+7=x^2+y^2+2z^2$ với x, y, z là các số nguyên. Vì vậy $4^l(8k+7)=(2^l x)^2+(2^l y)^2+2(2^l z)^2$ do đó số ban đầu có dạng $a^2+b^2+2c^2$, a, b, c nguyên. □

6. Chứng minh một số $\neq 0$ là tổng ba bình phương các số hữu tỷ thì nó có thể biểu diễn vô hạn cách dưới dạng đó.

Chứng minh. Kết quả này là hệ quả trực tiếp của định lý đã được chứng minh trong bài tập 2 mục 1: mọi số $\neq 0$ là tổng của hai bình phương các số hữu tỷ có vô hạn cách biểu diễn dưới dạng đó. □

7. Chứng minh định lý E.Lionnet nói rằng mọi số tự nhiên lẻ đều là tổng các bình phương của bốn số nguyên mà hai trong số đó là các số liên tiếp là hệ quả của định lý Gauss.

Chứng minh. Đặt $n=2k+1$ với $k=0,1,2...$ Từ định lý Gauss suy ra $4k+1$ là tổng của ba bình phương, tức là $4k+1=x^2+y^2+z^2$. Lưu ý rằng một trong các số x, y, z lẻ và các số còn lại là chẵn.

Đặt $x=2a, y=2b, z=2c+1$ với a, b, c là các số nguyên.

Vậy $n=2k+1=(a+b)^2+(a-b)^2+c^2+(c+1)^2$. Điều phải chứng minh. □

8. Chứng minh tồn tại vô hạn số nguyên tố có dạng $a^2+b^2+c^2+1$ với a, b, c là các số tự nhiên.

Chứng minh. Theo Định lý 1 Chương 9 thì tồn tại vô hạn số nguyên tố có dạng $8k+7$. Nếu p là số nguyên tố có dạng này thì $p-1=8k+6$. Nhưng từ định lý Gauss suy ra mọi số có dạng $8k+6$ đều là tổng các bình phương của ba số tự nhiên. Vì vậy $p-1=a^2+b^2+c^2$ với các số tự nhiên a, b, c vì vậy $p=a^2+b^2+c^2+1$. □

9. Tìm ví dụ chứng tỏ tích của hai số mà mỗi số là tổng ba bình phương không nhất thiết là tổng ba bình phương..

Lời giải. $63=3.21=(1^2+1^2+1^2)(1^2+2^2+4^2)$. Số 63 không có dạng $8k+7$ nên không là tổng ba bình phương. □

10. Từ định lý Gauss suy ra mọi số tự nhiên là tổng của 10 (hoặc ít hơn) bình phương các số lẻ (Pollock đã đặt ra bài toán này mà không kèm theo chứng minh [1], S.Turski đã đưa ra một chứng minh trong [1])

Chứng minh. Từ định lý Gauss suy ra mọi số tự nhiên có dạng $8k+3$ với k nguyên ≥ 0 đều là tổng của ba bình phương các số lẻ. Mặt khác mọi số tự nhiên $n\geq 3$ đều có dạng $8k+3+r$ với

$r = 0,1,2,3,4,5,6,7.$ Ta thấy r là tổng của nhiều nhất là 7 bình phương các số 1, do đó n là tổng của nhiều nhất là 10 bình phương các số tự nhiên lẻ. Có vô hạn các số tự nhiên không phải tổng của ít hơn 10 bình phương các số tự nhiên lẻ (bài tập 12). □

Ghi chú. Kết quả mà ta vừa chứng minh được gọi là Định lý T. Định lý này suy ra mọi số tự nhiên có dạng $8k+3$ với k là số nguyên không âm đều là tổng của ba bình phương lẻ. Thật vậy theo Định lý T thì nếu $k \geq 0$ ta có

(*) $$8k+3 = n_1^2 + n_2^2 + ... + n_s^2,$$

với số tự nhiên $s \leq 10, n_1, n_2, ..., n_s$ lẻ. Vì vậy ta có $n_i^2 = 1 (\mathrm{mod})$ với $i = 1,2,..,s$ và theo ***(*)*** thì $3 \equiv s (\mathrm{mod} 8)$ mà $1 \leq s \leq 10$ suy ra $s = 3$. Vậy theo ***(*)*** thì các số $8k+3$ đều là tổng của ba bình phương lẻ (Sierpinski [8]).

11. Chứng minh rằng lũy thừa bậc s (với s là số tự nhiên) của một số nguyên là tổng của ba bình phương các số nguyên cũng là tổng của ba bình phương các số nguyên.

Chứng minh. Nếu s là 1 hoặc 2 thì ta có điều phải chứng minh. Chỉ cần xét trường hợp s có dạng $2k+3, k$ là số nguyên không âm. Ta có $n^{2k+3} = \left(n^k\right)^2 n^3$ vì vậy chỉ cần chứng minh cho trường hợp s =3. Điều này suy ra từ đẳng thức Catalan:

$$\left(x^2+y^2+z^2\right)^3 = x^2\left(3z^2-x^2-y^2\right)^2 + y^2\left(3z^2-x^2-y^2\right)^2 + z^2\left(z^2-3x^2-3y^2\right)^2. \square$$

12. Chứng minh rằng tồn tại vô hạn các số tự nhiên không thể biểu diễn thành tổng của ít hơn 10 bình phương lẻ.

Chứng minh. Các số có dạng $72k+42$ với $k = 0,1,2,..$ có tính chất đó. Thật vậy giả sử $n = 72k+42$ là số tự nhiên là tổng của $s < 10$ bình phương lẻ. Do bình phương lẻ $\equiv 1 (\mathrm{mod}\ 8)$ nên ta có $n \equiv s (\mathrm{mod} 8)$ suy ra vì $n = 72t+42 \equiv 2 (\mathrm{mod} 8)$ nên $s \equiv 2 (\mathrm{mod} 8)$. Vậy $s = 2$.

Hệ quả là n là tổng của hai bình phương. Nhưng điều này là không thể vì $n = 3(24t+14) = 9(8t+4)+6$ chia hết cho 3 nhưng không chia hết cho 9.

Tương tự có thể chứng minh các số $72k+66, k = 0,1,2,..,$ cũng có tính chất này. □

5. Biểu diễn bởi tổng bốn bình phương

Ta chứng minh định lý Lagrange sau đây

Định lý 4 (Lagrange). *Mọi số nguyên không âm đều là tổng của bốn bình phương*.

Bổ đề 1. *Giả sử số nguyên tố lẻ p là ước số của một tổng bốn bình phương và ít nhất một trong các bình phương đó không chia hết cho p thì p là tổng của bốn bình phương.*

Chứng minh bổ đề 1. Giả sử số nguyên tố p có tính chất đó. Khi đó tồn tại bội số của p là tổng của bốn bình phương mà có ít nhất một số không chia hết cho p. Giả sử n là bội số nhỏ nhất như vậy của p. Ta có

(10) $$n = mp$$

Với m là số tự nhiên và

(11) $$n = a^2 + b^2 + c^2 + d^2,$$

với a, b, c, d là các số nguyên và ít nhất một trong chúng không chia hết cho p, giả sử là a.

Giả sử a_1, b_0, c_0, d_0 là các số nguyên thỏa mãn

(12) $a_0 \equiv a(\mathrm{mod}\, p),\ \ b_o \equiv b(\mathrm{mod}\, p),\ \ \ c_0 = c(\mathrm{mod}\, p),\ \ \ d_0 = d(\mathrm{mod}\, p)$

và

(13) $|a_0| < p/2,\ |b_0| < p/2,\ \ |c_0| < p/2,\ \ |d_0| < p/2$

Để tính a_0 chỉ cần tính số dư r nhận được khi chia a cho p và đặt $a_0 = r$ nếu $r < p/2$, hoặc $a_0 = r - p$ nếu $r > p/2$. Vì a không chia hết cho p nên a_0 cũng thế và từ ***(12),(10)*** và ***(11)*** suy ra $a_0^2 + b_0^2 + c_0^2 + d_0^2 = a^2 + b^2 + c^2 + d^2 \equiv 0(\mathrm{mod}\, p)$. Vì vậy theo định nghĩa của n và ***(13)*** suy ra $n \le a_0^2 + b_0^2 + c_0^2 + d_0^2 < 4(p/2)^2$. Hệ quả là $n < p^2$ và theo ***(10)*** suy ra $mp < p^2$ từ đó ta có

(14) $m < p$

Từ ***(10)*** và ***(11)*** suy ra ta chỉ còn cần chứng minh $m = 1$.

Giả sử $m \neq 1$. Vì m là số tự nhiên nên theo ***(14)*** ta có

(15) $1 < m < p$.

Ta tìm các số tự nhiên a_1, b_1, c_1, d_1 thỏa mãn các điều kiện

(16) $a_1 \equiv a(\mathrm{mod}\, m),\ \ b_1 \equiv b(\mathrm{mod}\, m),\ \ c_1 \equiv c(\mathrm{mod}\, m);$
$c_1 = c(\mathrm{mod}\, m)$

(17) $|a_1| \le m/2,\ \ |b_1| \le m/2,\ \ \ |c_1| \le m/2,\ \ |d_1| \le m2.$

Từ ***(16)*** ta có $a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv a^2 + b^2 + c^2 + d^2 (\mathrm{mod}\, m)$ và suy ra theo ***(11)*** và ***(10)*** thì $m \mid a_1^2 + b_1^2 + c_1^2 + d_1^2$ do đó

(18) $a_1^2 + b_1^2 + c_1^2 + d_1^2 = ml,$

Với số nguyên $l \ge 0$. Nếu $l = 0$ thì theo ***(18)***, $a_1 = b_1 = c_1 = d_1 = 0$ suy ra theo ***(16)*** tất cả các số a, b, c, d đều chia hết cho m và suy ra theo ***(11)*** thì n chia hết cho m^2 và do đó theo ***(10)*** thì $m \mid p$ nhưng điều này mâu thuẫn với ***(15)*** vì p nguyên tố. Do đó l là số tự nhiên. Giả sử rằng

(19) $|a_1| \equiv |b_1| \equiv |c_1| \equiv |d_1| \equiv m/2$

Điều này chỉ có thể xảy khi m chẵn, nghĩa là khi

(20) $m = 2k,$

với k là số tự nhiên. Từ đồng dư thức $a_1 \equiv a(\mathrm{mod}\, m)$ suy ra $a = a_1 + mt$ với t là số nguyên. Do đó theo ***(20)*** và ***(19)*** ta có $a = \pm k + 2kt = (2t \pm 1)k = k_1 k$ với k_1 lẻ. Tương tự ta chứng minh được $a = k_1 k,\ b = k_2 k,\ c = k_3 k,\ d = k_4 k,$ với k_1, k_2, k_3, k_4 lẻ.

Vì vậy theo ***(20)***, ***(10)*** và ***(11)*** ta có $n - 2kp = k^2\left(k_1^2 + k_2^2 + k_3^2 + k_4^2\right)$.

Hệ quả là $2p = k\left(k_1^2 + k_2^2 + k_3^2 + k_4^2\right)$. Vì mọi bình phương lẻ đều đồng dư với 1(mod4) suy ra nhân tử thứ hai trong vế phải của đẳng thức cuối cùng là chia hết cho 4 và do đó $2 \mid p$ mâu thuẫn với giả thiết. Suy ra ***(19)*** là không thể có. Hệ quả là với ít nhất một trong các bất đẳng thức ***(17)*** thì đẳng thức không thể xảy ra. Suy ra $a_1^2 + b_1^2 + c_1^2 + d_1^2 < 4.\frac{m^2}{4}$ vì vậy theo ***(18)*** ta có $ml < m^2$ và do đó

(21) $l < m$.

So sánh với đồng nhất thức Euler

$$(a^2+b^2+c^2+d^2)(a_1^2+b_1^2+c_1^2+d_1^2) = (aa_1+bb_1+cc_1+dd_1)^2 + \\ +(ab_1-ba_1+cd_1-dc_1)^2+(ac_1-ca_1+db_1-bd_1)^2 + \\ +(ad_1-da_1+bc_1-cb_1)^2. \tag{22}$$

Theo ***(11)***, ***(10)*** và ***(18)*** thì vế trái bằng m^2lp. Theo ***(16)*** ta có

$$a_1 = a+ma_2, \quad b_1 = b+mb_2, \quad c_1 = c+mc_2, \\ d_1 = d+md_2, \tag{23}$$

với a_2, b_2, c_2, d_2 là các số nguyên. Theo ***(11)*** và ***(10)*** công thức ***(23)*** suy ra

$$\begin{aligned} aa_1+bb_1+cc_1+dd_1 &= a^2+b^2+c^2+d^2+m(aa_2+bb_2+cc_2+dd_2) \\ &= m(p+aa_2+bb_2+cc_2+dd_2) = mt_1, \\ ab_1-ba_1+cd_1-dc_1 &= m(ab_2-ba_2+cd_2-dc_2) = mt_2, \\ ac_1-ca_1+db_1-bd_1 &= m(ac_2-ca_2+db_2-bd_2) = mt_3, \\ ad_1-da_1+bc_1-cb_1 &= m(ad_2-da_2+bc_2-cb_2) = mt_4, \end{aligned}$$

với t_1, t_2, t_3, t_4 là các số nguyên.

Thế các đẳng thức này vào ***(22)*** ta có $m^2lp = m^2\left(t_1^2+t_2^2+t_3^2+t_4^2\right)$ và từ đây suy ra

$$lp = t_1^2+t_2^2+t_3^2+t_4^2. \tag{24}$$

Nếu các số t_1, t_2, t_3, t_4 đều chia hết cho p thì $p^2 \mid lp$ và do đó $p \mid l$, vô lý vì l là số tự nhiên và theo ***(21)*** và ***(14)*** thì $l < p$. Công thức ***(24)*** cho ta biểu diễn của số lp thành tổng của bốn bình phương mà trong đó có số không chia hết cho p. Từ định nghĩa của n suy ra $n \le lp$ và do đó theo ***(10)*** thì $mp \le lp$ suy ra $m \le l$ mâu thuẫn với ***(21)***. Vì vậy từ giả thiết $m \ne 1$ dẫn tới mâu thuẫn. Suy ra $m = 1$ và ta có điều phải chứng minh. □

Bổ đề 2. *Mọi số nguyên tố đều là tổng của bốn bình phương*.

Chứng minh bổ đề 2. Ta có $2 = 1^2+1^2+0^2+0^2$ do đó không giảm tổng quát giả sử p là số nguyên tố lẻ. Theo Bổ đề 1 thì ta chỉ cần chứng minh p là ước số của một tổng bốn bình phương các số nguyên mà trong đó có ít nhất một số không chia hết cho p.

Số dư nhận được khi chia các số

$$1+0^2, 1+1^2, \ldots, 1+\left(\frac{p-1}{2}\right)^2 \tag{25}$$

cho p là khác nhau vì ta đã biết theo Chương 5 mục 5 thì các số $0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ khi chia cho p sẽ cho các số dư khác nhau. Tương tự các số sau khi chia cho p cũng cho các số dư khác nhau

$$-0^2, -1^2, \ldots, -\left(\frac{p-1}{2}\right)^2 \tag{26}$$

Giả sử các số dư nhận được khi chia các số trong dãy ***(25)*** cho p và các số dư nhận được khi chia các số trong dãy ***(26)*** cho p là khác nhau thì khi đó tổng số các số dư phân biệt nhận được từ cả hai dãy là $2\left(1+\frac{p-1}{2}\right) = p+1$. Vô lý. Vậy tồn tại phần tử $1+x^2$ thuộc dãy ***(25)*** có cùng số dư khi

chia cho p với phần tử $-y^2$ của dãy ***(26)***. Khi đó ta có $p\left|1^2+x^2+y^2+0^2\right.$ và suy ra p là ước số của một tổng bốn bình phương các số nguyên mà không chia hết cho p. Điều phải chứng minh. □

Chứng minh định lý 4. Theo đẳng thức ***(22)*** thì tích của hai số mà mỗi số đều là tổng bốn bình phương thì cũng là tổng bốn bình phương. Sử dụng một phép quy nạp đơn giản suy ra điều này đúng với tích hữu hạn các số như vậy. Bởi vì mọi số >1 đều là tích của các số nguyên tố mà theo Bổ đề 2 thì tất cả các số nguyên tố đều là tổng bốn bình phương nên bản thân số ban đầu cũng là tổng bốn bình phương. Hơn nữa $0=0^2+0^2+0^2+0^2+0^2$ và $1=1^2+0^2+0^2+0^2$. Định lý được chứng minh. □

D.H.Lehmer [4] đã chứng tỏ rằng trong các số tự nhiên thì chỉ có các số 1, 2, 5, 7, 11, 15, 23 và các số có dạng $4^h m$ với $h=0,1,2..,m=2,6$ hoặc 14 là có biểu diễn duy nhất dưới dạng trên (không tính các hoán vị). S.Ramanujan [2] đã nghiên cứu các bộ số tự nhiên a, b, c, d mà mọi số tự nhiên n đều có thể biểu diễn ở dạng $ax^2+by^2+cz^2+dt^2$ với x, y, z, t là các số nguyên. Ông ta đã chứng minh rằng với giả thiết $a\le b\le c\le d$ thì tồn tại đúng 54 bộ số như vậy, tất cả đều có dạng $1,1,1,d$ với $d=1,2,...,7$ hoặc $1,1,2,d$ với $d=2,3,..,14$ hoặc $1,1,3,$d với $d=3,4,5,6$ hoặc $1,2,2,$d với $d=$ $2,3,...,7$ hoặc $1,2,3,d$ với d =6,7,...,10 (Dickson [6] trang 104 định lý 95).

Ta chứng minh định lý Jacobi: *mọi số tự nhiên đều có dạng* $x^2+2y^2+3z^2+6t^2$ *với* x, y, z, t *nguyên.*

Chứng minh. Giả sử n là số tự nhiên. Theo Định lý 4 thì tồn tại các số nguyên a,b,c,d mà

(27) $$n=a^2+b^2+c^2+d^2.$$

Ta sẽ chứng minh với phép đổi dấu thích hợp thi ta có $3\left|a+b+c\right.$.

Điều này hiển nhiên nếu ít nhất ba trong các số a,b,c,d chia hết cho 3. Giả sử chỉ có hai số c và d chia hết cho 3 thế thì $a\equiv\pm1\ (\mathrm{mod}\ 3)$ và $b\equiv\pm1\left(\mathrm{mod}\,3\right)$ suy ra với phép đổi dấu thích hợp ta có $3\left|a\pm b\right.$ do đó $3\left|a\pm b+c\right.$. Cuối cùng nếu có ba trong các số a,b,c,d là a,b,c không chia hết cho 3 thì với phép chọn dấu $\pm$ thích hợp ta có $3\left|a\pm b\right.$ $3\left|a\pm b\pm c\right.$.

Không giảm tổng quát giả sử

(28) $$a+b+c=3z,$$

với z là số nguyên. Nhưng trong ba số nguyên luôn có ít nhất hai số đồng dư mod 2 nên có thể giả sử $a\equiv b\left(\mathrm{mod}\,2\right)$ suy ra $a+b=2k$ với k là số nguyên. Ta có đẳng thức

$$3\left(a^2+b^2+c^2\right)=\left(a+b+c\right)^2+2\left(\frac{a+b}{2}-c\right)^2+6\left(\frac{a-b}{2}\right)^2,$$

Suy ra $3\left(a^2+b^2+c^2\right)=\left(a+b+c\right)^2+2\left(k-c\right)^2+6y^2$, mà theo ***(28)*** suy ra $3\mid k-c$ do đó $k-c=3t$ với t là số nguyên. Vì vậy theo ***(28)*** ta có $a^2+b^2+c^2=3x^2+6t^2+2y^2$ và từ ***(27)*** ta có $n=d^2+2y^2+3z^2+6t^2$. □

Bài tập. ***1.*** Từ Định lý 4 chứng minh mọi số tự nhiên chia hết cho 8 là tổng của 8 bình phương lẻ.

Chứng minh, Nếu n là số tự nhiên thì theo Định lý 4 suy ra tồn tại 4 số nguyên a,b,c,d thỏa mãn $n-1=a^2+b^2+c^2+d^2$ và

$$8n=(2a-1)^2+(2a+1)^2+(2b-1)^2+(2b+1)^2+(2c-1)^2+(2c+1)^2+(2d-1)^2+(2d+1)^2$$

2. Chứng minh rằng không tồn tại số tự nhiên chia hết cho 8 là tổng của ít hơn 8 bình phương lẻ.

Chứng minh. Tổng của s bình phương lẻ có dạng $8k+s$ với k là số nguyên không âm. Do đó nếu tổng này chia hết cho 8 thì $8|s$ và do đó $s \geq 8$. □

6. Tổng của bốn bình phương các số tự nhiên

Hệ quả trực tiếp của Định lý 4 là mọi số tự nhiên đều là tổng của bốn (hoặc ít hơn) bình phương các số tự nhiên. Sử dụng định lý Gauss ta sẽ chứng minh

Định lý 5. *Số tự nhiên n là tổng bình phương của 4 số tự nhiên khi và chỉ khi nó không thuộc dãy các số 1,3,5,9,11,17,29,41,* $4^h.2, 4^h.6, 4^h.14$ *với* $h = 0,1,2,....$

Định lý này đã được Descartes đặt ra dưới dạng một giả thuyết (G.Pall [1] trang 11).

Chứng minh. Ta nói một số tự nhiên là S_m nếu nó là tổng bình phương của m số tự nhiên.

Dễ dàng chứng minh không có số nào trong các số 1,3,5,9,11,29,41 là S_4.

Ta chứng minh tính chất này đối với số 41. Giả sử ngược lại 41 là S_4 nghĩa là $41 = a^2+b^2+c^2+d^2$ với a,b,c,d là các số tự nhiên và $a \geq b \geq c \geq d$. Vì vậy $a^2 < 41 \leq 4a^2$ và do đó $4 \leq a \leq 6$. Nếu $a=6$ thì $5 = b^2+c^2+d^2$ vô lý. Nếu $a=5$ thì $16 = b^2+c^2+d^2$ vô lý vì 16 không phải S_3. Nếu $a=4$ thì $25 = b^2+c^2+d^2$ vô lý vì 25 không phải S_3. Do đó 41 không phải S_4.

Bây giờ ký hiệu m là một trong các số 2,6,14. Khi đó m có dạng $4k+2$. Giả sử tồn tại số nguyên không âm h thỏa mãn $4^h m$ là S_4. Ký hiệu h là số nguyên nhỏ nhất như vậy. Vì 2,6,14 không phải $S_4, h \geq 1$. Ta có $4^h m = a^2+b^2+c^2+d^2$ với a,b,c,d là các số tự nhiên và vế trải của đẳng thức chia hết cho 8 vì $h \geq 1$ và $m = 2(2k+1)$. Từ đây suy ra a,b,c,d đều chẵn. Vì vậy $a = 2a_1, b = 2b_1, c = 2c_1, d = 2d_1$ với a_1,b_1,c_1,d_1 là các số tự nhiên. Do đó $4^{h-1}m = a_1^2+b_1^2+c_1^2+d_1^2$ suy ra $4^{h-1}m$ là S_4 mâu thuẫn với định nghĩa của h. Vậy ta đã chứng minh các số $4^h m$ với $m =$ 2,6,14 không phải S_4 với mọi số nguyên không âm h. Từ đây suy ra điều kiện cần.

Ký hiệu n là số tự nhiên lẻ thỏa mãn điều kiện trong Định lý 5. Hệ quả là $n \neq 1,3,5,9,11,17,29,41$. Vì n lẻ nên nó có dạng $8k+1, 8k+3, 8k+5, 8k+7$.

Giả sử $n = 8k+1$. Ta xét bốn trường hợp $k = 4t, k = 4t+1, k = 4t+2, k = 4t+3$. Nếu $k = 4t$ thì $n = 32t+1$ và vì $n \neq 1$ nên ta có $t \geq 1$m và do đó $t = u+1$ với u là số nguyên không âm. Vì vậy $n = 32(u+1)+1 = 4(8u+6)+9$. Theo định lý Gauss thì số $8u+6$ là tổng ba bình phương các số nguyên. Vì $8u+6 = 2(4u+3)$ không phải tổng bình phương hai số nguyên nên ta thấy $8u+6$ là S_3 và suy ra $n = 2^2(8u+6)+3^2$ là S_4. Nếu $k = 4t+1$ thì $n = 32t+9$. Do đó vì $n \neq 9$ và $n \neq 41$ nên ta có $t \geq 2$ do đó $t = u+2$ với u là số nguyên ≥ 0. Vì vậy $n = 32(u+2)+9 = 2^2(8u+6)+7^2$ suy ra n là S_4. Nếu $k = 4t+2$ thì $n = 32t+17$ và vì $n \neq 17$ ta có $t \geq 1$ và do đó $t = u+1$ với u là số nguyên ≥ 0. Vì vậy $n = 32(u+1)+17 = 2^2(8u+6)+5^2$ suy ra n là S_4. Nếu $k = 4t+3$ thì $n = 32t+25$ $= 2^2(8t+6)+1^2$. Vậy ta có điều kiện đủ trong trường hợp $n = 8k+1$.

Giả sử $n = 8k+3$. Do $n \neq 3$ và $n \neq 11$ nên ta có $k \geq 2$ và do đó $k = t+2$ với t là số nguyên không âm. Ta có $n = 8(t+2)+3 = 8t+3+4^2$ suy ra theo định lý Gauss thì $8t+3$ là tổng bình phương ba số lẻ và suy ra n là S_4. Trường hợp $n = 8k+3$ được chứng minh.

Tiếp theo giả sử $n = 8k+5$. Ta xét bốn trường hợp $k = 4t, k = 4t+1, k = 4t+2, k = 4t+3$. Nếu $k = 4t$ thì $n = 32t+5$ và vì $n \neq 5$ ta có $t > 0$, do đó $t = u+1$ với u là số nguyên không âm. Do đó

$n=32(u+1)+5=2^2(8u+3)+5^2$ suy ra n là S_4. Nếu $k=4t+1$ thì $n=32t+13=2^2(8t+3)+1^2$ suy ra n là S_4. Nếu $k=4t+2$ thì $n=32t+21=2^2(8t+3)+3^2$ suy ra n là S_4. Nếu $k=4t+3$ thì $n=32t+29$ và vì $n\neq 29$ nên ta có $t>0$ và do đó $t=u+1$ với $u\geq 0$ suy ra $n=32(u+1)+29=2^2(8u+3)+7^2$, nên n là S_4. Trường hợp $n=8k+5$ được chứng minh.

Cuối cùng xét $n=8k+7$. Theo Định lý 4 thì tồn tại các số nguyên a,b,c,d mà $n=a^2+b^2+c^2+d^2$. Mặt khác theo Định lý 3 thì vì $n=8k+7$ nên không có số nào trong các số a,b,c,d bằng 0. Do đó n là S_4.

Vậy *một số tự nhiên lẻ là tổng của bốn bình phương các số tự nhiên khi và chỉ khi nó không phải 1,3,5,9,11,17,29,41. Chứng tỏ mọi số lẻ* >41 *đều là tổng của bốn bình phương các số tự nhiên.*

Bây giờ ký hiệu n là số tự nhiên chẵn không có dạng $4^h.2$, $4^2.6$, $4^h.14$ với $h=0,1,2\ldots$ Ký hiệu 4^h là lũy thừa cao nhất của 4 là ước số của n. Ta có $n=4^h m$ với m không chia hết cho 4. Hệ quả là $m=4k+1,\ m=4k+2,$ hoặc $m=4k+3$.

Nếu $m=4k+1$ với k chẵn, nghĩa là $k=2t$, thì $m=8t+1,$ số này là S_4, Nếu $m\neq 1,9,17,41$ thì $n=4^h m$ cũng là S_4. Nhưng vì n chẵn và vì m không chia hết cho 4 nên $h>0$. Rõ ràng 4 là S_4, $4.17=68=1^2+3^2+3^2+7^2$, $4.41=164=1^2+1^2+9^2+9^2$ suy ra tất cả các số sau đều là S_4

$$4^h.1=4\left(2^{h-1}\right)^2,\quad 4^h.9=4\left(2^{h-1}.3\right)^2, 4^h.17=4.17\left(2^{h-1}\right)^2, 4^h.41=4.41\left(2^{h-1}\right)^2$$

Vậy nếu $m=4k+1$ và k chẵn thì $n=4^h m$ là S_4.

Nếu $m=4k+1$ với k lẻ, nghĩa là $k=2t+1$, thì $m=8t+5$ là S_4 với $m\neq 5$ và $m\neq 29$. Nhưng $4.5=20=1^2+1^2+3^2+3^2$, $4.29=116=1^2+3^2+5^2+9^2$ suy ra vì m lẻ, n chẵn và h là số tự nhiên suy ra tất cả các số này đều là S_4. Vậy nếu $m=4k+1$ thì $n=4^h m$ là S_4.

Giả sử $m=4k+2$ thì nếu $k=2t$ ta có $m=8t+2$. Vì $n\neq 4^h.2$ và $n=4^h m$ ta có $m\neq 2$ và do đó $t>0$ nghĩa là $t=u+1$ với u là số nguyên không âm. Ta có $m=8(u+1)+2=8u+6+2^2$. Vì $8u+6$ là S_3 suy ra m là S_4, và do đó $n=4^h m$ cũng là S_4. Trong trường hợp $k=2t+1$ ta có $m=8t+6$ và vì $n\neq 4^h.6$ và $n\neq 4^h.14$, ta có $t\geq 2$ do đó $t=u+2$ với u là số nguyên không âm. Vì vậy $m=8(u+2)+6=8u+6+4^2$ mà $8u+6$ là S_3 suy ra m là S_4 nên $n=4^h m$ cũng là S_4. Vậy ta đã chứng minh được nếu $m=4k+2,$ thì $n=4^h m$ là S_4.

Cuối cùng nếu $m=4k+3$ thì nếu $k=2t$ ta có $m=8t+3$. Nhưng với $m\neq 3$ và $m\neq 11$ số $m=8t+3$ là S_4. Vì vậy nếu $m=4k+3$ thì số $n=4^h m$ là S_4 với $n\neq 4^4.3, n\neq 4^h.11$. Nhưng $4.3=12=1^2+1^2+1^2+3^2$ và $4.11=44=1^2+3^2+3^2+5^2$. Vì vậy $n=4^h m$ với $h>0$ là S_4 vì n chẵn và m lẻ. Nếu $k=2t+1$ ta có $m=8t+7$ và do đó m là S_4. Suy ra $n=4^h m$ cũng là S_4.

Tổng hợp các kết quả này suy ra *nếu* n *chẵn không có dạng* $4^h.2, 4^h.6, 4^h.14$ *với* $h=0,1,2,..,$ *thì* n *là* S_4. Kết hợp với kết quả ở trên ta có Định lý 5 được chứng minh. □

Hệ quả. Bình phương một số tự nhiên >1 ngoại trừ 3^2 đều là tổng bình phương bốn số tự nhiên.

Bài tập. Không sử dụng định lý Gauss hãy chứng minh rằng mọi số hữu tỷ dương đều là tổng bình phương của bốn hữu tỷ dương.

Chứng minh. Ký hiệu r là số hữu tỷ dương, $r=m/l$, với l và m là các số tự nhiên.

Theo Định lý 4 suy ra mọi số tự nhiên đều là tổng bình phương của bốn (hoặc ít hơn) các số tự nhiên. Nếu $lm = a^2 + b^2 + c^2 + d^2$ với a, b, c, d là các số tự nhiên thì

$$r = l/m = (a/m)^2 + (b/m)^2 + (c/m)^2 + (d/m)^2$$

suy ra r là tổng bình phương của 4 số tự nhiên. Nếu $lm = a^2 + b^2 + c^2$ với a, b, c là các số tự nhiên thì $r = l/m = (a/m)^2 + (b/3m)^2 + (3c/5m)^2 + (4c/5m)^2$. Nếu $lm = a^2 + b^2$ với a, b là các số tự nhiên thì $r = lm = (a/m)^2 + (b/3m)^2 + (2b/3m)^2 + (2b/3m^2)$. Cuối cùng nếu $lm = a^2$ với a là số tự nhiên thì $r = l/m = 4(a/2m)^2$.

Vậy trong mọi trường hợp r đều là tổng bình phương bốn số hữu tỷ dương. □

Ghi chú. Có thể chứng minh rằng mỗi số hữu tỷ dương đều là tổng bình phương của bốn số hữu tỷ dương khác nhau và với mọi số hữu tỷ dương thì tồn tại vô hạn cách biểu diễn như thế.

Trong mục 4 ta đã chứng minh các số 2^n với $n = 1, 2, \ldots,$ và hệ quả là các số $4^h.2, h = 0, 1, 2, \ldots,$ đều không phải S_3. Mặt khác $3 = 1^2 + 1^2 + 1^2$, $9 = 1^2 + 2^2 + 2^2$, $11 = 1^1 + 1^1 + 3^2$, $17 = 2^2 + 2^2 + 3^2$, $29 = 2^2 + 3^2 + 4^2$, $41 = 1^2 + 2^2 + 6^2$, $4^h.6 = (2^h)^2 + (2^h)^2 + (2^{h+12})$, $4^h.14 = (2^h)^2 + (2^{h+1})^2 + (2^h.3)^2$ với $h = 0, 1, 2, \ldots$ Vì vậy từ Định lý 5 suy ra

Định lý 6. *Số tự nhiên n là tổng bình phương của ba hoặc bốn số tự nhiên khi và chỉ khi n không phải 1,5 và $4^h.2$ với $h = 0, 1, 2\ldots$*

Từ đây ta có hệ quả

Hệ quả. Số tự nhiên lẻ n là tổng bình phương của ba hoặc bốn số tự nhiên khi và chỉ khi n không phải 1 hoặc 5.

Hệ quả này được sử dụng trong chứng minh định lý dưới đây

Định lý 7 (Hurwitz [2]). *Tất cả các số tự nhiên n mà n^2 không phải tổng bình phương của ba số tự nhiên là các số $n = 2^h$ và $n = 2^h.5$ với $h = 0, 1, 2\ldots$*

Chứng minh. Trong mục 4 ta đã chứng minh nếu k không phải S_3 thì $4k$ cũng không phải S_3. Nhưng vì 1 và 5^2 không phải S_3 nên các số 4^h và $4^h.5$, h=0, 1, 2..., cũng không phải S_3. Vậy còn phải chứng minh nếu n là số tự nhiên $\neq 2^h$ và $\neq 2^h.5$ với $h = 0, 1, 2 \ldots,$ thì n^2 là S_3.

Giả sử n là số tự nhiên thỏa mãn $n \neq 2^h$ và $n \neq 2^h.5$ với $h = 0, 1, 2, \ldots$

Gọi s là lũy thừa lớn nhất mà 2^s là ước số của n. Ta có $n = 2^s m$ với m lẻ. Hơn nữa theo giả thiết của n, m phải khác 1 và 5. Từ hệ quả của Định lý 6 suy ra m là tổng bình phương của ba hoặc bốn số tự nhiên, $m = a^2 + b^2 + c^2 + d^2$ với a, b, c là các số tự nhiên và d là số nguyên không âm. Vì vậy

$$m^2 = (a^2 + b^2 + c^2 + d^2)^2 = (a^2 + b^2 - c^2 - d^2)^2 + (2(ac + bd))^2 +$$
$$(2(ad - bc))^2 = (a^2 + b^2 - c^2 - d^2)^2 + (2(ad + bc))^2 + (2(ac - bd))^2$$

Vì m lẻ nên từ $m = a^2 + b^2 + c^2 + d^2$ suy ra trong các số a, b, c, d có hoặc một hoặc ba số là lẻ, các số còn lại chẵn. Vì vậy $a^2 + b^2 - c^2 - d^2$ lẻ và khác 0. Vì a, b, c là các số tự nhiên, $ac + bd$ và $ad + bc$ cũng là các số tự nhiên.

Ta sẽ chứng minh có ít nhất một trong các số $ad - bc$, $ac - bd$ là khác 0. Thật vậy giả sử $ad = bc$ và $ac = bd$ thì $adc = dc^2$ và $acd = bd^2$ suy ra $db^2 = bd^2$ và do đó vì $b > 0, c^2 = d^2$. Vì vậy từ

$c>0$, $a=b$ suy ra $m=2\left(a^2+c^2\right)$ vô lý vì m lẻ. Do đó hoặc $ad-bc\neq 0$ hoặc $ac-bd\neq 0$ (hoặc cả hai). Vậy ít nhất một trong các tổng ở trên cho một biểu diễn m^2 thành tổng bình phương của ba số tự nhiên. Do đó ta có $m^2=x^2+y^2+z^2$ với x, y, z là các số tự nhiên. Vì vậy $n^2=\left(2^s x\right)^2+\left(2^s y\right)^2+\left(2^s z\right)^2$ chứng tỏ n^2 là S_3. Định lý 7 được chứng minh. □

Từ Định lý 2 suy ra số tự nhiên n là đường chéo chính của hình hộp chữ nhật với các cạnh có độ dài là số tự nhiên khi và chỉ khi nó không có dạng 2^h hoặc $2^h.5$ với $h=0, 1, 2...$ Từ định lý 7 suy ra với mọi số tự nhiên lẻ t khác 1 và 5 tồn tại số tự nhiên x, y, z thỏa mãn $t^2=x^2+y^2+z^2$.

Câu hỏi được đặt ra là có phải với mọi số tự nhiên lẻ t khác 1 và 5 thì đều tồn tại các số tự nhiên x, y, z thỏa mãn (x, y, z)=1 và $x^2+y^2+z^2=t^2$. A.Schinzel ([10] Hệ quả 1) đã chứng minh câu trả lời khẳng định cho dự đoán này (dễ dàng chứng minh rằng với số chẵn t thì không tồn tại x, y, z như vậy). F.Ssteiger [1] đã tìm ra 347 hệ x, y, z như vậy với $t\leq 10$. Ví dụ $3^2=1^2+2^2+2^2$,
$7^2=2^2+3^2+6^2, 9^2=1^2+4^2+8^2=4^2+4^2+7^2, 11^2=2^2+6^2+9^2, 13^2=3^2+4^2+12^2$,
$15^2=2^2+5^2+14^2=2^2+10^2+11^2, 17^2=1^2+12^2+12^2=8^2+9^2+12^2$,
$19^2=1^2+6^2+18^2=6^2+6^2+17^2=6^2+10^2+15^2$.

A.Schinzel ([10] Định lý 1) đã cho điều kiện cần và đủ để một số tự nhiên n có thể biểu diễn dưới dạng $x^2+y^2+z^2$ với x, y, z là các số tự nhiên thỏa mãn $(x, y, z)=1$. Các điều kiện này khá phức tạp. Bài toán biểu diễn một số tự nhiên thành tổng của bốn bình phương các số nguyên phân biệt cũng đã được đặt ra.

Ta có định lý G.Pall [1]: *tất cả các số tự nhiên không thể biểu diễn thành tổng bình phương bốn số nguyên là các số $4^h a$ với $h=0, 1, 2,..., a=1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 23, 25, 27, 31, 33, 37, 43, 47, 55, 67, 73, 97, 103, 2, 6, 10, 18, 22, 34, 58, 82.$*

F.Halter-Koch [1] đã tính tất cả các số không phải tổng bình phương bốn số dương phân biệt.

7. Tổng của $m\geq 5$ bình phương dương

Từ Định lý 5 suy ra mọi số tự nhiên lẻ >41 đều là S_4. Vì vậy với mọi số như thế ta cộng thêm với 1^2 hoặc 2^2 và ta thấy mọi số chẵn >42 và mọi số lẻ >45 đều là S_5. Vì vậy ta chỉ xét các số ≤ 45. Từ Định lý 5 thì các số 4, 7, 10, 12, 15, 16, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 30, 31, 33, 34, 35, 36, 37, 38, 39, 40, 42, 43, 44 đều là S_4. Do đó cộng thêm 1 hoặc 4 vào các số đó ta nhận được các số S_5. Bây giờ vẫn còn lại các số 1,2,3,4,6,7,9,10,12,15,18 và 33.

Dễ dàng chứng minh các số này không phải S_5. Chẳng hạn giả sử 33 là S_5 nghĩa là 33= $a^2+b^2+c^2+d^2+e^2$ với a, b, c, d, e là các số tự nhiên $a\geq b\geq c\geq d\geq e$. Vì vậy $a^2+4\leq 33\leq 5a^2$ do đó $6<a^2\leq 29$ suy ra $3\leq a\leq 5$ nghĩa là $a=3$ hoặc 4 hoặc 5. Trong trường hợp $a=3$ số $33-a^2=24=4.6$ là S_4 mâu thuẫn với Định lý 5. Nếu $a=4$ thì số $33-a^2=17$ là S_4 mâu thuẫn với Định lý 5. Nếu $a=5$ thì $33-a^2=8=4.2$ mâu thuẫn với Đinh lý 5. Ta có

Định lý 8. *Tất cả các số tự nhiên không là tổng bình phương của 5 số tự nhiên là các số 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 15, 18, 33.*

Giả sử m là số tự nhiên ≥ 6. Ta sẽ tìm tất cả các số tự nhiên $\leq m+13$ là S_m. Giả sử n là một số như vậy. Khi đó tồn tại các số tự nhiên $a_1, a_2,..., 1_m$ thỏa mãn $a_1\geq a_2\geq ....a_m$ và $n=a_1^2+a_2^3+...+a_m^2$. Vì vậy $a_1^2+(m-1)\leq n\leq m+13$ suy ra $a_1^2\leq 14$ tức là $a_1\leq 3$. Nếu $a_1=1$ suy ra $a_1=a_2=...=a_m=1$ và do đó $m=n$. Giả sử $a_1=2$. Nếu ít nhất bốn số trong các số $a_2, a_3,..., a_m$ bằng 2 thì $n\geq 5.4+$

$(m-5)=m+15$ mâu thuẫn với giả thiết $n\le m+3$. Hệ quả là chỉ có nhiều nhất ba trong các số $a_2,a_3,...,a_m$ có thể bằng 2.

Vì vậy có bốn khả năng: (1) không có số nào 2 và do đó $n=4+(m-1)=m+3$; (2) một số bằng 2 khi đó $n-2.4+(m-2)=m+6$; (3) ba số bằng 2 do đó $n=3.4+(m-3)=m+9$; (4) ba trong số các số $a_2,a_3,...,a_m$ bằng 2 khi đó $n=4.4+(m-4)=m+12$. Vậy ta chỉ cần xét trường hợp $a_1=3$. Khi đó $n-9=a_2^2+a_3^2+...+a_m^2$. Nếu $a_2=3$ thì $n\ge 18+(m-2)$ mâu thuẫn với giả thiết $n\le m+13$. Hệ quả là $a_2\le 2$. Nếu $a_2=1$ thì $a_3=a_4=...=a_m=1$ do đó $n=3^2+m-1=m+8$. Nếu $a_2=2$ và trong các số $a_2,a_3,..,a_m$ có hai hoặc nhiều hơn các số bằng 2 thì $n\ge 3^2+2^2+2^2+(m-3)=m+14$ mâu thuẫn với giả thiết $n\le m+13$. Vì vậy $a_3+a_4=..=a_m=1$ suy ra $m=3^2+2^2+(m-2)=m+11$. Do đó ta đã chứng minh được trong các số tự nhiên $\le m+13$ thì chỉ có các số m, $m+3$, 6, $m+8$, $m+9$, $m+11, m+12$ là S_m. Bây giờ giả sử n là số tự nhiên $>m+13$. Nếu $n=m+28$ thì vì $m\ge 6$ ta có $n=m+28=2.3^2+4.2^2+(m-6).1^2$ suy ra n là S_m. Giả sử $n\ne m+28$ thì $n-(m-5)>18$ (vì $n>m+13$) và $n-(m-5)\ne 33$. Theo Định lý 8 suy ra số $n-(m-5)$ là S_5 do đó số $n=n-(m-5)+(m-5).1^2$ là S_m. Kết hợp các kết quả này ta nhận được

Định lý 9 (Pall [1]). *Nếu m là số tự nhiên ≥ 6 thì tất cả các số nguyên dương không phải tổng bình phương của m số tự nhiên là các số 1, 2, 3, ..., $m-1, m+1, m+2, m+4, m+5, m+7, m+10, m+13$.*

Từ các định lý 8 và 9 suy ra nếu m là số tự nhiên ≥ 5 thì mọi số tự nhiên đủ lớn đều là tổng bình phương của m số tự nhiên. Điều này không đúng với $m=1, 2, 3, 4$ vì tồn tại vô hạn số tự nhiên mà tất cả các số đó đều

1. *không phải bình phương một số tự nhiên (chẳng hạn các số n^2+1 với $n=1, 2, ...$),*
2. *không phải S_2 (chẳng hạn các số $4k+3$ với $k=0, 1, 2...$),*
3. *không phải S_3 (chẳng hạn các số $8k+7$ với $k=0,1,2..$),*
4. *không phải S_4 (chẳng hạn các số $4^h.2$ với $k=0, 1, 2...$).*

Tồn tại vô hạn các số tự nhiên không phải là tổng bình phương của ba (hoặc ít hơn) các số tự nhiên chẳng hạn các số có dạng $8k+7$ với $k=0,1,2$. Tuy nhiên theo định lý Lagrange thì mọi số tự nhiên đều là tổng bình phương của bốn (hoặc ít hơn) các số tự nhiên.

Bài tập. ***1.*** Chứng minh rằng với mọi số tự nhiên m tồn tại vô hạn số tự nhiên là S_i, $i=1, 2,.., m,.$

Chứng minh. Ta chứng minh rằng mọi số có dạng $(13k)^2$ lớn hơn $m+3$ đều có tính chất yêu cầu. Thật vậy ta có $n=(13k)^2=(5k)^2+(12k)^2=(3k)^2+(4k)^2+(12k)^2=(2k)^2+(4k)^2+(7k)^2+(10k)^2$.

Vậy n là S_1, S_2, S_3 và S_4. Nếu $i>4$ và $i\le m$ thì ta có $n=(13k)^2>33$ và $n>m+13$ do đó n là S_i

Ghi chú. Số tự nhiên nhỏ nhất đồng thời là S_1, S_2 và S_3 là 169. Số này là S_i với mọi $i\le 155$ và trong các chỉ số i nằm giữa 155 và 169 thì nó là S_i chỉ với $i=157, 158, 160, 161, 163, 166$ và 169. Chứng minh 169 là S_{100} suy ra từ công thức $169=23.2^2+77.1^2$ hoặc $169=8^2+2.2^2+97.1^2$.

2. Tìm số tự nhiên nhỏ nhất n là S_i với mọi $i\le 1000$.

Lời giải. Ta có $n=34^2$. Thật vậy vì n là S_i nên $n=k^2$, với k là số tự nhiên. Ta có n là S_{1000}, $k^2\ge 1000$ do đó $k\ge 32$. Nhưng theo Định lý 2 thì các số $32^2=2^{10}$ và $33^2=(3.11)^2$ không phải S_2.

Tuy nhiên $34^2 = 16^2 + 30^2 = 2^2 + 24^2 + 24^2$ suy ra 34^2 là S_1, S_2, S_3. Theo Định lý 5 ta thấy 34^2 là S_i với $34^2 > i + 13$ và $i \geq 6$. Do đó 34^2 là S_i với mọi $i \leq 1142$. Một biểu diễn của 34^2 thành tổng của 1000 bình phương là $34^2 = 2.8^2 + 2.4^2 + 996.1^2$.

3. Chứng minh rằng tất cả các số tự nhiên n mà n^2 không phải S_5 là 1,2,3 và tất cả các số tự nhiên n mà n^2 không phải S_6 là 1,2,4. Chứng minh suy trực tiếp từ Định lý 8 và 9.

8. Hiệu của hai bình phương

Định lý 10. *Số nguyên k là hiệu của hai bình phương khi và chỉ khi k không có dạng $4t+2$ với t là số nguyên.*

Chứng minh. Nếu a và b là hai số chẵn thì $a^2 - b^2$ chia hết cho 4. Nếu a và b cùng lẻ thì $a^2 - b^2$ chia hết cho 8. Nếu trong hai số có một số chẵn một số lẻ thì $a^2 - b^2$ lẻ. Do đó ta đã chứng minh được điều kiện cần. Giả sử số nguyên k không có dạng $4t+2$. Hệ quả là hoặc k lẻ hoặc nó chia hết cho 4. Nếu k lẻ thì $k-1$ và $k+1$ đều chẵn và do đó $(k-1)/2$ và $(k+1)/2$ nguyên. Ta có $k = \left(\frac{k+1}{2}\right)^2 - \left(\frac{k-1}{2}\right)^2$. Nếu k chia hết cho 4 thì $k = \left(\frac{k}{4}+1\right)^2 - \left(\frac{k}{4}-1\right)^2$. Vậy ta đã chứng minh được điều kiện đủ. Định lý 10 được chứng minh. □

Lập luận sử dụng trong chứng minh trên cho ta kết quả sau

Định lý 10$^\alpha$. *Mọi số tự nhiên khác 1 và 4 và không có dạng $4t+2$ đều là hiệu của bình phương hai số tự nhiên.*

Dễ dàng chứng minh không có số nào trong các số 1 và 4 có thể biểu diễn thành hiệu của hai bình phương các số tự nhiên. Bây giờ ta sẽ xác định tất cả các biểu diễn của một số tự nhiên cho trước thành hiệu hai bình phương các số tự nhiên.

Giả sử n là số tự nhiên khác 1 và 4 và không có dạng $4z+2$. Giả sử $n = x^2 - y^2$ với x, y là các số tự nhiên thì ta có $n = (x+y)(x-y)$ và nếu $d = x - y$ thì d là ước số tự nhiên của n và nhỏ hơn ước số $d' = x + y$. Hơn nữa các ước số d và d' có cùng tính chẵn lẻ vì $d' - d = 2y$. Ký hiệu d là ước số tự nhiên tùy ý của n mà nhỏ hơn ước số $d' = n/d$ và thỏa mãn d và d' có cùng tính chẵn lẻ. Thế thì $x = \frac{d'+d}{2}$, $y = \frac{d'-d}{2}$ là các số tự nhiên và $x^2 - y^2 = \left(\frac{d'+d}{2}\right)^2 - \left(\frac{d'-d}{2}\right)^2 = dd' = n$. Do đó $n = x^2 + y^2$. Theo cách này thì ta nhận được mọi biểu diễn của n thành hiệu hai bình phương các số tự nhiên. Vì vậy số cách biểu diễn như thế là bằng với số ước số tự nhiên của n và nhỏ hơn đối ước số tương ứng và thỏa mãn cả ước số đó và đối ước số tương ứng của nó là có cùng tính chẵn lẻ. Vậy mọi số nguyên tố lẻ có đúng một biểu diễn theo cách này, đó là $p = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2$. Một hệ quả khác là nếu một số tự nhiên lẻ không phải bình phương đúng thì nó có đúng $d(n)/2$ cách biểu diễn như vậy. Nếu n là bình phương thì nó có $(d(n)-1)/2$ cách biểu diễn như vậy ($d(n)$ là số ước số của n). Từ đây chứng tỏ không chỉ các số nguyên tố lẻ là chỉ có đúng một biểu diễn thành hiệu hai bình phương các số tự nhiên mà bình phương của các số đó cũng có tính chất này. Ta có biểu diễn $p^2 = \left(\frac{p^2+1}{2}\right)^2 - \left(\frac{p^2-1}{2}\right)^2$. Nhưng mọi hợp số lẻ không là bình phương một số nguyên tố lẻ thì có ít nhất hai biểu diễn như vậy. Dễ dàng chứng minh trong số các số chia hết cho 4 thì chỉ có các số có dạng $4p$ hoặc $4p^2$ với p là số nguyên tố ≥ 2 là có đúng một biểu diễn dạng này.

Bài tập. Chứng minh rằng với mọi số tự nhiên m thì đều tồn tại số tự nhiên n có đúng m biểu diễn thành hiệu hai bình phương các số tự nhiên.

Chứng minh. Ta đặt $n=2^{2m+1}$. Thật vậy số này có đúng m biểu diễn thỏa mãn vì dễ thấy các biểu diễn đó là $2^{2m+1}=\left(2^{2m-k}+2^{k-1}\right)^2-\left(2^{2m-k}-2^{k-1}\right)^2$, $k=1, 2, ..., m$

9. Tổng của hai lập phương

Dễ dàng chứng minh mọi số nguyên $\neq 0$ đều có hữu hạn $l\geq 0$ cách biểu diễn thành tổng hai lập phương. Rõ ràng chỉ cần chứng minh với các số tự nhiên. Số cách biểu diễn một số thành tổng của hai lập phương không âm là hữu hạn. Giả sử $n=x^3+y^3$ với x, y là các số nguyên, $x>0, y<0$. Ta có $n=(x+y)\left(x^2-xy+y^2\right)$ với $-xy>0$. Nhưng vì $x+y>0$ suy ra $x+y\geq 1$ và ta có $x^2-xy+y^2\leq n$ mà $-xy>0$ suy ra $x<\sqrt{n}$ và $0<-y<\sqrt{n}$. Từ đây suy ra số cặp x, y là hữu hạn.

Mặt khác các lập phương đồng dư với 0,1 hoặc 8 (mod 9) nên có thể chứng minh không có số nguyên nào có dạng $9k\pm 4$ với k nguyên lại là tổng của ba (hoặc ít hơn) các lập phương. Hệ quả là tồn tại vô hạn số tự nhiên không phải tổng của hai lập phương.

Câu hỏi khi nào thì một số nguyên tố có thể biểu diễn thành tổng của hai lập phương cũng tương đối đơn giản. Giả sử $p=x^3+y^3$ với x, y là các số tự nhiên thì $p=(x+y)\left((x-y)^2+xy\right)$ suy ra vì $x+y\geq 2$ ta phải có $p=x+y$ và $(x-y)^2+xy=1$ suy ra $x=y$ và $xy=1$ tức là $x=y=1$ và $p=2$. Vậy 2 là số nguyên tố duy nhất là tổng của hai lập phương các số tự nhiên.

Bây giờ ta giả sử số nguyên tố p là tổng của lập phương hai số nguyên mà chỉ có một trong hai số là số tự nhiên. Khi đó số nguyên tố p là hiệu của hai lập phương các số tự nhiên. Đặt $p=a^3-b^3$ ta có $p=(a-b)\left(a^2+ab+b^2\right)$ suy ra $a-b=1$ và $p=a^2+ab+b^2=3b(b+1)+1$. Từ đây suy ra nếu số nguyên tố p là hiệu của hai lập phương các số tự nhiên thì p có dạng $p=3b(b+1)+1$ với b là số tự nhiên. Mặt khác nếu p có dạng đó thì $p=(b+1)^3-b^3$. Vì vậy các số nguyên tố có dạng $3b(b+1)+1$ là tất cả các số có thể biểu diễn thành hiệu của hai lập phương các số tự nhiên. Ta chưa biết có tồn tại vô hạn các số nguyên tố có dạng này hay không (từ giả thuyết H suy ra câu trả lời khẳng định). Tuy nhiên ta đã biết rất nhiều số nguyên tố có dạng này. Chẳng hạn $7=2^3-1^3$, $19=3^3-2^3$, $37=4^3-3^3$, $61=5^3-4^3$, $127=7^3-6^3$.

Định lý 11. *Với mọi số tự nhiên m thì đều tồn tại số tự nhiên n có thể biểu diễn thành tổng của hai lập phương theo ít nhất là m cách phân biệt.*

Chứng minh. Theo mục 15 Chương 2 ta đã chứng minh tồn tại dãy vô hạn các hệ $x_k, y_k, z_k\ (k=1, 2, ...)$ các số nguyên thỏa mãn $(x_k, y_k)=1$, $x_k^3+y_k^3=7z_k^3$ và $0<|z_1|<|z_2|<...$ Đổi dấu nếu cần thiết các số x_k và y_k ta có thể giả sử $z_k>0$ với mọi $k=1, 2, ...$

Đặt $n=7z_1^3z_2^3...z_m^3$, $a_k=\dfrac{z_1z_2...z_m}{z_k}x_k$, $b_k=\dfrac{z_1z_2...z_m}{z_k}y_k$ với $k=1, 2, ..., m$.

Tất cả các số a_k và b_k đều nguyên và hơn nữa $a_k^3+b_k^3=n$. Với các chỉ số i, j nào đó của dãy 1,2,...,m ta có $a_i=a_j$ khi đó vì $z_k\neq 0$ với mọi $k=1,2,..m$, $x_i/z_i=x_j/z_j$ suy ra vì $(x_i, z_i)=(x_j, z_j)$=1 ta có $x_i=x_j$ và $z_i=z_j$ vô lý.

Tương tự nếu $a_i=b_j$ thì $x_i/z_i=y_j/z_j$ mà $(x_i, z_i)=(y_j, z_j)=1$ nên ta có vô lý.

Vậy ta nhận được m cách biểu diễn khác nhau số n thành tổng hai lập phương. Định lý 11 được chứng minh. □

Định lý 12. *Ký hiệu n là số tự nhiên không phải lập phương một số tự nhiên và cũng không phải hai lần một lập phương một số tự nhiên. Nếu n là tổng của hai lập phương các số hữu tỷ thì n có vô hạn cách biểu diễn như vậy.*

Chứng minh. Ký hiệu r là số nguyên lớn nhất mà r^3 là ước số của n. Thế thì $n=r^3a$ với a là số tự nhiên không chia hết cho bất kỳ lập phương một số tự nhiên >1 nào. Theo giả thiết a không thể bằng 1 hoặc 2. Giả sử n là tổng hai lập phương các số hữu tỷ. Ta quy đồng các phân số đó với mẫu số chung và có thể viết $n=(u/t)^3+(v/t)^3$, với u, v là các số nguyên và t là số tự nhiên. Vì vậy $u^3+v^3=a(rt)^3$. Các số u,v là khác 0 vì theo giả sử n không phải lập phương một số tự nhiên, và do đó nó không phải lập phương một số hữu tỷ. Vì vậy $d=(u,v)$ là số tự nhiên. Đặt $u=dx$, $v=dy$ với x, y là các số nguyên thỏa mãn $(x,y)=1$. Ta có $d^3\,|\,a(rt)^3$ suy ra vì a không chia hết cho bất kỳ lập phương một số tự nhiên >1 nào nên $d\,|\,rt$. Và do đó $rt=dz$ suy ra z là số tự nhiên. Ta thấy các số x, y, z thỏa mãn phương trình $x^3+y^3=az^3$. Vì vậy theo Định lý 10 mục 15 Chương 2 suy ra phương trình này có vô hạn nghiệm nguyên x, y, z với $(x,y)=(x,z)=(y,z)$ =1 và $z\neq 0$. Với mọi nghiệm như vậy thì ta có $nz^3=a(rz)^3=(rx)^3+(ry)^3$ suy ra $n=(rx/z)^3+(ry/z)^3$. Hơn nữa ta thấy các nghiệm khác nhau cho tương ứng các biểu diễn khác nhau vì các phân số x/z và y/z đều là tối giản. Định lý 12 được chứng minh. □

Hệ quả. *Nếu r là số hữu tỷ không phải lập phương một số hữu tỷ mà cũng không phải hai lần lập phương một số hữu tỷ thì nếu r có thể biểu diễn thành tổng hai lập phương các số hữu tỷ thì sẽ có vô hạn cách biểu diễn như vậy*

Chứng minh. Rõ ràng có thể giả sử r là số hữu tỷ dương, nghĩa là $r=l/m$ với l và m là các số tự nhiên và $(l,m)=1$. Theo giả thiết thì tồn tại các số nguyên u,v và số tự nhiên t thỏa mãn $\dfrac{l}{m}=\left(\dfrac{u}{t}\right)^3+\left(\dfrac{v}{t}\right)^3$ suy ra $lm^2=\left(\dfrac{um}{t}\right)^3+\left(\dfrac{vm}{t}\right)^3$. Vì vậy số tự nhiên lm^2 là tổng hai lập phương các số hữu tỷ và nó không là lập phương của số hữu tỷ hay là hai lần lập phương một số hữu tỷ bởi vì nếu ngược lại thì $r=l/m$ sẽ là lập phương một số hữu tỷ hoặc hai lần lập phương một số hữu tỷ, mâu thuẫn với giả thiết.

Vậy theo Định lý 12 suy ra số lm^2 có vô hạn cách biểu diễn thành tổng hai lập phương các số hữu tỷ, suy ra số $r=lm^2/m^3$ cũng có tính chất đó. Hệ quả được chứng minh. □

10. Phương trình $x^3+y^3=z^3$

Bây giờ ta trình bày lời giải sơ cấp cho trường hợp riêng của Định lý cuối cùng của Fermat với số mũ 3. Lời giải này được trình bày bởi J.Browkin dựa trên ý tưởng cơ bản của R.D.Carmichael trong [4] trang 67-70.

Định lý 13. *Phương trình sau đây không có nghiệm nguyên x, y, $z\neq 0$.*

(29) $$x^3+y^3=z^3$$

Bổ đề. Tất cả các nghiệm nguyên a,b,s của phương trình

(30) $$s^3=a^2+3b^2$$

mà (a,b)=1, s lẻ, được cho bởi công thức sau

(31) $$s=\alpha^2+3\beta^2,\ a=\alpha^3-9\alpha\beta^2,\ b=3\alpha^2\beta-3\beta^3,$$

Với các số $\alpha,\ \beta$ thỏa mãn điều kiện

(32) $$\alpha \not\equiv \beta \pmod 2,\quad (\alpha,3\beta)=1$$

Chứng minh bổ đề. Đầu tiên ta giả sử các số nguyên α,β thỏa mãn ***(32)***. Xét các số a,b,s xác định bởi ***(31)***. Khi đó sử dụng đẳng thức

(33) $$\left(A^2+3B^2\right)^3=\left(A^3-9AB^2\right)^2+3\left(3A^2B-3B^3\right)^2,$$

suy ra các số a,b,s thỏa mãn ***(30)***. Từ ***(32)*** suy ra

$$(a,b)=(\alpha\left(\alpha^2-9\beta^2\right),\ 3\beta\left(a^2-\beta^2\right))=\left(\alpha^2-9\beta^2,\alpha^2-\beta^2\right)=\left(8\beta^2,\alpha^2-\beta^2\right)=1$$

và s lẻ. Giả sử các số nguyên a,b,s thỏa mãn ***(30)*** và (a,b)=1 và s lẻ. Để chứng minh bổ đề ta tìm các số nguyên α,β thỏa mãn ***(31)*** và ***(32)***.

Lưu ý mọi ước số nguyên tố của s đều có dạng $6k+1$. Thật vậy nếu $p\mid s$ thì vì s lẻ, $p\geq 3$. Nếu $p=3$ thì vì ***(30)***, $3\mid a^2$ do đó $3\mid a$, và theo ***(30)***, $9\mid 3b^2$ suy ra $3\mid b$, mâu thuẫn với $(a,b)=1$. Vậy $p>3$. Vì $p\mid s$ và (a,b)=1 theo ***(30)*** suy ra $(b,p)=1$ nên $0\equiv a^2+3b^2\equiv b^2\left(a^2b^{p-3}+3\right)\pmod p$. Vậy $\left(ab^{(p-3/2)}\right)^2\equiv -\pmod p$. Chứng tỏ -3 là thặng dư bậc hai mod p. Suy ra p có dạng $6k+1$.

Sự khác tính chẵn lẻ của α,β được suy ra bằng quy nạp theo n là số các ước số nguyên tố của s. Nếu $n=0$ thì vì $s^3=a^2+3b^2\geq 0$ ta có $s=1$. Do đó $a=\pm 1, b=0$. Nên $\alpha=\pm 1,\ \beta=0$. Suy ra ***(31)*** và ***(32)*** được thỏa mãn. Bây giờ giả sử bổ đề được chứng minh với số tự nhiên $n\geq 0$. Ký hiệu s là số nguyên có $n+1$ ước số nguyên tố và hai số nguyên tố cùng nhau a,b thỏa mãn ***(30)***. Ký hiệu p là ước số nguyên tố của s do đó $s=tp$ với t có n ước số nguyên tố. Vì p có dạng $6k+1$ nên tồn tại các số nguyên α_1,β_1 mà $p=\alpha_1^2+3\beta_1^2$ với α_1,β_1 thỏa mãn ***(32)***. Nếu $c=\alpha_1^3-9\alpha_1\beta_1^2, d=3\alpha_1^2\beta_1$ -$3\beta_1^3$, Theo đẳng thức ***(33)*** suy ra $p^3=c^3+3d^2$ và theo ***(32)*** thì $(c,d)=1$. Ta có

(34) $$t^3p^6=s^3p^3=\left(a^2+3b^2\right)\left(c^2+3d^2\right)=\left(ac\pm 3bd\right)^2+3\left(ad\mp bc\right)^2.$$

Xét tích

(35) $$\begin{aligned}(ad-bc)(ad+bc)&=(ad)^2-(bc)^2=\left(a^2+3b^2\right)d^2-b^2\left(c^2+3d^2\right)\\&=t^3p^3d^2-b^2p^3=p^3\left(t^3d^2-b^2\right).\end{aligned}$$

Nếu $p\mid ad-bc$ và $p\mid ad+bc$ thì $p\mid 2ad$ và $p\mid 2bc$ suy ra vì p lẻ nên $p\mid ad$ và $p\mid bc$. Nhưng $p^3=c^2+3d^2$ và $(c,d)=1$. Vì vậy $(p,c)=(p,d)=1$ và do đó $p\mid a$ và $p\mid b$, mâu thuẫn với $(a,b)=1$. Vậy chỉ có một trong hai số $ad-bc$ và $ab+bc$ là chia hết cho p. Nhưng theo ***(35)*** số này chia hết cho p^3. Hệ quả là với lựa chọn dấu thích hợp trong đẳng thức ***(34)*** thì số trong dấu ngoặc cuối cùng vế phải là chia hết cho p^3. Hơn nữa vế trái của ***(34)*** chia hết cho p^6 suy ra số còn lại trong dấu ngoặc của vế phải công thức ***(34)*** chia hết cho p^3.

Do đó với lựa chọn dấu thích hợp thì

(36) $$u=\frac{ac\pm 3bd}{p^3}\ \text{và}\ v=\frac{ad\mp 3bc}{p^3}$$

là các số nguyên. Công thức ***(34)*** trở thành

(37) $$t^3=u^2+3v^2$$

Ta tìm nghiệm của phương trình ***(36)*** với a và b. Ta có $a=uc+3vd$ và $\pm b=ud-vc$ mà $(a,b)=1$ suy ra $(u,v)=1$. Theo giả thiết quy nạp và công thức ***(37)*** thì tồn tại các số nguyên α_2,β_2 thỏa mãn ***(32)*** mà

$$t=\alpha_2^2+3\beta_2^2,\quad u=\alpha_2^3+9\alpha_2\beta_2^2,\quad v=3\alpha_2^2\beta_2-3\beta_2^3.$$

Ta viết $\alpha=\alpha_1\alpha_2+3\beta_1\beta_2,\quad \beta=\alpha_2\beta_1-\beta_2\alpha_1$. Khi đó

$$\begin{aligned}
s &= tp=(\alpha_1^2+3\beta_1^2)(\alpha_2^2+3\beta_2^2)=\alpha^2+3\beta^2,\\
a &= cu+3dv=(\alpha_1^3-9\alpha_1\beta_1^2)(\alpha_2^3-9\alpha_2\beta_2^2)+\\
&\quad +3(3\alpha_1^2\beta_1-3\beta_1^3)(3\alpha_2^2\beta_2-3\beta_2^3)=\alpha^3-9\alpha\beta^2,\\
\pm b &= du-cv=(3\alpha_1^2\beta_1-3\beta_1^3)(\alpha_2^3-9\alpha_2\beta_2^2)-\\
&\quad -(\alpha_1^3-9\alpha_1\beta_1^2)(3\alpha_2^2\beta_2-3\beta_2^3)=3\alpha^2\beta-3\beta^3.
\end{aligned}$$

Đổi dấu nếu cần thiết đối với β ta thấy α,β thỏa mãn ***(31)***. Do $(a,b)=1$ suy ra các số α,β thỏa mãn ***(32)***. Bổ đề được chứng minh. □

Chứng minh định lý 13. Giả sử các số x, y, z thỏa mãn ***(29)*** và hơn nữa chúng được chọn với $|xyz|\neq 0$ nhỏ nhất có thể. Rõ ràng x, y, z đôi một nguyên tố cùng nhau vì nếu ngược lại trong số chúng có hai số có ước số chung là $d>1$ thì ước số này là ước số chung của cả ba số đó và do đó ta có thể chia các vế phương trình ***(29)*** cho d^3 và nhận được một nghiệm nhỏ hơn. Dễ dàng thấy các số x,y,z không cùng lẻ và có đúng một số trong chúng là chẵn. Giả sử z chẵn và x, y lẻ. Do đó các số $x+y$ và $x-y$ chẵn suy ra

(38) $$x+y=2u,\quad x-y=2w.$$

Vì vậy

(39) $$x=u+w,\quad y=u-w.$$

Mà $(x,y)=1$, x, y lẻ suy ra $(u,w)=1$ và $u\neq w\,(\text{mod}2)$. Thế các giá trị trong ***(39)*** vào ***(29)*** ta có

(40) $$2u\left(u^2+3w^2\right)=z^3.$$

Nếu $(u,3)=1$ thì vì $u\neq w\,(\text{mod}2)$ ta có $\left(2u,u^2+3w^2\right)=1$ do đó

(41) $$2u=t^3,\ u^2+3w^2+s^3,$$

với s là số lẻ và (u,v)=1. Theo bổ đề thì tồn tại các số nguyên α,β thỏa mãn ***(32)*** và $u=\alpha^3-9\alpha\beta^2$. Vì vậy theo ***(41)*** thì $t^3=2u=2\alpha(\alpha-3\beta)(\alpha+3\beta)$. Dễ dàng kiểm tra các số 2α, $\alpha-3\beta,\alpha+3\beta$ đôi một nguyên tố cùng nhau do đó $2\alpha=\sigma^3,\alpha-3\beta=\tau^3,\alpha+3\beta=\varrho^3$ suy ra $\sigma^3=\varrho^3+\tau^3$. Nhưng $|\varrho\,\sigma\tau|=|t^3|=|2u|=|x+y|=0$ và $|x+y|\leq|xyz|<|xyz|^3$ mâu thuẫn với giả thiết về tính nhỏ nhất của $|xyz|$. Nếu $3|u$ nghĩa là $u=3v$ thì ***(40)*** trở thành

(42) $$18v\left(3v^2+w^2\right)=z^3,$$

suy ra vì $3v\neq w\,(\text{mod}2)$ và $(3v,w)=1$ ta có $\left(18v,3v^2+w^2\right)=1$ do đó

(43) $18v = t^3, \quad 3v^2 + w^2 = s^3,$

Với s lẻ và (v, w)=1. Theo bổ đề tồn tại các số nguyên α, β thỏa mãn ***(32)*** và $v = 3\beta\alpha^2 - 3\beta^3$.

Vì vậy theo ***(43)*** thì $t^3 = 18v = 27.2\beta(\alpha+\beta)(\alpha-\beta)$. Dễ dàng kiểm tra các số $2\beta, \alpha+\beta, \alpha-\beta$ đôi một nguyên tố cùng nhau. Vậy $2\beta = \sigma^3, \alpha+\beta = \tau^3, \alpha-\beta = Q^3$ suy ra $\tau^3 = \sigma^3 + Q^3$. Nhưng $|\tau\sigma Q|^3 = \left|\frac{1}{27}t^3\right| = |\frac{2}{3}v| = \frac{2}{9}|u| = \frac{1}{9}|x+y| \neq 0$ và $\frac{1}{9}|x+y| \le |xyz| \le |xyz|^3$ mâu thuẫn với giả thiết về tính nhỏ nhất của $|xyz|$. Định lý 13 được chứng minh. □

Hệ quả trực tiếp của Định lý 13 là

Hệ quả. *Phương trình $x^3 + y^3 = z^3$ không có nghiệm hữu tỷ $\neq 0$.*

Bài tập. ***1.*** Chứng minh rằng Định lý 13 tương đương với định lý nói rằng phương trình $3x^2 + 1 = 4y^3$ không có nghiệm hữu tỷ nào ngoại trừ $x = \pm 1,\ y = 1$.

Chứng minh. Nếu hai số hữu tỷ $x \neq \pm 1$ và y thỏa mãn $3x^2 + 1 = 4y^3$ thì $u = (3x-1)/2$ là số hữu tỷ, $u \neq 1$ và $u \neq -2$. Hơn nữa từ $u^2 + u + 1 = 3y^2$ suy ra $y \neq 0$ (vì phương trình $u^2 + u + 1 = 0$ không có nghiệm hữu tỷ). Hệ quả là $(2+u)^3 + (1-u)^3 = (3y)^3$ mâu thuẫn với hệ quả của Định lý 13. Giả sử Định lý 13 sai. Khi đó tồn tại các số hữu tỷ u, v khác 0 thỏa mãn $u^3 + v^3 = 1$ và $x = (u-v)/(u+v),\ y = 1/(u+v)$ là các số hữu tỷ thỏa mãn $3x^2 + 1 = 4y^3$. Nếu $x = \pm 1$ và $y = 1$ thì $u + v = 1,\ u - v = \pm 1$, suy ra $u = 0$ hoặc $v = 0$, mâu thuẫn. □

2. Chứng minh rằng phương trình $x^3 + y^3 = z^3 + 1$ có vô hạn nghiệm tự nhiên x, y, z.

Lời giải. Suy trực tiếp từ đẳng thức Gerardin: $(9n^4)^3 + (9n^3+1)^3 = (9n^4+3n)^3 + 1, \quad n = 1, 2, \ldots$

Chẳng hạn với $n = 1, 9^3 + 10^3 = 12^3 + 1$; nếu $n = 2, 144^3 + 73^3 = 150^3 + 1$.

Ta cũng có $64^3 + 94^3 = 103^3 + 1$. □

3. Tìm ba số tự nhiên phân biệt a, b, c mà $\sqrt[3]{a}, \sqrt[3]{b}, \sqrt[3]{c}$ là các số vô tỷ và $\sqrt[3]{a} + \sqrt[3]{b} = \sqrt[3]{c}$.

Lời giải. $a = 2,\ b = 16,\ c = 54$. □

11. Tổng của ba lập phương

Trong mục 9 ta đã lưu ý rằng không có số nguyên có dạng $9k \pm 4$ mà là tổng của ba (hoặc ít hơn) các lập phương. Mặt khác ta chưa biết có phải mọi số nguyên không có dạng $9k \pm 4$ (với k nguyên) đều là tổng của ba lập phương hay không. Điều này đúng với mọi số nguyên $n, -30 < n < 30$, nhưng ta chưa biết cách nào biểu diễn 30 thành tổng của ba lập phương và chưa biết một biểu diễn như thế có tồn tại hay không. V.L.Gardiner, R.B.Lazarus và P.R.Stein [1] đã tìm ra nghiệm của phương trình $x^3 + y^3 - z^3 = \varepsilon k$ với $0 < k < 1000$ và các số nguyên x, y, z, ε thỏa mãn $0 \le x \le y \le 2^{16},\ \varepsilon = \pm 1$. Họ cũng chứng minh phương trình này không có nghiệm với k=30, 33, 39, 42, 52, 74, 75, 84 và với $k = 12, \varepsilon = 1$ thì tồn tại duy nhất nghiệm $z = 11, y = 10, x = 7$. Kết quả này không chỉ ra rằng khi nào thì phương trình này có nghiệm nguyên x, y, z mà có ít nhất hai số trong chúng có giá trị tuyệt đối lớn hơn 2^{16}. Đối với một số trường hợp của số nguyên k ta có thể chứng minh tồn tại vô hạn cách biểu diễn nó thành tổng của ba lập phương chẳng hạn (Mordell [4])

$$0 = n^3 + (-n)^3 + 0^3,\ 1 = (9n^4)^3 + (1-9n^3)^3 + (3n-9n^4)^3,\ 2 = (1+6n^3)^3 + (1-6n^3)^3 + (-6n^2)^3$$

với mọi $n=0,\pm1,\pm2,...$ Với $k=1$ thì có những nghiệm không nhận được từ công thức trên. Chẳng hạn $1=94^3+64^3+\left(-103\right)^3$.

D.H.Lehmer [7] đã chứng minh rằng tồn tại vô hạn biểu diễn như vậy (Godwin [1]).

Thật vậy, lấy $x=3^3t^4\left(2^43^2t^6-5\right), y=-3t\left(6^4t^9+2^43^3t^6+3^3t^3-1\right), z=2^43^5t^9+2^33^4t^6-3^2t^3+1$.

Khi đó dễ dàng kiểm tra rằng với mọi t, $x^3+y^3+z^3=1$. Nếu t là số tự nhiên không chia hết cho 3 thì tất cả các nghiệm nhận được đều khác $9n^4, 1-9n^3, 3n-9n^4$ bởi vì kiểm tra trực tiếp ta thấy không có giá trị nào của x,y,z bằng $9n^4$ vì y, z không chia hết cho 9 và nếu $x=9n^4$ thì vì $3^3t^4\mid x$ suy ra $3t\mid n$ do đó $n=3ut$ (u là số nguyên) suy ra $2^43^2t^6-5=3^3u^4$ vô lý.

Thay $t=1$ ta có $x=3753, y=-5262, z=4528$. Với $t=-1$ ta có $x=3753, y=-2676, z=-3230$.

Với $k=2$ ta chưa biết biểu diễn nào của k thành tổng của ba lập phương ngoài cách trình bày ở trên. Ta chưa biết số nguyên k nào không có dạng $9t\pm4$ mà có hữu hạn biểu diễn thành tổng ba lập phương. Mặt khác dễ dàng chứng minh tồn tại vô hạn k không có dạng $9t\pm4$ mà không thể biểu diễn thành tổng lập phương của ba số tự nhiên. Với $k=3$ ta chỉ biết 4 cách biểu diễn k thành tổng ba lập phương, đó là $(x,y,z)=(1,1,1), (-5,4,4), (4,-5,4), (4,4,-5)$ và ta chưa biết có tồn tại các biểu diễn khác hay không.

Sau đây ta sẽ chứng minh số 3 và rất nhiều các số hữu tỷ dương khác có thể biểu diễn vô hạn cách thành tổng của ba lập phương các số hữu tỷ dương (Định lý 14).

Ta nghiên cứu các biểu diễn số nguyên dưới dạng $x^3+y^3+2z^3$ với x,y,z là các số nguyên.

Lai, Russel and Blundon [1] đã chứng minh với mọi số tự nhiên ≤1000 ngoại trừ 19 số trong chúng (ba trong số này được tìm lại bởi J.C.Littejohn trong các cuộc trao đổi với M.Lai) là có ít nhất một biểu diễn như vậy. Chẳng hạn $13=\left(-35\right)^3+\left(-62\right)^3+2\left(52\right)^3$, $20=63^3+\left(-3\right)^3+2\left(-50\right)^3$, $31=53^3+31^3+2\left(-44\right)^3$. Số 76 là số tự nhiên nhỏ nhất mà chúng ta chưa biết nó có dạng $x^3+y^3+2z^3$ với x, y, z là các số nguyên hay không. Số 2 ngoại trừ phân tích tầm thường $2=t^3+\left(-t\right)^3+2.1^3$ thì có vô hạn biểu diễn dạng trên. Điều này suy ra từ đẳng thức $2=\left(1-t-t^2\right)^3+\left(1+t-t^2\right)^3+2\left(t^2\right)^3$ với mọi số nguyên t. Đây là hệ quả của đẳng thức cho bởi B.Segre [1] (trường hợp $t=2^m$ cho bởi Niewiadomski [1]).

Định lý 14. *Mọi số hữu tỷ dương đều có thể biểu diễn vô hạn cách thành tổng của ba lập phương các số hữu tỷ (Hardy và Wright [1] trang 197-199 Định lý 34).*

Chứng minh. Với r là số hữu tỷ dương cho trước ký hiệu v là số hữu tỷ thỏa mãn $\sqrt[3]{3r/2}<v<\sqrt[3]{3r}$. Đặt $u=\left(3r-v^3\right)/\left(3r+v^3\right), s=v\left(1+u\right)$ $z=su, t=s/3\left(1-u^2\right), x=s-t, y=t-z$.

Vì $v<\sqrt[3]{3r}$ suy ra u là số dương và nhỏ hơn 1. Các số u,s,z,t là hữu tỷ dương và x, y là các số hữu tỷ. Vì $v>\sqrt[3]{3r/2}$ nên ta có $v^3>\frac{3}{2}r$ suy ra $u=6r/\left(3r+v^3\right)-1<\frac{1}{3}$. Hệ quả là $3\left(1-u^2\right)>1$, $s>t$ và $3u\left(1-u^2\right)<1$ suy ra $z<1$. Do đó $x>0$ và $y>0$. Nhưng

$$x^3+y^3+z^3=\left(s-t\right)^3+\left(t-z\right)^3+z^3=s^3-3\left(s^2-z^2\right)t+3\left(s-z\right)t^2$$

và $3\left(s^2-z^2\right)=3s^2\left(1-u^2\right)$ suy ra $3\left(s^2-z^2\right)t=s^3,$ do đó

$$x^3+y^3+z^3=3\left(s-z\right)t^2=3s\left(1-u\right)t^2=$$

$$=\frac{s^3(1-u)}{3(1-u^2)^2}=\frac{s^3}{3(1+u)(1-u^2)}=\frac{v^3(1+u)^2}{3(1-u^2)}=\frac{v^3(1+u)}{3(1-u)}=r$$

Do v có thể chọn là một số hữu tỷ bất kỳ nhỏ hơn $\sqrt[3]{3r}$ và đủ gần $\sqrt[3]{3r}$ nên u (và do đó $su=z$) có thể nhỏ tùy ý. Suy ra phương trình có vô hạn nghiệm hữu tỷ dương.

Định lý 14 được chứng minh. □

Với $r=3,\ v=1$ công thức này suy ra $3=\left(\frac{2}{15}\right)^3+\left(\frac{17}{75}\right)^3+\left(\frac{36}{25}\right)^3$.

Định lý 14 có hai hệ quả sau đây

Hệ quả 1. *Với mọi số tự nhiên n thì $x^3+y^3+z^3=nt^3$ có vô hạn nghiệm tự nhiên x, y, z, t mà $(x,y,z,t)=1$.*

Hệ quả 2. *Với mọi số tự nhiên $s\geq 3$ mọi số hữu tỷ dương có vô hạn cách biểu diễn thành tổng lập phương của s số hữu tỷ dương.*

Nếu trong chứng minh Định lý 14 ta chọn v đủ gần và lớn hơn $\sqrt[3]{3r}$ thì $u<0, 1+u>0, 1-u^2>0$, $u^2<\frac{2}{3}$ do đó $s>0,\ z<0, t>0, y>0, x>0$. Từ đây ta có định lý: *mọi số hữu tỷ dương đều có vô hạn cách biểu diễn dưới dạng $x^3+y^3-z^3$ với x, y, z là các số hữu tỷ dương.* Áp dụng với $r+t^3$ khi r, t là các số hữu tỷ dương ta có

Định lý 15. *Mọi số hữu tỷ đều có vô hạn biểu diễn dưới dạng $x^3+y^3-z^3-t^3$ với x, y, z, t là các số hữu tỷ dương.*

12. Tổng của bốn lập phương

Cách đây vài năm tác giả đặt ra giả thuyết C: mọi số nguyên g đều có vô hạn biểu diễn dưới dạng $x^3+y^3-z^3-t^3$ với x, y, z, t là các số tự nhiên. Giả thuyết này được chứng minh bởi Demyanenko [2] với các số nguyên mà $-1000\leq g\leq 1000$ và với mọi $g\neq \pm 14 \pmod 9$. Chứng minh đó dựa trên trên kết quả sau của L.J.Mordell [13]: *nếu $g=a^3+b^3-c^3-d^3$ với a, b, c, d là các số nguyên $(a+b)(c+d)>0$ và $a\neq b$ hoặc $c\neq d$ và hơn nữa nếu $(a+b)(c+d)$ không phải bình phương một số tự nhiên thì giả thuyết C là đúng với g.* Với g=0 giả thuyết C là hệ quả trực tiếp của đẳng thức $0=n^3+1^3-n^3-1^3$ với mọi $n=1, 2, \ldots$. Ta trình bày chứng minh giả thuyết C với g=1.

Chỉ cần chứng minh phương trình $(t+13)^3+(u+14)^3-(t+3)^3-(u+17)^3=1$ có vô hạn nghiệm nguyên t, u. Phương trình này đúng với $t=u=0$ và nếu nó đúng với t và u thì các số $t_1=11t+6u+173, u_1=20t+11u+315$ cũng thỏa mãn phương trình. Chẳng hạn do $t=0$ và $u=0$ thỏa mãn phương trình nên $t_1=173,\ u_1=315$ cũng thế và hơn nữa $186^3+329^3-176^3-332^3=1$.

Do phương trình $x^3+y^3-z^3-t^3=1$ có vô hạn nghiệm tự nhiên x, y, z, t suy ra tồn tại vô hạn số tự nhiên n mà n và $n+1$ đều là tổng hai lập phương dương.

Nếu g=2 thì giả thuyết C được suy ra từ đẳng thức $2=(9n^4)^3+1^3-(9n^3-1)^3-(9n^4-3n)^3$ với mọi $n=1, 2, \ldots$ Đặc biệt với $n=1$ ta có $2=9^3+1^3-8^3-6^3$.

Nếu g=3 thì giả thuyết C được suy ra từ $3=(6n^3+1)^3+1^3-(6n^3-1)^3-(6n^2)^3$ với $n=1, 2, \ldots$.

Ta cũng biết một số nghiệm nguyên dương của phương trình $x^3+y^3+z^3-t^3=1$. Chẳng hạn $4^3+4^3+6^3-7^3=1.4^3+38^3+58^3-63^3=1.4^3+37^3+63^3-67^3=1$. Gần đây J.A.Gabowicz [1] đã chứng minh rằng phương trình này có vô hạn nghiệm tự nhiên.

Mặt khác từ đẳng thức $\left(6n^3+1\right)^3-1^3-\left(6n^2\right)^3-\left(6n^3-1\right)^3=1$ với $n=1,2,\ldots$ dễ dàng chứng minh tồn tại vô hạn nghiệm tự nhiên x,y,z,t của phương trình $x^3-y^3-z^3-t^3=1$.

A.Makowski ([1] trang 121) đã chứng minh phương trình $x^3-y^3-z^3-t^3=2$ có vô hạn nghiệm tự nhiên. Điều này suy ra từ đẳng thức $\left(3n^3+1\right)^3-\left(3n^3-1\right)^3-\left(3n^2\right)^3-\left(3n^2\right)^3=2$ với $n=1,2,..$ Phương trình này còn có các nghiệm không nhận được từ đẳng thức này chẳng hạn $235^3-3^3-69^3-233^3=2.683^3-650^3-353^3-2^3=2$.

Bài tập. Chứng minh rằng tồn tại vô hạn số tự nhiên g mà các phương trình g= $x^3+y^3-z^3-t^3$, g= $x^3+y^3+z^3-t^3$ và g= $x^3-y^3-z^3-t^3$ đều có vô hạn nghiệm tự nhiên $x,\ y,\ z,\ t$.

Chứng minh. Các số g = a^3-b^3 với $b<a$ là các số tự nhiên tùy ý thỏa mãn tính chất yêu cầu vì

$$a^3-b^3=a^3+n^3-b^3-n^3.$$
$$a^3-b^3=a^3+((9n^3-1)b)^3+((9n^4-3n)b)^3-(9n^4b)^3.$$
$$a^3-b^3=(9n^4a)^3-((9n^3-1)a)^3-((9n^4-3n)a)^3-b^3.$$

(Schinzel và Sierpinski [2] trang 26-27). Dễ dàng chứng minh rằng mọi số nguyên đều có vô hạn cách biểu diễn như là tổng của 5 lập phương. Đẳng thức $6t=\left(t+1\right)^3+\left(t-1\right)^3+\left(-t\right)^3+\left(-t\right)^3$ chứng tỏ mọi số nguyên chia hết cho 6 đều là tổng của 4 lập phương. Để chứng minh mọi số nguyên đều có vô hạn cách biểu diễn thành tổng của 5 lập phương ta chỉ cần chứng minh rằng với mọi số nguyên, tồn tại số tự nhiên đủ lớn mà hiệu của số nguyên ban đầu và lập phương của số tự nhiên này là chia hết cho 6. Ký hiệu g là số nguyên tùy ý, r là phần dư nhận được khi chia g cho 6. Khi đó g= $6k+r$. Với mọi số tự nhiên n ta có $6k+r-\left(6n+r\right)^3\equiv r-r^3\equiv 0\left(\mathrm{mod}\,6\right)$ do đó $6\left|\text{g-}\left(6n+r\right)^3\right.$.

13. Một số tổng các lập phương có giá trị bằng nhau

Trong mối liên hệ với Định lý 13 một câu hỏi thú vị được đặt ra là với các số tự nhiên m và $n\geq m$ nào thì phương trình

(44) $$x_1^3+x_2^3+....+x_m^3=y_1^3+y_2^3+...+y_n^3$$

có nghiệm là các số tự nhiên phân biệt $x_1,\ x_2,...,x_m,y_1,y_2,...,y_n$. Rõ ràng phương trình không có nghiệm như vậy với $n=m=1$. Định lý 13 suy ra phương trình cũng không có nghiệm khi $m=1,\ n=2$. Ta chứng minh định lý sau đây

Định lý 16. *Phương trình **(44)** với n,m là các số tự nhiên $n\geq m$ là có nghiệm tự nhiên phân biệt $x_1,\ x_2,...,\ x_m,y_1,y_2,...,y_n$ khi và chỉ khi không xảy ra trường hợp $m=n=1$ và $m=1,n=2$ (Sierpinski [24]).*

Ta chỉ cần chứng minh điều kiện đủ.

Bổ đề. *Với mọi số tự nhiên $n>2$ thì luôn tồn tại số tự nhiên mà lập phương của nó là tổng của n lập phương dương phân biệt.*

Chứng minh bổ đề. Các công thức $6^3=3^3+4^3+5^3$ và $13^3=5^3+7^3+9^3+11^3$ chứng minh bổ đề trong trường hợp $n=3$ và $n=4$. Giả sử bổ đề đúng với số tự nhiên $n>2$. Tồn tại các số tự nhiên $a_1<a_2<...<a_n<a_0$ thỏa mãn $a_0^3=a_1^3+a_2^3+...+a_n^3$. Vì vậy

$$\left(6a_0\right)^3=\left(3a_1\right)^3+\left(4a_1\right)^3+\left(5a_1\right)^3+\left(6a_2\right)^3+\left(6a_3\right)^3+...+\left(6a_n\right)^3$$

và hơn nữa $3a_1 < 4a_1 < 5a_1 < 6a_2 < \ldots < 6a_n$ suy ra bổ đề đúng với $n+2$. Vậy nếu bổ đề đúng với số tự nhiên n thì nó đúng với $n+2$. Kết hợp với nhận xét ở trên suy ra bổ đề đúng với mọi số tự nhiên $n > 2$. □

Hệ quả. *Định lý 16 đúng với mọi số tự nhiên m, n với $m > 3$, $n > 3$.*

Chứng minh hệ quả. Nếu $m > 3$ và $n > 3$ thì theo bổ đề tồn tại các số tự nhiên $b_1 < b_2 < \ldots < b_{n-1} < a_1$ thỏa mãn $a_1^3 = b_1^3 + b_2^3 + \ldots + b_{n-1}^3$ và các số $a_2 < a_3 < \ldots < a_m < b_n$ thỏa mãn $a_2^3 + a_3^3 + \ldots + a_m^3 = b_n^3$. Hơn nữa có thể giả sử $a_2 > a_1$ vì nếu không ta có thể thay các số $a_2, a_3, \ldots, a_m, b_n$ bởi tích của chúng với $a_1 + 1$. Do đó các số $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n$ là phân biệt. Cộng các đẳng thức theo vế suy ra $a_1^3 + a_2^3 + \ldots + a_m^3 = b_1^3 + b_2^3 + \ldots + b_n^3$. Đây là điều cần chứng minh trong Định lý 16. Hệ quả được chứng minh. □

Để chứng minh Định lý 16 trong trường hợp tổng quát chỉ cần kiểm tra hai trường hợp $m = 2$ và $m = 3$ và $n \geq m$. Nếu $m = 2$, $n = 2, 3, 4, 5$ thì Định lý 16 suy ra từ công thức

$$9^3 + 10^3 = 1^3 + 11^3, \quad 7^3 + 8^3 = 1^3 + 5^3 + 9^3,$$

$$6^3 + 36^3 = 4^3 + 5^3 + 27^3 + 30^3, \; 26^3 + 28^3 = 2^3 + 3^3 + 4^3 + 5^3 + 34^3.$$

Nếu $m = 2$ và $n > 5$ thì theo bổ đề tồn tại các số tự nhiên $b_1 < b_2 < \ldots < b_{n-3} < a_1$ thỏa mãn $a_1^3 = b_1^3 + b_2^3 + \ldots + b_{n-3}^3$ suy ra

$$a_1^3 + (6a_1)^3 = (3a_1^3) + (4a_1)^3 + (5a_1)^3 + b_1^3 + b_2^3 + \ldots + b_{n-3}^3$$

mà $a_1 < 3a_1 < 4a_1 < 5a_1 < 6a_1$ suy ra định lý đúng với n và m. Nếu $m = 3, n = 3, 4$ thì Định lý 16 suy ra từ công thức $1^3 + 12^3 + 15^3 = 2^3 + 10^3 + 16^3$, $12^3 + 13^3 + 14^3 = 3^3 + 9^3 + 10^3 + 17^3$. Nếu $m = 3, n > 4$ thì theo bổ đề tồn tại các số tự nhiên $b_1 < b_2 < .. < b_{n-2} < a_1$ mà $a_1^3 = b_1^3 + b_2^3 + \ldots + b_{n-2}^3$ suy ra

$$a_1^3 + (2a_1)^3 + (16a_1)^3 = (9a_1)^3 + (15a_1)^3 + b_1^3 + b_2^3 + \ldots + b_{n-2}^3$$

và do đó vì $a_1 < 2a_1 < 9a_1 < 15a_1 < 16a_1$ suy ra Định lý 16 đúng với m, n.

Định lý được chứng minh hoàn toàn. □

14. Tổng của các trùng phương

Từ Định lý cuối cùng của Fermat trong trường hợp số mũ 4 (Chương 2 mục 6) ta thấy không có các trùng phương nào là tổng của hai trùng phương dương. Giả thuyết của Euler nói rằng không có các trùng phương là tổng của ba trùng phương dương.

Tuy nhiên có các trùng phương là tổng của bốn trùng phương chẳng hạn $353^4 = 30^4 + 120^4 + 272^4 + 315^4$, $15^4 = 4^4 + 6^4 + 8^4 + 9^4 + 14^4$, $91^4 = 14^4 + 24^4 + 34^4 + 49^4 + 58^4 + 84^4$.

Định lý 17. *Với mọi số tự nhiên $n > 3$ tồn tại trùng phương là tổng của n trùng phương dương.*

Chứng minh. Ký hiệu S là tập tất cả các số tự nhiên $n > 1$ mà tồn tại trùng phương là tổng của n trùng phương dương. Ta vừa chứng minh 4, 5, 6 thuộc S.

Bây giờ ta chứng minh nếu n, m thuộc S thì $m + n - 1$ cũng thuộc S. Thật vậy nếu m và n thuộc S thì tồn tại các số tự nhiên $a_1 < a_2 < \ldots < a_m < a_0$ và $b_1 < b_2 < \ldots < b_n < b_0$ thỏa mãn $a_0^4 = a_1^4 + a_2^4 + \ldots + a_n^4$, $b_0^4 = b_1^4 + b_2^4 + \ldots + b_n^4$. Vì vậy

$$(a_0 b_0)^4 = (a_1 b_1)^4 + (a_1 b_2)^4 + \ldots + (a_1 b_n)^4 + (a_2 b_0)^4 + (a_3 b_0)^4 + \ldots + (a_m b_0)^4$$

Hơn nữa $a_1 b_1 < a_1 b_2 < \ldots < a_1 b_n < a_2 b_0 < a_3 b_0 < \ldots < a_m b_0$ suy ra $m + n - 1$ thuộc S.

Ta lưu ý nếu tập S chứa 4,5 thì theo tính chất trên suy ra S chứa mọi số tự nhiên ≥ 7. Thật vậy, vì 4,5 thuộc S nên 4+4-1=7, 5+4-1=8, 5+5-1=9 thuộc S, theo quy nạp suy ra nếu m thuộc S thì $m+3k$ với $k=1,2...$ cũng thuộc S (vì $m+3k=m+3(k-1)+4-1$). Hệ quả là S chứa mọi số có dạng $7+3k$, $8+3k$, $9+3k$ với $k=0, 1, 2,...,$ nghĩa là mọi số tự nhiên ≥ 7. Vậy S chứa mọi số tự nhiên >3. Định lý 17 được chứng minh. □

Có một số số tự nhiên có thể biểu diễn thành tổng của hai trùng phương theo hai cách. Chẳng hạn $133^4+134^4=59^4+158^4$. Tuy nhiên ta chưa biết số tự nhiên nào có nhiều hơn hai biểu diễn như vậy (không tính các hoán vị). Đẳng thức sau đây đúng $8^4+9^4+17^4=3^4+13^4+16^4$. Lưu ý rằng đẳng thức sau đây suy ra mọi số hữu tỷ là tổng của bốn trùng phương hữu tỷ:

$$4^4255^4x=\left(8(255+2x)\right)^4-\left(8(255-2x)\right)^4+(32x-255)^4-(32x+255)^4.$$

Có thể chứng minh rằng với mọi số tự nhiên $n\geq 4$ thì luôn tồn tại lũy thừa bậc 5 là tổng các lũy thừa bậc 5 của n số tự nhiên khác nhau. Chẳng hạn (Lander và Parkin [2] và A.S.Bang [1])

$$144^5=27^5+84^5+110^5+133^5, 12^5=4^5+5^5+6^5+7^5+9^5+11^5,$$
$$92^5=2^5+9^5+11^5+22^5+51^5+58^5+89^5, 32^5=3^5+6^5+7^5+8^5$$
$$+10^5+11^5+13^5+14^5+15^5+16^5+18^5+31^5$$

P.Erdos đã chứng minh với mọi số tự nhiên m thì luôn tồn tại số tự nhiên k_m mà với mọi số tự nhiên $n>k_m$ thì đều tồn tại số tự nhiên $l_{n,m}$ thỏa mãn mọi số tự nhiên lớn hơn $l_{n,m}$ đều là tổng của n số phân biệt mà mỗi số là lũy thừa dương bậc m.

15. Định lý Waring

Năm 1770 Waring đã đặt ra định lý sau mà không kèm theo chứng minh: *với mọi lũy thừa s tồn tại số tự nhiên k mà mọi số tự nhiên n là tổng của k lũy thừa không âm bậc s.*

Định lý này được chứng minh bởi D.Hilbert năm 1909. Chứng minh sơ cấp của định lý Waring được trình bày bởi Yu.V.Linnik [2] và dựa trên ý tưởng của L.Schnirelman. Chứng minh này có trong cuốn sách của A.Ya.Khinchin [1]. Với $s=1$ định lý Waring hiển nhiên đúng. Nếu $s=2$ Định lý 4 (Lagrange) cho khẳng định với $k=4$. Với $s=3$ Waring nhận xét rằng có thể chọn k bằng 9, nghĩa là mọi số tự nhiên đều là tổng của 9 (hoặc ít hơn) các lập phương dương. Mãi tới năm 1909 A.Wieferich mới chứng minh điều này là đúng. Với $s=4$ Waring chỉ ra rằng $k=19$. Kết quả này được chứng minh gần đây (theo cách không sơ cấp) bởi R.Balasubramanian, F.Dress và J.M.Deshonilles [1]. Ta sẽ trình bày chứng minh sơ cấp rằng k có thể chọn là 50 (xem Định lý 18).

Với mọi số tự nhiên s ký hiệu $g(s)$ là số tự nhiên nhỏ nhất k mà mọi số tự nhiên đều là tổng của k (hoặc ít hơn) các lũy thừa bậc s. Khi đó định lý Waring nói rằng với mọi số tự nhiên s thì số tự nhiên $g(s)$ tồn tại. Ta chứng minh

(45) $$(s)\geq 2^s+\left[\left(\frac{3}{2}\right)^s\right]-2, \qquad s=1,2,...$$

Đặt

(46) $$n=2^s\left[\left(\frac{3}{2}\right)^s\right]-1.$$

Rõ ràng n là số tự nhiên và vì $[x]\leq x$ ta có

(47) $$n<3^s.$$

Từ định nghĩa của $g(s)$ suy ra tồn tại các số nguyên không âm x_i ($i=1,2,...,g(s)$) thỏa mãn

(48) $$n=x_1^s+x_2^s+...+x_{g(s)}^s.$$

Theo ***(47)*** thì mọi số $x_i\left(i=1,2,\ldots,\mathfrak{g}(s)\right)$ phải nhỏ hơn 3. Do đó các số x_i chỉ nhận các giá trị 0, 1, 2. Giả sử trong các số đó có k số 2, l số 1 và r số 0. Khi đó k, l, r là các số nguyên không âm và

(49) $$\mathfrak{g}(s)=k+l+r\geq k+l$$

Với

(50) $$n=2^s k+l.$$

Vì vậy $n\geq 2^s k,$ và theo công thức ***(46)*** thì $n<2^s\left[\left(\frac{3}{2}\right)^s\right]$ ta nhận được $k<\left[\left(\frac{3}{2}\right)^s\right]$ nghĩa là

(51) $$k\leq\left[\left(\frac{3}{2}\right)^s\right]-1.$$

Từ ***(50)*** ta có $l=n-2^s k$ và do đó

(52) $$k+l=k+n-2^s k=n-\left(2^s-1\right)k.$$

Vì s là số tự nhiên nên 2^s-1 cũng là số tự nhiên. Nhân ***(51)*** với số này suy ra $\left(2^s-1\right)k\leq\left(2^s-1\right)\left(\left[\left(\frac{3}{2}\right)^s\right]-1\right)$. Vì vậy từ ***(49)***,***(52)*** và ***(46)*** ta có

$$g(s)\geqslant k+l\geqslant n-(2^s-1)\left(\left[\left(\tfrac{3}{2}\right)^s\right]-1\right)=2^s+\left[\left(\tfrac{3}{2}\right)^s\right]-2,$$

suy ra ***(45)***. Nếu $s=2$ từ ***(45)*** suy ra $\mathfrak{g}(2)\geq 2^2+\left[\frac{9}{4}\right]-2=4+2-2$ và do đó $\mathfrak{g}(2)\geq 4$. Nhưng ta đã biết $\mathfrak{g}(2)=4$ và nếu $s=3$ thì từ ***(45)*** suy ra $\mathfrak{g}(s)\geq 2^3+\left[\frac{27}{8}\right]-2=9$.

Tồn tại các số tự nhiên (chẳng hạn 23) không thể biểu diễn thành tổng của 8 lập phương không âm. Như đã đề cập ở trên, Wieferich đã chứng minh $\mathfrak{g}(3)=9$.

Nếu $s=4$ thì ***(45)*** suy ra $\mathfrak{g}(4)\geq 2^4+\left[\frac{81}{16}\right]-2=19$.

Theo ***(46)*** thì tồn tại số các tự nhiên (ví dụ 79) không thể biểu diễn thành tổng của 18 trùng phương không âm. Blasubramanian, Dress và Deshonilles đã chứng minh $\mathfrak{g}(4)=19$.

Nếu $s=5,$ từ ***(45)*** suy ra $\mathfrak{g}(5)\geq 37$. J.R.Chen [1] đã chứng minh $\mathfrak{g}(5)=37$.

l.E.Dickson [4],[5] (xem Pillai [3]) đã chứng minh công thức $\mathfrak{g}(s)=2^s+\left[\left(\frac{3}{2}\right)^s\right]-2$ đúng với $6\leq s\leq 400$ (thật ra điều này cũng đúng với $s\leq 5$). K.Mahler [1] đã chứng minh công thức trên là đúng với mọi số đủ lớn s và R.M.Stemmler [1] đã kiểm tra với $400<s\leq 200000$.

Với mọi số tự nhiên s ký hiệu $G(s)$ là số tự nhiên nhỏ nhất k mà mọi số tự nhiên đủ lớn (nghĩa là tất cả các số trừ ra nhiều nhất là hữu hạn trường hợp) đều biểu diễn được thành tổng của k lũy thừa không âm bậc s. Ta đã chứng minh được $G(2)=4, G(3)\leq 7, G(4)=16, G(5)\leq 21, G(6)\leq 31$ (Davenport [1] và Vaughan [1],[2]). Bất đẳng thức $G(3)\leq 7$ được chứng minh bởi Yu.V.Linnik [1] năm 1942 và được làm đơn giản hơn bởi G.L.Waton [1], xem thêm McCurley [1].

Bây giờ ta trình bày phương pháp sơ cấp chứng minh $\mathfrak{g}(4) \le 50$.

Đầu tiên cần nhắc lại đẳng thức được E.Lucas tìm ra năm 1876 dưới đây

$$(53)\quad 6(x_1^2+x_2^2+x_3^2+x_4^2)^2 = (x_1+x_2)^4+(x_1-x_2)^4+(x_1+x_3)^4+$$
$$+(x_1-x_3)^4+(x_1+x_4)^4+(x_1-x_4)^4+$$
$$+(x_2+x_3)^4+(x_2-x_3)^4+(x_2+x_4)^4+$$
$$+(x_2-x_4)^4+(x_3+x_4)^4+(x_3-x_4)^4.$$

Với mọi số tự nhiên n chia hết cho 6, nghĩa là $n=6m$ với m là số tự nhiên, thì theo Định lý 4 ta có $m=a^2+b^2+c^2+d^2$ với a,b,c,d là các số nguyên không âm. Vì vậy $n=6a^2+6b^2+6c^2+6d^2$. Nhưng theo Định lý 4 thì tồn tại các số nguyên không âm x_1,x_2,x_3,x_4 mà $a=x_1^2+x_2^2+x_3^2+x_4^2$. Vì vậy theo ***(53)*** ta có $6a^2=a_1^4+a_2^4+\ldots+a_{12}^4$ với $a_i\,(i=1,2,\ldots,12)$ là các số nguyên không âm. Ta biểu diễn các số $6b^2,6c^2,6d^2$ dưới dạng tương tự thành tổng của 12 trùng phương. Từ đây suy ra $n=6m$ là tổng của 48 trùng phương. Do đó ta đã chứng minh được mọi số tự nhiên chia hết cho 6 đều là tổng của 48 trùng phương. Mọi số tự nhiên không lớn hơn 95 đều có dạng 2^4k+r với $0\le k\le 5,\ 0\le r\le 15$ và do đó là tổng của 20 trùng phương. Giả sử số tự nhiên n lớn hơn 95. Khi đó $n=6m+r$ với $m>15$ và $0\le r\le 5$. Các số $m,m-2,m-13$ dương và do đó với $r=0, 1, 2, \ldots, 5$ ta có $n=6m$, $n=6m+1^4$, $n=6m+1^4+1^4, n=6(m-13)+3^4, n=6(m-2)+2^4, n=6(m-2)+1^4+2^4$ tương ứng. Vì vậy mọi số tự nhiên đều là tổng của 50 trùng phương. Điều phải chứng minh.

Định lý 18. *Mọi số tự nhiên đều là tổng của 50 trùng phương.*

Sử dụng định lý Gauss có thể chứng minh $\mathfrak{g}\le 30$ (Dress [1]). Với mọi số tự nhiên s ký hiệu $v(s)$ là số tự nhiên nhỏ nhất k mà mọi số tự nhiên là tổng của k lũy thừa bậc s các số nguyên. Dễ thấy $v(2)=3$ và $4\le v(3)\le 5$ tuy nhiên ta không biết $v(3)$ bằng 4 hay 5. Có thể chứng minh $9\le v(4)\le 10, 5\le v(5)10$. Bây giờ ta chứng minh với mọi số tự nhiên s thì $v(s)$ tồn tại. Ta có đẳng thức P.Tardy [1] (xem Dickson [7] tập 2 trang 723, 728)

$$\sum_{\alpha_1,\alpha_2,\ldots,\alpha_s} (-1)^{\alpha_1+\alpha_2+\ldots+\alpha_s}((-1)^{\alpha_1}x_1+(-1)^{\alpha_2}x_2+\ldots+(-1)^{\alpha_s}x_s)^s$$
$$= s!2^s x_1 x_2 \ldots x_s,$$

Với s là số tự nhiên và tổng ở vế trái lấy trên 2^s dãy $\alpha_1,\alpha_2,\ldots,\alpha_s$ các phần tử nhận giá trị 0 và 1. Vì vậy với $x_1=x_2=\ldots=x_s=1$ suy ra mọi số nguyên chia hết cho $s!2^s$ đều là tổng của 2^s lũy thừa bậc s. Mặt khác vì mọi số nguyên đều có dạng $2!2^sk\pm r$ với k,r là các số nguyên và $0\le r\le s!2^{s-1}$ nên mọi số nguyên đều là tổng của $2^s+s!2^{s-1}$ lũy thừa bậc s. Ta có $v(s)\le 2^s+s!2^{s-1}$ với mọi $s=1, 2,\ldots$

CHƯƠNG 12

MỘT SỐ BÀI TOÁN CỦA LÝ THUYẾT CỘNG TÍNH CỦA CÁC SỐ

1. Phân hoạch dạng tổng

Leibmiz, Bernoulli và sau đó là Euler là những người đầu tiên nghiên cứu bài toán tính số g_n tất cả các biểu diễn số tự nhiên n cho trước thành tổng của các số tự nhiên không tăng. Bài toán này được biết đến với tên gọi là bài toán phân hoạch dạng tổng. Sau đây là 10 giá trị đầu tiên của hàm số g: $g_1=1$, $g_2=2$, $g_3=3$, $g_4=5$, $g_5=7$, $g_6=11$, $g_7=15$, $g_8=22$, $g_9=30$, $g_{10}=42$. Mac Mahon đã tính được $g_{100}=1905692292$, $g_{200}=3972999029388$. Có thể chứng minh g_n chính là hệ số của khai triển dạng chuỗi $\prod_{n=1}^{\infty}\frac{1}{1-x^n}=1+\sum_{n=1}^{\infty}g_n x^n$ với $|x|<1$.

Ký hiệu h_n là số các biểu diễn của n thành tổng của dãy tăng các số tự nhiên. Khí đó với $|x|<1$, $\prod_{n=1}^{\infty}\left(1+x^n\right)=1+\sum_{n=1}^{\infty}h_n x^n$. Các số g_n ($n=1,2,\ldots$) thỏa mãn công thức truy hồi

$$ng_n=\sigma(n)+g_1\sigma(n-1)+g_2\sigma(n-2)+\ldots+g_{n-1}\sigma(1)$$

Từ công thức này ta xây dựng được quy tắc để tính các số g_n (Vahlen [1]). Sau đây là 10 giá trị đầu tiên của hàm h_n: $h_1=1$, $h_2=1$, $h_3=2$, $h_4=2$, $h_5=3$, $h_6=4$, h_7 =5, $h_8=6$, $h_9=8$, $h_{10}=10$.

Ký hiệu k_n là số tất cả các phép phân tích n thành tổng của các số tự nhiên mà hai phân tích được coi là khác nhau ngay cả khi chúng chỉ sai khác thứ tự các hạng tử. Bằng quy nạp ta chứng minh được $k_n=2^{n-1}$ với $n=1, 2, \ldots$ Đặc biệt số 4 có 8 cách phân tích khác nhau thành tổng của các số tự nhiên. Đó là $4=3+1=1+3=2+2=2+1+1+1=1+2+1=1+1+2=1+1+1+1$.

Cuối cùng ký hiệu l_n là số cách phân tích số tự nhiên n thành tổng các số lẻ không tăng. Với $|x|<1$ ta có $\prod_{n=1}^{\infty}\frac{1}{1-x^{2n-1}}=1+\sum_{n=1}^{\infty}l_n x^n$. Ta có $l_n=h_n$ với mọi $n=1, 2, \ldots$

Ký hiệu q_n là hàm (với đối số là số tự nhiên n) xác định bởi số cách phân hoạch tập hợp n phần tử thành các tập không rỗng rời nhau, hai phân hoạch khác nhau chỉ khi các tập con trong phân hoạch đó không tương ứng bằng nhau. Các giá trị đầu tiên của hàm số này là $q_1=1, q_2=2$, $q_3=5, q_4=15, q_5=52$. Ta có công thức tính q_n là $e^{e^x-1}=\sum_{n=1}^{\infty}q_n x^m/n!$. (Whitworth [1] trang 88).

Ta cũng có (Rota [1]) $q_{n+1}=1+\sum_{k=1}^{n}\binom{n}{k}q_{k.}$.

Ta tính số cách khác nhau để biểu diễn một số nguyên thành tổng của các đồng dư khác nhau modulo m trong dãy 1,2,..., $m-1$. Các biểu diễn cũng được tính theo đồng dư modulo m. M.A.Stern [1] đã chứng minh rằng nếu p là số nguyên tố lẻ thì với mọi đồng dư modulo p có đúng $\left(2^{p-1}-1\right)/p$ biểu diễn như vậy với các hạng tử là 1,2,..., $p-1$. Ví dụ với $p=5$ ta có

$$0\equiv 1+4\equiv 2+3\equiv 1+2+3+4\pmod 5,$$
$$1\equiv 1\equiv 2+4\equiv 1+2+3\pmod 5,$$
$$2\equiv 2\equiv 3+4\equiv 1+2+4\pmod 5,$$
$$3\equiv 3\equiv 1+2\equiv 1+3+4\pmod 5,$$
$$4\equiv 4\equiv 1+3=2+3+4\pmod 5.$$

2. Biểu diễn thành tổng của n hạng tử không âm

Ta sẽ chứng minh rằng nếu n và k là hai số tự nhiên cho trước thì số $F_{n,k}$ tất cả các cách biểu diễn k thành tổng của n số nguyên không âm mà hai biểu diễn là khác nhau ngay cả khi thứ tự các hạng tử là khác nhau là $\binom{n+k-1}{k}$. Thật vậy ta có $F_{1,k}=1=\binom{k}{k}$.

Giả sử với n là số tự nhiên thì công thức $F_{n,k}=\binom{n+k-1}{k}$ đúng với mọi $k=1,\ 2,\ldots.$. Khi đó ta có

$$F_{n+1,k}=F_{n,k}+F_{n,k-1}+F_{\ n,k-2}+\ldots+F_{n,1}+1$$
$$=\binom{n+k-1}{k}+\binom{n+k-2}{k-1}+\binom{n+k-3}{n-2}+\ldots.+\binom{n}{1}+1.$$

Ta lại có $\binom{n+k}{k}=\binom{n+k-1}{k}+\binom{n+k-1}{k-1}$.

Suy ra $\binom{n+k}{k}=\binom{n+k-1}{k}+\binom{n+k-2}{k-1}+\ldots+\binom{n}{1}+\binom{n}{0}$.

Từ đó $F_{n+1,k}=\binom{n+k}{k}$, suy ra công thức $F_{n,k}=\binom{n+k-1}{k}$ (với $k=1,\ 2,\ldots$) đúng với mọi n.

Một cách chứng minh khác là như sau: với mỗi phân tích $k=a_1+a_2+\ldots+a_n$ của số tự nhiên k thành tổng của n số nguyên không âm ta xét dãy các số $l_i=a_1+a_2+\ldots+a_i+i$ với $i=1,2,\ldots,n-1$. Rõ ràng dãy này chứa các số tự nhiên tăng mà mỗi số đều không vượt quá $n+k-1$. Số các dãy như vậy đúng bằng $\binom{n+k-1}{n-1}=\binom{n+k-1}{k}$.

T.Skolem [3] đã xét bài toán trong đó số tự nhiên n thỏa mãn tính chất: tập các số 1, 2, ..., $2n$ có thể chia thành n cặp $(a_i,\ b_i)(i=1,2,\ldots,n)$ mà $b_i-a_i=i$ với mọi $i=1,2,\ldots,\ n$. Nếu n có tính chất này thì $\sum_{i=1}^{n}b_i-\sum_{i=1}^{n}a_i=1+2+\ldots+n=n(n+1)/2$. Nhưng do các số $a_1,\ b_1,\ a_2,b_2,\ldots,a_n,b_n$ đúng bằng với các số $1,2,\ldots,2n$ nên $\sum_{i=1}^{n}a_i+\sum_{i=1}^{n}b_i=1+2+\ldots+2n=n(2n+1)$. Vì vậy $\sum_{i=1}^{n}b_i=\frac{1}{4}n(5n+3)$ nhưng đây không phải số nguyên vì n đồng dư với 2 hoặc 3 (mod4). Ngược lại T.Skolem đã chứng minh (O.Keefe [1]) nếu n đồng dư với 0 hoặc 1 (mod 4) thì phân tích ở trên là tồn tại. Ví dụ với $n=4$ thì các cặp đó là (6,7), (1,3), (2, 5), (4, 8). Nếu $n=5$ thì các cặp là (2,3), (6,8), (7,10), (1,5), (4,9).

3. Ma phương

Hình vuông chứa các số 1, 2, ... , n^2 trong các ô riêng biệt mà tổng các số trong hàng ngang, cột dọc, đường chéo đều bằng nhau được gọi là ma phương bậc n. Dễ dàng tính ra giá trị chung này là $\frac{1}{2}n(n^2+1)$. Trường hợp $n=1$ là tầm thường. Với $n=2$ thì không tồn tại ma phương tương ứng. Với $n=3$ ta có ma phương

8	1	6
3	5	7
4	9	2

Với $n=4$ ta có các ma phương

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

10	5	11	8
3	16	2	13
6	9	7	12
15	4	14	1

1	15	10	8
14	4	5	11
7	9	16	2
12	6	3	13

4	10	15	5
7	13	12	2
14	8	1	11
9	3	6	16

14	1	12	7
11	8	13	2
5	10	3	16
4	15	6	2

2	13	8	11
12	7	14	1
15	4	9	6
5	10	3	16

Dưới đây là các ví dụ về ma phương với cấp $n=5,6,7$

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	8	25	2	9

1	35	4	33	32	6
25	11	9	28	8	30
24	14	18	16	17	22
13	23	19	21	20	15
12	26	27	10	29	7
36	2	34	3	5	31

30	39	48	1	10	19	28
38	47	7	9	18	27	29
46	6	8	17	26	35	37
5	14	16	25	34	36	45
13	15	24	33	42	44	4
21	23	32	41	43	3	12
22	31	40	49	2	11	20

Tồn tại duy nhất (sai khác một phép quay và phản xạ gương một ma phương) với $n=3$. Frenicle đã chỉ ra 880 ma phương với $n=4$. Tồn tại ma phương cấp tùy ý $n\geq 3$ (Bieberbach [1]). Chứng minh sau đây thuộc về A.Makowski [8]. Đầu tiên ta chứng minh rằng từ hai ma phương Q_n và Q_m với bậc n và m lần lượt thì ta có thể nhận được một ma phương Q_{nm} bậc nm. Thật vậy, ta chỉ cần thay các ô chứa phần tử i của ma phương Q_m bằng ma phương nhận được từ việc cộng thêm $n^2(i-1)$ vào tất cả các ô trong ma phương Q_n. Khi đó ta thu được ma phương bậc mn với tổng các hàng, cột và đường chéo của Q_{nm} đều bằng $\frac{1}{2}mn\left(n^2+1\right)+\frac{1}{2}n^3m\left(m^2-1\right)$. Từ chứng minh này ta cũng có ngay một phương pháp xây dựng các ma phương bậc 3^k, $k=1, 2,\ldots,$ từ ma phương bậc 3.

Ma phương bậc lẻ được gọi là hoàn hảo nếu tổng của hai số trong hai ô đối xứng với nhau qua ô trung tâm đúng bằng hai lần số trong ô trung tâm. Mọi ma phương bậc 3 là hoàn hảo (số ở ô trung tâm bằng 5). Tuy nhiên tồn tại ma phương bậc 5 mà không hoàn hảo. Stifel đã chỉ ra một ví dụ như thế. Dưới đây là một ma phương hoàn hảo bậc 5

11	4	17	10	23
24	12	5	18	6
7	25	13	1	19
20	8	21	14	2
3	16	9	22	15

Ma phương bậc 7 trình bày ở trên là hoàn hảo.

Có các ma phương chứa n^2 số nguyên phân biệt nhưng không phải 1, 2, ..., n^2. Ví dụ

18	2	13
6	11	16
9	20	4

43	1	67
61	37	13
7	73	31

17	13	2	8
1	9	16	14
18	12	3	7
4	6	19	1

Một ví dụ tổng quát hơn là với $s > 18$ ta có ma phương

$s-3$	1	$s-6$	8
$s-7$	9	$s-4$	2
6	$s-8$	3	$s-1$
4	$s-2$	7	$s-9$

$s > 18$

Ma phương (hiểu theo nghĩa rộng) có thể chỉ chứa các số nguyên tố phân biệt.

Ví dụ (xem Moessner [2] và [3])

569	59	449
239	359	479
269	659	149

17	317	397	67
307	157	107	227
127	277	257	137
347	47	37	367

A.Makowski đã nhận xét rằng nếu các phần tử của cấp số cộng $a+b, 2a+b,\ldots,n^2a+b$ đều là số nguyên tố thì thay các số i bởi các số $ia+b$ trong hình vuông chứa các số $1,2,\ldots, n^2$ ta nhận được ma phương (theo nghĩa rộng) chỉ chứa các số nguyên tố. Từ giả thuyết H suy ra tính tồn tại của x mà tất cả các số $x+1, 2x+1,\ldots,n^2x+1$ đều nguyên tố. Vì vậy từ giả thuyết H có thể suy ra tính tồn tại của ma phương bậc b với mọi $n > 2$ mà chỉ chứa các số nguyên tố.

A.Moessner đã xây dựng ma phương bậc 8 chỉ chứa các số tam giác $t_0,\ldots.,t_{63}$. Ma phương này có tổng các hàng ngang, cột dọc và đường chéo đúng bằng số tam giác t_{104} (Moessner [1]).

Ma phương (theo nghĩa rộng) gọi là cận ma phương nếu nó tạo thành bởi các số $s, s+1,\ldots,s+n^2$. Rõ ràng các ma phương như vậy sẽ trở thành ma phương theo nghĩa thông thường nếu tất cả các số cùng được trừ đi $s-1$. L. Bieberbach [1] đã thông báo vào năm 1544 Michael Stifel đã đưa ra nhận xét rằng cận ma phương khi bỏ đi hàng đầu tiên, hàng dưới cùng, cột đầu tiên và cột cuối cùng thì vẫn là cận ma phương. Có thể chứng minh tồn tại các ma phương như vậy với số hàng lớn hơn 4 tùy ý. Đây là ví dụ của Stifel

5	6	23	24	7
22	12	17	10	4
18	11	13	15	8
1	16	9	14	25
19	20	3	2	21

Ma phương này (theo nghĩa thông thường) được tạo thành từ các số 1, 2, … , 25. Sau khi bỏ đi hàng đầu tiên, hàng dưới cùng, cột đầu tiên và cột cuối cùng ta nhận được cận ma phương tạo thành bởi 9, 10, ... , 17.

Ta cũng nghiên cứu các hình vuông được tạo thành bởi các số tự nhiên mà tích của các số trong mỗi hàng, mỗi cột và đường chéo đều bằng nhau. Dưới đây là một số hình vuông như vậy (Goodstein [1]):

2	256	8
64	16	4
32	1	128

6	36	8
16	12	9
18	4	24

24	81	24
36	36	36
54	16	54

Quá trình phát triển lý thuyết về các ma phương tính tới thế kỷ 20 được tổng kết trong P.Bachmann [1]. Rất nhiều phương pháp xây dựng ma phương khác đã được trình bày trong Postnikov [1].

4. Định lý Schur và các hệ quả

Bổ đề. *Nếu* k *là số tự nhiên,* $N=[ek!]$ *nếu* $a_0<a_1<a_2<\ldots<a_N$ *là dãy các số nguyên và nếu tập hợp các hiệu* a_j-a_i *với* $0\le i<j\le N$ *được chia thành* k *lớp rời nhau thì tồn tại ít nhất một lớp chứa các hiệu* $a_m-a_l, a_n-a_l, a_n-a_m$ *với* l, m, n *nào đó thỏa mãn* $0\le l<m<n<N$.

Chứng minh. Giả sử phản chứng tồn tại số tự nhiên k mà bổ đề không đúng. Đặt K_1 là lớp chứa nhiều nhất các hiệu có dạng a_j-a_0 trong đó $0<j\le N$ và đặt $a_{j_1}-a_0$, $a_{j_2}-a_0,\ldots, a_{j_{k_1-a_0}}$ là các phần tử của lớp K_1 được sắp xếp theo độ lớn. Khi đó ta có $N\le k_1k$. Theo giả thiết thì k_1-1 hiệu

(1) $$a_{j_2}-a_{j_1} \qquad a_{j_3}-a_{j1}, \quad \ldots, \quad a_{j_{k_1}}-a_{j_1}$$

không thuộc lớp K_1. Do đó chúng thuộc $k-1$ lớp còn lại.

Ký hiệu K_2 là lớp chứa nhiều nhất các số k_2 các hiệu trong ***(1)***. Giả sử K_2 chứa các hiệu

(2) $$a_{j_\alpha}-a_{j_1}, \qquad a_{j_\beta}-a_{j_1}, \qquad a_{j_\gamma}-a_{j_1},\ldots,$$

trong đó $\alpha<\beta<\gamma<\ldots$. Rõ ràng $k_1-1\le k_2(k-1)$.

Nếu số đầu tiên trong ***(2)*** là hiệu của cặp nào đó trong k_2-1 số còn lại thì ta có các hiệu

(3) $$a_{j_\beta}-a_{j_\alpha}, \quad a_{j_\gamma}-a_{j_\alpha}, \quad \ldots,$$

không thuộc K_1 và K_2. Suy ra chúng thuộc $k-2$ lớp còn lại. Ký hiệu K_3 là lớp chứa nhiều nhất k_3 các số trong ***(3)***. Ta có $k_2-1\le k_3(k-2)$. Tiếp tục như vậy cho tới khi ta nhận được dãy các số tự nhiên $k_1, k_2,\ldots, k_s$ với $s\le k$ và

(4) $$k-1\le k_{i+1}(k-i) \quad \text{với} \quad i=1, 2, \ldots, s-1,$$

trong đó $k_s=1$ vì nếu $k_s>1$ thì lập luận ở trên tiếp tục và ta thu được k_{s+1}. Theo ***(4)*** suy ra

$$\frac{k_i}{(k-i)!}\le\frac{k_{i+1}}{(k-i-1)!}+\frac{1}{(k-i)!}, \qquad i=1, 2, \ldots, s-1$$

Cộng các bất đẳng thức theo vế ta có $\dfrac{k_1}{(k-1)!}\le\dfrac{1}{(k-1)!}+\dfrac{1}{(k-2)!}+\ldots+\dfrac{1}{(k-s)!}<e-\dfrac{1}{k!}$.

Vì vậy $N \le k_1 k < ek!-1$, mâu thuẫn với định nghĩa của N. Bổ đề được chứng minh. □

Định lý 1 (I.Schur [1], Leveque [2] tập 1 trang 60). *Giả sử với số tự nhiên k thì các số 1, 2, ..., $[ek!]$ được chia thành k lớp. Khi đó tồn tại ít nhất một lớp chứa hai phần tử của dãy và chứa cả hiệu của chúng.*

Chứng minh. Trong bổ đề đặt $a_i = i,\ i = 1, 2, ..., [ek!]$ và lưu ý rằng giữa các số 1, 2, .., $[ek!]$ tất cả các hiệu $a_j - a_i$ với $0 \le i \le j \le [ek!]$ đều xuất hiện ít nhất một lần và hơn nữa $a_n - a_m = (a_n - a_1) - (a_m - a_1)$. Suy ra định lý được chứng minh. □

Liên quan tới Định lý 1 có một câu hỏi được đặt ra như sau: *cho trước một số tự nhiên k, tìm số tự nhiên nhỏ nhất $N = N(k)$ có tính chất giống như số $[ek!]$, nghĩa là nếu tập hợp 1, 2,..., N được chia thành k lớp thì ít nhất một lớp chứa hai phần tử và cả hiệu của chúng.*

Từ Định lý 1 suy ra rằng $N(k) \le [ek!]$ vì vậy $N(1) \le 2$, $N(2) \le 5$, $N(3) \le 6$. Mặt khác, rõ ràng $N(1) \ne 1$ nên $N(1) = 2$. Do các số 1, 2, 3, 4 có thể chia thành hai lớp là 1, 4 và 2, 3, mà cả hai lớp đều không chứa hiệu các phần tử của chúng suy ra $N(2) > 4$ do đó $N(2) = 5$.

I.Schur, đã chứng minh $N(k+1) \ge 3N(k) - 1$ (xem bài tập 1). Vì vậy $n(k) \ge (3^k + 1)/2$, đẳng thức xảy ra chỉ trong các trường hợp $k = 1, 2, 3.$ L.D.Baumert [1] đã chứng minh $N(4) = 45$.

Gần đây ước lượng Schur đã được làm chặt hơn. E.G.Whitehead [1] đã chứng minh $N(k) \le \left[k!\left(e - \frac{1}{24}\right)\right]$, H.L.Abbott và D.Hanson [1] đã chứng minh

(5) $$N(n+m) \ge (2N(m) - 1)N(n) - N(m) + 1.$$

H.Fredericksen [1] đã chứng minh $N(5) \ge 158$ suy ra từ đẳng thức ***(5)*** với $m = 5$ ta có

(6) $$N(k) \ge 1 + 315^{(k-1)/5}, \quad k = 1, 2, 3, ...$$

Định lý 2. *Đặt $0 < a_0 < a_1 < ... < a_N$ là dãy các số nguyên với $N = [ek!]$. Nếu dãy này không chứa cấp số cộng với ít nhất ba phần tử thì mọi phân hoạch của tập hợp 1, 2, ..., a_N thành k lớp có tính chất ít nhất một lớp chứa hai số khác nhau và hiệu của chúng.*

Chứng minh được suy ra từ bổ đề và ba lưu ý sau đây

1) *Trong các số 1, 2,... a_N chứa tất cả các hiệu $a_j - a_i$ với $0 \le i < j \le N$*

2) $a_n - a_l = (a_n - a_m) + (a_m - a_l)$,

3) $a_n - a_m \ne a_m - a_l$ *do các số này không tạo thành cấp số cộng.*

Hệ quả 1. *Nếu k là số tự nhiên, $n \ge 2^{[ek!]}$ và tập hợp các số 1, 2,.., n được chia thành k lớp thì ít nhất một lớp chứa hai số khác nhau và tổng của chúng.*

Để chứng minh hệ quả chỉ cần xét $a_i = 2^i, i = 0, 1, 2, ..., [ek!]$ và áp dụng Định lý 2 với chú ý rằng dãy $2^i\ (i = 0, 1, 2, ...)$ không chứa bất kỳ cấp số cộng 3 phần tử nào. Hệ quả của hệ quả 1 là

Hệ quả 2. *Nếu tập tất cả các số tự nhiên được chia thành hữu hạn lớp thì ít nhất một trong các lớp đó chứa hai số tự nhiên khác nhau và tổng của chúng (xem Rado [1]).*

Hệ quả 1 được phát triển tiếp bởi R.W.Irving [1]. Khi đó $2^{[ek!]}$ có thể thay bằng $\left[\frac{1}{2}ek!(2k+1)\right]+2$.

Liên quan tới Định lý 2 ta có câu hỏi sau đây: *cho trước số tự nhiên k, tìm số nhỏ nhất $n=n(k)$ có tính chất nếu các số 1, 2,..., n được chia thành k lớp thì ít nhất một lớp chứa các số khác nhau và tổng của chúng*. Rõ ràng ta có $n(1)=3$. Có thể chứng minh $n(2)=9$. Bất đẳng thức $n(2)\ge 9$ được suy ra từ việc dãy các số 1, 2, ... ,8 có thể chia thành hai lớp $A=\{1, 2, 4, 8\}$ và $B=\{3, 5, 6, 7\}$ mà không có lớp nào chứa tổng của hai số chứa trong nó. Từ đó để chứng minh $n(2)=9$ ta chỉ cần chỉ ra nếu tập 1, 2, ... ,9 được chia thành hai lớp thì ít nhất một trong chúng chứa hai phần tử và tổng của chúng. Chứng minh tính chất này có trong Sierpinski [26] trang 427-428.

Ta có $n(3)\ge 24$. Thật vậy, dãy 1, 2, ... ,23 có thể chia thành ba lớp A, B, C mà không có lớp nào chứa tổng của hai phần tử chứa trong nó. Thật vậy ta có $A=\{1, 2, 4, 8, 11, 22\}$, $B=\{3, 5, 6, 7, 19, 21, 23\}$, $C=\{9, 10, 12, 13, 14, 15, 16, 17, 18, 20\}$.

Mặt khác G.W.Walker [1] đã thông báo rằng $n(3)=24$, $n(4)=67$, $n(5)=197$ nhưng không kèm theo chứng minh chi tiết. Trong tài liệu đó cũng đưa ra bát đẳng thức $2n(k)<n(k+1)\le 3n(k)$ với mọi $k=1, 2,...$ Một phần của bất đẳng thức này được chứng minh trong bài tập 2 và phần còn lại thì không đúng theo hệ quả của bất đẳng thức ***(6)*** ở trên.

Một bài toán khác có liên quan tới chủ đề này là: *cho trước số tự nhiên N, tìm số lớn nhất $r=r(N)$ mà tồn tại dãy $a_1, a_2, ..., a_r$ các số tự nhiên $\le N$ và không chứa cấp số cộng nào có ba phần tử (dãy $a_1, a_2, ..., a_r$ gọi là dãy loại A cấp N).*

Dễ dàng có $r(1)=1$, $r(2)=r(3)=2$, $r(4)=3$, $r(5)=r(6)=r(7)=4$.

P.Erdos và P.Turan [1] đã chứng minh $r(8)=4$, $r(9)=r(10)=5$, $r(11)=r(12)=6$, $r(13)=7$, $r(14)=r(15)=r(16)=r(17)=r(18)=r(19)=8$, $r(21)=r(22)=r(23)=9$ và chỉ ra $r(20)=8$, nhưng điều này không đúng vì A.Makowski [2] đã chứng minh $r(20)=9$.

G.Szekeres đã đặt ra giả thuyết $r\left(\frac{1}{2}(3^k+1)\right)=2^k$ với mọi $k=0, 1, 2,...$. Tuy nhiên giả thuyết này không đúng vì F.Behrend [1] đã chứng minh $r(N)>N^{1-c/\sqrt{\log N}}$ với c là hằng số (Salem và Spencer [1],[2], Moser [3]). S.S.Wagstaff, Jr [1] đã tính $r(n)$ với $n\le 53$ và tìm được
$r(24)=r(25)=10$, $r(26)=...=r(29)=11$, $r(30)=r(31)=12$, $r(32)=...=r(35)=13$,
$r(36)=...=r(39)=14$, $r(40)=15$, $r(41)=...=r(50)=16$, $r(51)=r(52)=r(53)=17$.

Mặt khác K.F.Roth [1] đã chứng minh với C thích hợp ta có $r(n)<C-\frac{n}{\log\log n}$, vì vậy $\lim\limits_{n\to\infty}\frac{r(n)}{n}=0$. Kết quả cuối cùng của Roth và kết quả của Behrend lần lượt được mở rộng cho dãy không chứa cấp số cộng k phần tử bởi Szemeredi [1] và R. A. Rankin [1].

Bài tập. ***1.*** Chứng minh từ Định lý Schur có thể suy ra rằng $N(k+1)\ge 3N(k)-1$.

Chứng minh. Từ định nghĩa của $N(k)$ suy ra tập hợp các số 1, 2,..., $N(k)-1$ có thể chia thành k lớp mà không có lớp nào chứa hiệu của hai phần tử chứa trong nó. Đặt $K_i=\left\{x_1^{(i)},\ x_2^{(i)},\ ...,\ x_{s_i}^{(i)}\right\}$ $(i=1,2,...,k)$ và $L_i=\left\{3x_1^{(1)}-1, 3x_1^{(i)}-1, 3x_2^{(i)},..., 3x_{s_i}^{(i)}, 1, 3x_{s_i}^{(i)}\right\}, i=1,2,...,k$

$$L_{k+1}=\left\{1,\ 4,\ 7,\ ...,\ 3N(k)-2\right\}.$$

Dễ thấy tất cả các lớp $L_i\left(i=1,2,...,k+1\right)$ đều không chứa hiệu của hai phần tử nào đó chứa trong chúng và tất cả các lớp $L_i\left(i=1,\ 2,\ ...,\ k+1\right)$ chứa toàn bộ các số tự nhiên 1, 2, ..., $3N(k)-2$. Từ định nghĩa của $N(k+1)$ suy ra $N(k+1)>3N(k)-2$ và do đó $N(k+1)\geq 3N(k)-1$. □

2. Chứng minh rằng $n(k+1)\geq 2n(k)+1.$

Chứng minh. Từ định nghĩa của $n(k)$ suy ra các số 1, 2, ..., $n(k)-1$ có thể chia thành k lớp mà không lớp nào chứa tổng của hai phần tử chứa trong chúng. Đối với các lớp nào ta bổ sung một lớp khác chứa các số $n(k)$, $n(k)+1$, $n(k)+2$,..., $2n(k)$. Khi đó ta nhận được phân hoạch của tập các số 1, 2, ..., $2n(k)$ thành $k+1$ lớp có tính chất như trên. Từ định nghĩa của $n(k+1)$ suy ra $n(k+1)\geq 2n(k)+1$. □

Ghi chú. A.Makowski [3] đã chứng minh bất đẳng thức mạnh hơn $n(k+1)\geq 2n(k)+\frac{1}{2}k(k+1)+1.$

3. Chứng minh rằng $r(m+n)\leq r(m)+r(n)$ (Erdos và Turan).

Chứng minh được suy ra từ nhận xét rằng nếu $a_1<a_2<...<a_r$ là các dãy A cấp N thì $a_1-k,...a_r-k$ cũng là dãy A cấp N với mọi $k<a_1$. □

4. Chứng minh rằng $r(2n)\leq n$ với $n\geq 8$ (Erdos và Turan).

Chứng minh quy nạp theo n suy ra từ công thức $r(2.8)=8$, $r(2.9)<9$, $r(2.10)<10$, $r(2.11)<11$ và nếu $r(2n)\leq n$ thì $r(2(n+4))=r(2n+8)\leq r(2n)+r(8)\leq n+4$. □

5. Chứng minh rằng nếu $n\geq m$ thì $r(2n+m-1)\geq r(m)+r(n)$.

Kết quả này suy ra từ việc nếu $a_1<a_2...<a_{r(n)}$ là dãy A cấp n và $b_1<b_2<...<b_{r(m)}$ là dãy A cấp m thì với $n\geq m$, $a_1<a_2<...<a_{r(n)}<2a_{r(n)}+b_1-1<2a_{r(n)}+b_2-1<...<a_{r(n)}<2a_{r(n)}+b_{r(m)}-1$ là dãy A cấp $2n+m-1$ chứa $r(n)+r(m)$ phần tử. □

6. Chứng minh rằng $r\left(\frac{1}{2}\left(3^k+1\right)\right)\geq 2^k$ (Erdos và Turan).

Chứng minh. Chứng minh quy nạp. Ta có $r\left(\frac{1}{2}\left(3^0+1\right)\right)=r(1)-1=2^0$ và nếu $r\left(\frac{1}{2}\left(3^k+1\right)\right)\geq 2^k$ thì theo bài tập 5 ta có

$$r\left(\frac{1}{2}\left(3^{k+1}+1\right)\right)=r\left(2\left(\frac{1}{2}\left(3^k+1\right)\right)+\frac{1}{2}\left(3^k+1\right)-1\right)$$

$$\geq r\left(\frac{1}{2}\left(3^k+1\right)\right)+r\left(\frac{1}{2}\left(3^k+1\right)\right)\geq 2^{k+1}$$

7. Chứng minh rằng $r(51) \geq 17$.

Chứng minh. Chứng minh suy trực tiếp từ nhận xét của S.Maslowski rằng dãy 1, 2, 5, 6, 12, 14, 15, 17, 21, 35, 38, 39, 42, 44, 47, 48, 51 không chứa cấp số cộng ba phần tử nào. □

M.Hall Jr. [2] đã chứng minh sự tồn tại của tập Z các số tự nhiên phân biệt mà mọi số tự nhiên là hiệu của đúng một cặp trong tập Z. Ta sẽ xây dựng dãy vô hạn các số tự nhiên Z có tính chất như vậy (Browkin [2]). Đặt $a_1 = 1, a_2 = 2$. Hơn nữa ký hiệu n là số tự nhiên và giả sử các số $a_1, a_2, ..., a_{2n}$ đã xác định. Đặt $a_{2n+1} = 2a_{2n}$. Giả sử r_n là số tự nhiên nhỏ nhất không biểu diễn được dưới dạng $a_j - a_i$ với $1 \leq i < j \leq 2n+1$. Ta xác định a_{2n+2} như là $a_{2n+1} + r_n$. Ta thấy dãy $a_1, a_2, ...$ được định nghĩa bằng quy nạp. Bảy phần tử đầu tiên là 1, 2, 4, 8, 16, 21, 42. Từ định nghĩa của r_n suy ra các số 1, 2, ..., r_n đều có dạng $a_j - a_i$ với $1 \leq i < j \leq 2n+2$. Vì vậy $r_{n+1} > r_n$ với mọi $n = 1, 2, ...$ Do đó mọi số tự nhiên có thể biểu diễn dưới dạng $a_j - a_i$ với các chỉ số i, j thích hợp.

Để hoàn thiện chứng minh ta chỉ cần chỉ ra rằng với mọi số tự nhiên h, k, l, m với $h < k$ và $l < m, k < m$ thì $a_k - a_h \neq a_m - a_l$. Giả sử ngược lại $a_k - a_h = a_m - a_l$. Do $m > k > h \geq 1$ ta có $m \geq 3$. Nếu m lẻ nghĩa là $m = 2n+1$ với n là số tự nhiên thì $a_{2n+1} < a_l + a_k \leq 2a_{m-1} = 2a_{2n} = a_{2n+1}$, vô lý. Nếu m chẵn nghĩa là $m = 2n+2$ trong đó n là số tự nhiên thì nếu $l = 2n+1$ ta có $a_m - a_l = a_{2n+2} - a_{2n+1} = r_n$ mà do $a_k - a_h = a_m - a_l$ suy ra $r_n = a_k - a_h$ trong đó $h < k \leq m-1 = 2n+1$, mâu thuẫn với định nghĩa của r_n. Nếu $l < 2n+1$ (vì $l < m$ nên giá trí $l = 2n+1$ bị loại bỏ) với $k = 2n+1$ ta có $a_m - a_k = a_l - a_h$ suy ra vì $k < m$, ta có $h < l \leq 2n$ và $a_m - a_k = a_{2n+2} - a_{2n+1} = r_n$ do đó $r_n = a_l - a_h$ với $h < l \leq 2n$, mâu thuẫn với định nghĩa của r_n. Cuối cùng nếu $l < 2n+1$ và $k < 2n+1$ thì $a_{2n+2} = a_m = a_l + a_k - a_h < a_l + a_k < a_{2n} + a_{2n} = a_{2n+1}$, vô lý.

Vậy ta thấy dãy $a_1, a_2, ...$ có tính chất yêu cầu.

Sử dụng tiên đề chọn thì tính chất tương tự có thể chứng minh cho các số thực. Nghĩa là tồn tại tập hợp X các số thực mà mọi số thực dương có thể biểu diễn duy nhất dưới dạng hiệu hai phần tử của X (Picard [1], Lindenbaum [1]).

5. Các số lẻ không có dạng $2^k + p$ với p nguyên tố

Năm 1849 A.de Polignac [1] đặt ra giả thuyết rằng mọi số lẻ $n > 1$ đều có dạng $2^k + p$ với k là số tự nhiên và p là số nguyên tố hoặc là 1. Năm Erdos [10] đã chứng minh tồn tại vô hạn số lẻ mà giả thuyết sai (Van de Corput [3]).

Định lý 3 (Erdos [10]). *Tồn tại cấp số cộng vô hạn các số lẻ không có dạng $2^k + p$, $k = 0,1,2,$ p nguyên tố.*

Bổ đề. *Mọi số tự nhiên đều thỏa mãn ít nhất một trong sáu đồng dư thức sau*

$(1)\ k \equiv 0 \pmod 2$, $(2)\ k \equiv 0 \pmod 3$, $(3)\ k \equiv 1 \pmod 4$,

$(4)\ k \equiv 3 \pmod 8$, $(5)\ k \equiv 7 \pmod{12}$, $(6)\ k = 23 \pmod{24}$.

Chứng minh bổ đề. Nếu k không thỏa mãn ***(1)*** hoặc ***(2)*** thì nó không chia hết cho 2 và 3, do đó nó có dạng $24t + r$ với t là số nguyên và r là một trong các số 1, 5, 7, 11, 13, 17, 19, 23. Thử trực tiếp ta thấy k thỏa mãn ***(3), (3), (5), (4), (3), (3), (4), (6)*** tương ứng.

Hệ quả. Nếu k là số nguyên không âm thì ít nhất một trong các đồng dư thức sau đúng

$(7)\ 2^k = 1 \pmod 3$, $(8)\ 2^k = 1 \pmod 7$

$(9)\ 2^k = 2 \pmod 5$, $(10)\ 2^k = 2^3 \pmod{17}$

$(11)\ 2^k = 2^7 \pmod{13}$, $(12)\ 2^k = 2^{23} \pmod{241}$.

Chứng minh hệ quả. Kiểm tra trực tiếp ta nhận thấy $2^2 \equiv 1 \pmod 3, 2^3 \equiv 1 \pmod 7, 2^4 \equiv 1 \pmod 5$, $2^8 \equiv 1 \pmod{17}$, $2^{12} \equiv 1 \pmod{13}$, $2^{12} \equiv -1 \pmod{241}$ suy ra $2^{24} \equiv 1 \pmod{241}$. Từ đây suy ra các đồng dư thức ***(1), (2), (3), (4), (5), (6)*** suy ra ***(7), (8), (9), (10), (11), (12)*** tương ứng.

Chứng minh định lý. Từ định lý số dư Trung Hoa suy ra tồn tại số tự nhiên a thỏa mãn các đồng dư thức $a \equiv 1 \pmod 2, a \equiv 1 \pmod 3$, $a \equiv 1 \pmod 7, a \equiv 2 \pmod 5, a \equiv 2^3 \pmod{17}, a \equiv 2^7 \pmod{13}$, $a \equiv 2^{23} \pmod{241}$, $a \equiv 3 \pmod{31}$ và hơn nữa tồn tại cấp số cộng vô hạn các phần tử a mà mỗi số đều thỏa mãn các đồng dư thức này. Rõ ràng các phần tử của cấp số cộng này là lẻ. Nếu a là phần tử bất kỳ của cấp số cộng thì nó thỏa mãn các đồng dư thức. Từ hệ quả của bổ đề suy ra số $a - 2^k$ chia hết cho ít nhất một trong các số nguyên tố 3, 7, 5, 17, 13, 241. Mặt khác $a \equiv 3 \pmod{31}$ và với mọi $k = 1, 2, \ldots$ số 2^k đồng dư với một trong các số 1, 2, 4, 8, 16 (mod 31) bởi vì $2^5 = 1 \pmod{31}$ suy ra $a - 2^k$ đồng dư với một trong các số 2, 1, -1, -5, -13(mod31). Nhưng không có số nào đồng dư (mod 31) với các số 3, 7, 5, 17, 13, 241. Vì vậy số $a - 2^k$ không phải một trong các số đó, nhưng mặt khác nó chia hết cho ít nhất một trong các số đó. Vì vậy nó là hợp số. Do đó $a - 2^k$ không phải số nguyên tố với mọi số nguyên không âm k suy ra a không có dạng $a = 2^k + p$, trong đó $k = 0, 1, 2, \ldots,$ và p là số nguyên tố. Vậy ta thấy các phần tử của cấp số cộng định nghĩa ở trên có tính chất cần thiết. Định lý 3 được chứng minh. □

Chứng minh của Định lý 3 suy ra tồn tại vô hạn số tự nhiên n mà với mọi số nguyên không âm k thì số $-n - 2^k$ (và vì vậy cả số $n + 2^k$) đều chia hết cho ít nhất một trong các số 3, 7, 5, 17, 13, 241.

Ký hiệu P là tích của các số nguyên tố như vậy. Như trên ta đã chứng minh số $n + 2^{k[\varphi(P)-1]}$ có ước số nguyên tố $p \mid P$. Nhưng $2^{k\varphi(P)} \equiv 1 \pmod P$ mà $n + 2^{2[\varphi(P)-1]} \equiv 0 \pmod p$ suy ra $n.2^k + 1 = 0 \pmod p$ với n đủ lớn (ví dụ $n > 241$) từ đó ta có hợp số $n.2^k + 1$. Ta có hệ quả sau

Hệ quả. *Tồn tại vô hạn số tự nhiên n mà các số $n.2^k + 1$ với $k = 0, 1, 2, \ldots,$ đều là hợp số (xem Sierpinski [28] và Chương 10 mục 4 bài tập 3).*

Định lý 4 (R.Crocker). *Tồn tại vô hạn số tự nhiên không thể biểu diễn thành tổng của hai lũy thừa bậc nguyên không âm khác nhau của 2 và một số nguyên tố.*

Chứng minh. Ta chứng minh các số $2^{2^n} - 1$, $n = 3, 4, \ldots$ có tính chất như vậy.

Thật vậy giả sử với số tự nhiên $n > 2$ ta có $2^{2^n} - 1 = 2^k + 2^l + p$ với k, l là các số nguyên và $k > l \geq 0$. Không thể xảy ra trường hợp $l = 0$ vì nếu ngược lại ta sẽ có $p = 2^{2^n} - 2^k - 2$ $= 2\left(2^{2^n - 1} - 2^{k-1} - 1\right)$ và do $2^n > k$, $k - 1 \leq 2^n - 2$ suy ra $2^{2n-1} - 2^{k-1} \geq 2^{2n-1} - 2^{2n-2} = 2^{2^n - 2} \geq 2^{2^3 - 2} = 2^6$

như vậy $2^{2^n - 1} - 2^{k-1} \geq 2^6 - 1 > 1$, mâu thuẫn với việc p là số nguyên tố. Vậy $l \geq 1$ và do đó $k > 1$.

Ký hiệu h là lũy thừa không âm lớn nhất mà 2^h là ước số của $k - l$.

Số $(k - l)/2^h$ lẻ và $2^{2^h} + 1 \mid 2^{k-l} + 1$. Do $p = 2^{2n} - 2^k - 2^l - 1 = 2^{2^n} - 1 - 2^l\left(2^{k-l} + 1\right)$ suy ra $2^{2^h + 1} \mid p$ mà p nguyên tố nên $p = 2^{2^h} + 1$. Khi đó $2^{2^n} = 2^k + 2^l + 2^{2^h + 2}$. Do $2^n > k > 1$ suy ra số $2^l + 2^{2^k} + 2$ chia hết cho 4. Vì vậy $l = 1$ hoặc $2^h = 1$. Nếu $2^h = 1$ thì $l > 1$ và do đó $2^{2n-2} = 2^{k-2} + 2^{l-2} + 1$, vô lý vì vế trái chia hết cho 2^6. Vậy $l = 1, 2^h > 1$ do đó $2^{2^n - 2} = 2^{k-2} + 2^{2h-2} + 1$ mà $2^n - 2 \geq 6$ suy ra có đúng một trong hai khả năng $k = 2$ và $2^h = 2$ xảy ra. Nếu $k = 2$ thì $2^h \mid k - l = 1$ vô lý vì $2^h > 1$, nếu $2^h = 2$ thì $k \geq 3$ và $2^{2^n - 3} = 2^{k-3} + 1$, mà $n \geq 3$ suy ra $k = 3$. Do đó $n = 2$, vô lý.

Vậy các số $2^{2^n}-1$ có tính chất cần thiết. □

Hệ quả (Crocker [1]). *Không có số nào trong các số* $2^{2^n}-5$ *với n =3, 4, 5..., có dạng* 2^k+p *với k = 0, 1, 2, ... và* p *là số nguyên tố.*

Chứng minh. Nếu $2^{2^n}-5=2^k+p$ với k là số nguyên không âm và p là số nguyên tố thì $2^{2^n}-1=2^k+2^2+p$ với $n\geq 3$ suy ra k phải bằng 2 hệ quả là $2^{2^n}-1=2^3+p$ và do đó $p=2^{2^n}-9=\left(2^{2^n-1}-3\right)\left(2^{2n+1}+3\right)$ suy ra $2^{2^n-1}-3=1$ mâu thuẫn với giả thiết $n\geq 3$. □

Với những lập luận tương tự trong chứng minh Định lý 4, R.Crocker [2] đã chứng minh được sự tồn tại vô hạn các số tự nhiên lẻ không thể biểu diễn được thành tổng các lũy thừa của 2 (không cần phân biệt) và một số nguyên tố.

CHƯƠNG 13

SỐ NGUYÊN PHỨC

1. Chuẩn của số nguyên phức. Các số liên kết

Số nguyên phức (hoặc số nguyên Gauss) là các số phức $a+bi$ với a, b là các số nguyên. Lý thuyết về các số nguyên phức là quan trọng vì mấy lý do. Thứ nhất là vì số nguyên phức là một dạng tổng quát của các số nguyên thông thường, do đó sẽ rất có ích khi tìm hiểu xem các tính chất nào của các số nguyên là không mở rộng được cho lớp rộng hơn. Thứ hai là từ việc tìm hiểu tính chất của các số nguyên phức ta có thể trực tiếp suy ra một số tính chất của các số nguyên thông thường. Các tính chất như vậy thường gặp rất nhiều khó khăn để có thể chứng minh theo cách khác.

Các phép cộng, trừ, nhân của các số nguyên phức được sử dụng giống hệt như các phép toán số học tương ứng của các số phức.

Bài tập. ***1.*** Tìm tất cả các biểu diễn của 0 thành tổng bình phương hai số nguyên phức.

Lời giải. Ta có $0=\left(a+bi\right)^2+\left(\pm b\mp ai\right)^2$ với a, b là các số nguyên tùy ý. □

2. Tìm số nguyên phức $x+yi$ là tổng của hai bình phương các số nguyên phức.

Lời giải. Số nguyên phức $x+yi$ là tổng hai bình phương các số nguyên phức khi và chỉ khi y chẵn và nếu x có dạng $4t+2$ thì y chia hết cho 4. Điều kiện cần được suy ra vì nếu $x+yi=(a+bi)^2+(c+di)^2$ thì $x=a^2-b^2+c^2-d^2$, $y=2(ab+cd)$. Vì vậy nếu x có dạng $4t+2$ thì ít nhất một trong các số a và b và ít nhất một trong các số c và d là chẵn. Nhưng khi đó $ab+cd$ chẵn suy ra y chia hết cho 4.

Điều kiện đủ được suy ra vì nếu $x=2t+1$ và $y=2u$ thì $x+yi=\left(t+1+ui\right)^2+\left(u-ti\right)^2$. Nếu $x=4t+2$ và $y=4u$ thì $x+yi=\left(t+u+1+\left(u-t\right)i\right)^2+\left(t-u+1+\left(t+u\right)i\right)^2$. Nếu $x=4t$ và $y=4u$ thì $x+yi=\left(t+1+ui\right)^2+\left(u+\left(1-t\right)i\right)^2$, cuối cùng nếu $x=4t$ và $y=4u+2$ thì

$$x+yi=\left(t+u+1+\left(u+1-t\right)i\right)^2+\left(t-u+\left(t+u\right)i\right)^2.$$

3. Chứng minh rằng số nguyên phức $x+yi$ là tổng của ba bình phương các số nguyên phức khi và chỉ khi y chẵn.

Gợi ý. Sử dụng bài tập 2 và đẳng thức $4t+2+2ui=4t+1+2ui+1^2$.

4. Chứng minh rằng số nguyên phức $a+bi\neq 0$ là bình phương một số nguyên phức khi và chỉ khi $a^2+b^2=c^2$, $c+a=2x^2$ và $c-a=2y^2$ với c là số tự nhiên và x, y là các số nguyên. Chứng minh rằng khi đó $a+bi=\left(\pm x\pm yi\right)^2$, với các dấu dương nếu $b>0$ và âm nếu $b<0$.

Ghi chú. Định lý trong bài tập 4 có thể xác định như là một phép thử để quyết định xem một số nguyên phức cho trước có là bình phương một số nguyên phức nào đó hay không. Đồng thời định lý cũng cho biết một phương pháp để tính căn bậc hai của một số nguyên phức (nếu tồn tại).

Với số nguyên phức $z=a+bi$ ký hiệu z' là số nguyên phức liên hợp của nó, nghĩa là $z'=a+bi$.

Từ định nghĩa các phép toán số học cho các số nguyên phức ta có

(1) nếu $z=t+u$ thì $z'=t'+u'$,
(2) nếu $z=t-u$ thì $z'=t'-u'$,
(3) nếu $z=tu$ thì $z'=t'u'$.

Rõ ràng các số z và z' cùng là số nguyên phức hoặc cùng không phải. Số $(z')'$ liên hợp với z' chính là z.

Tích zz' của hai số liên hợp gọi là chuẩn của z và ký hiệu là $N(z)$. Ta có $N(x)=zz'$ do đó nếu $z=a+bi$ (với a, b là các số thực) thì $N(z)=a^2+b^2$ suy ra chuẩn của số nguyên phức luôn là số thực không âm và bằng 0 chỉ khi $a=b=0$, nghĩa là $z=0$. Hơn nữa chuẩn của một số nguyên phức khác 0 là số tự nhiên. Các số liên hợp có cùng chuẩn.

Ta nói số nguyên phức z chia hết cho số phức t nếu tồn tại số nguyên phức u thỏa mãn

(4) $z=tu.$

Khi đó ta viết $t \mid z$.

Để tính xem khi nào thì số nguyên phức $a+bi$ chia hết cho số phức $c+di$ khác 0 thì ta biến đổi

$$\frac{a+bi}{c+di}=\frac{(a+bi)(c-di)}{c^2+d^2}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i$$

Suy ra $c+di \mid a+bi$ khi và chỉ khi $c^2+d^2 \mid ac+bd$ và $c^2+d^2 \mid bc-ad$.

Chẳng hạn $3+5i \mid 21+i$ vì $34 \mid 68$ và $34 \mid -102$, $1+i \mid 2$ vì $2 \mid 2$ và $2 \mid -2$. Mặt khác $1-2i \nmid 1+2i$ vì $5 \nmid -3$

Từ ***(3)*** suy ra nếu $t \mid z$ thì $t' \mid z'$ và nếu $z=tu$ thì $zz'=tut'u'=tt'uu'$, suy ra theo định nghĩa của chuẩn các số nguyên phức ta có

(5) $N(z)=N(t)N(u).$

Vậy chuẩn của tích hai số nguyên phức là tích các chuẩn của các số đó.

Định lý này đúng với tích hữu hạn các số nguyên phức.

Theo ***(5)*** ta có $N(t) \mid N(z)$ và do đó nếu số nguyên phức t là ước số của z, thì chuẩn của t là ước số của chuẩn của z. Điều ngược lại không đúng, chẳng hạn $N(1-2i)=N(1+2i)$ but $1-2i \nmid 1+2i$.

Hai số nguyên phức khác 0 mà là ước số của nhau thì được gọi là các số liên kết.

Nghĩa là *z* và *t* là các số liên kết khi và chỉ khi *t|z* và *z|t*. Khi đó ta có *N(t)|N(z)* và *N(z)|N(t)* mà vì chuẩn của các số nguyên phức khác 0 là khác 0 nên *N(t) = N(z).*

Vậy hai số nguyên phức liên kết thì luôn có cùng chuẩn. Điều ngược lại không đúng, chẳng hạn các số $1-2i$ và $1+2i$ có cùng chuẩn nhưng không phải các số liên kết vì $1-2i \mid 1+2i$.

Bây giờ ta tìm tất cả các số liên kết với số nguyên phức *z≠0* cho trước.

Giả sử *t* là số liên kết với *z* thì với số nguyên phức *u* nào đó ta có *t = zu* và suy ra

(6) *N(t) = N(z) N(u)*

Nhưng do các số liên kết thì có cùng chuẩn nên $N(z)=N(t)$ và $N(z)\neq 0$ vì $z\neq 0$ do đó từ ***(6)*** suy ra $N(u)=1$. Đặt $u=a+bi$ suy ra *a² + b² = 1.* Do đó *a = ± 1* và *b = 0* hoặc *a = 0* và *b = ± 1*. Từ đây suy ra *u* là một trong bốn số *1, -1, i, -i* và do đó *t = zu* là một trong bốn số

(7) *z, -z, iz, -iz.*

Vậy mọi số liên kết của *z* là một trong các số trong ***(7)***. Ngược lại, dễ thấy các số trong ***(7)*** là liên kết với *z*. Vì *z = (-1)(-z) = (-i)iz = i(-iz).* Ta có định lý

Định lý 1. *Mọi số nguyên phức z khác* 0 *có đúng bốn số liên kết là các số trong* ***(7)****.*

Rõ ràng bốn số liên kết này là phân biệt (vì *z ≠ 0*).

Trong các bài toán liên quan tới tính chia hết của các số nguyên phức thì các số liên kết có thể thay thế cho nhau vì nếu *z* chia hết cho *t* thì mọi số liên kết của *z* chia hết cho mọi số liên kết của *t.*

Rõ ràng nếu *z* liên kết với *t* thì *z'* liên kết với *t'.*

Nếu hai số nguyên phức z_1 và z_2 đều chia hết cho t thì tổng và hiệu của chúng cũng chia hết cho t bởi vì nếu $z_1 = tu$ và $z_2 = tv$ thì $z_1 \pm z_2 = t(u \pm v)$.

Nếu số nguyên phức z chia hết cho t và t chia hết cho u thì z chia hết cho u. Thật vậy, nếu $z = tw$ và $t = uv$ thì $z = uvw$.

Do đó nếu t là ước số chung của các số nguyên phức $z_1, z_2, \ldots, z_n$ và nếu $u_1, u_2, \ldots, u_n$ là các số nguyên phức bất kỳ thì $t \mid z_1u_1 + z_2u_2 + \ldots + z_nu_n$.

2. Thuật toán Euclid và ước số chung lớn nhất của các số nguyên phức

Bây giờ ta chứng minh

Định lý 1. *Nếu z và $t \neq 0$ là các số nguyên phức thì tồn tại các số nguyên phức c và r thỏa mãn*

(8) $$z = ct + r$$

và

(9) $$N(r) \leq \tfrac{1}{2} N(t)$$

Từ đó suy ra $N(r) \leq N(t)$.

Chứng minh. Đặt

(10) $$z/t = x + yi,$$

với x, y là các số hữu tỷ. Ký hiệu ξ và η là các số nguyên gần x và y nhất. Khi đó

(11) $$x = \xi + x_1, \qquad y = \eta + y_1,$$

với x_1 và y_1 là các số hữu tỷ thỏa mãn

(12) $$|x_1| \leq \frac{1}{2}, \qquad |y_1| = \frac{1}{2},$$

Đặt

(13) $$c = \xi + \eta i, \qquad r = z - ct$$

Rõ ràng c, r là các số nguyên phức và thỏa mãn ***(8)***. Theo ***(10)***, ***(11)***, ***(13)*** ta có

$$r = z - ct = (x + yi)t - (\xi + \eta i)t = (x_1 + y_1 i)t$$

Vì chuẩn của một tích là bằng tích các chuẩn các nhân tử nên theo ***(12)*** thì

$$N(r) = N(x_1 + y_1 i)N(t) = (x_1^2 + y_1^2)N(t), \qquad x_1^2 + y_1^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

suy ra ***(9)*** và đồng thời định lý được chứng minh. □

Định lý vừa chứng minh cho ta một thuật toán tương tự với thuật toán Euclid đối với các số nguyên. Theo đó để tìm ước số chung lớn nhất của hai số nguyên phức cho trước z và $t \neq 0$ thì đầu tiên theo Định lý 2 ta tìm các số c, r. Theo ***(8)*** ta suy ra các số z và t có cùng ước số chung giống như các số t và r. Hơn nữa từ ***(5)*** suy ra $N(r) < N(t)$. Vì vậy ta chỉ cần tìm ước số chung của các số t và r với $N(r) < N(t)$.

Nếu $r = 0$ thì ước số chung của các số z và t chính là các ước số của t.

Nếu $r \neq 0$ thì áp dụng thủ tục trên với các số t, r thay thế cho z, t. Vì vậy để tìm các ước số chung của các số t, r ta tìm các ước số chung của các số r, r_1 với $N(r_1) = N(r)$.

Nếu $r_1 \neq 0$ ta tìm số r_2 và cứ như vậy.

Dãy $r, r_1, r_2, \ldots$ không thể kéo dài vô hạn vì chuẩn các phần tử của dãy là dãy các số tự nhiên giảm nghiêm ngặt. Do đó với n nào đó ta có $r_n = 0$. Khi đó các ước số chung của r_{n-1} và r_{n-2} chính là các ước số của r_n. Vậy ta kết luận rằng tồn tại số nguyên phức Q mà các ước số của nó chính là các ước số chung của các số z và t.

Chứng tỏ hai số nguyên phức khác 0 cho trước có ít nhất một ước số chung chia hết cho mọi ước số chung của chúng. Ta có thể gọi ước số này là ước số chung lớn nhất của hai số nguyên phức.

Bây giờ ta tính số các ước chung lớn nhất của hai số nguyên phức. Ký hiệu d và δ là các ước số chung lớn nhất của các số nguyên phức z, t. Các số d, δ là các số liên kết. Vì vậy theo Định lý 2 ta có

Hệ quả. *Hai số nguyên phức khác* 0 *luôn có đúng 4 ước số chung lớn nhất là các số liên kết.*

Lưu ý rằng các số nguyên cũng có hai ước số chung lớn nhất trái dấu. Ta không phân biệt các ước số sai khác dấu. Tương tự trong trường hợp số nguyên phức ta có thể chỉ xác định một ước số chung lớn nhất sai khác một liên kết. Tùy trường hợp ta sẽ chọn cách gọi thuận tiện nhất.

Ví dụ. ***1.*** Ta tìm ước số chung lớn nhất của $6 - 17i$ và $18 + I$ bằng thuật toán nêu trên. Áp dụng các bước trong thuật toán cho ta các đẳng thức

$$\frac{6-17i}{18+i} = \frac{(6-17i)(18-i)}{18^2+i} = \frac{91-312i}{325} = -i + \frac{91+13i}{325}$$

$6 - 17i = -i(18 + i) + (5 + i)$,

$$\frac{18+i}{5+i} = \frac{(18+i)(5-i)}{5^2-1} = \frac{91-13i}{26} = 3 + \frac{1-i}{2},$$

$18 + i = 3 (5 + i) + 3 - 2i$,

$$\frac{5+i}{3-2i} = \frac{(5+i)(3+2i)}{3^2+2^2} = 1+i$$

Vậy ước số chung lớn nhất của $6 - 17i$ và $18 + I$ là $3 - 2i$ và các số liên kết $-3 + 2i$, $2 + 3i$, $-2 - 3i$.

2. Tính ước số chung lớn nhất của $2 + 3i$ và $2 - 3i$. Ta có

$$\frac{2+3i}{2-3i} = \frac{(2+3i)^2}{2^2+3^2} - \frac{-5+12i}{13} = 1 + \frac{-5-i}{13},$$

$2 + 3i = i(2 - 3i) + i - 1$,

$$\frac{2-3i}{i-1} = \frac{-(2-3i)(i+1)}{2} = \frac{-5+i}{2} = -3 + \frac{1+i}{2},$$

$2 - 3i = -3(i - 1) - 1$

Do đó ước số chung lớn nhất của $2 + 3i$ và $2 - 3i$ là 1 và các số liên kết $- 1$, i và $- i$.

3. Tính ước số chung lớn nhất của các số $31 + i$ và $5 + I$. Ta có

$$\frac{31+i}{5+i} = \frac{(31+i)(5-i)}{5^2-1^2} = \frac{156-21i}{26} = 6-i$$

Do đó ước số chung lớn nhất của $31 + i$ và $5 + i$ là $5 + i$ và các số liên kết $-5 - i$, $-1 + 5i$ và $1 - 5i$.

Dễ thấy các ước số chung lớn nhất có chuẩn lớn nhất trong các ước số. Điều ngược lại cũng đúng. Do đó ước số chung lớn nhất có thể định nghĩa là các ước số chung có chuẩn là lớn nhất có thể. Tuy nhiên không dễ để chứng minh các ước số chung lớn nhất như thế chia hết cho mọi ước số khác.

Lý thuyết về các ước số chung lớn nhất của hai hoặc nhiều hơn các số nguyên phức có thể trình bày dựa vào các dạng tuyến tính như trong trường hợp số nguyên. Thật vậy, giả sử $a_1, a_2, ..., a_m$ là các số nguyên phức khác 0. Ký hiệu Z là tập hợp các số khác 0 có dạng $a_1z_1 + a_2z_2 + ... + a_mz_m$, với $z_1, z_2, ..., z_m$ là các số nguyên phức. Cuối cùng ký hiệu M là tập hợp các giá trị của chuẩn của các số trong Z. Rõ ràng M chỉ chứa các số tự nhiên. Gọi n là số tự nhiên nhỏ nhất trong M. Khi đó tồn tại số ζ trong Z mà $N(\zeta) = n$, nghĩa là tồn tại các số nguyên phức $\zeta_1, \zeta_2, ..., \zeta_m$ mà

(14) $$\zeta = a_1\zeta_1 + a_2\zeta_2 + ... + a_m\zeta_m.$$

Bây giờ ta chứng minh các số trong Z chia hết cho ζ. Thật vậy, giả sử z là số bất kỳ trong Z. Khi đó tồn tại các số nguyên phức $z_1, z_2, ..., z_m$ thỏa mãn

(15) $$z = a_1z_1 + a_2z_2 + ... + a_mz_m.$$

Hơn nữa theo Định lý 2 suy ra tồn tại các số nguyên phức c và r thỏa mãn

(16) $$z = c\zeta + r \text{ và } N(r) < N(\zeta).$$

Nếu $r \neq 0$ thì r thuộc Z vì từ ***(14)***,***(15)*** và ***(12)*** thì

$$r = z - c\zeta = a_1(z_1 - c\zeta_1) + a_2(z_2 - c\zeta_2) + ... + a_m(z_m - c\zeta_m),$$

hơn nữa các số $z_j - c\zeta_j, j = 1, 2, ..., m,$ là các số nguyên phức. Nhưng theo ***(16)*** suy ra r là số có chuẩn nhỏ hơn chuẩn n của ζ, điều này mâu thuẫn với định nghĩa của n. Do đó $r = 0$ và suy ra theo ***(16)*** thì $z = c\zeta$ và do đó $\zeta \mid z$. Rõ ràng các số $a_1, a_2, ..., a_m$ đều thuộc Z. Vì vậy số nguyên phức ζ là ước số chung của các số $a_1, a_2, ..., a_m$.

Giả sử δ là ước số chung tùy ý của các số này. Khi đó tồn tại các số nguyên phức $t_1, t_2, ..., t_m$ thỏa mãn $a_j = t_j\delta$ với mọi $j = 1, 2, ..., m$. Vì vậy theo ***(14)*** thì $\zeta = (t_1\zeta_1 + t_2\zeta_2 + ... + t_m\zeta_m)\delta$, chứng tỏ $\delta \mid \zeta$. Từ đây ta suy ra ζ là ước số chung của các số $a_1, a_2, ..., a_m$ nhận mọi ước số chung khác là ước số của nó. Ta cũng nhận thấy ζ có dạng ***(14)*** với $\zeta_1, \zeta_2, ..., \zeta_m$ là các số nguyên phức.

Hai số nguyên phức bất kỳ a, b luôn có ít nhất bốn ước số chung là I, $-1, i, -i$.

Nếu các số nguyên phức a, b không có nhiều hơn bốn ước số chung thì chúng gọi là các số nguyên tố cùng nhau. Ta viết $(a, b) = 1$.

Dễ dàng thấy rằng tồn tại các số nguyên phức x, y thỏa mãn

(17) $$ax + by = 1.$$

Thật vậy, nếu $(a, b) = 1$ thì ζ xác định bởi ***(14)*** với $a = a_1, b = a_2, m = 2$ sẽ là một trong các số 1, $-1, i, -i$. Do đó một trong các số $\zeta, -\zeta, i\zeta, -i\zeta$ bằng 1 suy ra với lựa chọn phù hợp thì ***(17)*** đúng.

Mặt khác từ ***(17)*** suy ra mọi ước số chung của các số a, b đều là ước số của 1 và do đó a, b không có ước số chung nào khác $1, -1, i, -i$, nghĩa là $(a, b) = 1$.

Định lý 3. *Hai số nguyên phức a, b nguyên tố cùng nhau khi và chỉ khi tồn tại các số nguyên phức x, y mà* $ax + by = 1$.

Bây giờ ta xét ba số nguyên phức a, b, c với $(a, b) = 1$ và $b \mid ac$. Ta chứng minh $b \mid c$.

Thật vậy, vì $(a, b) = 1$ nên theo Định lý 3 thì tồn tại các số nguyên phức x, y thỏa mãn ***(17)***.

Nhân cả hai vế với với c, ta có

(18) $acx+bcy=c$.

Theo giả thiết $b\,|\,ac$ và rõ ràng $b\,|\,bc$ với mọi b suy ra ***(18)*** kéo theo $b\,|\,c$. Điều phải chứng minh.

Định lý 4. *Với mọi số nguyên phức* a,b,c *mà* $(a,b)=1$ *và* $b\,|\,ac$ *thì* $b\,|\,c$.

Hệ quả khác của Định lý 3 là

Định lý 5. *Nếu* $(a,b)=1$ *và* $(a,c)=1$ *thì* $(a,bc)=1$.

Chứng minh. Nếu $(a,b)=1$ *và* $(a,c)=1$ thì tồn tại các số nguyên phức x,y,u,v thỏa mãn $ax+by=1$ và $au+cv=1$. Nhân hai vế ta có $a\big(x(au+cv)+buy\big)+bcyv=1$ suy ra $(a,bc)=1$. □

3. Bội số chung nhỏ nhất của các số nguyên phức

Ký hiệu $a_1,a_2,\ldots,a_m$ là các số nguyên phức khác 0. Khi đó tồn tại bội số chung của các số đó, chẳng hạn ta có thể lấy một bội số chung chính là tích của tất cả các số đó. Trong số các bội số chung này ta chọn số có chuẩn nhỏ nhất, nghĩa là chuẩn của nó không lớn hơn chuẩn của bất kỳ bội số chung nào khác của các số đó. Ký hiệu bội số chung này là v.

Ta sẽ chứng minh rằng mọi bội số chung của $a_1,a_2,\ldots,a_m$ đều chia hết cho v.

Thật vậy, giả sử z là bội số chung tùy ý. Theo Định lý 2 thì tồn tại các số nguyên phức c,r thỏa mãn $z=cv+r$ và $N(r)<N(v)$. Nếu r khác 0 thì r khi đó sẽ là bội số chung của $a_1,a_2,\ldots,a_m$, và có chuẩn nhỏ hơn v, điều này mâu thuẫn với định nghĩa của v. Ngược lại nếu $r=0$ thì tồn tại ít nhất một bội số chung của các số ban đầu chia hết cho nó.

Chuẩn của mọi bội số chung có tính chất này thì không lớn hơn chuẩn của mọi bội số chung khác 0 của các các số $a_1,a_2,\ldots,a_m$. Ta gọi nó là bội số chung nhỏ nhất của các số $a_1,a_2,\ldots,a_m$.

Dễ thấy tất cả các bội số chung nhỏ nhất của $a_1,a_2,\ldots,a_m$ là các số liên kết và chuẩn của chúng là nhỏ nhất trong các chuẩn của các bội số chung khác 0 của các số đó.

Bài tập. Tính nghiệm nguyên phức của phương trình $x+y+z=xyz=1$.

Lời giải. Vì $xyz=1$ nên các số x,y,z là ước số của đơn vị, nghĩa là các số $1,-1,i,-i$. Lại vì $xyz=1$ nên suy ra các số này không cùng thuần ảo, mặt khác vì $x+y+z=1$ nên nếu ba số đó đều là số thực thì có hai số bằng 1 và số còn lại bằng -1, nhưng khi đó thì mâu thuẫn với $xyz=1$. Vì vậy ít nhất một trong các số x,y,z là thuần ảo, nhưng khi đó vì $x+y+z=1$ nên ít nhất hai trong ba số là thuần ảo. Vì vậy ta có thể kết luận một trong các số x,y,z phải bằng i, các số khác là $-i$ và 1. Ta thấy nghiệm duy nhất là $x=1,y=i,z=-i$ và các hoán vị. Có tất cả 6 nghiệm như vậy.

Ghi chú. J.W.S.Cassels [4] đã chứng minh hệ phương trình $x+y+z=xyz=1$ không có nghiệm hữu tỷ (một chứng minh đơn giản khác được cho bởi Sansone và Cassels [1]).

4. Các số nguyên tố phức

Vì mọi số nguyên phức đều có ít nhất bốn ước số là $1,-1,i,-i$ và hơn nữa mọi số nguyên phức z không liên kết với 1 đều có bốn ước số là $z,-z,iz,-iz$ nên suy ra các số nguyên phức này có ít nhất tám ước số.

Các số nguyên phức có đúng tám ước số gọi là các số nguyên tố phức.

Nói cách khác, số nguyên phức là nguyên tố nếu nó không có ước số nào ngoại trừ các số liên kết của nó và các số liên kết của 1 và hơn nữa nó không liên kết với 1.

Rõ ràng định nghĩa này tương đương với: *số nguyên phức là nguyên tố nếu chuẩn của nó lớn hơn 1 và nó không biểu diễn được thành tích của các số nguyên phức với chuẩn lớn hơn 1.*

Thật vậy, nếu ζ là số nguyên phức, $N(\zeta)>1$ và $\zeta=\mu\nu$, với $N(\mu)>1$ và $N(\nu)>1$ thì số μ không thể liên kết với 1 vì nếu như vậy thì $N(\mu)=1$, và nó cũng không liên kết với ζ vì nếu thế thì $N(\mu)=N(\zeta)$, suy ra vì $N(\zeta)=N(\mu)N(\nu)$ ta sẽ có $N(\nu)=1$, mâu thuẫn với giả thiết. Do đó ζ có ước số μ không liên kết với 1 và ζ, do đó nó không phải số nguyên tố.

Mặt khác, nếu ζ là số nguyên phức với $N(\zeta)>1$ và nó không phải số nguyên tố thì theo định nghĩa nó có ước số μ không liên kết với 1 và ζ. Khi đó ta có $\zeta=\mu\nu$ với ν là số nguyên phức.

Nếu $N(\mu)=1$ thì μ liên kết với 1, mâu thuẫn với giả thiết (thật vậy, nếu với số nguyên phức $a+bi$ ta có $N(a+bi)=1$ thì $a^2+b^2=1$ suy ra vì a,b nguyên nên $a=\pm1$ và $b=0$ hoặc $a=0$ và $b=\pm1$).

Nếu $N(\nu)=1$ thì ν liên kết với 1, suy ra vì $\zeta=\mu\nu$, số μ liên kết với ζ, mâu thuẫn.

Hệ quả là $N(\nu)=1$ và $N(\nu)>1$ và do đó ζ là tích của hai số nguyên phức với chuẩn lớn hơn 1.

Rõ ràng *mọi số nguyên phức liên kết hoặc liên hợp với số nguyên tố phức cũng là số nguyên tố phức.*

Định lý 6. *Mọi số nguyên phức với chuẩn lớn hơn 1 đều có thể biểu diễn được thành tích của hữu hạn số nguyên tố phức.*

Chứng minh. Giả sử phản chứng rằng tồn tại số nguyên phức với chuẩn n lớn hơn 1 mà không biểu diễn được thành tích của hữu hạn số nguyên tố phức. Ký hiệu M là tập hợp các giá trị của chuẩn của các số nguyên phức với tính chất này. Khi đó M là tập hợp không rỗng các số tự nhiên.

Ký hiệu m là số nhỏ nhất trong M. Khi đó tồn tại số nguyên phức z với chuẩn m mà không biểu diễn thành tích của hữu hạn số nguyên tố phức. Theo giả thiết z không phải số nguyên tố và chuẩn của nó là $m>1$. Do đó nó là tích của hai số nguyên phức μ và ν với chuẩn lớn hơn 1.

Hơn nữa $m=N(z)=N(\mu\nu)=N(\mu)N(\nu)$, suy ra $N(\mu)<m$ và $N(\nu)<m$. Từ định nghĩa của m suy ra các số μ,ν biểu diễn được thành tích của hữu hạn số nguyên tố phức. Nhưng từ đây lại suy ra số $z=\mu\nu$ cũng có tính chất đó, mâu thuẫn với định nghĩa của z.

Định lý được chứng minh. □

Theo định nghĩa thì mọi số nguyên tố phức π đều có đúng tám ước số $1,-1,i,-i,\pi,-\pi,i\pi,-i\pi$. Do đó nếu một số nguyên phức λ không chia hết cho số nguyên tố phức π thì $(\lambda,\pi)=1$.

Nếu một số tự nhiên nào đó là số nguyên tố phức thì rõ ràng nó cũng là số nguyên tố theo nghĩa thông thường. Điều ngược lại không đúng vì có những số nguyên tố không phải là số nguyên tố phức. Chẳng hạn $2=(1+i)(1-i)$ và $N(1+i)=N(1-i)=2>1$.

Các số $1+i$ và $1-i$ là nguyên tố phức vì nếu $1\pm i=\mu\nu$ thì $N(\mu)N(\nu)=N(\mu\nu)=N(1\pm i)=2$; do đó (lưu ý chuẩn của số nguyên phức là số tự nhiên) ta có $N(\mu)=1$ hoặc $N(\nu)=1$, chứng tỏ μ hoặc ν là liên kết với 1.

Các số $1+i$ và $1-i$ là liên kết vì $1-i=-i(1+i)$. Vì vậy 2 liên kết với căn của một số nguyên phức.

Sử dụng Định lý 4 suy ra biểu diễn của số nguyên phức thành tích của các số nguyên tố phức là duy nhất sai khác hoán vị và các liên kết.

Ta sẽ mô tả các số nguyên tố phức trong tập hợp tất cả các số nguyên tố phức.

Xét các số tự nhiên (cũng là số nguyên phức) là số nguyên tố phức. Rõ ràng các số này đều là số nguyên tố theo nghĩa thông thường và hơn nữa đó là số lẻ vì 2 không phải số nguyên tố phức. Vì vậy ta xét các số nguyên tố có dạng $4k+1$ và $4k+3$ với k là số tự nhiên.

Giả sử p là số nguyên tố có dạng $4k+1$.

Theo Định lý 9 Chương 5 thì tồn tại các số tự nhiên a,b thỏa mãn $p=a^2+b^2$ và suy ra $p=(a+bi)(a-bi)$ và hơn nữa $N(a\pm bi)=a^2+b^2=p>1$. Vậy p không phải số nguyên tố phức.

Các nhân tử $a+bi$ và $a-bi$ là các số nguyên tố phức. Thật vậy, nếu $a+bi=\mu\nu$ với

(19) $$N(\mu)>1 \text{ and } N(\nu)>1,$$

thì $p=N(a+bi)=N(\mu)N(\nu)$, vô lý vì p là số nguyên tố.

Từ đây suy ra các ước số phức của số nguyên tố có dạng $4k+1$ với k là số tự nhiên là các số nguyên tố phức. Rõ ràng các ước số này không liên kết.

Thật vậy, đẳng thức $a+bi=-(a-bi)$ là không thể xảy ra vì nó suy ra $b=0$ và $p=a^2$. Đẳng thức $a+bi=-(a-bi)$ cũng không thể vì nó suy ra $a=0, p=b^2$. Nếu $a+bi=i(a-bi)$ thì $a=b$ và do đó $p=2a^2$, vô lý. Cuối cùng nếu $a+bi=-i(a-bi)$ thì $a=-b$ và do đó $p=2a^2$, vô lý.

Với các số nguyên tố có dạng $4k+3$ với k là số nguyên không âm ta sẽ chứng minh chúng đều là các số nguyên tố phức.

Thật vậy, nếu số nguyên tố $p=4k+3$ là tích của hai số nguyên phức với chuẩn lớn hơn 1 thì $p=(a+bi)(c+di)$, suy ra $p^2=(a^2+b^2)(c^2+d^2)$, với $a^2+b^2>1$ và $c^2+d^2>1$. Vì p là số nguyên tố nên suy ra $p=a^2+b^2$, nhưng điều này không thể có vì p có dạng $4k+3$.

Vậy trong các số nguyên tố thì chỉ có các số có dạng $4k+3$ là số nguyên tố phức. Các số nguyên tố phức khác là $1+i$ và các ước số liên hợp của các ước số phức của các số nguyên tố có dạng $4k+1$.

Ở trên ta đã chứng minh mọi số tự nhiên >1 đều là tích của số nguyên tố phức mà ta vừa liệt kê hoặc các số liên kết của các số đó.

Rõ ràng không còn số nguyên tố phức nào khác vì nếu π là một số như vậy thì vì biểu diễn một số phức thành thành tích của các số nguyên tố phức là duy nhất nên π không phải ước số nguyên tố phức của mọi số tự nhiên. Nhưng $\pi\pi'=N(\pi)$ nên ta có mâu thuẫn.

Vậy ta đã chứng minh được

Định lý 7. *Tất cả các số nguyên tố phức là các số thuộc về ba lớp sau đây và các liên kết của chúng*

1. $1+i$
2. *ước số nguyên tố phức của các số nguyên tố có dạng* $4k+1$
3. *các số nguyên tố có dạng* $4k+3$

Dưới đây là các số nguyên tố phức (không tính các liên kết) với chuẩn nhỏ hơn 100

$$1+i,\quad 1\pm 2i,\quad 3,\quad 2\pm 3i,\quad 1\pm 4i,\quad 2\pm 5i,\quad 1\pm 6i,$$
$$4\pm 5i,\quad 7,\quad 2\pm 7i,\quad 5\pm 6i,\quad 3\pm 8i,\quad 5\pm 8i,\quad 4\pm 9i.$$

Hai số nguyên tố phức với hiệu bằng 2 được gọi là cặp số nguyên tố sinh đôi. Chẳng hạn $4+i, 6+i, 3i, 2+3i, 3+2i, 5+2i, 7i, 2+7i.$ Có các cặp số nguyên tố sinh đôi lập thành cấp số cộng ba phần tử. Chẳng hạn $2+i, 4+i, 6+i$ và $1+2i, 3+2i, 5+2i$.

Từ giả thuyết H (Chương 3 mục 8) suy ra tồn tại vô hạn cặp số nguyên tố phức sinh đôi.

Thật vậy, đặt $f_1(x)=x^2-2x+2,\ f_2(x)=x^2+2x+2$. Các đa thức $f_1(x)$ và $f_2(x)$ không có nghiệm hữu tỷ và do đó bất khả quy. Ta cũng có $f_1(0)\,f_2(0)=4,\ f_1(1)\,f_2(1)=5,$ chứng tỏ điều kiện C được thỏa mãn. Do đó theo giả thuyết H thì tồn tại vô hạn số tự nhiên x thỏa mãn $f_1(x)$ và $f_2(x)$ đều là số nguyên tố. Nhưng $f_1(x)=(x-1)^2+1,\ f_2(x)=(x+1)^2+1$ và x lẻ vì nếu ngược lại thì $2\mid f_2(x)$ và $f_2(x)>2,$ suy ra $f_2(x)$ là hợp số. Hệ quả là các số $f_1(x)$ và $f_2(x)$ đều có dạng $4k+1$ và do đó các số $x-1\pm i$ và $x+1\pm i$ đều là số nguyên tố phức và hiệu của chúng bằng 2. Vì vậy ta nhận được dãy vô hạn các cặp số nguyên tố phức sinh đôi phân biệt. Các cặp đó nhận được với $x=3,5,15,25,55,\ldots$ Tuy nhiên có những cặp số nguyên tố phức sinh đôi không nhận được theo cách này, chẳng hạn $1+2i,3+2i$ hoặc $3+8i$ và $5+8i$.

Các cặp số nguyên tố phức sinh đôi đã được xác định bởi D.Shanks [1].

5. Phân tích của số nguyên phức thành các ước số nguyên tố phức

Ta trình bày phương pháp biểu diễn một số nguyên phức z thành tích của các số nguyên tố phức.

Đặt $N(z)=n$. Mọi ước số nguyên tố của z đều là ước số nguyên tố của chuẩn $n=zz'$. Ước số nguyên tố phức của số tự nhiên n có thể nhận được bằng cách tìm các ước số nguyên tố của số đó.

Thật vậy, đặt

(20) $$n=2^{\alpha}\,p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}q_1^{\beta_1}q_2^{\beta_2}\ldots q_l^{\beta_l},$$

với p_i là các số nguyên tố có dạng $4t+1$ và q_j là các số nguyên tố có dạng $4t+3$. Giả sử π_j và $\pi'_j,\ j=1,2,\ldots,k$, là các ước số nguyên tố phức liên hợp của p_j. Đặt $\pi_j=a+bi$ và $\pi'_j=a-bi$ thì $p_j=a^2+b^2$. Khi đó phân tích của n thành thừa số nguyên tố phức là

(21) $$z=i^{\nu}(1+i)^{\lambda}\,\pi_1^{\lambda_1}\pi'^{\lambda'_1}_1\,\pi_2^{\lambda_2}\pi'^{\lambda'_2}_2\ldots\pi_k^{\lambda_k}\pi'^{\lambda'_k}_k\,q_1^{\mu_1}q_2^{\mu_2}\ldots q_l^{\mu_l},$$

Với $n=zz'$ ta có

(22) $$z=i^{\nu}(1+i)^{\lambda}\,\pi_1^{\lambda_1}\pi'^{\lambda'_1}_1\,\pi_2^{\lambda_2}\pi'^{\lambda'_2}_2\ldots\pi_k^{\lambda_k}\pi'^{\lambda'_k}_k\,q_1^{\mu_1}q_2^{\mu_2}\ldots q_l^{\mu_l},$$

với ν là một trong các số $1,2,3,4,$ các lũy thừa $\lambda,\lambda_1,\lambda'_1,\ldots,\lambda_k,\lambda'_k,\mu_1,\ldots,\mu_1$ là nguyên không âm. Lấy chuẩn của ***(22)*** và lưu ý $N(\pi_j)=p_j,\ N(q_j)=q_j^2$ ta có

$$N(z)=2^{\lambda}\,p_1^{\lambda_1+\lambda'_1}p_2^{\lambda_2+\lambda'_2}\ldots q_k^{\lambda_k+\lambda'_k}q_1^{2\mu_1}q_2^{2\mu_2}\ldots q_l^{2\mu_l},$$

suy ra theo ***(21)*** và lưu ý $N(z)=n$, so sánh các số mũ của các số nguyên tố ta có

$$\lambda=\alpha,\ \lambda_1+\lambda'_1=\alpha,\ \lambda_2+\lambda'_2=\alpha_2,\ldots,\ \lambda_k+\lambda'_k=\alpha_k,$$

(23) $$2\mu_1=\beta_1,\ 2\mu_2=\beta_2,\ldots,\qquad 2\mu_l=\beta_l,$$

Các đẳng thức ***(23)*** chứng tỏ tất cả các số mũ β đều chẵn.

Vì vậy nếu số tự nhiên n là chuẩn của một số nguyên phức thì trong phân tích n thành thừa số nguyên tố các số nguyên tố có dạng $4k+3$ có số mũ chẵn.

Hơn nữa từ ***(23)*** suy ra $\lambda=\alpha,\ \mu_1=\frac{1}{2}\beta_1,\ \mu_2=\frac{1}{2}\beta_2,\ldots,\ \mu_1=\frac{1}{2}\beta_1.$

Vì vậy $\lambda,\mu_1,\mu_2,\ldots,\mu_l$ được xác định duy nhất.

Để tính λ_j và $\lambda'_j,$ với $j=1,2,\ldots,k,$ ta sử dụng một quy tắc khác được xác định như sau.

Với k_j là lũy thừa lớn nhất mà $p_j^{k_j} \mid z$, nghĩa là k_j là lũy thừa lớn nhất mà $p_j^{k_j}$ là ước số của cả a và b với $z = a + bi$. Khi đó

(24) $\left.\begin{matrix}\lambda_j = \alpha_j = k_j \\ \lambda_j^{'} = k_j\end{matrix}\right\}$ nếu $p_j^{k_j+1} \pi_j \mid z$, $\left.\begin{matrix}\lambda_j^{'} = \alpha_j - k_j \\ \lambda_j = k_j\end{matrix}\right\}$ nếu $p_j^{k_j+1} \pi_j \mid z$.

Thật vậy, từ định nghĩa của số mũ k_j suy ra số nguyên phức $z / p_j^{k_j}$ không chia hết cho π_j và p'_j vì nếu như vậy thì vì $(\pi_j, \pi'_j) = 1$ suy ra nó chia hết cho $\pi_j \pi'_j = p_j$, suy ra $p_j^{k_j+1} \mid z$, mâu thuẫn với định nghĩa của k_j. Hệ quả là nếu $\pi_j \mid \left(z / p_j^{k_j}\right)$, thì số $z / p_j^{k_j}$ không chia hết cho π'_j. Vì vậy từ $p_j^{k_j} = \pi_j^{k_j} \pi_j^{'k_j}$, theo ***(22)*** suy ra $\lambda'_j = k_j$, nên theo ***(23)*** thì $\lambda_j = \alpha_j - k_j$. Nếu số $z / p_j^{k_j}$ không chia hết cho π_j, thì $\lambda_j = k_j$ và $\lambda'_j = \alpha_j - k_j$. Theo ***(24)*** suy ra quy tắc được chứng minh.

Cuối cùng số mũ v tìm được từ phép chia z cho tích tất cả các ước số nguyên tố có số mũ đã biết.

Ví dụ. ***1.*** Với $z = 22 + 7i$. Ta có $N(z) = 484 + 49 = 533 = 13 \cdot 41$, $p_1 = 13 = 2^2 + 3^2$, $p_2 = 41 = 4^2 + 5^2$.

Hệ quả là $z = i^v \pi_1^{\lambda_1} \pi_1^{'\lambda_j} \pi_2^{\lambda_2} \pi_2^{'\lambda'_2}$, với $\pi_1 = 2 + 3i, \pi_1^{'} = 2 - 3i, \pi_2 = 4 + 5i, \pi_2^{'} = 4 - 5i$. Rõ ràng $k_1 = k_2 = 0$. Số $z / \pi_1 = (22 + 7i) / (2 + 3i) = (22 + 7i)(2 - 3i) / 13 = 5 - 4i$ là số nguyên phức do đó $\lambda_1 = \alpha_1 - 0 = 1, \lambda_1 = 0$. Tương tự, thương số z / π_2 cũng tính được nhưng chỉ cần lưu ý rằng $5 - 4i$ là số nguyên tố phức. Vì vậy $22 + 7i = (2 + 3i)(5 - 4i)$ là biểu diễn cần tính. □

2. Với $z = 19 + 17i$. Ta có $N(z) = 361 + 289 = 650 = 2 \cdot 5^2 \cdot 13 = 2 \cdot p_1^2 \cdot p_2$.

Hệ quả là $z = i^v (1 + i) \pi_1^{\lambda_1} \pi_1^{'\lambda_j} \pi_2^{\lambda_2} \pi_2^{'\lambda'_2}$, với $\pi_1 = 1 + 2i, \pi_1^{'} = 1 - 2i, \pi_2 = 2 + 3i, \pi_2^{'} = 2 - 3i, \alpha_1 = 2, \alpha_2 = 1$.

Vì ta đều không có $5 \mid z$ và $13 \mid z$, nên $k_1 = k_2 = 0$. Hơn nữa số $(19 + 17i) / (1 + 2i)$ không phải số nguyên phức và do đó $\lambda_1 = 0$ và $\lambda_1^{'} = 2$. Số $(19 + 17i) / (2 + 3i)$ không phải số nguyên phức. Do đó $\lambda_2 = 0$ và $\lambda_2^{'} = 1$. Vậy ta có $z = i^v (1 + i)(1 - 2i)^2 (2 - 3i)$, với phép chia đơn giản suy ra $\upsilon = 2$. Vậy phân tích cần tìm là $19 + 17i = (1 + i)(1 - 2i)^2 (-2 + 3i)$. □

3. Với $z = 10 + 100i$. Ta có $z = 10(1 + 10i) = 101$ và vì $10 + 100i = -i(1 + i)^2 (1 + 2i)(1 - 2i)(1 + 10i)$ nên chỉ cần tính biểu diễn của $1 + 10i$. Ta có $N(1 + 10i) = 101$. Đây là số nguyên tố có dạng $4k + 1$. Vì vậy theo Định lý 7, $1 + 10i$ là số nguyên tố phức. Do đó $10 + 100i = -i(1 + i)^2 (1 + 2i)(1 - 2i)$, □

Bài tập. Tìm phân tích thành số nguyên tố phức của các số nguyên phức $1 + 7i, 9 + i, 7 + 9i$, $107 + 198i, 10 + i, 7 + 24i$.

Lời giải. Ta có $1 + 7i = -(1 + i)(1 + 2i)^2, 9 + i = -i(1 + i)(4 + 5i), 7 + 9i = (1 + i)(1 + 2i)(3 - 2i)$,

$107 + 198i = -(1 + 6i)^3, 10 + i = 10 + i, 7 + 24i = -(1 + 2i)^4$. □

6. Số các số nguyên phức với chuẩn cho trước

Ta sẽ tính xem có bao nhiêu số nguyên phức có chuẩn bằng một số tự nhiên cho trước n. Vấn đề này không chỉ tự nó quan trọng mà còn vì nó tương đương với bài toán tìm tất cả các cặp số nguyên x, y mà $x^2 + y^2 = n$. Nói cách khác số $\tau(n)$ các số nguyên phức với chuẩn bằng n bằng với số cách biểu diễn số n thành tổng hai bình phương các số nguyên.

Do đó hàm $\tau(n)$ ở đây cũng đã được nghiên cứu trong Chương 11.

Gọi ***(20)*** là phân tích thành thừa số nguyên tố của n và ***(21)*** là biểu diễn của số đó thành tích các số nguyên tố phức. Ta đã chứng minh trong mục 5 thì $N(z)=n$ chỉ khi các lũy thừa $\beta_j, j=1,2,...,l$ đều chẵn. Giả sử điều kiện này được thỏa mãn, khi đó số z với chuẩn n có phân tích thành thừa số nguyên tố phức dạng ***(22)***, các đẳng thức ***(23)*** đối với các số mũ của các lũy thừa cũng được thỏa mãn và v là một trong các số $1,2,3,4.$ Ngược lại nếu $\lambda,\lambda_1,\lambda_1^{'},\lambda_2,\lambda_2^{'}...,\lambda_k,\lambda_k^{'},\ \mu_1,\mu_2,...,\mu_l$ là các bộ số nguyên không âm tùy ý thỏa mãn các đẳng thức ***(23)*** và v là một trong các số 1,2,3,4 thì số z xác định duy nhất bởi ***(22)*** sẽ có chuẩn n. Mà các số $\lambda,\mu_1,\mu_2,...,\mu_l$ được xác định duy nhất bởi các điều kiện ***(23)*** nên vấn đề tính số các số nguyên phức phân biệt có chuẩn bằng số n tương đương với việc tính số các bộ số nguyên không âm phân biệt $v,\lambda_1,\lambda_1^{'},\lambda_2,\lambda_2^{'}...,\lambda_k,\lambda_k^{'}$ thỏa mãn

$$1\le v\le 4,\ \lambda_1+\lambda_1^{'}=\alpha_1,\ \lambda_2+\lambda_2^{'}=\alpha_2,...,\ \lambda_k+\lambda_k^{'}=\alpha_k.$$

Có bốn giá trị v có thể nhận là 1,2,3,4. Với $\lambda_1,\lambda_1^{'}$ ta có α_1+1 khả năng có thể xảy ra là $0,\alpha_1;1,\alpha_1-1;2,\alpha_1-2;...;\alpha_1,0$. Tương tự ta có α_2+1 giá trị ứng với $\lambda_2,\lambda_2^{'}$ và cứ như thế. Chứng tỏ

(25) $$\tau(n)=4(\alpha_1+1)(\alpha_2+1)...(\alpha_k+1).$$

Công thức này nhận được với giả thiết là số mũ của các số nguyên tố dạng $4t+3$ trong phân tích thành thừa số nguyên tố của n đều chẵn. Trong trường hợp ngược lại thì phương trình $N(z)=n$ không có nghiệm nguyên phức z, do đó $\tau(n)=0$. Vậy ta có định lý

Định lý 8. *Nếu số tự nhiên n có phân tích thành thừa số nguyên tố dạng **(20)** thì số $\tau(n)$ các cách biểu diễn n thành tổng hai bình phương các số nguyên là bằng $4(\alpha_1+1)(\alpha_2+1)...(\alpha_k+1)$ với giả thiết số mũ của các số nguyên tố dạng $4t+3$ trong phân tích đều chẵn. Trong trường hợp ngược lại $\tau(n)=0.$*

Định lý nhận được từ Chương 11 mục 1 (theo một cách khác) là hệ quả của Định lý 8.

Đặc biệt nếu n là số nguyên tố có dạng $4t+1$ thì $\tau(n)=8$ suy ra Định lý 9 Chương 5.

Bây giờ xét hàm $f(h)$ định nghĩa như sau

(26) $$f(h)=\begin{cases}0 & khi\ 2\mid k\\ +1 & khi\ k=4t+1\\ -1 & khi\ k=4t+3\end{cases}$$

Với mọi số nguyên a,b thì $f(ab)=f(a)f(b)$. Nên nếu $n=h_1^{\alpha_1}h_2^{\alpha_2}...h_k^{\alpha_k}$ là phân tích thành thừa số nguyên tố của n thì $\sum_{d\mid n}f(d)=\left(f(1)+f(h_1)+f(h_1^2)+...+f(h_1^{\alpha_1})\right)...\left(f(1)+f(h_k)+...+f(h_k^{\alpha_k})\right).$

Theo ***(26)*** ta có $f(1)+f(2)+f(2^2)+...+f(2^{\alpha})=1.$

Nếu $h=4t+1,$ thì $f(1)+f(h)+f(h^2)+...+f(h^{\alpha})=\alpha+1.$

Nếu $h=4t+3,$ thì

(27) $$f(1)+f(h)+f(h^2)+...+f(h^{\alpha})=1-1+1-...+(-1)^{\alpha}=\frac{1+(-1)^{\alpha}}{2}.$$

Theo công thức của $\sum_{d\mid n}f(d)$ ta có $\sum_{d\mid n}f(d)=\prod_{h_i\equiv 1(\mathrm{mod}\,4)}(\alpha+1)$ suy ra theo Định lý 8 thì

(28) $$\tau(n) = 4\sum_{d|n} f(d),$$

nếu mọi số nguyên tố có dạng $4t+3$ trong phân tích của n đều có số mũ chẵn trong phân tích thành thừa số nguyên tố của n. Trong trường hợp ngược lại thì từ ***(27)*** ta có $\sum_{d|n} f(d) = 0$ và theo Định lý 8 chứng tỏ ***(28)*** đúng. Do đó nó đúng với mọi n. Vậy ta đã chứng minh định lý Jacobi sau

Định lý 9. *Số cách biểu diễn một số tự nhiên n thành tổng bình phương hai số tự nhiên là bằng bốn lần hiệu của số ước số có dạng $4t+1$ của n và số các ước số có dạng $4t+3$ của n.*

Thật vậy, trong ***(28)*** thì các hạng tử $+1$ xuất hiện với số lần đúng bằng số các ước số có dạng $4t+1$ của n và các hạng tử -1 xuất hiện với số lần đúng bằng số ước số có dạng $4t+3$ của n.

Theo ***(28)*** ta có

(29) $$\frac{1}{4}\sum_{n=1}^{[x]}\tau(n) = \sum_{k=1}^{[x]} f(k)\left[\frac{x}{k}\right].$$

do các hạng tử $f(d)$ xuất hiện trong tổng $\sum_{n=1}^{[x]}\sum_{d|n} f(d)$ với số lần đúng bằng số các số $n \le s$ mà $d \mid n$, nghĩa là $\left[\frac{x}{d}\right]$ lần.

Theo công thức ***(6)*** Chương 11 mục 2 ta có $\frac{1}{4}\sum_{n=1}^{[x]}\tau(n) = \sum_{k=0}^{[\sqrt{x}]}\left[\sqrt{x-k^2}\right]$, suy ra

(30) $$\sum_{k=0}^{[\sqrt{x}]}\left[\sqrt{x-k^2}\right] = \sum_{k=1}^{[\sqrt{x}]} f(k)\left[\frac{x}{k}\right],$$

Và do đó $\left[\sqrt{x}\right] + \left[\sqrt{x-1^2}\right] + \left[\sqrt{x-2^2}\right] + \ldots = \left[\frac{x}{1}\right] - \left[\frac{x}{3}\right] + \left[\frac{x}{5}\right] - \left[\frac{x}{7}\right] + \ldots.$

Các tổng trong đẳng thức này đều chứa hữu hạn hạng tử. Đẳng thức này gọi là đồng nhất thức Liouville. Với *x = 10* ta có

$$\left[\sqrt{10}\right] + \left[\sqrt{9}\right] + \left[\sqrt{6}\right] + \left[\sqrt{1}\right] = \left[\frac{10}{1}\right] - \left[\frac{10}{3}\right] + \left[\frac{10}{5}\right] - \left[\frac{10}{7}\right] + \left[\frac{10}{9}\right],$$

Tức là $3 + 3 + 2 + 1 = 10 - 3 + 2 - 1 + 1.$

Đẳng thức Liouville cũng được suy ra từ định lý Jacobi theo một cách khác.

Dựa vào các đẳng thức trong Chương 11 mục 2 thì đồng nhất thức Liouville suy ra khai triển Leibniz của π là $\frac{\pi}{4} = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \ldots$ theo một cách sơ cấp. Đây là phương pháp thuần túy số học mà dẫn tới một công thức của một hằng số hình học quan trọng nhất: *tỷ số của chu vi và đường kính của hình tròn*. Công thức này có dạng rất đơn giản (chuỗi tổng nghịch đảo các số lẻ liên tiếp với các dấu cộng trừ liên tục). Một công thức tính π dựa vào các số lẻ liên tiếp khác được cho bởi Euler: $\frac{\pi^2}{8} = \frac{1}{1^2} + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \frac{1}{9^2} + \ldots$. Công thức này cũng nhận được theo cách sơ cấp,

Ta có một số công thức khác của π được chứng minh bằng giải tích là

Công thức Wallis: $\frac{\pi}{4} = \left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right)\left(1 - \frac{1}{7^2}\right)\left(1 - \frac{1}{9^2}\right)\ldots$

Công thức Euler: $\frac{\pi^3}{32}=\frac{1}{1^3}-\frac{1}{3^3}+\frac{1}{5^3}-\frac{1}{7^3}+\frac{1}{9^3}-\ldots$

Công thức *Brouncker:* $\frac{4}{\pi}=1+\frac{1^2\big|}{\big|2}+\frac{3^2\big|}{\big|2}+\frac{5^2\big|}{\big|2}+\frac{7^2\big|}{\big|2}+\frac{9^2\big|}{\big|2}+\ldots$

7. Định lý Jacobi về tổng bốn bình phương

Bây giờ ta chứng minh định lý Jacobi về việc biểu diễn một số thành tổng bốn bình phương.

Đầu tiên ta xét trường hợp khi số tự nhiên n có dạng $n = 4u$. Giả sử

(31) $\qquad 4u = x^2 + y^2 + z^2 + t^2$

là một biểu diễn của $4u$ thành tổng của bốn bình phương lẻ.

Rõ ràng vì x, y, z, t lẻ nên

(32) $\qquad x^2 + y^2 = 2u'$ và $z^2 + t^2 = 2u"$

Với u' và $u"$ là các số tự nhiên lẻ. Theo ***(31)*** và ***(32)*** ta có

(33) $\qquad 2u = u' + u".$

Mặt khác nếu w là số lẻ và $2w = a^2 + b^2$ nên các số a,b lẻ vì nếu a,b đều chẵn thì $2w$ chia hết cho 4, mâu thuẫn với giả thiết w lẻ và nếu một trong các số a,b lẻ và số kia chẵn thì số $2w$ lẻ, vô lý.

Vì vậy để tìm tất cả các biểu diễn của $4u$ thành tổng của bốn bình phương lẻ ta chỉ cần tìm các biểu diễn $2u$ thành tổng của hai số lẻ u' và $u"$ và sau đó tìm số cách biểu diễn của các số $u', u"$ thành tổng hai bình phương.

Ký hiệu $0(4u)$ là số cách biểu diễn $4u$ thành tổng của bốn bình phương lẻ.

Với mọi cặp hai số lẻ cố định u' và $u"$ thỏa mãn ***(33)*** thì theo ***(28)*** và $\tau(2m)=\tau(m),\ m=1,2,\ldots,$ suy ra từ ***(25)*** ta có số cách biểu diễn $4u$ thành tổng bốn bình phương lẻ là

$$\tau(2u')\tau(2u")=16\sum_{d'\mid u'}f(d')\sum_{d"\mid u"}f(d").$$

Vì vậy tổng số cách biểu diễn là

(34) $\qquad 0(4u)=16\sum_{u'+u"=2u}\left(\sum_{d'\mid u'}f(d').\sum_{d"\mid u"}f(d")\right)$

Trong mỗi hạng tử thì tổng lấy trên mọi cặp số tự nhiên $u', u"$ thỏa mãn ***(33)***. Vì mọi ước số của số lẻ đều là số lẻ nên theo ***(26)*** ta có $\sum_{d'\mid u'}f(d')=\sum_{d'\mid u'}(-1)^{\frac{1}{2}(d'-1)}$ và tương tự $\sum_{d"\mid u"}f(d")=\sum_{d"\mid u"}(-1)^{\frac{1}{2}(d"-1)}$

từ đó sử dụng ***(34)*** suy ra

(35) $\qquad 0(4u)=16\sum_{u'+u"=2u}\left(\sum_{d'\mid u'}(-1)^{\frac{1}{2}(d'-1)}.\sum_{d"\mid u"}(-1)^{\frac{1}{2}(d"-1)}\right).$

Sử dụng quy tắc

$$\sum_{m=1}^{p}a_m\sum_{n=1}^{q}b_n=\left(a_1+a_2+\ldots+a_p\right)\left(b_1+b_2+\ldots+b_q\right)=\sum_{m=1}^{p}\sum_{n=1}^{q}a_mb_n$$

Từ ***(35)*** suy ra

(36) $$0(4u) = 16 \sum_{u'+u''=2u} \sum_{d'|u'} \sum_{d''|u''} (-1)^{\frac{1}{2}(d'-1)+\frac{1}{2}(d''-1)}$$

Dựa vào đẳng thức $\frac{1}{2}(d'-1) + \frac{1}{2}(d''-1) = \frac{1}{2}(d'-d'') + d''-1$ và vì d'' là ước số của số lẻ nên nó là số lẻ, ta có $(-1)^{\frac{1}{2}(d'-1)+\frac{1}{2}(d''-1)} = (-1)^{\frac{1}{2}(d'-d'')}$

Vì vậy ***(36)*** trở thành

(37) $$0(4u) = 16 \sum_{u'+u''=2u} \sum_{d'|u'} \sum_{d''|u''} (-1)^{\frac{1}{2}(d'-d'')}$$

Với mọi cặp số tự nhiên lẻ u' và u'' thỏa mãn ***(33)*** và với mọi cặp các ước số d' và d'' ta ký hiệu các đối ước số của chúng là δ', δ''. Ta có

(38) $$u' = d'\delta', \qquad u'' = d''\delta''.$$

Theo ***(33)*** suy ra

(39) $$2u = d'\delta' + d''\delta'',$$

với δ' và δ'' là các ước số của số lẻ nên chúng là các số lẻ. Hệ quả là mỗi hạng tử của tổng ***(37)*** ứng với một bộ bốn số lẻ duy nhất

(40) $$d', \quad d'', \quad \delta', \quad \delta''.$$

thỏa mãn ***(39)***. Ngược lại, do hai số đầu tiên trong các số $d', d'', \delta', \delta''$ đã được cho trước và hai số còn lại được xác định bởi ***(38)*** nên tổng ***(37)*** được lấy trên tất cả các số tự nhiên thỏa mãn ***(39)***.

Vì vậy ta có thể viết

(41) $$0(4u) = 16 \sum_{d'\delta' + d''\delta'' = 2u} (-1)^{\frac{1}{2}(d'-d'')}$$

Trong đó tổng ở vế phải lấy trên mọi bộ số ***(40)*** gồm bốn số lẻ thỏa mãn ***(39)***.

Bây giờ ta chia các hạng tử của ***(41)*** thành hai lớp, lớp thứ nhất chứa các hạng tử mà $d' = d''$ và lớp thứ hai chứa các hạng tử mà $d' \neq d''$.

Với số tự nhiên lẻ d cho trước ta tính tổng các hạng tử của ***(41)*** với $d' = d'' = d$.

Từ ***(39)*** ta thấy *d* là ước số của *2u* và nó là số lẻ nên nó là ước số của *u*. Vậy ta có $u = d\delta,$ do đó theo ***(39)*** thì $2\delta = \delta' + \delta''$. Điều này chứng tỏ số các hạng tử trong ***(41)*** mà $d' = d'' = d$ là bằng với số cách biểu diễn của 2δ thành tổng của hai số tự nhiên lẻ, tức là bằng δ. Nhưng mọi hạng tử đó đều bằng +1 nên tổng của chúng bằng $\delta = u/d$.

Từ đây suy ra tổng các hạng tử thuộc lớp thứ nhất là $\sum_{d|u} \frac{u}{d} = \sum_{d|u} d = \sigma(u).$

Các hạng tử thuộc lớp thứ hai lại được chia thành hai lớp, lớp thứ nhất chứa các hạng tử mà $d' > d''$ và lớp thứ hai gồm các hạng tử mà $d'' > d'$. Mỗi hạng tử xác định bởi các bộ số thuộc lớp thứ nhất ứng với đúng một hạng tử thuộc lớp thứ hai xác định bởi bộ số $d', d'', \delta', \delta''$. Do đó chỉ cần tính tổng các hạng tử thuộc lớp thứ nhất sau đó nhân với hai.

Đặt

(42) $$\vartheta = \left[\frac{d''}{d'-d''} \right]$$

Mọi hạng tử thuộc lớp thứ nhất xác định bởi ***(40)*** đều tương ứng với hạng tử xác định bởi bộ số

(43) $$d_1,\quad d_2,\quad \delta_1,\quad \delta_2,$$

với

(44) $$\begin{aligned} d_1 &= \delta' + (\vartheta+1)(\delta'+\delta''), & d_2 &= \delta' + \vartheta(\delta'+\delta''),\\ \delta_1 &= d'' - \vartheta(d'-d''), & \delta_2 &= (\vartheta+1)(d'-d'') - d''. \end{aligned}$$

Đầu tiên ta chứng minh hệ ***(43)*** xác định bởi công thức ***(44)*** sẽ tương ứng với hạng tử thuộc lớp thứ nhất. . Vì ϑ là số nguyên và các số trong ***(40)*** là lẻ nên các số $\delta' + \delta''$ và $d' - d''$ chẵn.

Vì vậy từ ***(44)*** suy ra các số trong ***(43)*** đều là các số nguyên lẻ.

Theo ***(42)*** thì số ϑ là không âm vì với hạng tử thuộc lớp thứ nhất thì $d' > d''$. Hệ quả là theo ***(44)*** thì các số d_1 và d_2 dương. Hơn nữa theo ***(42)*** thì $\dfrac{d''}{d'-d''} - 1 < \vartheta \le \dfrac{d''}{d'-d''}$ và nhân với $d' - d'' > 0$ suy ra $d'' - (d'-d'') < \vartheta(d'-d'') \le d''$. Mà theo ***(44)*** suy ra $\delta_1 \ge 0$ và $\delta_2 > 0$. Nhưng số δ_1 là lẻ và khác 0 do đó $\delta_1 > 0$. Vậy bốn số trong ***(43)*** là lẻ và dương. Hơn nữa theo ***(44)*** ta có

(45) $$d_1 - d_2 = \delta' + \delta''.$$

chứng tỏ $d_1 > d_2$. Hơn nữa

(46) $$\delta_1 + \delta_2 = d' - d'',$$

Theo ***(45)*** và $d_1\delta_1 + d_2\delta_2 = d_1(\delta_1+\delta_2) - (d_1-d_2)\delta_2,$ thì $d_1\delta_1 + d_2\delta_2 = d_1(d'-d'') - (\delta'+\delta'')\delta_2.$

Vì vậy theo ***(44)*** ta có $d_1\delta_1 + d_2\delta_2 = \delta'(d'-d'') + (\delta'+\delta'')d''.$

Theo ***(39)*** thì $d_1\delta_1 + d_2\delta_2 = 2u$.

Từ đây suy ra bộ số ***(43)*** tương ứng với một hạng tử trong nhóm thứ nhất.

Bộ số ***(43)*** khác với ***(40)*** vì nếu hai bộ số là trùng nhau thì theo ***(45)*** ta có $d' - d'' = \delta'+\delta''$ suy ra theo ***(39)*** thì $2u = (d'-d'')\delta' + (\delta'+\delta'')d'' = (\delta'+\delta'')(\delta'+d'')$ và do đó vì $\delta' + \delta''$ và $\delta' + d''$ chẵn nên *2u* chia hết cho 4, mâu thuẫn với giả thiết u lẻ.

Để tính các số ***(40)*** ta giải phương trình ***(44)*** và suy ra theo ***(45)*** và ***(46)*** ta nhận được

$$\delta' = d_1 - (\vartheta+1)(d_1-d_2) = d_2 - \vartheta(d_1-d_2), \qquad d'' = \delta_1 + \vartheta(\delta_1+\delta_2).$$

Vì vậy theo ***(45)*** và ***(46)*** thì

$$\begin{aligned} \delta'' &= d_1 - d_2 - \delta' = (\vartheta+1)(d_1-d_2) - d_2\\ d' &= \delta_1 + \delta_2 + d'' = \delta_1 + (\vartheta+1)(\delta_1+\delta_2) \end{aligned}$$

Theo ***(44)*** và ***(42)*** ta nhận được

(47) $$\vartheta_1 = \left[\frac{d_2}{d_1-d_2}\right] = \left[\frac{\delta'+\vartheta(\delta'+\delta'')}{\delta'+\delta''}\right] = \left[\frac{\delta'}{\delta'+\delta''} + \vartheta\right] = \vartheta$$

Vì ϑ là số nguyên và $\delta'/(\delta'+\delta'')$ là phân số mà tử số nhỏ hơn mẫu số. Do đó

(48) $$\begin{aligned} d' &= \delta_1 + (\vartheta_1+1)(\delta_1+\delta_2), & d'' &= \delta_1 + \vartheta_1(\delta_1+\delta_2),\\ \delta' &= d_2 - \vartheta_1(d_1-d_2), & \delta'' &= (\vartheta_1+1)(d_1-d_2) - d_2. \end{aligned}$$

So sánh ***(47)*** và ***(48)*** với ***(42)*** và ***(44)*** ta kết luận rằng các bộ số ***(43)*** và ***(40)*** tương ứng với nhau theo tương ứng xác định như trên. Nói cách khác tương ứng mà ta vừa xác định chứng tỏ các hạng tử thuộc lớp thứ nhất có thể chia thành các cặp mà mỗi cặp chứa hai hạng tử, một hạng tử xác định bởi ***(40)*** và hạng tử kia xác định bởi ***(43)***. Các hạng tử này tương ứng với nhau bởi công thức ***(44)***.

Bây giờ ta tính các hạng tử thuộc cùng một cặp, nghĩa là tổng

(49) $$(-1)^{(d'-d'')/2} + (-1)^{(d_1-d_2)/2},$$

với d', d'', d_1 và d_2 tương ứng xác định theo ***(44)***.

Theo ***(39)*** và ***(45)*** ta có $2u = (d'-d'')\delta' + (d_1-d_2)d''$ và do đó $\frac{d'-d''}{2} + \frac{d_1-d_2}{2} = u$.

Mà các số δ', d'' và u là lẻ nên $\frac{d'-d''}{2} + \frac{d_1-d_2}{2} \equiv 1 \pmod 2$

Chứng tỏ tổng ***(49)*** bằng 0. Nói cách khác các hạng tử trong cùng cặp triệt tiêu nhau.

Vì vậy tổng của các hạng tử thuộc lớp thứ nhất bằng 0 và do đó tổng tất cả các hạng tử trong lớp thứ hai trong phân hoạch thứ nhất là bằng 0. Mà tổng các hạng tử thuộc lớp thứ nhất của phân hoạch thứ nhất là bằng $\sigma(u)$ suy ra theo ***(41)*** ta có định lý

Định lý 10. *Nếu u là số tự nhiên lẻ thì* $\theta(4u) = 16\sigma(u)$.

Định lý này được phát biểu lần đầu tiên theo một cách khác và được chứng minh bởi Jacobi [1] (Bachmann [2] trang 349-354).

Bây giờ giả sử

(50) $$u = \xi^2 + \eta^2 + \zeta^2 + \vartheta^2$$

là biểu diễn một số tự nhiên lẻ *u* thành tổng bốn bình phương và đặt

(51)
$$x' = \xi + \eta + \zeta + \vartheta, \qquad y' = \xi + \eta - \zeta - \vartheta$$
$$z' = \xi - \eta + \zeta - \vartheta, \qquad t' = \xi - \eta - \zeta + \vartheta$$

Vì $w^2 \equiv w \pmod 2$ với mọi số nguyên *w* nên theo ***(50)*** ta có $x' \equiv u \pmod 2$ mà u lẻ suy ra x' lẻ. Hơn nữa từ công thức ***(50)*** suy ra

$$y' = x' - 2(\zeta+\vartheta), \qquad z' = x' - 2(\eta+\vartheta), \qquad t' = x' - 2(\eta+\zeta),$$

với các số x', y', z', t' đều lẻ. Theo ***(50)*** và ***(51)*** ta thấy $x'^2 + y'^2 + z'^2 + t'^2 = 4u$ do đó bộ số

(52) $$x', y', z', t'$$

xác định bởi ***(50)*** cho một biểu diễn *4u* thành tổng bốn bình phương lẻ.

Mặt khác đặt

(53)
$$x'' = -\xi + \eta + \zeta + \vartheta, \qquad y'' = \xi - \eta + \zeta + \vartheta$$
$$z'' = \xi + \eta - \zeta + \vartheta, \qquad t'' = \xi + \eta + \zeta - \vartheta$$

Các số

(54) $$x'', y'', z'', t''$$

đều lẻ và $x''^2 + y''^2 + z''^2 + t''^2 = 4u$.

Có thể thấy các bộ số ***(52)*** và ***(54)*** là phân biệt vì theo ***(51)*** và ***(53)*** ta có

(55) $$x' + y' + z' + t' = 4\xi, \quad x'' + y'' + z'' + t'' = 2(\xi+\eta+\zeta+\vartheta)$$

Mà $\xi+\eta+\zeta+\vartheta$ lẻ nên tổng các số ***(52)*** chia hết cho 4 trong khi tổng các số ***(54)*** thì không.

Theo ***(51)*** và ***(53)*** thì mọi biểu diễn một số lẻ *u* thành tổng bốn bình phương tương ứng với hai biểu diễn phân biệt các số *4u* thành tổng bốn bình phương lẻ.

Bây giờ ta chứng minh mọi biểu diễn ***(31)*** của số *4u* thành tổng bốn bình phương lẻ tương ứng với biểu diễn duy nhất của số u thành tổng bốn bình phương.

Thật vậy, số $s=x+y+z+t$ là tổng bốn số lẻ trong ***(31)*** nên nó là số chẵn. Ta xét hai trường hợp

(i) Nếu $s\equiv 0 \pmod 4$ thì từ công thức ***(53)*** suy ra ***(55)*** và do đó không tồn tại các số nguyên ξ,η,ζ,ϑ thỏa mãn ***(50)*** và thỏa mãn các số x'', y'', z'', t'' xác định bởi chúng là tương ứng bằng với *x, y, z, t* vì từ sự tồn tại các số nguyên như vậy suy ra *s* không chia hết cho 4, mâu thuẫn với giả thiết. Mặt khác tồn tại đúng một bộ số nguyên ξ,η,ζ,ϑ thỏa mãn ***(50)*** với

(56)
$$x=\xi+\eta+\zeta+\vartheta,\qquad y=\xi+\eta-\zeta-\vartheta,$$
$$z=\xi-\eta+\zeta-\vartheta,\qquad t=\xi-\eta+\zeta-\vartheta$$

Từ ***(56)*** suy ra

(57)
$$\frac{x+y+z+t}{4}=\xi,\qquad \frac{x+y-z-t}{4}=\eta,$$
$$\frac{x-y+z-t}{4}=\zeta,\qquad \frac{x-y-z+t}{4}=\vartheta.$$

Và suy ra bộ số *x, y, z, t* tương ứng với nhiều nhất một bộ số ξ,η,ζ,ϑ mà thỏa mãn ***(57)***. Nếu ta tính các số ξ,η,ζ,ϑ từ ***(57)*** thì các số nhận được là nguyên và thỏa mãn ***(56)*** và theo ***(31)*** thì chúng thỏa mãn ***(50)*** và suy ra bộ số x,y,z,t tương ứng với ít nhất một bộ số như vậy. Vì vậy trong trường hợp ***(i)*** thì ta có tương ứng một-một giữa các biểu diễn ***(31)*** và các biểu diễn ***(50)*** của u thành tổng của bốn bình phương.

(ii) Nếu $s\equiv 2 \pmod 4$ thì từ công thức ***(51)*** suy ra công thức ***(55)***. Không tồn tại các số nguyên ξ,η,ζ,ϑ mà công thức ***(51)*** cho hệ $x'=x, y'=y, z'=z, t'=t$ vì nếu ngược lại thì tổng s chia hết cho 4, mâu thuẫn với giả thiết. Mặt khác tồn tại duy nhất bộ số nguyên ξ,η,ζ,ϑ thỏa mãn ***(50)*** và thỏa mãn

(58)
$$x=-\xi+\eta+\zeta+\vartheta,\qquad y=\xi-\eta+\zeta+\vartheta,$$
$$z=\ \ \xi+\eta-\zeta+\vartheta,\qquad t=\xi+\eta+\zeta-\vartheta$$

Vì từ ***(58)*** suy ra

(59)
$$\frac{-x+y+z+t}{4}=\xi,\qquad \frac{x-y+z+t}{4}=\eta,$$
$$\frac{x+y-z+t}{4}=\zeta,\qquad \frac{x+y+z-t}{4}=\vartheta.$$

Chứng tỏ bộ số x,y,z,t tương ứng với nhiều nhất một bộ số ξ,η,ζ,ϑ thỏa mãn ***(59)***. Nếu các số ξ,η,ζ,ϑ được tính từ công thức ***(59)*** thì chúng là số nguyên thỏa mãn ***(58)***. Vì ***(31)***, ***(58)*** suy ra bộ số x,y,z,t tương ứng với ít nhất một bộ số ξ,η,ζ,ϑ.

Do đó trong trường hợp ***(ii)*** thì tồn tại tương ứng một-một giữa các biểu diễn ***(31)*** và các biểu diễn ***(50)*** của số u thành tổng của bốn bình phương.

Vậy số cách biểu diễn 4u thành tổng của bốn bình phương lẻ là hai lần lớn hơn số $\tau_4(u)$ là số cách biểu diễn của số u (lẻ) thành tổng bốn bình phương.

Vì vậy từ Định lý 10 ta suy ra công thức

(60) $$\tau_4(u) = 8\sigma(u)$$

đúng với mọi số tự nhiên lẻ u. Vậy ta có định lý

Định lý 11. *Số cách biểu diễn một số lẻ thành tổng bốn bình phương là bằng với tổng các ước số của nó nhân với 8.*

Do số các ước số của một số lẻ >1 ít nhất là 4 nên theo Định lý 11 ta thấy mọi số tự nhiên lẻ >1 đều có ít nhất 32 biểu diễn thành tổng bốn bình phương. Vì mọi bình phương lẻ đều có đúng 8 biểu diễn thành tổng bốn bình phương mà ba trong số đó là bằng 0 nên suy ra mọi bình phương lẻ lớn hơn 1 đều là tổng của bốn bình phương mà ít nhất hai trong số đó là khác 0. Vì vậy từ Định lý Lagrange ta suy ra hệ quả sau đây

Hệ quả. *Mọi số tự nhiên lẻ lớn hơn 1 đều là tổng của bốn bình phương mà ít nhất hai trong số đó là khác* 0.

Bây giờ ta tính số cách biểu diễn của 4u (với u lẻ) thành tổng của bốn bình phương.

Giả sử

(61) $$4u = x^2 + y^2 + z^2 + t^2$$

là một biểu diễn như vậy.

Nếu một trong các số x, y, z, t là chẵn và chỉ có một số là lẻ (hoặc chỉ có một số là chẵn) thì khi đó ta có tổng của các bình phương là lẻ, mâu thuẫn với ***(61)***.

Nếu hai trong số các số x, y, z, t là chẵn và hai số còn lại là lẻ thì tổng các bình phương có dạng $4k+2$, mâu thuẫn với ***(61)***.

Do đó tất cả các số x, y, z, t cùng chẵn hoặc cùng lẻ.

Trường hợp x, y, z, t cùng lẻ đã được xét trong Định lý 10, từ đó suy ra số cách biểu diễn 4u thành tổng của bốn bình phương lẻ.

Vậy chỉ cần xét số cách biểu diễn 4u thành tổng bốn bình phương chẵn.

Dễ thấy mọi biểu diễn như vậy có dạng $4u=(2\xi)^2+(2\eta)^2+(2\zeta)^2+(2\vartheta)^2$ tương ứng với biểu diễn của u thành tổng bốn bình phương là $u = \xi^2+\eta^2+\zeta^2+\vartheta^2$, và cứ như vậy. Từ đây suy ra số cách biểu diễn 4u thành tổng bốn bình phương chẵn bằng với số cách biểu diễn của u thành tổng của bốn bình phương, do đó theo ***(60)*** thì số này bằng $8\sigma(u)$.

Vậy tổng số biểu diễn 4u (với u lẻ) thành tổng bốn bình phương là $16\sigma(u)+8\sigma(u) = 24\sigma(u)$.

Vì vậy với mọi số lẻ u ta có

(62) $$\tau_4(4u) = 24\sigma(u)$$

Cuối cùng ta tính số cách biểu diễn 2u thành tổng bốn bình phương.

Ta sẽ chứng minh rằng

(63) $$\tau_4(2u) = \tau_4(4u).$$

Thật vậy, nếu ***(61)*** là biểu diễn của 4u (với u lẻ) thành tổng bốn bình phương thì các số x, y, z, t cùng chẵn hoặc cùng lẻ. Trong mọi trường hợp thì

(64) $$\xi = \frac{x+y}{2},\ \eta = \frac{x-y}{2},\ \zeta = \frac{z+t}{2},\ \vartheta = \frac{z-t}{2}$$

đều là các số tự nhiên. Ta viết lại ***(61)*** dưới dạng

$$2u = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2,$$

Suy ra ta nhận được biểu diễn

(65) $$2u = \xi^2 + \eta^2 + \zeta^2 + \vartheta^2$$

Vì vậy mọi biểu diễn ***(61)*** của 4u thành tổng bốn bình phương đều tương ứng với biểu diễn ***(65)*** của 2u thành tổng bốn bình phương. Mặt khác rõ ràng mọi biểu diễn ***(65)*** của 2u thành tổng bốn bình phương đều tương ứng với đúng một biểu diễn ***(61)*** của 4u thành tổng bốn bình phương. Chứng minh tính chất này được suy ra dễ dàng vì biểu diễn ***(65)*** tương ứng với biểu diễn ***(61)*** theo tương ứng xác định ở trên, do đó công thức ***(64)*** đúng. Vậy ta nhận được

$$\xi + \eta = x,\ \xi - \eta = y,\ \zeta + \vartheta = z,\ \zeta - \vartheta = t,$$

Công thức này xác định duy nhất biểu diễn ***(64)***.

Vậy tương ứng một-một giữa các biểu diễn 4u thành tổng bốn bình phương và các biểu diễn 2u thành tổng bốn bình phương đã được xác định. Công thức ***(63)*** được chứng minh. Từ ***(62)*** suy ra

(66) $$\tau_4(2u) = 24\sigma(u)$$

đúng với mọi số lẻ u.

Bây giờ ta tính số cách biểu diễn của $2^h u$ ($h = 3,4,\ldots$ và u lẻ) thành tổng bốn bình phương.

Giả sử

(67) $$2^h u = x^2 + y^2 + z^2 + t^2$$

là một biểu diễn như vậy. Các số x, y, z, t không cùng lẻ vì nếu như vậy thì vế phải của ***(67)*** đồng dư với 4 modulo 8 trong khi vế trái chia hết cho 8. Tương tự nếu hai trong số chúng là chẵn và các số kia là lẻ thì vế phải của ***(67)*** đồng dư với 2 modulo 4, vô lý. Vậy tất cả các số x, y, z, t cùng chẵn.

Đặt $x = 2\xi,\ y = 2\eta,\ z = 2\zeta,\ t = 2\vartheta,$ với $\xi, \eta, \zeta, \vartheta$ nguyên. Theo ***(67)*** ta có

(68) $$2^{h-2} u = \xi^2 + \eta^2 + \zeta^2 + \vartheta^2$$

Vì vậy mọi biểu diễn dạng ***(67)*** của $2^h u$ thành tổng của bốn bình phương tương úng với biểu diễn ***(68)*** của số $2^{h-2} u$ thành tổng bốn bình phương. Mặt khác rõ ràng mọi biểu diễn của $2^h u$ đều tương ứng với biểu diễn $2^h u = (2\xi)^2 + (2\eta)^2 + (2\zeta)^2 + (2\vartheta)^2$. Vì vậy

(69) $$\tau_4\left(2^h u\right) = \tau_4\left(2^{h-2} u\right)$$

với mọi $h \geq 3$ và với mọi số tự nhiên lẻ u. Bây giờ đặt s là số tự nhiên và u là số tự nhiên lẻ.

Nếu $s = 1$ hoặc $s = 2,$ thì theo ***(66)*** hoặc ***(62)*** tương ứng ta có

(70) $$\tau_4\left(2^s u\right) = 24\sigma(u).$$

Nếu $s > 2$, ta xét hai trường hợp

(i) Nếu $s = 2k$ thì từ ***(69)*** ta có $\tau_4\left(2^s u\right) = \tau_4\left(2^{2k} u\right) = \tau_4\left(2^{2k-2} u\right) = \tau_4\left(2^{2k-4} u\right) = \ldots = \tau_4\left(2^2 u\right)$ suy ra công thức ***(70)*** đúng.

(ii) Nếu $s = 2k+1$ thì theo ***(69)*** ta có $\tau_4\left(2^s u\right) = \tau_4\left(2^{2k+1} u\right) = \tau_4\left(2^{2k-1} u\right) = \ldots = \tau_4\left(2^3 u\right) = \tau_4(2u),$ suy ra theo ***(66)*** thì công thức ***(70)*** đúng.

Vậy công thức ***(70)*** đúng với mọi số tự nhiên s và số tự nhiên lẻ u.

Công thức ***(60)*** và ***(70)*** có thể kết hợp thành một định lý: *giả sử n là số tự nhiên tùy ý và ký hiệu $\sigma^*(n)=\sigma(n)$ là tổng các ước số của số tự nhiên n mà không chia hết cho 4.*

Nếu $n=u$ lẻ thì không có ước số nào của n chia hết cho 4 do đó

(71) $$\sigma^*(n)=\sigma(n).$$

Nếu n chẵn thì đặt $n=2^s u$ với s là số tự nhiên và u là số tự nhiên lẻ. Rõ ràng mọi ước số của số $2^s u$ mà không chia hết cho 4 cũng là ước số của $2u$ và ngược lại mọi ước số của $2u$ đều là ước số của $2^s u$ mà không chia hết cho 4. Do đó $\sigma^*(n)=\sigma^*(2^s u)=\sigma(2u),$ mà $(2,u)=1$ suy ra

$$\sigma(2u)=\sigma(2)\sigma(u)=3\sigma(u),$$

Ta có

(72) $$\sigma^*(n)=3\sigma(u).$$

Các công thức ***(71)*** và ***(72)*** kết hợp với ***(60)*** và ***(70)*** chứng tỏ

(73) $$\tau_4(n)=8\sigma^*(n)$$

với mọi số tự nhiên n. Vậy ta đã chứng minh được định lý

Định lý 12. *Số cách biểu diễn một số tự nhiên n thành tổng của bốn bình phương là bằng với tám lần tổng các ước số không chia hết cho 4 của n.*

Vì mọi số tự nhiên đều có ít nhất một ước số không chia hết cho 4 (chẳng hạn ước số bằng 1) nên từ Định lý 12 suy ra mọi số tự nhiên là tổng của bốn bình phương. Định lý này đã được chứng minh trong Chương 11 theo một cách khác. Một tài liệu có liên quan tới số cách biểu diễn một số thành tổng các bình phương được cho bởi E.Grosswald [2].

Bài tập. Theo ***(70)*** ta có $\tau_4(100)=24\sigma(25)=24\dfrac{5^3-1}{5-1}=24.31=744.$ Do đó 100 có 744 biểu diễn thành tổng bốn bình phương. Tương tự $\tau_4(90)=24\sigma(45)=24\dfrac{3^3-1}{3-1}.\dfrac{5^2-1}{5-1}=24.13.6=1872.$ Đây là số ≤ 100 có nhiều biểu diễn thành tổng bốn bình phương nhất. Ta có $\tau_4(7)=8\sigma(7)=8.8=64,$ $\tau_4(6)=24\sigma(3)=24.4=96,$ $\tau_4(96)=24\sigma(3)=24.4=96,$ $\tau_4(1024)=\tau_4(2^{10})=24\sigma(1)=24.$

Theo ***(73)*** ta có $\sum_{n=1}^{[x]}\tau_4(n)=8S(x)-32S\left(\dfrac{x}{4}\right).$ với $S(x)=\sum_{k=1}^{[x]}k\left[\dfrac{x}{k}\right]=\dfrac{1}{2}\sum_{k=1}^{[x]}\left[\dfrac{x}{k}\right]\left(\left[\dfrac{x}{k}\right]+1\right).$ k.

Từ đây suy ra $\left|\sum_{n=1}^{[x]}\tau_4(n)-\dfrac{\pi^2x^2}{2}\right|<100x\sqrt{x},$ với mọi số nguyên x và suy ra công thức Euler $\dfrac{\pi^2}{6}=\dfrac{1}{1^2}+\dfrac{1}{2^2}+\dfrac{1}{3^2}+\dfrac{1}{4^2}+\ldots$ bằng phương pháp thuần túy số học.

TÀI LIỆU THAM KHẢO

ABBOTT, H.L và HANSON, D., [1] A problem of Schur amd its generalizations, *Acta Arith*. **20** (1972) 175-187.

AIGNER, A., [1] Folgen der Art $ar^n + b$, welche nur teilbare Zahlen liefern, *Math, Narch* **23** (1961) 259-264.

ALAOGLU, L, và ERDOS, P, [1] On highly composite and similar numbers, *Trans.Ames.Math.Soc* **56** (1944) 448-469. [2] A conjecture in elementary number theory, *Bull.Ames.Math.Soc* **50** (1944) 881-882.

ANKENY, N.C, [1] Sum of the three squares, *Proc.Ames.Math.Soc* **8** (1957) 316-319.

ANNING, N.H, và ERDOS, P, [1] Integral distances, *Bull.Ames.Math.Soc* **51** (1945) 598-600.

AVANESOV, E.T, [1] Solution of a problem on figurate numbers (tiếng Nga), *Acta.Arith*. **12** (1966) 409-420

AVANESOV, E.T và GUSEV, V.A, [1] On a problem of Steinhaus (tiếng Nga), *Math.Chasopis* **21** (1971) 29-32

[2] On Steinhaus's problem (tiếng Nga), bản thảo tại *Referativny Zhurnal Math*. (1984), No 7A102.

BACHMANN, P, [1] Niedere Zahlentheorie, *Encyklopadie der Mathematischenwwissen shafeten mit Einschlussihrer Anwendungen* **I**C 1, 555-581, (Leipzig 1989 -1904)

[2] $Niedere\ Zahlentheorie$ **II** (Leipzig 1901, in lại tại New York 1968).

BAILLIE, R.[1] Table of $\varphi(n) = \varphi(n+1)$, UMT file, *Math.Comp.* **30** (1976) 289-190.

[2] Solutions of $\varphi(n) = \varphi(n+1)$ For Euler's function, UMT file, cf. $Math, Comp.$ **32** (1978) 1326.

BAILLIE, R, CORMACK, G.V và WILLIAM, H.C, [1] The problem of Sierpinski concerning $k \cdot 2^n + 1, Math.Comp.$ **37** (1981) 229-231, Corrigendum, tài liệu đã dẫn **39** (1982) 308.

BAKER, A., [1] Contributions to the theoru of Diophantine equations II. The Diophatine equation $y^2 = x^3 + k$, $Philos.Trans.Roy.Soc.London$ A **263** (1968) 193 – 208.

BAKER, C.L và GRUENBERGER, F.J, [1] The first six million prime numbers. Madison, Wisc. 1959 (Microcards)

BALASUBRAMANIAN,R, DRESS, F. và DESHONILLES, J, M, [1] Probléme de Waring pour les bicarrés, *C.R.Acad.Sci.Paris.*

BALOG, A,. [1] $p + a$ Without large prime factors, *Tagungsbericht* **44** (1984), *Mathematisches Forschungsbericht,* Oberwolfach.

BANG, A.S, [1] Ü ber Summen von f ü nften Potenzen, $Neuvie`me\ congre`s\ des\ math.Scand.$ 1938,292-296 (Helsinki 1939).

BANG, T, [1] Large prime numbers (tiếng Đan Mạch), $Nordisk\ Mat.Tidskr.$ **2** (1954) 157-168

BAUMERT, L.D, [1] Sum-free sts, $jet\ Propulsion\ Laboratory\ Res.Summary$ No 36-10, 1 (1961) 16-18.

BECK, W.E và NAJAR, R.M [1] A lower bound for odd triperfects, $Math, Comp.$ **38** (1982) 249-251

BEEGER, N.G.W.H, [1] On even numbers m dividing $2^m - 2, Amer.Math.Monthly$ **58** (1951) 553-555

[2] Cullen numbers, $Math, Tables\ Aids\ Comp$.**8**(1954) 188

BEHREND, F.A [1] On sets of integers which contain no three terms in arithmetical progression, $Proc.Nat.Acad.Sci.U.S.A.$. **32** (1946) 331-332

BELL, E.T [1] Reciprpcal arrays and Diophantine anlaysis, $Amer.J.Math$ **55** (1933) 50-66

BENDZ, T.R, [1] O*fver diophantiskaekvantionen* $x^n + y^n = z^n$. Diss, (Upsala 1901).

BEST, M.R và te RIELE, H.J.J [1] $On\ a\ Conjecture\ of\ Erdös\ Concerning\ Sums\ of\ Powers\ of\ Integers$, Report NW 23/76 Mathematishch Centrum,(Amsterdam 1976)

BEYER, W.A, METROPOLIS, N, và NEUGERARD, J.R [1] Squares roots of integers 2 to 15 in various bases 2 to 10: 88062 binary digits or equivalent, UMT file, cf. $Math, Comp.$ **23** (1969) 679

BIEBERBACJ, L, [1] Uber Stefelsche magische Quadrate I, $Arch.Math.$ **5**. (1954) 4-11

BLANUSA, D, [1] Une interprétation géometrique du crible d'Erathostene (Sebo-Crotian), $Glasnik\ Mat.Fiz.Astronom.Drustvo\ Mat.Fiz.Hrvatske$ (2) **4** (1949) 201-202

BOCHNER, S, [1] Remåk on the Euclidean algorithm, $J.London\ Math.Soc.$ **9**(1934) 4.

BORMAN, J, [1] The number of primes less than a given limit, $Nordisk\ Tidskr.$ $Informationsbehandling$ (BIT), **12** (1972) 576-577

[2] Some computational results regarding the prime numbers below 2000000000, $Nordisk\ Tidskr.Informationsbehandling$ (BIT), **13** (1973) 242-244

BOREL, E [1] Les probabitites denombrables et leurs applications arithmetiques,

Rend.Circ.Mat.Palermo **27** (1909) 247-271

[2] Sur les chiffres decimaux de $\sqrt{2}$ Et divers problèmes de probabité en chaine, *C.R.Acad.Sci.Paris* **230** (1950) 591-593

BORHO, W, [1] Befreundete Zahlen: ein zewitausend Jahre altes Thema der elementaren Zahkentheorie, in *Lebendige Zahlen*. 5-38 (**B**asel- Boston- Stuttgart 1981)

BOROZDKIN, K.G [1] On the problem of I.M. Vinogradov's constant (tiếng Nga), *Trudy tretego vsesojuznogo matematicheskogo s'ezda*, Vol. **I**, 3, (Moskva 1956)

BOUNIAKOWSKY, V, [1] Notes sur quelques points de l'analyse indeterminee, *Bull.Acad.Sci.St.Pe'tersbourg* **6** (1848) 196-199

[2] Sur les diviseurs numerriques invariables des functions rationales entieres, *Acad.Sci.St.Pe'tersbourg Me'm.* (6), *Sci.math.et phys* .**6** (1857) 305-329

BRAUER, A, [1] Uber einige spezielle diophantische Glechungen, *Math.Z*. **25** (1926) 499-504

[2] On a property of k consecutive integers, *Bull.Amer.Math.Soc.* **47** (1941) 328-331

BRAUER, A, và REYNOLDS, R.L, [1] On a theorem of Aubry'Thue, *Canadian J.Math.*3. (1951) 367-374

BREDIHIN, B.M [1] Binary addictive problems of indeterminate type (tiếng Nga) I, II, I *zv* . *Akad.Nauk.SSSR,Ser.mat*. **27** (1963) 439-462, 577-612

BREMNER, A, [1] Integer points in a special cubric surface, *Duke Math.J*. **44** (1977) 757-765

BRENT, R.P, [1] The first occurrence of large gaps between successive primes, *Math.Comp* **27** (1973) 959-963.
[2] Irregularities of distribution of primes and twin primes, *Math.Comp* **29** (1975) 43-56.
[3] Tables concerning irregularities in the distribution of primes and twin primes, UMT file, cf. *Math.Comp.* **30** (1976) 379.
[4] The first occurrence of certain large prime gaps, *Math.Comp.* **35** (1980) 1435-1436.

BRILLHART, J., LEHMER, D.H., SELFRIDGE, J.H., TUCKERMAN, B., WAGSTAFF, S.S. Jr.,
[1] *Factorization of* $b^n \pm 1, b = 2,3,5,6,7,10,11,12$ *up to High Power*, (Providence 1983).

BRILLHART, J., TONASCIA, J. và WEINBER GER, P.,[1] On the Fermat quotient, in: A.O.L. Atkin and B.J Birch (eds.), *Computers in Number Theory*, 213-222 (London 1971).

BROMHEAD, T., [1] On square sums of squares, *Math.Gaz* . **44** (1960) 219-220.

BROWKIN, J., [1] Certain property of triangular numbers (in Polish), *Wiadom.Mat*. **2** (1957-59) 253-255.
[2] Solution of a certain problem of A.Schinzel (in Polish), *Prace Mat*. **3** (1959) 205-207.

BROWN, A.L., [1] Multiperfect numbers, *Scripta Math.* **20** (1954) 103-106.
[2]Multiperfect numbers - Cousins of the perfect numbers - No.1, *Recreational Math.Mag*. **14** (1964) 31-39.

BROWN, J.L. Jr., [1] On Lame's Theorem, *Fibon.Quart* . **5** (1967) 153-160.
[2] Generalization of Richert's theorem, *Amer. Math. Monthly* **83** (1976) 631-634.

BRUN, V., [1] La série $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\ldots$ ou lé denominateur
[4] On a Diophantine equation, *Acta Arith*. 6 (1960) 47-52.

CATTANEO, P., [1] Sui numeri quasiperfetti, *Boll. Un. Mat. Ital*. (3) **6** (1951) 59-62.

Cel, J., [1] On decomposition of a cube into the difference of two biquadrates (in Polish), *Matematyka* **36** (1983) 308-310.

CHAKRABARTI, M.C., [1] On the limit points of a function connected with the three-square problem, *Bull. Calcutta Math. Soc*. **32** (1940) 1-6.

CHAMPERNOWNE, G.D., [1] Construction of decimals normal in the scale often, *J. London Math. Soc.* **8** (1933) 254-260.

CHEIN, E. Z., [1] Some remarks on the exponential Diophantine equation, *Notices Amer. Math. Soc*, **26** (1979) A-426.
[2] Remark on the binomial coefficients, *Notices Amer. Math. Soc*. **26** (1979) A-506.

CHEN, J. R., [1] Waring's problem for g(5*), Sc. Sinica* **12** (1964), 1547-1568.
[2] On the representation of a large even number as the sum of a prime and the product of at most two primes, *Sc. Sinica* **16** (1973) 157-176.
[3] On the least prime in an arithmetical progression and theorems

concerning the zeros of Dirichlet's L functions, *Sci. Sinica* **22**.(1979) 859-889.
CHERNICK, J, [1] On Fermat's simple theorem*, Bull. Amer. Math. Soc*. **45** (1939) 269-274.
CHIKAWA, K.,ISÉKI, K. và KUSAKABE, T., [1] Ona problem by H. Steinhaus, Acta Arith. 1 (1962) 251-252.
CHIKAWA, K., ISÉKI, K., Kusakabe, T. và SHIBAMURA, K., [1] Computation of cyclic parts of Steinhaus problem for power 5, *Acta Arith*. **7** (1962) 253- 254 and Corrigendum, ibid**. 8** (1963) 259.
CHOI, S.L.G., [1] Covering the set of integers by congruence classes of distinct moduli,
Math. Comp. **25** (1971) 885-895.
CHOJNACKA-PNIEWSKA, M., [1] Sur les congruences aux racines donn6es, *Ann. Polon. Math*. **3** (1956) 9-12.
CHOWLA, S., [1] An extension of Heilbronn's class-number theorem.
Quart.J. Math. Oxford Ser. **5** (1934), 304-307.
[2] There exists an infinity of 3-combinations of primes in A.P.,
Proc. Lahore Philos. Ser. **6**, no 2 (1944) 15-16.
CHOWLA, S. và BRIGGS, W.E., [1] On discriminants of binary quadratic forms with a
single class in each genus, *Canadian J. Math*. **6** (1954) 463-470.
CIPOLLA, M., [1] Sui numeri composti P, che verificano la congruenza di Fermat $a^{P-1} \equiv 1 \bmod P$, *Ann. Mat. Pura Appl.* (3) **9** (1903) 139-160.
CLEMENT, P.A., [1] Congruences for sets of primes, Amer. Math. Monthly 56(1949) 23-25.
[2] Representation of integers in the form: a-th power plus a prime,
Amer. Math. Monthly 56 (1949) 561.
COBLYN, [1] Sur les couples de nombres premiers, *Soc. Math, de France, C.R. des Stances* **55** (1913), 55-57.
COGHLAN, F.B., và STEPHENS, N. M., [1] The diophantine equation $x^3 - y^2 = k$, in: A.O.
L. Atkin and BJ. Birch (eds), *Computers in number theory*, 199-205 (London 1971).
COHEN, E., [1] Arithmetical notes. V. A divisibility property of the divisor function,
Amer. J. Mart. **83** (1961) 693-697.
COHEN, G.L. và HAGIS, P. Jr., [1] On the number of prime factors of n if $\varphi(n) \mid n-1$,
Nieuw Arch. Wisk. (3) **28** (1980) 177-185.
COHEN, H., [1] On amicable and sociable numbers, *Math. Comp*. **24** (1970) 423-429.
COLOMBO, M., [1] Tavole numeriche e diagrammi sulla distribuzione delle coppie di numeri primi a differenza fissa, 1st. *Lombardo Sci. Lett. Rend. A* **93** (1959) 95-133.
de COMBEROUSSE, C, [1] Algèbre supérieure **1** (Paris 1887).
COPELAND, A. và ERDOS, P., [1] Note on normal numbers, *Bull. Amer. Math. Soc,* **52** (1946) 857-860.
CORMACK, G.V. và WILLIAMS, H.C. [1] Some very large primes of the form $k \cdot 2^n + 1$,
Math. Comp. **35** (1980) 1419-1421.
van der CORPUT, J.G., [1] Sur l'hypothese de Goldbach pour presque tous les nombres pairs,
Acta Arith. **2** (1937) 266-290.
[2] Über Summen von Primzahlen und Primzahlquadraten, *Math. Ann*. **116** (1939) 1-50.
[3] On de Polignac's conjecture (in Dutch), *Simon Stevin* **27** (1950) 99-105.
COUSTAL, R., [1] Calcul de $\sqrt{2}$, et reflexion sur une espérance mathérnatique,
C.R. *Acad. Sci. Paris* **230** (1950) 431-432.
CRAMÈR, H., [1] On the order of magnitude of the difference between consecutive prime numbers,
Acta Arith. **2** (1936) 396-403.
CROCKER, R., [1] A theorem concerning prime numbers, *Math. Mag*. **34** (1960/61) 3.16,344.
[2] On the sum of a prime and of two powers of two*. Pacific J. Math*. **36** (1971) 103-107.
CUNNINGHAM, A.J.C. và Woodall, H.J., [1] Factorization of $O = \left(2^q \pm q\right)$ and $\left(q^{2^q} \pm 1\right)$.
Messenger Math. **47** (1917) 1-38.

DANILOV, L.V., [1] Letter to the editors (tiếng Nga) *Mat. Zam*. **36** (1984) 457-459.
DAVENPORT, H., [1] On Waring's problem for fourth powers, *Ann. of Math.* (2) **40** (1939) 731-747.
[2] *The Higher Arithmetic, An Introduction to the Theory of Numbers*
(London and New York 1952, fifth ed. Cambridge 1982).
DEM'YANENKO, VA., [1] On Jeśmanowicz problem for Pythagorean numbers (tiếng Nga),
Izv. Vyssh. Uchebn. Zaved. Matematika .1965, no **5** (48) 52-56.
[2] Sums of four cubes (tiếng Nga), Izv. Vyssh. Uchebn. Zaved. Matematika 1966, no **5** (54) 64-69.
[3] On a conjecture of A. Schinzel (tiếng Nga),
Izv. Vyssh. Uchebn. Zaved. Matematika 1975, no **8** (159) 33-45.
[4] On a conjecture of A. Mqkowski (tiếng Nga),
Izv. Vyssh. Uchebn. Zaved. Matematika 1976, no **10** (173) 29-31.

DÉNES, P, [1] Über die Diophantische Gleichung $x^l + y^l = cz^l$ *Acta Math*. **88** (1952) 212-251.

DEPMAN, I.YA., [1] The notable Slavic computers G. Vega and Ya. F. Kulik (tiếng Nga), *Istor.-Mat. Issled.* **6** (1953) 593-604.

DESBOVES, A., [1] Sur un théorème de Legendre et son application àla recherche de limites qui comprennent entre elles des nombres premiers, *Nouv. Ann. Math*. **14** (1855) 281-295.

DEVITT, J.S. [1] Aliquot sequences, MSc. thesis, The Univ. of Calgary 1976, cf. *Math. Comp*. **32** (1978) 942-943.

DICKSON, L.E., [1] A new extension of Dirichlet's theorem on prime numbers, *Messenger Math.* **33** (1904) 155-161.
[2] Amicable number triples*, Amer. Math. Monthly* 20 (1913) 84 91.
[3] Theorems and tables on the sum of the divisors of a number, *Quart. J. Pure Appl. Math.* **44** (1913) 264-296.
[4] Proof of the ideal Waring theorem for exponents 7-180, *Amer. J. Math*. **58** (1936) 521-529.
[5] Solution of Waring's problem, *Amer. J. Math*. **58** (1936) 530-535.
[6] *Modern Elementary Theory of Numbers* (Chicago 1939).
[7] *History of the Theory of Numbers,* 3 vols. (Washington 1919-1923, in lại tại New York 1966)

DIRICHLET, P.G.L., [1] Sur l'équation $t^2 + u^2 + v^2 + \mathrm{w}^2 = 4m$, *J. Math. Pures* Appl. (2) **1** (1856) 210-214.

DIXON, J.D., [1] The numbers of steps in the Euclidean algorithm. *J. Number Theory* **2** (1970) 414-422.
[2] A simple estimate for the number of steps in the Euclidean algorithm, *Amer. Math. Monthly* **78** (1971) 374-376.

DRESS, F., [1] Amélioration de la majoration de $g(4)$ dans le probleme de Waring:

$g(4) \le 30$, *Acta Arith*. **22** (1973) 173-147

DRESSLER, R.E., MAKOWSKI, A. và PARKER, T, [1] Sums of distinct primes from congruence classes modulo 12, *Math. Comp*. **28** (1974) 651-652.

DUPARC, HJ.A., [1] On Carmichael numbers, *Simon Stevin* **39** (1952) 21-24.
[2] On Mersenne numbers and Poulet numbers, Math. Centrum Amsterdam, Rapport ZW 1953 — 001 (1953).

DUTKA, J., [1] The square root of 2 to 1000000 decimals, *Math. Comp*. **25** (1971) 927-930.

DYER-BENNET, J., [1] A theorem on partitions of the set of positive integers, *Amer. Math. Monthly* **47** (1940) 152-154.

EDITORIAL NOTE, [1] Editorial Note, *Math. Comp*. **15** (1961) 82.

ERDÖS, P., [1] Beweis eines Satzes von Tschebyschef, *Acta Litt. Sci. Szeged* **5** (1932) 194-198.
[2] A theorem of Sylvester and Schur, *J. London Math. Soc*. **9** (1934) 282-288.
[3] On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ -function, *Quart, J. Math. Oxford Ser*. **6** (1935) 205-213.
[4] On the sum and difference of squares of primes, *J. London Math. Soc*. **12** (1937) 133-136, 168-171.
[5] Note on products of consecutive integers, *J. London Math. Soc*. **14** (1939) 194-198.
[6] Integral distances, *Bull. Amer. Math. Soc*. **51** (1945) 996.
[7] On some applications of Brun's method. *Acta Unir. Szeged Sect. Sci. Math*. **13**(1949) 57-63.
[8] On the converse of Fermat's theorem, *Amer. Math. Monthly* **56** (1949) 623-624.
[9] On a new method in elementary number theory which leads to an elementary proof of the prime number theorem, *Proc. Nat. Acad. Sci. U.S.A*. **35** (1949) 374-384.
[10] On integers of the form $2^k + p$ and some related problems, *Summa Brasil. Math*. **2** (1950)113-123.
[11] On a Diophantine equation, *J. London Math. Soc*. **26** (1951) 176-178.
[12] On consecutive integers, *Nieuw Arch. Wisk*. (3) **3** (1955) 124-128.
[13] On amicable numbers, *Publ. Math. Debrecen* **4** (1955) 108-111.
[14] Some remarks on Euler's φ function. *Acta Arith*. **4 (**1958) 10-19.
[15] Solution of two problems of Jankowska, *Bull. Acad. Polon Sci. Ser. Sci. Math.Astr.Phys*. **6** (1958) 545-547.
[16] Some remarks on the functions <p and a, *Bull. Acad. Polon. Sci. Se'r. Sci. Math. Astr. Phys.* **10** (1962) 617-619.
[17] Über die Zahlen der Form $\sigma(n)-n$ and $n-\varphi(n)$ *Elem. Math.* **28** (1973) 83-86.

ERDÖS, P. và MIRSKY, L, [1] The distribution of values of the divisor function $d(n)$,
Proc.London Math. Soc. (3) **2** (1952) 257-271.
ERDÖS, P. và OBLÁTH, R., [1] Über diophantische Gleichungen der Form $n! = x^p \pm y^p$ and $n! \pm m! = x^p$,
Acta Litt. Sci. Szeged **8** (1936) 241-255.
ERDÖS, P. và RÉNYI, A., [1] Some problems and results on consecutive primes,
Simon Stevin **27** (1950) 115-125.
ERDÖS, P. và SCHINZEL, A., [1] Distributions of the values of some arithmetical functions.
Acta Arith. **6 (**1961) 473-485.
ERDÖS, P. và SELFRIDGE, J.L., [1] The product of consecutive integers is never a power.
Illinois J. Math. **19** (1975) 292-301.
ERDÖS, P. và TURÁN, P., [1] On some sequences of integers, *J. London Math. Soc*. **11** (1936) 261-264.
[2] On some new questions on the distribution of prime numbers,
Bull. Amer. Math. Soc. **54** (1948) 371-378.
ESTERMANN, T, [1] Einige Satze über quadratfreie Zahlen, *Math. Ann*. **105** (1931) 653-662.
[2] Note on a paper of A- Rotkiewicz, *Acta Arith*. **8** (1963) 465-467.

FABER, G., [1] Über die Abzählbarkeit der rationalen Zahlen, *Math. Ann***. 60** (1905)196-203.
FERMAT, P., [1] *Oeuvres,* vol. **II** (Paris 1894).
FINSLER, P., [1] Über die Primzahlen zwischen n und $2n$,
Festschrift zum 60. *Geburtstag von Prof. Dr Andreas Speiser*, 118-122 (Zürich 1945).
FRANQUI, B., và GARCIA, M, [1] Some new multiply perfect numbers,
Amer. Math.Monthly **60** (1953) 459-462.
[2] 57 new multiply perfect numbers, *Scripta Math*. **20** (1954) 169-171.
FREDERICKSEN, H, [1] Schur numbers and the Ramsey number $N(3,3,\ldots,3;2)$ *J.*
Combin.Theory, Ser. A. **27** (1979) 376-377.
FROBENIUS, G., [1] Über quadratische Formen, die viele Primzahlen darstellen,
S. Ber. Preuss. Akad. Wss. Phys. Math. Kl. 1912, 966-980.
FRÖBERG, C.E., [1] Some Computations of Wilson and Fermat Remainders,
Math. Tables Aids Comp. **12** (1958) 281.
[2] Investigation of the Wilson remainders in the interval $3 \le p \le 50000$,
Ark. Mat. **4** (1963) 479-499.
FRÜCHTL, K., [1] Statistische Untersuchung uber die Verteilung von Primzahl-Zwillin-gen,
Anz. Öster. Akad. Wiss. Math. Nat. Kl. **87** (1950) 226-232.
FUETER, R., [1] Über kubische diophantische Gleichungen, *Comment. Math. Helv*. **2** (1930) 69-89.

GABARD, E., [1] Factorisations et équation de Pell, *Mathesi* **67** (1958) 218-220.
GABOWICZ, JA., [1] Solutions of the equation $x^3 + y^3 + z^3 - t^3 = 1$ in natural numbers (tiếng Ba Lan),
Wiadom. Mat. **7** (1963) 63-64.
GARDINER, V.L., Lazarus, R.B. và Stein, P.R., [1] Solutions of the diophantine equation $x^3 + y^3 = z^3 - d$,
Math. Comp. **18** (1964) 408-413.
GASPER, R.WJr., [1] Table of simple continued fractions for π and the derived decimal approximation,
UMT file, cf. *Math. Comp.* **31** (1977) 1044.
GELFOND, A.O., [1] A common property of number systems (tiếng Nga*),*
Izv. Akad. Nauk SSSR, Ser. Mat. **23** (1959) 809-814.
GEORGIEV, G., [1] On the solution in rational numbers of certain diophantine equations (tiếng Ba Lan)
Prace Mat. **1** (1955) 201-238.
GERONO, C.G., [1] Note sur la résolution en nombres entiers et positife de l'équation $x^m = y^n + 1$,
Nouv. Ann. Math. (2) 9 (1870) 469-471, 10 (1871) 204-206.
GILLOUD, J.và BOURGEr, M., [1] *Un million de decimals de* π (Paris 1974)
GINSBURG, J., [1] The generators of a Pythagorean triangle, *Scripta Math*. **11** (1945) 188.
GIUGA, G, [1] Su una presumabile proprietà caratteristica dei numeri primi,
Ist. Lombardo Sci. Lett. Rend CI. Sci. Mat. Nat. (3) **14** (1950) 511-528.
GLAISHER, J.W.L., [1] Mathematical notes 1. An arithmetical proposition,
Messenger of Mart. (2) **2** (1873)41-43.
[2] *Number Divisor Tables* (Cambridge 1940).
GODWIN, HJ.,[1] A note $x^3 + y^3 + z^3 = 1$, *J. London Math. Soc*. **32** (1957) 501-503.

GOLOMB, S., [1] Sets of primes with intermediate density, *Math. Scand*. **3** (1955) 264-274.
GOLUBEW, WA., [1] Abzählung von „Vierlingen" von 2000000 bis 3000000 und von „Fünflingen" von 0 bis 2000000, *Anz. Österr. Akad. Wiss. Math. Nat. Kl*. **93** (1956)153-157.
[2] Abzählung von „Vierlingen" und ..Fünflingen" bis zu 5000000 und von „Sechslingen" von 0 bis 14000000, *Anz. Österr. Akad. Wiss. Math Nat. Kl*. **94** (1957) 82-87.
[3] Abzählung von „Vierlingen" und „Fünflingen" bis zu 10000000, Einige Formeln, *Anz. Österr. Akad. Wiss. Math. Nat. Kl.* **94** (1957) 274-280.
[4] Abzählung von „Vierlingen" und „Fünflingen" bis zu 15000000, *Anz. Österr. Wiss. Math. Nat. Kl*. **96** (1959) 227-232.
[5] Primzahlen der Form x^2+1, *Anz. Österr. Akad. Wiss. Math. Nat. Kl*. **95** (1958) 9- 13; **96** (1959) 126-129; **97** (1960) 39-44, 312-319; **98** (1961) 59-63; **99** (1962) 33-37.
[6] Primzahlen der Form x^2+7, *Anz. Österr. Akad. Wiss. Math. Nat. Kl*. **98** (1961) 165- 169; **100** (1963) 244-251.
GOODSTEIN E., [1] A note on magic squares, *Math. Gaz*. **24** (1940) 117.
GRAHAM, S., [1] On Linnik's constant, *Acta Arith*. **39** (1981) 163-179.
GROSSWALD, E., [1] Negative discriminants of binary quadratic forms with one class in each gems, *Acta Arith*. **8** (1963) 295-306.
[2] *Representation of integers as sums of squares* (New York 1985).
GROSSWALD, E., CALLOWAY, A., and CALLOWAY, J., [1] The representation of integers by three positive squares, *Proc. Amer, Math. Soc*. **10** (1959) 451-455.
GROSSWALD, E. và HAGIS, P., Jr., [1] Arithmetic progressions consisting only of primes, *Math. Comp*. **33** (1979) 1343-1352.
GRUBE, F., [1] Ueber Einige Euler'sche Sätze aus der Theorie der quadratischen Formen, *Zeitschr. Math. Phys*. **90** (1874) 492-519.
GUPTA, **H.,** [1] Congruence properties of $\sigma(n)$, *Math. Student* **13** (1945) 25-29.
[2] A table of values of $N_2(t)$, *Res. Bull. East Penjab Univ*. 1952 no. **20**, 13-93.
GUY, **R.K.** [1] *Unsolved Problems in Number Theory* (New York-Heidelberg-Berlin 1981).
GUY, **R.K.** và Shanks, D., [1] A constructed solution of $\sigma(n)=\sigma(n+1)$, *Fibon. Quart*. **12** (1974) 299.

HADWIGER, H., [1] Ungelöste Probleme Nr 24, *Elem. Math*. **13** (1958) 85.
HAGIS, P., Jr., [1] A lower bound for the set of odd perfect numbers, *Math. Comp*. **27** (1973) 951-953.
[2] Outline of a proof that every odd perfect number has at least eight prime factors, *Math. Comp*. **34** (1980) 1027-1032.
HAGIS, P., Jr., và COHEN, G.L., [1] Some results concerning quasiperfect numbers, *J. Austral. Math. Soc.* **33** (1982) 275-286.
HALL,M., Jr., [1] On the sum and product of continued fractions *Ann. of Math*. (2) **48** (1947) 966-993.
[2] Cyclic projective planes, *Duke Math*., **J. 4** (1947) 1079-1090.
[3] The Diophantine equation x^3-y^3, in: A. O. L. Atkin and B.J. Birek (eds.). *Computer in Number Theory,* 173-198 (London 1971).
HALTER-KOCH, F., [1] Darstellung natürlicher Zahlen als Summe von Quadraten, *Acta Arith.* **42** (1982) 11-20.
HANLY, V.S., [1] A proposition equivalent to Dirichlet's theorem, *Amer. Math. Monthly M* **64** (1957) 742.
HARDY, G.H. và WRIGHT, E.M., [1] *An Introduction to the Theory of Numbers* (Oxford 1954)
HARRIS, V.C, [1] A modification of the sieve of Eratosthenes, *Amer. Math. Monthly* **60** (1953) 325-326.
HASSE, H., [1] *Vorlesungen liber Zahlentheorie* (Berlin-Göttingen-Heidelberg 1950)
[2] Über eine diophantische Gleichung von Ramanujan-Nagell und ihre Verall meinerung, *Nagoya Math.* **J. 21** (1966) 77-102.
HAUSDORFF, F., [1] *Grundzllge der Mengenlehre* (Leipzig 1914)
HAUSSNER, R.,[1] Uber die Verteilung von LUcken und Primzahlen, *J.ReineAngew. Math.* **168** (1932) 192.
HEATH-BROWN, D.R., [1] The divisior function at consecutive integers. *Mathematika* **31** (1984) 141-149.
HECKE, E., [1] Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen II, Math. Z. **6** (1920) 11-51.
HEMER, O., [1] *On the Diophantine* Equation $y^2-k=x^3$, Diss. (Upsala 1952).
[2] Note on the Diophantine equation $y^2-k=x^3$, *Ark. Mat.* **3** (1954) 67-77.

HENSEL, K., [1] Ueber den grössten gemeinsamen Theiler aller Zahlen, welche durch erne ganze Function von n Veränderlichen darstellbar sind, *J. Reine. Angew. Math*. **116** (1896) 350-356.
HENSLEY, D. và RICHARDS, I., [1] Primes in intervals, *Acta Arith*. **25** (1974) 375-391.
HILL, J.D., [1] Solution of the problem 3449, *Amer. Math. Monthly* **38** (1931) 298-299.
HORNFECK, B. und WIRSING, E., [1] Über die Häufigkeit vollkommener Zahlen,
Math.Ann. **133** (1957) 431-438.
HOOLEY, C, [1] On the power-free values of polynomials, *Mathematika* **14** (1967) 21-26.
HUNSUCKER, J.L., NEBB, J. và STARNS, R.E., [1] Computational results concerning some equations involving $\sigma(n)$, *Math. Student* **41** (1973) 285-289.
HURWITZ, A., [1] Uber eine besondere Art der Kettenbruch-Entwicklung reeller Grbssen,
Acta Math. 12 (1889) 367-405.
[2] Somme de trois carrés, Intermédiaire *Math*. **14** (1907) 106-107.
HYYRÖ, S., [1] On the Catalan problem (in Finnish), *Archimede*s **1** (1963) 53-54.

IRVING, R.W., [1] An extension of Schur's theorem on sum-free partitions, *Acta Arith*. **25** (1973) 55-63.
ISÈKI, K., [1] A problem of number theory, *Proc. Japan Acad*. **36** (1960) 578-583.
[2] Necessary results for computation of cyclic parts in Steinhaus problem,
Proc. Japan Acad. **36**(1960)650-651.
ISEKI, K. và TAKADA, I., [1] On Steinhaus problem in number theory, Computation of cyclic parts of Steinhaus problem for power 9, *Mathem. Seminar Notes Kobe Univ*. **8** (1980) 227 231.
IVIC A., [1] *The Riemann Zeta-F unction, the Theory of the Riemann Zeta-Function with Applications* (New York-Chichester-Brisbane-Toronto-Singapore 1985).
IWANIEC, H., [1] Almost primes represented by quadratic polynomials, *Invent. Math*. **47** (1978) 171-188.

JACOBI, C, [1] De compositione numerorum ex quatuor quadratis, *J. Reine Angew. Math.* **12** (1834) 167-172.
JAESCHKE, G., [1] On the smallest k such that all $k\cdot 2^n+1$ are composite, *Math. Comp*. **40** (1983)381-384.
JAKOBCZYK, F., [1] Les applications de la fonction $\lambda_g(n)$ à l'étude des fractions périodiques et de la congruence chinoise $2^n-2\equiv 0(\mathrm{mod}\, n)$, *Ann. Univ. Mariae Curie-Sklodowska*, *Sect*. A, **5** (1951) 97-138.
JANKOWSKA, S., [1] Les solutions du systeme d'équations $\varphi(x)=\varphi(y)$ et $\sigma(x)=\sigma(y)$ pour $x<y<10000$, *Bull. Acad. Polon. Sci. Ser Sc. Math. Astr. Phys*. **6** (1958) 541-543.
JESMANOWICZ, L., [1] Several remarks on Pythagorean triangles (in Polish), *Wiadom. Mat.* **1** (1956) 196-202,de JONCOURT, E., [1] *De Natura et Praeclaro Usu Simplicissimae Speciei NumerorumTrigonalium* (Hagae 1762).
JONEs, B.W. và PALL, G., [1] Regular and semiregular positive ternary quadratic forms.
Acta Math. **70** (1939) 165-191.
JORDAN, C, [1] *Traité des substitutions* (Paris 1870).
JOZEFIAK, T., [1] A curiosity concerning triangular numbers (in Polish*), Matematyka* **13** (1960) 327.
[2] On a hypothesis of L. Jeśmanowicz concerning Pythagorean numbers (tiếng Ba Lan),
Prace Mat. **5** (1961) 119-123.

KANOLD, H.J., [1] Untere Schranken für teilerfremde befreundete Zahlen, *Arch. Math*. **4** (1953) 399-401.
[2] Über zahlentheoretische Funktionen, *J. Reine Angew. Math*. **195** (1955) 180-191.
KELLER, W., [1] Factors of Fermat numbers and large primes of the form $k\cdot 2^n+1$,
Math. Comp. **41** (1983)661-673.
[2] New factors of Fermat numbers*, Abstracts Amer. Math. Soc*. **5** (1984) 391-392.
[3] The 17th prime of the form $5\cdot 2^n+1$, *Abstracts Amer. Math. Soc*. **6** (1985) 31.
KHATRI, M.N., [1] Triangular numbers and Pythagorean triangles, *Scripta Math*. **21** (1955) 94.
KHINCHIN,'A.Ya., [1*] Three Pearls of Number Theory* (Rochester 1952)
KILLGROVE, R.B. và RALSTON, K.E., [1] On a conjecture concerning primes*,*
Math. Tables Aids Comp. **13** (1959) 121-122.
KLEE, V.L. Jr., [1] On the equation $\varphi(x)=2m$, *Amer. Math. Monthly* **53** (1946) 327-328.
[2] Some remarks on Euler's totient, *Amer. Math. Monthly* **54** (1947) 332.
[3] A generalization of Euler's φ function, *Amer. Math. Monthly* **55** (1948) 358-359.
KNÖDEL, W., [1] Carmichaelsche Zahlen, *Math. Nachr.* **9** (1953) 343-350.

KOGBETLIANZ, E và KRIKORIAN, A., [1 *] Handbook of First Complex Prime Numbers, Part 2, Tables of Decompositions of Real Primes of Type* $4N+11$ *into Sums of two Squares* (London-New York-Paris 1971).

KOCHAO, [1] Note on the Diophantine equation $x^x y^y = z^z$, J. *Chinese Math. Soc*. **2** (1940) 205-207.

[2] Remark on Pythagorean numbers (tiếng Trung Quốc), *Acta Sc. Nat. Univ. Szechuan*, 1958,73-80.

[3] On a conjecture of Jeśmanowicz (tiếng Trung Quốc), *Acta Sc. Nat. Univ. Szechuan*, 1958, 81-90.

[4] On a Diophantine equation $\left(a^2-b^2\right)^x+\left(2ab\right)^y=\left(a^2+b^2\right)^z$ (tiếng Trung Quốc), *Acta Sc. Nat. Univ. Szechuan,* 1959, 25-34.

KOLESNIK, G., [1] On the method of exponent pairs, *Acta Arith*. **45** (1985) 115-143.

KOREC, I., [1] Nonexistence of small perfect rational cuboid, II *Acta Math. Univ. Comen.* **44-45** (1984) 39-48.

KORHONEN, O., [1] On the diophantine equation $Ax^2+2B=y^n$, *Acta Univ. Duluensis,Ser. A, Math.* ***No*** **17** (1979).

KRAÏTCHIK. M., [1] *Théorie des nombres* **II** (Paris 1926).

[2] *Recherches sur la Théorie des Nombres* **II**, Factorisation (Paris 1929).

[3] *Théorie des nombres* **III**. *Analyse diophantienne et applications aux cuboides rationnels (*Paris 1947).

[4] *Introduction à la Théorie des Nombres* (Paris 1952).

KRISHNAWAMI, AA, [1] On isoperimetrical Pythagorean triangles, *Tohoku Math*. J. **27** (1926) 332-348.

KULIK, J.PH., POLETTI, L.et PORTER, R.J., [1 *] Liste des nombres premiers du onzième million (plus précisément de* 100006741 *à* 10999997 *) d'après des tables manuscrites* (Amsterdam. 1951)

KULIKOWSKI, T., [1] Sur l'existence d'une sphère passant par un nombre donné de points aux coordonnées entières, *Enseignement Math*. (2) **5** (1959) 89-90.

LAGARIAS, J.C, MILLER, V.S. và ODLYZKO A.M., [1] Computing $\pi\left(x\right)$: The Meissel-Lehmer method, *Math. Comp*. **44** (1985) 537-560.

LAGRANGE, J., [1] Sets of n squares of which any $n-1$ have their sum square, *Math. Comp*. **41** (1983) 675-681.

LAL, M. và GILLARD, P., [1] On the equation $\phi\left(n\right)=\phi\left(n+k\right)$, *Math. Comp.* **25** (1972) 579-583.

LAL, M., RUSSELL, W. và BLUNDON, W.J., [1] A note on sums of four cubes, *Math. Comp*. **23** (1969) 423-424.

LAMÉ, G., [1] Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers, *C.R. Acad. Sci. Paris* **19** (1844) 867-870.

LANDAU, E., [1] Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate, *Arch. Math. Phys.* (3) **13** (1908) 305-312.

[2] *Vorlesungen uber Zahlentheorie*, 3 vols (Leipzig 1927, reprint New York 1947).

[3] *Handbuch der Lehre von der Verteilung der Primzahlen*, 2 vols, 2nd ed. with an Phụ lục bởi P.T. Bateman (New York 1953)

LANDER, L.J. và PARKIN, T.R., [1] Equal sums of biquadrates, *Math. Comp*. 20 (1966) 450-451; Corrigendum, ibid. **21** (1967) 296.

[2] A counterexample to Euler's sum of powers conjecture, *Math. Comp*. 21 (1967)101-103.

[3] On first appearance of prime difference*, Math. Comp*. **21** (1967) 483-488.

[4] Consecutive primes in anthmetic progression, *Math. Comp*. **21** (1967) 489.

LANDER, L.J., PARKI n, T.R. và SELFRIDGE, J.L., [1] A survey of equal sums of like powers, *Math. Comp*. **21** (1967) 446-459.

LANGEVIN, M., [1] Quelques applications de nouveaux résultats de van der Poorten, *Séminaire Delange-Phot-Poitou* **17** (1975/76) No 12, 1-11.

LEBESGUE, H., [1] Sur certaines démonstrations d'existence, *Bull. Soc. Math. France* **45** (1917) 132-144.

LEBESGUE, V.A., [1] Sur l'impossibilité en nombres entiers de l'équation $x^m=y^2+1$. *Nouv. Ann. Math.* **9** (1850) 178-181.

[2] Note sur quelques équations indéterminées, *Nouv. Ann. Math*. (2**) 8** (1869) 452-456,559.

LEE, E.J., MADACHY, J.S, [1] The history and discovery of amicable numbers, *J. Recreational Math*. **5 (**1972) 77-93,155-173; 231-249, Errata, ibid. 6 (1973) 164,229.

LEECH, J., [1] Note on the distribution of prime numbers*, J. London Math. Soc*. **32** (1957) 56-58.

[2] The rational cuboid revisited, *Amer. Math. Monthly* **84** (1977) 518-533, các chỉnh sửa rong tài lieu đã dẫn **85** (1978) 473.

LEGENDRE, A.M., [1] *Essai sur la théorie des nombres* (Paris 1798).

LEHMER, D.H., [1] On Euler's totient function, *Bull. Amer. Math. Soc*. **38** (1932) 745-751.

[2] On Lucas's test for the primality of Mersenne's numbers,

J. London Math. Soc. **10** (1935) 162-165.
[3] On the converse on Fermat's theorem, *Amer. Math. Monthly* **43** (1936) 347-354.
[4] On the partition of numbers into squares, *Amer. Math. Monthly* **55** (1948) 476-481.
[5] On a conjecture of Krishnaswami, *Bull. Amer. Math. Soc*. **54** (1948) 1185-1190.
[6] On the converse of Fermat's theorem II, *Amer. Math. Monthly* **56** (1949) 300-309.
[7] On the Diophantine equation $x^3 + y^3 + z^3 = 1$, *J. London Math. Soc*. **31** (1956) 275-282.
[8] On the exact number of primes less than a given limit, *Illinois J. Math*. **3** (1959) 381-388.
[9] On Fermat's quotient, base 2, *Math. Comp*. **36** (1981) 289-290.

LEHMER, D.N., [1] *Factor Table for the First Ten Millions Containing the Smallest Factor of Every Number not Divisible by 2, 3, 5 or 7 Between the Limits 0 and* 10017000 (Washington 1909, in lại tại New York 1956).

LERCH, M., [1] Zur Theorie der Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$, *Math. Ann*. **60** (1905) 471-490.

LESZCZYNSKI, B., [1] On the equation $n^x + (n+1)^y = (n+2)^z$ (in Polish), *Wiadom. Mat*. **3** (1959-60) 37-39.

LE VEQUE, W.J., [1] The distribution of values of multiplicative functions,
Michigan Math. **J. 2** (1953-54) 179-192.
[2] *Topics in Number Theory, 2 vols*. (Reading 1956).

LIETZMANN, W., [1] *Lustiges und merkwiirdiges von Zahlen und Formen* (Gottingen 1930).

LIGHT, W.A., FORREST, J., HAMMOND, N. và ROE, S., [1] A note on Goldbach's conjecture, *Nordisk Tidskr. Informationsbehandling* (**BIT) 20** (1980) 525.

LIND, C.E., [1] *Untersuchungeniiber die rationalen Punkte derebenen kubischenKurven von Geschlecht Eins, Diss*. (Uppsala 1940)

LINDENBAUM, A, [1] Sur les ensembles dans lesquels toutes les équations d'une famille donnée ont un nombre de solutions fixe d'advance, *Fund. Math.* **20** (1933) 1-**29**.

LINNIK, Yu.V., [1] On the representation of large numbers as sums of seven cubes,
Mat. Sb.N.S. **12** (1943) 220-224.
[2] An elementary solution of the problem of Waring by the Schnirelman method (tiếng Nga*),*
Mat. Sb. N. S. **12** (1943) 225-230.

LIOUVILLE. J., [1] Sur l'équation $1\cdot 2\cdot 3....(p-1)+1 = p^m$, *J. Math. Pures Appl*. (2) 1 (1856) 351-352.

LITVER, E. L., YUDINA, G.E., [1] Primitive roots for the first million primes and their powers (tiếng Nga), *Matematiceskij analiz i ego primienienija, vol.* 3, 106-109 (Rostov on Don 1971).

LIUNGGREN,W., [1] ZurTheorieder Gleichung $x^2 + 1 = Dy^4$. *Avh.Norske Vid.Akad.Oslo I, 1942, no 5.*
[2] Über einige Arcustangensgleichungen die auf interessante unbestimmte Gleichun-gen führen,
Ark. Mat. Astr. Fys. 39 A no 13 (1943).
[3] On the Diophantine equation $x^2 + p^2 = y^n$
Norske Vid. Selsk. Forh. (Trondheim) **16** (1943) 27-30.
[4] Solution complète de quelques équations du sixième degré à deux indéterminées,
Arch-Math. Naturvid. **48** (1946) 177-212.
[5] New solution of a problem proposed by E. Lucas*, Norsk Mat. Tidsskr*. **34** (1952) 65-72.

LOCHS, G., [1] Die ersten 968 Kettenbruchnenner von π, *Monatsh. Math*. **67** (1963) 311-316.

LONDON, H. và FINKELSTEIN, R., [1] OnMordeWs Equationy $y^2 - k = x^3$ (Bowling Green, Ohio 1973)

LUCAS, E., [1] Question 1180, *Nouv. Ann. Math*. (2) **14** (1875) 336.
[2] *Théorie des nombres,* Vol. I (Paris 1891, reprint Paris 1961).

LU WEN-TWAN, [1] On Pythagorean numbers $4n^2 - 1,\ 4n^2 + 1$ (tiếng Trung Quốc),
Acta Sc. Nat. Univ. Szechuan 1959, 39-42.

MAHLER, K., [1] On the fractional parts of the powers of a rational number (II),
Mathematika **4** (1957) 122-124.

MAIER, H. và POMERANCE, C, [1] On the number of distinct values of Euler's (ϕ function), *Acta Arith*. **49.**

MAKNIS, M., [1] Density theorems for Mecke Z-functions and the distribution of the prime numbers of an imaginary quadratic field (tiếng Nga*), Litovsk. Mat. Sb*. **16** (1976) no 1, 173-180.

MARGENSTERN, M., [1] Résultats et conjectures sur les nombres pratiques, *C.R. Acad. Sci. Paris, Sér. I Math.* **299** (1984) 895-898.

MASAI, P. và VALETTE, A. [1] A lower bound for a counterexample to Carmichaers conjecture, *Boll. Unione Mat. Ital*. (6) Al (1982) 313-316.

MASON, Th.E., [1] On amicable numbers and their generalizations, *Amer. Math. Monthly* **28** (1921) 195-200.

MAYAH, B.H., [1] The second Goldbach conjecture revisited*, Nordisk Tidskr. Informationsbehandling* (BIT) **8** (1968) 128- 133.

MAKOWSKI, A., [1] Sur quelques problemes concemant lessommes de quatre cubes, *Acta Arith.* **5** (1959) 121-123.

[2] Remark on a paper of Erdös and Turán, *J. London Math. Soc*. **34** (1959) 480.

[3] On an arithmetic function (in Polish), *Matematyka* **10** (1959) 145-147.

[4] On some equations involving functions $\varphi(n)$ and $\sigma(n)$, *Amer. Math. Monthly* **67** (1960), pp. 668-670; Correction, ibidem **68** (1961) 650.

[5] Remarques sur les fonctions $\Theta(n), \varphi(n)$ et $\sigma(n)$, *Mathesis* **69** (1960) 302-303.

[6] Three consecutive integers cannot be powers, Colloq. Math. 9 (1962) 297.

[7] Generalization of Morrow's D numbers, *Simon Stevin* **36** (1962) 71.

[8] Remarques sur les carrés magiques, *Mathesis* **70** (1962) 17-19.

[9] Some equations involving the sum of divisors, *Elem. Math*. **34** (1979) 82.

McCURLEY, K. S., [1] An effective seven cube theorem, *J. Number Theory* **19** (1984) 176-183.

MELNIKOV, I.G., [1] La découverte des "nombres commodes" par Euler (tiếng Nga) 1st. *Mat. Issled.* **13** (1960) 187-216.

MEYL, A, [1] Question 1194, *Nouv. Ann. Math*. (2) **17** (1878) 464-467.

MIENTKA, W.E. và VOGT, R.L. [1] Computational results relating to problems concerning $\sigma(n)$, *Mat. Vestnik* **7** (1970) 35-36.

MOESSNEr, A., [1] A magic square of triangular numbers*, Math. Student* **10** (1942-43)95.

[2] Magic squares, *Math. Student* **19** (1951) 124-126.

[3] All-prime magic squares, *SCRIPTA MATH*. **18** (1953) 303.

MORDELL, L.J., [l]The Diophantine equation $y^2 - k = x^3$,*Proc. London Math. Soc*. (2)**13** (1913) 60-80.

[2] Note on the integer solutions of the equation $Ey^2 = Ax^3 + Bx^2 + Cx + D$, *Messenger of Math*. **51** (1922) 169-171.

[3] On the four integer cubes problem, *J. London Math. Soc.* **11** (1936) 208-218, Addendum, *tài liệu đã dẫn* 12 (1937) 80, and Corrigendum, *ibidem* **32** (1957) 383.

[4] On sums of three cubes, *J. London Math. Soc*. **17** (1942) 139-144.

[5] On the integer solutions of the equation $x^2 + y^2 + z^2 + 2xyz = n$, J*. London Math*. *Soc*. **28** (1953) 500-510 and Corrigendum, *ibidem* 32 (1957) 383.

[6] On intervals containing an affinely equivalent set of n integers $\bmod k$, *Proc. Amer. Math. Soc.* **5** (1954) 854-859.

[7] On the representation of a number as a sum of three squares, *Rev. Math. Pures Appl.* **3** (1958)25-27.

MORET-BLANC, [1] Question 1175, *Nouv. Ann. Math*. (2) **15** (1876) 44-46.

MORROW, D.C., [1] Some properties of D numbers, *Amer. Math. Monthly* **58** (1951) 329-330.

Moser, L.,[l] Some equations involving Euler's totient function, Amer. Math. Monthly **56** (1949) 22-23.

[2] On the Diophantine equation $1^n + 2^n + \ldots + (m-1)^n = m^n$ *Scripta Math*. **19** (1953) 84-88.

[3] On non-averaging sets of integers, *Canadian J. Math.* **5** (1953) 245-252.

[4] On the theorems of Wilson and Fermat, *Scripta Math*. **22** (1957) 288.

MÜLLER, M., [1] Über die Approximation reeller Zahlen durch die Näherungsbrüche ihres regelmassigen Kettenbruches*, Arch. Math*. **6** (1955) 253-258.

NAGELL, T., [1] Zur Arithmetik der Polynome, *Abh. Math. Sem. Univ. Hamburg* **1** (1922)184-188.

[2] Sur l'impossibilité de quelques équations à deux indéterminées. *Norsk Mat. Forenings Skrifter* **1** Nr 13 (1923).

[3] Einige Gleichungen von der Form $ay^2 + by + c = dx^3$, *Norske Vid. Akad. Skrifter, Oslo* I, 1930, no 7.

[4] Solved problems (in Norwegian) *Norsk Mat. Tidsskr*. **30** (1948) 60-64.

[5] *Introduction to the Number Theory* (New York and Stockholm 1951, reprint 1964).

[6] Sur un théorème d'Axel Thue, *Ark. Mat*. **1** (1951) 489-496.

[7] On a special class of Diophantine equations of the second degree, *Ark. Mat*. **3** (1954) 51-65.

[8] Verallgemeinerung eines Fermatschen Satzes, *Arch. Math*. **5** (1954) 153-159.

[9] Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns, *Nova Acta Soc. Sci. Upsal*. (4) **16** (1954) no 2.

[10] On the Diophantine equation $x^2+8D=y^n$, *Ark. Mat.* **3** (1954) 103-112.

[11] Sur une classe d'équations exponentielles, *Ark. Mat.* **3** (1958) 569-582.

[12] The diophantine equation $x^2+7=2^n$, *Ark. Mat.* **4** (1961) 182-185.

NIEWIADOMSKL R., [1] Question 4202, *Intermédiate Math*. **20** (1913) 78.

OBLÁTH, R., [1] Une propriété des puissances parfaites, *Mathesis* **65** (1956) 356-364.

O'KEEFE, E.S., [1] Verification of a conjecture of Th. Skolem., *Math. Scand*. **9** (1961) 80- 82.

ORE, O., [1] *Number Theory and its History* (New York 1948)

PALL, G., [1] On sums of squares, *Amer. Math. Monthly* **40** (1933) 10-18.

Patz, W., [1] *Tafel der regelmässigen Kettenbriüche und Over vollständigen Quotienten fiir die Quadratwurzeln aus den natiirlichen Zahlen von* 1-10000 (Berlin 1955)

PAWLAK, Z. và WAKULICZ, A., [1] Use of expansions with a negative basis in the arithmometer of a digital computer*, Bull, Acad. Polon. Sci., CI.* **Ill, 5** (1957) 233-236.

PEANO, G., [1] Formulaire de Mathématique (Torino 1901)

PEPIN, T., [1] *Sur certains nombres complexes de la forme* $a+b\sqrt{-c}$,

J. Math. Pures Appl. (3) **1** (1875) 317-372.

PERRON, O., [1] *Die Lehre von den Kettenbrüchen* I (Stuttgart 1954).

Piccard, S., [1] Sur les ensembles de distances des ensembles de points d'un espace euclidien (Paris 1939)

PILLAL S.S., [1] On some empirical theorem of Scherk*, J. Indian Math. Soc.* **17** (1927- 28) 164-171.

[2] On some functions connected with $\varphi(n)$, *Bull. Amer. Math. Soc*. **35** (1929) 832-836.

[3] On Waring's problem II, *J. Indian Math. Soc*. (N.S) **2** (1936) 16**-44**.

[4] On m consecutive integers I, *Proc. Indian Acad. Sci., Sect*. A **12** (1940) 6-12.

[5] On m consecutive integers III. *Proc. Indian Acad. Sci., Sect*. A **13** (1941) 530-533.

[6] On m consecutive integers IV, *Bull. Calcutta Math*. *Soc.* **36** (1944) 99-101.

[7] On the smallest primitive root of a prime, J, Indian Math. Soc. (N. S) 8 (1944) 14-17.

[8] On the equation $2^x-3^y=2^x+3^y$, *Bull. Calcutta Math. Soc.* **37** (1945) 15-20.

PIPPING, N, [1] Neue Tafeln fur das Goldbachsche Gesetz nebst Berichtigungen zu den Haussnerschen Tafeln*, Comment. Phys. Math*. **4** (1027-29) no 4.

[2] Über Goldbachsche Spaltungen grosser Zahlen, *Comment. Phys. Math*.**4** (1927-29) no 10.

POCKLINGTON, H.C., [1] Some diophantine impossibilities, *Proc. Cambridge Philos. Soc*. **17** (1914) 108-121.

PODSYPANIN, V.D., [1] On a property of Pythagorean numbers (tiếng Nga*),*

Izv. Vyssh. Uchebn. Zaved. Matematika 1962, no **4** (29) 130-133.

van der POL, B., và SPEZIALI, P., [1] The primes in $k(\mathcal{Q})$, *Indag. Math*. **13** (1951) 9-15.

de POLIGNAC, A., [1] Six propositions arithmologiques déduites du crible d'Eratosthène,

Nouv. Ann. Math. **8** (1849) 423-429.

POLLOCK, F., [1] On the extension of the principle of Fermat's theorem of the polygonal numbers to the higher orders of series whose ultimate differences are constant. With a new theorem proposed, applicable to all the orders, *Proc. Roy. Soc. London* **5** (1851) 922-924.

POLLACK, R.M., và SHAPIRO, H.N, [1] The next to the last case of a factorial diophantine equation,

Comm. Pure Appl. Math. **26** (1973) 313-325.

Polya G. và SzegSG., [1] *Aufgaben und Lehrsatze aus der Analysis*, Bd II (Berlin 1925).

POMERANCE, C, [1] On the congruences $\sigma(n)\equiv a(\mathrm{mod}\, n)$ and $n\equiv a(\mathrm{mod}\,\varphi(n))$,

Acta Arith. **26** (1975) 265-272.

[2] On the distribution of amicable numbers II, *J. Reine Angew. Math*. **325** (1981) 183-188.

[3] On the distribution of pseudoprimes*, Math. Comp*. **37** (1981) 587-593.

[4] A new lower bound for the pseudoprime counting function, *Illinois J. Math*. **26** (1982) 4-9.

POMERANCE,C.,SELFRIDGE,J.L.và WAGSTAFF,S.S.Jr, [1] The pseudoprimes to $25\cdot 10^9$,

Math. Comp. **35** (1980) 1003-1026.

PORGES, A., [1] A set of eight numbers, *Amer. Math. Monthly* **52** (1945) 379-382.

POSTNIKOV, M.M., [1] *Magicheskie kvadraty (MagicSquares*, tiếng Nga) (Moscow 1964).

POULET, P., [1] *La chasse aux nombres, Fasc*. 1 (Bruxelles 1929)

[2] Table de nombres composes vérifiant le théorème de Fermat pour le module 2 jusqu'à 100000000, *Sphinx* **8** (1938) 42-52.

[3] Suites de totalics en départ de $n<2000$, Hectographed copy in possession of

D.H. Lehmer, cf. *Math. Tables Aids Comp*. **3** (1948) 120.
PRACHAR, K., [1] *Primzahlverteilung* (Berlin-Göttingen-Heidelberg 1957, reprint 1978).
PRITCHARD, P.A., [1] Long arithmetic progressions of primes: some old, some new,
Math. Comp. **45** (1985) 263-267.

RADO, R., [1] Some solved and unsolved problems in the theory ofnumbers, *Math. Gaz*. **25** (1941) 72-77.
RAMANUJAN, S., [1] Problem 465, *J. Indian Math. Soc*. **5** (1913) 120.
[2] On the expression of a number in the form $ax^2 + by^2 + cz^2 + du^2$,
Proc. Cambridge Philos. Soc. **19** (1917) 11-21.
RANKIN, R.A, [1] Sets of integers containing no more than a given number of terms in arithmetical progression, *Proc. Royal Soc. Edinburgh Sect*. A **65** (1960/61) 318-331.
REICHARDT, H„ [1] Über die Diophantische Gleichung $ax^4 + bx^2y^2 + cy^4 = ez^2$,
Math.Ann. 117 (1940) 235-276.
RICCI, G., [1] Sull'andamento della differenza di numeri primi consecutivi,
Riv. Mat. Univ. Parma **5** (1954) 3-54.
[2] Sull'insieme dei valori di condensazione de rapporto $\left(p_{n\_1} - p_n\right) / \ln p_n \left(n = 1, 2, 3, , \ldots\right)$
Riv. Mat. Univ. Parma **6** (1955) 353-361.
RICHERT, H.-E., [1] Über Zerlegungen in paarweise verschiedene Zahlen,
Norsk Mat. Tidssk. **31** (1949) 120-122.
[2] Über Zerfällungen in ungleiche Primzahlen, *Math. Z.* **52** (1950) 342-343. te RIELE, HJ.J., [1] New very large amicable pairs, in: *Number Theory, Noordwijkerhout* 1983, (ed H. Jager) Lecture Notes in Mathematics 1068 (Berlin-Heidelberg-NewYork-Tokyo 1984).
[2] *Computation of All Amicable Pairs Below* 10^{10}. Report NM-R8503,
Centrum voor Wiskunde en Informatica (Amsterdam 1985).
RIESEl, H. và Vaughan, R.C., [1] On sums of primes, *Arkiv. Mat*. **21** (1983) 45-74.
ROBINSON, R.M., [1] Mersenne and Fermat numbers, *Proc. Amer. Math. Soc.* **5** (1954) 842-846.
[2] A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers,
Proc. *Amer. Math. Soc*. **9** (1958) 673-681.
de ROCQUIGNY, G., [1] Question 1408, *Intermédiate Math*. **5** (1898) 268.
RÖHR [1] *Zeitschrift Math. NaturW. Unterricht* **50** (1919) 95-96.
ROSE, K., và BRUDNO, S., [1] More about four biquadrates equal one biquadrate,
Math, Comp. **27** (1973) 491-494.
ROSSER, J.B., [1] The $n-$ th prime in greater than $n \log n$, *Proc. London Math. Soc*. (2) **45** (1939) 21-44.
ROSSER, J.B., và SCHOENFELD, L., [1] Approximate formulas for some function of prime numbers,
Illinois J. Math. **6** (1962) 64-89.
[2] Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$ *Math. Comp*. **29** (1975) 243-269.
ROTA, G.C., [1] The number of partitions ofa set, *Amer. Math. Monthly* **71** (1964)498-504.
ROTH, K.F., [1] On certain sets of integers, *J. London Math. Soc*. **28** (1953) 104-109.
ROTKIEWICZ, A., [1] Sur les nombres composés n qui divisent $a^{n-1} - b^{n-1}$.
Rend. Circ. Mat. Palermo (2) **8** (1959) 115-116.
[2] Sur les nombres pairs n pour lesquels les nombres $a^n b - ab^n$, respectivement $a^{n-1} - b^{n-1}$, sont divisible par n, *Rend. Circ. Mat. Palermo* (2) **9** (1959) 341-342.
[3] On the properties of the expression $a^n - b^n$ (in Polish), *Prace Mat.* **6** (1961) 1-20.
[4] Demonstration arithmétique d'existence d'une infinité de nombres premiers de la forme $nk + 1$, *Enseignement Math*. (2) **7** (1962) 277-280.
[5] Sur les nombres pseudopremiers de la forme $ax + b$,
C.R. Acad. Sci. Paris **257** (1963) 2601-2604.
[6] On the pseudoprimes of the form $ax + b$, *Proc. Cambridge Philos. Soc*. **63** (1967) 389-392.
[7] Un problème sur les nombres pseudopremiers, *Indag. Math*. **34** (1972) 86-91.
[8] *Pseudoprime Numbers and Their Generalizations* (Novi Sad 1972).

SALEM, R. và SPENCER, D.C, [1] On sets of integers which contain no three terms
in arithmetical progression, *Proc. Nat. Acad. U.S.A.*, **28** (1942) 561-563.
[2] On sets of integers which do not contain a given number of terms in arithmetical progression,
Nieuw Arch. Wisk. (2) **23** (1952) 133-143.

SALZER, H., [1] On numbers expressible as the sum of four tetrahedral numbers,
J. London Math. Soc. **20** (1945) 3-4.
SALZER, H. và LEVINE, NJ., [1] Tables of integers not exceeding 10000000 that are not expressible as the sum of four tetrahedral numbers, *Math. Tables Aids Comp*. **12** (1958) 141-144.
SANSONE, G. và CASSELS, J.W.S., [1] Sur le problème de M. Werner Mnich, *Acta Arith*. **7** (1962)187-190.
SARDI, S. [1] Sulle somme dei divisori dei numeri*, Giorn. Mat. Battaglini* **7** (1869) 112-116.
SATHE, L.G., [1] On a problem of Hardy on the distribution of integers having a given number of prime factors, *J. Indian Math. Soc*. *N.S*. **17** (1953) 63-141,18 (1954) 27-81.
SCAROWSKY, M. và BOYARSKY, A., [1] A note on the diophantine equation $x^n + y^n + z^n = 3$,
Math. Comp. **41** (1984) 235-237.
SCHERK, H.F., [1] Bemerkungen über die Bildung der Primzahlen aus einander, *J. Relne Angew. Math.* **10** (1833) 201-208.
SCHINZEL, A., [1] Sur la décomposition des nombres naturels en somme de nombres triangulares distincts, *Bull. Acad. Polon. Sci. CI.* **Ill, 2** (1954) 409-410.
[2] Sur une propriété du nombre de diviseurs, *Publ. Math. Debrecen* **2** (1954) 261-262.
[3] Generalization of a theorem of B.S.K.R. Somayajulu on the Euler's function $\varphi(n)$,
Ganita **5** (1954) 123-128.
[4] On the equation $x_1 x_2 \ldots x_n = t^k$ *Bull. Acad. Polon. Sci. CI*. **Ill, 3** (1955) 17-19.
[5] Sur un probleme concernant la fonction φ, *Czechoslovak Math. J.* **6**(1956) 164-165.
[6] Sur l'équation $\varphi(x) = m$, *Elem. Math*. **11** (1956) 75-78.
[7] Sur l'existence d'un cercle passant par un nombre donné de points aux coordonnées entières, *Enseignement Math*. (2) **4** (1958) 71-72.
[8] Sur l'équation $\varphi(x+k) = \varphi(x)$, *Acta Arith.* **4** (1958) 181-184.
[9] Sur les nombres.composes nqui divisent $a^n - a$, *Rend. Circ. Mat. Palermo* (2) **7** (1958) 1-5.
[10] Sur les sommesde trois carrés, *Bull. Acad. Polon, Sci. Sér. Sci. Math. Astr. Phys.***7** (1959)307-309.
[11] Sur une consequence de l'hypothèse de Goldbach,
Bulgar. Akad. N'auk. Izv. Mat. Inst. **4** (1959) 35-38.
[12] Sur l'équation diophantienne $\sum_{k=1}^{n} A_k x_k^{\partial_k} = 0$ (in Polish), *Prace Mat.* **4** (1960) 45-49.
[13] Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers",
Acta Arith. **7** (1961)'1-8.
[14] On the composite integers of the form $c(ak+b)! \pm 1$, *Nordisk Mat. Tidskr*. **10** (1962) 8-10.
SCHINZEL, A. và SIERPINSKI, W., [1] Sur quelques propriétés des fonctions $\varphi(n)$ et $\sigma(n)$,
Bull. Acad. Polon. Sci. CI. Ill, **2** (1954) 463-465.
[2] Sur les sommes de quatre cubes*, Acta Arith*. **4** (1958) 20-30.
[3] Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958),
185-208, and Corrigendum, *ibidem* 5 (1960) 259.
[4] Sur les congruences $x^x \equiv c \pmod m$ et $a^x \equiv b \pmod p$ *Collect. Math*. **11** (1959) 153-164.
SCHINZEL, A. và TIJDEMAN, R., [1] On the equation $y^m = P(x)$ *Acta Arith*. **31** (1976) 199-204.
SCHINZEL, A. et WAKULICZ, A., [1] Sur l'équation $\varphi(x+k) = \varphi(x)$ **II**,*Acta Arith*.**5** (1959) 425-426.
Schmidt, W.M., [1] Über die Normalitat von Zahlen zu verschiedenen Basen, *Acta Arith*. 7 (1962) 299-309.
SCHNIRELMAN, L., [1] Über additive Eigenschaften von Zahlen, *Math. Ann.* **107** (1933) 649-690.
SCHOENBERG, I. J., [1] Über asymptotische Verteilung reeller Zahlen mod 1, *Math. Z*. **28** (1928) 171-200.
SCHOLOMITI, N.C., [1] An expression for the Euler φ -function, *Amer. Math, Monthly* **61** (1954) 36-37.
SCHOLZ, A. và SCHOENBERG, B., [1] *Einführung in die Zahlentheorie* (Berlin 1955).
SCHUR, I, [1] Über die Kongruenz $x^m + y^m \equiv z^m \pmod p$.
Jber. Deutsch. Math. Verein. **25** (1916) Abt. 1, 114-117.
[2] Einige Sätze über Primzahlen mit Anwendung auf Irreduzibilitätsfragen, S-.B.
Preuss. Akad. Whs. Phys. Math. Kl. **23** (1929) 1-24.
SEGAL, S.L., [1] On $\pi(x+y) \le \pi(x) + \pi(y)$ *Trans. Amer. Math. Soc.* **104** (1962) 523-527.

SEGRE, B., [1] A note on arithmetical properties of cubic surfaces, *J. London Math. Soc*. **18** (1943) 24-31.
SELBERG, A., [1] An elementary proof of the prime-number theorem, *Ann. of Math*. (2) **50** (1949) 305-313.
[2] Note on a paper by L.G. Sathe, *J. Indian Math. Soc*, (N.S.) **18** (1953) 83-87.
Selmer, E.S., [1] The Diophantine equation $ax^3+by^3+cz^3=0$, *Acta Math*. **85** (1951) 203-362.
[2] The Diophantine equation $ax^3+by^3+cz^3=0$. Completion of the tables, *Acta Math*. **92** (1954) 191-197.
[3] The rational solutions of the Diophantine equation $\eta^2=\xi^3-D$ for $|D|$, *Math. Scand.* **4** (1956) 281-286.
SELMER, E.S. và NESHEIM, G., [1] Tafel der Zwillingsprimzahlen bis 200000, *Norske Vid. Selsk. Fork* (Trondheim) **15** (1942) 95-98.
SEXTON, C.R., [1] Counts of twin primes less than 100000, *Math. Tables Aids Comp*. **8** (1954) 47-49.
[2] Computo del numero delle coppie di numeri primi gemelli comprese fra 100000 et 1100000, distinte secondo ciffre terminali, *Boll. Un. Mat. Ital.* (3) **10** (1955) 99-101.
[3] Abzählung der Vierlingen von 1000000 bis 2000000, *Am. Österr. Akad. Wiss. Math.-Nat. Kl*. **92** (1955) 236-239.
SHANKS, D. [1] A note on Gaussian twin primes, *Math. Comp*. **14** (1960) 201-203.
SHANKS, D. và WRENCH, W.J., Jr., [1] Calculation of π to 100000 decimals, *Math. Comp*. **16** (1962) 76-99.
[2] Calculation of e to 100000 decimals, deposited in the UMT file, cf. *Math. Comp*. **23** (1969) 679.
SHOREY, T.N., và TUDEMAN, R. [1] New applications of Diophantine approximations to Diophantine equations, *Math. Scand*. **39** (1967) 5-18.
SIERPISINSKI, W., [1] Sur un problène du calcul des fonctions asymptotiques (tiếng Ba Lan), *Prace Mat. Fiz.* **17** (1906) 77-118.
[2] Sur les rapports entre les propriétés fondamentales du symbole de Legendre (tiếng Ba Lan), *C.R. Soc. Sci. Lettr. Varsovie* **2** (1909) 260-273.
[3] Sur quelques algorithmes pour développer les nombres réels en séries (tiếng Ba Lan), *C.R. Soc. Sci. Lettr. Varsovie* **4** (1911) 56-77.
[4] Sur un algorithme pour développer les nombres réels en séries rapidement convergentes, *Bull. Acad. Sci. Cracovie, CI. Sci. Math. Se'rie A,* 1911, 113-117.
[5] Démonstration élementaire d'un théorème de M. Borel sur les nombres absolument normaux et détermination effective d'un tel nombre, *Bull. Soc. Math. France* **45** (1917) 125-132.
[6] Remarque sur une hypothèse des Chinois concernant les nombres $\left(2^n-2\right)/n$, *Colloq. Math*. **1** (1947) 9.
[7] *Dzialania nieslconczone* (*Infinite Operations*, in Polish) (Warszawa-Wroclaw 1948).
[8] Remarques sur la décomposition des nombres en sommes des carrés de nombres impairs, *Colloq. Math.* **2** (1949) 52-53.
[9] Contribution à l'étude des restes cubiques, *Ann. Soc. Polon. Math*. **22** (1949) 269-272.
[10] Un théorème sur les nombres premiers, *Mathematiche (Catania*) **5** (1950) 66-67.
[11] Sur les puissances du nombre 2, *Ann. Soc. Polon. Math*. **23** (1950) 246-251.
[12*] Teoria liczb (Theory of Numbers*, in Polish) Warszawa-Wroclaw 1950.
[13] Une proposition de la géométrie élémentaire équivalente à l'hypothèse du continu, *C.R. Acad. Sci. Paris* **252** (1951) 1046-1047.
[14] Sur une propriété des nombres premiers, *Bull. Soc. Roy. Sci. Liège* **21** (1952) 537-539.
[15] Remarques sur les racines d'une congruence, *Ann. Polon. Math.* **1** (1954) 89-90.
[16] Sur une propriété des nombres naturels, *Ann. Mat. Pura Appl.* (4) **39** (1955) 69-74.
[17] On the equation $3^x+4^y=5^z$ (in Polish), *Wiadom. Mat.* (2) **1** (1955/56) 194-195.
[18] Sur une propriete de la fonction $\varphi(n)$, *Publ. Math. Debrecen* **4** (1956) 184-185.
[19] Sur quelques problemes concernant les points aux coordonnées entières, *Einseignement Math*. (2) **4** (1958) 25-31.
[20] Sur les nombres premiers de la forme n^n+1, *Enseignement Math*. (2) **4** (1958) 211-212.
[21] Sur les ensembles de points aux distances rationelles sirués sur le cercle, *Elem. Math.* **14** (1959) 25-27.
[22] *Cardinal and Ordinal Numbers* (Warszawa 1959).
[23] Sur l'équivalence de deux hypothèses concernant les nombres premiers, *Bulgar, Akad. Nauk. Izv. Mat. Inst.* **4** (1959) 3-6.
[24] Sur les sommes égales des cubes distincts de nombres naturels, *Bulgar. Akad. Nauk. Izv. Mat. Inst.* **4** (1959) 7-9.

[25] Sur les nombres premiers ayant des chiffres initiaux et finals donnés.
Acta Arith. **5** (1959) 265-266.
[26] *Teoria liczb, Cześć II (Theory of Numbers, Part II*, in Polish) (Warszawa 1959).
[27] Sur les nombres dont la somme des diviseurs est une puissance du nombre 2.
The Golden Jubilee Commemoration Volume (1958-59) Part I, 7-9 (Calcutta 1963).
[28] Sur un problème concernant les nombres $k \cdot 2^n + 1$,
Elem. Math. **15** (1960) 73-74, and Corrigendum, *ibidem* **17** (1962) 85.
[29] Sur les nombres impairs admettant une seule décomposition en une somme
de deux carrés de nombres naturels premiers entre eux, *Elem. Math*. **16** (1961) 27-30.
[30] Sur les nombres triangulaires carrés, *Bull. Soc. Roy. Sci. Liege* **30** (1961) 189-194,
and *Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz*. **65** (1961) 1-4.
[31] Démonstration élémentaire d'un théoréme sur les sommes de trois
nombres premiers distincts,
GlasnikMat.-Fiz. Astronom. Drustvo Mat. Fiz. Hrvatske (2) 16(1961) 87-88.
[32] Sur une propriété des nombres triangulaires, *Elem. Math*. **17** (1962) 28.
[33] Sur une propriété des nombres tétraédraux, *Elem. Math*. **17** (1962) 29-30.
[34] Sur quelques conséquences d'une hypothèse de MA. Schinzel,
Bull. Soc. Roy. Sci. Liege **31** (1962) 317-320.
[35] *Pythagorean triangles* (New York 1962).
[36] Sur une propriété des nombres naturels, *Elem. Math*. **19** (1964) 27-29.

SISPANOV, S, [1] On pseudo-prime numbers (in Spanish), *Bol. Mat*. **14** (1941) 99-106.

SKOLEM,T., [1] Unlöbsbarkeit von Gleichungen deren entsprechende Kongruenzfür jeden Modul löbsbar ist,
Avh. Norske Vid. Akad. Oslo I, no **4** (1942).
[2] *Diophantische Gleichungen* (Berlin 1938, reprint New York 1950)
[3] On certain distributions of integers in pairs with given differences*, Math. Scand*. **5** (1957)57-68.

SRINIVASAN, A.K., [1] Practical numbers, *Current Sci*. **17** (1948) 179-180.

STARK, H.M., [1] A complete determination of the complex quadratic fields of class-number one,
Michigan Math. J. **14** (1967) 1-27.
[2] Effective estimates of solutions of some diophantine equations, *Acta Arith*. **24** (1973) 251-259.

STEIGER, F, [1] Über die Grundlosung der Gleichung $a^2 + b^2 + c^2 = d^2$, *Elem. Math*. **11** (1956) 105-108,

STEIN, M.L. và STEIN, P.R. [1] New experimental results on the Goldbach conjecture,
Math. Mag. **38** (1965) 72-80.

STEINHAUS, H., [1] Problem 498 (in Polish), *Matematyka* **10** (1957) No 2, 58.

STEINIG, J., [1] On Euler's idoneal numbers, *Elem. Math*. **21** (1966) 73-88.

STEMMLER, R.M., [1] The ideal Waring theorem for exponents $401-200000$,
Math. Comp. **18** (1964)144-146.

STEPHANOS, G., [1] Sur une propriété remarquable des nombres incommesurables,
Bull. Soc. Math. France **7** (1879) 81-83.

STERN, M.A., [1] Über eine der Theilung von Zahlen ähnliche Untersuchung und deren Anwendung auf die Theorie der quadratischen Reste, *J. Reine Angew. Math*. **61** (1863) 66-94.

STEUERWALD,R.,[l]EinSatz über natürliche Zahlen mit $\sigma(N) = 3N$, *Arch. Math*. **5** (1954) 449-451.

STEWART, B.M., [1] Sums of functions of digits, *Canadian J. Math*. **12** (1960) 374-389.
[2] Sums of distinct divisors, *Amer. J. Math.* **76** (1954) 779-785.

STORCHI, E., [1] Alcuni criteri di divisibilità per i numeri di Mersenne e il carattere 6^{10}, $12^{mo}, 24^{mo}, 48^{mo}$ dell'intero 2, Boll. Un. Mat. Ital. (3) **10** (1955) 363-375.

STRAUSS, E.,[1] Eine Verallgemeinerung der dekadischen Schreibeweise nebst funktionen-Theoretischer Anwendung, *Acta Math.* **11** (1887) 13-18.

SUBBA RAO, K., [1] An interesting property of numbers, *Math. Student* **27** (1959) 57-58.

SWIFT, E., [1] Solution of the problem 213, Amer. *Math. Monthly* **22** (1915) 70-71.

SYLVESTER, JJ., [1] On arithmetical series, *Messenger Math*. **21** (1892) 1-19, 87-120.

SZELE, T., [1] Une généralisation de la congruence de Fermat, *Mat. Tidsskr*. B, 1948, 57-59.

SZEMEREDI, E., [1] On sets of integers containing no k elements in arithmetic progression,
Acta Arith. **27** (1975) 199-245.

TAKADA, J., [1] Computation of cyclic parts of steinhaus problem for power 8,
Math.Seminar notes kobe univ. **7** (1959) 543-546.

TAMURA, Y. và KANADA, Y., [1] Calculation of π to 4196239 decimals based on
Gauss-Legendre algorithm (preprint), *cf. Canadian Math. Bull*. **27** (1984) 443.

TARDY, P., [1] Transformazione di un prodotto di n fattori, *Ann. Sc. Mat. Fb*. **2** (1851) 287-291.

TCHACALOFF, L. et KARANICOLOFF, C, [1] Résolution de l'équation $Ax^m + By^n = z^p$ en nombres rationnels, C.R. *Acad. Sci. Paris* **210** (1940) 281-283.

TEILHET, P.F., [1] Equations indéterminees, *Intérmediate Math*. **12** (1905) 209-210.

TEUFFEL, R., [1] Beweise fur zwei Satze von H.F. Scherk über Primzahlen, *Jber. Deutsch*. *Math. Verein*. **58** (1955) Abt. 1, 43-44.

THUE, A., [1] Suggestions to a method in number theory (tiếng Nauy), *Vid. Sekk.Forhandlinger Kristiania* 1902 No 7.

[2] Über die Unlösbarkeit der Gleichung $ax^2 + bx + c = dy^n$ in grossen ganzen Zahlen x und y, *Arch. Math. Naturvid*. **34** (1917) No 16.

TIETZE, H., [1] Tafel der Primzahl-Zwillinge unter 300000, S.-B. Bayer. *Akad. Wiss. Math. Nat. Kl*. 1947, 57-62.

TUDEMAN, R, [1] On the equation of Catalan, *Acta Arith*. **29** (1976) 197-207.

TROST, E., [1] Aufgabe 79, *Elem. Math*. **6** (1951) 18-19.

[2] Bemerkung zu einem Satz über Mengen von Punkten mit ganzzahligen Entfernungen, *Elem. Math*. **6** (1951) 59-60.

[3] *Primzahlen* (Basel-Stuttgart 1953, 2nd ed. 1968).

TUNNEL, J. B., [1] A classical Diophantine problem and modular forms of weight 3/2, *Invent. Math*. **72** (1983) 323-334.

TURAN, P, [1] Results of number theory in the Soviet Union (in Hungarian), *Mat. Lapok* **1** (1950) 243-266.

TURSKL. S., [1] Décomposition de nombres entiers en sommes de carres de nombres impairs, *Bull. Soc. Roy. Sci. Liège* **2** (1933) 70-71.

UHLER, H.S., [1] Many figure approximations to $\sqrt{2}$ and distribution of digits in $\sqrt{2}$ and $1/\sqrt{2}$, *Proc. Nat. Acad. Sci. USA*. **37** (1951) 63-67.

[2] A brief history of the investigations on Mersenne numbers and the latest immense primes, *Scripta Math*. **18** (1952) 122-131.

[3] On the 16th and 17th perfect numbers, *Scripta Math*. **19** (1953) 128-131.

USPENSKY, J.V. và HEASLET, MA., [1] *Elementary Number Theory* (New York and London 1939)

VAHLEN, Th., [1] Beiträge zu einer additiven Zahlentheorie, *J. Reine Angew. Math*. **112** (1893) 1-36.

VAUGHAN, R.C., [1] On Waring's problem for smaller exponents, *Proc. London Math. Soc*. (3) **52** (1986)445-463.

[2] On Waring's problem for sixth powers, *J. London Math. Soc*. (2) **33** (1986) 227-236.

VEHKA, T, [1] Explicit construction of an admissible set for the conjecture that sometimes $\pi(x+y) > \pi(x) + \pi(y)$, *Notices Amer. Math. Soc*. **26** (1979) A-453.

VIJAYARAGHAVAN, T, [1] The general rational solution of some Diophantine equations of the form $\sum_{r=1}^{k+1} A_p X_p^n = 0$, *Proc. Indian Acad. Sci., Sect.* A, **12** (1940) 284-289. r = l

WAGSTAFF,S.S., Jr., [1] On k -free sequences of integers, *Math. Comp*. **26** (1972) 767-771.

[2] Greatest of the least primes in arithmetic progressions having a given modulus, *Math. Comp*. **33** (1979) 1073-1080.

WAKULICZ, A., [1] On the equation $x^3 + y^3 = 2z^3$, *Colloq. Math.* **5** (1957) 11-15.

WALKER, G.W., [1] Solution of the problem E 985, *Amer. Math. Monthly* **59** (1952) 253.

WALSH, CM, [1] Fermat's Note XIV, *Ann. of Math*. (2) **29** (1928) 412-432.

WARD, M., [1] A type of multiplicative diophantine systems, *Amer. J. Math*. **55** (1933) 67-76.

WATSON, G.L., [1] A proof of the seven-cube theorem, *J. London Math. Soc*. **26** (1951) 153-156.

[2] Sums of eight values of a cubic polynomial, *J. London Math. Soc.* **27** (1952) 217-224.

WATSON, G.N, [1] The problem of the square pyramid, *Messenger Math*. **48** (1918) 1-22.

WEINBERGER, P., [1] Exponents of the class groups of complex quadratic fields, *Acta Arith*. **22** (1972)117-124.

WEINTRAUB, S., [1] a large prime gap, *Math. Comp*. **36** (1981) 279.

WERTHEIM, G., [1] *Anfangsgrilnde der Zahlenlehre* (Braunschweig 1902)

WHITEHEAD, E.G., [1] The Ramsey number $N(3,3,\ 3,\ 3;\ 2)$, *Discrete Mathematics* **4** (1973) 389-396.

WHITTEN, S, [1] Tables of the totient and reduced totient function, Manuscript deposited in UMT file, cf. *Math. Tables Aids Comp*. **4** (1950) 29-31.
WHITWORTH, W.A., [1] *Choice and Chance with One Thousand Exercises* (Cambridge 1901, New York 1951).
van WUNGARDEN, A., [1] A table of partitions into two squares with an application to rational triangles. *Indag. Math*. **12** (1950) 313-325.
WILLEY, M., [1] Solution of the problem E 68, *Amer. Math. Monthly* **41** (1934) 330.
WILLIAMS, H.C. và DUBNER, H., [1] The primality of R 1031, *Math. Comp*. **47** (1986) 703-711.
WIRSING, E., [1] Bemerkung zu der Arbeit über vollkommene Zahlen, *Math. Ann*. **137** (1959) 316-318.
WOJCIK, J., [1] On sums of three squares, *Colloq. Math*. **24** (1971) 117-119.
WUNDERLICH, M., [1] Certain properties of pyramidal and figurate numbers, *Math. Comp*. **16** (1962) 482-486.
[2] On the Gaussian primes on the line $\mathrm{Im}(X)=1$, *Math. Comp*. **27** (1973) 399-400.
YANNEY, B.F., [1] Another definition of amicable numbers and some of their relations to Dickson's amicables, *Amer. Math. Monthly* **30** (1923) 311-315.
YATES, S., [1] Sinkers of titanics, *J. Recreational Math.* **17** (1984/85) 268-274.
YORINAGA, M., [1] Numerical investigation of some equations involving Euler's φ function, Math. *J. Okayama Univ*. **20** (1978) 51-58.
ZAHLEN, J.P., [1] Sur les nombres premiers à une suite d'entiers consécutifs, *Euclides* (Madrid) 8 (1948) 115-121.
ZAJTA, AJ., [1] Solutions of the Diophantine equation $x^4+y^4=z^4+t^4$ *Math. Comp*. **41** (1983) 635-659.
ZARANKIEWICZ, K., [1] On triangular numbers (in Polish), *Matematyka* **2** (1949), No 4,1-7 and No 5, 1-8.

Phụ lục dành cho các chứng minh

BEDOCCHI. E., [1] Nota ad una congettura sui numeri primi, *Riv. Mat. Univ. Parma* (**4**) **11** (1985) 229-236.

DANH SÁCH TRA CỨU CÁC NHÀ TOÁN HỌC

TRA CỨU NHANH CÁC CHỦ ĐỀ

PHỤ LỤC VÀ BỔ SUNG (THÁNG 7 NĂM 1987)

1. Tính tới nay (7/1987) người ta đã tìm ra cặp số nguyên tố sinh đôi lớn hơn cặp số nguyên tố sinh đôi $260497545 \cdot 2^{26625} \pm 1$ là $107570463 \cdot 10^{2250} \pm 1$. Xem bài báo của DUBNER H. Và DUBNER R có tiêu đề: "về sự phát triển trong tính toán số học bằng máy tính điện tử" đăng trên J. Recreational Math. **18** (1985/6), 92-96.

2. Các sai số tốt nhất cho bởi các công thức ước lượng đối với các hàm $T(x)$ trang 144 và $T(x)$ trang 337 được trình bày bởi Iwaniec và Mozzocchi (xem IWANIEC, H. và MOZZOCCHI, C.J On the divisor and circle problems. Preprint). Họ đã chứng minh các sai số không vượt quá $C(\varepsilon) X^{7/22+\varepsilon}$ với X bằng x hoặc n tương ứng, ε là số dương tùy ý và $C(\varepsilon)$ là hằng số chỉ phụ thuộc vào ε.

3. Thông tin trong trang 196 nói rằng các nhà toán học Trung Hoa từ 25 thế kỷ trước đã cho rằng $n \mid 2^n - 2$ chỉ khi n nguyên tố là không chính xác. Thông tin này dựa trên trích dẫn của J.H.Jeans trong Dickson [7] tập 1 trang 91 và một lỗi dịch thuật. Xem NEEDHAM J., *Science and Civilization in China*, tập 3*: Mathematics and the Sciences of the Heavens and the Earth*, Cambridge 1959 trang 54 ghi chú cuối trang. Trích dẫn tài liệu của Dickson trang 196 đúng ra là tài liệu [7] tập 1 trang 91.

4. Bài báo [3] của V.A.Demyanenko được trích dẫn trong trang 93 chứa một lỗi nghiêm trọng, do đó định lý này chưa thể coi là đã được chứng minh. Tuy nhiên nếu $x^x y^y = z^z$ thì mọi ước số nguyên tố của x là ước số của y hoặc mọi ước số nguyên tố của y là ước số của x, xem SCHINZEl A., Sur l'équation diophantienne $x^x y^y = z^z$, Acta Sc. Nat. Univ. Szechuansis **18** (1958), 81-83.