HÀ HUY KHOÁI

# CHUYÊN ĐỀ BỒI DƯỠNG HỌC SINH GIỎI TOÁN TRUNG HỌC PHỔ THÔNG

# SỐ HỌC

NHÀ XUẤT BẢN GIÁO DỤC

# Lời nói đầu

*Số học là một trong những lĩnh vực cổ xưa nhất của Toán học, và cũng là lĩnh vực tồn tại nhiều nhất những bài toán, những giả thuyết chưa có câu trả lời. Trên con đường tìm kiếm lời giải cho những giả thuyết đó, nhiều tư tưởng lớn, nhiều lí thuyết lớn của toán học đã nẩy sinh. Hơn nữa, trong những năm gần đây, Số học không chỉ là một lĩnh vực của toán học lí thuyết, mà còn là lĩnh vực có rất nhiều ứng dụng, đặc biệt trong lĩnh vực bảo mật thông tin. Vì thế, việc trang bị những kiến thức cơ bản về Số học cho học sinh ngay từ trường phổ thông là hết sức cần thiết. Không như nhiều ngành khác của toán học, có rất nhiều thành tựu hiện đại và quan trọng của Số học có thể hiểu được chỉ với những kiến thức phổ thông được nâng cao một bước. Do đó, đây chính là lĩnh vực thuận lợi để đưa học sinh tiếp cận nhanh với khoa học hiện đại. Tuy nhiên, trong chương trình Số học ở trường phổ thông hiện nay, môn Số học chưa được giành nhiều thời gian. Cũng vì thế mà học sinh thường rất lúng túng khi giải các bài toán Số học, đặc biệt là trong các kì thi chọn học sinh giỏi. Tình hình đó đòi hỏi phải có những sách tham khảo về số học cho học sinh, đặc biệt là học sinh giỏi, cũng như sách để làm tài liệu giảng dạy cho giáo viên, nhất là giáo viên các lớp chuyên toán.*

*Hiện nay cũng đã có một số sách tham khảo về Số học cho học sinh. Tuy nhiên, chúng tôi hi vọng rằng, cuốn sách này có thể bổ sung được một số mảng chưa được đề cập đến một cách đầy đủ.*

*Thứ nhất, về mặt lí thuyết, ngoài những kiến thức cơ sở về lí thuyết chia hết, đồng dư, cuốn sách trình bày khá kĩ về một số hàm số học, số hoàn hảo, số Mersenne. Đây là những vấn đề cổ điển và quan trọng của Số học, cũng là những vấn đề đang tìm thấy nhiều ứng dụng trong thực tiễn. Cũng như vậy, lí thuyết các phân số liên tục (Chương 4) không chỉ nhằm để trình bày việc giải phương trình Điôphăng bậc 2 (Chương 5), mà còn nhằm mục tiêu trang bị cho học sinh kiến thức cơ sở về lí thuyết này. Điều đó sẽ có ích cho họ khi tìm hiểu các thuật toán mới nhất về phân tích số nguyên (không trình bày trong sách này), một vấn đề rất thời sự của toán học. Trong Chương 6, các tính chất của dãy số Fibonacci cũng được trình bày khá chi tiết. Ta biết rằng, các số Fibonacci tham gia vào nhiều vấn đề của toán học đến nỗi từ nhiều năm nay, có một tạp chí toán học chỉ chuyên dành nghiên cứu các số Fibonacci.*

*Thứ hai, cuốn sách nhằm cung cấp cho học sinh một nguồn bài tập chọn lọc về Số học. Có tổng cộng khoảng hơn 200 bài tập cuối các chương. Các bài tập cuối mỗi chương nhằm mục tiêu giúp học sinh nắm vững phần lí thuyết đã trình bày trong chương đó. Việc đặt các bài tập cuối chương đã là một gợi ý cho học sinh khi giải các bài tập này. Vì thế, không có phần trả lời hoặc chỉ dẫn giành cho các bài tập cuối chương, mặc dù trong đó có những bài tập không dễ.*

*Phần thứ hai của cuốn sách gồm hơn 100 bài tập, có kèm theo lời giải. Đây là những bài tập tương đối tổng hợp, và để giải chúng, học sinh cần biết vận dụng nhiều phần khác nhau của lí thuyết. Đa số các bài tập trong phần này đều là các bài tập khó, với mức độ gần như các bài tập thường được cho trong các kì thi chọn học sinh giỏi quốc gia và quốc tế (đánh giá theo kinh nghiệm của tác giả). Do khuôn khổ của cuốn sách, tác giả chỉ có thể trình bày lời giải mà không giải thích một điều rất quan trọng là tại sao lại phải giải như vậy. Vì thế, khi đọc phần này, sau khi đã hiểu được bài, học sinh nên cố gắng tự mình trả lời câu hỏi đó. Làm được như vậy, chúng ta học được một phương pháp giải, chứ không chỉ học được cách giải một bài toán cụ thể. Các lời giải cho trong sách này chưa phải là lời giải hay nhất, và độc giả có thể cải tiến để các lời giải ngắn gọn, sáng sủa hơn.*

*Cuốn sách không tránh khỏi những khiếm khuyết. Tác giả mong nhận được ý kiến đóng góp của độc giả, nhất là của các thầy, cô giáo và các em học sinh trực tiếp sử dụng cuốn sách này, để có thể chỉnh lí và hoàn thiện hơn trong lần in sau.*

**HÀ HUY KHOÁI**

# Phần I

# NHỮNG KIẾN THỨC CƠ BẢN

Chương 1.

# LÍ THUYẾT CHIA HẾT

## § 1. NGUYÊN LÍ QUY NẠP TOÁN HỌC

Trước hết, ta nhắc lại tiên đề quan trọng sau đây:

**Tính chất sắp xếp thứ tự tốt.** *Mỗi tập không rỗng các số nguyên dương đều có phần tử bé nhất.*

Dựa vào tiên đề nêu trên, chúng ta chứng minh được nguyên lí quy nạp toán học, là một trong những công cụ hữu hiệu nhất thường dùng khi chứng minh các mệnh đề toán học.

**Nguyên lí quy nạp toán học.** *Giả sử $S$ là tập hợp nào đó các số nguyên dương, chứa số $1$. Khi đó, nếu với mọi $n \in S$, $S$ đều chứa số $n+1$, thì $S$ là tập hợp tất cả các số nguyên dương.*

***Chứng minh.*** Giả sử ngược lại, $S$ không phải là tập hợp tất cả các số nguyên dương. Khi đó, tồn tại những số nguyên dương nào đó không thuộc $S$. Theo nguyên lí sắp thứ tự tốt, vì tập hợp các số nguyên dương không thuộc $S$ là khác rỗng, tồn tại số nguyên dương $n$ nhỏ nhất không thuộc $S$. Theo giả thiết, $n \neq 1$. Do $n > 1$ nên $n-1$ là số nguyên dương nhỏ hơn $n$, nên $n-1 \in S$. Nhưng khi đó, $(n-1)+1 = n \in S$, mâu thuẫn. □

Như vậy, để chứng minh một mệnh đề nào đó đúng với tập hợp số nguyên dương, ta chỉ ra hai điều kiện. Thứ nhất, mệnh đề đúng với $n = 1$. Thứ hai, nếu mệnh đề đúng với số nguyên dương $n$ thì cũng đúng với số nguyên dương $n+1$.

Nguyên lí quy nạp toán học còn có dạng phát biểu thay đổi chút ít như sau.

**Nguyên lí quy nạp toán học thứ hai.** *Giả sử $T$ là tập hợp nào đó các số nguyên dương, chứa $1$. Hơn nữa, $T$ có tính chất : nếu $1, 2, \ldots, k$ thuộc $T$ thì $k+1$ thuộc $T$. Khi đó $T$ là tập hợp tất cả các số nguyên dương.*

***Chứng minh.*** Giả sử $T$ là tập hợp nào đó các số nguyên dương chứa $1$, và nếu $1, 2, \ldots, k$ thuộc $T$ thì $k+1$ cũng thuộc $T$. Giả sử $S$ là tập hợp các số

nguyên dương $n$ sao cho mọi số nguyên dương nhỏ hơn hoặc bằng $n$ đều thuộc $T$. Khi đó, $1 \in S$, và theo giả thiết, nếu $k \in S$ thì $k+1 \in S$. Theo nguyên lí quy nạp, $S$ là tập hợp tất cả các số nguyên dương, và do đó, $T$ cũng là tập hợp tất cả các số nguyên dương.

Nguyên lí quy nạp toán học cho ta một phương pháp để tìm giá trị của các hàm xác định trên tập hợp các số nguyên dương.

**Định nghĩa 1.1.** Ta nói rằng hàm $f$ được xác định một cách *đệ quy* nếu giá trị của $f$ tại 1 đã được cho trước, đồng thời có một quy tắc xác định $f(n+1)$ khi biết $f(n)$.

Các hàm đệ quy có vai trò hết sức quan trọng trong số học, lôgich và khoa học máy tính. Từ nguyên lí quy nạp toán học suy ra rằng, giá trị của hàm đệ quy tại mỗi số nguyên dương được xác định một cách duy nhất. Ví dụ đơn giản nhất của hàm đệ quy là *hàm giai thừa* $f(n) = n!$ được định nghĩa như sau :

$$f(1) = 1 \ ; \ f(n+1) = (n+1)f(n).$$

Ta quy ước $0! = 1$.

Hàm giai thừa được dùng để định nghĩa các *hệ số nhị thức* như sau.

**Định nghĩa 1.2.** Giả sử $m, k$ là các số nguyên không âm. *Hệ số nhị thức* $C_m^k$, cũng thường dùng kí hiệu $\binom{m}{k}$, được định nghĩa bởi hệ thức

$$C_m^k = \frac{m!}{k!(m-k)!}.$$

**Mệnh đề 1.3.** *Giả sử $n$ và $k$ là các số nguyên không âm, $k \leq n$. Khi đó*

*i)* $C_n^0 = C_n^n = 1$,

*ii)* $C_n^k = C_n^{n-k}$.

***Chứng minh.*** Ta có

$$C_n^0 = \frac{n!}{0!n!} = \frac{n!}{n!} = 1,$$

$$C_n^n = \frac{n!}{n!0!} = \frac{n!}{n!} = 1.$$

Để thử lại ii) ta có :

$$C_n^k = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!\big[n-(n-k)\big]!} = C_n^{n-k}. \qquad \square$$

Một tính chất quan trọng của các hệ số nhị thức là đồng nhất thức sau :

**Định lí 1.4.** *Giả sử $n$ và $k$ là các số nguyên dương với $n \geq k$. Khi đó*

$$C_n^k + C_n^{k-1} = C_{n+1}^k.$$

***Chứng minh.*** Ta có

$$\begin{aligned} C_n^k + C_n^{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= \frac{n!(n-k+1)}{k!(n-k+1)!} + \frac{n!k}{k!(n-k+1)!} \\ &= \frac{n!\big[(n-k+1)+k\big]}{k!(n-k+1)!} \\ &= \frac{n!(n+1)}{k!(n-k+1)!} \\ &= \frac{(n+1)!}{k!(n-k+1)!} \\ &= C_{n+1}^k \end{aligned} \qquad \square$$

Định lí 1.4 cho ta một cách xây dựng dễ dàng các số nhị thức bằng *tam giác Pascal*. Trong tam giác này, hệ số nhị thức $C_n^k$ là số thứ $(k+1)$ trong dòng $(n+1)$. Sau đây là chín dòng đầu tiên của tam giác Pascal.

$$\begin{array}{ccccccccccc} & & & & & 1 & & & & & \\ & & & & 1 & & 1 & & & & \\ & & & 1 & & 2 & & 1 & & & \\ & & 1 & & 3 & & 3 & & 1 & & \\ & 1 & & 4 & & 6 & & 4 & & 1 & \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\ & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\ 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 \\ & 1 & & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1 \\ & & & & & \cdots & & & & & \end{array}$$

Hình 1.1. Tam giác Pascal.

Các số ngoài cùng của tam giác là 1. Để có một số bên trong, ta chỉ cần lấy tổng hai số ở hàng trên ở về hai phía của vị trí đang xét.

Các số nhị thức xuất hiện trong định lí nhị thức sau đây.

**Định lí nhị thức.** *Giả sử $x$, $y$ là các biến và $n$ là số nguyên dương. Khi đó :*

$$(x+y)^n = C_n^0 x^n + C_n^1 x^{n-1} y + C_n^2 x^{n-2} y^2 + \cdots + \\ + C_n^{n-2} x^2 y^{n-2} + C_n^{n-1} x y^{n-1} + C_n^n y^n,$$

*tức là*

$$(x+y)^n = \sum_{j=0}^{n} C_n^j x^{n-j} y^j .$$

***Chứng minh.*** Ta sử dụng nguyên lí quy nạp toán học. Do $C_1^1 = C_1^0 = 1$ nên trường hợp $n = 1$ là rõ ràng. Giả sử định lí đúng với $n$, tức là

$$(x+y)^n = \sum_{j=0}^{n} C_n^j x^{n-j} y^j$$

Ta thử lại công thức cho trường hợp $n+1$. Ta có

$$(x+y)^{n+1} = (x+y)^n (x+y) = \left( \sum_{j=0}^{n} C_n^j x^{n-j} y^j \right) (x+y)$$

$$= \sum_{j=0}^{n} C_n^j x^{n-j+1} y^j + \sum_{j=0}^{n} C_n^j x^{n-j} y^{j+1} .$$

Mặt khác,

$$\sum_{j=0}^{n} C_n^j x^{n-j+1} y^j = x^{n+1} + \sum_{j=1}^{n} C_n^j x^{n-j+1} y^j ,$$

$$\sum_{j=0}^{n} C_n^j x^{n-j} y^{j+1} = \sum_{j=0}^{n-1} C_n^j x^{n-j} y^{j+1} + y^{n+1} = \sum_{j=1}^{n} C_n^{j-1} x^{n-j+1} y^j + y^{n+1}.$$

Từ đó ta có :

$$(x+y)^{n+1} = x^{n+1} + \sum_{j=1}^{n} \left( C_n^j + C_n^{j-1} \right) x^{n-j+1} y^j + y^{n+1}.$$

Áp dụng định lí 1.4 ta nhận được :

$$(x+y)^{n+1} = x^{n+1} + \sum_{j=1}^{n} C_{n+1}^j x^{n-j+1} y^j + y^{n+1} = \sum_{j=0}^{n+1} C_{n+1}^j x^{n+1-j} y^j . \quad \square$$

## § 2. TÍNH CHIA HẾT

**Định nghĩa 1.5.** Giả sử $a$, $b$ là các số nguyên. Ta nói $a$ *chia hết* $b$ (hay $b$ chia hết cho $a$) nếu tồn tại số nguyên $c$ sao cho $b = ac$.

Nếu $a$ chia hết $b$, ta thường dùng kí hiệu $a \mid b$ hoặc $b \vdots a$, nếu $a$ không chia hết $b$, ta viết $a \nmid b$ hoặc $b \not\vdots a$. Khi $a \mid b$, ta nói $a$ là *ước* của $b$.

**Mệnh đề 1.6.** *Giả sử $a$, $b$, $c$ là các số nguyên. Nếu $a \mid b$, $b \mid c$ thì $a \mid c$.*

**Mệnh đề 1.7.** *Giả sử $a$, $b$, $c$, $m$ và $n$ là các số nguyên. Nếu $c \mid a$ và $c \mid b$ thì $c \mid (ma + nb)$.*

Chứng minh các Mệnh đề 1.6 và 1.7 được dành cho độc giả.

**Thuật toán chia.** Giả sử $a$, $b$ là các số nguyên và $b > 0$. Khi đó tồn tại duy nhất các số nguyên $q$ và $r$ sao cho

$$a = bq + r, \quad 0 \le r < b.$$

Ta gọi $q$ là *thương* và $r$ là *phần dư*. Như vậy, $a$ chia hết cho $b$ nếu và chỉ nếu phần dư trong phép chia bằng $0$. Để chứng minh thuật toán chia, ta cần đến định nghĩa sau.

**Định nghĩa 1.8.** Giả sử $x$ là một số thực. *Phần nguyên* của $x$, kí hiệu qua $[x]$, là số nguyên lớn nhất không vượt quá $x$.

***Ví dụ :*** $[1,5] = 1$; $[-2,4] = -3$; $[11] = 11$.

**Mệnh đề 1.9.** *Với mọi số thực $x$,*

$$x - 1 < [x] \le x.$$

Mệnh đề 1.9 suy ra ngay từ định nghĩa.

***Chứng minh thuật toán chia.*** Chú ý rằng, trong chứng minh, ta sẽ cho công thức tính thương và phần dư.

Giả sử $q = [a/b]$, $r = a - b[a/b]$. Rõ ràng $a = bq + r$. Theo Mệnh đề 1.9 ta có

$$\frac{a}{b} - 1 < [a/b] \le \frac{a}{b}.$$

Từ đó,

$$a - b < a[a/b] \le a,$$

suy ra

$$0 \le r = a - b[a/b] < b.$$

Như vậy, $r$ thỏa mãn tính chất đòi hỏi trong thuật toán chia.

Còn phải chứng minh $q$ và $r$ được xác định một cách duy nhất. Giả sử ta có $a = bq_1 + r_1$ và $a = bq_2 + r_2$, trong đó $0 \le r_1 < b$ ; $0 \le r_2 < b$. Trừ từng vế ta nhận được

$$0 = b(q_1 - q_2) + (r_1 - r_2).$$

Suy ra

$$r_2 - r_1 = b(q_1 - q_2).$$

Như vậy $b \mid (r_2 - r_1)$. Vì $0 \le r_1 < b$ ; $0 \le r_2 < b$ nên $-b < r_2 - r_1 < b$. Do đó $b \mid (r_2 - r_1)$ nếu và chỉ nếu $r_2 - r_1 = 0$, tức là $r_1 = r_2$. Suy ra $q_1 = q_2$. □

## § 3. BIỂU DIỄN SỐ NGUYÊN

Ta thường quen biểu diễn một số nguyên qua tổng các lũy thừa của 10. Thật ra không có lí do đặc biệt nào quyết định việc đó (ngoài việc ta có 10 ngón tay !) Cũng có nhiều dân tộc dùng những hệ đếm khác : người Babilon dùng cơ số 60, người Maia dùng cơ số 12, ... Máy tính điện tử thường dùng cơ số 2, 8 hoặc 16.

Trong tiết này ta sẽ chứng tỏ rằng mọi số nguyên dương lớn hơn 1 đều có thể dùng làm cơ số.

**Định lí 1.10.** *Giả sử $b$ là số nguyên và $b > 1$. Khi đó mọi số nguyên dương $n$ đều có thể viết một cách duy nhất dưới dạng*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0,$$

*trong đó $a_j$ là số nguyên, $0 \le a_j \le b_1$ với $j = 0, \ldots, k$, đồng thời $a_k \ne 0$.*

***Chứng minh***. Ta áp dụng liên tiếp thuật toán chia. Trước tiên chia $n$ cho $b$, ta được :

$$n = bq_0 + a_0, \quad 0 \le a_0 \le b - 1.$$

Lại chia $q_0$ cho $b$, ta có :

$$q_0 = bq_1 + a_1, \quad 0 \le a_1 \le b - 1.$$

Tiếp tục quá trình trên, ta nhận được :

$$
\begin{aligned}
q_1 &= bq_2 + a_2, && 0 \le a_2 \le b-1,\\
q_2 &= bq_3 + a_3, && 0 \le a_3 \le b-1,\\
&\cdots\\
q_{k-2} &= bq_{k-1} + a_{k-1}, && 0 \le a_{k-1} \le b-1,\\
q_{k-1} &= b.0 + a_k, && 0 \le a_k \le b-1.
\end{aligned}
$$

Quá trình kết thúc khi ta có thương bằng $0$. Điều đó đạt được sau hữu hạn bước, vì

$$n > q_0 > q_1 > q_2 > \cdots \ge 0,$$

và mọi dãy giảm các số nguyên không âm nhất định dừng ở $0$ sau hữu hạn bước.

Như vậy ta có :

$$
\begin{aligned}
n = bq_0 + a_0 &= b(bq_1 + a_1) + a_0 = b^2q_1 + a_1b + a_0\\
&= b^3q_2 + a_2b^2 + a_1b + a_0\\
&= \cdots\\
&= a_kb^k + a_{k-1}b^{k-1} + \cdots + a_1b + a_0,
\end{aligned}
$$

trong đó $0 \le a_j \le b-1$ với $j = 0, 1, \ldots, k$ ; $a_k \ne 0$ (do $a_k = q_{k-1}$ là thương khác $0$ cuối cùng).

Để chứng minh biểu diễn nói trên là duy nhất, ta giả thiết rằng có hai biểu diễn của $n$ :

$$
\begin{aligned}
n &= a_kb^k + a_{k-1}b^{k-1} + \cdots + a_1b + a_0\\
&= c_kb^k + c_{k-1}b^{k-1} + \cdots + c_1b + c_0,
\end{aligned}
$$

trong đó $0 \le a_k < b$ ; $0 \le c_k < b$ (nếu cần, ta thêm vào phía trước một trong hai biểu diễn các hệ số $0$ để số từ trong hai biểu diễn như nhau). Ta có:

$$(a_k - c_k)b^k + (a_{k-1} - c_{k-1})b^{k-1} + \cdots + (a_1 - c_1)b + (a_0 - c_0) = 0.$$

Nếu hai biểu diễn khác nhau thì tồn tại số $j$ nguyên nhỏ nhất, $0 \le j \le k$ sao cho $a_j \ne c_j$. Khi đó

$$b^j\left[(a_k - c_k)b^{k-j} + \cdots + (a_j - c_j)\right] = 0,$$

suy ra

$$(a_k - c_k)b^{k-j} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j) = 0.$$

Do đó

$$a_j - c_j = b\left[(c_k - a_k)b^{k-j-1} + \cdots + (c_{j+1} - a_{j+1})\right],$$

tức là $b \mid (a_j - c_j)$. Nhưng $0 \le a_j < b$ ; $0 \le c_j < b$ nên $-b < a_j - c_j < b$. Do đó $b \mid (a_j - c_j)$ chỉ khi $a_j = c_j$, mâu thuẫn với giả thiết. □

Biểu diễn số $n$ như trong Định lí 1.10 được gọi là biểu diễn *trong cơ số* $b$. Khi $b = 2$, ta thường gọi là *biểu diễn nhị phân*, $b = 10$: *biểu diễn thập phân*. Các hệ số $a_j$ được gọi là các *chữ số* của biểu diễn. Để phân biệt các biểu diễn số nguyên trong các cơ số khác nhau, ta viết $(a_k a_{k-1}, \ldots, a_1 a_0)_b$ thay cho $a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$.

## § 4. SỐ NGUYÊN TỐ

Số 1 chỉ có đúng một ước dương. Mỗi số nguyên dương khác đều có ít nhất hai ước dương (chẳng hạn, 1 và chính nó). Các số nguyên dương chỉ có đúng hai ước dương là các số quan trọng nhất trong số học, chúng được gọi là *số nguyên tố*.

**Định nghĩa 1.11.** Số *nguyên tố* là số nguyên dương lớn hơn 1 chỉ chia hết cho 1 và chính nó.

**Định nghĩa 1.12.** Số nguyên dương khác 1 và không là số nguyên tố được gọi là *hợp số*.

***Ví dụ :*** 2, 3, 5, 7, 11 là các số nguyên tố ; 4, 6, 9, 12, 115 là các hợp số. Tồn tại rất nhiều giả thuyết lớn của toán học liên quan đến các số nguyên tố. Ở đây ta chỉ xét một vài tính chất thường được sử dụng.

**Bổ đề 1.13.** *Mỗi số nguyên dương lớn hơn* 1 *đều có ước nguyên tố.*

***Chứng minh.*** Giả sử ngược lại, tồn tại số nguyên dương không có ước nguyên tố nào. Vì tập hợp các số như vậy, theo giả thiết phản chứng, là không rỗng, nên từ nguyên lí sắp xếp thứ tự tốt suy ra rằng, tồn tại số nguyên dương $n$ bé nhất không có ước nguyên tố. Vì $n$ là ước của chính nó, mà theo giả thiết, $n$ không có ước nguyên tố, nên $n$ không phải là số nguyên tố. Ta có $n = ab$, $1 < a < n$, $1 < b < n$. Vì $a < n$ nên $a$ phải có ước nguyên tố. Theo Mệnh đề 1.6, mọi ước của $a$ đều là ước của $n$, nên $n$ có ước nguyên tố : mâu thuẫn. □

**Định lí 1.14.** *Tồn tại vô hạn số nguyên tố.*

***Chứng minh.*** Xét số

$$Q_n = n! + 1, \quad n \geq 1.$$

Khi đó $Q_n$ có ít nhất một ước nguyên tố, kí hiệu qua $q_n$. Nếu $q_n \leq n$ thì $q_n \mid n!$, và do đó $q_n \mid (Q_n - n!) = 1$, mâu thuẫn. Vậy $q_n > n$. Như vậy, với mọi số nguyên dương $n$, đều có số nguyên tố lớn hơn $n$, nên tập hợp các số nguyên tố là vô hạn. □

Trong nhiều vấn đề ứng dụng, chẳng hạn trong việc xây dựng các hệ mật mã khóa công khai, người ta cần tìm những số nguyên tố rất lớn. Định lí sau đây chỉ ra rằng, bằng cách chia $n$ cho các số nguyên tố không vượt quá $\sqrt{n}$, ta xác định được $n$ có là số nguyên tố hay không.

**Định lí 1.15.** *Nếu $n$ là một hợp số, thì $n$ có ước nguyên tố không vượt quá $\sqrt{n}$.*

***Chứng minh.*** Do $n$ là hợp số, $n = ab$, trong đó $a$, $b$ là các số nguyên, $1 < a \leq b < n$. Ta phải có $a \leq \sqrt{n}$, vì nếu ngược lại thì $ab > \sqrt{n}.\sqrt{n} = n$. Vì $a$ có ước nguyên tố, ước này cũng là ước của $n$, nên $n$ có ước nguyên tố không vượt quá $\sqrt{n}$.

Ta có thể dùng Định lí 1.15 để tìm tất cả các số nguyên tố không vượt quá một số nguyên dương $n$ cho trước. Để minh họa, ta xét trường hợp $n = 100$. Theo Định lí 1.15, mỗi hợp số nhỏ hơn 100 phải có một ước nguyên tố nhỏ hơn 10, tức là phải chia hết cho ít nhất một trong các số 2, 3, 5 hoặc 7.

Trước tiên, trong các số từ 1 đến 100, ta gạch đi các số chia hết cho 2. Sau đó trong những số còn lại, bỏ đi các số chia hết cho 3, rồi lại bỏ đi các số chia hết cho 5, cho 7. Các số còn lại (trừ số 1) là các số nguyên tố. Quá trình mô tả trên đây được gọi là *sàng Eratosthenes*.

Sàng Eratosthenes có vẻ như là một cách rất đơn giản để tìm tất cả các số nguyên tố. Tuy nhiên, vì số phép chia cần làm trong quá trình này rất lớn nên trên thực tế, không thể tìm được các số nguyên tố lớn theo cách nêu trên. Để ước lượng được thời gian cần thiết để tìm được một số nguyên tố lớn, người ta cần tìm hiểu về *phân bố các số nguyên tố*. Đó là một trong những bài toán lớn của toán học. Định lí sau đây, được gọi là *Định lí số nguyên tố*, là một trong những định lí nổi tiếng nhất của số học :

**Định lí 1.16.** *Kí hiệu qua $\pi(x)$, với $x$ là số thực dương, số các số nguyên tố không vượt quá $x$. Khi đó*

$$\lim_{x \to \infty} \pi(x) \Big/ \frac{x}{\ln x} = 1.$$

Định lí số nguyên tố được phát biểu bởi K. Gauss năm 1793 và chỉ được

chứng minh sau đó hơn 100 năm, vào năm 1896, bởi J. Hadamard và C. I. de la Vallée-Poussin. Chứng minh của Định lí vượt ra ngoài khuôn khổ cuốn sách này.

Các số nguyên tố được phân bố rất phức tạp. Có những cặp số nguyên tố "sinh đôi" như $(3, 5)$, $(11, 13)$, $(17, 19)$, ... (người ta chưa biết có hữu hạn hay vô hạn cặp như vậy). Tuy vậy, hai số nguyên tố liên tiếp có thể "xa nhau" tùy ý, theo định lí sau đây.

**Định lí 1.17.** *Với mọi số nguyên dương $n$, tồn tại ít nhất $n$ số liên tiếp, mà mỗi một trong chúng đều là hợp số.*

***Chứng minh.*** Xét dãy các số nguyên liên tiếp

$$(n+1)! + 2,\ (n+1)! + 3,\ \ldots,\ (n+1)! + (n+1).$$

Khi $2 \le j \le n+1$, $j \mid (n+1)!$ nên $j \mid (n+1)! + j$. Vậy các số trong dãy nói trên đều là hợp số.

Một trong những giả thuyết nổi tiếng nhất của số học (chưa được chứng minh hay bác bỏ) là giả thuyết sau đây về số nguyên tố.

**Giả thuyết Goldbach.** *Mỗi số nguyên dương chẵn lớn hơn hai đều có thể viết dưới dạng tổng hai số nguyên tố.*

Giả thuyết trên được nêu lên trong bức thư của Goldbach gửi Ơ-le năm 1742.

## § 5. ƯỚC CHUNG LỚN NHẤT. THUẬT TOÁN Ơ-CLÍT

### 5.1. ƯỚC CHUNG LỚN NHẤT

Nếu $a$, $b$ là các số nguyên không đồng thời bằng $0$ thì tập hợp các ước chung của $a$, $b$ là tập hợp hữu hạn (chứa $\pm 1$).

**Định nghĩa 1.18.** Ước chung lớn nhất của hai số $a$ và $b$ không đồng thời bằng $0$ là số nguyên lớn nhất chia hết cả $a$ và $b$.

Ta dùng kí hiệu $(a, b)$ để chỉ ước chung lớn nhất của $a$ và $b$.

Ta đặc biệt quan tâm đến trường hợp hai số nguyên không có ước chung nào lớn hơn $1$.

**Định nghĩa 1.19.** Các số nguyên $a$ và $b$ được gọi là *nguyên tố cùng nhau* nếu $(a, b) = 1$.

Chú ý rằng, $(a, b) = (|a|, |b|)$, nên ta chỉ cần quan tâm đến ước chung lớn nhất của các số nguyên dương. Sau đây là một số tính chất của ước chung lớn nhất.

**Mệnh đề 1.20.** *Giả sử $a$, $b$, $c$ là các số nguyên, $(a, b) = d$. Khi đó ta có :*

*i)* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$,

*ii)* $(a + cb, b) = (a, b)$.

***Chứng minh.*** i) Giả sử $a$ và $b$ là các số nguyên và $(a, b) = 1$. Giả sử $e$ là một ước chung dương của $a/d$ và $b/d$ : $e \mid (a/d)$, $e \mid (b/d)$. Khi đó tồn tại các số nguyên $k$ và $l$ sao cho $\frac{a}{d} = ke$, $\frac{b}{d} = le$, tức là $a = dek$, $b = del$. Do đó, $de$ là ước chung của $a$ và $b$. Vì $d$ là ước chung lớn nhất của $a$ và $b$ nên $e = 1$. Vậy $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

ii) Giả sử $a$, $b$, $c$ là các số nguyên. Ta sẽ chỉ ra rằng, các ước chung của $a$ và $b$ hoàn toàn trùng với các ước chung của $a + cb$ và $b$, từ đó suy ra $(a + cb, b) = (a, b)$. Giả sử $e$ là một ước chung của $a$ và $b$. Do Mệnh đề 1.7, $e \mid (a + cb)$, nên $e$ là ước chung của $a + cb$ và $b$. Ngược lại, giả sử $f$ là ước chung của $a + cb$ và $b$. Khi đó, $f \mid [(a + cb) - cb]$, tức là $f \mid a$. Vậy $f$ là ước chung của $a$ và $b$. □

Ta sẽ chứng tỏ rằng, ước chung lớn nhất của các số nguyên $a$ và $b$ (không đồng thời bằng $0$) có thể viết dưới dạng tổng các bội của $a$ và $b$.

**Định nghĩa 1.21.** Nếu $a$ và $b$ là các số nguyên, thì *tổ hợp tuyến tính* của $a$ và $b$ là một tổng có dạng $ma + nb$, trong đó $m$, $n$ là các số nguyên.

**Định lí 1.22.** *Ước chung lớn nhất của các số nguyên $a$ và $b$ không đồng thời bằng $0$ là số nguyên dương nhỏ nhất biểu diễn được bởi một tổ hợp tuyến tính của $a$ và $b$.*

***Chứng minh.*** Giả sử $d$ là số nguyên dương nhỏ nhất biểu diễn bởi một tổ hợp tuyến tính của $a$ và $b$. Số nhỏ nhất như vậy tồn tại theo tính chất sắp thứ tự tốt, vì có một trong hai tổ hợp tuyến tính $1.a + 0.b$ và $(-1).a + 0.b$ ($a \neq 0$) là số dương. Giả sử

$$d = ma + nb, \tag{1}$$

trong đó $m$, $n$ là các số nguyên. Ta chỉ ra rằng, $d \mid a$ và $d \mid b$. Do thuật toán chia, ta có

$$a = dq + r, \quad 0 \leq r < d. \tag{2}$$

Từ (1) và (2) ta được

$$r = a - dq = a - q(ma + nb) = (1 - qm)a - qnb.$$

Như vậy, $r$ cũng là một tổ hợp tuyến tính của $a$ và $b$. Vì $0 \leq r < d$, mà $d$ là tổ hợp tuyến tính dương nhỏ nhất của $a$ và $b$ nên $r = 0$, tức là $d \mid a$. Tương tự, $d \mid b$.

Bây giờ ta chứng tỏ $d$ là ước chung lớn nhất của $a$ và $b$. Giả sử $c$ là một ước chung tùy ý của $a$ và $b$. Do $c \mid a$ và $c \mid b$ nên theo Mệnh đề 1.7, $c \mid d$. □

**Hệ quả 1.23.** *Hai số nguyên $a$ và $b$ nguyên tố cùng nhau khi và chỉ khi tồn tại các số nguyên $m$ và $n$ sao cho*

$$ma + nb = 1.$$

Ta cũng có thể xét ước chung lớn nhất của nhiều số nguyên.

**Định nghĩa 1.24.** Giả sử $a_1, a_2, \ldots, a_n$ là các số nguyên không đồng thời bằng $0$. *Ước chung lớn nhất* của các số đó là số nguyên lớn nhất mà là ước chung của các số đã cho. Ta kí hiệu ước chung lớn nhất qua $(a_1, a_2, \ldots, a_n)$.

**Bổ đề 1.25.** *Giả sử $a_1, a_2, \ldots, a_n$ là các số nguyên, không đồng thời bằng $0$. Khi đó*

$$(a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, (a_{n-1}, a_n)).$$

***Chứng minh.*** Mọi ước chung của $n$ số nguyên $a_1, a_2, \ldots, a_{n-1}, a_n$ đều là ước của $a_{n-1}$ và $a_n$, nên là ước của $(a_{n-1}, a_n)$. Ngược lại, mọi ước chung của $a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n)$ là ước chung của $n$ số $a_1, a_2, \ldots, a_{n-1}, a_n$. Từ đó suy ra Bổ đề.

**Định nghĩa 1.26.** Ta nói rằng các số nguyên $a_1, a_2, \ldots, a_n$ là *nguyên tố cùng nhau đồng thời* nếu $(a_1, a_2, \ldots, a_n) = 1$. Các số nguyên đó là *nguyên tố cùng nhau từng đôi một* nếu với mọi cặp $a_i$, $a_j$ trong tập hợp, ta có $(a_i, a_j) = 1$.

Rõ ràng tập hợp nào đó các số nguyên tố cùng nhau từng đôi sẽ là nguyên tố cùng nhau đồng thời. Ngược lại không đúng. Ví dụ : $(9, 3, 2, 4) = 1$, tuy nhiên $(9, 3) = 3$, $(2, 4) = 2$.

## 5.2. THUẬT TOÁN Ơ-CLÍT

Trong mục này, ta sẽ nghiên cứu một phương pháp, hay *thuật toán*, để tìm ước chung lớn nhất của hai số nguyên dương. Thuật toán này gọi là thuật toán Ơ-clít, và có lẽ là thuật toán cổ nhất của toán học (được biết đến cách đây khoảng 2000 năm).

**Thuật toán Ơ-clít.** *Giả sử* $r_0 = a$, $r_1 = b$ *là các số nguyên không âm,* $b \neq 0$. *Ta áp dụng liên tiếp thuật toán chia*

$$r_j = r_{j+1}q_{j+1} + r_{j+2},$$

*với* $0 < r_{j+2} < r_{j+1}$, $j = 0, 1, 2, \ldots, n-2$, $r_n = 0$. *Khi đó* $(a, b) = r_{n-1}$ *(phần dư khác* $0$ *cuối cùng của phép chia).*

Để chứng minh rằng thuật toán Ơ-clít cho ta ước chung lớn nhất, trước tiên ta chứng minh bổ đề sau.

**Bổ đề 1.27.** *Giả sử* $c$ *và* $d$ *là các số nguyên, đồng thời* $c = dq + r$, *trong đó* $q$ *và* $r$ *là các số nguyên. Khi đó*

$$(c, d) = (d, r).$$

**Chứng minh.** Giả sử $e$ là một ước chung của $c$ và $d$, khi đó $e \mid r$. Ngược lại, nếu $e \mid d$, $e \mid r$ thì $e \mid c$. Như vậy, các ước chung của $c$ và $d$ trùng với các ước chung của $d$ và $r$, nên $(c, d) = (d, r)$. □

Bây giờ ta xét thuật toán Ơ-clít. Giả sử $r_0 = a$, $r_1 = b$ là các số nguyên dương với $a \geq b$. Bằng cách áp dụng liên tiếp thuật toán chia, ta được

$$\begin{aligned}
r_0 &= r_1q_1 + r_2, && 0 \leq r_2 < r_1\\
r_1 &= r_2q_2 + r_3, && 0 \leq r_3 < r_2\\
&\cdots\\
r_{n-3} &= r_{n-2}q_{n-2} + r_{n-1}, && 0 \leq r_{n-1} < r_{n-2}\\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, && 0 \leq r_n < r_{n-1}\\
r_{n-1} &= r_nq_n.
\end{aligned}$$

Chú ý rằng, ta đi đến phép chia với phần dư $0$ sau hữu hạn bước, vì

$$a = r_0 > r_1 > r_2 > \cdots \geq 0.$$

Do Bổ đề 1.27, $(a,b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n$. Vậy $(a,b) = r_n$, phần dư khác không cuối cùng. □

## § 6. ĐỊNH LÍ CƠ BẢN CỦA SỐ HỌC

Định lí sau đây là một trong những định lí quan trọng nhất của Số học (và của Toán học), nó cho thấy các số nguyên tố là nền tảng để xây dựng nên các số nguyên.

**Định lí.** *Mọi số nguyên dương đều biểu diễn được một cách duy nhất dưới dạng tích các số nguyên tố, trong đó các thừa số nguyên tố được viết theo thứ tự không giảm.*

Ví dụ : $2000 = 2.2.2.2.5.5.5 = 2^4.5^3$.

Để thuận tiện, ta thường nhóm các thừa số nguyên tố bằng nhau thành một lũy thừa của nó. Cách biểu diễn số nguyên như vậy được gọi là *phân tích thành lũy thừa nguyên tố.*

Để chứng minh Định lí cơ bản của số học, ta cần bổ đề sau.

**Bổ đề 1.28.** *Giả sử* $a$, $b$, $c$ *là các số nguyên dương, đồng thời* $(a,b) = 1$, $a \mid bc$. *Khi đó* $a \mid c$.

***Chứng minh.*** Vì $(a,b) = 1$ nên tồn tại các số nguyên $x, y$ sao cho $ax + by = 1$. Nhân hai vế của phương trình này với $c$, ta có $acx + bcy = c$. Ta thấy $a \mid (acx + bcy)$, vì đó là một tổ hợp tuyến tính của $a$ và $bc$. Do đó $a \mid c$. □

**Hệ quả 1.29.** *Nếu* $p \mid a_1 a_2, \ldots, a_n$, *trong đó* $p$ *là số nguyên tố và* $a_1, a_2, \ldots, a_n$ *là các số nguyên dương, thì tồn tại* $i$, $1 \leq i \leq n$ *sao cho* $p \mid a_i$.

***Chứng minh.*** Ta chứng minh bằng quy nạp. Trường hợp $n = 1$ là hiển nhiên. Giả sử mệnh đề đúng với $n$. Xét tích $n+1$ số nguyên, $a_1 \ldots a_{n+1}$ và giả sử $p \mid a_1 \ldots a_{n+1}$. Khi đó $p \mid (a_1 \ldots a_n) a_{n+1}$, nên theo Bổ đề 1.28, $p \mid a_1 \ldots a_n$ hoặc $p \mid a_{n+1}$. Nếu $p \mid a_1 \ldots a_n$ thì theo giả thiết quy nạp tồn tại $i$i, $1 \leq i \leq n$ sao cho $p \mid a_i$. Do đó $p \mid a_i$ với $i$ nào đó, $1 \leq i \leq n+1$. □

Ta chuyển sang chứng minh Định lí cơ bản của số học. Trước hết ta chứng tỏ rằng mỗi số nguyên dương đều có thể viết dưới dạng tích các số nguyên tố, ít nhất là bằng một cách. Giả sử ngược lại, tồn tại các số nguyên dương không có tính chất trên. Gọi $n$ là số bé nhất trong các số đó. Nếu $n$

là số nguyên tố thì hiển nhiên nó biểu diễn được dưới dạng tích các số nguyên tố (ở đây tích chỉ gồm một phần tử). Như vậy, $n$ là hợp số. Đặt $n = ab$, với $1 < a < n$ và $1 < b < n$. Nhưng vì $a$ và $b$ nhỏ hơn $n$ nên chúng phải là tích các số nguyên tố, và do đó, $n$ cũng là tích các số nguyên tố. Mâu thuẫn này chứng minh rằng số nguyên tùy ý biểu diễn được dưới dạng tích các số nguyên tố.

Ta chứng minh biểu diễn nói trên là duy nhất. Giả sử tồn tại số nguyên dương có hơn một cách biểu diễn. Gọi $n$ là số nguyên dương nhỏ nhất trong các số đó, và $n$ có hai cách biểu diễn :

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t,$$

trong đó $p_1, p_2, \ldots, p_s$, $q_1, q_2, \ldots, q_t$ đều là các số nguyên tố, $p_1 \le p_2 \le \cdots \le p_s$ và $q_1 \le q_2 \le \cdots \le q_t$. Trước tiên ta sẽ chỉ ra rằng $p_1 = q_1$. Giả sử $p_1 \ne q_1$. Không giảm tổng quát, có thể giả thiết $p_1 < q_1$. Như vậy, $p_1 < q_i$ với mọi $i = 1, 2, \ldots, t$ (vì các số nguyên tố trong mỗi biểu diễn được xếp theo thứ tự không giảm). Khi đó, $p_1 \nmid q_i$ với mọi $i$. Theo Hệ quả 1.29, $p_1 \nmid q_1 \ldots q_t = n$ : vô lí. Vậy $p_1 = q_1$ và $n / p_1 = p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_t$. Vì $n / p_1$ là số nguyên dương nhỏ hơn $n$, mà $n$ là số nguyên dương nhỏ nhất có quá một biểu diễn, nên $n / p_1$ chỉ có thể biểu diễn dạng tích các số nguyên tố theo một cách duy nhất. Như vậy, $s = t$ và $q_i = p_i$ với mọi $i$. Định lí được chứng minh. □

Bây giờ ta chỉ ra cách dùng Định lí cơ bản để tìm ước chung lớn nhất. Giả sử các số $a$ và $b$ có phân tích thành thừa số nguyên tố như sau :

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n} \quad ; \quad b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n},$$

trong đó mỗi số mũ là số nguyên không âm, và mỗi số nguyên tố xuất hiện ở ít nhất một trong hai phân tích của $a$ và $b$ đều được đưa vào cả hai tích, có thể với số mũ $0$. Khi đó ta có

$$(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \ldots p_n^{\min(a_n, b_n)}$$

vì với mỗi số nguyên tố $p_i$, $a$ và $b$ cùng chia hết cho lũy thừa $\min(a_i, b_i)$ của $p_i$, và đó là lũy thừa cao nhất có thể.

Phân tích ra thừa số nguyên tố cũng được dùng để tìm bội chung nhỏ nhất của các số nguyên dương.

**Định nghĩa.** *Bội chung nhỏ nhất* của hai số nguyên dương $a$ và $b$ là số nguyên dương nhỏ nhất chia hết cho $a$ và $b$.

Ta thường dùng kí hiệu $[a, b]$ để chỉ bội chung nhỏ nhất của $a$ và $b$.

***Ví dụ :*** $[24,10] = 120$.

Khi biết phân tích ra thừa số của các số $a$ và $b$, ta dễ dàng tìm được $[a, b]$. Giả sử

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \quad ; \quad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n},$$

trong đó $p_1, p_2, \dots, p_n$ là các số nguyên tố xuất hiện trong phân tích của $a$ và $b$. Khi đó, nếu một số nguyên chia hết cho cả $a$ và $b$ thì trong phân tích của nó, mỗi số $p_j$ phải xuất hiện với số mũ ít nhất là $\max(a_j, b_j)$. Như vậy, bội chung nhỏ nhất của các số $a$, $b$ là :

$$[a,b] = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \dots p_n^{\max(a_n,b_n)}.$$

Trên đây là một cách tìm bội chung nhỏ nhất của hai số. Tuy nhiên, phân tích một số nguyên ra thừa số là việc làm rất khó khăn (đối với các số lớn), nên thường để tìm bội chung nhỏ nhất, người ta dùng một số phương pháp thuận tiện hơn. Trước tiên ta có bổ đề sau :

**Bổ đề 1.29.** *Với các số thực $x$ và $y$, ta có*

$$\max(x, y) + \min(x, y) = x + y.$$

***Chứng minh.*** Giả sử $x \geq y$. Khi đó $\max(x, y) = x$, $\min(x, y) = y$ nên $\max(x, y) + \min(x, y) = x + y$. Nếu $x < y$ thì $\min(x, y) = x$, $\max(x, y) = y$ và $\max(x, y) + \min(x, y) = y + x$. □

**Định lí 1.30.** *Giả sử $a$, $b$ là các số nguyên dương. Khi đó*

$$[a,b] = \frac{ab}{(a,b)},$$

*trong đó $[a,b]$ là bội chung nhỏ nhất, $(a,b)$ là ước chung lớn nhất của hai số.*

***Chứng minh.*** Giả sử $a$, $b$ được phân tích ra thừa số nguyên tố dưới dạng sau :

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \; ; \; b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n},$$

trong đó $a_i$, $b_i$ là các số nguyên không âm $(i = 1, 2, \dots, n)$. Đặt $M_i = \max(a_i, b_i)$, $m_i = \min(a_i, b_i)$. Ta có

$$[a,b](a,b) = p_1^{M_1} p_2^{M_2} \dots p_n^{M_n} p_1^{m_1} p_2^{m_2} \dots p_n^{m_n}$$
$$= p_1^{M_1+m_1} p_2^{M_2+m_2} \dots p_n^{M_n+m_n}$$
$$= p_1^{a_1+b_1} p_2^{a_2+b_2} \dots p_n^{a_n+b_n}$$
$$= ab \ ;$$

vì $M_i + m_i = \max(a_i, b_i) + \min(a_i, b_i) = a_i + b_i$ theo **Bổ đề 1.29**. Hệ quả sau đây của Định lí cơ bản sẽ được sử dụng về sau.

**Bổ đề 1.31.** *Giả sử $m$, $n$ là các số nguyên dương nguyên tố cùng nhau. Khi đó, nếu $d$ là ước chung của $mn$, thì tồn tại cặp duy nhất các ước dương $d_1$ của $m$, $d_2$ của $n$ sao cho $d = d_1 d_2$. Ngược lại, nếu $d_1$ và $d_2$ là các ước dương tương ứng của $m$ và $n$, thì $d = d_1 d_2$ là ước dương của $mn$.*

***Chứng minh.*** Giả sử $m$ và $n$ có phân tích ra thừa số nguyên tố như sau :

$$m = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s} \ ; \ n = q_1^{n_1} q_2^{n_2} \dots q_t^{n_t}.$$

Vì $(m,n) = 1$ nên tập hợp các số nguyên tố $p_1, p_2, \dots, p_s$ và tập hợp các số nguyên tố $q_1, q_2, \dots, q_t$ không có phần tử chung. Do đó phân tích ra thừa số của $mn$ có dạng :

$$mn = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s} q_1^{n_1} q_2^{n_2} \dots q_t^{n_t}.$$

Như vậy, nếu $d$ là một ước chung của $mn$ thì

$$d = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s} q_1^{f_1} q_2^{f_2} \dots q_t^{f_t},$$

trong đó $0 \le e_i \le m_i \ (i = 1,2,\dots,s)$ ; $0 \le f_i \le n_i \ (j = 1,2,\dots,t)$. Đặt

$$d_1 = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s},$$
$$d_2 = q_1^{f_1} q_2^{f_2} \dots q_t^{f_t}.$$

Rõ ràng $d = d_1 d_2$ và $(d_1, d_2) = 1$.

Ngược lại, giả sử $d_1$ và $d_2$ là các ước dương tương ứng của $m$ và $n$. Khi đó

$$d_1 = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s},$$

trong đó $0 \le e_i \le m_i \ (i = 1,2,\dots,s)$, và

$$d_2 = q_1^{f_1} q_2^{f_2} \dots q_t^{f_t}.$$

trong đó $0 \le f_i \le n_i \ (j = 1,2,\dots,t)$. Số nguyên

$$d = d_1 d_2 = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s} q_1^{f_1} q_2^{f_2} \dots q_t^{f_t},$$

rõ ràng là ước của

$$mn = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s} q_1^{n_1} q_2^{n_2} \dots q_t^{n_t},$$

vì lũy thừa của mỗi số nguyên tố xuất hiện trong phân tích ra thừa số nguyên tố của $d$ bé hơn hoặc bằng lũy thừa của số nguyên tố đó trong phân tích của $mn$.

## § 7. CÁC SỐ PHECMA

Như đã nói, bài toán phân tích số nguyên ra thừa số nguyên tố là một bài toán khó khi phải làm việc với các số lớn. Mặc dù thuật toán phân tích một số nguyên ra thừa số là khá đơn giản, thời gian để thực hiện nó là quá lớn. Vì thế, khi phân tích một số nguyên, người ta thường phải dựa vào dạng của nó để tìm thuật toán thích hợp. Trong phần này, chúng ta sẽ tìm hiểu một số phương pháp phân tích các số nguyên đặc biệt, thường gọi là các số Phecma.

Trước tiên, ta giới thiệu thuật toán phân tích sau đây, gọi là phân tích Phecma.

**Bổ đề 1.32.** *Giả sử $n$ là một số nguyên dương lẻ. Khi đó tồn tại tương ứng một – một giữa tập hợp các cách phân tích $n$ ra tích hai số nguyên dương và tập hợp các cách biểu diễn $n$ dưới dạng hiệu hai số chính phương.*

***Chứng minh.*** Giả sử $n$ là số nguyên dương lẻ, và $n = ab$ là một cách phân tích $n$ thành tích hai số nguyên dương. Khi đó ta có thể viết $n$ dưới dạng hiệu hai bình phương

$$n = ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2,$$

trong đó $\dfrac{a+b}{2}$ và $\dfrac{a-b}{2}$ là các số nguyên, vì $a$, $b$ đều lẻ.

Ngược lại, nếu $n$ là hiệu của hai bình phương, chẳng hạn $n = s^2 - t^2$, thì ta có thể phân tích $n$ thành $n = (s-t)(s+t)$. □

Để áp dụng phương pháp phân tích Phecma, ta tìm nghiệm của phương trình $n = x^2 - y^2$ bằng cách tìm các số chính phương có dạng $x^2 - n$. Như vậy để phân tích $n$, ta tìm các số chính phương trong dãy số nguyên

$$t^2 - n, \quad (t+1)^2 - n, \quad (t+2)^2 - n, \quad \dots$$

trong đó $t$ là số nguyên nhỏ nhất lớn hơn $\sqrt{n}$. Quá trình này kết thúc sau hữu hạn bước. Thật vậy, vì

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2$$

nên trong dãy nói trên sẽ có số chính phương $\leq \left(\frac{n-1}{2}\right)^2$.

***Ví dụ :*** Phân tích số $6077$ bằng phương pháp Phecma. Vì $77 < \sqrt{6077} < 78$ nên ta tìm số chính phương trong dãy

$$78^2 - 6077 = 7$$
$$79^2 - 6077 = 164$$
$$80^2 - 6077 = 323$$
$$81^2 - 6077 = 484 = 22^2.$$

Vậy $6077 = 81^2 - 22^2$, tức là $6077 = (81-22)(81+22) = 59.103$. Phương pháp Phecma thuận tiện hơn phương pháp chia $n$ lần lượt cho các số nguyên tố không vượt quá $\sqrt{n}$. Chẳng hạn ở ví dụ trên, ta đã tránh được việc làm phép chia $6077$ cho các số nguyên tố $< 77$. Tuy nhiên, với phân tích Phecma, ta phải kiểm tra khoảng $\frac{n+1}{2} - \sqrt{n}$ số nguyên xem nó có là số chính phương hay không. Việc làm đó cũng đòi hỏi nhiều phép tính. Phương pháp phân tích Phecma thuận tiện khi áp dụng cho các số nguyên có hai thừa số độ lớn chênh lệch không nhiều.

Trong nhiều vấn đề của lí thuyết và ứng dụng, ta thường gặp các *số Phecma*, định nghĩa bởi

$$F_n = 2^{2^n} + 1.$$

Phecma đề ra giả thuyết rằng, $F_n$ là số nguyên tố với mọi $n \geq 0$. Giả thuyết đó đúng đối với một số số đầu tiên : $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. Tuy nhiên, $F_5$ lại là một hợp số. Ta có mệnh đề sau.

**Mệnh đề 1.32.** *Số Phecma* $F_5 = 2^{2^5} + 1$ *chia hết cho* $641$.

***Chứng minh.*** Ta có

$$641 = 5.2^7 + 1 = 2^4 + 5^4.$$

Do đó,

$$2^{2^5}+1=2^{32}+1=2^4.2^{28}+1=(641-5^4)2^{28}+1$$
$$=641.2^{28}-(5.2^7)^4+1=641.2^{28}-(641-1)^4+1$$
$$=641(2^{28}-641^3+4.641^2-6.641+4).$$

Cho đến nay, người ta chưa biết thêm số Phecma nào ngoài $F_0$, $F_1$, $F_2$, $F_3$, $F_4$ mà là số nguyên tố.

Ta có thể sử dụng các số Phecma để chứng minh tập hợp các số nguyên tố là vô hạn.

**Bổ đề 1.33.** *Giả sử $F_k=2^{2^k}+1$ là số Phecma thứ $k$, trong đó $k$ là số nguyên không âm. Khi đó, với mọi số nguyên dương $n$, ta có :*

$$F_0F_1F_2\dots F_{n-1}=F_n-2.$$

***Chứng minh.*** Ta dùng quy nạp theo $n$. Với $n=1$, ta được

$$F_0=3=F_1-2 \quad (\text{vì } F_1=5).$$

Giả sử ta có

$$F_0F_1\dots F_{n-1}=F_n-2.$$

Khi đó

$$F_0F_1\dots F_{n-1}F_n=(F_0F_1\dots F_{n-1})F_n$$
$$=(F_n-2)F_n=(2^{2^n}-1)(2^{2^n}+1)$$
$$=(2^{2^n})^2-1=2^{2^{n+1}}-1=F_{n+1}-2. \qquad \square$$

**Định lí 1.34.** *Giả sử $m$ và $n$ là các số nguyên không âm khác nhau. Khi đó các số Phecma $F_m$ và $F_n$ nguyên tố cùng nhau.*

***Chứng minh.*** Giả sử $m<n$. Từ Bổ đề 1.33 ta có

$$F_0F_1F_2\dots F_m\dots F_{n-1}=F_n-2.$$

Giả sử $d$ là một ước chung của $F_m$ và $F_n$. Khi đó

$$d\mid(F_n-F_0F_1\dots F_{n-1}),$$

tức là $d\mid 2$. Như vậy $d=1$ hoặc $2$. Vì $F_m$, $F_n$ lẻ nên $d=1$, tức là $(F_n,F_m)=1$. $\square$

Sử dụng các số Phecma, ta có thể đưa ra một chứng minh khác về sự

vô hạn của các số nguyên tố. Thật vậy, mỗi số Phecma $F_n$ có ước nguyên tố $p_m$. Vì $(F_m, F_n) = 1$ nên $p_m \neq p_n$ khi $m \neq n$. Từ đó suy ra có vô hạn số nguyên tố. □

**Nhận xét.** Các số nguyên tố Phecma còn có vai trò quan trọng trong hình học. Ta phát biểu (không chứng minh) định lí sau đây.

**Định lí. 1.35.** *Một đa giác đều $n$ cạnh có thể dựng được bằng thước kẻ và compa nếu và chỉ nếu $n$ có dạng*

$$n = 2^a p_1 \dots p_t,$$

*trong đó $p_i$, $i = 1,2,\dots,t$, là các số nguyên tố Phecma khác nhau và $a$ là số nguyên không âm.*

## BÀI TẬP CHƯƠNG 1

**1.** Hàm đệ quy $f(n)$ xác định trên tập hợp các số nguyên dương bởi quy tắc : $f(1) = 1$, $f(2) = 5$, $f(n+1) = f(n) + 2f(n-1)$ với mọi $n > 2$. Dùng phương pháp quy nạp, chứng minh rằng $f(n) = 2^n + (-1)^n$.

**2.** Tính các tổng

$$\sum_{k=0}^{n} C_n^k (-1)^k \quad ; \quad \sum_{k=0}^{n} C_n^k \quad ; \quad \sum_{k=0}^{2\left[\frac{n}{2}\right]} C_n^{2k} \quad ; \quad \sum_{k=1}^{2\left[\frac{n-1}{2}\right]+1} C_n^{2k-1}.$$

**3.** Chứng minh rằng, nếu $n$ là số nguyên dương thì

$$(2n)! < 2^{2n}(n!)^2.$$

**4.** Bài toán "Tháp Hà Nội" (được Lucas đề xuất năm 1896). Có 3 cái cọc và $n$ cái đĩa có kích thước khác nhau từng cặp, được lồng vào một cọc theo thứ tự cái to ở dưới, cái nhỏ ở trên. Mục tiêu đặt ra là chuyển các đĩa sang một cọc khác, sắp xếp theo thứ tự như vậy, mỗi lần chuyển một đĩa và không bao giờ đặt đĩa to lên đĩa bé hơn trong quá trình chuyển. Cọc thứ ba được dùng làm "trung chuyển". Chứng minh rằng số lần dịch chuyển tối thiểu để đạt mục tiêu đề ra là $2^n - 1$.

**5.** Tìm tất cả các số nguyên dương $x$, $y$, $z$ sao cho

$$x! + y! = z!.$$

**6.** Giả sử $a$, $b$ là các số nguyên dương lẻ. Chứng minh rằng tồn tại các số nguyên $s$ và $t$ sao cho $a = bs + t$, trong đó $t$ lẻ và $|t| < b$.

7. Chứng minh rằng nếu $a$, $b$ là các số nguyên dương thì tồn tại các số nguyên $q$, $r$ và $e = \pm 1$ sao cho $a = bq + er$, trong đó $-\frac{b}{2} < r \leq \frac{b}{2}$.

8. Chứng minh rằng nếu $a$, $b$ là các số thực thì

$$[a + b] \geq [a] + [b].$$

9. Chứng minh rằng nếu $a$, $b$ là các số thực dương thì

$$[ab] \geq [a][b].$$

Xét trường hợp ít nhất một trong hai số là số âm.

10. Chứng minh rằng nếu $n$ là số nguyên và $x$ là số thực thì

$$[x + n] = [x] + n.$$

11. Chứng minh rằng $n$ là số chẵn nếu và chỉ nếu

$$n - 2\left[\frac{n}{2}\right] = 0.$$

12. a) Chứng minh rằng số các số nguyên dương không vượt quá $x$ và chia hết cho số nguyên dương $d$ là $\left[\frac{x}{d}\right]$.

b) Tìm số các số nguyên dương không vượt quá 2000 và chia hết cho 5; cho 25 ; cho 125 ; cho 625.

13. Chứng minh rằng nếu $a$ là số nguyên thì $a^3 - a \vdots 3$.

14. Chứng minh rằng tích các số nguyên dạng $4^k + 1$ lại là số nguyên có dạng đó, trong khi tích hai số nguyên dạng $4^k + 3$ lại có dạng $4^k + 1$.

15. Chứng minh rằng bình phương của mọi số nguyên lẻ đều có dạng $8k + 1$.

16. Giả sử $n$ là số nguyên dương. Định nghĩa

$$T(n) = \begin{cases} \dfrac{n}{2} & \text{nếu } n \text{ chẵn} \\ \dfrac{3n+1}{2} & \text{nếu } n \text{ lẻ} \end{cases}$$

Lập dãy $n$, $T(n)$, $T(T(n))$, $T(T(T(n)))$, ... Chứng minh rằng nếu $n = (2^k - 1)/3$, ($k > 1$ và $k$ nguyên), thì từ lúc nào đó, dãy sẽ có dạng 1, 2, 1, 2,...

(*Giả thuyết Collatz* sau đây chưa được chứng minh : với mọi $n$, từ lúc nào đó dãy sẽ có dạng $1, 2, 1, 2, \ldots$).

**17.** Chứng minh rằng mọi số nguyên $n \neq 0$ đều có thể biểu diễn duy nhất dưới dạng

$$n = e_k 3^k + e_{k-1} 3^{k-1} + \cdots + e_1 3 + e_0,$$

trong đó $e_j = -1, 0, 1$, $j = 0, 1, 2, \ldots, k$.

**18.** Chứng minh rằng, mọi số nguyên dương đều có khai triển duy nhất dưới dạng sau (khai triển Cantor) :

$$n = a_m m! + a_{m-1}(m-1)! + \cdots + a_2 .2! + a_1 .1!$$

**19.** Giả sử $a$ là số nguyên có $4$ chữ số (trong hệ thập phân). Ta lập số $a'$ bằng cách xếp các chữ số của $a$ theo thứ tự giảm dần, $a''$ là số gồm các chữ số của $a$ xếp theo thứ tự tăng dần. Đặt

$$T(a) = a' - a''.$$

Ví dụ : $T(2001) = 2100 - 12 = 2088$, $T(2088) = 8632$, $T(8632) = 6264$, $T(6264) = 4176$, $T(4176) = 6174$.

Chứng minh rằng, nếu $a$ không phải là số với $4$ chữ số như nhau thì dãy $a$, $T(a)$, $T(T(a))$, $T(T(T(a)))$, ... sẽ dừng ở số $6174$.

**20.** Dùng sàng Eratosthenes để tìm tất cả các số nguyên tố $< 200$.

**21.** Tìm tất cả các số nguyên dương $n$ sao cho $n^3 + 1$ là số nguyên tố.

**22.** Chứng minh rằng nếu $a$ và $n$ là các số nguyên dương sao cho $a^n - 1$ nguyên tố thì $a = 2$ và $n$ là số nguyên tố.

**23.** Cho $p_1, \ldots, p_n$ là các số nguyên tố. Chứng minh rằng

$$Q_n = p_1 p_2 \ldots p_n + 1$$

có ước nguyên tố khác $p_i$, $i = 1, \ldots, n$.

**24.** Giả sử $p_1, \ldots, p_n$ là $n$ số nguyên tố đầu tiên, $m$ là số nguyên và $1 < m < n$. Giả sử $Q$ là tích của $m$ số nguyên tố nào đó trong danh sách trên, $R$ là tích các số còn lại. Chứng minh rằng $Q + R$ không chia hết cho bất kì số nguyên tố nào trong dãy.

(Từ các Bài tập 23, 24 ta có các cách khác để chứng minh tập hợp các số nguyên tố là vô hạn).

**25.** Chứng minh rằng nếu ước nguyên tố nhỏ nhất $p$ của số nguyên dương $n$ vượt quá $\sqrt[3]{n}$ thì $n/p$ là số nguyên tố.

**26.** Chứng minh rằng mọi số nguyên lớn hơn 11 là tổng của hai hợp số.

**27.** Chứng minh rằng nếu

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

là đa thức với hệ số nguyên, thì tồn tại $y$ sao cho $f(y)$ là hợp số.

**28.** Chứng minh rằng nếu $a_1, a_2, \ldots, a_n$ là các số nguyên, và $b$ là số nguyên khác sao cho $(a_1, b) = (a_2, b) = \cdots = (a_n, b) = 1$, thì $(a_1 a_2 \ldots a_n, b) = 1$.

**29.** Chứng minh rằng nếu $a$, $b$ là các số nguyên và $a^n \mid b^n$ thì $a \mid b$ ($n$ là số nguyên dương).

**30.** Chứng minh rằng nếu $a$, $b$, $c$ là các số nguyên nguyên tố cùng nhau đồng thời thì $(ab, c) = (a, b)(a, c)$.

**31.** Chỉ ra 5 ví dụ về tập hợp 3 số nguyên nguyên tố cùng nhau đồng thời nhưng không nguyên tố cùng nhau từng cặp.

**32.** Chứng minh rằng nếu $a$, $b$ là các số nguyên dương nguyên tố cùng nhau thì $((a^n - b^n)/(a - b),\ a - b) = 1$ hoặc $n$.

**33.** Giả sử $m$ và $n$ là các số nguyên dương, $a$ là số nguyên lớn hơn 1. Chứng minh rằng

$$(a^n - 1, a^m - 1) = a^{(m, n)} - 1.$$

**34.** Giả sử $n$ là số nguyên dương. Chứng minh rằng lũy thừa của số nguyên tố $p$ xuất hiện trong phân tích ra thừa số nguyên tố của $n!$ là

$$[n/p] + [n/p^2] + [n/p^3] + \cdots$$

**35.** Số $(2000)!$ tận cùng có bao nhiêu chữ số 0?

**36.** Tìm các số nguyên dương $n$ sao cho số $n!$ tận cùng có 500 chữ số 0.

**37.** Tồn tại hay không số $n$ sao cho $n!$ tận cùng có 2005 chữ số không?

**38.** Số nguyên dương $n$ nào chia hết cho mọi số nguyên dương không vượt quá $\sqrt{n}$.

**39.** Chứng minh rằng nếu $a$, $b$ là các số nguyên dương thì

$$([a, b], c) = [(a, c), (b, c)]$$

$$[(a, b), c] = ([a, c], [b, c]).$$

**40.** Giả sử $a$, $b$, $c$ là các số nguyên dương. Chứng minh rằng

$$(a, b, c)[a, b, c] = \frac{abc}{(a, b)(a, c)(b, c)}.$$

**41.** Giả sử $n$ là số nguyên dương. Có bao nhiêu cặp số nguyên dương thỏa mãn $[a,b] = n$?

**42.** Chứng minh rằng tồn tại vô hạn số nguyên tố dạng $6k + 5$, trong đó $k$ là một số nguyên dương.

**43.** Giả sử $a$, $b$ là các số nguyên. Chứng minh rằng, với mọi $n$, tồn tại $n$ số hạng liên tiếp của cấp số cộng

$$a,\ a + b,\ a + 2b,\ \ldots$$

mà mỗi một trong chúng đều là hợp số.

**44.** Chứng minh rằng nếu ước nguyên tố nhỏ nhất của $n$ là $p$, thì $x^2 - n$ không phải là số chính phương nếu $x > (n + p^2)/2p$.

**45.** Giả sử $a$ là số nguyên dương và $a^m + 1$ là số nguyên tố. Chứng minh rằng $m = 2^n$ với số nguyên dương $n$ nào đó.

**46.** Chứng minh rằng chữ số tận cùng của $F_n = 2^{2^n} + 1$ là 7.

Chương 2.

# LÍ THUYẾT ĐỒNG DƯ

## § 1. KHÁI NIỆM CƠ BẢN

Đồng dư là một trong những khái niệm quan trọng nhất của số học và đại số. Trong mục này, ta sẽ làm quen với những định nghĩa và tính chất đơn giản nhất.

**Định nghĩa 2.1.** Giả sử $a$, $b$ là các số nguyên. Ta nói rằng $a$ *đồng dư* $b$ *môđulô* $m$ nếu $m \mid (a-b)$.

Khi $a$ đồng dư $b$ môđulô $m$, ta viết

$$a \equiv b \pmod{m}$$

Nếu $a$ không đồng dư $b$ môđulô $m$, ta viết

$$a \not\equiv b \pmod{m}$$

**Mệnh đề 2.2.** *Nếu $a$, $b$ là các số nguyên thì $a \equiv b \pmod{m}$ khi và chỉ khi tồn tại số nguyên $k$ sao cho $a = b + km$.*

***Chứng minh.*** Giả sử $a \equiv b \pmod{m}$. Khi đó $m \mid (a-b)$, tức là $a - b = km$ với số nguyên $k$ nào đó. Ngược lại, nếu tồn tại số nguyên $k$ sao cho $a = b + km$ thì $m \mid (a-b)$, tức là $a \equiv b \pmod{m}$. □

Mệnh đề sau đây cho thấy quan hệ "$a$ đồng dư $b$" là một "quan hệ tương đương".

**Mệnh đề 2.3.** *Giả sử $m$ là một số nguyên dương. Quan hệ đồng dư môđulô $m$ thỏa mãn các tính chất sau đây :*

*1) (Tính chất phản xạ). Nếu $a$ là một số nguyên, thì*

$$a \equiv a \pmod{m}$$

*2) (Tính chất đối xứng). Giả sử $a$, $b$ là các số nguyên. Khi đó, nếu*

$a \equiv b \pmod{m}$ *thì* $b \equiv a \pmod{m}$.

*3) (Tính chất bắc cầu). Giả sử* $a$, $b$, $c$ *là các số nguyên. Khi đó, nếu* $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ *thì* $a \equiv c \pmod{m}$.

***Chứng minh.*** 1) Ta có $a \equiv a \pmod{m}$ vì $m \mid (a-a)$.

2) Giả sử $a \equiv b \pmod{m}$, tức là $m \mid (a-b)$. Khi đó, $m \mid (b-a)$ và $b \equiv a \pmod{m}$.

3) Nếu $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ thì $m \mid (a-b)$ và $m \mid (b-c)$. Do đó, $m \mid (a-c)$ vì $(a-c) = (a-b) + (b-c)$. □

Nhờ tính chất trên, với mỗi số nguyên dương $m$, ta có thể chia tập hợp các số nguyên thành *các lớp đồng dư môđulô* $m$. Hai số nguyên cùng thuộc vào một lớp đồng dư môđulô $m$ khi và chỉ khi chúng đồng dư với nhau môđulô $m$.

***Ví dụ :*** 1 và 21 cùng thuộc một lớp đồng dư môđulô 5 :

$$1 \equiv 21 \pmod{5}.$$

Số nguyên tùy ý đều thuộc cùng một lớp đồng dư môđulô 5 với một trong các số : 0, 1, 2, 3, 4.

Giả sử $a$ là một số nguyên. Với số nguyên $m > 1$ cho trước, bởi thuật toán chia, ta có $a = bm + r$, trong đó $0 \le r \le m-1$. Từ đẳng thức trên, $a \equiv r \pmod{m}$. Như vậy, mỗi số nguyên đồng dư môđulô $m$ với một trong các số nguyên của tập hợp $0,1,\ldots,m-1$, cụ thể là đồng dư với phần dư trong phép chia số nguyên đó cho $m$. Vì không có hai số nào trong các số $0,1,\ldots,m-1$ đồng dư với nhau môđulô $m$, tập hợp trên đây là tập hợp các số nguyên sao cho mỗi số nguyên đồng dư với đúng một phần tử thuộc tập hợp. Tuy nhiên, $0,1,\ldots,m-1$ không phải là tập hợp duy nhất có tính chất đó.

**Định nghĩa 2.4.** Một hệ thặng dư đầy đủ môđulô $m$ là một tập hợp các số nguyên sao cho mỗi số nguyên tùy ý đều đồng dư môđulô $m$ với đúng một số của tập hợp.

***Ví dụ :*** 1) Tập hợp các số $0,1,\ldots,m-1$ là một hệ thặng dư đầy đủ môđulô $m$. Hệ này gọi là *hệ thặng dư không âm bé nhất môđulô* $m$.

2) Giả sử $m$ là một số nguyên lẻ. Khi đó tập hợp các số nguyên

$$-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}$$

là một hệ thặng dư đầy đủ, được gọi là *hệ thặng dư tuyệt đối bé nhất môđulô* $m$.

Ta sẽ chỉ ra rằng, có thể cộng, trừ, nhân hai vế của một đồng dư với cùng một số.

**Định lí 2.5.** *Giả sử* $a$, $b$, $c$ *và* $m$ *là các số nguyên,* $m > 0$ *và* $a \equiv b \pmod{m}$. *Khi đó :*

*1)* $a + c \equiv b + c \pmod{m}$,

*2)* $a - c \equiv b - c \pmod{m}$,

*3)* $ac \equiv bc \pmod{m}$.

***Chứng minh.*** Vì $a \equiv b \pmod{m}$ nên $m \mid (a - b)$. Do $(a + c) - (b + c) = a - b$ nên $m \mid [(a + c) - (b - a)]$: 1) được chứng minh. Tương tự, 2) được suy ra từ chỗ $(a - c) - (b - c) = a - c$. Để chứng minh 3) ta chú ý rằng $ac - bc = c(a - b)$, nên từ $m \mid (a - c)$ suy ra $m \mid c(a - b)$, tức là $ac \equiv bc \pmod{m}$. □

Tuy nhiên, nói chung không thể làm phép "chia hai vế" của một đồng dư cho cùng một số. Chẳng hạn

$$2002 \equiv 4 \pmod{6} \text{ nhưng } \frac{2002}{2} = 1001 \not\equiv 2 \pmod{6}.$$

Định lí sau đây chỉ ra điều kiện để có thể làm phép chia như vậy :

**Định lí 2.6.** *Giả sử* $a$, $b$, $c$, $m$ *là các số nguyên,* $m > 0$, $ac \equiv bc \pmod{m}$ *và* $d = (c, m)$. *Khi đó ta có*

$$a \equiv b \left(\mathrm{mod}\, \frac{m}{d}\right).$$

***Chứng minh.*** Giả sử $ac \equiv bc \pmod{m}$. Ta có $m \mid (ac - bc) = c(a - b)$. Do đó tồn tại số nguyên $k$ sao cho $c(a - b) = km$. Chia hai vế cho $d$, ta được :

$$\frac{c}{d}(a - b) = k \cdot \frac{m}{d}.$$

Vì $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$ nên từ đó suy ra $\frac{m}{d} \mid (a - b)$, tức là

$$a \equiv b \left(\mathrm{mod}\, \frac{m}{d}\right).$$ □

***Ví dụ :*** $2002 \equiv 2 \pmod 5$. Do $(2, 5) = 1$ nên ta có

$$1001 \equiv 1 \pmod 5.$$

Định lí sau đây là hệ quả của Định lí 2.6.

**Định lí 2.7.** *Nếu* $a$, $b$, $c$, $m$ *là các số nguyên sao cho* $m > 0$, $(c, m) = 1$, *và* $ac \equiv bc \pmod m$. *Khi đó* $a \equiv b \pmod m$.

Định lí 2.5 có thể mở rộng thành định lí sau đây, cho ta thấy rằng có thể làm một số phép tính số học đối với các lớp đồng dư như đối với các số nguyên.

**Định lí 2.8.** *Giả sử* $a$, $b$, $c$, $d$, $m$ *là các số nguyên,* $m > 0$, $a \equiv b \pmod m$, $c \equiv d \pmod m$. *Khi đó :*

1) $a + c \equiv b + d \pmod m$,

2) $a - c \equiv b - d \pmod m$,

3) $ac \equiv bd \pmod m$.

***Chứng minh.*** Vì $a \equiv b \pmod m$, $c \equiv d \pmod m$ nên $m \mid (a - b)$, $m \mid (c - d)$. Do đó tồn tại các số nguyên $k$ và $l$ sao cho $km = a - b$, $lm = c - d$.

Để chứng minh 1), ta nhận xét rằng $(a + c) - (b + d) = km + lm = (k + l)m$. Do đó $m \mid [(a + c) - (b + d)]$ tức là $a + c \equiv b + d \pmod m$.

Để chứng minh 2) ta chú ý rằng $(a - c) - (b - d) = (a - b) - (c - d) = km - lm = (k - l)m$. Do đó $m \mid [(a - b) - (c - d)]$, tức là $a - c \equiv b - d \pmod m$.

Để chứng minh 3), ta thấy $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = ckm + blm = m(ck + bl)$, tức là $m \mid (ac - bd)$. Do đó $ac \equiv bd \pmod m$. □

**Định lí 2.9.** *Giả sử* $r_1, r_2, \ldots, r_m$ *là hệ đầy đủ các thặng dư môđulô* $m$, $a$ *là số nguyên dương và* $(a, m) = 1$. *Khi đó*

$$ar_1 + b,\ ar_2 + b,\ \ldots,\ ar_m + b$$

*cũng là một hệ thặng dư đầy đủ môđulô* $m$.

***Chứng minh.*** Trước tiên ta chỉ ra rằng, trong các số nguyên

$$ar_1 + b,\ ar_2 + b,\ \ldots,\ ar_m + b$$

không có hai số nào đồng dư nhau môđulô $m$. Thật vậy, nếu

$$ar_j + b \equiv ar_k + b \pmod{m}$$

thì

$$ar_j \equiv ar_k \pmod{m}.$$

Do $(a, m) = 1$ nên theo Định lí 2.7 ta có

$$r_j \equiv r_k \pmod{m}.$$

Vì $r_j \not\equiv r_j \pmod{m}$ nếu $j \neq k$ nên ta suy ra $j = k$.

Do tập hợp các số nguyên trên đây gồm $m$ số nguyên không đồng dư môđulô $m$ nên các số nguyên đó lập thành hệ thặng dư đầy đủ môđulô $m$ □

Định lí sau cho thấy rằng, các đồng dư được bảo toàn nếu cả hai vế được nâng lên cùng một lũy thừa nguyên dương.

**Định lí 2.10.** Giả sử $a$, $b$, $k$, $m$ là các số nguyên, đồng thời $k > 0$, $m > 0$, $a \equiv b \pmod{m}$. Khi đó

$$a^k \equiv b^k \pmod{m}.$$

***Chứng minh.*** Do $a \equiv b \pmod{m}$, ta có $m \mid (a - b)$. Vì

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}),$$

nên $(a - b) \mid (a^k - b^k)$. Vậy $m \mid (a^k - b^k)$, tức là $a^k \equiv b^k \pmod{m}$. □

Trong trường hợp các số $a$, $b$ đồng dư nhau môđulô nhiều số nguyên dương khác nhau, ta có thể kết hợp lại theo định lí sau.

**Định lí 2.11.** *Giả sử* $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ... , $a \equiv b \pmod{m_k}$, *trong đó* $a, b, m_1, \ldots, m_k$ *là các số nguyên,* $m_1, m_2, \ldots, m_k > 0$. *Khi đó*

$$a \equiv b \pmod{[m_1 \ldots m_k]},$$

*trong đó* $[m_1 \ldots m_k]$ *là bội chung nhỏ nhất của* $m_1, m_2, \ldots, m_k$.

***Chứng minh.*** Vì $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ... , $a \equiv b \pmod{m_k}$ nên ta có $m_1 \mid (a - b)$, $m_2 \mid (a - b)$, ... , $m_k \mid (a - b)$. Từ đó suy ra rằng

$$[m_1, m_2, \ldots, m_k] \mid (a-b),$$

tức là

$$a \equiv b \pmod{[m_1 \ldots m_k]}.$$ □

**Hệ quả 2.12.** *Giả sử* $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., $a \equiv b \pmod{m_k}$, *trong đó* $a$, $b$ *nguyên,* $m_1, m_2, \ldots, m_k$ *là các số nguyên dương nguyên tố cùng nhau từng cặp. Khi đó*

$$a \equiv b \pmod{m_1 \ldots m_k}$$

***Chứng minh.*** Do $m_1, m_2, \ldots, m_k$ nguyên tố cùng nhau từng cặp nên ta có

$$[m_1 m_2 \ldots m_k] = m_1 m_2 \ldots m_k.$$

Khi đó Hệ quả suy trực tiếp từ Định lí 2.11. □

## § 2. ĐỒNG DƯ TUYẾN TÍNH

Một đồng dư dạng

$$ax \equiv b \pmod{m},$$

trong đó $x$ là số nguyên chưa biết, được gọi là *đồng dư tuyến tính* một biến. Ta sẽ thấy rằng, việc nghiên cứu các đồng dư như vậy hoàn toàn tương tự việc nghiên cứu phương trình nghiệm nguyên hai biến.

Trước tiên ta nhận xét rằng nếu $x = x_0$ là một nghiệm của đồng dư $ax \equiv b \pmod{m}$ và nếu $x_1 \equiv x_0 \pmod{m}$, thì $ax_1 \equiv ax_0 \equiv b \pmod{m}$, nên $x_1$ cũng là một nghiệm. Như vậy, nếu một phần tử của một lớp đồng dư môđulô $m$ nào đó là một nghiệm, thì mọi phần tử của lớp đó cũng là nghiệm. Vì thế có thể đặt câu hỏi: trong $m$ lớp đồng dư môđulô, có bao nhiêu lớp cho nghiệm, hay một cách tương đương, có bao nhiêu nghiệm không đồng dư môđulô $m$.

**Định lí 2.13.** *Giả sử* $a$, $b$, $m$ *là các số nguyên,* $m > 0$ *và* $(a, m) = d$. *Nếu* $d \nmid b$ *thì đồng dư* $ax \equiv b \pmod{m}$ *vô nghiệm. Nếu* $d \mid b$ *thì* $ax \equiv b \pmod{m}$ *có đúng* $d$ *nghiệm không đồng dư môđulô* $m$.

***Chứng minh.*** Số nguyên $x$ là nghiệm của đồng dư $ax \equiv b \pmod{m}$ nếu và chỉ nếu tồn tại số nguyên $y$ sao cho $ax - by = b$. Vì $d = (a, m)$ nên $d \mid b$. Vậy, nếu $d \nmid b$ thì đồng dư đang xét không tồn tại nghiệm.

Bây giờ giả sử $d \mid b$. Vì $d = (a,m)$ nên tồn tại các số nguyên $s$, $t$ sao cho

$$d = as + mt.$$

Mặt khác, tồn tại số nguyên $e$ sao cho $b = de$. Từ đó ta được $b = a(se) + m(te)$. Như vậy, ta có thể lấy một nghiệm của đồng dư là $x_0 = se$. Ta sẽ chứng tỏ rằng, các số

$$x = x_0 + \left(\frac{m}{d}\right)k, \tag{1}$$

trong đó $k$ nguyên, đều là nghiệm của đồng dư đang xét. Thật vậy

$$ax = ax_0 + m\left(\frac{a}{d}\right)k,$$

mà $ax_0 \equiv b \pmod m$, $\frac{a}{d}$ nguyên nên

$$ax \equiv ax_0 \equiv b \pmod m.$$

Ngược lại, mọi nghiệm của đồng dư đều phải có dạng (1). Thật vậy, giả sử $x$ là một nghiệm tùy ý,

$$ax - my = b.$$

Ta có :

$$a(x - se) - m(y + te) = 0,$$

tức là

$$a(x - se) = m(y + te).$$

Chia hai vế cho $d$, ta được

$$\frac{a}{d}(x - se) = \frac{m}{d}(y + te).$$

Do $d = (a,m)$ nên $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$, suy ra $\frac{a}{d} \Big| (y + te)$. Vậy phải tồn tại số nguyên $k$ sao cho $\frac{a}{d} \cdot k = y + te$, tức là $y = \frac{a}{d} \cdot k - te$. Do đó $a(x - se) = \frac{a}{d}mk$. Vậy,

$$x = se + \frac{m}{d} \cdot k = x_0 + \frac{m}{d} \cdot k.$$

Còn phải chứng minh rằng, có đúng $d$ nghiệm không đồng dư môđulô $m$. Giả sử các nghiệm $x_1 = x_0 + \frac{m}{d}t_1$ và $x_2 = x_0 + \frac{m}{d}t_2$ đồng dư môđulô $m$:

$$x_0 + \frac{m}{d} \cdot t_1 \equiv x_0 + \frac{m}{d}t_2 \pmod{m}.$$

Ta có

$$\frac{m}{d} \cdot t_1 \equiv \frac{m}{d}t_2 \pmod{m}.$$

Vì $\frac{m}{d} \mid m$ nên $\left(m, \frac{m}{d}\right) = \frac{m}{d}$ nên theo Định lí 2.6,

$$t_1 \equiv t_2 \pmod{d}$$

Như vậy, hệ đầy đủ các nghiệm không đồng dư nhận được bằng cách đặt $x = x_0 + \frac{m}{d}t$, trong đó $t$ chạy qua hệ đầy đủ các thặng dư môđulô $d$. Tập hợp đó có đúng $d$ phần tử, cho bởi $t = 0, 1, 2, \ldots, d-1$. □

*Ví dụ :* Tìm các nghiệm của đồng dư

$$9x \equiv 12 \pmod{15}.$$

Ta thấy $(9,15) = 3$ và $3 \mid 9$ có đúng 3 nghiệm không đồng dư. Trước hết, ta cần tìm một nghiệm riêng $x_0$, sau đó chỉ cần cộng thêm các bội số thích hợp của $\frac{15}{3} = 5$.

Phương pháp tổng quát để giải các phương trình nghiệm nguyên dạng $ax + by = c$ sẽ được trình bày trong Chương 5. Ở đây, ta có thể thấy $x = 8$ là một nghiệm của đồng dư đang xét. Như vậy, 3 nghiệm không đồng dư môđulô 15 cần tìm là 8, 13 và 18.

Trường hợp đặc biệt của đồng dư tuyến tính là đồng dư

$$ax \equiv 1 \pmod{m}.$$

Theo Định lí 2.13, đồng dư có nghiệm khi và chỉ khi $(a, m) = 1$, đồng thời mọi nghiệm đều đồng dư nhau môđulô $m$.

**Định nghĩa 2.14.** Giả sử $a$, $m$ là các số nguyên, $m > 1$. Nghiệm của đồng dư

$$ax \equiv 1 \pmod{m}$$

được gọi là *nghịch đảo của $a$ môđulô $m$*.

Đặc biệt, có những số là nghịch đảo của chính nó môđulô một số nguyên tố $p$.

**Mệnh đề 2.15.** *Giả sử $p$ là một số nguyên tố. Số nguyên $a$ là nghịch đảo môđulô $p$ của chính nó khi và chỉ khi*

$$a \equiv 1 \pmod{p} \text{ hoặc } a \equiv -1 \pmod{p}.$$

***Chứng minh.*** Nếu $a \equiv 1 \pmod{p}$ hoặc $a \equiv -1 \pmod{p}$ thì $a^2 \equiv 1 \pmod{p}$ nên $a$ là nghịch đảo của chính nó.

Ngược lại, giả sử $a$ là nghịch đảo của chính nó, tức là $a^2 = a.a \equiv 1 \pmod{p}$. Khi đó $p \mid (a^2 - 1)$. Vì $a^2 - 1 = (a-1)(a+1)$ mà $p$ nguyên tố, nên $p \mid (a-1)$ hoặc $p \mid (a+1)$. Do đó, $a \equiv 1 \pmod{p}$ hoặc $a \equiv -1 \pmod{p}$. □

## § 3. ĐỊNH LÍ TRUNG QUỐC VỀ PHẦN DƯ

Tương truyền rằng, Hàn Tín (danh tướng đời Hán) khi kiểm điểm quân số thường làm như sau. Ông cho lính xếp thành hàng 3, sau đó hàng 5, rồi hàng 7. Mỗi lần như vậy, quân lính báo cho Hàn Tín số người ở hàng cuối cùng (có thể không đủ 3, 5, 7). Từ đó, ông ta suy ra số quân chính xác. Thực chất là Hàn Tín đã giải một hệ đồng dư tuyến tính theo môđulô $3$, $5$ và $7$. Bài toán trên nổi tiếng dưới tên gọi "Hàn Tín điểm binh", và thuật toán mà ông dùng dựa trên một trong những định lí nổi tiếng nhất của toán học : Định lí Trung Quốc về phần dư.

**Định lí 2.16.** (Định lí Trung Quốc về phần dư).

*Giả sử $m_1, m_2, \ldots, m_r$ là các số nguyên tố cùng nhau từng cặp. Khi đó hệ các đồng dư tuyến tính*

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_r \pmod{m_r}$$

*có nghiệm duy nhất môđulô $M = m_1 m_2 \ldots m_r$.*

***Chứng minh.*** Trước tiên, ta xây dựng một nghiệm của hệ đồng dư tuyến tính trên. Đặt

$$M_k = \frac{M}{m_k} = m_1 m_2 \dots m_{k-1} m_{k+1} \dots m_r.$$

Vì $(m_k, m_j) = 1$ với $j \neq k$ nên $(M_k, m_k) = 1$. Do đó, tồn tại nghịch đảo $y_k$ của $M_k$ môđulô $m_k$

$$M_k y_k \equiv 1 \pmod{m_k}.$$

Lập tổng

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_r M_r y_r.$$

Khi đó, $x$ sẽ là nghiệm của hệ đồng dư $x \equiv a_j \pmod{m_j}$, $j = 1, \dots, r$. Thật vậy, ta có $m_j \mid M_k$ khi $j \neq k$ nên $M_j \equiv 0 \pmod{m_k}$, $j \neq k$. Từ đó suy ra

$$x \equiv a_k M_k y_k \pmod{m_k}.$$

Do $M_k y_k \equiv 1 \pmod{m_k}$ nên $x \equiv a_k \pmod{m_k}$.

Bây giờ ta chỉ ra rằng, hai nghiệm tùy ý của hệ sẽ đồng dư nhau môđulô $M$. Giả sử $x_0$, $x_1$ là hai nghiệm của hệ $r$ đồng dư đang xét. Khi đó, với mỗi $k$, $x_0 \equiv x_1 \equiv a_k \pmod{m_k}$. Do đó $m_k \mid (x_0 - x_1)$. Từ đó suy ra $x_0 \equiv x_1 \pmod{M}$. Vậy hệ đồng dư đang xét có nghiệm duy nhất môđulô $M$. □

Ngoài vai trò quan trọng trong các vấn đề lí thuyết, Định lí Trung Quốc về phần dư còn là cơ sở cho các phép toán số học thực hiện trong máy tính. Ví dụ, để làm phép cộng hai số $a$, $b$ không vượt quá $10^6$, ta chọn bốn số nguyên tố cùng nhau từng cặp $m_1 = 99$, $m_2 = 98$, $m_3 = 97$, $m_4 = 95$ có tích lớn hơn $10^6$. Giả sử $a \equiv a_j \pmod{m_j}$, $b \equiv b_j \pmod{m_j}$, $j = 1, 2, 3, 4$ ; $a_j$, $b_j < 98$. Từ đó ta có $(a + b) \equiv (a_j + b_j) \pmod{m_j}$. Định lí Trung Quốc về phần dư cho giá trị $(a + b) \pmod{(95.97.98.99)}$. Khi biết một ước lượng của $a + b$, ta dễ dàng tìm được giá trị chính xác của $a + b$. Đó chính là cách mà Hàn Tín đã dùng. Để minh họa, xét một trường hợp cụ thể : tính tổng của $x = 123684$ và $y = 413456$. Ta có

$$x \equiv 33 \pmod{99} \quad y \equiv 32 \pmod{99}$$

$$x \equiv 8 \pmod{98} \quad y \equiv 92 \pmod{98}$$

$$x \equiv 9 \pmod{97} \quad y \equiv 42 \pmod{97}$$
$$x \equiv 89 \pmod{95} \quad y \equiv 16 \pmod{95}$$

Do đó

$$x + y \equiv 65 \pmod{99}$$
$$x + y \equiv 5 \pmod{98}$$
$$x + y \equiv 51 \pmod{97}$$
$$x + y \equiv 10 \pmod{95}.$$

Ta có, $M = 99.98.97.95 = 8940390$, $M_1 = M/99 = 903070$, $M_2 = M/98 = 912288$, $M_3 = M/97 = 921690$, $M_4 = M/95 = 941094$. Mặt khác, có thể tìm được $y_1 \equiv 37 \pmod{99}$, $y_2 \equiv 38 \pmod{98}$, $y_3 \equiv 24 \pmod{97}$, $y_4 \equiv 4 \pmod{95}$. Vậy :

$$\begin{aligned} x + y &\equiv 65.903070.37 + 2.912285.33 + 51.921690.24 + 10.941094.4 \\ &= 339788480 \\ &= 537140 \pmod{89403930}. \end{aligned}$$

Rõ ràng $x + y < 89403930$ nên ta có $x + y = 537140$. Bạn đọc có thể cho là cách cộng dựa vào Định lí Trung Quốc về phần dư trên đây phức tạp hơn cách cộng "thông thường". Tuy nhiên, đó chính là cách mà máy tính sử dụng, vì nó cho phép làm các phép toán số học đối với những số lớn (khi thay chúng bởi đồng dư theo môđulô nào đó).

Khi sử dụng phương pháp trên đây, ta cần xác định các số $m_1, m_2, \ldots, m_r$ thích hợp. Mặt khác, máy tính thường dùng cơ số 2 nên ta thường gặp bài toán : *bao giờ thì hai số dạng* $2^m - 1$ *nguyên tố cùng nhau*. Điều đó được cho bởi các mệnh đề sau.

**Bổ đề 2.17.** *Giả sử* $a$, $b$ *là các số nguyên dương. Khi đó thặng dư bé nhất của* $2^a - 1$ *môđulô* $2^b - 1$ *là* $2^r - 1$, *trong đó* $r$ *là thặng dư dương bé nhất của* $a$ *môđulô* $b$.

***Chứng minh.*** Từ thuật toán chia ta có

$$a = bq + r$$

trong đó $r$ là thặng dư dương bé nhất của $a$ môđulô $b$. Mặt khác,

$$(2^a - 1) = (2^{bq+1} - 1) = (2^b - 1)(2^{b(q-r)+1} + \cdots + 2^{b+r} + 2^r) + (2^r - 1).$$

Như vậy, phần dư trong phép chia $2^a - 1$ cho $2^b - 1$ là $2^r - 1$, đó chính là thặng dư dương bé nhất của $2^a - 1$ môđulô $2^b - 1$.

**Bổ đề 2.18.** *Nếu $a$ và $b$ là các số nguyên dương thì ước chung lớn nhất của $2^a - 1$ và $2^b - 1$ là $2^{(a,b)} - 1$.*

***Chứng minh.*** Dùng thuật chia Ơ-clit với $a = r_0$, $b = r_1$ ta được :

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 , && 0 \le r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3 , && 0 \le r_3 < r_2 \\
&\cdots\cdots \\
r_{n-3} &= r_{n-2} q_{n-2} + r_{n-1} , && 0 \le r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1} q_{n-1} ,
\end{aligned}$$

trong đó phần dư cuối cùng $r_{n-1}$ là ước chung lớn nhất của $a$ và $b$. Theo Bổ đề 2.17, khi áp dụng thuật toán Ơ-clit cho cặp $2^a - 1 = R_0$, $2^b - 1 = R_1$, ta được :

$$\begin{aligned}
R_0 &= R_1 Q_1 + R_2 , && R_2 = 2^{r_2} - 1 \\
R_1 &= R_2 Q_2 + R_3 , && R_3 = 2^{r_3} - 1 \\
&\cdots\cdots \\
R_{n-3} &= R_{n-2} Q_{n-2} + R_{n-1} , && R_{n-1} = 2^{r_{n-1}} - 1 \\
R_{n-2} &= R_{n-1} Q_{n-1} .
\end{aligned}$$

Ở đây, phần dư khác 0 cuối cùng $R_{n-1} = 2^{r_{n-1}} - 1 = 2^{(a,b)} - 1$. □

**Định lí 2.19.** *Các số nguyên dương $2^a - 1$ và $2^b - 1$ nguyên tố cùng nhau khi và chỉ khi $a$, $b$ nguyên tố cùng nhau.*

## § 4. ĐỊNH LÍ PHECMA BÉ VÀ ĐỊNH LÍ WILSON

Trong mục này, ta sẽ nghiên cứu hai đồng dư rất quan trọng, có nhiều ứng dụng trong số học.

**Định lí 2.20** (Định lí Wilson). *Với mọi số nguyên tố $p$, ta có*

$$(p - 1)! \equiv -1 \pmod{p}.$$

***Chứng minh.*** Khi $p = 2$, ta có : $(p - 1)! \equiv 1 \equiv -1 \pmod{2}$. Như vậy, định

lí Wilson đúng với $p = 2$. Bây giờ, giả sử $p$ là là số nguyên tố lớn hơn 2. Khi đó, với mỗi số nguyên $a$ với $1 \le a \le p-1$, tồn tại nghịch đảo $\overline{a}$, $1 \le \overline{a} \le p-1$ sao cho $a\overline{a} \equiv 1 \pmod{p}$. Theo Mệnh đề 2.15, các số nguyên dương nhỏ hơn $p$ mà là nghịch đảo của chính nó là 1 và $p-1$. Như vậy, ta có thể nhóm các số nguyên từ 2 đến $p-2$ thành $\frac{p-3}{p}$ cặp, mà tích của chúng đồng dư 1 môđulô $p$. Do đó

$$2.3\ldots(p-3)(p-2) \equiv 1 \pmod{p}.$$

Nhân hai vế với 1 và $p-1$ ta được

$$(p\text{-}1)! \equiv 1.(p-1) \equiv -1 \pmod{p}.$$

Mệnh đề đảo của Định lí Wilson cũng đúng. □

**Định lí 2.21.** *Giả sử $n$ là số nguyên dương sao cho $(n-1)! \equiv -1 \pmod{n}$. Khi đó $n$ là số nguyên tố.*

Chứng minh. Giả sử ngược lại, $n$ là hợp số và $(n-1)! \equiv -1 \pmod{n}$. Vì $n$ là hợp số, ta có : $n = ab$, trong đó $1 < a < n$ và $1 < b < n$. Khi đó $a \mid (n-1)!$. Mặt khác, do $(n-1)! \equiv -1 \pmod{n}$ nên $n \mid [(n-1)!+1]$, suy ra $a \mid [(n-1)!+1]$. Như vậy, $a \mid (n-1)!$ và $a \mid [(n-1)!+1]$ nên $a \mid 1$ : mâu thuẫn. □

Khi ta xét các đồng dư có sự tham gia của các lũy thừa, định lí sau đây là hết sức quan trọng.

**Định lí 2.22** (Định lí Phecma bé). *Giả sử $p$ nguyên tố và $a$ là số nguyên dương với $p \nmid a$. Khi đó $a^{p-1} \equiv 1 \pmod{p}$.*

***Chứng minh.*** Xét $p-1$ số nguyên $a, 2a, \ldots, (p-1)a$. Không số nguyên nào trong các số nói trên chia hết cho $p$, vì nếu $p \mid ja$ với $j$ nào đó thì $p \mid j$ do $(a,p) = 1$. Mà ta có $1 \le j \le p-1$. Hơn nữa, không có hai số nguyên nào trong dãy trên đồng dư môđulô $p$. Thật vậy nếu $ja \equiv ka \pmod{p}$ thì do $(a,p) = 1$ nên suy ra $j \equiv k \pmod{p}$, tức là $j = k$, (vì $1 \le j,\ k \le p-1$). Như vậy, các số nguyên $a, 2a, \ldots, (p-1)a$ là tập hợp $(p-1)$ số nguyên không đồng dư 0 và không có hai số nào đồng dư nhau môđulô $p$, nên các thặng dư dương bé nhất của hệ đó phải là $1, 2, \ldots, p-1$ xếp theo thứ tự nào đó. Từ đó suy ra

$$a.2a\ldots(p-1)a \equiv 1.2\ldots(p-1) \pmod{p}.$$

Vậy

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Vì $((p-1)!, p) = 1$ nên ta được

$$a^{p-1} \equiv 1 \pmod{p}.$$

**Hệ quả 2.23.** *Giả sử $p$ là số nguyên tố và $a$ là số nguyên dương. Khi đó $a^p \equiv a \pmod{p}$.*

***Chứng minh.*** Nếu $p \nmid a$ thì theo Định lí Phecma bé, ta có

$$a^{p-1} \equiv 1 \pmod{p}.$$

Nhân hai vế với $a$ ta được

$$a^p \equiv a \pmod{p}.$$

Ngược lại, nếu $p \mid a$ thì $p \mid a^p$ nên $a^p \equiv a \equiv 0 \pmod{p}$. □

**Hệ quả 2.24.** *Giả sử $p$ là số nguyên tố và $a$ là số nguyên với $p \nmid a$. Khi đó $a^{p-2}$ là nghịch đảo của $a$ môđulô $p$.*

***Chứng minh.*** Giả sử $p \nmid a$. Khi đó theo Định lí Phecma bé ta có

$$a.a^{p-2} = a^{p-1} \equiv 1 \pmod{p}.$$

Vậy $a^{p-2}$ là nghịch đảo của $a$ môđulô $p$. □

**Hệ quả 2.25.** *Giả sử $a$, $b$ là các số nguyên dương và $p$ là số nguyên tố, $p \nmid a$. Khi đó nghiệm của đồng dư tuyến tính*

$$ax \equiv b \pmod{p}$$

*là các số nguyên $x$ sao cho $x \equiv a^{p-2}b \pmod{p}$.*

***Chứng minh.*** Giả sử $ax \equiv b \pmod{p}$. Vì $p \nmid a$ nên $a^{p-2}$ là một nghịch đảo của $a \pmod{p}$. Từ đó ta có :

$$x \equiv a^{p-2}ax \equiv a^{p-2}b \pmod{p}.$$ □

## § 5. SỐ GIẢ NGUYÊN TỐ

Theo Định lí Phecma bé, nếu $n$ là số nguyên tố thì với mọi số nguyên

$b$ ta có $b^n \equiv b \pmod{n}$. Như vậy, nếu có số nguyên $b$ sao cho $b^n \not\equiv b \pmod{n}$ thì $n$ phải là hợp số. Tuy nhiên, Định lí Phecma bé lại không cho ta cách kiểm tra xem một số $n$ có phải là số nguyên tố hay không. Nói cách khác, phần đảo của Định lí Phecma bé không phải bao giờ cũng đúng. Ví dụ, với $n = 341$, $b = 2$ ta có : $n = 11.31$,

$$2^{340} = (2^{10})^{31} \equiv 1 \pmod{11};$$

$$2^{340} = (2^5)^{68} = (32)^{68} \equiv 1 \pmod{31}.$$

Từ đó suy ra $2^{340} \equiv 1 \pmod{341}$, nhưng $n = 341$ là hợp số.

**Định nghĩa 2.26.** Giả sử $b$ là một số nguyên dương. Nếu $n$ là một hợp số nguyên dương và $b^n \equiv b \pmod{n}$ thì $n$ được gọi là số *giả nguyên tố cơ sở* $b$.

Ví dụ trên đây cho thấy rằng 341 là một số giả nguyên tố cơ sở 2.

Chú ý rằng, nếu $(b,n) = 1$ thì từ $b^n \equiv b \pmod{n}$, ta suy được $b^{n-1} \equiv 1 \pmod{n}$. Ta cũng thường dùng đẳng thức này để làm định nghĩa cho các số giả nguyên tố cơ sở $b$ và nguyên tố cùng nhau với $b$.

Các số giả nguyên tố rất "thưa", chẳng hạn trong $10^{10}$ số tự nhiên đầu tiên có 455.052.512 số nguyên tố, nhưng chỉ có 14.884 số giả nguyên tố cơ sở 2. Tuy nhiên, với mọi số nguyên $b > 1$, tồn tại vô hạn số giả nguyên tố cơ sở $b$. Ta sẽ chứng minh điều này cho trường hợp $b = 2$. Trước hết ta có bổ đề sau.

**Bổ đề 2.27.** *Giả sử $d$, $n$ là các số nguyên dương sao cho $d \mid n$. Khi đó $(2^d - 1) \mid (2^n - 1)$.*

***Chứng minh.*** Vì $d \mid n$ nên tồn tại số nguyên $t$ để $dt = n$. Đặt $x = 2^d$, từ khai triển $x^t - 1 = (x-1)(x^{t-1} + x^{t-2} + \cdots + 1)$ ta có :

$$2^n - 1 = (2^d - 1)(2^{d(t-1)} + 2^{d(t-2)} + \cdots + 2^d + 1),$$

tức là $(2^d - 1) \mid (2^n - 1)$. □

**Định lí 2.28.** *Tồn tại vô hạn số giả nguyên tố cơ sở 2.*

***Chứng minh.*** Giả sử $n$ là một số giả nguyên tố cơ sở 2. Ta sẽ chứng tỏ rằng, $m = 2^n - 1$ cũng là số giả nguyên tố cơ sở 2. Theo giả thiết, $n$ là hợp số, chẳng hạn $n = dt$ $(1 < d, t < n)$ và $2^{n-1} \equiv 1 \pmod{n}$. Vì

$(2^d - 1) \mid (2^n - 1)$ nên $m$ là hợp số. Do $n$ là số giả nguyên tố, $2^n \equiv 2 \pmod{n}$, tức là tồn tại $k$ sao cho $2^n - 2 = kn$. Ta có : $2^{m-1} = 2^{2^n - 2} = 2^{(kn+2)-2} = 2^{kn}$. Do đó

$$m = (2^n - 1) \mid (2^{nk} - 1) = 2^{m-1} - 1,$$

tức là

$$2^{m-1} \equiv 1 \pmod{m}.$$

Vậy $m$ là số giả nguyên tố cơ số 2. □

Để kiểm tra xem một số có phải là số nguyên tố hay không, trước tiên ta xem nó có là số giả nguyên tố cơ sở 2 hay không, sau đó tiếp tục kiểm tra đối với các cơ sở khác. Tuy nhiên, mặc dù các hợp số giả nguyên tố "rất ít", vẫn tồn tại vô hạn hợp số là giả nguyên tố với bất kì cơ sở nào !.

**Định nghĩa 2.29.** Hợp số nguyên $n$ thỏa mãn $b^{n-1} \equiv 1 \pmod{n}$ với mọi số nguyên dương $b$ sao cho $(b, n) = 1$ được gọi là số *Carmichael*.

***Ví dụ :*** Số nguyên $561 = 3.11.17$ là một số Carmichael. Thật vậy, nếu $(b, 561) = 1$ thì $(b, 3) = (b, 11) = (b, 17) = 1$. Theo Định lí Phecma bé ta có :

$$b^2 \equiv 1 \pmod{3}\ ;\ b^{10} \equiv 1 \pmod{11}\ ;\ b^{16} \equiv 1 \pmod{17}.$$

Do đó, viết 560 dưới dạng $560 = 2.280 = 10.56 = 16.35$ ta có :

$$b^{560} = (b^2)^{280} \equiv 1 \pmod{3},$$

$$b^{560} = (b^{10})^{56} \equiv 1 \pmod{11},$$

$$b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}.$$

Từ đó suy ra

$$b^{560} \equiv 1 \pmod{561}.$$

Sự kiện tồn tại vô hạn số Carmichael mới được chứng minh vào năm 1993.

Định lí sau đây cho ta một cách tìm các số Carmichael.

**Định lí 2.30.** *Nếu $n = q_1 q_2 \ldots q_k$, trong đó $q_j$ là các số nguyên tố khác nhau thỏa mãn $(q_j - 1) \mid (n - 1)$ thì $n$ là một số Carmichael.*

***Chứng minh.*** Thật vậy, giả sử $b$ là số nguyên dương và $(b, n) = 1$. Khi đó $(b, q_j) = 1$ với mọi $j = 1, 2, \ldots, k$ nên ta có :

$$b^{q_j - 1} \equiv 1 \pmod{q_j}.$$

Do $(q_j - 1) \mid (n-1)$ nên

$$b^{n-1} \equiv 1 \pmod{q_j},$$

từ đó suy ra $b^{n-1} \equiv 1 \pmod{n}$. □

Phần đảo của định lí trên đây cũng đúng, nhưng chứng minh của nó vượt quá khuôn khổ của cuốn sách này.

## § 6. ỨNG DỤNG ĐỒNG DƯ ĐỂ TÌM DẤU HIỆU CHIA HẾT

Lí thuyết đồng dư có thể áp dụng để tìm dấu hiệu chia hết của các số nguyên dựa trên khai triển của chúng trong các cơ số khác nhau.

Trước tiên ta xét vài dấu hiệu chia hết trong cơ số 10. Giả sử $n = (a_k a_{k-1} \dots a_1 a_0)_{10}$. Khi đó

$$n = a_k.10^k + a_{k-1}.10^{k-1} + \dots + a_1.10 + a_0,$$

với $0 \le a_j \le q,\ j = 0,1,2,\dots,k.$

Trước hết ta xét dấu hiệu chia hết cho một lũy thừa của 2. Do $10 \equiv 0 \pmod 2$ nên $10^j \equiv 0 \pmod{2^j}$ với mọi số nguyên $j$. Ta có :

$$n \equiv (a_0)_{10} \pmod 2$$

$$n \equiv (a_1 a_0)_{10} \pmod{2^2}$$

$$\dots$$

$$n \equiv (a_{j-1} a_{j-2} \dots a_2 a_1 a_0)_{10} \pmod{2^j}.$$

Các đồng dư trên đây chỉ ra rằng, số nguyên $n$ chia hết cho 2 khi và chỉ khi số tận cùng chia hết cho 2. Tương tự, số nguyên $n$ chia hết cho $2^j$ khi và chỉ khi số nguyên lập nên bởi $j$ chữ số tận cùng của $n$ chia hết cho $2^j$.

***Ví dụ :*** Xét $n = 32688048$. Ta có $2 \mid n$, vì $2 \mid 6$ ; $4 \mid n$ vì $4 \mid 48$ ; $8 \mid n$ vì $8 \mid 48$ ; $16 \mid n$ vì $16 \mid 8048$ nhưng $32 \nmid n$ vì $32 \nmid 88048$.

Để xét dấu hiệu chia hết cho lũy thừa của 5, trước tiên ta nhận xét rằng $10 \equiv 0 \pmod 5$ nên $10^j \equiv 0 \pmod{5^j}$. Như vậy, dấu hiệu chia hết cho 5 cũng tương tự như dấu hiệu chia hết cho 2. Để xem $n$ có chia hết cho $5^j$ hay không, ta chỉ cần xem số nguyên lập bởi $j$ chữ số tận cùng của $n$ chia hết cho $5^j$ hay không.

***Ví dụ :*** $n = 15535375$. Vì $125 \mid 375$, $625 \nmid 5375$ nên $125 \mid n$, $625 \nmid n$.

Bây giờ ta xét dấu hiệu chia hết cho 3 và 9. Ta thấy $10 \equiv 1 \pmod 3$ và $10 \equiv 1 \pmod 9$ nên $10^k \equiv 1 \pmod 3$)3), $10^k \equiv 1 \pmod 9$ với mọi $k$. Do đó

$$\begin{aligned}(a_k a_{k-1} \ldots a_0)_{10} &\equiv a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_0 \\ &\equiv a_k + a_{k-1} + \cdots + a_0 \pmod 3 \text{ và } \pmod 9.\end{aligned}$$

Như vậy, một số chia hết cho 3 (cho 9) khi và chỉ khi tổng các chữ số của nó chia hết cho 3 (cho 9).

Ta cũng có thể tìm dấu hiệu đơn giản để nhận biết một số nguyên dương có chia hết cho 11 hay không. Ta có $10 \equiv -1 \pmod{11}$. Do đó

$$\begin{aligned}(a_k a_{k-1} \ldots a_1 a_0)_{10} &\equiv a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1.10 + a_0 \\ &\equiv a_k(-1)^k + a_{k-1}(-1)^{k-1} + \cdots - a_1 + a_0 \pmod{11}.\end{aligned}$$

Như vậy, $(a_k a_{k-1} \ldots a_1 a_0)$ chia hết cho 11 khi và chỉ khi $a_0 - a_1 + a_2 - \cdots + (-1)^k a_k$ (lập bởi tổng đan dấu các chữ số) chia hết cho 11.

***Ví dụ :*** $n = 723160823$. Tổng đan dấu cần xét là

$$3 - 2 + 8 - 0 + 6 - 1 + 3 - 2 + 7 = 22.$$

Vậy $11 \mid n$.

Ta chuyển sang xét dấu hiệu chia hết cho 7, 11, 131. Ta có : $7.11.13 = 1001$, $10^3 = 1000 \equiv -1 \pmod{1001}$. Do đó

$$\begin{aligned}(a_k a_{k-1} \ldots a_1 a_0)_{10} &= a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1.10 + a_0 \\ &\equiv (a_0 + 10a_1 + 100a_2) + 1000(a_3 + 10a_4 + 100a_5) + \\ &\quad + 1000^2(a_6 + 10a_7 + 100a_8) + \cdots \\ &\equiv (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + \\ &\quad + (100a_8 + 10a_7 + a_6) - \cdots \\ &\equiv (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - \cdots \pmod{1001}.\end{aligned}$$

Như vậy, một số nguyên chia hết cho 7, 11, 13 khi và chỉ khi tổng đan dấu của các số lập nên bởi các bộ 3 chữ số, nhóm từ bên phải, chia hết cho 7, 11, hoặc 13.

*Ví dụ :* Xét $n = 59358208$. Ta có tổng đan dấu cần xét là $208 - 358 + 59 = -91$ : chia hết cho $7$, $13$ nhưng không chia hết cho $11$. Vậy $7 \mid n$, $13 \mid n$ nhưng $11 \nmid n$.

Bây giờ ta chuyển sang xét dấu hiệu chia hết của các số biểu diễn trong cơ số $b$.

**Dấu hiệu 1.** *Giả sử $a \mid b$, $j$ và $k$ là các số nguyên dương, $j < k$. Khi đó $(a_k a_{k-1} \dots a_1 a_0)_b$ chia hết cho $d^j$ nếu và chỉ nếu $(a_{j-1} \dots a_1 a_0)_b$ chia hết cho $d^j$.*

***Chứng minh.*** Vì $b \equiv 0 \pmod{d}$ nên $b^j \equiv 0 \pmod{d^j}$. Do đó

$$\begin{aligned}(a_k a_{k-1} \dots a_1 a_0)_b &= a_k b^k + \dots + a_j b^j + a_{j-1} b^{j-1} + \dots + a_1 b + a_0 \\ &\equiv a_{j-1} b^{j-1} + \dots + a_1 b + a_0 \\ &\equiv (a_{j-1} \dots a_1 a_0)_b \pmod{d^j}.\end{aligned}$$

Do đó $d \mid (a_k \dots a_1 a_0)_b$ khi và chỉ khi $d \mid (a_{j-1} \dots a_1 a_0)_b$. □

**Dấu hiệu 2.** *Giả sử $d \mid (b-1)$, khi đó $n = (a_k \dots a_1 a_0)_b$ chia hết cho $d$ khi và chỉ khi $a_k + \dots + a_1 + a_0$ chia hết cho $d$.*

***Chứng minh.*** Vì $d \mid (b-1)$, ta có $b \equiv 1 \pmod{d}$. Do đó $b^j \equiv 1 \pmod{d}$ với mọi số nguyên dương $b$. Vậy,

$$(a_k \dots a_1 a_0)_b = a_k b^k + \dots + a_1 b + a_0 \equiv a_k + \dots + a_1 + a_0 \pmod{d}.$$

Từ đó suy ra $d \mid n$ nếu và chỉ nếu $d \mid (a_k + \dots + a_1 + a_0)$. □

**Dấu hiệu 3.** *Giả sử $d \mid (b+1)$. Khi đó $n = (a_k \dots a_1 a_0)$ chia hết cho $d$ nếu và chỉ nếu $(-1)^k a_k + \dots - a_1 + a_0$ chia hết cho $d$.*

***Chứng minh.*** Vì $d \mid (b+1)$ nên $b \equiv -1 \pmod{d}$. Do đó $b^j \equiv (-1)^j \pmod{d}$ và $n = (a_k \dots a_1 a_0)_b \equiv (-1)^k a_k + \dots - a_1 + a_0 \pmod{d}$. Suy ra $d \mid n$ nếu và chỉ nếu $d \mid ((-a)^k a_k + \dots - a_1 + a_0)$. □

*Ví dụ :* $n = (1001001111)_2$. Khi đó $n \equiv 1 - 1 + 1 - 1 + 0 - 0 + 1 - 0 + 0 - 1 \equiv 0 \pmod{3}$. Vậy $3 \mid n$.

## BÀI TẬP CHƯƠNG 2

**1.** Chứng minh rằng nếu $a$ là số nguyên chẵn thì $a^2 \equiv 0 \pmod 4$, nếu $a$ là số nguyên lẻ thì $a^2 \equiv 1 \pmod 4$.

**2.** Chứng minh rằng nếu $a$ là số nguyên lẻ thì $a^2 \equiv 1 \pmod 8$.

**3.** Chứng minh rằng nếu $a$, $b$, $m$ là các số nguyên và $m > 0$, $n > 0$, $n \mid b$, $a \equiv b \pmod m$ thì $a \equiv b \pmod n$.

**4.** Chứng minh rằng nếu $a$, $b$, $c$, $m$ là các số nguyên, $c > 0$, $m > 0$, $a \equiv b \pmod m$ thì $ac \equiv bc \pmod{mc}$.

**5.** Chứng minh rằng nếu $a$, $b$, $c$ là các số nguyên, $c > 0$, sao cho $a \equiv b \pmod c$, thì $(a,c) = (b,c)$.

**6.** Giả sử $a^k \equiv b^k \pmod m$, $a^{k+1} \equiv b^{k+1} \pmod m$ trong đó $a$, $b$, $k$, $m$ là các số nguyên với $k > 0$, $m > 0$ sao cho $(a,m) = 1$. Chứng minh rằng $a \equiv b \pmod m$. Nếu điều kiện $(a,m) = 1$ không thỏa mãn, kết luận còn đúng hay không ?

**7.** Với số nguyên $n$ nào ta có

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 \equiv 0 \pmod n ?$$

**8.** Chứng minh rằng nếu $n \equiv 3 \pmod 4$ thì $n$ không thể là tổng của hai số chính phương.

**9.** a) Chứng minh rằng nếu $p$ là số nguyên tố thì các nghiệm của đồng dư $x^2 \equiv x \pmod p$ chỉ là các số nguyên $x$ sao cho $x \equiv 0$ hoặc $x \equiv 1 \pmod p$.

b) Chứng minh rằng nếu $p$ là số nguyên tố, và $k$ là số nguyên dương thì các nghiệm của đồng dư $x^2 \equiv x \pmod{p^k}$ là các số nguyên $x$ sao cho $x \equiv 0$ hoặc $x \equiv 1 \pmod{p^k}$.

**10.** Giả sử $a$, $b$, $m$ là các số nguyên dương $(a,m) = 1$. Chứng minh rằng nếu $x$ là nghiệm của $ax \equiv b \pmod m$ thì $x$ cũng là nghiệm của

$$a_1 x \equiv b\left[\frac{m}{a}\right] \pmod m,$$

trong đó $a_1$ là thặng dư dương bé nhất của $m$ môđulô $a$.

**11.** Chứng minh rằng với cách làm như trong Bài tập 10, xuất phát từ $ax \equiv b \pmod{m}$ ta được dãy $a_0 = a > a_1 > a_2 > \cdots > a_n = 1$ với $n$ nào đó. (Khi đó ta có nghiệm $x \equiv B \pmod{m}$).

**12.** Dùng Bài tập 11 để tìm $x$ sao cho $6x \equiv 7 \pmod{23}$.

**13.** Chứng minh rằng nếu $\bar{a}$ là một nghịch đảo của $a$ môđulô $m$, $\bar{b}$ là nghịch đảo của $b$ môđulô $m$, thì $\bar{a}\bar{b}$ là nghịch đảo của $ab$ môđulô $m$.

**14.** Tìm nghiệm của các hệ đồng dư sau :

a) $\begin{cases} x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod{17} \end{cases}$

b) $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$

c) $\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}$

d) $\begin{cases} x \equiv 2 \pmod{11} \\ x \equiv 3 \pmod{12} \\ x \equiv 4 \pmod{13} \\ x \equiv 5 \pmod{17} \\ x \equiv 6 \pmod{19} \end{cases}$

**15.** Tìm một số chia hết cho 11 sao cho khi chia cho 2, 3, 5, 7 đều dư 1.

**16.** Chứng minh rằng với mọi $n$, đều tồn tại $n$ số tự nhiên liên tiếp sao cho mỗi một trong chúng đều có ít nhất một ước số là chính phương.

**17.** Chứng minh rằng nếu $a$, $b$, $c$ là các số nguyên với $(a,b) = 1$ thì tồn tại số nguyên $n$ sao cho $(an + b, c) = 1$.

**18.** Chứng minh rằng hệ các đồng dư

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

có nghiệm nếu và chỉ nếu $(m_1, m_2) \mid (a_1 - a_2)$. Hơn nữa, khi đó tồn tại nghiệm duy nhất môđulô $[m_1, m_2]$.

**19.** Dùng Bài tập 18 để tìm nghiệm các hệ đồng dư sau

a) $\begin{cases} x \equiv 4 \pmod 6 \\ x \equiv 13 \pmod{15} \end{cases}$ b) $\begin{cases} x \equiv 7 \pmod{10} \\ x \equiv 4 \pmod{15}. \end{cases}$

**20.** Chứng minh rằng hệ các đồng dư

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

có nghiệm nếu và chỉ nếu $(m_i, m_j) \mid (a_i - a_j)$ với mọi cặp số nguyên $(i, j)$, $1 \le i < j \le r$. Chỉ ra rằng, nếu nghiệm tồn tại thì nó là duy nhất môđulô $[m_1, m_2, \ldots, m_r]$.

**21.** Dùng Bài tập 20, giải các hệ đồng dư sau đây :

a) $\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 3 \pmod{10} \\ x \equiv 8 \pmod{15} \end{cases}$ b) $\begin{cases} x \equiv 2 \pmod{14} \\ x \equiv 16 \pmod{21} \\ x \equiv 10 \pmod{30} \end{cases}$

c) $\begin{cases} x \equiv 2 \pmod 9 \\ x \equiv 8 \pmod{15} \\ x \equiv 10 \pmod{25} \end{cases}$ d) $\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 4 \pmod 8 \\ x \equiv 2 \pmod{14} \\ x \equiv 14 \pmod{15} \end{cases}$

e) $\begin{cases} x \equiv 7 \pmod 9 \\ x \equiv 2 \pmod{10} \\ x \equiv 3 \pmod{12} \\ x \equiv 6 \pmod{15}. \end{cases}$

**22.** Một tập hợp $S$ các đồng dư (với môđulô khác nhau) được gọi là *một tập phủ đồng dư* nếu mỗi số nguyên thỏa mãn ít nhất một đồng dư thuộc $S$.

Chứng minh rằng các tập hợp đồng dư sau đây là các phủ đồng dư :

a) $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 4$,
$x \equiv 1 \pmod 6$, $x \equiv 11 \pmod{12}$.

b) $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 0 \pmod 5$,
$x \equiv 0 \pmod 7$, $x \equiv 1 \pmod 6$, $x \equiv 1 \pmod{10}$,
$x \equiv 1 \pmod{14}$, $x \equiv 2 \pmod{15}$, $x \equiv 2 \pmod{21}$,
$x \equiv 23 \pmod{30}$, $x \equiv 4 \pmod{35}$, $x \equiv 5 \pmod{42}$,
$x \equiv 59 \pmod{70}$, $x \equiv 104 \pmod{105}$.

**23.** Tìm lũy thừa cao nhất của 2 chia hết các số sau đây :

a) 201984 b) 1423408

c) 89375744 d) 41578912246 .

**24.** Tìm lũy thừa cao nhất của 5 chia hết các số sau đây :

a) 112250 b) 4860625

c) 235555790 d) 48126953125.

**25.** Trong các số nguyên dương chỉ gồm toàn chữ số 1, số nào chia hết cho 7 ? cho 13 ? Những số nào ít hơn 10 chữ số và là số nguyên tố ?

**26.** Xét các số mà trong biểu diễn cơ số $b$ gồm toàn chữ số 1.

a) Số nào chia hết cho các ước số của $b-1$ ?

b) Số nào chia hết cho các ước số của $b+1$ ?

**27.** Hãy tìm dấu hiệu chia hết cho 37.

**28.** Tìm dấu hiệu chia hết cho số $n$ trong cơ số $b$, trong đó $n$ là ước của $b^2+1$.

**29.** Áp dụng Bài tập 28, trả lời các câu hỏi sau :

a) $(101110110)_2$ chia hết cho 5 hay không ?

b) $(12100122)_3$ chia hết cho 2, cho 5 ?

c) $(364701244)_8$ chia hết cho 5, cho 13 ?

d) $(5837041320219)_{10}$ chia hết cho 101?

**30.** Tìm thặng dư $2^{1000000}$ môđulô 17, $3^{10}$ 121.

**31.** Tìm chữ số cuối cùng của $3^{100}$ trong cơ số 7.

**32.** Chứng minh rằng nếu $n$ là hợp số nguyên, $n \neq 4$ thì $(n-1)! \equiv 0 \pmod{n}$.

**33.** Chứng minh rằng nếu $p$ là số nguyên tố lẻ thì $2(p-3)! \equiv -1 \pmod{p}$.

**34.** Chứng minh rằng nếu $n$ lẻ, $3 \nmid n$ thì $n^2 \equiv 1 \pmod{24}$.

**35.** Chứng minh rằng $42 \mid (n^7 - n)$ với mọi số nguyên dương $n$.

**36.** Chứng minh rằng nếu $p$, $q$ là các số nguyên tố khác nhau thì

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

**37.** Chứng minh rằng nếu $p$ là số nguyên tố, $a$ và $b$ là các số nguyên sao cho $a^p \equiv b^p \pmod{p}$ thì $a^p \equiv b^p \pmod{p^2}$.

**38.** Chứng minh rằng nếu $p$ là số nguyên tố lẻ thì

$$1^2.3^2 \ldots (p-4)^2.(p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

**39.** Chứng minh rằng nếu $p$ là số nguyên tố và $p \equiv 3 \pmod{4}$ thì

$$[(p-1)/2]! \equiv \pm 1 \pmod{p}.$$

**40.** Giả sử $p$ là số nguyên tố, $r$ là số nguyên dương nhỏ hơn $p$ sao cho $(-1)^r r! \equiv -1 \pmod{p}$. Chứng minh rằng

$$(p-r+1)! \equiv -1 \pmod{p}.$$

Áp dụng chứng minh $61! \equiv 63! \equiv -1 \pmod{71}$.

**41.** Chứng minh rằng nếu $p$ là số nguyên tố, $p \equiv 1 \pmod{4}$ thì đồng dư $x^2 \equiv -1 \pmod{p}$ có hai nghiệm không đồng dư cho bởi

$$x \equiv \pm 1((p-1)/2)! \pmod{p}.$$

**42.** Chứng minh rằng nếu $p$ là số nguyên tố và $0 < k < p$, thì

$$(p-k)!(k-1)! \equiv (-1)^k \pmod{p}.$$

**43.** Chứng minh rằng nếu $p$ là số nguyên tố và $a$ nguyên thì

$$p! \mid (a^p + (p-1)!a).$$

**44.** Với $n$ nào thì $n^4 + 4^n$ là số nguyên tố ?

**45.** Chứng minh rằng $n$ và $n+2$ là cặp số nguyên tố sinh đôi nếu và chỉ nếu $4[(n-1)!+1]+n \equiv 0 \pmod{n(n+2)}$, trong đó $n \neq 1$.

**46.** Chứng minh rằng các số nguyên dương $n$ và $n+k$, trong đó $n > k$, $k$ là số nguyên dương chẵn, đều là nguyên tố nếu và chỉ nếu

$$(k!)^2[(n-1)!+1]+n(k!-1)(k-1)! \equiv 0 \pmod{n(n+k)}.$$

**47.** Chứng minh rằng nếu $p$ nguyên tố thì $C_{2p}^{p} \equiv 2 \pmod{p}$.

**48.** Chứng minh rằng nếu $a$, $b$ là các số nguyên, $p$ nguyên tố thì

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

**49.** Cho $m$ là số nguyên dương. Chứng minh rằng tích các số nguyên dương nhỏ hơn $m$ và nguyên tố cùng nhau với $m$ đồng dư $1 \pmod{m}$, trừ các trường hợp $m = 4$, $m = p^t$ hoặc $m = 2p^t$, trong đó $p$ là số nguyên tố lẻ, $t$ là số nguyên dương. Trong các trường hợp đó, tích nói trên $\equiv -1 \pmod{m}$.

**50.** Giả sử $p$ là số nguyên tố và $a_1, a_2, \ldots, a_p$; $b_1, b_2, \ldots, b_p$ là các hệ thặng dư đầy đủ môđulô $p$. Chứng minh rằng $a_1b_1$, $a_2b_2$, ..., $a_pb_p$ không phải là hệ thặng dư đầy đủ môđulô $p$.

**51.** Chứng minh rằng 91 là số giả nguyên tố cơ sở 3.

**52.** Chứng minh rằng 45 là số giả nguyên tố cơ sở 17 và 19.

**53.** Chứng minh rằng các số $n = 161038$ thỏa mãn $2^n \equiv 2 \pmod{n}$; số 161038 là số giả nguyên tố chẵn bé nhất cơ sở 2.

**54.** Chứng minh rằng nếu $n$ là hợp số lẻ và $n$ là số giả nguyên tố cơ sở $a$, thì $n$ là số giả nguyên tố cơ sở $n-a$.

**55.** Chứng minh rằng nếu $n = (a^{2p}-1)/(a^2-1)$, trong đó $a$ là số nguyên, $a > 1$ và $p$ là số nguyên tố lẻ, $p \nmid a(a^2-1)$ thì $n$ là số giả nguyên tố cơ sở $a$. Từ đó suy ra có vô hạn số giả nguyên tố cơ số $a$ tùy ý.

**56.** Chứng minh rằng nếu số Phecma $F_m = 2^{2^m}+1$ là hợp số, thì nó là số giả nguyên tố cơ sở 2.

**57.** Giả sử $p$ là số nguyên tố sao cho $2^p - 1$ là hợp số. Chứng minh rằng

$2^p - 1$ là số giả nguyên tố cơ sở 2.

58. Chứng minh rằng nếu $n$ là số giả nguyên tố cơ sở $a$ và $b$, thì $n$ là số giả nguyên tố cơ sở $ab$.

59. Chứng minh rằng nếu $n$ là số giả nguyên tố cơ sở $a$, thì $n$ cũng là số giả nguyên tố cơ sở $\overline{a}$, trong đó $\overline{a}$ là nghịch đảo của $a$ môđulô $m$.

60. Chứng minh rằng nếu $n$ là số giả nguyên tố cơ sở $a$, nhưng không giả nguyên tố cơ sở $b$ thì $n$ không là số giả nguyên tố cơ sở $ab$.

61. Chứng minh rằng nếu tồn tại một số nguyên $b$ với $(b,n) = 1$, sao cho $n$ không là số giả nguyên tố cơ sở $b$, thì số các số $a$ sao cho $n$ là giả nguyên tố cơ sở $a$ không vượt quá số các số bé hơn $n$ và nguyên tố cùng nhau với $n$.

Chương 3.

# MỘT SỐ HÀM THƯỜNG GẶP VÀ ỨNG DỤNG

## § 1. CÁC HÀM CÓ TÍNH CHẤT NHÂN

**Định nghĩa 3.1.** Một hàm xác định trên tập hợp các số nguyên dương gọi là *hàm số học*.

Nói chung, ta quan tâm đến các hàm số học có tính chất sau.

**Định nghĩa 3.2.** Hàm số học $f$ được gọi là *có tính chất nhân* nếu $f(mn) = f(m)f(n)$ khi $m$, $n$ nguyên tố cùng nhau.

***Ví dụ :*** Hàm $f(n) = 1$ với mọi $n$ là một hàm có tính chất nhân. Tương tự như vậy, hàm $g(n) = n$ cũng có tính chất nhân. Hơn nữa, với mọi $m$, $n$ (không nhất thiết nguyên tố cùng nhau) ta có : $g(mn) = g(m)g(n)$. Những hàm có tính chất như vậy được gọi là *hàm có tính chất nhân đầy đủ*.

Đối với những hàm có tính chất nhân, ta có thể tìm công thức đơn giản để tính $f(n)$ khi biết phân tích $n$ thành thừa số nguyên tố.

**Định lí 3.3.** *Giả sử $f$ là hàm có tính chất nhân, và*

$$n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$$

*là phân tích ra thừa số nguyên tố của $n$. Khi đó*

$$f(n) = f(p_1^{a_1}) \dots f(p_s^{a_s}).$$

***Chứng minh.*** Vì $f$ là hàm có tính chất nhân, và $(p_1^{a_1}, p_2^{a_2} \dots p_s^{a_s}) = 1$, ta có

$$f(n) = f(p_1^{a_1}).f(p_2^{a_2} \dots p_s^{a_s}).$$

Lại do $(p_2^{a_2}, p_3^{a_3} \dots p_s^{a_s}) = 1$ nên

$$f(p_2^{a_2} \dots p_s^{a_s}) = f(p_2^{a_2}) f(p_3^{a_3} \dots p_s^{a_s}).$$

Tiếp tục như vậy, ta được

$$f(n) = f(p_1^{a_1}).f(p_2^{a_2})\dots f(p_s^{a_s}).$$ □

## § 2. PHI-HÀM Ơ-LE

**Định nghĩa 3.4.** Giả sử $n$ là một số nguyên dương. *Phi-hàm Ơ-le* được định nghĩa là số các số nguyên dương không vượt quá $n$ và nguyên tố cùng nhau với $n$.

Kí hiệu Phi-hàm Ơ-le qua $\varphi(n)$.

***Ví dụ :*** $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$.

Phi-hàm Ơ-le có nhiều ứng dụng trong số học. Ở đây, trước tiên ta xét việc sử dụng Phi-hàm Ơ-le để nghiên cứu đồng dư môđulô một hợp số (tương tự như đã sử dụng Định lí Phecma bé để xét đồng dư môđulô một số nguyên tố).

**Định nghĩa 3.5.** Một hệ thặng dư thu gọn môđulô $n$ là một tập hợp gồm $\varphi(n)$ số nguyên sao cho mỗi phần tử của tập hợp đều nguyên tố cùng nhau với $n$, và không có hai phần tử khác nhau nào đồng dư môđulô $n$.

***Ví dụ :*** Tập hợp $1, 3, 5, 7$ là một hệ thặng dư thu gọn môđulô $8$. Tập hợp $-3, -1, 1, 3$ cũng vậy.

**Định lí 3.6.** *Giả sử $r_1, r_2, \dots, r_{\varphi(n)}$ là hệ thặng dư thu gọn môđulô $n$, $a$ là số nguyên dương và $(a, n) = 1$. Khi đó, tập hợp $ar_1, ar_2, \dots, ar_{\varphi(n)}$ cũng là hệ thặng dư thu gọn môđulô $n$.*

***Chứng minh.*** Trước tiên ta chứng tỏ rằng, mỗi số nguyên $ar_j$ là nguyên tố cùng nhau với $n$. Giả sử ngược lại, $(ar_j, n) > 1$ với $j$ nào đó. Khi đó tồn tại ước nguyên tố $p$ của $(ar_j, n)$. Do đó, hoặc $p \mid a$, hoặc $p \mid r_j$, tức là hoặc $p \mid a$ và $p \mid n$, hoặc $p \mid r_j$ và $p \mid n$. Tuy nhiên, không thể có $p \mid r_j$ và $p \mid n$, vì $r_j$ và $n$ nguyên tố cùng nhau. Tương tự, không thể có $p \mid a$ và $p \mid n$. Vậy, $ar_j$ và $n$ nguyên tố cùng nhau với mọi $j = 1, 2, \dots, \varphi(n)$.

Còn phải chứng tỏ không có hai số $ar_j$, $ar_k$ $(j \neq k)$ nào đồng dư nhau môđulô $n$. Giả sử $ar_j \equiv ar_k \pmod{n}$, $j \neq k$ và $1 \leq j \leq \varphi(n)$ ; $1 \leq k \leq \varphi(n)$. Vì $(a, n) = 1$ nên ta suy ra $r_j \equiv r_k \pmod{n}$. Điều này mâu thuẫn vì $r_j$, $r_k$ cùng thuộc hệ thặng dư thu gọn ban đầu môđulô $n$. □

***Ví dụ :*** Tập hợp $1, 3, 5, 7$ là một hệ thặng dư thu gọn môđulô $8$. Do $(3,8) = 1$ nên $3, 9, 15, 21$ cũng là một hệ thặng dư thu gọn môđulô $8$.

**Định lí Ơ-le.** *Giả sử $m$ là số nguyên dương và $a$ là số nguyên với $(a,m) = 1$. Khi đó $a^{\varphi(m)} \equiv 1 \pmod m$.*

***Chứng minh.*** Giả sử $r_1, r_2, \ldots, r_{\varphi(m)}$ là một hệ thặng dư thu gọn gồm các số nguyên dương không vượt quá $m$ và nguyên tố cùng nhau với $m$. Do Định lí 3.6 và do $(a,m) = 1$, tập hợp $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ cũng là một hệ thặng dư thu gọn môđulô $m$. Như vậy, các thặng dư dương bé nhất của $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ phải là các số nguyên $r_1, r_2, \ldots, r_{\varphi(m)}$ xếp theo thứ tự nào đó. Vì thế, nếu ta nhân các từ trong hệ thặng dư thu gọn trên đây, ta được :

$$ar_1.ar_2 \ldots ar_{\varphi(m)} \equiv r_1.r_2 \ldots r_{\varphi(m)} \pmod m.$$

Do đó

$$a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \equiv r_1 r_2 \ldots r_{\varphi(m)} \pmod m.$$

Vì $(r_1 r_2 \ldots r_{\varphi(m)}, m) = 1$ nên

$$a^{\varphi(m)} \equiv 1 \pmod m. \qquad \square$$

Ta có thể tìm nghịch đảo môđulô $m$ bằng cách sử dụng Định lí Ơ-le. Giả sử $a$, $m$ là các số nguyên tố cùng nhau, khi đó

$$a.a^{\varphi(m)-1} = a^{\varphi(m)} \equiv 1 \pmod m.$$

Vậy $a^{\varphi(m)-1}$ là một nghịch đảo của $a$ môđulô $m$.

***Ví dụ :*** $2^{\varphi(9)-1} = 2^{6-1} = 2^5 = 32 \equiv 5 \pmod 9$ là một nghịch đảo của $2$ môđulô $9$.

Cũng có thể giải các đồng dư tuyến tính một ẩn theo nhận xét trên. Giả sử cần giải đồng dư $ax \equiv b \pmod m$, $(a,m) = 1$. Ta nhân hai vế với $a^{\varphi(m)-1}$ :

$$a^{\varphi(m)-1} ax \equiv a^{\varphi(m)-1} b \pmod m.$$

Như vậy, nghiệm là các số nguyên $x$ sao cho $x \equiv a^{\varphi(m)-1} b \pmod m$.

***Ví dụ :*** Giải đồng dư $3x \equiv 7 \pmod{10}$ : $x = 3^{\varphi(10)-1} 7 \equiv 3^3.7 \equiv 9 \pmod{11}$.

Bây giờ ta sẽ cho công thức tính giá trị của phi-hàm Ơ-le tại $n$ khi biết

phân tích của $n$ ra thừa số nguyên tố.

**Định lí 3.7.** *Với số nguyên tố $p$ ta có : $\varphi(p) = p - 1$. Ngược lại, nếu $p$ là số nguyên dương sao cho $\varphi(p) = p - 1$, thì $p$ là số nguyên tố.*

***Chứng minh.*** Nếu $p$ là số nguyên tố thì mọi số nguyên dương nhỏ hơn $p$ đều nguyên tố cùng nhau với $p$. Do có $p - 1$ số nguyên dương như vậy nên $\varphi(p) = p - 1$.

Ngược lại, nếu $p$ là hợp số thì $p$ có ước $d$, $1 < d < p$. Tất nhiên $p$ và $d$ không nguyên tố cùng nhau. Như vậy, trong các số $1, 2, \ldots, p - 1$ phải có những số không nguyên tố cùng nhau với $p$, nên $\varphi(p) \leq p - 2$. Theo giả thiết, $\varphi(p) = p - 1$, vậy $p$ là số nguyên tố. □

**Định lí 3.8.** *Giả sử $p$ là số nguyên tố và $a$ là số nguyên dương. Khi đó $\varphi(p^a) = p^a - p^{a-1}$.*

***Chứng minh.*** Các số nguyên dương nhỏ hơn $p^a$ không nguyên tố cùng nhau với $p$ là các số không vượt quá $p^{a-1}$ và chia hết cho $p$. Có đúng $p^{a-1}$ số như vậy. Do đó tồn tại $p^a - p^{a-1}$ số nguyên nhỏ hơn $p^a$ và nguyên tố cùng nhau với $p^a$. Vậy, $\varphi(p^a) = p^a - p^{a-1}$. □

***Ví dụ :*** $\varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 100$ ; $\varphi(2^{10}) = 2^{10} - 2^9 = 512$.

Để thiết lập công thức tính $\varphi(n)$ khi biết phân tích ra thừa số của $n$, trước tiên ta cần chứng tỏ $\varphi(n)$ là hàm nhân.

**Định lí 3.9.** *Nếu $m$, $n$ là các số nguyên dương nguyên tố cùng nhau, thì*

$$\varphi(mn) = \varphi(m).\varphi(n).$$

***Chứng minh.*** Ta viết các số nguyên dương không vượt quá $mn$ thành bảng sau :

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
m & 2m & 3m & \cdots & mn
\end{array}$$

Bây giờ giả sử $r$ là một số nguyên không vượt quá $m$. Giả sử $(m, r) = d > 1$. Khi đó, không số nào trong dòng thứ $r$ nguyên tố cùng nhau với

$mn$, vì mỗi phần tử của dòng đó đều có dạng $km + r$, trong đó $1 \le k \le n-1$, $d \mid (km + r)$ vì $d \mid m$, $d \mid r$.

Vậy, để tìm các số trong bảng mà nguyên tố cùng nhau với $mn$, ta chỉ cần xem các dòng thứ $r$ với $(m,r) = 1$. Ta xét một dòng như vậy, nó chứa các số $r, m + r, \ldots, (n-1)m + r$. Vì $(r,m) = 1$ nên mỗi số nguyên trong dòng đều nguyên tố cùng nhau với $n$. Như vậy, $n$ số nguyên trong dòng lập thành hệ thặng dư đầy đủ môđulô $n$. Do đó có đúng $\varphi(n)$ số trong hàng đó nguyên tố cùng nhau với $n$. Do các số đó cũng nguyên tố cùng nhau với $m$ nên chúng nguyên tố cùng nhau với $mn$.

Vì có $\varphi(m)$ dòng, mỗi dòng chứa $\varphi(n)$ số nguyên tố cùng nhau với $mn$, nên ta suy ra $\varphi(mn) = \varphi(m)\varphi(n)$. □

Kết hợp hai định lí trên đây, ta được :

**Định lí 3.10.** *Giả sử* $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ *là phân tích* $n$ *ra thừa số nguyên tố. Khi đó*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

***Chứng minh.*** Vì $\varphi$ là hàm có tính chất nhân nên nếu $n$ có phân tích như trên, ta được :

$$\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2})\cdots\varphi(p_k^{a_k}).$$

Mặt khác,

$$\varphi(p_j^{a_j}) = p_j^{a_j} - p_j^{a_j - 1} = p_j^{a_j}\left(1 - \frac{1}{p_j}\right), \quad j = 1, 2, \ldots, k.$$

Vậy,

$$\begin{aligned}\varphi(n) &= p_1^{a_1}\left(1 - \frac{1}{p_1}\right) p_2^{a_2}\left(1 - \frac{1}{p_2}\right)\cdots p_k^{a_k}\left(1 - \frac{1}{p_k}\right)\\ &= p_1^{a_1} p_2^{a_2}\cdots p_k^{a_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)\\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).\end{aligned}$$ □

Công thức sau đây liên quan đến giá trị của phi-hàm cũng thường được sử dụng trong số học.

**Định lí 3.11.** *Giả sử $n$ là một số nguyên dương. Khi đó :*

$$\sum_{d|n} \varphi(d) = n.$$

***Chứng minh.*** Tổng trên đây được lấy theo các ước số của $n$. Ta phân chia tập hợp các số tự nhiên từ 1 đến $n$ thành các lớp theo cách sau đây. Lớp $C_d$ gồm các số nguyên $m$, $1 \le m \le n$, mà $(m,n) = d$. Như vậy $m$ thuộc $C_d$ nếu và chỉ nếu $d$ là ước chung của $m$, $n$ và $(m/d, n/d) = 1$. Như vậy, số phần tử của $C_d$ là số các số nguyên dương không vượt quá $n/d$ và nguyên tố cùng nhau với $n/d$ ; tức là $C_d$ gồm $\varphi(n/d)$ phần tử. Vì mỗi số nguyên $m$ từ 1 đến $n$ thuộc một và chỉ một lớp $C_d$ nào đó $(d = (m,n))$ nên $n$ bằng tổng của số các thành phần trong các lớp $C_d$, $d$ là ước số của $n$. Ta có :

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right).$$

Mặt khác, khi $d$ chạy qua mọi ước của $n$ thì $n/d$ cũng chạy qua mọi ước của $n$, nên từ đó suy ra

$$n = \sum_{d|n} \varphi(d).$$

Định lí được chứng minh. □

## § 3. TỔNG VÀ SỐ CÁC ƯỚC SỐ

Số các ước số của một số nguyên và tổng các ước số của một số nguyên là các hàm số học quan trọng.

**Định nghĩa 3.12.** Hàm *tổng các ước số*, kí hiệu qua $\sigma$ được xác định bởi : $\sigma(n)$ bằng tổng mọi ước dương của $n$.

***Ví dụ :*** $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.$

**Định nghĩa 3.13.** Hàm *số các ước số*, kí hiệu qua $\tau$, được xác định bởi : $\tau(n)$ bằng số các ước số dương của $n$.

***Ví dụ :*** $\tau(1) = 1$, $\tau(2) = 2$, $\tau(12) = 6$.

Ta có thể biểu diễn hàm $\tau(n)$, $\sigma(n)$ dưới dạng

$$\sigma(n) = \sum_{d|n} d$$

$$\tau(n) = \sum_{d|n} 1$$

Để chứng minh rằng các hàm $\sigma(n)$ và $\tau(n)$ là các hàm có tính chất nhân, ta dùng định lí sau đây.

**Định lí 3.14.** *Giả sử $f$ là một hàm có tính chất nhân. Khi đó hàm*

$$F(n) = \sum_{d|n} f(d)$$

*cũng có tính chất nhân.*

***Chứng minh.*** Ta sẽ chỉ ra rằng, nếu $m$, $n$ là các số nguyên dương nguyên tố cùng nhau, thì $F(mn) = F(m)F(n)$. Giả sử $(m,n) = 1$, ta có :

$$F(mn) = \sum_{d|mn} f(d).$$

Vì $(m,n) = 1$ nên theo Bổ đề 1.31, mỗi ước số của $mn$ có thể viết duy nhất dưới dạng tích các ước $d_1$ của $m$, $d_2$ của $n$ và $d_1$, $d_2$ nguyên tố cùng nhau, đồng thời mỗi cặp ước số $d_1$ của $m$, $d_2$ của $n$ tương ứng với ước $d = d_1d_2$ của $mn$. Do đó ta có thể viết

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1d_2)$$

Vì $f$ là hàm có tính chất nhân và $(d_1, d_2) = 1$ nên

$$F(nm) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2) = \sum_{d_1|m} f(d_1) \cdot \sum_{d_2|n} f(d_2) = F(m).F(n)$$

Từ định lí trên đây suy ra rằng các hàm $\tau(n)$ và $\sigma(n)$ có tính chất nhân. Vì thế ta có thể viết công thức của chúng khi biết phân tích thành thừa số nguyên tố của $n$.

**Bổ đề 3.15.** *Giả sử $p$ là số nguyên tố, $a$ là số nguyên dương. Khi đó*

$$\sigma(p^a) = (1 + p + p^2 + \cdots + p^a) = \frac{p^{a+1}}{p-1},$$

$$\tau(p^a) = a + 1.$$

***Chứng minh.*** Các ước của $p^a$ là $1, p, p^2, \ldots, p^a$. Do đó, $p^a$ có đúng $a+1$ ước dương, $\tau(p^a) = a + 1$. Mặt khác,

$$\sigma(p^a) = 1 + p + p^2 + \cdots + p^{a-1} + p^a = \frac{p^{a+1} - 1}{p - 1}.$$

**Định lí 3.16.** *Giả sử số nguyên dương $n$ có phân tích ra thừa số nguyên tố*

$$n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}.$$

*Khi đó*

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots \frac{p_s^{a_s+1} - 1}{p_s - 1} = \prod_{j=1}^{s} \frac{p_j^{a_j+1} - 1}{p_j - 1},$$

$$\tau(n) = (a_1 + 1)(a_2 + 1)\cdots(a_s + 1) = \prod_{j=1}^{s} (a_j + 1).$$

***Chứng minh.*** Do hai hàm $\sigma$ và $\tau$ đều có tính chất nhân nên ta có

$$\sigma(n) = \sigma(p_1^{a_1})\sigma(p_2^{a_2})\cdots\sigma(p_s^{a_s}),$$

$$\tau(n) = \tau(p_1^{a_1})\tau(p_2^{a_2})\cdots\tau(p_s^{a_s}).$$

Định lí 3.16 suy ra từ Bổ đề 3.15. □

## § 4. SỐ HOÀN HẢO VÀ SỐ MERSENNE

Người Hi Lạp cổ đại thường xem mỗi số tự nhiên biểu hiện một điều bí ẩn nào đó của vũ trụ. Vì thế, họ đặc biệt quan tâm đến những số có tính chất "kì lạ", chẳng hạn như các số bằng tổng các ước dương thực sự của nó. Họ gọi đó là các số hoàn hảo.

**Định nghĩa 3.17.** Số nguyên dương $n$ được gọi là *số hoàn hảo* nếu $2n = \sigma(n)$.

***Ví dụ*** : $12 = 1 + 2 + 3 + 6$ : 6 là số hoàn hảo.

$56 = 1 + 2 + 4 + 7 + 14 + 28$ : 28 là số hoàn hảo.

Ta có định lí sau.

**Định lí 3.18.** *Số nguyên dương chẵn $n$ là số hoàn hảo nếu và chỉ nếu*

$$n = 2^{m-1}(2^m - 1),$$

*trong đó $m$ là số nguyên dương sao cho $2^m - 1$ là số nguyên tố.*

***Chứng minh.*** Trước tiên, giả sử $n = 2^{m-1}(2^m - 1)$, trong đó $2^m - 1$ là số nguyên tố. Vì $2^m - 1$ là số lẻ nên ta có

$$(2^{m-1}, 2^m - 1) = 1.$$

Do $\sigma$ là hàm có tính chất nhân nên

$$\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1).$$

Từ Bổ đề 3.15 ta được $\sigma(2^{m-1}) = 2^m - 1$, $\sigma(2^m - 1) = 2^m$, vì $2^m - 1$ là số nguyên tố. Vậy

$$\sigma(n) = (2^{m-1})2^m = 2n,$$

và $n$ là số hoàn hảo.

Ngược lại, giả sử $n$ là số hoàn hảo chẵn. Ta viết $n = 2^s t$, trong đó $s$, $t$ là các số nguyên dương và $t$ lẻ. Vì $(2^s, t) = 1$, từ Bổ đề 3.15 ta được :

$$\sigma(n) = \sigma(2^s, t) = \sigma(2^s)\sigma(t) = (2^{s+1} - 1)\sigma(t).$$

Do $n$ là số hoàn hảo nên

$$\sigma(n) = 2n = 2^{s+1}t.$$

Từ đó ta có

$$(2^{s+1} - 1)\sigma(t) = 2^{s+1}t.$$

Do $(2^{s+1}, 2^{s+1} - 1) = 1$ nên từ đẳng thức trên suy ra

$$2^{s+1} \mid \sigma(t).$$

Vậy tồn tại số nguyên $q$ sao cho $\sigma(t) = 2^{s+1}q$. Do đó

$$(2^{s+1} - 1)2^{s+1}q = 2^{s+1}t,$$

tức là

$$(2^{s+1} - 1)q = t.$$

Vậy $q \mid t$ và $q \neq t$. Từ đó ta có :

$$t + q = (2^{s+1} - 1)q + q = 2^{s+1}q = \sigma(t).$$

Ta sẽ chỉ ra rằng $q = 1$. Nếu $q \neq 1$ thì tồn tại ít nhất ba ước nguyên tố khác nhau của $t$, cụ thể là $1$, $q$ và $t$. Khi đó $\sigma(t) \geq t + q + 1$, mâu thuẫn. Vậy $q = 1$, và $t = 2^{s+1} - 1$. Từ đó suy ra $\sigma(t) = t + 1$, nên $t$ là số nguyên tố, vì $t$ không có ước dương nào khác ngoài $1$ và $t$. Vậy $n = 2^s(2^{s+1} - 1)$,

trong đó $2^{s+1} - 1$ là số nguyên tố. □

Từ Định lí 3.18 ta thấy rằng, để tìm các số hoàn hảo chẵn, ta chỉ cần tìm các số nguyên tố dạng $2^m - 1$. Trước tiên ta có nhận xét rằng, nếu số có dạng như trên là nguyên tố thì số mũ $m$ phải là số nguyên tố.

**Định lí 3.19.** *Nếu $2^m - 1$ là số nguyên tố thì $m$ là số nguyên tố.*

***Chứng minh.*** Giả sử ngược lại, $m = ab$, trong đó $1 < a < m$, $1 < b < m$. Khi đó

$$2^m - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1).$$

Vì mỗi nhân tử ở vế phải đều lớn hơn 1, nên $2^m - 1$ là hợp số. Định lí được chứng minh. □

**Định nghĩa 3.20.** Nếu $n$ là số nguyên dương thì

$$M_n = 2^n - 1$$

được gọi là *số Mersenne thứ $n$*. Hơn nữa, nếu $p$ là số nguyên tố và $M_p = 2^p - 1$ cũng là số nguyên tố thì $M_p$ được gọi là *số nguyên tố Mersenne*.

***Ví dụ :*** $M_7 = 2^7 - 1$ là một số nguyên tố Mersenne, trong khi $M_{11} = 2^{11} - 1 = 2047 = 23.89$ là một hợp số.

Các số Mersenne có vai trò quan trọng trong việc tìm những số nguyên tố lớn (vấn đề có nhiều ứng dụng trong lí thuyết thông tin, mật mã). Vì thế, người ta đã nghiên cứu rất nhiều thuật toán để xác định xem một số Mersenne có phải là số nguyên tố hay không. Định lí sau đây liên quan đến vấn đề đó.

**Định lí 3.21.** *Giả sử $p$ là một số nguyên tố lẻ. Khi đó mọi ước của số Mersenne $M_p = 2^p - 1$ đều có dạng $2kp + 1$, trong đó $k$ là số nguyên dương.*

***Chứng minh.*** Giả sử $q$ là một ước nguyên tố của $M_p = 2^p - 1$. Từ Định lí Phecma bé ta có : $q \mid (2^{q-1} - 1)$. Theo Bổ đề 2.18

$$(2^p - 1, 2^{q-1} - 1) = 2^{(p, q-1)} - 1.$$

Vì $q$ là ước chung của $2^p - 1$ và $2^{q-1} - 1$ nên

$$(2^p - 1, 2^{q-1} - 1) > 1.$$

Vậy, $(p, q-1) = p$, vì nếu ngược lại, $(p, q-1) = 1$ thì $(2^p - 1, 2^{q-1} - 1) = 1$. Do đó $p \mid (q-1)$, tức là tồn tại số nguyên dương $m$ để $(q-1) = mp$. Vì $q$ lẻ nên $m$ chẵn, giả sử $m = 2k$. Vậy $q = mp + 1 = 2kp + 1$. □

Nhờ Định lí 3.21, để kiểm tra một số Mersenne $M$ có phải là số nguyên tố hay không, ta không cần chia nó cho mọi số nguyên tố bé hơn $\sqrt{M}$, mà chỉ cần chia cho các số nguyên tố có dạng đã nói trong định lí và nhỏ hơn $\sqrt{M}$.

***Ví dụ :*** 1) $M_{13} = 2^{13} - 1 = 8191$. Để xem $8191$ có phải là số nguyên tố hay không, ta chỉ cần xem $8191$ có ước nguyên tố nào dạng $26k + 1$ và bé hơn $\sqrt{8191} = 90,50\ldots$ hay không. Như vậy, chỉ cần làm phép chia $8191$ cho $53$ và $79$, ta rút ra kết luận $8191$ là số nguyên tố Mersenne.

2) Xét $M_{23} = 2^{23} - 1 = 8388607$. $\sqrt{M} = 2896,309\ldots$ Số nguyên tố bé nhất có dạng $46k + 1$ là $47$. Làm phép chia $8388607$ cho $47$, ta được : $8388607 = 47.178481$ : số Mersenne $M_{23}$ không phải là số nguyên tố.

Cho đến nay, số nguyên tố Mersenne lớn nhất được tìm thấy là số $M_{13466917}$, gồm $4053946$ chữ số !

Để tìm hiểu thêm về lịch sử các số Mersenne, tiểu sử Mersenne và số Mersenne lớn nhất được tìm thấy, bạn đọc có thể truy cập vào Internet theo địa chỉ : http://www.utm.edu/research/primes.

Mặc dù các số hoàn hảo và số Mersenne đã được nghiên cứu hàng trăm năm nay, vẫn tồn tại nhiều giả thuyết chưa được chứng minh.

**Giả thuyết 1.** *Không tồn tại số tự nhiên lẻ nào là số hoàn hảo.*

**Giả thuyết 2.** *Tồn tại vô hạn số nguyên tố Mersenne.*

## § 5. BẬC CỦA MỘT SỐ NGUYÊN. CĂN NGUYÊN THỦY

Từ Định lí Ơ-le ta có, nếu $m$ là số nguyên dương và nếu $a$ là số nguyên, nguyên tố cùng nhau với $m$ thì $a^{\varphi(m)} \equiv 1 \pmod{m}$. Do đó, phương trình đồng dư

$$a^x \equiv 1 \pmod{m}$$

luôn luôn có nghiệm. Theo tính chất thứ tự tốt của tập hợp các số nguyên dương, phải tồn tại số nguyên dương $x$ bé nhất thỏa mãn đồng dư nói trên.

**Định nghĩa.3.22.** Giả sử $a$ và $m$ là các số nguyên dương nguyên tố cùng nhau. Khi đó, số nguyên dương $x$ nhỏ nhất sao cho $a^x \equiv 1 \pmod{m}$ được gọi là *bậc của $a$ môđulô $m$*.

Ta kí hiệu bậc của $a$ môđulô $m$ bởi $\mathrm{ord}_m a$.

***Ví dụ :*** Ta tìm bậc của 2 môđulô 5 :

$$2^1 \equiv 2 \pmod{5};\ 2^2 \equiv 4 \pmod{5};\ 2^3 \equiv 3 \pmod{5};\ 2^4 \equiv 1 \pmod{5}.$$

Vậy bậc của 2 môđulô 5 là 4 : $\mathrm{ord}_5 2 = 4$.

Tìm bậc của 4 môđulô 5 :

$$4^1 \equiv 4 \pmod{5};\ 4^2 \equiv 1 \pmod{5} : \text{bậc } \mathrm{ord}_5 4 = 2.$$

Để có thể tìm được tất cả các nghiệm của đồng dư thức $a^x \equiv 1 \pmod{m}$, ta cần đến định lí sau :

**Định lí 3.23.** *Nếu $a$ và $n$ là các số nguyên nguyên tố cùng nhau, $n > 0$, thì số nguyên $x$ là nghiệm của $a^x \equiv 1 \pmod{n}$ nếu và chỉ nếu $x \vdots \mathrm{ord}_n a$.*

***Chứng minh.*** Nếu $\mathrm{ord}_n a \mid x$ thì $x = k.\mathrm{ord}_n a$, với $k$ là số nguyên dương. Do đó

$$a^x = a^{k.\mathrm{ord}_n a} = \left(a^{\mathrm{ord}_n a}\right)^k \equiv 1 \pmod{n}.$$

Ngược lại, giả sử $a^x \equiv 1 \pmod{n}$. Khi đó $x \geq \mathrm{ord}_n a$. Dùng thuật toán chia, ta viết

$$x = q.\mathrm{ord}_n a + r, \quad 0 \leq r < \mathrm{ord}_n a.$$

Từ phương trình này, ta thấy

$$a^x = a^{q.\mathrm{ord}_n a + r} = \left(a^{\mathrm{ord}_n a}\right)^q . a^r \equiv a^r \pmod{n} \equiv 1 \pmod{n}.$$

Do $0 \leq r < \mathrm{ord}_n a$ và $\mathrm{ord}_n a$ là số nguyên dương bé nhất thỏa mãn phương trình đồng dư đang xét, ta có $r = 0$. Vậy $x = q.\mathrm{ord}_n a$, tức là $x \vdots \mathrm{ord}_n a$. □

**Hệ quả.3.24.** *Nếu $a$ và $n$ là các số nguyên nguyên tố cùng nhau, $n > 0$, thì $\mathrm{ord}_n a \mid \varphi(n)$.*

***Chứng minh.*** Do $(a, n) = 1$, Định lí Ơ-le cho ta

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Vậy hệ quả suy ra ngay từ định lí vừa chứng minh. □

***Ví dụ :*** Tìm bậc của $5 \pmod{11}$ và $7 \pmod{11}$.

- $5^1 \equiv 5 \pmod{11}$; $5^2 \equiv 3 \pmod{11}$; $5^3 \equiv 4 \pmod{11}$;
  $5^4 \equiv 9 \pmod{11}$; $5^5 \equiv 1 \pmod{11}$.

Vậy : $\mathrm{ord}_{11}5 = 5$.

- $7^1 \equiv 7 \pmod{11}$; $7^2 \equiv 5 \pmod{11}$; $7^3 \equiv 2 \pmod{11}$;
  $7^4 \equiv 3 \pmod{11}$; $7^5 \equiv 10 \pmod{11}$; $7^6 \equiv 4 \pmod{11}$;
  $7^7 \equiv 6 \pmod{11}$; $7^8 \equiv 9 \pmod{11}$; $7^9 \equiv 8 \pmod{11}$;
  $7^{10} \equiv 1 \pmod{11}$.

Vậy : $\mathrm{ord}_{11}5 = 5$.

Mặt khác, $\varphi(11) = 10$. Vậy $\mathrm{ord}_{11}7$, $\mathrm{ord}_{11}5$ đều là ước của $\varphi(11)$, đặc biệt $\mathrm{ord}_{11}7 = \varphi(11)$.

Định lí sau đây sẽ được dùng về sau.

**Định lí 3.25.** *Nếu $a$ và $n$ là các số nguyên nguyên tố cùng nhau và $n > 0$ thì đồng dư thức*

$$a^i \equiv a^j \pmod{n}$$

*nghiệm đúng nếu và chỉ nếu $i \equiv j \pmod{\mathrm{ord}_n a}$.*

***Chứng minh.*** Giả sử $i \equiv j \pmod{\mathrm{ord}_n a}$, và $0 \le j \le i$. Khi đó ta có

$$i = j + k\ \mathrm{ord}_n a,$$

trong đó $k$ là một số nguyên dương. Do đó

$$a^i = a^{j + k\,\mathrm{ord}_n a} = a^j.(a^{\mathrm{ord}_n a})^k \equiv a^j \pmod{n},$$

vì $a^{\mathrm{ord}_n a} \equiv 1 \pmod{n}$.

Ngược lại, giả sử rằng $a^i \equiv a^j \pmod{n}$ với $i \ge j$. Vì $(a, n) = 1$ nên $(a^j, n) = 1$. Do đó, từ đồng dư thức

$$a^i \equiv a^j a^{i-j} \equiv a^j \pmod{n}$$

suy ra rằng

$$a^{i-j} \equiv 1 \pmod{n}.$$

Từ Định lí 3.25 suy ra $\mathrm{ord}_n a$ chia hết $(i-j)$, tức là $i \equiv j \pmod{\mathrm{ord}_n a}$. Chứng minh xong. □

Cho trước số nguyên $n$, ta quan tâm đến các số $a$ sao cho bậc môđulô $n$ của nó đúng bằng $\varphi(n)$, tức là có bậc lớn nhất có thể.

**Định nghĩa 3.26.** Nếu $r$ và $n$ là các số nguyên nguyên tố cùng nhau, $n > 0$, đồng thời $\mathrm{ord}_n r = \varphi(n)$, thì $r$ được gọi là *căn nguyên thủy* môđulô $n$.

***Ví dụ :*** Ta đã thấy ở Ví dụ trước : $\mathrm{ord}_5 2 = 4 = \varphi(5)$. Vậy 2 là căn nguyên thủy môđulô 5. Tương tự như vậy, $\mathrm{ord}_{11} 7 = 10 = \varphi(11)$ : 7 là căn nguyên thủy môđulô 11.

Không phải số nguyên nào cũng có căn nguyên thủy. Chẳng hạn, không có số nào là căn nguyên thủy môđulô 8. Thật vậy, tất cả các số nguyên nhỏ hơn 8, nguyên tố cùng nhau với 8 là 1, 3, 5, 7. Ta có $\mathrm{ord}_8 1 = 1$, $\mathrm{ord}_8 3 = \mathrm{ord}_8 5 = \mathrm{ord}_8 7 = 2$. Trong khi đó, $\varphi(8) = 4$.

Bây giờ ta sẽ xét vấn đề khi nào thì một số nguyên có căn nguyên thủy. Trước hết, ta chứng minh định lí sau.

**Định lí 3.27.** *Giả sử $r$, $n$ là các số nguyên dương nguyên tố cùng nhau, $n > 0$ và $r$ là căn nguyên thủy môđulô $n$. Khi đó các số*

$$r^1, r^2, \ldots, r^{\varphi(n)}$$

*lập thành một hệ thặng dư thu gọn môđulô $n$.*

***Chứng minh.*** Ta cần chứng tỏ rằng các số nói trên nguyên tố cùng nhau với $n$, và không có hai số nào đồng dư môđulô $n$.

Do $(r, n) = 1$ nên $(r^k, n) = 1$ với mọi số nguyên dương $k$. Vậy mọi lũy thừa trên đây nguyên tố cùng nhau với $n$.

Giả sử trong dãy nói trên có hai số đồng dư môđulô $n$ :

$$r^i \equiv r^j \pmod{n}.$$

Từ Định lí 3.25 suy ra $i \equiv j \pmod{\varphi(n)}$, do $r$ là căn nguyên thủy. Vì $1 \le i \le \varphi(n)$, $1 \le j \le \varphi(n)$ nên ta có $i = j$. Vậy trong dãy trên đây không có hai số nào đồng dư nhau môđulô $n$. Định lí được chứng minh. □

*Ví dụ :* Ta có $2^1 \equiv 2 \pmod 9$, $2^2 \equiv 4 \pmod 9$, $2^3 \equiv 8 \pmod 9$, $2^4 \equiv 7 \pmod 9$, $2^5 \equiv 5 \pmod 9$, $2^6 \equiv 1 \pmod 9$. Mặt khác, $\varphi(9) = 6$, nên 2 là căn nguyên thủy môđulô 9, đồng thời 2, 4, 8, 7, 5, 1 là một hệ thặng dư thu gọn môđulô 9.

Nếu một số nguyên nào đó có căn nguyên thủy, thì nó có nhiều căn nguyên thủy khác nhau. Trước tiên ta có định lí sau.

**Định lí 3.28.** *Giả sử* $\operatorname{ord}_m a = t$ *và* $u$ *là một số nguyên dương. Khi đó*

$$\operatorname{ord}_m(a^u) = \frac{t}{(t,u)}.$$

***Chứng minh.*** Đặt $s = \operatorname{ord}_m(a^u)$, $v = (t,u)$, $t = t_1 v$, $u = u_1 v$, với $(t_1, u_1) = 1$. Ta có

$$(a^u)^{t_1} = (a^{u_1 v})^{t_1} = (a^{u_1 v})^{t/v} = (a^t)^{u_1} \equiv 1 \pmod m,$$

vì $\operatorname{ord}_m a = t$. Vậy, $t_1$ chia hết $s$ : $s \mid t_1$.

Mặt khác, do

$$(a^u)^s = a^{us} \equiv 1 \pmod m,$$

nên $t \mid us$. Vậy ta có : $vt_1 \mid (u, vs)$, suy ra $t_1 \mid u_1 s$. Nhưng vì $(t_1, u_1) = 1$ nên ta có $t_1 \mid s$.

Vậy $s \mid t_1$, $t_1 \mid s$ nên suy ra $s = t_1 = \dfrac{t}{v} = \dfrac{t}{(t,u)}$. Định lí được chứng minh. □

**Hệ quả 3.29.** *Giả sử* $r$ *là căn nguyên thủy môđulô* $m$, *trong đó* $m$ *là số nguyên,* $m > 1$. *Khi đó* $r^u$ *là căn nguyên thủy môđulô* $m$ *nếu và chỉ nếu* $(u, \varphi(m)) = 1$.

**Chứng minh.** Từ định lí trên đây ta có

$$\operatorname{ord}_m r^u = \frac{\operatorname{ord}_m r}{(u, \operatorname{ord}_m r)} = \frac{\varphi(m)}{(u, \varphi(m))}.$$

Do đó, $\operatorname{ord}_m r^u = \varphi(m)$, và $r^u$ là căn nguyên thủy môđulô $m$ nếu và chỉ nếu $(u, \varphi(m)) = 1$. □

Từ hệ quả trên ta suy ra ngay định lí sau đây.

**Định lí 3.30.** *Nếu số nguyên dương $m$ có căn nguyên thủy, thì nó có cả thảy $\varphi(\varphi(m))$ căn nguyên thủy.*

***Chứng minh.*** Giả sử $r$ là một căn nguyên thủy môđulô $m$. Khi đó các số $r, r^2, \ldots, r^{\varphi(m)}$ lập thành một hệ thặng dư thu gọn môđulô $m$. Theo hệ quả trên đây $r^u$ là căn nguyên thủy môđulô $m$ nếu và chỉ nếu $(u, \varphi(m)) = 1$. Vì tồn tại đúng $\varphi(\varphi(m))$ số nguyên $u$ như thế, nên có đúng $\varphi(\varphi(m))$ căn nguyên thủy môđulô $m$. □

***Ví dụ :*** Ta đã biết 7 là căn nguyên thủy môđulô 11. Mặt khác, $\varphi(\varphi(11)) = \varphi(10) = 4$ nên có đúng bốn số là căn nguyên thủy môđulô 11, đó là $7^1$, $7^3$, $7^7$, $7^9$ môđulô 11, tức là các số 2, 6, 7, 8.

## § 6. SỰ TỒN TẠI CỦA CĂN NGUYÊN THUỶ

### 6.1. CĂN NGUYÊN THỦY CỦA CÁC SỐ NGUYÊN TỐ

Mục tiêu của phần này là chứng tỏ rằng, mọi số nguyên tố đều có căn nguyên thủy. Trước tiên, ta cần đến một số kết quả về đồng dư đa thức.

Giả sử $f(x)$ là một đa thức hệ số nguyên. Ta nói rằng số nguyên $c$ là nghiệm của $f(x)$ môđulô $m$ nếu $f(c) \equiv 0 \pmod{m}$. Dễ thấy rằng, nếu $c$ là nghiệm của $f(x)$ môđulô $m$ thì mỗi số nguyên đồng dư với $c$ môđulô $m$ cũng là nghiệm môđulô $m$.

***Ví dụ :*** 1) Đa thức $f(x) = x^2 + x - 1$ có đúng hai nghiệm môđulô 7 không đồng dư nhau, cụ thể là $x \equiv 2 \pmod{7}$ và $x \equiv 4 \pmod{7}$.

2) Đa thức $g(x) = x^2 + 2$ không có nghiệm môđulô 5.

3) Từ Định lí Phecma bé suy ra rằng, đa thức $h(x) = x^{p-1} - 1$ có đúng $(p-1)$ nghiệm môđulô $p$ không đồng dư nhau, đó là $x \equiv 1, 2, 3, \ldots, (p-1) \pmod{p}$.

Định lí sau đây là một kết quả quan trọng về nghiệm của đa thức môđulô $p$, khi $p$ là số nguyên tố.

**Định lí Lagrange.** *Giả sử*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

*là đa thức bậc $n$ với hệ số nguyên, hệ số cao nhất $a_n$ không chia hết cho $p$.*

*Khi đó $f(x)$ có nhiều nhất là $n$ môđulô $p$ không đồng dư nhau.*

***Chứng minh.*** Ta dùng phương pháp quy nạp toán học. Khi $n = 1$, $f(x)$ là đa thức bậc nhất $f(x) = a_1x + a_0$, trong đó $p \nmid a_1$. Một nghiệm môđulô $p$ của $f(x)$ là một nghiệm của đồng dư tuyến tính $a_1x \equiv -a_0 \pmod{p}$. Do $(a_1, p) = 1$ nên phương trình đồng dư này có đúng một nghiệm $x \equiv a_1^{-1}.(-a_0) \pmod{p}$. Như vậy, chỉ có đúng một nghiệm môđulô $p$ của $f(x)$ : định lí đúng khi $n = 1$.

Bây giờ giả sử định lí đã được chứng minh với các đa thức bậc $n-1$, và giả sử $f(x)$ là đa thức bậc $n$, hệ số cao nhất $a_n$ không chia hết cho $p$. Giả sử đa thức $f(x)$ có $(n+1)$ nghiệm môđulô $p$ không đồng dư nhau, kí hiệu là $c_0, c_1, \ldots, c_n$. Ta có :

$$f(c_k) \equiv 0 \pmod{p},\ k = 0,1,\ldots,n,$$

$$\begin{aligned} f(x) - f(c_0) &= a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \cdots + a_1(x - c_0) \\ &= a_n(x - c_0)(x^{n-1} + x^{n-2}c_0 + \cdots + c_0^{n-1}) + \\ &\quad + a_{n-1}(x - c_0)(x^{n-2} + x^{n-3}c_0 + \cdots + c_0^{n-2}) + \\ &\quad + \cdots + a_1(x - c_0) \\ &= (x - c_0)g(x), \end{aligned}$$

trong đó $g(x)$ là đa thức bậc $(n-1)$, hệ số cao nhất là $a_n$. Bây giờ ta chỉ ra rằng $c_1, c_2, \ldots, c_n$ là các nghiệm môđulô $p$ của $g(x)$. Giả sử $k$ là số nguyên, $1 \le k \le n$. Do $f(c_k) \equiv f(c_0) \equiv 0 \pmod{p}$ nên

$$f(c_k) - f(c_0) = (c_k - c_0)g(c_k) \equiv 0 \pmod{p}.$$

Vì $p$ nguyên tố, mà $c_k \not\equiv c_0 \pmod{p}$ nên suy ra $g(c_k) \equiv 0 \pmod{p}$. Vậy $c_k$, $(k = 1,\ldots,n)$, là các nghiệm môđulô $p$ của $g(x)$. Nhưng $g(x)$ có bậc $(n-1)$ nên theo giả thiết quy nạp, nó có không quá $(n-1)$ nghiệm môđulô $p$ không đồng dư nhau. Mâu thuẫn này kết thúc chứng minh định lí. □

Định lí Lagrange cho phép chứng minh kết quả sau đây.

**Định lí 3.31.** *Giả sử $p$ là số nguyên tố, $d$ là một ước của $p-1$. Khi đó đa thức $x^d - 1$ có đúng $d$ nghiệm môđulô $p$ không đồng dư nhau.*

***Chứng minh.*** Giả sử $p - 1 = de$. Khi đó

$$x^{p-1} - 1 = (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^e + 1) = (x^d - 1)g(x).$$

Từ Định lí Phecma bé ta thấy rằng $x^{p-1} - 1$ có $(p-1)$ nghiệm môđulô $p$ không đồng dư nhau. Do $p$ nguyên tố nên các nghiệm này phải là nghiệm của $x^d - 1$ hoặc của $g(x)$ môđulô $p$. Theo Định lí Lagrange, $g(x)$ có nhiều nhất là $d(e-1)$ nghiệm môđulô $p$. Vì mỗi nghiệm của $x^{p-1} - 1$ môđulô $p$ mà không là nghiệm môđulô $p$ của $g(x)$ phải là một nghiệm môđulô $p$ của $x^d - 1$, nên $x^d - 1$ phải có ít nhất là $(p-1) - d(e-1)$ nghiệm. Ta có $(p-1) - d(e-1) = d$. Mặt khác, theo Định lí Lagrange, $x^d - 1$ có không quá $d$ nghiệm môđulô $p$, từ đó suy ra $x^d - 1$ có đúng $d$ nghiệm môđulô $p$ không đồng dư nhau. □

Định lí trên đây cho phép trả lời câu hỏi : có bao nhiêu số nguyên không đồng dư nhau có cùng bậc môđulô $p$ cho trước.

**Định lí 3.32.** *Giả sử $p$ là số nguyên tố và $d$ là ước dương của $p-1$. Khi đó số các số nguyên bậc $d$ môđulô $p$ không đồng dư nhau là $\varphi(d)$.*

***Chứng minh.*** Với mỗi số nguyên dương $d$ là ước của $p-1$, ta đặt $F(d)$ là số các số nguyên dương bậc $d$ môđulô $p$ và bé hơn $p$. Do bậc môđulô $p$ của một số nguyên không chia hết cho $p$ là ước của $\varphi(p) = p-1$, nên ta có

$$p - 1 = \sum_{d|(p-1)} F(d).$$

Mặt khác, theo tính chất của phi-hàm Ơ-le ta có :

$$p - 1 = \sum_{d|(p-1)} \varphi(d).$$

Ta sẽ chứng tỏ rằng, với mọi $d \mid (p-1)$, ta có $F(d) \le \varphi(d)$. Điều đó sẽ suy ra $F(d) = \varphi(d)$ với mọi $d \mid (p-1)$, vì ta đã có

$$\sum_{d|(p-1)} F(d) = \sum_{d|(p-1)} \varphi(d).$$

Giả sử $d$ là một ước của $p-1$. Nếu $F(d) = 0$ thì bất đẳng thức $F(d) \le \varphi(d)$ là hiển nhiên. Giả sử $F(d) \neq 0$, tức là tồn tại số nguyên $a$ bậc $d$ môđulô $p$. Do $\mathrm{ord}_p a = d$ nên các số $a$, $a^2$, ... , $a^d$ không đồng dư nhau môđulô $p$. (Nếu ngược lại, $a^i \equiv a^j \pmod p$ thì $i - j \vdots \mathrm{ord}_p a = d$). Mặt khác, với mỗi $k$ nguyên dương,

$$(a^k)^d \equiv (a^d)^k \equiv 1 \pmod{p}.$$

Như vậy, $a^k$ là nghiệm môđulô $p$ của đa thức $x^d - 1$. Đa thức này có đúng $d$ nghiệm không đồng dư nhau, nên mỗi nghiệm phải đồng dư với một số $a^k$ nào đó $(1 \le k \le d)$. Tuy nhiên, $a^k$ có bậc $d$ chỉ khi $(k,d) = 1$, mà có đúng $\varphi(d)$ số $k$ như vậy với $1 \le k \le d$. Vậy, nếu tồn tại phần tử bậc $d$ môđulô $p$, thì phải có đúng $\varphi(d)$ số $k$ như vậy nhỏ hơn $d$. Do đó $F(d) \le \varphi(d)$, định lí được chứng minh. □

**Hệ quả 3.33.** *Mọi số nguyên tố đều có căn nguyên thủy.*

***Chứng minh.*** Giả sử $p$ là số nguyên tố. Theo định lí trên đây, có $\varphi(p-1)$ số nguyên bậc $p-1$ môđulô $p$ không đồng dư nhau. Theo định nghĩa, mỗi số đó là một căn nguyên thủy môđulô $p$, và như vậy, $p$ có $\varphi(p-1)$ căn nguyên thủy. □

## 6.2. SỰ TỒN TẠI CĂN NGUYÊN THỦY

Chúng ta đã biết rằng mọi số nguyên tố đều có căn nguyên thủy. Trong tiết này, ta sẽ tìm mọi số nguyên dương có căn nguyên thủy.

**Định lí 3.34.** *Giả sử $p$ là một số nguyên tố lẻ, có căn nguyên thủy $r$. Khi đó, hoặc $r$, hoặc $r+p$ là căn nguyên thủy môđulô $p^2$.*

***Chứng minh.*** Vì $r$ là căn nguyên thủy môđulô $p$ nên ta có

$$\operatorname{ord}_p r = \varphi(p) = p - 1.$$

Giả sử $n = \operatorname{ord}_{p^2} r$. Do $r^n \equiv 1 \pmod{p^2}$, nên

$$r^n \equiv 1 \pmod{p}.$$

Như vậy, $\operatorname{ord}_p r \mid n$. Mặt khác, do $n$ là cấp của $r$ môđulô $p^2$ nên $n \mid \varphi(p^2)$. Vậy $n \mid p(p-1)$, đồng thời $(p-1) \mid n$. Từ đó suy ra, hoặc $n = p-1$, hoặc $n = p(p-1)$. Nếu $n = p(p-1)$ thì $r$ là căn nguyên thủy môđulô $p^2$, vì $\operatorname{ord}_{p^2} r = \varphi(p^2)$. Nếu $n = p-1$ thì $r^{p-1} \equiv 1 \pmod{p^2}$. Đặt $s = r + p$. Khi đó, vì $s \equiv r \pmod{p}$ nên $s$ cũng là căn nguyên thủy môđulô $p$. Vậy $\operatorname{ord}_{p^2} s$ hoặc là $(p-1)$ hoặc là $p(p-1)$ (theo chứng minh trên). Ta sẽ chỉ ra rằng, $\operatorname{ord}_{p^2} s \ne p-1$. Ta có

$$s^{p-1} = (r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2}p + C_{p-1}^2 r^{p-3}p^2 + \cdots + p^{p-1}$$

$$\equiv r^{p-1} + (p-1)p.r^{p-2} \pmod{p^2}.$$

Do đó :

$$s^{p-1} \equiv 1 + (p-1)p.r^{p-2} \equiv 1 - pr^{p-2} \pmod{p^2}.$$

Vậy

$$s \not\equiv 1 \pmod{p^2},$$

vì nếu ngược lại thì $pr^{p-2} \equiv 0 \pmod{p^2}$, suy ra $r^{p-2} \equiv 0 \pmod{p}$ : vô lí vì $p \nmid r$ (ta nhớ rằng $r$ là căn nguyên thủy môđulô $p$). Như vậy, $\text{ord}_{p^2} s = p(p-1) = \varphi(p^2)$, tức là $s = r + p$ là căn nguyên thủy môđulô $p^2$.

***Ví dụ :*** Ta có 3 là căn nguyên thủy môđulô 7. Mặt khác, $7^2 = 49$, và $3^6 \not\equiv 1 \pmod{49}$, nên theo chứng minh định lí trên, $\text{ord}_{49} 3 = 7(7-1)$, và 3 là căn nguyên thủy môđulô 49.

**Nhận xét.** Rất ít khi ta có $r^{p-1} \equiv 1 \pmod{p^2}$ đối với căn nguyên thủy $r$ môđulô $p$. Vì thế, phần lớn căn nguyên thủy môđulô $p$ cũng đồng thời là căn nguyên thủy môđulô $p^2$. Số $p$ nhỏ nhất để có căn nguyên thủy của $p$ mà không là căn nguyên thủy của $p^2$ là $p = 487$ : trong trường hợp này, 10 là căn nguyên thủy môđulô 487, nhưng $10^{486} \equiv 1 \pmod{487^2}$. Vậy, 10 không phải là căn nguyên thủy môđulô $487^2$. Từ định lí trên đây, ta thấy $10 + 487 = 497$ là căn nguyên thủy môđulô $487^2$.

Bây giờ ta xét trường hợp lũy thừa tùy ý của một số nguyên tố

**Định lí 3.35.** *Giả sử $p$ là một số nguyên tố lẻ. Khi đó $p^k$ có căn nguyên thủy với mọi số nguyên dương $k$. Hơn nữa, nếu $r$ là một căn nguyên thủy môđulô $p^2$, thì $r$ là căn nguyên thủy môđulô $p^k$ với mọi số nguyên dương $k$.*

***Chứng minh.*** Ta đã biết nếu $r$ là căn nguyên thủy môđulô $p$ thì hoặc $r$, hoặc $r + p$ là căn nguyên thủy môđulô $p^2$. Vậy, với mỗi số nguyên tố $p$, tồn tại căn nguyên thủy $r$ môđulô $p$ sao cho nó cũng là căn nguyên thủy môđulô $p^2$, tức là

$$r^{p-1} \not\equiv 1 \pmod{p^2}. \tag{1}$$

Khi đó, ta sẽ chứng minh rằng, với $r$ nói trên ta có

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}. \tag{2}$$

Nếu (2) đã được chứng minh, thì ta sẽ chứng tỏ được rằng, $r$ là căn nguyên thủy môđulô $k$ với mọi $k \geq 1$. Thật vậy, giả sử

$$n = \text{ord}_{p^k} r.$$

Khi đó

$$n \mid \varphi(p^k) = p^{k-1}(p-1).$$

Mặt khác, do

$$r^n \equiv 1 \pmod{p^k}$$

nên

$$r^n \equiv 1 \pmod{p}.$$

Vậy $\varphi(p) \mid n$ tức là $(p-1) \mid n$. Hơn nữa, $n \mid p^{k-1}(p-1)$ nên $n = p^t(p-1)$ với $t$ nào đó, $0 \leq t \leq k-1$. Nếu $t \leq k-2$ thì

$$r^{p^{k-2}(p-1)} = (r^{p^t(p-1)})^{p^{k-2-t}} \equiv 1 \pmod{p^k},$$

mâu thuẫn với (2). Vậy,

$$\text{ord}_{p^k} r = p^{k-1}(p-1) = \varphi(p^k),$$

tức $r$ là căn nguyên thủy môđulô $p^k$.

Như vậy, để chứng minh định lí, chỉ cần phải chứng minh (2). Ta dùng quy nạp toán học. Trường hợp $k = 2$ chính là (1). Giả sử (2) đúng với số $k$ nào đó $\geq 2$. Ta có

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Vì $(r, p) = 1$ nên $(r, p^{k-1}) = 1$. Do đó, theo Định lí Ơ-le,

$$r^{\varphi(p^{k-1})} = r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}.$$

Vậy, tồn tại số nguyên $d$ sao cho

$$r^{p^{k-2}(p-1)} = 1 + dp^{k-1},$$

trong đó $p \nmid d$ do giả thiết quy nạp. Nâng lên lũy thừa bậc $p$ hai vế của đẳng thức trên, ta có :

$$\begin{aligned} r^{p^{k-1}(p-1)} &= (1 + dp^{k-1})^p \\ &= 1 + p(dp^{k-1}) + (C_p^2(dp^{k-1})^2 + \cdots + (dp^{k-1})^p \end{aligned}$$

$$\equiv 1 + dp^k \pmod{p^{k+1}}.$$

Do $p \nmid d$ nên suy ra

$$r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}},$$

kết thúc chứng minh quy nạp, và do đó, kết thúc chứng minh định lí. □

***Ví dụ :*** $r = 3$ là căn nguyên thủy môđulô $7$ và $7^2$. Theo định lí trên đây $r = 3$ là căn nguyên thủy môđulô $7^k$ với mọi số nguyên dương $k$.

Trên đây ta đã xét lũy thừa của các số nguyên tố lẻ, bây giờ ta xét các lũy thừa của $2$. Ta thấy rằng, $2$ có căn nguyên thủy là $1$, $2^2 = 4$ có căn nguyên thủy là $3$. Ta sẽ chứng minh rằng, các lũy thừa bậc cao hơn của $2$ không có căn nguyên thủy.

**Định lí 3.36.** *Nếu $a$ là một số nguyên lẻ, $k$ nguyên, $k > 3$ thì*

$$a^{\varphi(2^k)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

***Chứng minh.*** Ta dùng quy nạp toán học. Giả sử $a$ là số nguyên lẻ, $a = 2b + 1$, trong đó $b$ là số nguyên. Do đó

$$a^2 = (2b+1)^2 = 4b^2 + 4b + 1 = 4b(b+1) + 1.$$

Hoặc $b$ hoặc $(b+1)$ chẵn nên

$$a^2 \equiv 1 \pmod{8}.$$

Vậy đồng dư cần chứng minh đúng với $k = 3$. Giả sử rằng

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

Khi đó tồn tại $d$ sao cho

$$a^{2^{k-2}} = 1 + d.2^k.$$

Bình phương hai vế ta được

$$a^{2^{k-1}} = 1 + d2^{k+1} + d^2 2^{2k}.$$

Suy ra

$$a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}},$$

định lí được chứng minh. □

**Nhận xét :** Từ định lí trên suy ra rằng, không có lũy thừa nào của $2$ khác $2$ và $4$ có căn nguyên thủy, vì khi $a$ là số nguyên lẻ, $\operatorname{ord}_{2^k} a \neq \varphi(2^k)$, do

$$a^{\varphi(2^k)/2} \equiv 1 \pmod{2^k}.$$

Ta cũng chỉ ra rằng tồn tại số có bậc môđulô $2^k$ cao nhất có thể, tức là bậc $\varphi(2^k)/2$.

**Định lí 3.37.** *Giả sử $k$ là số nguyên, $k \geq 3$. Ta có*

$$\mathrm{ord}_{2^k} 5 = \varphi(2^k)/2 = 2^{k-2}.$$

***Chứng minh.*** Từ định lí trên đây ta được

$$5^{2^{k-2}} \equiv 1 \pmod{2^k},$$

khi $k \geq 3$. Từ đó suy ra $\mathrm{ord}_{2^k} 5 \mid 2^{k-2}$. Nếu ta chứng tỏ rằng $\mathrm{ord}_{2^k} 5 \nmid 2^{k-3}$ thì sẽ suy ra

$$\mathrm{ord}_{2^k} 5 = 2^{k-2}.$$

Dễ chỉ ra $\mathrm{ord}_{2^k} 5 \mid 2^{k-3}$, ta chứng minh quy nạp đồng dư sau :

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} \not\equiv 1 \pmod{2^k}, \quad k \geq 3.$$

Với $k = 3$, ta có

$$5 \equiv 1 + 4 \pmod{8}.$$

Bây giờ giả thiết rằng

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}.$$

Như vậy, tồn tại $d$ sao cho

$$5^{2^{k-3}} = 1 + 2^{k-1} + d.2^k.$$

Bình phương hai vế ta được :

$$5^{2^{k-2}} = (1 + 2^{k-1})^2 + 2(1 + 2^{k-1})d2^k + (d2^k)^2,$$

suy ra

$$5^{2^{k-2}} \equiv (1 + 2^{k-1})^2 = 1 + 2^k + 2^{2k-2} \equiv 1 + 2^k \pmod{2^{k+1}}.$$

Đồng dư này kết thúc chứng minh quy nạp, và ta có

$$\mathrm{ord}_{2^k} 5 = \frac{\varphi(2^k)}{2}.$$ □

Như vậy, ta đã xét trường hợp các lũy thừa của số nguyên tố lẻ hoặc lũy thừa của 2. Bây giờ ta chuyển sang trường hợp tổng quát.

**Định lí 3.38.** *Nếu $n$ không phải là lũy thừa của một số nguyên tố, hoặc hai lần lũy thừa một số nguyên tố, thì $n$ không có căn nguyên thủy.*

***Chứng minh.*** Giả sử $n$ được phân tích thành thừa số nguyên tố dạng :

$$n = p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}.$$

Giả sử rằng $n$ có căn nguyên thuỷ, tức là $(r,n) = 1$ và $\mathrm{ord}_n r = \varphi(n)$. Do $(r,n) = 1$ nên $(r,p^t) = 1$, trong đó $p^t$ là một trong các nhân tử là lũy thừa một số nguyên tố trong phân tích $n$. Do Định lí Ơ-le,

$$r^{\varphi(p^t)} \equiv 1 \pmod{p^t}.$$

Giả sử $U$ là bội chung nhỏ nhất của $\varphi(p_1^{t_1})$, $\varphi(p_2^{t_2})$, ... , $\varphi(p_m^{t_m})$. Vì $\varphi(p_i^{t_i}) \mid U$ nên

$$r^U \equiv 1 \pmod{p_i^{t_i}},\ i = 1,2,...,m.$$

Từ đó suy ra $r^U \equiv 1 \pmod{n}$, ($n$ là ước chung nhỏ nhất của $p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}$) và

$$\mathrm{ord}_n r = \varphi(n) \le U.$$

Do $\varphi$ là hàm nhân tính nên

$$\varphi(n) = \varphi(p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}) = \varphi(p_1^{t_1})\varphi(p_2^{t_2}) \dots \varphi(p_m^{t_m}).$$

Vậy

$$\varphi(p_1^{t_1})\varphi(p_2^{t_2}) \dots \varphi(p_m^{t_m}) \le U.$$

Như vậy, tích các số $\varphi(p_1^{t_1})$, $\varphi(p_2^{t_2})$, ... , $\varphi(p_m^{t_m})$ nhỏ hơn hoặc bằng bội chung nhỏ nhất của chúng. Điều này chỉ xảy ra khi các số đó là nguyên tố cùng nhau từng đôi một (và ta có đẳng thức).

Nhận xét rằng $\varphi(p^t) = p^{t-1}(p-1)$, nên $\varphi(p^t)$ chẵn nếu $p$ lẻ, hoặc $p = 2$, $t \ge 2$. Như vậy các số $\varphi(p_1^{t_1})$, $\varphi(p_2^{t_2})$, ... , $\varphi(p_m^{t_m})$ không thể nguyên tố cùng nhau từng cặp, trừ trường hợp $m = 1$ (và $n$ là lũy thừa một số nguyên tố), hoặc $m = 2$ và $n$ có dạng $n = 2p^t$, trong đó $p$ là số nguyên tố lẻ, $t$ nguyên dương. Định lí được chứng minh. □

Như vậy, để tìm tất cả các số nguyên có căn nguyên thủy, chỉ còn phải xét trường hợp $n = 2p^t$, trong đó $p$ là số nguyên tố lẻ và $t$ nguyên dương.

**Định lí 3.39.** *Nếu $n = 2p^t$, $p$ là số nguyên tố lẻ, $t$ nguyên dương thì $n$ có căn nguyên thủy. Cụ thể là, nếu $r$ là căn nguyên thủy môđulô $p^t$, và $r$ lẻ, thì nó là căn nguyên thủy môđulô $2p^t$, còn nếu $r$ chẵn thì $r + p^t$ là căn nguyên thủy môđulô $2p^t$.*

***Chứng minh.*** Giả sử $r$ là căn nguyên thủy môđulô $p^t$. Khi đó

$$r^{\varphi(p^t)} \equiv 1 \pmod{p^t},$$

và không số mũ dương nào bé hơn $\varphi(p^t)$ có tính chất đó. Ta có $\varphi(2p^t) = \varphi(2)\varphi(p^t) = \varphi(p^t)$, nên

$$r^{\varphi(2p^t)} \equiv 1 \pmod{p^t}.$$

Nếu $r$ lẻ thì

$$r^{\varphi(2p^t)} \equiv 1 \pmod{2}.$$

Do $(2, p^t) = 1$ nên từ đó suy ra

$$r^{\varphi(2p^t)} \equiv 1 \pmod{2p^t}.$$

Vì không có lũy thừa nào bé hơn của $r$ có tính chất đó nên ta suy ra $r$ là căn nguyên thương môđulô $2p^t$.

Bây giờ, giả sử $r$ chẵn, tức $r + p^t$ lẻ. Do đó

$$(r + p^t)^{\varphi(2p^t)} \equiv 1 \pmod{2}.$$

Vì $r + p^t \equiv r \pmod{p^t}$ nên

$$(r + p^t)^{\varphi(2p^t)} \equiv 1 \pmod{p^t}.$$

Vậy

$$(r + p^t)^{\varphi(2p^t)} \equiv 1 \pmod{2p^t},$$

và không lũy thừa nào bé hơn của $(r + p^t)$ có tính chất đó. Điều đó có nghĩa là, $(r + p^t)$ là căn nguyên thủy môđulô $2p^t$. □

***Ví dụ :*** Ta đã biết 3 là căn nguyên thủy môđulô $7^t$ với $t$ nguyên dương. Do 3 lẻ nên 3 cũng là căn nguyên thủy môđulô $2.7^t$ với $t$ nguyên dương. Chẳng hạn, 3 là căn nguyên thủy môđulô 14.

Tương tự, 2 là căn nguyên thủy môđulô $5^t$ với mọi $t$ nguyên dương. Do đó $2 + 5^t$ là căn nguyên thủy môđulô $2.5^t$ với $t$ nguyên dương. Chẳng hạn, 27 là căn nguyên thủy môđulô 50.

Kết hợp các kết quả đã nhận được ta có định lí sau.

**Định lí 3.40.** *Số nguyên dương $n$ có căn nguyên thủy khi và chỉ khi*

$$n = 2,\ 4,\ p^t,\ 2p^t,$$

*trong đó $p$ là số nguyên tố lẻ, $t$ nguyên dương.*

## BÀI TẬP CHƯƠNG 3

**1.** Tìm hệ thặng dư thu gọn môđulô $2^m$, trong đó $m$ là số nguyên dương.

**2.** Chứng minh rằng nếu $c_1, c_2, \ldots, c_{\varphi(m)}$ là một hệ thặng dư thu gọn môđulô $m$, thì $c_1 + c_2 + \cdots + c_{\varphi(m)} \equiv 0 \pmod{m}$.

**3.** Chứng minh rằng nếu $m$ là một số nguyên dương, $a$ là số nguyên tố cùng nhau với $m$, thì $1 + a + a^2 + \cdots + a^{\varphi(m)-1} \equiv 0 \pmod{m}$.

**4.** Tìm thặng dư dương bé nhất môđulô 35 của $3^{100.000}$.

**5.** Chứng minh rằng nếu $a$ là số nguyên thì $a^7 \equiv a \pmod{63}$.

**6.** Chứng minh rằng $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$ nếu $a$, $b$ nguyên dương và nguyên tố cùng nhau.

**7.** Chứng minh rằng các nghiệm của hệ đồng dư

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

trong đó $m_j$ nguyên tố cùng nhau từng cặp, được cho bởi

$$x \equiv a_1 M_1^{\varphi(m_1)} + a_2 M_2^{\varphi(m_2)} + \cdots + a_r M_r^{\varphi(m_r)} \pmod{M},$$

trong đó $M = m_1 m_2 \ldots m_r$, $M_j = M / m_j$, $j = 1, 2, \ldots, r$.

**8.** Tìm chữ số tận cùng trong khai triển thập phân của $7^{1000}$.

**9.** Chứng minh rằng nếu $m$ là số nguyên dương, $m > 1$, thì $a^m \equiv a^{m-\varphi(m)} \pmod{m}$ với mọi số nguyên dương $a$.

**10.** Tìm các số nguyên $n$ sao cho $\varphi(n)$ nhận các giá trị sau :

a) 1, b) 2, c) 3,

d) 6, e) 14, f) 24.

**11.** Với những số nguyên $n$ nào thì $\varphi(n)$

a) lẻ, b) chia hết cho 4, c) bằng $\frac{n}{2}$.

**12.** Chứng minh rằng với mọi $n$ nguyên dương ta có :

$$\varphi(2n) = \begin{cases} \varphi(n) & \text{nếu } n \text{ lẻ} \\ 2\varphi(n) & \text{nếu } n \text{ chẵn} \end{cases}$$

**13.** Chứng minh rằng nếu $n$ là số nguyên dương có $k$ ước nguyên tố lẻ khác nhau thì $\varphi(n)$ chia hết cho $2^k$.

**14.** Với những $n$ nào, $\varphi(n)$ là một lũy thừa của 2 ?

**15.** Chứng minh rằng nếu $m$ và $k$ là các số nguyên dương thì

$$\varphi(m^k) = m^{k-1}\varphi(m).$$

**16.** Với số nguyên dương $m$ nào thì $\varphi(m) \mid m$ ?

**17.** Chứng minh rằng nếu $a$, $b$ là các số nguyên dương thì

$$\varphi(ab) = (a,b)\varphi(a)\varphi(b)/\varphi((a,b)).$$

**18.** Chứng minh rằng nếu $m$ và $n$ lẻ là các số nguyên dương, $m \mid n$ thì $\varphi(m) \mid \varphi(n)$.

**19.** Chứng minh rằng số nguyên dương $n$ là hợp số nếu và chỉ nếu

$$\varphi(n) \le n - \sqrt{n}.$$

**20.** Giả sử $n$ là số nguyên dương. Lập dãy $n_1, n_2, n_3, \ldots$ bằng cách đặt $n_1 = \varphi(n)$, $n_{k+1} = \varphi(n_k)$, $k = 1, 2, 3, \ldots$ Chứng minh rằng tồn tại $r$ sao cho $n_r = 1$.

**21.** Các số nguyên dương nào có một số lẻ ước dương ?

**22.** Số nguyên dương nào có tổng các ước là lẻ ?

**23.** Tìm tất cả các số nguyên dương $n$ sao cho $\sigma(n)$ bằng

a) 12, b) 18, c) 24,

d) 48, e) 52, f) 84.

**24.** Tìm số nguyên dương $n$ nhỏ nhất sao cho $\tau(n)$ bằng

a) 1, b) 2, c) 3,

d) 6, e) 14, f) 100.

**25.** Chứng minh rằng nếu $k > 1$ là một số nguyên, thì phương trình

$\tau(n) = k$ có vô số nghiệm.

**26.** Những số nguyên nào có đúng $2$, $3$ hoặc $4$ ước dương ?

**27.** Tích các ước dương của số nguyên dương $n$ bằng bao nhiêu ?

**28.** Giả sử $\sigma_k(n)$ là tổng các lũy thừa bậc $k$ của các ước dương của $n$ :

$$\sigma_k(n) = \sum_{d|n} d^k .$$

Như vậy, $\sigma_0(n) = \tau(n)$, $\sigma_1(n) = \sigma(n)$.

a) Cho công thức tính $\sigma_k(p)$ khi $p$ nguyên tố.

b) Tính $\sigma_k(p^a)$, trong đó $p$ nguyên tố, $a$ nguyên dương.

c) Chứng minh rằng $\sigma_k(n)$ là hàm có tính chất nhân.

d) Cho công thức tính $\sigma_k(n)$ nếu $n$ có phân tích ra thừa số nguyên tố dưới dạng :

$$n = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m} .$$

**29.** Tìm tất cả các số nguyên dương $n$ sao cho

$$\varphi(n) + \sigma(n) = 2n.$$

**30.** Chứng minh rằng số các cặp số nguyên dương có bội chung nhỏ nhất $n$ là $\tau(n^2)$.

**31.** Giả sử $n$ là số nguyên dương. Lập dãy $n_1$, $n_2$, $n_3$, ... như sau : $n_1 = \tau(n)$, $n_{k+1} = \tau(n_k)$, $k = 1, 2, 3, \dots$ Chứng minh rằng tồn tại số nguyên $r$ sao cho $2 = n_r = n_{r+1} = n_{r+2} = \cdots$

**32.** Chứng minh rằng số nguyên dương $n$ là hợp số nếu và chỉ nếu

$$\sigma(n) > n + \sqrt{n}.$$

**33.** Chứng minh rằng nếu $n$ là số nguyên dương thì

$$\tau(n)^2 = \sum_{d|n} \tau(d)^3 .$$

**34.** Chứng minh rằng, nếu $\overline{a}$ là nghịch đảo của $a$ môđulô $n$ thì

$$\operatorname{ord}_n a = \operatorname{ord}_n \overline{a} .$$

**35.** a) Chứng minh rằng nếu $n$ là số nguyên dương, $a$, $b$ là các số nguyên

tố cùng nhau với $n$ sao cho $(\text{ord}_n a, \text{ord}_n b) = 1$, thì

$$(\text{ord}_n ab) = \text{ord}_n a.\text{ord}_n b.$$

b) Hãy cho công thức tính $(\text{ord}_n ab)$ khi bỏ điều kiện

$$(\text{ord}_n a, \text{ord}_n b) = 1.$$

**36.** Cho $m$ nguyên dương, $a$ nguyên tố cùng nhau với $m$. Chứng minh rằng, nếu $\text{ord}_m a = st$ thì $\text{ord}_m a^t = s$.

**37.** Giả thiết như Bài tập 36. Chứng minh rằng nếu $\text{ord}_m a = m - 1$ thì $m$ là số nguyên tố.

**38.** Chứng minh rằng $r$ là căn nguyên thủy môđulô $p$ trong đó $p$ là số nguyên tố lẻ, nếu và chỉ nếu

$$r^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$$

với mọi ước nguyên tố $q$ của $p - 1$.

**39.** Chứng minh rằng nếu $r$ là căn nguyên thủy môđulô $m$, $\bar{r}$ là nghịch đảo của $r$ môđulô $m$, thì $\bar{r}$ cũng là căn nguyên thủy môđulô $m$.

**40.** Chứng minh rằng $ord_{F_n} 2 \le 2^{n+1}$, trong đó $F_n = 2^{2^n} + 1$ là số Phecma thứ $n$.

**41.** Giả sử $p$ là một ước nguyên tố của số Phecma $F_n$. Chứng minh rằng

a) $\text{ord}_p 2 = 2^{n+1}$.

b) $2^{n+1} \mid (p - 1)$, và do đó $p$ phải có dạng $2^{n+1}k + 1$.

**42.** Cho $m = a^n - 1$, $a$ và $n$ là các số nguyên dương. Chứng minh rằng $n \mid \varphi(m)$.

**43.** Giả sử $p$ là số nguyên tố, $f(x)$ là đa thức bậc $n$ hệ số nguyên, có quá $n$ nghiệm môđulô $p$. Chứng minh rằng các hệ số của $f(x)$ đều chia hết cho $p$.

**44.** Giả sử $p$ là số nguyên tố. Chứng minh rằng các hệ số của đa thức

$$f(x) = (x-1)(x-2)\cdots(x-p+1) - x^{p-1} + 1$$

chia hết cho $p$. Từ đó suy ra định lí Wilson.

**45.** Giả sử $p$ là số nguyên tố, $p = 2q + 1$, trong đó $q$ là số nguyên tố, giả

sử $a$ là số nguyên dương, $1 < a < p-1$. Chứng minh rằng $p - a^2$ là căn nguyên thủy môđulô $p$.

**46.** Tìm căn nguyên thủy môđulô $11^2$, $13^2$, $17^2$, $19^2$.

**47.** Tìm căn nguyên thủy môđulô $3^k$, $11^k$, $13^k$, $17^k$ với mọi số nguyên dương $k$.

**48.** Tìm căn nguyên thủy môđulô $6$, $18$, $22$, $26$, $338$.

**49.** Giả sử $p$ là số nguyên tố lẻ, $t$ là số nguyên dương. Chứng minh rằng số các căn nguyên thủy môđulô $p^t$ bằng số các căn nguyên thuỷ môđulô $2p^t$.

**50.** Chứng minh rằng nếu $m$ có căn nguyên thủy, thì $x \equiv \pm 1 \pmod{m}$ là tất cả các nghiệm của $x^2 \equiv 1 \pmod{m}$.

**51.** Giả sử $n$ là số nguyên dương có căn nguyên thủy. Chứng minh rằng tích tất cả các số nguyên dương bé hơn $n$ và nguyên tố cùng nhau với $n$ sẽ đồng dư $-1$ môđulô $n$. (Khi $n$ là số nguyên tố, ta có định lí Wilson).

**52.** Chứng minh rằng, mỗi số nguyên lẻ đồng dư với đúng một số nguyên có dạng $(-1)^\alpha 5^\beta$, trong đó $\alpha = 0$ hoặc $1$, $\beta$ là số nguyên thỏa mãn $0 \le \beta \le 2^{k-2} - 1$, $k \ge 3$.

Chương 4.

# PHÂN SỐ LIÊN TỤC

Trong chương này, ta sẽ trình bày một số tính chất cơ sở nhất của phân số liên tục. Xét về nội tại cuốn sách, mục tiêu của chương là cung cấp công cụ cần thiết để giải các phương trình Điôphăng bậc 2 (được trình bày trong Chương 5). Tuy nhiên, xét một cách độc lập thì phân số liên tục là một đối tượng rất quan trọng của Số học, và mọi cuốn sách giáo khoa về Số học đều ít nhiều phải đề cập đến chủ đề này.

## § 1. SỐ HỮU TỈ VÀ SỐ VÔ TỈ

**Định nghĩa 4.1.** Số thực $\alpha$ được gọi là *số hữu tỉ* nếu $\alpha = \frac{a}{b}$, trong đó $a$, $b$ là các số nguyên, $b \neq 0$. Nếu $\alpha$ không phải là hữu tỉ, ta nói $\alpha$ là *số vô tỉ*.

**Định lí 4.2.** *Nếu $\alpha$, $\beta$ là các số hữu tỉ thì $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ và $\frac{\alpha}{\beta}$ (khi $\beta \neq 0$) là số hữu tỉ.*

***Chứng minh.*** Giả sử $\alpha$, $\beta$ là các số hữu tỉ, $\alpha = \frac{a}{b}$, $\beta = \frac{c}{d}$, trong đó $a$, $b$, $c$, $d$ là các số nguyên, $b \neq 0$, $d \neq 0$. Khi đó, mỗi số sau đây

$$\alpha + \beta = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

$$\alpha - \beta = \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd},$$

$$\alpha\beta = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

$$\frac{\alpha}{\beta} = \frac{a}{b} \Big/ \frac{c}{d} = \frac{ad}{bc}, \quad (\beta \neq 0)$$

đều là số hữu tỉ, vì chúng là thương của hai số nguyên với số chia khác $0$.

Khi viết các số vô tỉ như phân số $\frac{a}{b}$, trong đó $a$, $b$ nguyên và $b \neq 0$, ta thường dùng *dạng tối giản*, tức là $a$, $b$ nguyên tố cùng nhau.

Trong lịch sử, các số vô tỉ được phát hiện lần đầu tiên khi người ta tìm cách đo đường chéo của hình vuông với cạnh là 1. Ta có định lí sau

**Định lí 4.3.** *Số $\sqrt{2}$ là vô tỉ.*

***Chứng minh.*** Giả sử $\sqrt{2} = \frac{a}{b}$, trong đó $a$, $b$ là các số nguyên tố cùng nhau, $b \neq 0$. Khi đó ta có

$$2 = \frac{a^2}{b^2},$$

tức là

$$2b^2 = a^2.$$

Vì $2 \mid a^2$ nên $2 \mid a$. Đặt $a = 2c$, ta được

$$b^2 = 2c^2.$$

Vậy $2 \mid b^2$, nên $2 \mid b$. Nhưng $(a,b) = 1$ nên 2 không thể đồng thời là ước của $a$ và $b$. Vậy $\sqrt{2}$ là số vô tỉ. □

Trường hợp tổng quát của định lí trên là kết quả sau rất hay được dùng khi xét các phương trình nghiệm nguyên.

**Định lí 4.4.** *Giả sử $\alpha$ là một nghiệm của đa thức*

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0,$$

*trong đó các hệ số $c_0, c_1, \ldots, c_{n-1}$ nguyên. $c_0 \neq 0$. Khi đó $\alpha$ hoặc là số nguyên, hoặc là số vô tỉ.*

***Chứng minh.*** Giả sử $\alpha$ là số hữu tỉ. Khi đó ta có thể viết $\alpha = a/b$, trong đó $a$ và $b$ là các số nguyên nguyên tố cùng nhau với $b \neq 0$. Vì $\alpha$ là một nghiệm của đa thức $x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, nên ta có :

$$(a/b)^n + c_{n-1}(a/b)^{n-1} + \cdots + c_1(a/b) + c_0.$$

Nhân với $b^n$, ta được :

$$a^n + c_{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n = 0.$$

Vì $a^n = n(-c_{n-1}a^{n-1}b - \cdots - c_1 ab^{n-1} - c_0 b^{n-1})$ nên $b \mid a^n$. Giả sử $b \neq \pm 1$.

Khi đó, $b$ có ước nguyên tố $p$. Do $p \mid b$ và $b \mid a^n$ nên $p \mid a^n$. Suy ra $p \mid a$. Tuy nhiên $(a,b) = 1$, mâu thuẫn này chứng tỏ rằng $b = \pm 1$, nên nếu $\alpha$ hữu tỉ thì $\alpha = \pm a$, tức là $\alpha$ là một số nguyên. □

Ví dụ : Giả sử $a$ là số nguyên dương, không phải là lũy thừa bậc $m$ của một số tự nhiên. Khi đó $\sqrt[m]{a}$ là số vô tỉ, vì $\alpha = \sqrt[m]{a}$ là nghiệm của đa thức $x^m - a$. Như vậy, nếu $a$ là số không chính phương thì $\sqrt{a}$ là số vô tỉ.

## § 2. PHÂN SỐ LIÊN TỤC HỮU HẠN

Trong phần này, ta sẽ nghiên cứu cách biểu diễn một số dưới dạng *phân số liên tục*. Ví dụ :

$$\frac{7}{5} = 1 + \frac{2}{5} = 1 + \cfrac{1}{2 + \cfrac{1}{2}}.$$

Biểu diễn một số nhờ phân số liên tục có nhiều ứng dụng khác nhau, trong đó có việc ứng dụng để giải các phương trình nghiệm nguyên thuộc một số lớp thường gặp.

**Định nghĩa 4.5.** *Phân số liên tục* là một biểu thức có dạng

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

trong đó $a_0, a_1, a_2, \ldots, a_n$ là các số thực, $a_1, a_2, \ldots, a_n$ dương. Các số thực $a_1, a_2, \ldots, a_n$ được gọi là các *thương riêng* của phân số liên tục. Một phân số liên tục được gọi là *đơn* nếu $a_0, a_1, a_2, \ldots, a_n$ là các số nguyên.

Để đơn giản, ta dùng kí hiệu $[a_0 ; a_1, a_2, \ldots, a_n]$ để chỉ phân số liên tục nói trên.

Bây giờ ta sẽ chỉ ra rằng, mỗi phân số liên tục đơn hữu hạn biểu diễn một số hữu tỉ. Ngược lại, mỗi số hữu tỉ có thể biểu diễn như một phân số liên tục đơn hữu hạn.

**Định lí 4.6.** *Mỗi phân số liên tục đơn hữu hạn biểu diễn một số hữu tỉ.*

***Chứng minh.*** Ta dùng quy nạp toán học. Với $n = 1$, ta có

$$[a_0 \,;\, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$$

là một số hữu tỉ. Giả sử với số nguyên dương $k$, phân số liên tục đơn hữu hạn tùy ý $[a_0 \,;\, a_1, \ldots, a_k]$ là số hữu tỉ. Giả sử $a_0$, $a_1$, $\ldots$, $a_{k+1}$ là các số nguyên, trong đó $a_1$, $\ldots$, $a_{k+1}$ dương. Ta có

$$[a_0 \,;\, a_1, \ldots, a_{k+1}] = a_0 + \frac{1}{[a_1 \,;\, a_2, \ldots, a_{k+1}]}.$$

Do giả thiết quy nạp, $[a_1 \,;\, a_2, \ldots, a_{k+1}]$ là số hữu tỉ. Như vậy, tồn tại các số nguyên $r$, $s$, với $s \neq 0$ sao cho

$$[a_1 \,;\, a_2, \ldots, a_{k+1}] = \frac{r}{s}.$$

Từ đó ta có

$$[a_0 \,;\, a_1, \ldots, a_{k+1}] = a_0 + \frac{1}{r/s} = \frac{a_0 r + s}{r}.$$

Định lí được chứng minh. □

**Định lí 4.7.** *Mỗi số hữu tỉ có thể biểu diễn như là một phân số liên tục hữu hạn.*

***Chứng minh.*** Giả sử $x = \frac{a}{b}$, trong đó $a$, $b$ là các số nguyên, $b > 0$. Đặt $r_0 = a$, $r_1 = b$. Theo thuật chia O-clit, ta được

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 < r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3 && 0 < r_3 < r_2,\\
r_2 &= r_3 q_3 + r_4 && 0 < r_4 < r_3,\\
&\cdots && \cdots\\
r_{n-3} &= r_{n-2} q_{n-2} + r_{n-1} && 0 < r_{n-1} < r_{n-2},\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 < r_n < r_{n-1},\\
r_{n-1} &= r_n q_n
\end{aligned}$$

Trong các biểu thức trên, $q_2$, $q_3$, $\ldots$, $q_n$ là các số nguyên dương. Viết các biểu thức trên dưới dạng phân số liên tục, ta được :

$$\frac{a}{b} = \frac{r_0}{r_1} = q_1 + \frac{r_2}{r_1} = q_1 + \frac{1}{r_1 / r_2}$$

$$\frac{r_1}{r_2} = q_2 + \frac{r_3}{r_2} = q_2 + \frac{1}{r_2 / r_3}$$

$$\frac{r_2}{r_3} = q_3 + \frac{r_4}{r_3} = q_3 + \frac{1}{r_3 / r_4}$$

$$\ldots$$

$$\frac{r_{n-3}}{r_{n-2}} = q_{n-2} + \frac{r_{n-1}}{r_{n-2}} = q_{n-2} + \frac{1}{r_{n-2} / r_{n-1}}$$

$$\frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}} = q_{n-1} + \frac{1}{r_{n-1} / r_n}$$

$$\frac{r_{n-1}}{r_n} = q_n.$$

Thay giá trị $r_1 / r_2$ từ đẳng thức thứ hai vào đẳng thức thứ nhất, ta được

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \dfrac{1}{r_2 / r_3}}.$$

Tương tự, thay giá trị $r_2 / r_3$ vào đẳng thức vừa nhận được, ta có :

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \dfrac{1}{q_3 + \dfrac{1}{r_3 / r_4}}}.$$

Tiếp tục như trên, ta được

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}$$

Vậy $\frac{a}{b} = [q_1 ; q_2, \dots , q_n]$, tức là mỗi số hữu tỉ đều có thể viết dưới dạng phân số liên tục đơn hữu hạn.

**Chú ý :** Biểu diễn một số hữu tỉ dưới dạng phân số liên tục đơn không phải là duy nhất. Chẳng hạn, từ đồng nhất thức

$$a_n = (a_n - 1) + \frac{1}{1},$$

ta có :

$$[a_0 ; a_1, \dots , a_{n-1}, a_n] = [a_0 ; a_1, \dots , a_{n-1}, a_n - 1, 1]$$

và $a_n > 1$. Ví dụ :

$$\frac{7}{11} = [0 ; 1, 1, 1, 3] = [0, 1, 1, 1, 2, 1].$$

**Định nghĩa 4.8.** Các phân số liên tục $[a_0 ; a_1, a_2, \dots , a_k]$, trong đó $k$ là số nguyên, $0 \le k < n$, được gọi là *hội tụ thứ* $k$ của phân số liên tục $[a_0 ; a_1, a_2, \dots , a_k]$. Ta kí hiệu hội tụ thứ $k$ là $C_k$.

Sau đây, ta sẽ xét một số tính chất của phân số liên tục. Các tính chất này sẽ được dùng khi giải một số lớp phương trình nghiệm nguyên.

**Định lí 4.9.** *Giả sử* $a_0, a_1, a_2, \dots , a_n$ *là các số thực, trong đó* $a_i > 0$ *với* $i \ge 1$. *Xét dãy* $p_0, p_1, \dots , p_n$ *và* $q_0, q_1, \dots , q_n$ *xác định như sau :*

$$\begin{aligned} p_0 &= a_0, & q_0 &= 1, \\ p_1 &= a_0 a_1 + 1, & q_1 &= a_1, \\ p_k &= a_k p_{k-1} + p_{k-2}, & q_k &= a_k q_{k-1} + q_{k-2}, \end{aligned}$$

*với* $k = 2, 3, \dots , n$. *Khi đó, hội tụ thứ* $k$ : $C_k = [a_0 ; a_1, \dots , a_k]$ *được tính theo công thức*

$$C_k = \frac{p_k}{q_k}.$$

***Chứng minh.*** Ta dùng quy nạp toán học. Rõ ràng công thức đúng với $k = 0$. Với $k = 1$ ta có :

$$C_1 = [a_0 ; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}.$$

Vậy, công thức đúng cho $k = 1$. Bây giờ ta giả thiết rằng, định lí đúng với

mọi $k$, $2 \le k < n$. Ta có :

$$C_k = [a_0 \,;\, a_1, \ldots, a_k] = \frac{p_k}{q_k} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}}. \tag{1}$$

Theo định nghĩa của các số $p_j$, $q_j$, ta thấy rằng, các số thực $p_{k-1}$, $p_{k-2}$, $q_{k-1}$, $q_{k-2}$ chỉ phụ thuộc vào các thương riêng $a_0$, $a_1$, ... , $a_{k-1}$. Do đó, ta có thể thay số thực $a_k$ trong biểu thức (1) bởi $a_k + \dfrac{1}{a_k + 1}$ và nhận được :

$$\begin{aligned} C_{k+1} = [a_0 \,;\, a_1, \ldots, a_k, a_{k+1}] &= \left[a_0 \,;\, a_1, \ldots, a_{k+1}, a_k + \frac{1}{a_k}\right] \\ &= \frac{\left(a_k + \dfrac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \dfrac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} \\ &= \frac{a_{k+1}\left(a_k p_{k-1} + p_{k-2}\right) + p_{k-1}}{a_{k+1}\left(a_k q_{k-1} + q_{k-2}\right) + q_{k-1}} \\ &= \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} \\ &= \frac{p_{k-1}}{q_{k-1}}. \end{aligned}$$

Định lí được chứng minh. □

***Ví dụ*** : Ta xét phân số $\dfrac{173}{55} = [3 \,;\, 6, 1, 7]$. Các giá trị $p_j$, $q_j$ đầu tiên ($j = 0, 1, 2, 3$) là :

$$\begin{aligned} p_0 &= 3 & q_0 &= 1 \\ p_1 &= 3.6 + 1 = 19 & q_1 &= 6 \\ p_2 &= 1.19 + 3 = 22 & q_2 &= 1.6 + 1 = 7 \\ p_3 &= 7.22 + 19 = 173 & q_3 &= 7.7 + 6 = 55. \end{aligned}$$

Các hội tụ riêng sẽ là

$$C_0 = \frac{p_0}{q_0} = \frac{3}{1} = 3$$

$$C_1 = \frac{p_1}{q_1} = \frac{19}{6}$$
$$C_2 = \frac{p_2}{q_2} = \frac{22}{7}$$
$$C_3 = \frac{p_3}{q_3} = \frac{173}{55}.$$

Tính chất sau đây thường được dùng để giải phương trình nghiệm nguyên.

**Định lí 4.10.** *Giả sử $k$ là số nguyên dương, $k \geq 1$. Giả sử hội tụ thứ $k$ của phân số liên tục $[a_0\,;a_1,\ldots,a_k]$ là $C_k = \frac{p_k}{q_k}$ ; trong đó $p_k$, $q_k$ được định nghĩa trong Định lí 4.9 . Khi đó*

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

***Chứng minh.*** Ta dùng quy nạp toán học. Với $k = 1$, ta có

$$p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1).1 - a_0 a_1 = 1.$$

Giả sử định lí đúng với $1 \leq k < m$, tức là

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Khi đó ta có

$$\begin{aligned} p_{k+1} q_k - p_k q_{k+1} &= (a_{k+1} p_k + p_{k-1}) q_k - p_k (a_{k+1} q_k + q_{k-1}) \\ &= p_{k-1} q_k - p_k q_{k-1} = -(-1)^{k-1} = (-1)^k. \end{aligned}$$

Định lí được chứng minh. □

**Hệ quả 4.11.** *Giả sử $C_k = \frac{p_k}{q_k}$ là hội tụ riêng thứ $k$ của phân số liên tục đơn $[a_0\,;a_1,\ldots,a_n]$, trong đó các số nguyên $p_k$, $q_k$ được xác định như trong Định lí 4.9 . Khi đó, $p_k$, $q_k$ nguyên tố cùng nhau.*

***Chứng minh.*** Đặt $d = (p_k, q_k)$. Từ Định lí 4.10 ta có

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}.$$

Vậy $d \mid (-1)^{k-1}$, suy ra $d = 1$. □

**Hệ quả 4.12.** *Giả sử $C_k = \frac{p_k}{q_k}$ là hội tụ thứ $k$ của phân số liên tục đơn*

$[a_0 ; a_1, \ldots, a_k]$. *Khi đó*

$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

*với mọi số nguyên* $k$, $1 \leq k \leq m$ *và*

$$C_k - C_{k-2} = \frac{a_k (-1)^{k-1}}{q_k q_{k-2}}$$

*với mọi số nguyên* $k$, $2 \leq k \leq n$.

***Chứng minh.*** Theo Định lí 4.10 ta có

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}.$$

Ta nhận được đẳng thức thứ nhất :

$$C_k - C_{k-1} = \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

Để chứng minh đẳng thức thứ hai, ta nhận xét rằng

$$C_k - C_{k-2} = \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} + p_{k-2} q_k}{q_k q_{k-2}}.$$

Mặt khác ta có

$$\begin{aligned} p_k q_{k-2} - p_{k-2} q_k &= (a_k p_{k-1} + p_{k-2}) q_{k-2} - p_{k-2}(a_k q_{k-1} + q_{k-2}) \\ &= a_k (p_{k-1} q_{k-2} - p_{k-2} q_{k-1}) \\ &= a_k (-1)^{k-1}. \end{aligned}$$

Từ đó suy ra

$$C_k - C_{k-2} = \frac{a_k (-1)^{k-1}}{q_k q_{k-2}}$$

Hệ quả được chứng minh. □

Ta chuyển sang một định lí có vai trò quan trọng khi xây dựng các phân số liên tục vô hạn.

**Định lí 4.13.** *Giả sử* $C_k$ *là hội tụ thứ* $k$ *của phân số liên tục đơn* $[a_0 ; a_1, \ldots, a_k]$. *Khi đó*

$$C_1 > C_3 > C_5 > \cdots,$$

$$C_0 < C_2 < C_4 < \cdots ,$$

*đồng thời mỗi giới hạn riêng chỉ số lẻ đều lớn hơn các giới hạn riêng chỉ số chẵn.*

***Chứng minh.*** Với $k = 2, 3, \ldots, n$, ta có

$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}.$$

Từ đó suy ra

$$C_k < C_{k-2}$$

khi $k$ chẵn, và

$$C_k > C_{k-2}$$

khi $k$ lẻ. Do đó

$$C_1 > C_3 > C_5 > \cdots ,$$
$$C_0 < C_2 < C_4 < \cdots ,$$

Mặt khác, với mỗi $m \geq 1$ ta có

$$C_{2m} - C_{2m-1} = \frac{(-1)^{2m-1}}{q_{2m} q_{2m-1}} < 0,$$

nên $C_{2m-1} > C_{2m}$. Với $k$, $j$ tùy ý, $k > 0$, $j \geq 1$ ta có :

$$C_{2j-1} > C_{2j-1+2k} > C_{2j+2k} > C_{2k}.$$

Định lí được chứng minh. □

## § 3. PHÂN SỐ LIÊN TỤC VÔ HẠN

Giả sử ta có dãy vô hạn các số nguyên dương $a_0$, $a_1$, $a_2$, ... Vấn đề đặt ra là : có thể xây dựng một phân số liên tục vô hạn $[a_0 ; a_1, a_2, \ldots]$ hay không ? Mục tiêu của phần này là trả lời câu hỏi đó. Trước tiên ta nhắc lại định lí sau đây.

**Định lí 4.14.** *Giả sử $x_0$, $x_1$, $x_2$, ... là một dãy các số thực sao cho $x_0 \leq x_1 \leq x_2 \leq \cdots \leq U$ hoặc $x_0 \geq x_1 \geq \cdots \geq L$, trong đó $U$, $L$ là các số thực nào đó. Khi đó, dãy $x_0$, $x_1$, $x_2$, ... có giới hạn, tức là tồn tại số thực $x$ sao cho*

$$\lim_{n \to \infty} x_n = x.$$

Nói một cách ngắn gọn, Định lí 4.14 khẳng định rằng, các dãy đơn điệu bị chặn đều có giới hạn.

Sử dụng định lí trên, ta có thể định nghĩa một phân số liên tục vô hạn như là giới hạn của các phân số liên tục hữu hạn.

**Định lí 4.15.** *Giả sử* $a_0, a_1, a_2, \ldots$ *là dãy vô hạn các số nguyên với* $a_1, a_2, \ldots$ *dương. Giả sử* $C_k = [a_0 ; a_1, a_2, \ldots, a_k]$. *Khi đó, các hội tụ* $C_k$ *dần đến giới hạn* $\alpha$, *tức là*

$$\lim_{k\to\infty} C_k = \alpha.$$

*Giới hạn* $\alpha$ *nói trên được gọi là phân số liên tục đơn vô hạn.*

$$\alpha = [a_0 ; a_1, a_2, \ldots].$$

***Chứng minh.*** Giả sử $m$ là số nguyên dương. Từ Định lí 4.13 ta có

$$C_1 > C_3 > C_5 > \cdots > C_{m-1},$$

$$C_0 < C_2 < C_4 < \cdots < C_m,$$

đồng thời $C_{2j} < C_{2k+1}$ nếu $2j \le m$, $2k+1 < m$. Bằng cách xét mọi giá trị có thể của $m$, ta thấy

$$C_1 > C_3 > C_5 > \cdots > C_{2n-1} > C_{2n+1} > \cdots$$

$$C_0 < C_2 < C_4 < \cdots < C_{2n-2} < C_{2n} < \cdots$$

và $C_{2j} < C_{2k+1}$ với mọi số nguyên dương $j$ và $k$. Như vậy, các dãy $C_1$, $C_3$, $C_5$, ... và $C_0$, $C_2$, $C_4$, ... là các dãy đơn điệu bị chặn. Do đó, $C_1$, $C_3$, $C_5$, ... dần đến giới hạn $\alpha_1$, dãy $C_0$, $C_2$, $C_4$, ... dần đến giới hạn $\alpha_2$ tức là

$$\lim_{n\to\infty} C_{2n+1} = \alpha_1,$$

$$\lim_{n\to\infty} C_{2n} = \alpha_2.$$

Ta sẽ chứng minh rằng $\alpha_1 = \alpha_2$. Ta có

$$C_{2n+1} - C_{2n} = \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{(-1)^{(2n+1)-1}}{q_{n+1}q_{2n}} = \frac{1}{q_{2n+1}q_{2n}}.$$

Do $q_k \ge k$ với mọi số nguyên dương $k$ nên

$$\frac{1}{q_{2n+1}q_{2n}} < \frac{1}{(2n+1)(2n)},$$

nghĩa là

$$\lim_{n\to\infty}(C_{2n+1} - C_{2n}) = 0.$$

Vậy các dãy $C_1$, $C_3$, $C_5$, ... và $C_0$, $C_2$, $C_4$, ... có cùng giới hạn, tức là $\alpha_1 = \alpha_2$. Định lí được chứng minh. □

Trong tiết trước, ta đã chứng minh rằng các số hữu tỉ là các phân số liên tục đơn hữu hạn. Bây giờ, ta sẽ chỉ ra rằng giá trị của phân số liên tục đơn vô hạn tùy ý là số vô tỉ.

**Định lí 4.16.** *Giả sử $a_0$, $a_1$, $a_2$, ... là các số nguyên, với $a_1$, $a_2$, ... dương. Khi đó $[a_0\ ;\ a_1,\ a_2,\ ...]$ là số vô tỉ.*

***Chứng minh.*** Đặt $\alpha = [a_0\ ;\ a_1,\ a_2,\ ...]$ và giả sử

$$C_k = \frac{p_k}{q_k} = [a_0\ ;\ a_1,\ a_2,\ ...,\ a_k]$$

là hội tụ riêng thứ $k$ của $\alpha$. Với mọi số nguyên dương $n$, ta có

$$C_{2n} < \alpha < C_{2n+1}.$$

Do đó

$$0 < \alpha - C_{2n} < C_{n+1} - C_{2n}.$$

Mặt khác,

$$C_{2n+1} - C_{2n} = \frac{1}{q_{2n+1}q_{2n}},$$

suy ra

$$0 < \alpha - C_{2n} = \alpha - \frac{p_{2n}}{q_{2n}} < \frac{1}{q_{2n+1}q_{2n}}.$$

Vậy

$$0 < \alpha q_{2n} - p_{2n} < \frac{1}{q_{2n+1}}.$$

Giả sử $\alpha$ là số hữu tỉ, tức là $\alpha = \frac{a}{b}$, trong đó $a$, $b$ nguyên, $b \neq 0$. Khi đó

$$0 < \frac{aq_{2n}}{b} - p_{2n} < \frac{1}{q_{2n+1}},$$

suy ra

$$0 < aq_{2n} - bp_{2n} < \frac{b}{q_{2n+1}}.$$

Chú ý rằng, $aq_{2n} - bp_{2n}$ là số nguyên với mọi $n$, mà $q_{2n+1} > 2n + 1$, nên phải tồn tại $n$ để $q_{2n+1} > b$, tức là

$$0 < aq_{2n} - bp_{2n} < 1.$$

Mâu thuẫn này chứng tỏ $\alpha$ là số vô tỉ. □

Ta sẽ chứng minh điều ngược lại, tức là mỗi số vô tỉ có thể biểu diễn duy nhất dưới dạng phân số liên tục đơn vô hạn.

**Định lí 4.17.** *Giả sử $\alpha = \alpha_0$ là số vô tỉ và $a_0$, $a_1$, $a_2$, ... là dãy xác định theo công thức sau :*

$$a_k = [\alpha_k], \ \alpha_{k+1} = \frac{1}{\alpha_k - a_k}, \tag{1}$$

*với $k = 0, 1, 2, ...$ Khi đó, $\alpha$ là giá trị của phân số liên tục đơn vô hạn $[a_0 ; a_1, a_2, ...]$.*

***Chứng minh.*** Từ định nghĩa trên ta thấy $a_k$ là số nguyên với mọi $k$. Hơn nữa, dễ chứng minh rằng $\alpha_k$ là số vô tỉ với mọi $k$. Thật vậy, $\alpha_0 = \alpha$ là số vô tỉ. Nếu giả thiết $\alpha_k$ là số vô tỉ thì từ quan hệ

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$$

suy ra

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}}. \tag{2}$$

Nếu $\alpha_{k+1}$ là số hữu tỉ thì $\alpha_k$ là số hữu tỉ : vô lí. Như vậy, với mọi $k$, $\alpha_k \neq a_k$ và

$$a_k < \alpha_k < a_k + 1.$$

Do đó

$$0 < \alpha_k - a_k < 1$$

và

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k} > 1,$$

$$a_{k+1} = [\alpha_{k+1}] \geq 1$$

với $k = 0, 1, 2, ...$ Vậy $a_1, a_2, ...$ là các số nguyên dương.

Áp dụng liên tiếp (2) ta được :

$$\alpha = \alpha_0 = a_0 + \frac{1}{\alpha_1} = [a_0\ ;\ \alpha_1]$$

$$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{\alpha_2}} = [a_0\ ;\ a_1,\ \alpha_2]$$

$$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + a_k + \cfrac{1}{\alpha_{k+1}}}} = [a_0\ ;\ a_1,\ a_2,\ \ldots\ ,\ a_k,\ \alpha_{k+1}]$$

Bây giờ ta phải chứng minh rằng giá trị $[a_0\ ;\ a_1,\ a_2,\ \ldots\ ,\ a_k,\ \alpha_{k+1}]$ dần đến $\alpha$ khi $k$ dần ra vô cùng. Ta có :

$$\alpha = [a_0\ ;\ a_1,\ a_2,\ \ldots\ ,\ a_k,\ \alpha_{k+1}] = \frac{\alpha_{k+1}p_k + p_{k+1}}{\alpha_{k+1}q_k + q_{k+1}},$$

trong đó $C_j = \dfrac{p_j}{q_j}$ là hội tụ thứ $j$ của $[a_0\ ;\ a_1,\ a_2,\ \ldots\ ]$. Vậy

$$\alpha - C_k = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}} - \frac{p_k}{q_k} = \frac{-(p_kq_{k-1} - p_{k-1}q_k)}{(\alpha_{k+1}q_k + q_{k-1})q_k}$$

$$= \frac{(-1)^k}{(\alpha_{k+1}q_k + q_{k-1})q_k}.$$

Vì

$$\alpha_{k+1}q_k + q_{k-1} > \alpha_{k+1}q_k + q_{k-1} = q_{k+1}$$

nên

$$|\alpha - C_k| < \frac{1}{q_kq_{k+1}}.$$

Do $q_k > k$ nên suy ra $|\alpha - C_k| \to 0$ khi $k \to \infty$. Vậy, giá trị của phân số liên tục đơn vô hạn $[a_0\ ;\ a_1,\ a_2,\ \ldots\ ]$ là $\alpha$. □

Định lí sau đây cho thấy tính duy nhất của biểu diễn một số vô tỉ dưới dạng phân số liên tục đơn vô hạn.

**Định lí 4.18.** *Nếu hai phân số liên tục đơn vô hạn* $[a_0 ; a_1, a_2, \ldots]$ *và* $[b_0 ; b_1, b_2, \ldots]$ *biểu diễn cùng một số vô tỉ, thì* $a_k = b_k$ *với mọi* $k = 0, 1, 2, \ldots$

***Chứng minh.*** Giả sử $\alpha = [a_0 ; a_1, a_2, \ldots]$. Khi đó do $C_0 = a_0$, $C_1 = a_0 + \dfrac{1}{a_1}$ nên theo Định lí 4.13 ta có

$$a_0 < \alpha < a_0 + \frac{1}{a_1}.$$

Từ đó suy ra $a_0 = [\alpha]$. Hơn nữa,

$$[a_0 ; a_1, a_2, \ldots] = a_0 + \frac{1}{[a_1 ; a_2, a_3, \ldots]},$$

vì

$$\alpha = [a_0 ; a_1, a_2, \ldots] = \lim_{k\to\infty}[a_0 ; a_1, a_2, \ldots, a_k]$$

$$= a_0 + \frac{1}{\lim\limits_{k\to\infty}[a_1 ; a_2, a_3, \ldots, a_k]} = a_0 + \frac{1}{[a_1 ; a_2, a_3, \ldots]}$$

Giả sử

$$[a_0 ; a_1, a_2, \ldots] = [b_0 ; b_1, b_2, \ldots].$$

Chứng minh trên đây chỉ ra rằng

$$a_0 = b_0 = [\alpha]$$

đồng thời

$$a_0 + \frac{1}{[a_1 ; a_2, a_3, \ldots]} = b_0 + \frac{1}{[b_1 ; b_2, b_3, \ldots]}$$

Vậy

$$[a_1 ; a_2, a_3, \ldots] = [b_1 ; b_2, b_3, \ldots]$$

Bây giờ giả sử ta có $a_k = b_k$ và $[a_{k+1} ; a_{k+2}, \ldots] = [b_{k+1} ; b_{k+2}, \ldots]$. Lí luận như trên suy ra rằng $a_{k+1} = b_{k+1}$ và

$$a_{k+1} + \frac{1}{[a_{k+2} ; a_{k+3}, \ldots]} = b_{k+1} + \frac{1}{[b_{k+2} ; b_{k+3}, \ldots]}.$$

Do đó

$$[a_{k+2}\,;\,a_{k+3},\ldots] = [b_{k+2}\,;\,b_{k+3},\ldots]$$

Bằng phương pháp quy nạp ta suy ra $a_k = b_k$ với $k = 0,\ 1,\ 2,\ldots$ □

Định lí 4.18 cũng cho ta thuật toán tìm biểu diễn dạng phân số liên tục đơn của một số thực. Ta xét ví dụ cụ thể sau. Giả sử $\alpha = \sqrt{6}$. Khi đó ta có $a_0 = [\sqrt{6}] = 2$.

$$\alpha_1 = \frac{1}{\sqrt{6}-2} = \frac{\sqrt{6}+2}{2},\quad a_1 = \left[\frac{\sqrt{6}+2}{2}\right] = 2,$$

$$\alpha_2 = \frac{1}{\left(\dfrac{\sqrt{6}+2}{2}\right)-2} = \sqrt{6}+2,\quad a_2 = \left[\sqrt{6}+2\right] = 4,$$

$$\alpha_3 = \frac{1}{\left(\sqrt{6}+2\right)-4} = \frac{\sqrt{6}+2}{2} = \alpha_1.$$

Vì $\alpha_3 = \alpha_1$ nên $a_3 = a_1,\ a_4 = a_2,\ldots$ Ta có

$$\sqrt{6} = [2\,;\ 2,\ 4,\ 2,\ 4,\ldots]$$

Như vậy, phân số liên tục đơn của $\sqrt{6}$ là tuần hoàn. Về sau, ta sẽ nghiên cứu kĩ hơn các phân số liên tục vô hạn tuần hoàn.

**Nhận xét.** Các hội tụ của một phân số liên tục đơn vô hạn của một số hữu tỉ cho ta một xấp xỉ tốt số vô tỉ bởi số hữu tỉ. Thật vậy, giả sử $\dfrac{p_k}{q_k}$ là hội tụ thứ $k$ của phân số liên tục của số vô tỉ $\alpha$, khi đó

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}}.$$

Từ đó cũng suy ra

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^2},$$

vì $q_k < q_{k+1}$.

Sau đây ta sẽ chỉ ra rằng, xấp xỉ như vậy là tốt nhất theo nghĩa số hữu tỉ $\dfrac{p_k}{q_k}$ gần số $\alpha$ hơn bất kì số hữu tỉ nào khác với mẫu số bé hơn $q_k$.

**Định lí 4.19.** *Giả sử* $\alpha$ *là số vô tỉ,* $\dfrac{p_j}{q_j}$, $j = 1, 2, \ldots$ *là các hội tụ của phân số liên tục đơn vô hạn của* $\alpha$. *Giả sử* $r$, $s$ *là các số nguyên,* $s > 0$, *sao cho*

$$|s\alpha - r| < |q_k\alpha - p_k|.$$

*Khi đó*

$$s \geq q_{k+1}.$$

***Chứng minh.*** Giả sử $|s\alpha - r| < |q_k\alpha - p_k|$, nhưng $r \leq s < q_{k+1}$. Xét hệ phương trình

$$\begin{cases} p_k x + p_{k+1} y = r \\ q_k x + q_{k+1} y = s. \end{cases}$$

Nhân phương trình thứ nhất với $q_k$, phương trình thứ hai với $p_k$ và trừ cho nhau, ta được:

$$(p_{k+1}q_k - p_k q_{k+1})y = rq_k - sp_k.$$

Theo Định lí 4.10, $(p_{k+1}q_k - p_k q_{k+1}) = (-1)^k$. Từ đó ta có

$$y = (-1)^k(rq_k - sp_k).$$

Tương tự ta có

$$x = (-1)^k(sp_{k+1} - rq_{k+1}).$$

Chú ý rằng $x \neq 0$ và $y \neq 0$. Thật vậy, nếu $x = 0$ thì $sp_{k+1} = rq_{k+1}$. Vì $(p_{k+1}, q_{k+1}) = 1$ nên $q_{k+1} \mid s$, suy ra $s \geq q_{k+1}$ : mâu thuẫn. Nếu $y = 0$ thì $r = p_k x$, $s = q_k x$, nên

$$|s\alpha - r| = |x||q_k\alpha - p_k| \geq |q_k\alpha - p_k|,$$

vì $|x| \geq 1$, mâu thuẫn.

Bây giờ ta chỉ ra rằng $x$ và $y$ có dấu ngược nhau. Trước hết, giả sử $y < 0$. Do $q_k x = s - q_{k+1}y$ nên $x > 0$, vì $q_k x > 0$ và $q_k > 0$. Khi $y > 0$, do $q_{k+1}y \geq q_{k+1} > s$ nên $q_k x = s - q_{k+1}y < 0$, suy ra $x < 0$.

Do Định lí 4.15, hoặc ta có $\dfrac{p_k}{q_k} < \alpha < \dfrac{p_{k+1}}{q_{k+1}}$, hoặc $\dfrac{p_{k+1}}{q_{k+1}} < \alpha < \dfrac{p_k}{q_k}$ (tùy thuộc tính chẵn lẻ của $k$). Trong cả hai trường hợp, $q_k\alpha - p_k$ và $q_{k+1}\alpha - p_{k+1}$ có dấu ngược nhau. Từ hệ phương trình đang xét ta có

$$|s\alpha - r| = \left|(q_k x + q_{k+1} y)\alpha - (p_k x + p_{k+1} y)\right|$$
$$= \left|x(q_k\alpha - p_k) + y(q_{k+1}\alpha - p_{k+1})\right|.$$

Do $x(p_k\alpha - p_k)$ và $y(q_{k+1}\alpha - p_{k+1})$ có cùng dấu nên

$$|s\alpha - r| = |x|\left|q_k\alpha - p_k\right| + |y|\left|q_{k+1}\alpha - p_{k+1}\right|$$
$$\geq |x|\left|q_k\alpha - p_k\right|$$
$$\geq \left|q_k\alpha - p_k\right|$$

do $|x| \geq 1$. Bất đẳng thức $|s\alpha - r| \geq \left|q_k\alpha - p_k\right|$ trái giả thiết. Định lí được chứng minh. □

**Hệ quả 4.20.** *Giả sử $\alpha$ là số vô tỉ, $\frac{p_j}{q_j}$, $j = 1,2,...$ là các hội tụ của phân số liên tục đơn vô hạn $\alpha$. Nếu $\frac{r}{s}$ là số hữu tỉ, trong đó $r$, $s$ nguyên, $s > 0$ và*

$$\left|\alpha - \frac{r}{s}\right| < \left|\alpha - \frac{p_k}{q_k}\right|$$

*thì $s > q_k$.*

***Chứng minh.*** Giả sử $s \leq q_k$ và

$$\left|\alpha - \frac{r}{s}\right| < \left|\alpha - \frac{p_k}{q_k}\right|.$$

Ta có

$$s\left|\alpha - \frac{r}{s}\right| < q_k\left|\alpha - \frac{p_k}{q_k}\right|,$$

nên

$$|s\alpha - r| < \left|q_k\alpha - p_k\right|,$$

mâu thuẫn Định lí 4.19. □

***Ví dụ :*** Phân số liên tục đơn của $\pi$ là

$$\pi = [3\ ;\ 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, ...].$$

Từ đó suy ra các số hữu tỉ xấp xỉ tốt nhất của số $\pi$ là :

$$3, \frac{22}{7}, \frac{333}{106}, \frac{335}{113}, \frac{103993}{33102}, \ldots$$

Định lí sau đây chỉ ra rằng, một số hữu tỉ xấp xỉ đủ tốt một số vô tỉ $\alpha$ phải là một hội tụ của phân số liên tục đơn vô hạn của $\alpha$.

**Định lí 4.21.** *Giả sử $\alpha$ là một số vô tỉ, $\frac{r}{s}$ là số hữu tỉ (dạng tối giản), trong đó $r$, $s$ nguyên, $s > 0$, sao cho*

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2}.$$

*Khi đó $\frac{r}{s}$ là một hội tụ của phân số liên tục đơn của $\alpha$.*

***Chứng minh.*** Giả sử $\frac{r}{s}$ không phải là một hội tụ của phân số liên tục đơn của $\alpha$. Khi đó tồn tại các hội tụ liên tiếp $\frac{p_k}{q_k}$ và $\frac{p_{k+1}}{q_{k+1}}$ sao cho $q_k \le s < q_{k+1}$. Từ Định lí 4.19 ta có

$$|q_k\alpha - p_k| \le |s\alpha - r| = s\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s}.$$

Từ đó

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{2sq_k}.$$

Vì $|sp_k - rq_k| \ge 1$ (là số nguyên khác $0$, vì $\frac{r}{s} \ne \frac{p_k}{q_k}$) nên

$$\begin{aligned}\frac{1}{sq_k} &\le \frac{|sp_k - rq_k|}{sq_k}\\ &= \left|\frac{p_k}{q_k} - \frac{r}{s}\right|\\ &\le \left|\alpha - \frac{p_k}{q_k}\right| + \left|\alpha - \frac{r}{s}\right|\\ &< \frac{1}{2sq_k} + \frac{1}{2s^2}.\end{aligned}$$

Vậy

$$\frac{1}{2sq_k} < \frac{1}{2s^2}.$$

tức là $2sq_k > 2s^2$, suy ra $q_k > s$ : mâu thuẫn.

## § 4. PHÂN SỐ LIÊN TỤC TUẦN HOÀN

**Định nghĩa 4.22.** Một phân số liên tục đơn vô hạn $[a_0 ; a_1, a_2, ...]$ được gọi là *tuần hoàn* nếu tồn tại các số nguyên dương $N$ và $k$ sao cho $a_n = a_{n+k}$ với mọi số nguyên dương $n \geq N$.

Để viết một phân số liên tục tuần hoàn như mô tả trong Định nghĩa trên, ta dùng kí hiệu

$$[a_0 ; a_1, a_2, \dots, a_{N-1}, \overline{a_N, a_{N+1}, \dots, a_{N+k-1}}].$$

Ví dụ : $[2 ; 4, 11, \overline{1, 9, 4, 6}]$ là phân số $[2 ; 4, 11, 1, 9, 4, 6, 1, 9, ...]$. Sau đây, ta sẽ tìm những tiêu chuẩn đặc trưng của một phân số liên tục vô hạn tuần hoàn.

**Định nghĩa 4.23.** Số thực $\alpha$ được gọi là *vô tỉ bậc hai* nếu $\alpha$ là vô tỉ và $\alpha$ là nghiệm của phương trình bậc hai với hệ số nguyên, tức là

$$A\alpha^2 + B\alpha + C = 0,$$

trong đó $A$, $B$, $C$ là các số nguyên.

**Bổ đề 4.24.** *Số thực $\alpha$ là số vô tỉ bậc hai nếu và chỉ nếu tồn tại các số nguyên $a$, $b$, $c$ với $b > 0$, $c \neq 0$ sao cho $b$ không chính phương và*

$$\alpha = \frac{a + \sqrt{b}}{c}.$$

***Chứng minh.*** Nếu $\alpha$ là số vô tỉ bậc hai thì $\alpha$ là nghiệm của phương trình $A\alpha^2 + B\alpha + C = 0$ với $A$, $B$, $C$ nguyên nào đó, đồng thời biệt thức của phương trình là số không chính phương. Ta có

$$\alpha = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A},$$

với $B^2 - 4AC > 0$ không chính phương, $A \neq 0$. Như vậy $\alpha$ có dạng phát biểu trong bổ đề.

Ngược lại, nếu

$$\alpha = \frac{a + \sqrt{b}}{c}$$

trong đó $a$, $b$, $c$ nguyên, $c \neq 0$, $b > 0$ không chính phương, thì $\alpha$ sẽ là nghiệm của phương trình

$$c\alpha^2 - 2ac\alpha + (a^2 - b^2) = 0.$$

Mặt khác, $\alpha$ là số vô tỉ nên nó là số vô tỉ bậc hai. □

**Bổ đề 4.25.** *Nếu $\alpha$ là số vô tỉ bậc hai, $r$, $s$, $t$, $u$ là các số nguyên, thì $\dfrac{r\alpha + s}{t\alpha + u}$ hoặc là số hữu tỉ, hoặc là số vô tỉ bậc hai.*

***Chứng minh.*** Theo Bổ đề 4.24 tồn tại các số nguyên $a$, $b$, $c$, với $c \neq 0$, $b > 0$ không chính phương sao cho

$$\alpha = \frac{a + \sqrt{b}}{c}.$$

Ta có

$$\begin{aligned}
\frac{r\alpha + s}{t\alpha + u} &= \frac{\left[\dfrac{r\left(a + \sqrt{b}\right)}{c} + s\right]}{\left[\dfrac{t\left(a + \sqrt{b}\right)}{c} + u\right]} \\
&= \frac{(ar + cs) + r\sqrt{b}}{(at + cu) + t\sqrt{b}} \\
&= \frac{\left[(ar + cs) + r\sqrt{b}\right]\left[(at + cu) - t\sqrt{b}\right]}{\left[(at + cu) + t\sqrt{b}\right]\left[(at + cu) - t\sqrt{b}\right]} \\
&= \frac{\left[(ar + cs)(at + cu) - rtb\right] + \left[r(at + cu) - t(ar + cs)\right]\sqrt{b}}{(at + cu)^2 - t^2 b}.
\end{aligned}$$

Như vậy, $\dfrac{r\alpha + s}{t\alpha + u}$ là số hữu tỉ nếu hệ số của $\sqrt{b}$ trong biểu thức bằng $0$, và là số vô tỉ bậc hai trong trường hợp ngược lại.

Đối với số vô tỉ bậc hai, ta có khái niệm số vô tỉ bậc hai liên hợp.

**Định nghĩa 4.26.** Giả sử $\alpha = \dfrac{a + \sqrt{b}}{c}$ là một số vô tỉ bậc hai. Khi đó, liên

hợp của số $\alpha$, kí hiệu qua $\alpha'$, được định nghĩa bởi công thức

$$\alpha = \frac{a - \sqrt{b}}{c}.$$

**Bổ đề 4.27.** *Nếu số vô tỉ bậc hai $\alpha$ là nghiệm của đa thức $Ax^2 + Bx + C = 0$, thì nghiệm của đa thức là số liên hợp $\alpha'$.*

***Chứng minh.*** Ta có hai nghiệm của đa thức là

$$\frac{-B \pm \sqrt{B^2 - 4AC}}{2A}.$$

Nếu $\alpha$ là một trong hai nghiệm thì $\alpha'$ là nghiệm kia. □

**Bổ đề 4.28.** *Giả sử $\alpha_1 = \dfrac{a_1 + b_1\sqrt{d}}{c_1}$, $\alpha_2 = \dfrac{a_2 + b_2\sqrt{d}}{c_2}$ là các số vô tỉ bậc hai. Khi đó*

1) $(\alpha_1 + \alpha_2)' = \alpha_1' + \alpha_2'$;

2) $(\alpha_1 - \alpha_2)' = \alpha_1' - \alpha_2'$;

3) $(\alpha_1\alpha_2)' = \alpha_1'\alpha_2'$;

4) $\left(\dfrac{\alpha_1}{\alpha_2}\right)' = \dfrac{\alpha_1'}{\alpha_2'}$.

***Chứng minh.*** Chứng minh các đẳng thức trên không khó. Ta trình bày chi tiết, chẳng hạn, chứng minh của đẳng thức 4). Ta có

$$\left(\frac{\alpha_1}{\alpha_2}\right)' = \frac{\left(a_1 + b_1\sqrt{d}\right)/c_1}{\left(a_2 + b_2\sqrt{d}\right)/c_2} = \frac{c_2\left(a_1 + b_1\sqrt{d}\right)\left(a_2 - b_2\sqrt{d}\right)}{c_1\left(a_2 + b_2\sqrt{d}\right)\left(a_2 - b_2\sqrt{d}\right)}$$
$$= \frac{\left(c_2a_1a_2 - c_2b_1b_2d\right) + \left(c_2a_2b_1 - c_2a_1b_2\right)\sqrt{d}}{c_1\left(a_2^2 - b_2^2d\right)}.$$

Mặt khác,

$$\frac{\alpha_1'}{\alpha_2'} = \frac{\left(a_1 - b_1\sqrt{d}\right)/c_1}{\left(a_2 - b_2\sqrt{d}\right)/c_2} = \frac{c_2\left(a_1 - b_1\sqrt{d}\right)\left(a_2 + b_2\sqrt{d}\right)}{c_1\left(a_2 - b_2\sqrt{d}\right)\left(a_2 + b_2\sqrt{d}\right)}$$

$$= \frac{(c_2a_1a_2 - c_2b_1b_2d) - (c_2a_2b_1 - c_2a_1b_2)\sqrt{d}}{c_1\left(a_2^2 - b_2^2d\right)}.$$

Vậy $\left(\frac{\alpha_1'}{\alpha_2'}\right) = \frac{\alpha_1'}{\alpha_2'}$. □

Bây giờ ta sẽ chứng minh một tính chất đặc trưng của số vô tỉ bậc hai.

**Định lí Lagrange.** *Phân số liên tục đơn vô hạn của một số vô tỉ là tuần hoàn nếu và chỉ nếu số đó là số vô tỉ bậc hai.*

***Chứng minh.*** Trước tiên, giả sử phân số liên tục đơn của số vô tỉ $\alpha$ là tuần hoàn :

$$\alpha = [a_0\ ;\ a_1, a_2, \ldots, a_{N-1},\ \overline{a_N, a_{N+1}, \ldots, a_{N+k}}].$$

Đặt

$$\beta = [\overline{a_N\ ;\ a_{N+1}, \ldots, a_{N+k}}]$$

Khi đó

$$\beta = [a_N\ ;\ a_{N+1}, \ldots, a_{N+k}, \beta].$$

Từ đó ta có

$$\beta = \frac{\beta p_k + p_{k-1}}{\beta q_k + q_{k-1}} \tag{1}$$

trong đó $\frac{p_k}{q_k}$ và $\frac{p_{k-1}}{q_{k-1}}$ là các hội tụ của $[a_N\ ;\ q_{N+1}, \ldots, a_{N+k}]$. Vì phân số liên tục đơn của $\beta$ là vô hạn nên $\beta$ là số vô tỉ và từ (1) ta có

$$q_k\beta^2 + (q_{k-1} - p_k)\beta - p_{k-1} = 0.$$

Như vậy, $\beta$ là số vô tỉ bậc hai. Mặt khác,

$$\alpha = [a_0\ ;\ a_1, \ldots,\ a_{N-1},\ \beta]$$

nên

$$\alpha = \frac{\beta p_{N-1} + p_{N-2}}{\beta q_{N-1} + q_{N-2}},$$

trong đó $\frac{p_{N-1}}{q_{N-1}}$ và $\frac{p_{N-2}}{q_{N-2}}$ là các hội tụ của $[a_0\ ;\ a_1,\ a_2, \ldots,\ a_{N-1}]$. Do $\beta$ là số vô tỉ bậc hai nên $\alpha$ là số vô tỉ bậc hai (theo Bổ đề 4.25 và vì $\alpha$ là số vô tỉ).

Trước khi chứng minh phần ngược lại, ta có một số Bổ đề sau.

**Bổ đề 4.29.** *Giả sử $\alpha$ là số vô tỉ bậc hai. Khi đó $\alpha$ có thể viết dưới dạng*

$$\alpha = \frac{P + \sqrt{D}}{Q},$$

*trong đó $P$, $Q$ và $D$ là các số nguyên, $Q \neq 0$, $D > 0$ không chính phương và $Q \mid (D - P^2)$.*

***Chứng minh.*** Do $\alpha$ là số vô tỉ bậc hai nên

$$\alpha = \frac{a + \sqrt{b}}{c},$$

trong đó $a$, $b$, $c$ nguyên, $b > 0$, $c \neq 0$. Từ đó ta có

$$\alpha = \frac{a|c| + \sqrt{bc^2}}{c|c|},$$

Đặt $P = a|c|$, $Q = c|c|$, $D = bc^2$, ta có dạng biểu diễn cần tìm.

**Bổ đề 4.30.** *Giả sử $\alpha$ là số hữu tỉ bậc hai, biểu diễn dưới dạng*

$$\alpha = \frac{P_0 + \sqrt{D}}{Q_0},$$

*trong đó $Q_0 \neq 0$, $D > 0$ không chính phương, $Q_0 \mid (D - P_0^2)$. Xác định các số*

$$\alpha_k = \frac{P_k + \sqrt{D}}{Q_k},$$

$$\alpha_k = [a_k],$$

$$P_{k+1} = a_k Q_k - P_k,$$

$$Q_{k+1} = \frac{(D - P_{k+1}^2)}{Q_k},$$

*với $k = 0,\ 1,\ 2, \ldots$ Khi đó ta có*

$$\alpha = [a_0\ ;\ a_1,\ a_2, \ldots].$$

***Chứng minh.*** Bằng quy nạp, ta sẽ chứng tỏ rằng, $P_k$, $Q_k$ là các số nguyên

thỏa mãn điều kiện $Q_k \neq 0$, $Q_k \mid (D - P_k^2)$ với $k = 0,\ 1,\ 2, \ldots$ Từ giả thiết suy ra khẳng định đúng với $k = 0$. Giả sử khẳng định đúng với $k$. Khi đó

$$P_{k+1} = a_k Q_k - P_k$$

cũng là số nguyên. Hơn nữa,

$$\begin{aligned} Q_{k+1} &= \frac{D - P_{k+1}^2}{Q_k} \\ &= \frac{D - (a_k Q_k - P_k)^2}{Q_k} \\ &= \frac{D - P_k^2}{Q_k} + 2a_k P_k - a_k^2 Q_k \end{aligned}$$

Do $Q_k \mid (D - P_k^2)$ theo giả thiết quy nạp nên $Q_{k+1}$ là số nguyên. Hơn nữa, do $D$ không chính phương nên $D \neq P_k^2$, suy ra $Q_{k+1} = \dfrac{D - P_{k+1}^2}{Q_k} \neq 0$. Vì

$$Q_k = \frac{(D - P_{k+1}^2)}{Q_{k+1}}$$

nên suy ra $Q_{k+1} \mid (D - P_{k+1}^2)$.

Để chứng tỏ các số nguyên $a_0,\ a_1,\ a_2, \ldots$ là các thương riêng của phân số liên tục đơn của $\alpha$, ta dùng Định lí 4.17. Nếu ta chỉ ra rằng

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k},$$

$k = 0,\ 1,\ 2, \ldots$ thì ta thấy rằng $\alpha = [a_0\ ;\ a_1,\ a_2, \ldots]$. Nhận xét

$$\begin{aligned} \alpha_k - a_k &= \frac{P_k + \sqrt{D}}{Q_k} - a_k = \frac{\sqrt{D} - (a_k Q_k - P_k)}{Q_k} = \frac{\sqrt{D} - P_{k+1}}{Q_k} \\ &= \frac{(\sqrt{D} - P_{k+1})(\sqrt{D} + P_{k+1})}{Q_k(\sqrt{D} + P_{k+1})} = \frac{D - P_{k+1}^2}{Q_k(\sqrt{D} + P_{k+1})} \\ &= \frac{Q_k Q_{k+1}}{Q_k(\sqrt{D} + P_{k+1})} = \frac{Q_{k+1}}{\sqrt{D} + P_{k+1}} = \frac{1}{\alpha_{k+1}}. \end{aligned}$$

Vậy, $\alpha = [a_0\ ;\ a_1,\ a_2, ...]$.

Bây giờ ta sẽ kết thúc chứng minh Định lí Lagrange.

Giả sử $\alpha$ là số vô tỉ bậc hai. Khi đó ta có thể viết $\alpha$ dưới dạng

$$\alpha = \frac{P_0 + \sqrt{D}}{Q_0}.$$

Hơn nữa ta có $\alpha = [a_0\ ;\ a_1,\ a_2, ...]$., trong đó

$$\alpha_k = \frac{P_k + \sqrt{D}}{Q_k},$$

$$a_k = [\alpha_k],$$

$$P_{k+1} = a_k Q_k - P_{k+1},$$

$$Q_{k+1} = \frac{D - P_{k+1}^2}{Q_{k+1}},$$

với $k = 0,\ 1,\ 2, ...$

Vì $\alpha = [a_0\ ;\ a_1,\ a_2, ..., a_k]$ nên

$$\alpha = \frac{p_{k-1}\alpha_k + p_{k-2}}{q_{k-1}\alpha_k + q_{k-2}}.$$

Lấy liên hợp hai vế, sử dụng Bổ đề 4.28 ta có

$$\alpha' = \frac{p_{k-1}\alpha_k' + p_{k-2}}{q_{k-1}\alpha_k' + q_{k-2}}.$$

Từ đó ta có :

$$\alpha_k' = \frac{-q_{k-2}}{q_{k-1}} \left( \frac{\alpha' - \dfrac{p_{k-2}}{q_{k-2}}}{\alpha' - \dfrac{p_{k-1}}{q_{k-1}}} \right).$$

Chú ý rằng các hội tụ $\dfrac{p_{k-2}}{q_{k-2}}$ và $\dfrac{p_{k-1}}{q_{k-1}}$ dần đến $\alpha$ khi $k$ dần đến $\infty$, nên

$$\frac{\alpha' - \dfrac{p_{k-2}}{q_{k-2}}}{\alpha' - \dfrac{p_{k-1}}{q_{k-1}}}$$

dần đến 1. Như vậy, tồn tại số nguyên $N$ sao cho $\alpha'_k < 0$ với $k \geq N$. Vì $\alpha_k > 0$ với $k \geq 1$ nên

$$\alpha_k - \alpha'_k = \frac{P_k + \sqrt{D}}{Q_k} - \frac{P_k - \sqrt{D}}{Q_k} = \frac{2\sqrt{D}}{Q_k} > 0,$$

nên $Q_k > 0$ với $k \geq N$.

Vì $Q_k Q_{k+1} = D - P_{k+1}^2$ nên với $k \geq N$ ta có

$$Q_k \leq Q_k Q_{k+1} = D - P_{k+1}^2 \leq D.$$

Cũng với $k \geq N$ ta có

$$P_{k+1}^2 \leq D = P_{k+1}^2 - Q_k Q_{k+1},$$

nên

$$-\sqrt{D} < P_{k+1} < \sqrt{D}.$$

Từ các bất đẳng thức $0 \leq Q_k \leq D$, $-\sqrt{D} < P_{k+1} < \sqrt{D}$ (đúng với $k \geq N$) ta thấy tồn tại chỉ hữu hạn giá trị dương của cặp số nguyên $P_k$, $Q_k$ với $k > N$. Do có vô hạn số nguyên $k \geq N$ nên tồn tại $i$, $j$ sao cho $P_j = P_i$, $Q_j = Q_i$, với $i < j$. Từ các quan hệ xác định $\alpha_k$ ta thấy $\alpha_i = \alpha_j$. Vậy $\alpha_i = \alpha_j$, $a_{i+1} = a_{j+1}$, $a_{i+2} = a_{j+2}$, ... Do đó

$$\alpha = [a_0 ;\ a_1,\ a_2, \ldots,\ a_{i-1},\ a_i,\ a_{i+1}, \ldots,\ a_{j-1},\ a_i,\ a_{i+1}, \ldots,\ a_{j-1}]$$

$$= [a_0 ;\ a_1,\ a_2, \ldots,\ a_{i-1},\ a_i,\ a_{j+1}, \ldots,\ a_{j-1}].$$

Điều đó có nghĩa là, $\alpha$ là phân số liên tục đơn tuần hoàn. □

## BÀI TẬP CHƯƠNG 4

1. Chứng minh rằng nếu $p$ là số nguyên tố, $b$ là số nguyên dương và không là lũy thừa của $p$ thì $\log_p b$ là số vô tỉ.

2. Giả sử $b$ là số nguyên dương, $b > 1$. Chứng minh rằng

$$\frac{1}{b}+\frac{1}{b^4}+\frac{1}{b^9}+\frac{1}{b^{16}}+\cdots$$

là số vô tỉ.

**3.** Chứng minh rằng mỗi số thực có thể viết dưới dạng

$$c_0+\frac{c_1}{1!}+\frac{c_2}{2!}+\frac{c_3}{3!}+\cdots$$

trong đó $c_j$ là các số nguyên, $0 \le c_j < j,\ j = 1,\ 2,\ 3, \ldots$

**4.** Giả sử $n$ là số nguyên dương, $n > 1$. Chứng minh rằng

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$$

không phải là số nguyên.

**5.** Giả sử số hữu tỉ $a > 1$ có khai triển phân số liên tục đơn là $[a_1\ ;\ a_1, \ldots,\ a_k]$. Tìm khai triển phân số liên tục đơn của $\frac{1}{a}$.

**6.** Chứng minh rằng, nếu $a_0 \neq 0$ thì

$$\frac{p_k}{p_{k-1}} = [a_k\ ;\ a_{k-1}, \ldots,\ a_1,\ a_0]$$

$$\frac{q_k}{q_{k-1}} = [a_k\ ;\ a_{k-1}, \ldots,\ a_2,\ a_1]$$

trong đó $c_{k-1} = \frac{p_{k-1}}{q_{k-1}},\ c_k = \frac{p_k}{q_k},\ k \ge 1$ là các hội tụ liên tiếp của phân số liên tục $[a_0\ ;\ a_1, \ldots,\ a_n]$.

**7.** Chứng minh rằng mỗi số hữu tỉ có đúng hai khai triển phân số liên tục đơn.

**8.** Giả sử $[a_0\ ;\ a_1, \ldots,\ a_n]$ là khai triển phân số liên tục đơn của $\frac{r}{s}$, $(r, s) = 1$ và $r \ge 1$. Chứng minh rằng phân số liên tục này là đối xứng, tức là $a_0 = a_n,\ a_1 = a_{n-1}, \ldots$ nếu và chỉ nếu $s \mid (r^2+1)$ khi $n$ lẻ và $s \mid (r^2-1)$ khi $n$ chẵn.

**9.** Giả sử $a_0,\ a_1, \ldots,\ a_k$ là các số thực. $a_1,\ a_2, \ldots,\ a_k$ dương. Giả sử $x$

là số thực dương. Chứng minh rằng

$$[a_0\ ;\ a_1, \ldots,\ a_k] < [a_0\ ;\ a_1, \ldots,\ a_k + x] \text{ nếu } k \text{ lẻ}$$

và

$$[a_0\ ;\ a_1, \ldots,\ a_k] > [a_0\ ;\ a_1, \ldots,\ a_k + x] \text{ nếu } k \text{ chẵn.}$$

**10.** Tìm phân số liên tục của $\sqrt{5}$, $\dfrac{1+\sqrt{5}}{2}$.

**11.** Biết phân số liên tục đơn của $e$ là

$$e = [2\ ;\ 1,\ 2,\ 1,\ 1,\ 4,\ 1,\ 1,\ 6,\ 1,\ 1,\ 8, \ldots]$$

a) Tìm 8 hội tụ của phân số liên tục của $e$.

b) Tìm xấp xỉ hữu tỉ tốt nhất của $e$ có mẫu số nhỏ hơn 100.

**12.** Giả sử $\alpha$ là số vô tỉ với khai triển phân số liên tục đơn : $\alpha = [a_0\ ;\ a_1,\ a_2, \ldots]$. Chứng minh rằng khai triển phân số liên tục đơn của $-\alpha$ là $[-a_0 - 1\ ;\ a_1 - 1,\ a_2,\ a_3, \ldots]$ nếu $a_1 > 1$, là $[-a_0 - 1\ ;\ a_2 + 1,\ a_3, \ldots]$ nếu $a_1 = 1$.

**13.** Chứng minh rằng nếu $\dfrac{p_k}{q_k}$ và $\dfrac{p_{k+1}}{q_{k+1}}$ là các hội tụ liên tiếp của phân số liên tục đơn của số vô tỉ $\alpha$ thì

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{2q_k^2},$$

hoặc

$$\left|\alpha - \frac{p_{k+1}}{q_{k+1}}\right| < \frac{1}{2q_{k+1}^2}.$$

**14.** Giả sử $\alpha$ là số vô tỉ, $\dfrac{p_k}{q_k}$ là hội tụ thứ $k$ của phân số liên tục đơn của $\alpha$. Chứng minh rằng có ít nhất một trong ba hội tụ liên tiếp thỏa mãn bất đẳng thức

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{\sqrt{5}q_k^2}.$$

Từ đó suy ra tồn tại vô hạn số hữu tỉ $\dfrac{p}{q}$ với $p$, $q$ nguyên, $q \neq 0$ sao cho

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$$

**15.** Tìm khai triển phân số liên tục của các số :

a) $\sqrt{7}$ ; b) $\sqrt{11}$ ;

c) $\sqrt{23}$ ; d) $\sqrt{47}$ .

**16.** Tìm các số vô tỉ có các khai triển phân số liên tục đơn sau đây :

a) $[2\,;1,\overline{5}]$ ; b) $[2\,;\overline{1,5}]$ ;

c) $\overline{[2\,;1,5]}$ .

**17.** a) Giả sử $d$ là số nguyên dương. Chứng minh rằng phân số liên tục đơn của $\sqrt{d^2+1}$ là $[d\,;\overline{2d}]$.

b) Tìm phân số liên tục đơn của $\sqrt{101}$, $\sqrt{290}$, $\sqrt{2210}$.

**18.** Giả sử $d$ nguyên, $d \geq 2$.

a) Chứng minh rằng phân số liên tục đơn của $\sqrt{d^2-1}$ là $[1\,;\overline{2d-2}]$.

b) Chứng minh rằng phân số liên tục đơn của $\sqrt{d^2-d}$ là $[d-1\,;\overline{2,2d-2}]$.

c) Tìm phân số liên tục đơn của $\sqrt{99}$, $\sqrt{110}$, $\sqrt{272}$, $\sqrt{600}$.

**19.** a) Giả sử $d$ nguyên, $d \geq 3$. Chứng minh rằng phân số liên tục đơn của $\sqrt{d^2-2}$ là $[d-1\,;\overline{1,d-2,2d-2}]$.

b) Chứng minh rằng nếu $d$ nguyên dương thì phân số liên tục đơn của $\sqrt{d^2+2}$ là $[d\,;\overline{d,2d}]$.

c) Tìm phân số liên tục đơn của $\sqrt{47}$, $\sqrt{51}$, $\sqrt{187}$.

**20.** Giả sử $d$ nguyên dương lẻ. Chứng minh rằng :

a) Phân số liên tục đơn của $\sqrt{d^2+4}$ là

$$\left[d\,;\overline{\frac{d-1}{2},1,1,\frac{d-1}{2},2d}\right]$$

nếu $d > 1$.

b) Phân số liên tục đơn của $\sqrt{d^2 - 4}$ là

$$\left[d - 1\,;\, \overline{\frac{d-3}{2},\, 2,\, \frac{d-3}{2},\, 1,\, 2d-2}\right]$$

nếu $d > 3$.

**21.** Chứng minh rằng nếu $d$ là số nguyên dương thì phân số liên tục đơn của $\sqrt{d}$ có độ dài chu kì bằng $2$ nếu và chỉ nếu $d = a^2 + b$, trong đó $a$, $b$ nguyên, $b > 1$, $b \mid 2a$.

**22.** Với mọi số nguyên dương $k$, chứng minh rằng tồn tại vô hạn số nguyên dương $D$ sao cho khai triển phân số liên tục của $\sqrt{D}$ có chu kì độ dài $k$.

Chương 5.

# PHƯƠNG TRÌNH NGHIỆM NGUYÊN

## § 1. PHƯƠNG TRÌNH TUYẾN TÍNH

Sách "Đại thành toán pháp" của Lương Thế Vinh đã có hướng dẫn giải bài toán sau đây:

Một trăm con trâu
Một trăm bó cỏ
Trâu đứng ăn năm
Trâu nằm ăn ba
Trâu già ba con một bó.
Hỏi mỗi loại trâu có mấy con ?

Theo ngôn ngữ toán học bây giờ, ta có thể giải bài toán trên đây như sau. Gọi $x$ là số trâu đứng, $y$ là số trâu nằm và $z$ là số trâu già (theo quy ước của bài toán, trâu già không đứng, mà cũng không nằm !). Theo bài ra ta có :

$$\begin{cases} x + y + z = 100 \\ 5x + 3y + \dfrac{z}{3} = 100 \end{cases}$$

Nhân hai vế của phương trình với 3 rồi trừ từng vế cho phương trình thứ nhất, ta được :

$$14x + 8y = 200. \tag{1}$$

Phương trình thu được có hai ẩn $x$, $y$. Vì $x$, $y$ là "số trâu" nên rõ ràng $x$, $y$ phải nhận các giá trị nguyên không âm. Như vậy, phương trình (1) thuộc vào lớp phương trình Điôphăng tuyến tính.

**Định nghĩa 5.1.** *Phương trình Điôphăng tuyến tính* là phương trình có dạng

$$ax + by = c, \tag{2}$$

trong đó $a$, $b$, $c$ là các số nguyên, đồng thời các biến $x$, $y$ cũng chỉ nhận các giá trị nguyên.

Giải phương trình Điôphăng (2) tức là tìm các cặp số nguyên $(x, y)$ thỏa mãn (2).

Định lí sau đây trả lời câu hỏi khi nào thì phương trình Điôphăng tuyến tính có nghiệm, đồng thời chỉ ra các nghiệm khi chúng tồn tại.

**Định lí 5.2.** *Giả sử $a$, $b$ là các số nguyên dương, $d$ là ước chung lớn nhất của $a$ và $b$, $d = (a, b)$. Khi đó phương trình $ax + by = c$ không có nghiệm nguyên nếu $d \nmid c$. Nếu $d \mid c$ thì phương trình có vô số nghiệm. Hơn nữa, nếu $x = x_0$, $y = y_0$ là một nghiệm nào đó của phương trình, thì mọi nghiệm của phương trình có dạng :*

$$x = x_0 + \left(\frac{b}{d}\right)n, \quad y = y_0 + \left(\frac{a}{d}\right)n,$$

*trong đó $n$ là số nguyên.*

***Chứng minh.*** Giả sử $(x, y)$ là một nghiệm của phương trình. Do $d \mid a$, $d \mid b$ nên $d \mid c$. Như vậy, nếu $d \nmid c$ thì phương trình không có nghiệm nguyên.

Bây giờ giả sử $d \mid c$. Khi đó, tồn tại các số nguyên $s$, $t$ sao cho

$$d = as + bt \tag{3}$$

Do $d \mid c$ nên tồn tại $e$ nguyên sao cho $de = c$. Nhân hai vế của (3) với $e$ ta được :

$$c = de = (as + bt)e = a(se) + b(te).$$

Như vậy, ta có một nghiệm của phương trình cho bởi $x = x_0 = se$, $y = y_0 = te$.

Ta sẽ chứng tỏ tồn tại vô số nghiệm. Đặt $x = x_0 + \dfrac{b}{d}n$, $y = y_0 - \dfrac{a}{d}n$, trong đó $n$ nguyên. Ta thấy cặp $(x, y)$ xác định như trên là một nghiệm, vì

$$ax + by = ax_0 + a \cdot \frac{b}{d}n + by_0 - b \cdot \frac{a}{d}n = ax_0 + by_0 = c.$$

Chỉ còn phải chứng tỏ rằng, mọi nghiệm của phương trình phải có dạng nêu

trên. Giả sử $(x, y)$ là một nghiệm tùy ý, tức là $x.y$ nguyên và thỏa mãn $ax + by = c$. Khi đó

$$(ax + by) - (ax_0 + by_0) = 0,$$

suy ra

$$a(x - x_0) + b(y - y_0) = 0.$$

Tức là

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

Chia hai vế của đẳng thức cho $d$, ta được

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) \tag{4}$$

Do $d = (a, b)$ nên $\frac{a}{d}$ và $\frac{b}{d}$ nguyên tố cùng nhau. Từ đó suy ra $y_0 - y : \frac{a}{d}$, tức là tồn tại $n$ nguyên sao cho $\frac{a}{d}n = y_0 - y$. Suy ra $y = y_0 - \frac{a}{d}n$. Thay giá trị này của $y$ vào phương trình (4) ta được $x = x_0 + \frac{b}{d}n$. □

Định lí trên đây cho phương pháp giải phương trình Điôphăng tuyến tính. Ví dụ xét phương trình (1)

$$14x + 8y = 200.$$

Ta có $(14, 8) = 2$. Do $2 \mid 200$ nên phương trình có nghiệm. Dễ thấy $2 = 14.(-1) + 8.(+2)$. Nhân hai vế với 100 ta có :

$$14.(-100) + 8.(200) = 200.$$

Như vậy, ta được nghiệm $x_0 = -100$, $y_0 = 200$. Theo Định lí 4.2, các nghiệm của phương trình có dạng :

$$x = -100 + 4n, \qquad y = 200 - 7n.$$

Do $x \geq 0$ nên $n \geq 25$. Do $y \geq 0$ nên $n \leq \frac{200}{7}$, suy ra $n \leq 28$. Vậy $n$ chỉ có thể nhận các giá trị 25, 26, 27, 28. Tương ứng ta có các nghiệm (0, 25), (4, 18), (8, 11), (12, 4). Các nghiệm $(x, y, z)$ của bài toán ban đầu là (0, 25, 75), (4, 18, 78), (8, 11, 81), (12, 4, 84).

## § 2. PHƯƠNG TRÌNH FERMAT

### 2.1. CÁC BỘ SỐ PITAGO

Bộ ba số nguyên dương $(x, y, z)$ thỏa mãn

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

được gọi là một *bộ số Pitago*. Tên gọi đó xuất phát từ Định lí Pitago quen thuộc : bình phương độ dài cạnh huyền một tam giác vuông bằng tổng bình phương các cạnh góc vuông. Như vậy, một bộ ba số nguyên dương $(x, y, z)$ là một bộ số Pitago khi và chỉ khi tồn tại tam giác vuông có số đo các cạnh góc vuông là $x$ và $y$, số đo cạnh huyền là $z$. (Chẳng hạn bộ $\{3, 4, 5\}$, $\{6, 8, 10\}$, ...). Rõ ràng rằng, nếu $\{x, y, z\}$ là một bộ số Pitago thì $\{kx, ky, kz\}$ cũng là một bộ số Pitago với mọi số tự nhiên $k$. Do đó, ta chỉ cần xét các bộ ba số nguyên tố cùng nhau.

**Định nghĩa 5.3.** Bộ số Pitago $\{x, y, z\}$ được gọi là *nguyên thủy* nếu $(x, y, z) = 1$.

***Ví dụ :*** Các bộ số $\{3, 4, 5\}$, $\{5, 12, 13\}$ là nguyên thủy, bộ số $\{6, 8, 10\}$ không nguyên thủy.

Nếu bộ số Pitago $\{x, y, z\}$ là không nguyên thủy, chẳng hạn $(x, y, z) = d$, thì $\left\{\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right\}$ là một bộ số Pitago nguyên thủy. Để tìm các bộ số Pitago, ta cần một số Bổ đề sau.

**Bổ đề 5.4.** *Nếu $\{x, y, z\}$ là một bộ số Pitago nguyên thủy thì $(x, y) = (x, z) = (y, z) = 1$.*

***Chứng minh.*** Giả sử $\{x, y, z\}$ là một bộ số Pitago nguyên thủy và $(x, y) > 1$. Khi đó tồn tại số nguyên tố $p$ sao cho $p \mid (x, y)$. Vì $p \mid x$ và $p \mid y$ nên $p \mid (x^2 + y^2) = z^2$. Do $p$ nguyên tố mà $p \mid z^2$ nên $p \mid z$ : mâu thuẫn với giả thiết $(x, y, z) = 1$. Vậy $(x, y) = 1$. Tương tự ta có $(x, z) = (y, z) = 1$. □

**Bổ đề 5.5.** *Giả sử $\{x, y, z\}$ là một bộ số Pitago nguyên thủy. Khi đó $x$ chẵn, $y$ lẻ hoặc $x$ lẻ, $y$ chẵn.*

***Chứng minh.*** Giả sử $\{x, y, z\}$ là một bộ số Pitago nguyên thủy. Do Bổ đề

5.4, $(x, y) = 1$, nên $x$ và $y$ không thể cùng chẵn. Nếu $x$, $y$ cùng lẻ thì ta có

$$x^2 \equiv y^2 \equiv 1 \pmod 4,$$

nên

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4.$$

Điều đó vô lí. Vậy $x$ và $y$ không cùng tính chẵn lẻ. □

**Bổ đề 5.6.** *Giả sử $r$, $s$, $t$ là các số nguyên dương sao cho $(r, s) = 1$ và $rs = t^2$. Khi đó tồn tại các số nguyên $h$ và $l$ sao cho $r = l^2$ và $s = h^2$.*

***Chứng minh.*** Nếu $r = 1$ hoặc $s = 1$ thì Bổ đề là hiển nhiên. Ta giả sử $r > 1$ và $s > 1$. Giả sử các phân tích $r$, $s$, $t$ ra thừa số nguyên tố có dạng sau :

$$r = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

$$s = p_{n+1}^{\alpha_{n+1}} p_{n+2}^{\alpha_{n+2}} \dots p_m^{\alpha_m}$$

$$t = q_1^{\beta_1} q_2^{\beta_2} \dots q_k^{\beta_k}$$

Vì $(r, s) = 1$ nên các số nguyên tố xuất hiện trong các phân tích của $r$ và $s$ là khác nhau. Do $rs = t^2$ nên

$$p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} p_{n+1}^{\alpha_{n+1}} p_{n+2}^{\alpha_{n+2}} \dots p_m^{\alpha_m} = q_1^{2\beta_1} q_2^{2\beta_2} \dots q_k^{2\beta_k}.$$

Từ Định lí cơ bản của Số học ta suy ra rằng, các lũy thừa nguyên tố xuất hiện ở hai vế của đẳng thức phải như nhau. Vậy, mỗi $p_i$ phải bằng một $q_j$ nào đó, đồng thời $\alpha_i = 2\beta_j$. Do đó, mỗi số mũ $\alpha_i$ đều chẵn nên $\dfrac{\alpha_i}{2}$ nguyên. Từ đó suy ra $r = l^2$, $s = h^2$, trong đó $l$, $h$ là các số nguyên :

$$l = p_1^{\alpha_1/2} p_2^{\alpha_2/2} \dots p_n^{\alpha_n/2};$$

$$h = p_{n+1}^{\alpha_{n+1}/2} p_2^{\alpha_{n+2}/2} \dots p_m^{\alpha_m/2}.$$ □

Bây giờ ta có thể mô tả tất cả các bộ số Pitago nguyên thủy.

**Định lí 5.7.** *Các số nguyên dương $x$, $y$, $z$ lập thành một bộ số Pitago nguyên thủy, với $y$ chẵn, nếu và chỉ nếu tồn tại các số nguyên dương nguyên tố cùng nhau $m$, $n$ với $m > n$, $m$ lẻ, $n$ chẵn hoặc $m$ chẵn, $n$ lẻ sao cho*

$$x = m^2 - n^2$$
$$y = 2mn$$

$$z = m^2 + n^2.$$

***Chứng minh.*** Giả sử $x$, $y$, $z$ là một bộ số Pitago nguyên thủy. Bổ đề 5.5 cho thấy $x$ lẻ, $y$ chẵn, hoặc ngược lại. Vì ta đã giả thiết $y$ chẵn nên $x$, $z$ đều lẻ. Do $z+x$ và $z-x$ đều là số chẵn, nên các số $\dfrac{z+x}{2} = r$, $\dfrac{z-x}{2} = s$ đều là số nguyên.

Vì $x^2 + y^2 = z^2$ nên $y^2 = z^2 - x^2 = (z+x)(z-x)$. Vậy

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right) = rs.$$

Để ý rằng $(r,\ s) = 1$. Thật vậy, nếu $(r,\ s) = d$ thì do $d \mid r$, $d \mid s$ nên $d \mid (r+s) = z$ và $d \mid (r-s) = x$. Điều đó có nghĩa là $d \mid (z,\ x) = 1$ nên $d = 1$.

Áp dụng Bổ đề 5.6 ta thấy rằng tồn tại các số nguyên $m$ và $n$ sao cho $r = m^2$, $s = n^2$. Viết $x$, $y$, $z$ thông qua $m$, $n$ ta có

$$xr - s = m^2 - n^2$$

$$y\sqrt{4rs} = \sqrt{4m^2n^2} = 2mn$$

$$zr + s = m^2 + n^2.$$

Ta cũng có $(m,\ n) = 1$, vì mọi ước chung của $m$ và $n$ cũng là ước của $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$, nên là ước chung của $(x,\ y,\ z)$. Mà $x,\ y,\ z$ nguyên tố cùng nhau nên $(m,\ n) = 1$. Mặt khác, $m$ và $n$ không thể cùng lẻ vì nếu ngược lại thì $x$, $y$ và $z$ đều chẵn, mâu thuẫn điều kiện $(x,\ y,\ z) = 1$. Vì $(m,\ n) = 1$ và $m$, $n$ không đồng thời là hai số lẻ nên $m$ chẵn, $n$ lẻ hoặc ngược lại. Vậy mỗi bộ số Pitago nguyên thủy có dạng đã nêu.

Để chứng tỏ rằng bộ ba số

$$x = m^2 - n^2$$

$$y = 2mn$$

$$z = m^2 + n^2$$

trong đó $m$, $n$ là các số nguyên dương, $m > n$, $(m,\ n) = 1$ và $m \not\equiv n \pmod 2$ lập thành một bộ số Pitago nguyên thủy, trước tiên ta nhận xét rằng

$$\begin{aligned} x^2 + y^2 &= (m^2 - n^2)^2 + (2mn)^2 \\ &= (m^4 - 2m^2n^2 + n^4) + 4m^2n^2 \\ &= m^6 + 2m^2n^2 + n^4 \\ &= (m^2 + n^2)^2 \\ &= z^2. \end{aligned}$$

Ta chứng minh $x$, $y$, $z$ nguyên tố cùng nhau. Giả sử ngược lại, $(x, y, z) = d > 1$. Khi đó tồn tại số nguyên tố $p$ sao cho $p \mid (x, y, z)$. Ta thấy rằng $p \nmid 2$ vì $x$ lẻ (do $x = m^2 - n^2$, trong đó $m^2$ và $n^2$ không cùng tính chẵn lẻ). Lại do $p \mid x$, $p \mid z$ nên $p \mid (z + x) = 2m^2$ và $p \mid (z - x) = 2n^2$. Vậy $p \mid m$ và $p \mid n$ : mâu thuẫn với $(m, n) = 1$. Do đó $(x, y, z) = 1$, tức là $\{x, y, z\}$ là một bộ số Pitago nguyên thủy. □

Từ Định lí 5.7 ta có thể thu được các ví dụ về bộ số Pitago nguyên thủy. Chẳng hạn lấy $m = 5$, $n = 2$, ta có $m \not\equiv n \pmod 2$ và $(m, n) = 1$, $m > n$. Theo Định lí 5.7, bộ ba số

$$\begin{aligned} x &= m^2 - n^2 = 5^2 - 2^2 = 21 \\ y &= 2mn = 2.5.2 = 20 \\ z &= m^2 + n^2 = 5^2 + 2^2 = 29 \end{aligned}$$

là một bộ số Pitago nguyên thủy.

## 2.2. PHƯƠNG TRÌNH FERMAT

Ta thấy rằng, phương trình

$$x + y = z$$

có vô hạn nghiệm nguyên $(x, y, z)$. Các bộ số Pitago cũng cho ta vô hạn nghiệm nguyên của phương trình

$$x^2 + y^2 = z^2.$$

Tình hình sẽ như thế nào nếu số mũ của các biến tăng lên ? Nói cách khác, phương trình

$$x^n + y^n = z^n$$

với $n \geq 3$ có nghiệm nguyên hay không ? Nếu có thì số nghiệm là hữu hạn

hay vô hạn ? Chắc hẳn các bạn đọc đều biết rằng, đó chính là một trong những câu hỏi lớn nhất của Toán học, và chỉ mới nhận được câu trả lời trong mấy năm gần đây.

Tất cả đều bắt đầu từ mấy dòng chữ của P. Fermat viết bên lề cuốn "Số học" của Điôphăng, được công bố năm 1635, năm năm sau khi Fermat qua đời : "Không thể viết một lũy thừa bậc ba dưới dạng tổng hai lũy thừa bậc ba, lũy thừa bậc bốn dưới dạng tổng hai lũy thừa bậc bốn, và nói chung, một lũy thừa bậc cao hơn dưới dạng tổng hai lũy thừa cùng bậc. Tôi đã tìm ra một chứng minh kì diệu của sự kiện đó, nhưng tiếc rằng lề sách bé quá để có thể ghi ra".

Có thể phát biểu lại mấy lời của Fermat dưới dạng sau :

**Định lí Fermat.** *Phương trình*

$$x^n + y^n = z^n$$

*không có nghiệm nguyên* $x$, $y$, $z$ *khác* $0$ *khi* $n$ *là số nguyên,* $n \geq 3$.

Định lí Fermat được chứng minh năm 1993 bởi A. Wiles, với việc sử dụng những kiến thức cao nhất của nhiều ngành toán học khác nhau. Trong phần này, chúng ta sẽ chứng minh Định lí lớn Fermat cho trường hợp $n = 4$. Một trong những mấu chốt của chứng minh là phương pháp *quy nạp lùi vô hạn* do Fermat đề xuất

**Định lí 5.8.** *Phương trình*

$$x^4 + y^4 = z^4$$

*không có nghiệm nguyên* $x$, $y$, $z$ *khác* $0$.

***Chứng minh.*** Giả sử phương trình nói trên có nghiệm nguyên $x$, $y$, $z$ khác $0$. Vì ta có thể thay biến tùy ý bởi số đối của nó nên ta có thể xem $x$, $y$, $z$ là các số nguyên dương.

Ta cũng có thể giả thiết $(x, y) = 1$. Thật vậy, nếu $(x, y) = d$ thì $x = dx_1$, $y = dy_1$ với $(x_1, y_1) = 1$, trong đó $x_1$, $y_1$ là các số nguyên dương. Vì $x^4 + y^4 = z^2$ nên

$$(dx_1)^4 + (dy_1)^4 = z^2,$$

do đó

$$d^4(x_1^4 + y_1^4) = z^2.$$

Vậy $d^4 \mid z^2$, suy ra $d^2 \mid z$, nghĩa là $z = d^2 z_1$ với $z_1$ là số nguyên dương. Do đó

$$d^4(x_1^4 + y_1^4) = (d^2 z_1)^2 = d^4 z_1^2,$$

nên

$$x_1^4 + y_1^4 = z_1^2.$$

Ta nhận được nghiệm $x^4 + y^4 = z^2$ với các số nguyên dương $x = x_1$, $y = y_1$, $z = z_1$, trong đó $(x_1, y_1) = 1$.

Bây giờ giả sử $x = x_0$, $y = y_0$, $z = z_0$ là nghiệm của phương trình $x^4 + y^4 = z^2$, trong đó $(x_0, y_0) = 1$. Ta sẽ chỉ ra rằng tồn tại nghiệm khác gồm các số nguyên dương $x = x_1$, $y = y_1$, $z = z_1$ với $(x_1, y_1) = 1$ sao cho $z_1 < z_0$.

Vì $x_0^4 + y_0^4 = z_0^2$ nên

$$(x_0^2)^2 + (y_0^2)^2 = z_0^2,$$

tức là $\{x_0^2,\ y_0^2,\ z_0\}$ là một bộ số Pitago. Hơn nữa, $(x_0^2,\ y_0^2) = 1$, vì nếu $p$ là số nguyên tố, $p \mid x_0^2$, $p \mid y_0^2$ thì $p \mid x_0$, $p \mid y_0$, mâu thuẫn với $(x_0,\ y_0) = 1$. Như vậy, $\{x_0^2,\ y_0^2,\ z_0\}$ là một bộ số Pitago nguyên thủy, và theo Định lí 5.7, tồn tại các số nguyên dương $m$, $n$ với $(m,\ n) = 1$, $m \not\equiv n \pmod 2$ và

$$x_0^2 = m^2 - n^2$$

$$y_0^2 = 2mn$$

$$z_0 = m^2 + n^2,$$

trong đó ta có thể xem $y_0^2$ là số chẵn (nếu cần thì đổi kí hiệu $x_0^2$ và $y_0^2$).

Từ đẳng thức của $x_0^2$ ta được

$$x_0^2 + n^2 = m^2.$$

Do $(m,\ n) = 1$ nên $\{x_0,\ n,\ m\}$ là một bộ số Pitago nguyên thủy. Lại theo Định lí 5.7, tồn tại các số nguyên dương $r$, $s$ với $(r,\ s) = 1$, $r \not\equiv s \pmod 2$ và

$$x_0^2 = r^2 - s^2$$

$$n = 2rs$$

$$m = r^2 + s^2$$

Vì $m$ lẻ và $(m,\ n) = 1$, ta có $(m,\ 2n) = 1$. Do $y_0^2 = (2n)m$ nên theo Bổ đề 5.6, tồn tại các số nguyên dương $z_1$ và $w$ với $m = z_1^2$, $2n = w^2$. Vì $w$ chẵn, $w = 2u$, trong đó $u$ là số nguyên dương, nên

$$u^2 = \frac{n}{2} = rs$$

Do $(r,\ s) = 1$, theo Bổ đề 5.6, tồn tại các số nguyên dương $x_1$, $y_1$ sao cho $r = x_1^2$, $s = y_1^2$. Chú ý rằng vì $(r,\ s) = 1$ nên dễ suy ra $(x_1,\ y_1) = 1$. Như vậy,

$$x_1^4 + y_1^4 = z_1^2,$$

trong đó $x_1$, $y_1$, $z_1$ là các số nguyên dương với $(x_1,\ y_1) = 1$. Hơn nữa ta có $z_1 < z_0$, vì

$$z_1 \leq z_1^4 = m^2 < m^2 + n^2 = z_0.$$

Để kết thúc chứng minh định lí, giả sử $x^4 + y^4 = z^4$ có ít nhất một nghiệm nguyên. Do nguyên lí sắp thứ tự tốt, trong số các nghiệm nguyên dương, tồn tại nghiệm với giá trị $z_0$ bé nhất. Tuy nhiên ta đã chỉ ra rằng, từ nghiệm này, ta có thể tìm nghiệm khác với giá trị bé hơn của biến $z$. Mâu thuẫn này kết thúc chứng minh của định lí. □

## § 3. PHƯƠNG TRÌNH PELL

Mục đích của phần này là nghiên cứu phương trình Điôphăng có dạng sau

$$x^2 - dy^2 = n, \tag{1}$$

trong đó $d$ và $n$ là các số nguyên cố định. Khi $d < 0$ và $n < 0$, phương trình vô nghiệm. Khi $d < 0$ và $n > 0$, phương trình chỉ có thể có hữu hạn nghiệm, vì đẳng thức $x^2 - dy^2 = n$ suy ra $|x| \leq \sqrt{n}$, $|y| \leq \sqrt{\dfrac{n}{|d|}}$. Khi $d$ là một số chính phương, chẳng hạn $d = D^2$ thì

$$x^2 - dy^2 = x^2 - D^2y = (x + Dy)(x - Dy) = n.$$

Vậy, mọi nghiệm của (1) khi $d$ chính phương sẽ tương ứng với nghiệm của hệ phương trình

$$\begin{cases} x + Dy = a \\ x - Dy = b, \end{cases}$$

trong đó $a$ và $b$ là các số nguyên sao cho $n = ab$. Trong trường hợp đó, chỉ có hữu hạn nghiệm, vì tồn tại nhiều nhất là một nghiệm nguyên của hai phương trình trên ứng với một cách phân tích $n = ab$.

Trong phần còn lại, ta quan tâm phương trình $x^2 - dy^2 = n$, trong đó $d$ và $n$ là các số nguyên, $d$ là số nguyên dương không chính phương. Định lí sau đây chỉ ra rằng, phân số liên tục đơn giản của $\sqrt{d}$ rất quan trọng trong nghiên cứu phương trình trên.

**Định lí 5.9.** *Giả sử $d$ và $n$ là các số nguyên sao cho $d > 0$ và $d$ không là số chính phương, $|n| < \sqrt{d}$. Khi đó, nếu $x^2 - dy^2 = n$, thì $\frac{x}{y}$ là một tổng hội tụ riêng của phân số liên tục đơn của $\sqrt{d}$.*

***Chứng minh.*** Trước tiên xét trường hợp $n > 0$. Vì $x^2 - dy^2 = n$, nên ta có

$$(x + y\sqrt{d})(x - y\sqrt{d}) = n. \tag{2}$$

Từ (2) ta thấy $x - y\sqrt{d} > 0$ nên $x > y\sqrt{d}$. Do đó

$$\frac{x}{y} - \sqrt{d} > 0.$$

Hơn nữa, do $0 < n < \sqrt{d}$ nên

$$\begin{aligned} \frac{x}{y} - \sqrt{d} = \frac{x - y\sqrt{d}}{y} &= \frac{x^2 - dy^2}{y(x + y\sqrt{d})} \\ &< \frac{n}{y(2y\sqrt{d})} \\ &< \frac{\sqrt{d}}{2y^2\sqrt{d}} = \frac{1}{2y^2}. \end{aligned}$$

Do $0 < \frac{x}{y} - \sqrt{d} < \frac{1}{2y^2}$, từ Định lí 4.21 suy ra rằng $\frac{x}{y}$ là một tổng hội tụ riêng của phân số liên tục đơn $\sqrt{d}$.

Khi $n < 0$, chia hai vế của $x^2 - dy^2 = n$ cho $-d$, ta được :

$$y^2 - \left(\frac{1}{d}\right)x^2 = -\frac{n}{d}.$$

Lí luận tương tự như trên chỉ ra rằng, khi $n > 0$, $\frac{y}{x}$ là một tổng hội tụ riêng của phân số liên tục đơn của $\frac{1}{\sqrt{d}}$. Do đó, $\frac{x}{y} = 1\Big/\left(\frac{y}{x}\right)$ là một tổng hội tụ riêng của phân số liên tục đơn của $\sqrt{d} = 1\Big/\left(\frac{1}{\sqrt{d}}\right)$. □

Định lí sau đây cho ta phương pháp tìm nghiệm nguyên của phương trình $x^2 - dy^2 = n$ dựa trên phân số liên tục.

**Định lí 5.10.** *Giả sử $d$ là một số nguyên dương không chính phương. Đặt*

$$\alpha_k = (P_k + \sqrt{d})/Q_k,$$
$$a_k = [\alpha_k],$$
$$P_{k+1} = a_k Q_k - P_k,$$
$$Q_{k+1} = (d - P_{k+1}^2)/Q_k,$$

*với $k = 0, 1, 2, \ldots$, trong đó $\alpha_0 = \sqrt{d}$. Hơn nữa, giả sử $\frac{p_k}{q_k}$ là tổng riêng hội tụ thứ $k$ của phân số liên tục đơn của $\sqrt{d}$. Khi đó*

$$p_k^2 - dq_k^2 = (-1)^{k-1} Q_{k+1}.$$

Trước khi chứng minh Định lí 5.10, ta chứng minh Bổ đề sau.

**Bổ đề 5.11.** *Giả sử $r + s\sqrt{d} = t + u\sqrt{d}$, trong đó $r$, $s$, $t$, $u$ là các số hữu tỉ và $d$ là số nguyên dương không chính phương. Khi đó $r = t$ và $s = u$.*

***Chứng minh.*** Do $r + s\sqrt{d} = t + u\sqrt{d}$ nên nếu $s \neq u$ ta có

$$\sqrt{d} = \frac{r - t}{u - s}$$

Do $d$ không chính phương nên $\sqrt{d}$ phải là số vô tỉ và không thể có biểu diễn trên. Vậy $s = u$, và do đó, $r = t$. □

***Chứng minh Định lí 5.10.*** Vì $\sqrt{d} = \alpha_0 = [a_0 ; a_1, a_2, \ldots, a_k, \alpha_{k+1}]$ nên ta có :

$$\sqrt{d} = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}}.$$

Vì $\alpha_{k+1} = (P_{k+1} + \sqrt{d})/Q_{k+1}$, ta có :

$$\sqrt{d} = \frac{(P_{k+1} + \sqrt{d})p_k + Q_{k+1}p_{k-1}}{(P_{k+1} + \sqrt{d})q_k + Q_{k+1}q_{k-1}}.$$

Do đó ta thấy rằng

$$dq_k + (P_{k+1}q_k + Q_{k+1}q_{k-1})\sqrt{d} = (P_{k+1}p_k + Q_{k+1}p_{k-1}) + p_k\sqrt{d}.$$

Từ Bổ đề 5.11 ta có

$$dq_k = P_{k+1}p_k + Q_{k+1}p_{k-1},$$

$$P_{k+1}q_k + Q_{k+1}q_{k-1} = p_k.$$

Nhân phương trình thứ nhất với $q_k$, phương trình thứ hai với $p_k$ rồi trừ phương trình thứ hai cho phương trình thứ nhất, ta được :

$$p_k^2 - dq_k^2 = (p_kq_{k-1} - p_{k-1}q_k)Q_{k+1} = (-1)^{k-1}Q_{k+1}.$$

Định lí được chứng minh bằng cách áp dụng Định lí 4.10. □

Trường hợp đặc biệt của phương trình $x^2 - dy^2 = n$ khi $n = 1$ được gọi là *Phương trình Pell*. Ta sẽ dùng các Định lí 5.9 và 5.10 để tìm tất cả các nghiệm của phương trình Pell và phương trình liên quan $x^2 - dy^2 = -1$.

**Định lí 5.12.** *Giả sử $d$ là số nguyên dương không chính phương. Kí hiệu qua $p_k/q_k$ tổng riêng hội tụ thứ $k$ của phân số liên tục đơn của $\sqrt{d}$, $k = 1, 2, 3, \ldots$ và giả sử $n$ là độ dài chu kì của phân số liên tục này. Khi đó, nếu $n$ chẵn thì các nghiệm nguyên dương của phương trình $x^2 - dy^2 = 1$ là $x = p_{jn-1}$, $y = q_{jn-1}$, $j = 1, 2, 3, \ldots$ ; còn phương trình $x^2 - dy^2 = 1$ vô nghiệm. Khi $n$ lẻ, các nghiệm nguyên dương của phương trình $x^2 - dy^2 = 1$ là $x = p_{2nj-1}$, $y = q_{2nj-1}$, $j = 1, 2, 3, \ldots$ ; các nghiệm nguyên dương của $x^2 - dy^2 = -1$ là $x = p_{(2j-1)n-1}$, $y = q_{(2j-1)n-1}$, $j = 1, 2, 3, \ldots$*

***Chứng minh.*** Theo Định lí 5.9, nếu $x_0$, $y_0$ là nghiệm nguyên dương của $x^2 - dy^2 = \pm 1$ thì $x_0 = p_k$, $y_0 = q_k$, trong đó $p_k/q_k$ là tổng hội tụ riêng của phân số liên tục đơn giản của $\sqrt{d}$. Mặt khác, từ Định lí 5.10 ta có :

$$p_k^2 - dq_k^2 = (-1)^{k-1}Q_{k+1},$$

trong đó $Q_{k+1}$ như trong phát biểu của Định lí 5.10.

Vì chu kì của khai triển liên tục của $\sqrt{d}$ là $n$, ta biết rằng $Q_{jn} = Q_0 = 1$ với $j = 1, 2, 3, \ldots$ (do $\sqrt{d} = \dfrac{P_0 + \sqrt{d}}{Q_0}$). Vậy,

$$p_{jn-1}^2 - dq_{jn-1}^2 = (-1)^{jn} Q_{nj} = (-1)^{jn}.$$

Đẳng thức này chỉ ra rằng khi $n$ chẵn, $p_{jn-1}$, $q_{jn-1}$ là một nghiệm của $x^2 - dy^2 = 1$ với $j = 1, 2, 3, \ldots$ ; khi $n$ lẻ, $p_{2nj-1}$, $q_{2jn-1}$ là một nghiệm của $x^2 - dy^2 = 1$ và $p_{2(j-1)n-1}$, $q_{2(j-1)n-1}$ là một nghiệm của $x^2 - dy^2 = -1$ với $j = 1, 2, 3, \ldots$

Để chỉ ra rằng các phương trình $x^2 - dy^2 = 1$ và $x^2 - dy^2 = -1$ không có nghiệm khác các nghiệm đã tìm được ta chứng tỏ rằng $Q_{k+1} = 1$ suy ra $n \mid k$ và $Q_j \neq -1$ với $j = 1, 2, 3, \ldots$

Trước tiên nhận xét rằng, nếu $Q_{k+1} = 1$ thì

$$\alpha_{k+1} = P_{k+1} + \sqrt{d}.$$

Vì $\alpha_{k+1} = [a_{k+1} ; a_{k+2}, \ldots]$, khai triển phân số liên tục của $\alpha_{k+1}$ là tuần hoàn đơn. Do đó ta có $-1 < \alpha_{k+1} = P_{k+1} - \sqrt{d} < 0$. Từ đó suy ra $P_{k+1} = [\sqrt{d}]$, nên $\alpha_k = \alpha_0$, $n \mid k$.

Để chứng tỏ $Q_j \neq -1$ với $j = 1, 2, 3, \ldots$ ta chú ý rằng từ $Q_j = -1$ suy ra $\alpha_j = -P_j - \sqrt{d}$. Do $\alpha_j$ có khai triển phân số liên tục đơn giản chu kì đơn nên

$$-1 < \alpha_j = -P_j - \sqrt{d} < 0$$

và

$$\alpha_j = -P_j - \sqrt{d} > 1.$$

Từ bất đẳng thức thứ nhất suy ra $P_j > -\sqrt{d}$, từ bất đẳng thức thứ hai suy ra $P_j < -1 - \sqrt{d}$ : mâu thuẫn. Vậy $Q_j \neq -1$.

Vì ta đã tìm được tất cả các nghiệm của $x^2 - dy^2 = 1$ và $x^2 - dy^2 = -1$ trong đó $x$, $y$ nguyên dương, nên định lí được chứng minh đầy đủ. □

***Ví dụ :*** 1) Xét phương trình $x^2 - 13y^2 = 1$.

Phân số liên tục đơn của $\sqrt{13}$ là $[3\ ;\ 1,\ \overline{1,\ 1,\ 1,\ 6}]$. Các nghiệm nguyên dương của phương trình là $p_{10j-1}$, $q_{10j-1}$, $j = 1,\ 2,\ 3, \ldots$, trong đó $p_{10j-1}/q_{10j-1}$ là tổng riêng hội tụ thứ $(10j-1)$ của khai triển phân số liên tục $\sqrt{13}$. Nghiệm dương bé nhất là $p_9 = 649$, $q_9 = 180$. Các nghiệm dương của phương trình $x^2 - 13y^2 = -1$ là $p_{10j-6}$, $q_{10j-6}$, $j = 1,\ 2,\ 3, \ldots$ Nghiệm dương bé nhất là $p_4 = 8$, $q_4 = 5$.

2) Xét phương trình $x^2 - 14y^2 = 1$.

Phân số liên tục của $\sqrt{14}$ là $[3\ ;\ \overline{1,\ 2,\ 1,\ 6}]$. Các nghiệm nguyên dương là $p_{4j-1}$, $q_{4j-1}$, $j = 1,\ 2,\ 3, \ldots$, trong đó $p_{4j-1}/q_{4j-1}$ là tổng riêng hội tụ thứ $j$ của khai triển phân số liên tục $\sqrt{14}$. Nghiệm nguyên dương bé nhất là $p_3 = 15$, $q_3 = 4$. Phương trình $x^2 - 14y^2 = 1$ không có nghiệm, vì độ dài chu kì của phân số liên tục của $\sqrt{14}$ chẵn.

Đối với phương trình Pell, ta có thể tìm các nghiệm nguyên dương xuất phát từ nghiệm nguyên dương bé nhất mà không phải tìm các tổng hội tụ riêng của khai triển phân số liên tục của $\sqrt{d}$.

**Định lí 5.13.** *Giả sử $x_1$, $y_1$ là nghiệm nguyên dương bé nhất của phương trình Pell $x^2 - dy^2 = 1$, trong đó $d$ là một số nguyên dương không chính phương. Khi đó mọi nghiệm $x_k$, $y_k$ được cho bởi*

$$x_k + y_k\sqrt{d} = (x_1 + y_1\sqrt{d})^k,$$

*với $k = 1,\ 2,\ 3, \ldots$*

***Chứng minh.*** Ta chỉ ra $x_k$, $y_k$ với $k = 1,\ 2,\ 3, \ldots$ là nghiệm của phương trình, đồng thời mỗi nghiệm của phương trình đều có dạng trên.

Dễ thấy rằng nếu $x_k + y_k\sqrt{d} = (x_1 + y_1\sqrt{d})^k$ thì $x_k - y_k\sqrt{d} = (x_1 - y_1\sqrt{d})^k$ (vì $\sqrt{d}$ chỉ xuất hiện ở các lũy thừa lẻ của $-y_1\sqrt{d}$ trong khai triển nhị thức). Mặt khác,

$$\begin{aligned} x_k^2 - dy_k^2 &= (x_k + y_k\sqrt{d})(x_k - y_k\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})^k(x_1 - y_1\sqrt{d})^k \\ &= (x_1^2 - dy_1^2)^k = 1. \end{aligned}$$

Vậy $x_k$, $y_k$ là nghiệm với $k = 1, 2, 3, \ldots$

Ngược lại, giả sử $X$, $Y$ là một nghiệm nguyên dương khác với $x_k$, $y_k$, $k = 1, 2, 3, \ldots$ Khi đó tồn tại số $n$ sao cho

$$(x_1 + y_1\sqrt{d})^n < X + Y\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1}.$$

Nhân bất đẳng thức với $(x_1 + y_1\sqrt{d})^{-n}$ ta được :

$$1 < (x_1 - y_1\sqrt{d})^n(X + Y\sqrt{d}) < (x_1 + y_1\sqrt{d}),$$

(vì $x_1^2 - dy_1^2 = 1$ nên $x_1 - y_1\sqrt{d} = (x_1 + y_1\sqrt{d})^{-1}$).

Bây giờ giả sử

$$s + t\sqrt{d} = (x_1 - y_1\sqrt{d})^n(X + Y\sqrt{d}),$$

và chú ý rằng

$$\begin{aligned} s^2 - dt^2 &= (s - t\sqrt{d})(s + t\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})^n(X - Y\sqrt{d})(x_1 - y_1\sqrt{d})^n(X + Y\sqrt{d}) \\ &= (x_1^2 - dy_1^2)^n(X^2 - dY^2) = 1. \end{aligned}$$

Ta thấy $s$, $t$ là nghiệm của phương trình $x^2 - dy^2 = 1$. Hơn nữa, $1 < s + t\sqrt{d} < x_1 + y_1\sqrt{d}$. Mặt khác, vì $s + t\sqrt{d} > 1$ nên $0 < (s + t\sqrt{d})^{-1} < 1$. Do đó

$$s = \frac{1}{2}[(s + t\sqrt{d}) + (s - t\sqrt{d})] > 0,$$

$$t = \frac{1}{2\sqrt{d}}[(s + t\sqrt{d}) - (s - t\sqrt{d})] > 0.$$

Điều đó có nghĩa là $s$, $t$ là nghiệm dương $s \geq x_1$, $t \geq y_1$ do $x_1$, $y_1$ là nghiệm bé nhất. Điều này mâu thuẫn với bất đẳng thức $s + t\sqrt{d} < x_1 + y_1\sqrt{d}$. Vậy $X$, $Y$ là $x_k$, $y_k$ với $k$ nào đó.

***Ví dụ :*** Ta đã biết nghiệm nguyên dương bé nhất của phương trình $x^2 - 13y^2 = 1$ là $x_1 = 649$, $y_1 = 180$. Do đó, mọi nghiệm nguyên dương của phương trình là $x_k$, $y_k$ xác định bởi công thức :

$$x_k + y_k\sqrt{13} = (649 + 180\sqrt{13})^k$$

Chẳng hạn,

$$x_2 + y_2\sqrt{13} = 842361 + 233640\sqrt{13}.$$

Do đó $x_2 = 842361$, $y_2 = 233640$ là nghiệm nguyên dương bé nhất của phương trình khác với nghiệm đầu tiên $x_1 = 649$, $y_1 = 180$.

## § 4. VỀ VIỆC GIẢI PHƯƠNG TRÌNH ĐIÔPHĂNG

Trong các phần trước, chúng ta đã làm quen với phương pháp giải các phương trình Điôphăng bậc nhất (tuyến tính) và bậc 2. Đối với các phương trình bậc cao hơn, tồn tại hay không một phương pháp chung để giải ? Đó là câu hỏi đã được đặt ra từ thời Điôphăng, và là nội dung của *Bài toán Hilbert thứ 10* nổi tiếng. Xin nhắc lại rằng, tại Đại hội Toán học Quốc tế đầu thế kỉ 20, Hilbert, một trong những nhà toán học lớn nhất của mọi thời đại, đã đề ra *23 bài toán cho toán học của thế kỉ 20*. Cho đến nay, nhiều bài toán trong số đó vẫn đang chờ lời giải. Bài toán thứ 10 mà ta nhắc đến ở đây là : *Có hay không một thuật toán để giải các phương trình Điôphăng ?*. Nói một cách "nôm na" là : có hay không một phương pháp để khi cho một phương trình Điôphăng tuỳ ý, ta dùng phương pháp đó để, sau một thời gian hữu hạn, tìm ra nghiệm, hoặc chỉ ra rằng phương trình không tồn tại nghiệm (nguyên). Bài toán Hilbert thứ 10 đã được nhà toán học Nga Yuri Matijasievich giải năm 1970 khi ông mới 21 tuổi. Câu trả lời là : *không tồn tại thuật toán giải phương trình Điôphăng tổng quát*. Như vậy, với các phương trình Điôphăng bậc lớn hơn 2, ta chỉ có thể tìm cách giải từng phương trình cụ thể ! Tuy nhiên, cũng có thể kể ra đây vài phương pháp hay được dùng để giải các phương trình Điôphăng được cho trong chương trình toán phổ thông. Tư tưởng chung của các phương pháp đó là, do chỉ xét các nghiệm nguyên (nhiều khi là nghiệm nguyên dương) nên nếu ta thu hẹp được tập hợp chứa nghiệm (nếu có) thì có thể dùng cách thử toàn bộ để xác định nghiệm.

1. Sử dụng các tính chất chia hết để thu hẹp tập hợp nghiệm có thể

2. Dùng các ước lượng về độ lớn của nghiệm để thu hẹp tập hợp nghiệm có thể. Thông thường, để làm việc đó, cần dựa vào một "nghiệm cực trị" (nhỏ nhất hoặc lớn nhất theo một nghĩa nào đó).

Các "phương pháp" vừa nêu chỉ là các gợi ý. Việc vận dụng chúng một cách linh hoạt được cho qua các bài tập.

## BÀI TẬP CHƯƠNG 5

**1.** Chứng minh rằng phương trình Điôphăng

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

không có nghiệm nguyên nếu $d \nmid b$, trong đó $d = (a_1, a_2, \ldots, a_n)$, có vô hạn nghiệm nếu $d \mid b$.

**2.** Giả sử $a$, $b$ là các số nguyên dương nguyên tố cùng nhau, $n$ là số nguyên dương. Nghiệm nguyên $(x, y)$ của phương trình $ax + by = n$ được gọi là nghiệm không âm, nếu $x \geq 0$, $y \geq 0$. Chứng minh rằng :

a) Nếu $n \geq (a-1)(b-1)$ thì phương trình có nghiệm không âm.

b) Nếu $n = ab - a - b$ thì phương trình không có nghiệm không âm.

c) Có đúng $\dfrac{(a-1)(b-1)}{2}$ số nguyên dương $n$ sao cho phương trình có nghiệm không âm.

**3.** Chứng minh rằng nếu $x$, $y$, $z$ là một bộ số Pitago thì ít nhất một trong các số $x$, $y$, $z$ chia hết cho 4.

**4.** Chứng minh rằng mỗi số nguyên dương lớn hơn 3 là một thành phần của ít nhất một bộ số Pitago.

**5.** Xác định các dãy số sau :

$$\begin{aligned} x_1 &= 3,\ y_1 = 4,\ z_1 = 5 \\ x_{n+1} &= 3x_n + 2z_n + 1 \\ y_{n+1} &= 3x_n + 2z_n + 2 \\ z_{n+1} &= 4x_n + 3z_n + 2 \end{aligned}$$

khi $n \geq 1$. Chứng minh rằng $(x_n, y_n, z_n)$ là bộ số Pitago với mọi $n$.

**6.** Chứng minh rằng nếu $(x, y, z)$ là một bộ số Pitago, $y = x + 1$, thì $x, y, z$ là một trong các bộ số Pitago xác định trong Bài 5.

**7.** Tìm mọi nghiệm nguyên dương của phương trình $x^2 + 2y^2 = z^2$.

**8.** Tìm mọi nghiệm nguyên dương của phương trình $x^2 + 3y^2 = z^2$.

**9.** Tìm mọi nghiệm nguyên dương của phương trình $w^2 + x^2 + y^2 = z^2$.

**10.** Tìm công thức cho mọi bộ số Pitago $(x, y, z)$ với $z = y + 1$.

**11.** Hỏi tương tự Bài 10, $z = y + 2$.

**12.** Chứng minh rằng số các bộ số Pitago $(x, y, z)$ (với $x^2 + y^2 = z^2$) với

$x$ cố định là $\dfrac{\tau(x^2)-1}{2}$ nếu $x$ lẻ, $\dfrac{\tau\left(\dfrac{x^2}{4}\right)-1}{2}$ nếu $x$ chẵn.

**13.** Tìm mọi nghiệm nguyên dương của phương trình $x^2 + py^2 = z^2$, trong đó $p$ là số nguyên tố.

**14.** Chứng minh rằng nếu $x$, $y$, $z$ là một bộ số Pitago, $n$ nguyên $> 2$ thì $x^n + y^n \neq z^n$.

**15.** Chứng minh rằng phương trình $x^4 - y^4 = z^2$ không có nghiệm nguyên khác $0$.

**16.** Chứng minh rằng diện tích một tam giác vuông cạnh nguyên không phải là số chính phương.

**17.** Chứng minh rằng phương trình $x^4 + 4y^4 = z^2$ không có nghiệm nguyên khác $0$.

**18.** Chứng minh rằng phương trình $x^4 + 3y^4 = z^4$ có vô số nghiệm nguyên.

**19.** Chứng minh rằng trong bộ số Pitago có nhiều nhất là một số chính phương.

**20.** Chứng minh rằng phương trình $x^2 + y^2 = z^3$ có vô hạn nghiệm nguyên.

**21.** Giải các phương trình Điôphăng sau đây :

a) $x^2 + 3y^2 = 4$; b) $x^2 + 5y^2 = 7$;

c) $2x^2 + 7y^2 = 30$.

**22.** Giải các phương trình Điôphăng sau đây :

a) $x^2 - y^2 = 8$; b) $x^2 - 4y^2 = 40$;

c) $4x^2 - 9y^2 = 100$.

**23.** Tìm nghiệm nguyên dương bé nhất của các phương trình Điôphăng sau

a) $x^2 - 29y^2 = -1$; b) $x^2 - 29y^2 = 1$.

**24.** Tìm ba nghiệm dương bé nhất của phương trình Điôphăng :

$$x^2 - 37y^2 = 1.$$

**25.** Nghiệm dương bé nhất của phương trình Điôphăng $x^2 - 61y^2 = 1$ là $x_1 = 1766319049$, $y_1 = 226153980$. Tìm nghiệm dương bé nhất khác với $(x_1,\ y_1)$.

**26.** Chứng minh rằng nếu $\dfrac{p_k}{q_k}$ là một hội tụ của khai triển phân số liên tục đơn của $\sqrt{d}$ thì $\left|p_k^2 - dq_k^2\right| < 1 + \sqrt{d}$.

**27.** Chứng minh rằng nếu $d$ là số nguyên dương chia hết cho số nguyên tố nào đó dạng $4k + 3$, thì phương trình Điôphăng $x^2 - dy^2 = -1$ vô nghiệm.

**28.** Giả sử $d$, $n$ là các số nguyên dương. Chứng minh rằng :

a) Nếu $r$, $s$ là nghiệm của phương trình Điôphăng $x^2 - dy^2 = 1$ và $X$, $Y$ là nghiệm của phương trình Điôphăng $x^2 - dy^2 = n$ thì $Xr \pm dYs$, $Xs \pm Yr$ cũng là nghiệm của $x^2 - dy^2 = n$.

b) phương trình Điôphăng $x^2 - dy^2 = n$ hoặc vô nghiệm, hoặc có vô hạn nghiệm.

**29.** Chứng minh các phương trình Điôphăng sau vô nghiệm :

a) $x^4 - 2y^4 = 1$; b) $x^4 - 2y^2 = -1$.

**30.** Giả sử $a$, $b$, $n$ là các số nguyên dương, $a > b$, $n > b$. Chứng minh rằng nếu $c$ là số lớn hơn $0$ thỏa mãn $a^n + b^n = c^n$ thì $c$ không phải là số nguyên.

Chương 6.

# CÁC QUAN HỆ HỒI QUY

## § 1. QUAN HỆ HỒI QUY TỔNG QUÁT

Khi giải nhiều bài toán, đặc biệt là các bài toán tổ hợp, ta thường dùng phương pháp đưa bài toán đang xét (với $n$ đối tượng) về bài toán với số đối tượng ít hơn, cho đến khi dễ dàng giải chúng. Phương pháp như vậy gọi là phương pháp dùng các quan hệ hồi quy.

**Định nghĩa 6.1.** *Quan hệ hồi quy bậc* $k$ là một công thức cho phép tính giá trị $f(n+k)$ qua các giá trị $f(n), f(n+1), \ldots, f(n+k-1)$.

Ví dụ : 1) $f(n+2) = n^2 f(n+1) - f(n) + f(n-1)$

là quan hệ hồi quy bậc 3.

$$2)\ f(n+1) = f(n) + f(n-1) \tag{1}$$

là quan hệ hồi quy bậc 2.

Đối với một quan hệ hồi quy bậc $k$, nếu cho các giá trị $f(1), \ldots, f(k)$ thì các giá trị còn lại hoàn toàn được xác định. Chẳng hạn, trong quan hệ (1), nếu ta cho $f(1) = f(2) = 1$ thì ta nhận được dãy số nổi tiếng, gọi là các số Fibonacci.

Một dãy $f(n)$ thỏa mãn quan hệ hồi quy nào đó được gọi là một *nghiệm* của quan hệ đó. Để ý rằng, nếu quan hệ hồi quy bậc $k$ thì $k$ giá trị đầu của dãy có thể lấy tùy ý, các giá trị tiếp theo hoàn toàn được xác định.

Một nghiệm của quan hệ hồi quy bậc $k$ được gọi là *nghiệm tổng quát* nếu nó phụ thuộc $k$ hằng số tùy ý $C_1, \ldots, C_k$.

***Ví dụ :*** Xét quan hệ hồi quy

$$f(n+2) = 5f(n+1) - 6f(n). \tag{2}$$

Dễ dàng chứng minh rằng, với mọi số thực $C_1$, $C_2$, công thức

$$f(n) = C_1 2^n + C_2 3^n$$

cho ta nghiệm của quan hệ hồi quy đang xét (2). Nghiệm tùy ý được xác định qua giá trị $f(1)$, $f(2)$, chẳng hạn, nếu đặt $f(1) = a$, $f(2) = b$, ta được :

$$\begin{cases} 2C_1 + 3C_2 = a \\ 4C_1 + 9C_2 = b. \end{cases}$$

Hệ phương trình này có nghiệm $C_1$, $C_2$ với mọi giá trị của $a$, $b$.

## § 2. HỒI QUY TUYẾN TÍNH HỆ SỐ HẰNG

Nói chung, không có phương pháp chung để tìm nghiệm của quan hệ hồi quy. Ở đây, chúng ta sẽ nghiên cứu một phương pháp tìm nghiệm của một lớp quan hệ hồi quy đặc biệt, gọi là quan hệ *hồi quy tuyến tính với hệ số hằng*.

**Định nghĩa 6.2.** *Quan hệ hồi quy tuyến tính bậc $k$ với hệ số hằng* là quan hệ có dạng :

$$f(n+k) = a_1 f(n+k-1) + a_2 f(n+k-2) + \cdots + a_k f(n),$$

trong đó $a_1$, $a_2$, ... , $a_k$ là các hằng số nào đó (không phụ thuộc $n$).

Trước tiên ta xét trường hợp đơn giản : các quan hệ hồi quy tuyến tính hệ số hằng

$$f(n+2) = a_1 f(n+1) + a_2 f(n). \tag{3}$$

**Bổ đề 6.3.** *Nếu $f_1(n)$, $f_2(n)$ là các nghiệm của (3) thì với các số tùy ý $A$, $B$ dãy $f(n) = Af_1(n) + Bf_2(n)$ cũng là nghiệm của (3).*

***Chứng minh.*** Theo giả thiết ta có :

$$f_1(n+2) = a_1 f_1(n+1) + a_2 f_1(n)$$

$$f_2(n+2) = a_1 f_2(n+1) + a_2 f_2(n).$$

Từ đó suy ra

$$Af_1(n+2) + Bf_2(n+2) = a_1[Af_1(n+1) + Bf_2(n+1)] + a_2[Af_1(n) + Bf_2(n)].$$

Như vậy, $Af_1(n) + Bf_2(n)$ cũng là một nghiệm của (3). □

**Bổ đề 6.4.** *Giả sử $r_1$ là nghiệm của phương trình*

$$r^2 = a_1 r + a_2. \tag{4}$$

*Khi đó dãy* $\{r_1^n\}$ *là một nghiệm của quan hệ*

$$f(n+2) = a_1 f(n+1) + a_2 f(n). \tag{5}$$

***Chứng minh.*** Ta có $f(n) = r_1^n$, $f(n+1) = r_1^{n+1}$, $f(n+2) = r_1^{n+2}$. Thay vào (5) ta được

$$r_1^{n+2} = a_1 r_1^{n+1} + a_2 r_1^n.$$

Đẳng thức này đúng, vì $r_1^2 = a_1 r_1 + a_2$. □

**Nhận xét :** Dãy $\{r_1^{n+m}\}$ với $m$ tùy ý cũng là một nghiệm. Thật vậy, chỉ cần áp dụng Bổ đề 6.3 với $B = 0$, $A = r_1^m$.

Phương trình (4) gọi là *phương trình đặc trưng* của quan hệ (5).

Từ các Bổ đề 6.3 và Bổ đề 6.4, ta có định lí sau :

**Định lí 6.5.** *Giả sử cho quan hệ hồi quy*

$$f(n+2) = a_1 f(n+1) + a_2 f(n). \tag{6}$$

*Giả sử phương trình đặc trưng*

$$r^2 = a_1 r + a_2$$

*có hai nghiệm phân biệt* $r_1$ *và* $r_2$. *Khi đó, nghiệm tổng quát của* (6) *có dạng*

$$f(n) = C_1 r_1^{n-1} + C_2 r_2^{n-1}.$$

***Chứng minh.*** Theo Bổ đề 6.4, $f_1(n) = r_1^{n-1}$, $f_2(n) = r_2^{n-1}$ là các nghiệm của quan hệ đang xét. Theo Bổ đề 6.3, với mọi $C_1$, $C_2$ tùy ý, $C_1 r_1^n + C_2 r_1^n$ là nghiệm. Chỉ còn phải chứng minh rằng, nghiệm tùy ý của quan hệ (6) có thể viết dưới dạng đã nêu trong định lí. Mỗi nghiệm của hệ (6) được xác định duy nhất bởi các giá trị $f(1)$, $f(2)$. Vì thế, chỉ cần chỉ ra rằng, hệ phương trình

$$\begin{cases} C_1 + C_2 = a \\ C_1 r_1 + C_2 r_2 = b \end{cases}$$

có nghiệm với $a$, $b$ tùy ý. Dễ thấy rằng, các nghiệm đó là

$$C_1 = \frac{b - a r_2}{r_1 - r_2}, \quad C_2 = \frac{a r_1 - b}{r_1 - r_2}.$$

Định lí được chứng minh. □

Bây giờ ta chuyển sang xét trường hợp phương trình đặc trưng có nghiệm bội.

Giả sử phương trình đặc trưng của quan hệ đã cho có các nghiệm trùng nhau, chẳng hạn $r_1 = r_2$. Khi đó biểu thức $C_1 r_1^{n-1} + C_2 r_2^{n-1}$ không còn là nghiệm tổng quát nữa, vì nghiệm đó được viết dưới dạng $f(n) = C r_1^{n-1}$. Nói chung, không thể chọn hằng số $C$ sao cho hai điều kiện ban đầu $f(1) = a$, $f(2) = b$ được thỏa mãn.

**Định lí 6.6.** *Giả sử phương trình đặc trưng*

$$r^2 = a_1 r + a_2$$

*có nghiệm bội* $r_1$. *Khi đó, nghiệm tổng quát của quan hệ đang xét có dạng*

$$f(n) = r_1^{n-1}(C_1 + C_2 n),$$

*trong đó* $C_1$, $C_2$ *là các hằng số tùy ý.*

***Chứng minh.*** Vì phương trình đặc trưng có nghiệm bội nên theo Định lí Viét ta có : $a_1 = 2r_1$, $a_2 = -r_1^2$. Ta viết phương trình đặc trưng dưới dạng :

$$r^2 = 2r_1 r - r_1^2.$$

Như vậy quan hệ hồi quy sẽ có dạng

$$f(n+2) = 2r_1 f(n+1) - r_1^2 f(n). \tag{7}$$

Ta thử lại rằng $f_2(n) = n r_1^{n-1}$ là một nghiệm của quan hệ đang xét. Ta có : $f_2(n+2) = (n+2) r_1^{n+1}$, $f_2(n+1) = (n+1) r_1^n$. Thay các giá trị này vào (7) ta nhận được đồng nhất thức :

$$(n+2) r_1^{n+1} = 2(n+1) r_1^{n+1} - n r_1^{n+1}.$$

Vậy $n r_1^{n-1}$ đúng là một nghiệm.

Theo Bổ đề 6.3, với $C_1$, $C_2$ tùy ý,

$$f(n) = r_1^{n-1}(C_1 + C_2 n) \tag{8}$$

cũng là nghiệm. Mặt khác, với điều kiện $f(1) = a$, $f(2) = b$ tùy ý, ta luôn luôn xác định được $C_1$, $C_2$ sao cho (8) là một nghiệm của quan hệ đang xét. Vậy (8) cho ta công thức nghiệm tổng quát trong trường hợp phương trình đặc trưng có nghiệm bội. □

**Nhận xét.** Đối với quan hệ hồi quy tuyến tính hệ số hằng cấp $k$ tùy ý, ta cũng có kết quả hoàn toàn tương tự. Xét quan hệ hồi quy cấp $k$ dạng

$$f(n+k) = a_1 f(n+k-1) + \cdots + a_k f(n).$$

Phương trình đặc trưng tương ứng :

$$r^k = a_1 r^{k-1} + \cdots + a_k.$$

Nếu $r_1$, $r_2$, ..., $r_k$ là các nghiệm khác nhau của phương trình đặc trưng, thì nghiệm tổng quát sẽ là

$$f(n) = C_1 r_1^{n-1} + \cdots + C_k r_k^{n-1}.$$

Nếu có các nghiệm nào đó trùng nhau, chẳng hạn $r_1 = r_2 = \cdots = r_s$ thì nghiệm tổng quát sẽ là

$$f(n) = r_1^{n-1}(C_1 + C_2 n + \cdots + C_s n^{s-1}) + C_{s+1} r_{s+1}^{n-1} + \cdots + C_k r_k^{n-1}.$$

***Ví dụ :*** Xét quan hệ hồi quy

$$f(n+4) = 5f(n+3) - 6f(n+2) - 4f(n+1) + 8f(n).$$

Phương trình đặc trưng có dạng :

$$r^4 - 5r^3 + 6r^2 + 4r - 8 = 0.$$

Các nghiệm của phương trình là

$$r_1 = 2,\ r_2 = 2,\ r_3 = 2,\ r_4 = -1.$$

Nghiệm tổng quát của quan hệ hồi quy đang xét sẽ là

$$f(n) = 2^{n-1}(C_1 + C_2 n + C_3 n^2) + C_4(-1)^{n-1}.$$

**Chú ý.** Trong các lí luận trên đây, các nghiệm của phương trình đặc trưng có thể là nghiệm phức. Khi đó, để tìm nghiệm thực của quan hệ hồi quy, ta có thể sử dụng công thức

$$e^{i\varphi} = \cos\varphi + i\sin\varphi.$$

***Ví dụ :*** Xét quan hệ hồi quy

$$f(n+2) = f(n+1) - f(n).$$

Phương trình đặc trưng tương ứng là

$$r^2 - r + 1 = 0.$$

Phương trình này có các nghiệm phức

$$r_1 = \frac{1+i\sqrt{3}}{2},\quad r_2 = \frac{1-i\sqrt{3}}{2},$$

hay là

$$r_1 = e^{i\frac{\pi}{3}},\quad r_2 = e^{-i\frac{\pi}{3}}.$$

Như vậy, nghiệm (thực) tổng quát của quan hệ hồi quy đang xét là

$$f(n) = C_1 \cos\frac{n\pi}{3} + C_2 \sin\frac{n\pi}{3}.$$

## § 3. DÃY FIBONACCI

Các số Fibonacci là nghiệm của một quan hệ hồi quy đơn giản, nhưng do vai trò quan trọng của các số Fibonacci trong toán học, ta sẽ dành mục này để nghiên cứu một số tính chất của chúng.

Số Fibonacci xuất hiện lần đầu tiên trong bài toán sau đây, được đưa ra trong cuốn sách "Liber Abaci" của nhà toán học Italia Fibonacci, xuất bản năm 1202 :

*Bài toán* : Một cặp thỏ mỗi tháng sinh một lần, cho một cặp thỏ con (một đực, một cái). Cặp thỏ mới sinh ra sau hai tháng lại bắt đầu sinh cặp mới. Hỏi sau một năm sẽ có bao nhiêu con thỏ, nếu đầu năm ta có một cặp thỏ ?

Từ giả thiết suy ra rằng, sau một tháng sẽ có hai cặp thỏ. Sau hai tháng, cặp thứ nhất sinh ra một cặp nữa, và ta có ba cặp. Tháng tiếp theo, cặp thứ hai cũng sinh ra cặp mới, và ta có 5 cặp thỏ.

Kí hiệu qua $F(n)$ số cặp thỏ sau tháng thứ $n$ kể từ đầu năm. Ta thấy sau tháng $(n+1)$ thì sẽ có $F(n)$ cặp ban đầu, cộng thêm số cặp do các cặp đã có sau tháng thứ $(n-1)$ sinh ra. Số này là $F(n-1)$. Vậy

$$F(n+1) = F(n) + F(n-1). \qquad (9)$$

Theo giả thiết, $F(0) = 1$, $F(1) = 2$, nên ta có $F(2) = 3$, $F(3) = 5$, ..., $F(12) = 377$.

Các số $F(n)$ được gọi là các số Fibonacci.

Dựa vào kết quả của phần trước, ta có thể tính được công thức biểu diễn $F(n)$. Phương trình đặc trưng tương ứng của quan hệ (9) là :

$$r^2 - r - 1 = 0.$$

Phương trình này có các nghiệm :

$$r_1 = \frac{1+\sqrt{5}}{2},\ r_2 = \frac{1-\sqrt{5}}{2}.$$

Nghiệm tổng quát của quan hệ (9) có dạng :

$$f(n) = C_1\left(\frac{1+\sqrt{5}}{2}\right)^n + C_2\left(\frac{1-\sqrt{5}}{2}\right)^n. \tag{10}$$

Các số Fibonacci $F(n)$ được cho bởi (10) với điều kiện $F(0)=1$, $F(1)=2$. Tuy nhiên, để thuận tiện, ta thường xét với điều kiện ban đầu $F(0)=0$, $F(1)=1$. Khi đó các hằng số $C_1$, $C_2$ được tính từ hệ phương trình

$$\begin{cases} C_1 + C_2 = 0 \\ \dfrac{\sqrt{5}}{2}(C_1 - C_2) = 1 \end{cases}$$

Giải ra ta được $C_1 = \dfrac{1}{\sqrt{5}}$, $C_2 = -\dfrac{1}{\sqrt{5}}$. Vậy nghiệm tổng quát có dạng

$$F(n) = \frac{\left(\dfrac{1+\sqrt{5}}{2}\right)^n - \left(\dfrac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}.$$

Công thức trên đây được gọi là công thức Binê (Binet). Dựa vào công thức Binê, ta có định lí sau đây cho một tính chất thú vị của các số Fibonacci.

**Định lí 6.7.** *Số Fibonacci $F_n$ là số nguyên gần nhất đối với số* $\dfrac{1}{\sqrt{5}}\left(\dfrac{1+\sqrt{5}}{2}\right)^n$, *tức là số hạng $a_n$ của cấp số nhân với từ đầu tiên là* $\dfrac{1}{\sqrt{5}}\left(\dfrac{1+\sqrt{5}}{2}\right)$ *và công bội là* $\dfrac{1+\sqrt{5}}{2}$.

***Chứng minh.*** Rõ ràng chỉ cần chứng minh rằng trị tuyệt đối của hiệu giữa hai số $F_n$ và $a_n$ luôn luôn bé hơn $\dfrac{1}{2}$. Ta có

$$|F_n - a_n| = \left|\frac{r_1^n - r_2^n}{\sqrt{5}} - \frac{r_1^n}{\sqrt{5}}\right| = \left|\frac{r_1^n - r_1^n - r_2^n}{\sqrt{5}}\right| = \frac{|r_2|^n}{\sqrt{5}}.$$

Do $|r_2| = \left|\frac{1-\sqrt{5}}{2}\right| < \frac{3-1}{2} = 1$ nên $|F_n - a_n| < \frac{1}{2}$.

Sau đây ta sẽ chứng minh một số tính chất cơ bản của dãy số Fibonacci. Các tính chất sâu hơn sẽ được tìm hiểu thông qua bài tập.

Trong các mệnh đề sau đây, $F(n)$ dùng để kí hiệu số Fibonacci thứ $n$.

**Mệnh đề 6.8.** $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.

***Chứng minh.*** Ta có :

$$F_1 = F_3 - F_2$$
$$F_2 = F_4 - F_3$$
$$\cdots$$
$$F_{n-1} = F_{n+1} - F_n$$
$$F_n = F_{n+2} - F_{n+1}$$

Cộng từng vế đẳng thức này, ta có :

$$F_1 + F_2 + \cdots + F_n = F_{n+2} - F_2,$$

mà $F_2 = 1$.

**Mệnh đề 6.9.** $F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$.

***Chứng minh.*** Ta có :

$$F_1 = F_2$$
$$F_3 = F_4 - F_2$$
$$F_5 = F_6 - F_4$$
$$F_{2n-1} = F_{2n} - F_{2n-2}.$$

Cộng từng vế các bất đẳng thức, ta được công thức cần chứng minh. □

**Mệnh đề 6.10.** $F_2 + F_4 + \cdots + F_{2n} = F_{2n+1} - 1$.

***Chứng minh.*** Từ Mệnh đề 6.8 ta có :

$$F_1 + F_2 + F_3 + \cdots + F_{2n} = F_{2n+2} - 1.$$

Trừ từng vế đẳng thức này cho đẳng thức trong Mệnh đề 6.9 ta được :

$$F_2 + F_4 + \cdots + F_{2n} = F_{2n+2} - 1 - F_{2n} = F_{2n+1} - 1.$$ □

**Mệnh đề 6.11.** $F_1 - F_2 + F_3 - F_4 + \cdots + (-1)^{n+1}F_n = (-1)^{n+1}F_{n-1} + 1.$

***Chứng minh.*** Từ các Mệnh đề 6.9, 6.10 ta được :

$$F_1 - F_2 + F_3 - F_4 + \cdots + F_{2n-1} - F_{2n} = -F_{2n-1} + 1. \qquad (1)$$

Cộng thêm vào hai vế $F_{2n+1}$ ta có :

$$F_1 - F_2 + F_3 - F_4 + \cdots - F_{2n} + F_{2n+1} = F_{2n} + 1. \qquad (2)$$

Công thức trong Mệnh đề 6.11 chính là kết hợp của hai công thức (1) và (2) (tương ứng với $n$ lẻ và $n$ chẵn).

**Mệnh đề 6.12.** $F_1^2 + F_2^2 + \cdots + F_n^2 = F_nF_{n+1}.$

***Chứng minh.*** Ta có :

$$F_kF_{k+1} - F_{k-1}F_k = F_k(F_{k+1} - F_{k-1}) = F_k^2.$$

Do đó

$$F_1^2 = F_1F_2$$

$$F_2^2 = F_2F_3 - F_1F_2$$

$$F_3^2 = F_3F_1 - F_2F_3$$

$$\cdots$$

$$F_n^2 = F_nF_{n+1} - F_{n-1}F_n$$

Cộng từng vế các đẳng thức này, ta được công thức cần chứng minh. □

## BÀI TẬP CHƯƠNG 6

**1.** Tìm nghiệm tổng quát của các quan hệ hồi quy sau

a) $a_{n+2} - 7a_{n+1} + 12a_n = 0$ ;

b) $a_{n+2} + 3a_{n+1} - 10a_n = 0$ ;

c) $a_{n+2} - 4a_{n+1} + 13a_n = 0$ ;

d) $a_{n+2} + 9a_n = 0$ ;

e) $a_{n+2} + 4a_{n+1} + 4a_n = 0$ ;

f) $a_{n+3} - 9a_{n+2} + 26a_{n+1} - 24a_n = 0$ ;

g) $a_{n+3} + 3a_{n+2} + 3a_{n+1} + a_n = 0$ ;

h) $a_{n+4} + 4a_n = 0$ .

**2.** Tìm $\{a_n\}$ thỏa mãn :

$$a_1 = 1,\ a_2 = -7,\ a_{n+2} - 5a_{n+1} + 6a_n = 0\ (n \geq 1)$$

**3.** Tìm $\{a_n\}$ thỏa mãn :

$$a_1 = 2,\ a_2 = 4,\ a_{n+2} - 4a_{n+1} + 4a_n = 0\ (n \geq 1)$$

**4.** Tìm $\{a_n\}$ thỏa mãn :

$$a_1 = -\frac{1}{4},\ a_2 = -\frac{1}{2},\ a_{n+2} + a_{n+1} + a_n = 0\ (n \geq 1)$$

**5.** Tìm $\{a_n\}$ thỏa mãn :

$$a_1 = 1,\ a_2 = -3,\ a_3 = -29,\ a_{n+3} = 9a_{n+2} - 26a_{n+1} + 24a_n\ (n \geq 1)$$

**6.** Tìm $\{a_n\}$ thỏa mãn :

$$a_1 = \cos\alpha,\ a_2 = \cos 2\alpha,\ a_{n+2} = 2\cos\alpha a_{n+1} - a_n\ (n \geq 1)$$

**7.** Tìm $\{a_n\}$ thỏa mãn :

$$a_{n+2} + 2a_{n+1} - 8a_n = 2^n.$$

Kí hiệu qua $F_n$ số Fibonacci thứ $n$ .

**8.** Chứng minh rằng

$$F_3 + F_6 + \cdots + F_{3n} = \frac{F_{3n+2} - 1}{2}.$$

**9.** Chứng minh rằng

$$F_1^3 + F_2^3 + \cdots + F_n^3 = \frac{F_{3n+2} + (-1)^{n+1}6F_{n-1} + 5}{10}.$$

**10.** Đặt $\alpha = \dfrac{1+\sqrt{5}}{2}$. Chứng minh rằng

$$\frac{\alpha^{n-\frac{1}{n}}}{\sqrt{5}} \leq F_n \leq \frac{\alpha^{n+\frac{1}{n}}}{\sqrt{5}}$$

**11.** Chứng minh rằng nếu $n \vdots m$ thì $F_n \vdots F_m$.

**12.** Giả sử $m$ là số nguyên dương tùy ý. Chứng minh rằng tồn tại $n$ sao cho $m \mid F_n$ và $n \leq m^2 - 1$.

**13.** Chứng minh đẳng thức sau :

$$(F_n,\ F_m) = F_{(n,\ m)}.$$

**14.** Chứng minh rằng nếu $n$ lẻ thì mọi ước lẻ của $F_n$ có dạng $4k + 1$.

**15.** Chứng minh rằng $F_{mn-1} - F_{n-1}^m$ chia hết cho $F_n^2$.

**16.** Chứng minh rằng $F_{nm} - F_{n+1}^m + F_{n-1}^m$ chia hết cho $F_n^3$.

**17.** Chứng minh rằng :

a) Nếu $q$ là ước nguyên tố của $F_n$, $p$ là số nguyên tố khác $q$ thì $F_{np}/F_n$ không chia hết cho $q$.

b) Nếu $p$ là ước nguyên tố lẻ của $F_n$ thì $F_{np}/F_n$ chia hết cho $p$, nhưng không chia hết cho $p^2$.

c) Nếu $F_n$ chia hết cho $4$ thì $F_{2n}/F_n$ chia hết cho $2$, nhưng không chia hết cho $4$.

d) Nếu $F_n$ chia hết cho $2$, nhưng không chia hết cho $4$ thì $F_{2n}/F_n$ chia hết cho $4$, nhưng không chia hết cho $8$.

# Phần II

# BÀI TẬP TỔNG HỢP

# A. ĐỀ BÀI

**1.** Giả sử $S$ là tập hợp các số tự nhiên sao cho trong khai triển theo cơ số $4$ của các số thuộc $S$ chỉ gồm các chữ số $0$ và $1$. Chứng minh rằng

a) Nếu $x, y \in S$, $x \neq y$ thì $\dfrac{x+y}{2} \notin S$.

b) Nếu $T$ là tập con của tập hợp các số tự nhiên, $T$ chứa $S$ và không trùng với $S$ thì tồn tại các phần tử $x \in T$, $y \in S$, $x \neq y$ và $\dfrac{x+y}{2} \in S$.

**2.** Tìm các cơ số $r$ $(< 10000)$ sao cho số $2101$ (viết trong cơ số $r$) là số chính phương.

**3.** Cho $a$, $b$, $c$, $d$ là các số tự nhiên sao cho $b^2 + 1 = ac$, $c^2 + 1 = bd$. Chứng minh rằng $a = 3b - c$, $d = 3c - b$.

**4.** Giả sử $x$ và $n$ là các số tự nhiên sao cho mọi ước nguyên tố của $x$ đều không vượt quá $n$. Chứng minh rằng nếu $n^2 \geq 4x$ thì $n!$ chia hết cho $x$.

**5.** Cho $p$ là số nguyên tố, $p > 3$ ; $n = \dfrac{2^{2p} - 1}{3}$. Chứng minh rằng $2^n - 2 \vdots n$.

**6.** Cho $n$ là số tự nhiên. Đặt

$$Q(n) = \prod_{k=1}^{n-1} k^{2k-n+1}.$$

Chứng minh rằng nếu $n$ là số nguyên tố thì $Q(n)$ là số nguyên.

**7.** Cho $n$ là số tự nhiên. Tìm ước chung lớn nhất của các số

$$C_{2n}^{1}, C_{2n}^{3}, \ldots, C_{2n}^{2n-1}.$$

**8.** Cho $n$ là số tự nhiên, $n \geq 3$. Tìm số tự nhiên $k$ nhỏ nhất có tính chất sau : với mọi bộ $n$ số tự nhiên $d_1, \ldots, d_n$ nguyên tố cùng nhau sao cho tổng $d_1 + \cdots + d_n$ chia hết cho mọi $d_i$, $(1 \leq i \leq n)$, ta có $(d_1 + \cdots + d_n)^k$ chia hết cho tích $d_1 \ldots d_n$.

**9.** Cho $n$ là số tự nhiên, $p$ là số nguyên tố, $n \geq p$. Chứng minh rằng

$$C_n^p \equiv \left[\frac{n}{p}\right] (\mathrm{mod}\, p),$$

trong đó $[x]$ là kí hiệu phần nguyên của số $x$.

**10.** Giả sử $n$, $b$ là các số tự nhiên, đồng thời $n \geq 5$, $2 \leq b \leq n$. Chứng minh rằng $\left[\frac{(n-1)!}{b}\right]$ chia hết cho $(b-1)$, trong đó $[x]$ là kí hiệu phần nguyên của số $x$.

**11.** Giả sử $p$ là số nguyên tố lẻ. Chứng minh rằng

a) $1^2.3^2 \ldots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} (\mathrm{mod}\, p)$.

b) $2^2.4^2 \ldots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} (\mathrm{mod}\, p)$.

**12.** Giả sử $p$ là số nguyên tố có dạng $3n+2$. Chứng minh rằng không tồn tại số nguyên $x$ sao cho $(x^2+3)$ chia hết cho $p$.

**13.** Cặp số $(n,\ n+2)$ được gọi là một cặp số nguyên tố sinh đôi nếu $n$, $n+2$ đều là số nguyên tố. Ví dụ $(3,\ 5)$, $(5,\ 7)$, $(11,\ 13)$, $(17,\ 19)$ là các cặp số nguyên tố sinh đôi. Kí hiệu qua $C(x)$ số các cặp số nguyên tố sinh đôi $(n,\ n+2)$ với $n \leq x$. Chứng minh rằng

$$C(x) = 2 + \sum_{7 \leq n \leq x} \sin\left\{(n+2)\left[\frac{n!}{n+2}\right]\right\}\frac{\pi}{2} \sin\left\{n\left[\frac{(n-2)!}{n}\right]\right\}\frac{\pi}{2},$$

trong đó $[x]$ là kí hiệu phần nguyên của số thực $x$.

**14.** Chứng minh rằng nếu số tự nhiên $m$ có dạng $4k+1\,(k>0)$ mà biểu diễn được bởi không ít hơn hai cách dưới dạng tổng hai số chính phương thì $m$ là hợp số.

**15.** Tìm tất cả các số tự nhiên $n$ sao cho tồn tại các số nguyên $a_1, \ldots, a_n$ thỏa mãn đẳng thức sau :

$$n = \sum_{i=1}^{n} a_i = a_1 a_2 \ldots a_n.$$

**16.** Tìm tất cả các số tự nhiên $m$ sao cho nếu $m^n \equiv 1 \pmod{n}$ với số tự nhiên $n$ nào đó thì $m \equiv 1 \pmod{n}$.

**17.** Chứng minh rằng không tồn tại 14 số nguyên dương liên tiếp mà mỗi số đều có ước nguyên tố $p$ trong khoảng $2 \le p \le 11$.

**18.** Giả sử $p$ là số nguyên tố, $r$ là số tự nhiên nhỏ hơn $p$ sao cho

$$(-1)^r r! \equiv 1 \pmod{p} \tag{1}$$

Chứng minh rằng

$$(p-r-1)! + 1 \equiv 0 \pmod{p} \tag{2}$$

**19.** Cho $n+1$ số tự nhiên $a_1$, $a_2$, ... , $a_{n+1}$, sao cho $a_j \le 2n$ với mọi $j = 1, \ldots, n+1$. Chứng minh rằng có ít nhất một số thuộc dãy chia hết cho một số khác cùng dãy đó.

**20.** Giả sử $m$, $n$ là các số nguyên dương, $n > 2$. Chứng minh rằng $(2^m + 1)$ không chia hết cho $(2^n - 1)$.

**21.** Chứng minh rằng tồn tại số nguyên dương $k$ sao cho số $k2^n + 1$ là hợp số với mọi số nguyên dương $n$.

**22.** Chứng minh rằng

$$\frac{[a,b,c]^2}{[a,b][b,c][c,a]} = \frac{(a,b,c)^2}{(a,b)(b,c)(c,a)}.$$

**23.** Tìm $N_0$ có $n$ chữ số $N_0 = a_1 a_2 \ldots a_n$ $(a_1 \neq 0)$ sao cho khi chuyển $k$ chữ số đầu tiên $(k = 1, 2, \ldots, n-1)$ vào cuối, ta được các số (cả thảy có $(n-1)$ số) $N_1 = a_2 \ldots a_n a_1$, $N_2 = a_3 \ldots a_n a_1 a_2$, ... , $N_{n-1} = a_n a_1 a_2 \ldots a_{n-1}$, mỗi số đều là bội của $N_0$.

**24.** Cho số nguyên dương $n$ và cho hai số nguyên tố cùng nhau $a$, $b > 1$. Giả sử $p$, $q$ là hai ước lẻ lớn hơn 1 và nguyên tố cùng nhau của $a^{6^n} + b^{6^n}$. Hãy tìm số dư trong phép chia $p^{6^n} + q^{6^n}$ cho $6.(12)^n$.

**25.** Cho $A$ là số chẵn, $B$ là số lẻ, $A, B > 0$. Giả sử $n$ là số tự nhiên tùy ý. Chứng minh rằng tồn tại số mà các chữ số của nó chỉ gồm các chữ số

của $A$, $B$ và chia hết cho $2^n$.

**26.** Cho đa thức

$$P(x) = x^{2003} - x^{1000} + 1.$$

Tồn tại hay không các số tự nhiên $a_1, \ldots, a_{2004}$ sao cho tích $P(a_i)P(a_j)$ chia hết cho $a_i a_j$ với mọi $i \neq j$.

**27.** Đặt

$$a_n = 2^{2^n} + 2^{2^{n-1}} + 1.$$

Chứng minh rằng, với mọi $n$ nguyên dương, số $a_n$ có không ít hơn $n$ ước nguyên tố.

**28.** Giả sử $m$, $p$ là các số nguyên tố khác nhau. Chứng minh rằng nếu với số tự nhiên nào đó, $p$ là ước của số $(x^{m-1} + x^{m-2} + \cdots + 1)$ thì ta có $p \equiv 1 \pmod{m}$.

**29.** Các số tự nhiên $a$, $b$, $c$, $d$, $e$ thỏa mãn điều kiện

$$a^4 + b^4 + c^4 + d^4 = e^4.$$

Chứng minh rằng có ít nhất

a) ba số chẵn ;

b) ba số chia hết cho 5 ;

c) hai số chia hết cho 10.

**30.** Giả sử $d = (a, b)$, $n$ là số nguyên lớn hơn 1. Chứng minh rằng nếu $\dfrac{b}{d}$ lẻ thì $(n^a + 1, n^b - 1) \leq 2$.

**31.** Giả sử $r$, $a$ là các số tự nhiên lớn hơn 1. Với những giá trị nào của $r$ thì với mọi $n$ tùy ý, từ $n^r \equiv n \pmod{10^a}$ suy ra $n^2 \equiv n \pmod{10^a}$.

**32.** Với các giá trị nào của $n$ thì mọi hệ số trong khai triển nhị thức $(a+b)^n$ đều lẻ ?

**33.** Cho $n$ là số tự nhiên, $\alpha$ là số thực. Đặt :

$$S_n(\alpha) = \sum_{j=0}^{n-1} \left[ \sqrt{\alpha + \frac{j}{n}} \right],$$

trong đó $[x]$ là kí hiệu phần nguyên của số thực $x$.

a) Chứng minh rằng nếu $[\alpha]+1$ không phải là số chính phương thì

$$S_n(\alpha) = n[\sqrt{\alpha}].$$

b) Chứng minh rằng nếu $[\alpha]+1$ là số chính phương thì

$$S_n(\alpha) = n[\sqrt{\alpha}] + [n(\alpha - [\sqrt{\alpha}])].$$

**34.** Cho hàm $J(n)$ xác định trên tập hợp các số nguyên không âm bởi các điều kiện sau :

a) $J(0) = J(1) = 2$ ;

b) $J(n+1) = J(n) + \left[\dfrac{J(n-1)}{2}\right]$ với mọi $n \geq 1$, trong đó $[x]$ là kí hiệu phần nguyên của số thực $x$. Chứng minh rằng

$$[(J(n)+1)(\sqrt{3}-1)] = J(n-1) \text{ với mọi } n \geq 1.$$

**35.** Chứng minh rằng, với mọi số nguyên không âm $n$ ta có

$$[\sqrt{n} + \sqrt{n+1} + \sqrt{n+2}] = [\sqrt{9n+8}],$$

trong đó $[x]$ là kí hiệu phần nguyên của số thực $x$.

**36.** Chứng minh rằng phần nguyên của căn bậc 4 của tích 8 số tự nhiên liên tiếp bằng $n^2 + 7n + 6$, trong đó $n$ là số bé nhất trong 8 số đã chọn.

**37.** Chứng minh rằng

$$n - 1 = \sum_{k=1}^{\infty} \left[\frac{n + 2^{k-1} - 1}{2^k}\right],$$

trong đó [ ] dùng để chỉ phần nguyên.

**38.** a) Chứng minh rằng

$$[5x] + [5y] \geq [3x + y] + [3y + x]$$

trong đó $x$, $y \geq 0$.

b) Sử dụng a), chứng minh rằng

$$\frac{(5m)!(5n)!}{m!\,n!(3m+n)!(3n+m)!}$$

là số nguyên với mọi $m$, $n$ nguyên dương.

**39.** Cho $a_0 < a_1 < \cdots < a_n$ là các số tự nhiên. Chứng minh rằng

$$\frac{1}{[a_0,\ a_1]} + \frac{1}{[a_1,\ a_2]} + \cdots + \frac{1}{[a_{n-1},\ a_n]} \leq 1 - \frac{1}{2^n},$$

trong đó $[a,\ b]$ là kí hiệu bội chung nhỏ nhất của $a$, $b$.

**40.** Tìm tất cả các số tự nhiên $n$ có tính chất $n$ chia hết cho $\varphi(n)$, trong đó $\varphi$ là hàm Ơle.

**41.** Giả sử một số hoàn hảo nào đó có $n$ ước nguyên tố khác nhau. Chứng minh rằng trong các ước nguyên tố đó có ít nhất một số không vượt quá $n$.

**42.** Giả sử $a$, $m$ là các số tự nhiên tùy ý. Chứng minh rằng dãy

$$1,\ a,\ a^a,\ a^{a^a},\ \ldots \pmod m$$

từ lúc nào đó là hằng số.

**43.** Chứng minh rằng với mọi số $n$ tự nhiên $\geq 2$, ta có :

$$\sigma(n) + \varphi(n) \geq 2n \quad (n \geq 2).$$

**44.** a) Kí hiệu qua $T$ tập hợp các tam giác trong mặt phẳng mà các đỉnh có tọa độ là các số nguyên, đồng thời số đo của các cạnh cũng là số nguyên. Chứng minh rằng tam giác cân tuỳ ý thuộc $T$ là hợp của hai tam giác vuông cân thuộc $T$.

b) Kí hiệu qua $V$ tập hợp các tam giác trong không gian mà các đỉnh có tọa độ nguyên. Tồn tại hay không một tam giác đều thuộc $V$ có số đo của các cạnh là nguyên ?

**45.** Xét các tam giác với số đo các cạnh $x-1$, $x$, $x+1$, chiều cao $h$ hạ xuống cạnh $x$, diện tích $S$ đều là các số nguyên. Chứng minh rằng các quan hệ truy hồi sau đây sinh ra tất cả các tam giác như vậy :

$$x_{n+2} = 4x_{n+1} - x_n;\ h_{n+2} = 4h_{n+1} - h_n;\ S_{n+2} = 14S_{n+1} - S_n.$$

**46.** Tìm tất cả các số tự nhiên $m$, $n$ sao cho $2^m + 3^n$ là số chính phương.

**47.** Tìm tất cả các số tự nhiên $x$, $y$ thỏa mãn phương trình :

$$x^y - y^x = x + y.$$

**48.** Tồn tại hay không các số tự nhiên $a$, $b$, $m$, $n$ ; $a \neq b$, $n \geq 2$, $m \geq 2$ thỏa mãn hệ sau :

$$\underbrace{a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}}_{n \text{ lần}} = \underbrace{b^{b^{\cdot^{\cdot^{\cdot^{b}}}}}}_{m \text{ lần}}.$$

**49.** Tìm tất cả các số nguyên không âm $x$, $y$, $z$ thỏa mãn phương trình sau

$$\sqrt{xyz} - \sqrt{x} - \sqrt{y} - \sqrt{z} = 2.$$

**50.** Tìm tất cả các số tự nhiên $a$, $b$, $c$, $d$ khác nhau đôi một sao cho $(abcd - 1)$ chia hết cho tích $(a-1)(b-1)(c-1)(d-1)$.

**51.** Tìm tất cả các số tự nhiên $n$ để tồn tại các số tự nhiên $(x, y, z)$ sao cho $(x+y+z)^2$ chia hết cho $nxyz$.

**52.** Giả sử $s$ là số tự nhiên có $k$ ước số dương lẻ và khác $0$. Chứng minh rằng $s$ có thể viết được theo $k$ cách khác nhau dưới dạng tổng của không ít hơn hai số tự nhiên liên tiếp.

**53.** Phương trình sau đây có nghiệm nguyên hay không :

$$(x+1)^2 + a^2 = (x+2)^2 + b^2 = (x+3)^2 + c^2 = (x+4)^2 + d^2.$$

**54.** Tìm các nghiệm của phương trình

$$y^2 = 1 + x + x^2 + x^3 + x^4.$$

**55.** Tìm các bộ số nguyên $x$, $y$, $z$ thỏa mãn hệ phương trình

$$\begin{cases} x + y + z = m & (1) \\ x^2 + y^2 + z^2 = n & (2) \end{cases}$$

trong đó $m$, $n$ là các số nguyên.

**56.** Giả sử $x$, $y$, $n$ là các số nguyên dương, $x$ và $y$ nguyên tố cùng nhau. Chứng minh rằng mọi ước lẻ của số $x^{2^n} + y^{2^n}$ đều có dạng $2^{n+1}m + 1$.

**57.** Tìm số nguyên $n > 1$ nhỏ nhất sao cho

$$\left(\frac{1^2 + \cdots + n^2}{n}\right)^{\frac{1}{2}}$$

là số nguyên.

**58.** Tìm các nghiệm nguyên của phương trình sau :

$$x^2 + y^2 + z^2 = x^2y^2.$$

**59.** Tìm tất cả các số nguyên dương $n$ sao cho phương trình sau đây có nghiệm $x$, $y$, $u$, $v$ nguyên dương :

$$(x+y+u+v)^2 = n^2xyuv. \qquad (1)$$

**60.** a) Tìm 11 số tự nhiên liên tiếp mà tổng các bình phương của chúng là số chính phương.

b) Chứng minh khi $2 < n < 11$, không tồn tại $n$ số tự nhiên liên tiếp có tính chất trên.

**61.** Tìm tất cả các số nguyên dương $n$ sao cho phương trình

$$x^3 + y^3 + z^3 = nx^2y^2z^2$$

có nghiệm nguyên dương.

**62.** Chứng minh rằng phương trình

$$4x^n + (x+1)^2 = y^2,$$

$n$ nguyên dương, chỉ có nghiệm nguyên dương $(x,\ y)$ khi $n = 2$.

**63.** a) Chứng minh rằng, tổng $x^2 + y^2$ với $x$, $y$ nguyên không thể là số chính phương nếu $x$, $y$ không chia hết cho 3.

b) Chứng minh rằng nếu $x^2 + y^2 = z^2$, $x$, $y$ nguyên thì ít nhất một trong ba số $x$, $y$, $z$ chia hết cho 5.

**64.** a) Chứng minh rằng tồn tại vô hạn số tự nhiên $a$ sao cho $a+1$ và $3a+1$ đều là số chính phương.

b) Cho $a_1 < a_2 < \cdots$ là dãy tất cả các số thỏa mãn tính chất a). Chứng minh rằng $a_n a_{n+1} + 1$ là số chính phương với mọi $n \geq 1$.

**65.** Cho dãy số $\{x_n\}$ xác định bởi các điều kiện sau :

i) $x_0 = 0,\ x_1 = 1,\ x_2 = 0$ ;

ii) Với mọi $n \geq 1$,

$$x_{n+3} = \frac{(n^2+n+1)(n+1)}{n}x_{n+2} + (n^2+n+1)x_{n+1} - \frac{n+1}{n}x_n.$$

Chứng minh rằng $x_n$ là số chính phương với mọi $n \geq 0$.

**66.** Tìm công thức tính số hạng tổng quát $u_n$ theo các số hạng $u_0$, $u_1$ của dãy số $\{u_n\}$ xác định bởi quan hệ sau :

$$u_{n+2} = 2(2n+3)^2 u_{n+1} - 4(n+1)^2(2n+1)(2n+3)u_n$$

với $n \geq 0$.

**67.** Tìm tất cả các số nguyên $a$, $b$ sao cho $(a^2 + b^2 + 1)$ chia hết cho tích $ab$.

**68.** Tìm các cặp số tự nhiên $(m, n)$ sao cho $1 \leq m \leq n$, $m^2 \equiv -1 \pmod{n}$, $n^2 \equiv -1 \pmod{m}$.

**69.** Cho dãy số $\{y_n\}$ xác định bởi các điều kiện sau :

i) $y_2 = y_3 = 1$ ;

ii) $(n+1)(n-2)y_{n+1} = n(n^2 - n - 1)y_n - (n-1)^3 y_{n-1}$, với $n \geq 1$.

Tìm tất cả các giá trị của $n$ để $y_n$ là số nguyên.

**70.** Cho dãy số nguyên $\{a_n\}$, xác định bởi $a_0 = 1$, $a_n = a_{n-1} + a_{[n/3]}$ với mọi $n \geq 1$. Chứng minh rằng với mỗi số nguyên tố $p \leq 13$, tồn tại vô số số tự nhiên $k$ sao cho $a_k \vdots p$.

**71.** Tính tổng $k$ số hạng đầu tiên của dãy $\{x_n\}$ cho bởi công thức truy hồi sau :

$$x_1 = \frac{2}{3}, \quad x_{n+1} = \frac{x_n}{2(2n+1)x_n + 1}.$$

**72.** Tìm công thức tính số hạng tổng quát $a_n$ của dãy cho bởi công thức truy hồi sau :

$$a_0 = 20, \ a_1 = 100, \ a_{n+2} = 4a_{n+1} + 5a_n + 20$$

với $n \geq 1$.

**73.** Tìm tất cả các cặp số nguyên dương $(m, n)$ sao cho

$$|n^2 - mn - m^2| = 1.$$

**74.** Chứng minh rằng, tồn tại $n$ thoả mãn

$$\tau(n^2) = k\,\tau(n)$$

khi và chỉ khi $k$ là số lẻ.

**75.** Khi kiểm tra tính nguyên tố của số Mersenne, người ta thường dùng dãy truy hồi sau :

$$a_1 = 3,\ a_{n+1} = a_n^2 - 2,\ n \geq 1.$$

Chứng minh rằng $a_k = \dfrac{F_{2^{k+1}}}{F_{2^k}}$ $(k \geq 1)$, trong đó $F_k$ là số Fibonacci thứ $k$.

**76.** Cho dãy số tự nhiên $a_1, a_2, \ldots, a_n$ thỏa mãn :

$$0 < a_1 < a_2 < \cdots < a_n \leq 2n,\ n \neq 4 \text{ và } n \geq 3.$$

Chứng minh rằng

$$\min[a_i, a_j] \leq 6\left(\left[\frac{n}{2}\right] + 1\right),$$

trong đó $[a_i, a_j]$ là bội chung nhỏ nhất của hai số $a_i$, $a_j$.

**77.** Tìm tất cả các hàm số $f(x, y)$ xác định với mọi $(x, y)$ là số tự nhiên, nhận giá trị trong tập hợp các số tự nhiên và thỏa mãn các điều kiện sau với mọi số tự nhiên $x$, $y$ :

i) $f(x, y) = f(y, x)$ ;

ii) $f(x, x) = f(x)$ ;

iii) $(y - x)f(x, y) = yf(x, y - x)$ nếu $y > x$.

**78.** Chứng minh rằng căn bậc 3 của ba số nguyên tố khác nhau không thể là ba số hạng (không nhất thiết liên tiếp) của một cấp số cộng nào đó.

**79.** Kí hiệu qua $\pi(n)$ số các số nguyên tố không vượt quá $n$. Giả sử $a_1$, $a_2, \ldots, a_m$ là dãy các số tự nhiên nào đó thỏa mãn :

i) Không có $a_i$ nào là ước của tích các số còn lại.

ii) $a_1 < a_2 < \cdots < a_m \leq n$.

Tìm giá trị lớn nhất có thể của $m$.

**80.** Phân số có tử số bằng 1, mẫu số là số tự nhiên được gọi là phân số đơn dương. Hỏi có bao nhiêu cách biểu diễn phân số $\dfrac{1}{n}$ ($n$ là số tự nhiên) dưới dạng :

a) Tổng hai phân số đơn dương ;

b) Hiệu hai phân số đơn dương.

**81.** Xét một khoảng mở có độ dài $1/n$ của trục thực ($n$ là số tự nhiên). Tìm số cực đại các phân số tối giản dạng $p/q$ với $1 \le q \le n$ được chứa trong khoảng nói trên.

**82.** Giả sử $m$, $n$ là các số nguyên lẻ và $(n^2-1)$ chia hết cho $|m^2+1-n^2|$. Chứng minh rằng $|m^2+1-n^2|$ là số chính phương.

**83.** Số nguyên $n$ được gọi là *tốt* nếu có thể viết dưới dạng

$$n = a_1 + a_2 + \cdots + a_k,$$

trong đó $a_1, a_2, \ldots, a_k$ là các số nguyên dương (không nhất thiết khác nhau) thỏa mãn :

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} = 1.$$

Biết rằng $n$ tốt nếu $33 \le n \le 73$. Chứng minh rằng mọi số $n \ge 33$ đều là số tốt.

**84.** Chứng minh rằng nếu số chính phương $n$ là hiệu của các lập phương của hai số tự nhiên liên tiếp thì $\sqrt{n}$ là tổng các bình phương của hai số tự nhiên liên tiếp.

**85.** Giả sử $r$ là một số vô tỉ dương. Chứng minh rằng giữa hai số tự nhiên liên tiếp có một và chỉ một số hạng của một trong hai dãy sau đây :

$$(1+r),\ 2(1+r),\ 3(1+r),\ \ldots$$
$$\left(1+\frac{1}{r}\right),\ 2\left(1+\frac{1}{r}\right),\ 3\left(1+\frac{1}{r}\right),\ \ldots$$

**86.** Giả sử $f(x)$ là đa thức với hệ số hữu tỉ, bậc $\ge 2$ ; $a_1$, $a_2$ ... là dãy số hữu tỉ thỏa mãn điều kiện $f(a_{n+1}) = a_n$, $n \ge 1$. Chứng minh rằng tồn tại $k \ge 1$ để $a_{n+k} = a_n$ $(n \ge 1)$.

**87.** Với mọi số tự nhiên $m$, $n$, chứng minh rằng $(n!)$ chia hết cho $m$ khi và chỉ khi tồn tại đa thức hệ số nguyên

$$f(x) = \sum_{k=0}^{n} a_k x^k$$

thỏa mãn : $(a_0, a_1, \ldots, a_n, m) = 1$, $m \mid f(j)$ với mọi $j$ nguyên dương.

**88.** Giả sử $m$ là số tự nhiên, $p$ là một ước nguyên tố của $m$. Giả sử $n$, $k$ là các số tự nhiên thỏa mãn

$$p \le n,\ m \le n^{\frac{k+1}{2}}.$$

Chứng minh rằng $m$ biểu diễn được dưới dạng tích của $k$ số tự nhiên, mỗi số không vượt quá $n$.

**89.** Chứng minh rằng tồn tại vô hạn cặp $(m,\ m+1)$ các số tự nhiên liên tiếp sao cho mọi ước nguyên tố của $m$ và $m+1$ đều tham gia khai triển với số mũ lớn hơn 1.

**90.** Giả sử $a$ là số nguyên lớn hơn 4, $f(n)$ và $g(n)$ là hai dãy số nguyên xác định bởi 3 điều kiện sau :

i) $f(1) = 1$ ;

ii) $g(n) = na - 1 - f(n)$ ;

iii) $f(n+1)$ là số tự nhiên nhỏ nhất khác với các số $f(1)$, ... , $f(n)$, $g(1)$, ... , $g(n)$.

Chứng minh rằng tồn tại các hằng số $\alpha$, $\beta$ sao cho với mọi $n$ ta có

$$f(n) = [\alpha n],\ g(n) = [\beta n].$$

(Kí hiệu $[x]$ dùng để chỉ phần nguyên của $x$).

**91.** Giả sử dãy $a_1 < a_2 < \cdots$ là dãy vô hạn các số nguyên dương. Chứng minh rằng tồn tại dãy con vô hạn sao cho trong đó không có số hạng nào là bội của số khác cùng dãy con đó, hoặc tồn tại dãy con vô hạn mà mỗi số hạng đều là bội của các số trước nó.

**92.** Giả sử $a$, $b$ là các số nguyên lớn hơn 1, thỏa mãn điều kiện : $(b^n - 1) \mid (a^n - 1)$ với mọi $n$ nguyên dương. Chứng minh rằng tồn tại $k$ nguyên để $a = b^k$.

**93.** Ta lập 7 số có 7 chữ số từ các số 1, 2, ... , 7 lấy theo thứ tự khác nhau. Chứng minh rằng tổng các lũy thừa bậc 7 của một số số trong các số trên không thể bằng tổng các lũy thừa bậc 7 của các số còn lại.

**94.** Cho $n$ là số lẻ. Chứng minh rằng tích của $n$ số tự nhiên liên tiếp chia hết cho tổng của chúng, trừ khi $n$ là số nguyên tố.

**95.** Cho $n$ số thực tùy ý $a_1$, ... , $a_n$. Chứng minh rằng có thể chọn được một số số trong chúng (có thể chỉ 1 số) sao cho tổng các số đã chọn sai khác với số nguyên gần tổng đó nhất không quá $1/(n+1)$.

**96.** Với mỗi một tập con $T$ hữu hạn khác rỗng của tập hợp các số nguyên

dương, đặt $P(T)$ = tích các số thuộc $T$, $M(T)$ = max các số thuộc $T$, $m(T)$ = min các số thuộc $T$. Cho $m$ là số tự nhiên sao cho $m$ có ước nguyên tố $p > \sqrt{2m} + 1$. Tìm giá trị $M$ nhỏ nhất để tồn tại tập hợp $T$ có $m(T) = m$, $M(T) = M$ và $P(T)$ là số chính phương.

**97.** Tìm số nguyên dương $N$ lớn nhất sao cho các số nguyên chia hết cho 3 trong tập hợp $\{1, 2, \ldots, N\}$ bằng số các số nguyên trong tập hợp đó mà chia hết cho 5 hoặc 7.

**98.** Với mỗi số nguyên dương $n$, kí hiệu $S(n)$ là tổng các chữ số trong biểu diễn thập phân của $n$. Mỗi số nguyên dương nhận được bằng cách xóa một số chữ số tận cùng của $n$ (số chữ số bị xóa ít nhất là một) gọi là một giản số của $n$. Gọi $T(n)$ là tổng tất các các giản số của $n$. Chứng minh $n = S(n) + 9T(n)$.

**99.** Cho dãy các số nguyên dương $a_1 < a_2 < \cdots < a_n < 2n$, sao cho không có hai số nào của dãy chia hết cho nhau. Giả sử $k$ là số xác định bởi $3^k < 2n < 3^{k+1}$. Chứng minh rằng $a_1 \geq 2^k$.

**100.** Tìm tất cả các đa thức hệ số hữu tỉ $P(x)$ sao cho $P(x)$ nhận giá trị hữu tỉ khi và chỉ khi $x$ là số hữu tỉ.

**101.** Viết trên bảng các số 1, 2, ..., 2004. Có hai người chơi theo quy tắc sau. Đến lượt, mỗi người có quyền xóa hai số tùy ý $a$, $b$ trên bảng và thay vào đó số $a^b$. Trò chơi kết thúc khi trên bảng còn lại một số. Nếu số đó tận cùng là 2, 3, 7, 8 thì người đi trước được xem là thắng. Nếu ngược lại thì người đi sau thắng. Hỏi ai là người có chiến lược thắng trong trò chơi này ?

**102.** Xét các cấp số cộng hữu hạn số hạng (không ít hơn 3 số hạng), sao cho tích các số hạng là một ước của số có dạng $n^2 + 1$, với $n$ nào đó :

a) Chứng minh rằng tồn tại cấp số cộng như trên với công sai là 12.

b) Chứng minh rằng không tồn tại cấp số cộng như trên với công sai là 10 hoặc 11.

c) Cấp số cộng có công sai 12 và thỏa mãn tính chất đã nêu có thể có nhiều nhất là bao nhiêu số hạng ?

**103.** Chứng minh rằng, với mọi số tự nhiên $n$, ta có :

$$\left|\left\{\frac{n}{1}\right\} - \left\{\frac{n}{2}\right\} + \left\{\frac{n}{3}\right\} - \cdots - (-1)^n \left\{\frac{n}{n}\right\}\right| < \sqrt{2n},$$

trong đó $\{a\}$ là kí hiệu phần lẻ của $a$.

# B. LỜI GIẢI

**1.** a) Nếu $\dfrac{x+y}{2}$ thuộc $S$ thì trong khai triển cơ số $4$ của $(x-y)$ chỉ có chữ số $0$ và $2$. Do $x \neq y$ nên trong khai triển của $(x+y)$ ở cơ số $4$ phải chứa chữ số $1$, vì ít nhất tại vị trí nào đó, $x$, $y$ có chữ số khác nhau, mà chúng thuộc $S$ nên một số có chữ số $0$, số kia có chữ số $1$. Vậy $\dfrac{x+y}{2}$ không thể thuộc $S$.

b) Ta chỉ cần chứng minh rằng, với mọi $x$ không thuộc $S$, tồn tại $z$, $y$ thuộc $S$ sao cho $\dfrac{x+y}{2} = z$.

Ta viết các khai triển trong cơ số $4$:

$$x = \sum_{i=0}^{N} x_i 4^i, \quad (0 \leq x_i \leq 3).$$

$$t = \sum_{i=0}^{N+1} 4^i$$

$$x + t = \sum_{i=0}^{N+1} u_i 4^i, \quad (0 \leq u_i \leq 3).$$

Với mỗi $u_i$, ta xác định $y_i$, $z_i$ cho bởi bảng sau:

| $u_i$ | $y_i$ | $z_i$ |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 2 | 1 | 1 |
| 3 | 0 | 1 |

Giả sử $y$ , $z$ là các phân tử cho bởi :

$$y = \sum_{i=0}^{N+1} y_i 4^i$$

$$z = \sum_{i=0}^{N+1} z_i 4^i$$

Vì mỗi dòng của bảng nói trên thỏa mãn đẳng thức $2z_i + 1 = u_i + y_i$ nên ta có

$$2z - y = \sum_{i=0}^{N+1} (2z_i - y_i)4^i = \sum_{i=0}^{N+1} (u_i - 1)4^i = u - t = x.$$

Vậy, $z = \dfrac{y + x}{2}$.

**2.** Giả sử số 2101 là số chính phương trong cơ số $r$. Ta có :

$$2101 = 2r^3 + r + 1.$$

Viết 2101 dưới dạng :

$$2101 = s(r + 1),$$

trong đó

$$s = 2r^2 - r + 1 = 2r(r - 1) + r + 1.$$

Nếu $t$ là ước chung của $s$ và $r + 1$ thì $t$ là ước chung của $(r + 1)$ và $2r(r - 1)$, do đó $t$ là ước chung của $(r + 1)$ và $2(r - 1)$ $\Rightarrow$ $t \mid (2r - 2 - r - 1) \Rightarrow t \mid (r - 3) \Rightarrow t \mid [(r + 1) - (r - 3)] \Rightarrow t \mid 4$ .

Theo giả thiết, $s(r + 1)$ là số chính phương :

$$s(r + 1) = k^2.$$

Giả sử $p$ là một ước nguyên tố của $k^2$. Khi đó, $p^2 \mid s$, hoặc $p^2 \mid (r + 1)$, hoặc $p$ là ước chung của $s$ và $(r + 1)$, tức là $p^2 = 4$. Như vậy, $s$ và $(r + 1)$ hoặc đều là số chính phương, hoặc đều là hai lần một số chính phương. Ta xét hai trường hợp :

a) $r + 1 = n^2$. Do $r \leq 10$, suy ra $n \leq 3$.

Với $n = 2$, ta được $r = 3$, $s = 16$, $(2001)_3 = (22)_3^2$.

Với $n = 3$, ta được $r = 8$, $s = 121$, $(2001)_8 = (1103)_8^2$.

b) $r + 1 = 2n^2 \Rightarrow n \leq 2$. Với $n = 2$, ta có $r = 7$.

Thử trực tiếp cho thấy nghiệm này không thỏa mãn. Vậy, 2101 là số chính phương trong cơ số 3 và 8.

**3.** Ta thấy các đẳng thức sau đây là tương đương :

$$a = 3b - c \Leftrightarrow b^2 + 1 = (3b - c)c \Leftrightarrow b^2 + c^2 + 1 = 3bc \Leftrightarrow d = 3c - b.$$

Vậy, chỉ cần chứng minh rằng, nếu $c$ là ước của $b^2 + 1$, $b$ là ước của $c^2 + 1$ thì ta có $b^2 + c^2 + 1 = 3bc$.

Giả sử $b \leq c$. Ta chứng minh quy nạp theo tổng $b + c$. Nếu $b + c = 2$ thì $b = c = 1$ điều cần chứng minh là đúng. Nếu $c > 1$, $b \neq c$ thì $b \leq c - 1$ nên $b^2 + 1 < c^2$, suy ra $a < c$. Từ các đẳng thức $b^2 + 1 = ac$, $c^2 + 1 = bd$ suy ra $(b^2 + 1)^2 = a^2(bd - 1)$. Do đó

$$1 \equiv -a^2 \pmod{b}.$$

Vậy $b \mid (a^2 + 1)$. Do $a \mid (b^2 + 1)$ mà $(a + b) < (b + c)$ nên theo giả thiết quy nạp,

$$a^2 + b^2 + 1 = 3ab.$$

Vậy :

$$(b^2 + 1)^2 = a^2c^2 = (3ab - b^2 - 1)c^2 = 3abc^2 - (b^2 + 1)c^2.$$

Suy ra

$$(b^2 + 1)(b^2 + c^2 + 1) = 3abc^2 = 3bc(b^2 + 1).$$

Từ đó

$$b^2 + c^2 + 1 = 3bc.$$

**4.** Giả sử $p$ là ước nguyên tố của $x$, khi đó $p \leq n$ nên $p \mid n!$. Giả sử trong khai triển của $x$, $p$ có số mũ chẵn là $2s$, $s \geq 1$. Ta có

$$p^{2s} \leq x \leq \frac{n^2}{4}.$$

Suy ra

$$2p^s \leq n.$$

Như vậy, số mũ của $p$ tham gia trong khai triển của $n!$ sẽ lớn hơn hoặc bằng $2p^{s-1} \geq 2s$. Do đó $p^{2s} \mid n!$. Ta xét trường hợp lũy thừa cao nhất của $p$ trong khai triển của $x$ là số lẻ $2s+1$, $s \geq 1$. Khi đó

$$p^{2s+1} \leq \frac{n^2}{4} \Rightarrow n \geq 2\sqrt{p}.p^s.$$

Ta xét hai trường hợp :

a) $4p^s < n$. Khi đó $p^{2s+1} \mid n!$

b) $4p^s \geq n \Rightarrow 4p^s \geq n > 2\sqrt{p}.p^s \Rightarrow 2 \geq \sqrt{p} \Rightarrow 2\sqrt{p} \geq p \Rightarrow n \geq p^{s+1}$.

Như vậy, số mũ của $p$ trong $n!$ sẽ lớn hơn hoặc bằng

$$p^s + p^{s-1} + \cdots + p + 1 \geq 2^s + 2^{s-1} + \cdots + 2 + 1 = 2^{s+1} - 1 \geq 2s + 1.$$

Suy ra $p^{2s+1} \mid n!$.

Vì $p$ đang xét là ước nguyên tố tùy ý của $x$ nên suy ra $x \mid n!$.

5. Ta có :

$$n - 1 = \frac{2^{2p} - 1}{3} - 1 = \frac{4(2^{p-1} + 1)(2^{p-1} - 1)}{3}.$$

Vì $p$ là số nguyên tố lẻ nên

$$2^{p-1} \equiv 1 \pmod 3.$$

Mặt khác, theo Định lí Fermat bé,

$$2^{p-1} \equiv 1 \pmod p.$$

Vậy, nếu $p > 3$ thì

$$2^{p-1} - 1 \vdots 3p,$$

do đó

$$n - 1 \vdots 2p.$$

Từ đó suy ra

$$(2^{p-1} - 1) \vdots (2^{2p} - 1).$$

Nhưng $(2^{p-1} - 1) \vdots n$ nên suy ra

$$2^{n-1} - 1 \equiv 0 \pmod{n},$$

tức là

$$2^n - 2 \equiv 0 \pmod{n}.$$

**6.** Trước hết, ta chứng minh đẳng thức sau với mọi $n$ nguyên dương

$$\prod_{k=1}^{n-1} k! = \prod_{k=1}^{n-1} (n-k)! = \prod_{k=1}^{n-1} k^{n-k}. \tag{1}$$

Đẳng thức thứ nhất nhận được khi thay $k$ bởi $(n-k)$, vì ta có hai tích gồm các thừa số như nhau với thứ tự đảo ngược. Để chứng minh đẳng thức thứ hai, ta thấy :

$$\prod_{k=1}^{n-1} k! = (1).(1.2).(1.2.3)\ldots(1.2\ldots n-1).$$

Như vậy :

số 2 xuất hiện $n-2$ lần,

số 3 xuất hiện $n-3$ lần,

...

số $(n-1)$ xuất hiện 1 lần.

Từ đó suy ra đẳng thức. Vậy :

$$Q(n) = \prod_{k=1}^{n-1} \frac{k^{n-1}}{k^{2n-2k}} = \frac{\left(\prod_{k=1}^{n-1} k\right)^{n-1}}{\left(\prod_{k=1}^{n-1} k^{n-k}\right)^2}$$

$$= \frac{[(n-1)!]^{n-1}}{\prod_{k=1}^{n-1}[k!(n-k)!]} = \prod_{k=1}^{n-1} \frac{C_n^k}{n}.$$

Khi $n$ là số nguyên tố thì $n \mid C_n^k$ nên $Q(n)$ là số nguyên.

**7.** Theo tính chất của các số nhị thức, ta có

$$C_{2n}^1 + C_{2n}^3 + \cdots + C_{2n}^{2n-1} = 2^{2n-1}.$$

Như vậy, ước chung của các số $C_{2n}^1$, $C_{2n}^3$, ... , $C_{2n}^{2n-1}$ có dạng $2^p$. Ta

cần tìm số $p$ lớn nhất có thể.

Giả sử $n = 2^k q$, trong đó $q$ là số lẻ. Ta có

$$C_{2n}^{1} = 2^{k+1} q,$$

nên ước chung của các số đang xét $\leq 2^{k+1}$. Ta chứng minh ước chung đó chính là $2^{k+1}$. Ta có :

$$C_{2^{k+1}q}^{p} = \frac{2^{k+1} q}{p} C_{2^{k+1}q-1}^{p-1}. \tag{1}$$

Vì các số nhị thức là nguyên, và $p$ là số lẻ nên từ (1) suy ra rằng $C_{2^{k+1}q}^{p}$ chia hết cho $2^{k+1}$, tức là

$$C_{2^{k+1}q}^{p} = 2^{k+1} M_p,$$

$M_p$ nguyên, $p = 1, 3, \ldots, 2n-1$. Vậy $2^{k+1}$ là ước chung của các số đang xét, và là ước chung lớn nhất.

**8.** Giả sử $p$ là số nguyên tố, $p$ là ước của tích $d_1, \ldots, d_n$. Gọi $s$ là số lớn nhất sao cho tồn tại $j$, $1 \leq j \leq n$, để $d_j$ chia hết cho $p^s$. Vì $(d_1 + \cdots + d_n)$ chia hết cho $d_j$ nên $(d_1 + \cdots + d_n) \vdots p^s$. Từ đó suy ra $(d_1 + \cdots + d_n)^{n-2} \vdots p^{s(n-2)}$.

Vì $d_1, \ldots, d_n$ không có ước chung khác 1 nên phải tồn tại $d_1$ nào đó không chia hết cho $p$. Mặt khác, do tổng của các $d_i$ chia hết cho $p$ nên ngoài $d_1$ phải có ít nhất một $d_k$ khác cũng không chia hết cho $p$. Như vậy, lũy thừa cao nhất của $p$ chia hết tích $d_1 \ldots d_n$ không vượt quá $s(n-2)$. Vì $p$ được chọn là một ước nguyên tố tùy ý của tích nên ta có

$$(d_1 + \cdots + d_n)^{n-2} \vdots d_1 \ldots d_n.$$

Như vậy, số $k$ nhỏ nhất cần tìm thỏa mãn

$$k \leq n-2.$$

Ta chứng tỏ $k = n-2$, tức là nếu $k \leq n-3$ thì tồn tại $d_1, \ldots, d_n$ thỏa mãn giả thiết bài toán sao cho $(d_1 + \cdots + d_n)^{n-3}$ không chia hết cho tích $d_1 \ldots d_n$. Ta lấy $d_1 = 1$, $d_2 = n-1$, $d_i = n$ với $3 \leq i \leq n$. Khi đó $(d_1 + \cdots + d_n) = n(n-1) \vdots d_i$ với mọi $1 \leq i \leq n$. Mặt khác

$d_1 \ldots d_n = (n-1)n^{n-2}$. Do $(n,\ n-1) = 1$ nên lũy thừa bé hơn $(n-2)$ của tổng $(d_1 + \cdots + d_n)$ không thể chia hết cho tích $d_1 \ldots d_n$.

**9.** Xét dãy $n$, $n-1$, ..., $n-p+1$. Dãy gồm $p$ số tự nhiên liên tiếp nên có đúng một số của dãy chia hết cho $p$, giả sử số đó là $N$. Ta có

$$\frac{N}{p} = \left[\frac{n}{p}\right].$$

Loại số $N$ ra khỏi dãy và xét đồng dư môđulô $p$, ta được dãy $1,\ 2,\ \ldots,\ (p-1) \pmod p$ (xếp theo thứ tự nào đó). Gọi $Q$ là tích các số của dãy (sau khi loại bỏ $N$). Ta có :

$$Q = \frac{n(n-1)\ldots(n-p+1)}{N} \equiv (p-1)!\ (\mathrm{mod}\ p).$$

Suy ra

$$NQ \equiv (p-1)!N\ (\mathrm{mod}\ pN)$$

$$\frac{QN}{p} \equiv (p-1)!\frac{N}{p}\ \ (\mathrm{mod}\ p) \qquad (1)$$

Vì $(p,\ (p-1)!) = 1$ nên ta được

$$\frac{NQ}{p!} \equiv \frac{N}{p}\ (\mathrm{mod}\ p). \qquad (2)$$

Vậy

$$C_n^p \equiv \left[\frac{n}{p}\right]\ \ (\mathrm{mod}\ \ p).$$

**10.** Ta xét 4 trường hợp sau đây :

a) $b < n$

b) $b = n$ là một hợp số, nhưng không là bình phương của một số nguyên tố

c) $b = n = p^2$ với $p$ là số nguyên tố nào đó

d) $b = n = p$, trong đó $p$ là số nguyên tố.

• Trường hợp 1 : $b < n$. Ta có :

$$(n-1)!\ \vdots\ b(b-1),$$

nên $\dfrac{(n-1)!}{b}$ là số nguyên chia hết cho $(b-1)$.

• Trường hợp 2 : $b = n = rs$ với $1 < r < s < n$. Do $(n,\ n-1) = 1$ nên $s < (n-1)$. Suy ra $(n-1)! \ \vdots\ rs(n-1) = b(b-1)$ : ta trở lại như trong trường hợp 1.

• Trường hợp 3 : $b = n = p^2$, $p$ là số nguyên tố. Do $n = p^2 \geq 5$ nên suy ra $1 < p < 2p < p^2 - 1 = n - 1$. Vậy

$$(n-1)! \ \vdots\ p(2p)(n-1) = 2b(b-1),$$

và ta trở về trường hợp 1.

• Trường hợp 4 : $b = n = p$ nguyên tố. Theo Định lí Wilson,

$$(p-1)! + 1 \ \vdots\ p \Rightarrow \left[\frac{(p-1)!}{p}\right] = \left[\frac{(p-1)!+1}{p} - \frac{1}{p}\right]$$

$$= \frac{(p-1)!+1}{p} - 1$$

$$= \frac{(p-1)!-(p-1)}{p}.$$

Rõ ràng $(p-1)$ là ước của tử số, và do $p$, $p-1$ nguyên tố cùng nhau nên $(p-1)$ là ước của thương đang xét.

**11.** a) Theo Đnh lí Wilson ta có :

$$1.2\ldots(p-1) = (p-1)! \equiv -1 \pmod{p}. \qquad (1)$$

Mặt khác, với $i = 0,\ \pm 1,\ \pm 2,\ \ldots$ ta có đồng dư sau :

$$i \equiv -(p-i) \pmod{p}. \qquad (2)$$

Ta thay các số chẵn trong vế trái của (1) (có tất cả $\dfrac{p-1}{2}$ số) bởi số đồng dư với nó trong (2) (với $i = 2,\ 4,\ 6,\ \ldots,\ p-1$). Nhóm các nhân tử lại, ta nhận được :

$$1^2.3^2\ldots(p-2)^2(-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

tức là

$$1^2.3^2\ldots(p-2)^2 \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

b) Tương tự như phần a), ta thay $\frac{p-1}{2}$ số lẻ ở vế trái của (1) bởi số đồng dư với nó trong (2) rồi nhóm các nhân tử, ta nhận được :

$$2^2.4^2\ldots(p-2)^2 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

**12.** Giả sử ngược lại, tồn tại các số nguyên tố $p$ dạng $3n+2$ để phương trình đồng dư

$$x^2 + 3 \equiv 0 \pmod{p} \tag{1}$$

có nghiệm. Gọi $p_0$ là số bé nhất trong các số đó, và giả sử $x = e$ $(< p_0)$ thỏa mãn

$$x^2 + 3 \equiv 0 \pmod{p_0}.$$

Nếu cần thì thay $e$ bởi $(p-e)$, ta xem $e$ chẵn. Xét các trường hợp $e^2 \equiv 1 \pmod{3}$ và $e^2 \equiv 0 \pmod{3}$.

• Trường hợp 1. Từ $e^2 \equiv -3 \pmod{p_0}$ ta có :

$$e^2 = -3 + fp_0,$$

trong đó $f < p_0$ và $f$ lẻ. Như vậy

$$p_0 f = e^2 + 3 \equiv 4 \pmod{3}.$$

Do $p_0 \equiv 2 \pmod{3}$ nên $f \equiv 2 \pmod{3}$. Vậy $f$ lẻ có dạng $3n+2$. Suy ra rằng $f$ phải có ước nguyên tố lẻ $q$ dạng $3n+2$. Ta có

$$e^2 \equiv -3 \pmod{q} \tag{2}$$

Do $q < f < p_0$ nên (2) mâu thuẫn với cách chọn $p_0$.

• Trường hợp 2. $e^2 \equiv 0 \pmod{3}$. Suy ra $e = 3^a k$ với $k \not\vdots 3$ và $a$ nguyên dương. Do $e^2 \equiv -3 \pmod{p_0}$ nên

$$3^{2a}k^2 \equiv -3 \pmod{p_0}.$$

Suy ra

$$3^{2a-1}k^2 \equiv -1 \pmod{p_0},$$

$$3^{2a-1}k^2 + 1 = p_0 h, \quad h < p, \ h \text{ lẻ}.$$

Do đó

$$p_0 h \equiv 1 \pmod 3.$$

Nhưng $p_0 \equiv 2 \pmod 3$ nên $h \equiv 2 \pmod 3$. Suy ra $h$ lẻ, dạng $3n+2$. Do đó tồn tại ước nguyên tố $r$ của $h$ có dạng $3n+2$. Vậy $3^{2a-1}k^2 \equiv -1 \pmod h \equiv -1 \pmod r$, tức là $3^{2a}k^2 \equiv -3 \pmod r$: mâu thuẫn, vì $r < p_0$.

**13.** Nếu $n$ là hợp số và $n > 5$ thì $\dfrac{(n-2)!}{n}$ là số nguyên chẵn, do đó

$$\sin\left\{\frac{\pi}{2} n \left[\frac{(n-2)!}{n}\right]\right\} = 0.$$

Nếu $p$ là số nguyên tố thì theo Định lí Wilson,

$$(p-2)! \equiv -(p-1)! \equiv 1 \pmod p.$$

Do đó

$$\left[\frac{(p-2)!}{p}\right] = \frac{(p-2)!-1}{p}.$$

Vậy, khi $p > 5$, ta có $4 \mid (p-2)!$ nên

$$\sin\left\{\frac{\pi}{2} p \left[\frac{(p-2)!}{p}\right]\right\} = \sin\left\{\frac{\pi}{2} p\left[(p-2)!-1\right]\right\} = -1.$$

Từ đó suy ra rằng, nếu $n > 5$ thì số hạng thứ $n$ bằng $0$ khi $n$ hoặc $n+2$ là hợp số, bằng $(-1)(-1) = 1$ khi $n$ và $n+2$ đều là số nguyên tố. Như vậy,

$$\sum_{7 \le n \le x} \sin\left\{\frac{\pi}{2}(n+2)\left[\frac{n!}{n+2}\right]\right\} \sin\left\{\frac{\pi}{2} n \left[\frac{(n-2)!}{n}\right]\right\}$$

cho ta số các cặp số nguyên tố sinh đôi $(n,\ n+2)$ khi $x \ge n \ge 7$. Để có tất cả các cặp số nguyên nguyên tố sinh đôi $(n,\ n+2)$ với $n \le x$, ta cần thêm vào tổng nói trên 2 cặp : $(3,\ 5)$ và $(5,\ 7)$.

**Ghi chú :** Cho đến nay, người ta vẫn chưa chứng minh được là tồn tại hữu hạn hay vô hạn cặp số nguyên tố sinh đôi.

**14.** Giả sử số $m$ dạng $4k+1$ có hai cách biểu diễn dưới dạng tổng bình phương của hai số :

$$m = x^2 + y^2 = u^2 + v^2.$$

Vì $m$ là số lẻ nên trong mỗi tổng phải có một số lẻ, giả sử $x$ và $u$ lẻ, $y$ và $v$ chẵn. Không giảm tổng quát, giả sử $x > u$. Như vậy $y < v$. Các số $x \pm u$ và $v \pm y$ là các số dương chẵn. Ta viết $m$ dưới dạng :

$$\begin{aligned} m &= \left(\frac{x+u}{2} + \frac{x-u}{2}\right)^2 + \left(\frac{y+v}{2} - \frac{v-y}{2}\right)^2 \\ &= \left(\frac{x+u}{2}\right)^2 + \left(\frac{x-u}{2}\right)^2 + \left(\frac{y+v}{2}\right)^2 + \left(\frac{v-y}{2}\right)^2 \\ &= p^2 + q^2 + r^2 + s^2. \end{aligned}$$

Gọi $a$ là ước chung lớn nhất của $p$ và $r$, và giả sử $p = ab$, $r = ac$, trong đó $(b,c) = 1$. Khi đó ta có : $abq = acs \Rightarrow bq = cs$. Vậy $c \mid q$, giả sử $q = cd$. Khi đó $bcd = cs \Rightarrow s = bd$. Ta có :

$$m = a^2b^2 + c^2d^2 + a^2c^2 + b^2d^2 = (a^2 + d^2)(b^2 + c^2),$$

và $m$ không phải là số nguyên tố.

**15.** Ta chứng minh $n$ có tính chất đòi hỏi khi và chỉ khi $n \equiv 1 \pmod 4$ hoặc $n \equiv 0 \pmod 4$, $n \neq 4$.

a) Trước tiên, giả sử $n \equiv 1 \pmod 4$ : $n = 4k+1$, trong đó $k$ là số nguyên dương. Ta chọn các số $a_i$ như sau :

$$a_1 = \cdots = a_{2k} = -1$$

$$a_{2k+1} = \cdots = a_{4k} = 1$$

$$a_{4k+1} = n.$$

Dễ thử lại rằng, các số $\{a_i\}$ đã chọn thỏa mãn bài ra.

b) Giả sử $n \equiv 0 \pmod 4$, $n \neq 4$. Ta xét hai trường hợp :

i) $n = 4k$, $k$ chẵn. Ta chọn các số $a_i$ như sau :

$$a_1 = \cdots = a_k = -1$$

$$a_{k+1} = \cdots = a_{4k-2} = 1$$

$$a_{4k-1} = 2$$

$$a_{4k} = 2k.$$

ii) $k$ lẻ $> 1$. Chọn các số $a_i$ như sau :

$$a_1 = \cdots = a_{k-2} = -1$$

$$a_{k-1} = \cdots = a_{4k-2} = 1$$

$$a_{4k-1} = 2$$

$$a_{4k} = 2k.$$

Ngược lại, ta cần chứng tỏ rằng $n$ không có tính chất đòi hỏi nếu $n \equiv 4$ hoặc $n \equiv -1 \pmod 4$.

i) $n = 1$. Giả sử $a_1a_2a_3a_4 = 4$. Khi đó $a_i = \pm 1, \pm 2, \pm 4$. Do tổng các $a_i$ bằng 4 nên mọi $a_i \neq 4$ và $a_i \neq -1$. Vậy $a_i = 1$ hoặc $\pm 2$. Do tích bằng 4 nên có đúng hai số có trị tuyệt đối bằng 2, tổng hai số đó là 4, 0 hoặc $-4$. Dễ suy ra vô lí.

ii) $n \equiv -1 \pmod 4$ : vì tích các $a_i$ bằng $n$ nên các $a_i$ đều lẻ. Lại do tích đồng dư $-1 \pmod 4$ nên có một số lẻ các số $a_i$ đồng dư $-1 \pmod 4$, chẳng hạn có $2m + 1$ số đồng dư $-1 \pmod 4$. Khi đó tổng đồng dư với $(n - 2m - 1) - (2m + 1) \equiv n - 2 \pmod 4$ : vô lí.

**16.** Giả sử $m > 2$. Khi đó ta có

$$m^{(m-1)^2} \equiv (1 + (m-1))^{(m-1)^2} \equiv 1 \pmod{(m-1)^2}.$$

Mặt khác, $m \not\equiv 1 \pmod{(m-1)^2}$ : mọi giá trị $m > 2$ không thỏa mãn bài ra.

Khi $m = 1$: hiển nhiên thỏa mãn bài ra.

Xét $m = 2$, ta có :

$$2^n \equiv 1 \pmod n \text{ với mọi } n > 1.$$

Giả sử $p$ là ước nguyên tố nhỏ nhất của $n$, khi đó

$$2^n \equiv 1 \pmod p$$

Rõ ràng $p$ là số lẻ. Vì $n$ không chia hết cho các số nguyên tố nhỏ hơn $p$ nên $(n, p-1) = 1$. Như vậy, tồn tại các số nguyên $a$, $b$ sao cho

$$an + b(p-1) = 1.$$

Từ Định lí Fermat bé, ta có

$$2^1 = 2^{na}.2^{(p-1)^b} \equiv 1 \pmod{p}.$$

Mâu thuẫn này chứng tỏ rằng, giả thiết $m^n \equiv 1 \pmod{n}$ không bao giờ xảy ra.

Vậy ta có mệnh đề

$$m^n \equiv 1 \pmod{n} \Rightarrow m \equiv 1 \pmod{n}$$

đúng khi và chỉ khi $m = 1$ hoặc $2$.

**17.** Trong 14 số tự nhiên liên tiếp có 7 số chẵn, chúng có ước nguyên tố $p = 2$. Như vậy còn phải chỉ ra rằng trong 7 số lẻ còn lại, tồn tại ít nhất một số không chia hết cho một trong các số $3, 5, 7, 11$. Trong 7 số lẻ này, có nhiều nhất 3 số chia hết cho $3$, hai số chia hết cho $5$, một số chia hết cho $7$ và một số chia hết cho $11$. Như vậy, nếu mỗi một trong 7 số lẻ này chia hết cho một trong các số $3, 5, 7, 11$ thì mỗi số lẻ đang xét chỉ chia hết cho đúng một số trong các số $3, 5, 7, 11$, đồng thời có đúng 3 số chia hết cho $3$, hai số chia hết cho $5$, một số chia hết cho $7$, một số chia hết cho $11$. Điều này vô lí, vì để có 3 số chia hết cho $3$, chúng phải là số hạng đầu, giữa và cuối của 7 số lẻ đang xét. Nhưng khi đó, do hiệu của hai số tùy ý trong các số còn lại bé hơn $10$ nên không thể tồn tại hai số chia hết cho $5$.

**18.** Theo Định lí Wilson ta có

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Mặt khác,

$$(p-1)(p-2)\ldots(p-r) \equiv (-1)^r r! \pmod{p}$$

Suy ra

$$(p-1)! \equiv (p-r-1)(-1)^2 r! \pmod{p.}$$

Từ đó suy ra các đồng dư (1) và (2) là tương đương nhau.

**Nhận xét :** Hoàn toàn tương tự, ta chứng minh được đồng dư sau :

$$\left(\left[\frac{p-1}{2}\right]!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

**19.** Ta viết các số $a_1, \ldots, a_{n+1}$ dưới dạng

$$a_j = 2b^j c_j,$$

trong đó $b_j \geq 0$, $c_j$ lẻ $(j = 1, \ldots, n+1)$. Do các $c_j$ lẻ, $c_j < 2n$ nên phải có ít nhất hai giá trị $c_j$ nào đó trùng nhau (vì chỉ có $n$ số lẻ nhỏ hơn $2n$). Giả sử

$$c_k = c_l, \ k \neq l.$$

Khi đó

$$a_k = c_k.2^{b_k}, \ a_l = c_k.2^{b_l}.$$

Rõ ràng một trong hai số phải chia hết cho số kia.

**20.** Xét các trường hợp sau :

a) $m < n$ : Do $n > 2$, ta có $2^{n-1}(2-1) > 2$, tức là $2^{n-1} + 1 < 2^n - 1$. Vậy

$$2^m + 1 < 2^n - 1,$$

và hiển nhiên $2^m + 1$ không chia hết cho $2^n - 1$.

b) $m = n$ :

$$\frac{2^m + 1}{2^n - 1} = 1 + \frac{2}{2^n - 1},$$

không phải là số nguyên với $n \geq 1$.

c) $m > n$. Khi đó $m = kn + r$, trong đó $k$ nguyên dương, $r$ hoặc bằng $0$, hoặc nguyên dương nhỏ hơn $n$. Ta có

$$\frac{2^m + 1}{2^n - 1} = \frac{2^m - 2^{m-kn}}{2^n - 1} + \frac{2^r + 1}{2^n - 1}$$

$$= \frac{2^{m-kn}(2^{kn} - 1)}{2^n - 1} + \frac{2^r + 1}{2^n - 1}.$$

Tổng thứ nhất ở vế trái là số nguyên, tổng thứ hai không nguyên (do $0 \leq r < n$). Vậy $2^m + 1$ không chia hết cho $2^n - 1$.

**21.** a) Trước tiên ta chứng tỏ rằng, tồn tại số nguyên dương $k$ sao cho số $k2^n + 1$ là hợp số với mọi số nguyên dương $n$ thuộc một cấp số cộng vô hạn.

Giả sử $b > 1$ là số tự nhiên, $p$ là một ước số nguyên tố của $2^b - 1$. Tức là

$$2^b \equiv 1 \pmod{p} \qquad (1)$$

Giả sử $a$ là số nguyên dương tùy ý thỏa mãn $0 \leq a < b$, $k$ là số

nguyên lớn hơn $p$ sao cho

$$k \equiv -2^{b-a} \pmod{p}.$$

Giả sử $n$ là các số nguyên dương thỏa mãn

$$n \equiv a \pmod{p}, \tag{2}$$

tức là $n = a + bm$ với số nguyên $m \geq 0$ nào đó. Do (1),

$$k2^n \equiv -2^{b-a}.2^{a+bm} \equiv -1 \pmod{p}.$$

Vậy $k2^n + 1$ chia hết cho $p$, tức số đó là hợp số.

b) Ta xây dựng tập hợp *hữu hạn* các bộ ba $(p_j,\ a_j,\ b_j)$ có tính chất sau: các $p_j$ là các số nguyên tố khác nhau, $b_j$ là các số nguyên dương thỏa mãn

$$2^{b_j} \equiv 1 \pmod{p_j}, \tag{1}_j$$

$a_j$ là các số nguyên, $0 \leq a_j < b_j$ sao cho mọi số nguyên $n$ đều thỏa mãn một trong các đồng dư

$$n \equiv a_j \pmod{b_j}. \tag{2}_j$$

Rõ ràng rằng, nếu họ hữu hạn các bộ ba như trên tồn tại thì bài toán được giải. Thật vậy, khi đó theo Định lí Trung Quốc về phần dư, tồn tại số nguyên dương $k > p_j$ với mọi $j$ sao cho

$$k \equiv -2^{b_j - a_j} \pmod{p_j}$$

với mọi $j$. Với $k$ như vậy, $k2^n + 1$ là hợp số với mọi $n$ (chứng minh tương tự phần a).

Như vậy, việc giải bài toán được quy về việc xây dựng họ các bộ ba có tính chất đã nêu trong phần a).

Để kiểm tra xem $n$ thỏa mãn ít nhất một trong các đồng dư $(2)_j$, ta chỉ cần thử với mỗi một lớp đồng dư môđulô $b$, trong đó $b$ là bội chung nhỏ nhất của các $b_j$. Vì thế, ta nghĩ đến việc tìm một số $b$ có nhiều ước số. Chẳng hạn ta chọn $b = 24$ (có các ước lớn hơn 1 là 2, 3, 4, 6, 8, 12, 24). Để tìm các $p_j$, ta chú ý rằng $2^{b_j} - 1 \vdots p_j$.. Nhận xét rằng

$2^2 - 1 = 3$, $\qquad 2^3 - 1 = 7$,

$2^4 - 1 = 3.5$, $\qquad 2^6 - 1 = 3^2.7$,

$2^8 - 1 = 3.5.17$, $2^{12} - 1 = 3^2.5.7.13$,

$2^{24} - 1 = 3^2.5.7.13.17.241$.

Do các số $p_j$ phải khác nhau, để chọn $b_j$, ta phải loại số 6 (vì các ước nguyên tố của $2^6 - 1$ là 3, 7 đều đã xuất hiện trước đó). Vậy, các bộ 3 có thể chọn như sau

| $b_j$ | 2 | 3 | 4 | 8 | 12 | 24 |
|---|---|---|---|---|---|---|
| $a_j$ | 0 | 0 | 1 | 3 | 7 | 23 |
| $p_j$ | 3 | 7 | 5 | 17 | 13 | 241 |

(Các $a_j$ được chọn dễ dàng từ việc thử). Dễ thấy rằng mọi số tự nhiên $n$ đều thỏa mãn ít nhất một trong các đồng dư

$$n \equiv a_j \pmod{b_j},$$

(chỉ cần kiểm tra với các số $\leq 24$).

**22.** Giả sử

$$a = p_1^{\alpha_1} \dots p_k^{\alpha_k},\ b = p_1^{\beta_1} \dots p_k^{\beta_k},\ c = p_1^{\gamma_1} \dots p_k^{\gamma_k},$$

trong đó $p_j$ là ước nguyên tố của ít nhất một trong các số $a$, $b$, $c$ (như vậy, trong ba phân tích trên, có thể có những $p_j$ tham gia với số mũ bằng 0).

Ta có

$$[a,\ b] = p_1^{\max(\alpha_1,\beta_1)} \dots p_k^{\max(\alpha_k,\beta_k)}$$

$$(a,\ b) = p_1^{\min(\alpha_1,\beta_1)} \dots p_k^{\min(\alpha_k,\beta_k)},$$

và những hệ thức tương tự khác.

Để chứng minh hệ thức cần thiết, ta chỉ cần chứng minh hệ thức sau đối với mọi bộ số nguyên không âm $(m,\ n,\ l)$ tùy ý.

$$2\max(m,\ n,\ l) - \max(m,\ n) - \max(n,\ l) - \max(l,\ m)$$

$$= 2\min(m,\ n,\ l) - \min(m,\ n) - \min(n,\ l) - \min(l,\ m).$$

Không giảm tổng quát, có thể giả thiết $m \geq n \geq l$. Khi đó, đẳng thức trên trở thành đồng nhất thức sau đây :

$$2m - m - n - m = 2l - n - l - l.$$

**Nhận xét :** Bằng phương pháp trên, ta chứng minh được các đồng nhất thức sau đây :

1) $(a,\ [a,\ c]) = [(a,\ b),\ (a,\ c)]$

2) $[a,\ (b,\ c)] = ([a,\ b],\ [a,\ c])$

3) $([a,\ b],\ [b,\ c],\ [c,\ a]) = [(a,\ b),\ (b,\ c),\ (c,\ a)]$

4) $(ab,\ cd) = (a,\ c)(b,\ d)\left(\frac{a}{(a,\ c)},\ \frac{d}{(b,\ d)}\right)\left(\frac{c}{(a,\ c)},\ \frac{b}{(b,\ d)}\right)$

5) $a_1a_2\ldots a_n = G_rL_{n-r}$,

trong đó $G_r$ là ước chung lớn nhất của mọi tích có thể gồm $r$ thừa số là các $a_j$ (với $j$ khác nhau), còn $L_{n-r}$ là bội chung nhỏ nhất của các tích có thể gồm $n-r$ thừa số là các $a_j$ (với $j$ khác nhau).

**23.** Dĩ nhiên chỉ cần xét trường hợp không phải mọi chữ số đều bằng nhau.

Do $N_{j-1} \vdots N_0$ với mọi $j = 1,\ \ldots,\ n-1$, nên rõ ràng với $j = 1,\ \ldots,\ n-1$,

$$a_1 \le a_j. \tag{1}$$

Giả sử có một số chữ số bằng $a_1$. Gọi $(j+1)$ là chỉ số nhỏ nhất có tính chất đó. Do $N_j \vdots N_0$ mà $a_{j+1} = a_1$, $N_0$ và $N_j$ lại cùng số các chữ số nên suy ra $N_j = N_0$, tức là $a_{j+2} = a_2$, $a_{j+3} = a_3$, ... Vậy, dãy số $a_1$, $a_2$, ... , $a_n$ tuần hoàn với chu kì $a_1$, $a_2$, ... , $a_j$ ; đồng thời các chữ số của số $N_0' = a_1a_2\ldots a_j$ thỏa mãn (1).

Giả sử $a_1 = 1$. Chữ số cuối của $N_1$ là 1 nên $\frac{N_1}{N_0}$ lẻ $\ne 5$.

Giả sử $\frac{N_1}{N_0} = 3$. Do $\frac{a_2a_3\ldots a_n1}{1a_2\ldots a_n} = 3$ nên suy ra $a_n = 7$. Từ $\frac{a_2a_3\ldots 7.1}{1a_2\ldots a_{n-1}7} = 3$ suy ra $a_{n-1} = 5$. Tương tự, $a_{n-2} = 8$, $a_{n-3} = 2$, $a_{n-4} = 4$.

• Nếu $n = 6$ thì $a_{n-4} = a_2 = 4$ là chữ số đầu tiên của $N_1$, và $N_0 = 142857$.

• Nếu $n > 6$ thì nhóm số 142857 lập lại : $a_{n-5} = 1$, $a_{n-6} = 7$, $a_{n-7} = 5$, ... Khi đó, $N_0$ gồm một số nhóm 142857.

Ta chứng minh $N_0 = 142857$, hoặc là lập nên từ các nhóm số 142857 lập lại nhiều lần.

Khi $a = 1$, không tồn tại $a_2$ mà $\dfrac{a_2 \ldots a_n a_1}{a_1 a_2 \ldots a_n} = \dfrac{N_1}{N_0}$ bằng 7 hoặc 9.

Khi $a_1 = 2$ và $\dfrac{N_1}{N_0} = 2$, từ $\dfrac{a_2 \ldots a_n 2}{2a_2 \ldots a_n} = 2$ suy ra $a_n = 6$ (do (1), $a_n \neq 1$), nhưng không tồn tại $a_{n-1}$ mà $\dfrac{a_2 \ldots a_{n-1} 6.2}{2a_2 \ldots a_{n-1} 6} = 2$.

Khi $a_1 = 2$, $\dfrac{N_1}{N_0} = 3$ thì từ $\dfrac{a_2 \ldots a_n 2}{2a_2 \ldots a_n} = 3$ suy ra $a_n = 4$, $a_{n-1} = 1$ : mâu thuẫn (1).

Bằng lí luận tương tự, ta cũng loại được các giá trị khác của $a_1$, $\dfrac{N_1}{N_0}$.

Vậy, $a_1 = 1$, $\dfrac{N_1}{N_0} = 3$ và $N_0 = (142857)$.

**24.** Trước tiên, ta chứng minh các nhận xét sau :

**Nhận xét 1.** Nếu $d$ là một ước nguyên tố lẻ của $a^{6^n} + b^{6^n}$ thì

$$d \equiv 1 \pmod{2^{n+1}}.$$

*Chứng minh.* Đặt

$$a^{6^n} + b^{6^n} = kd,$$

trong đó $k$ là số nguyên dương. Ta viết $d$ dưới dạng

$$d = 2^m.v + 1,$$

trong đó $m$ nguyên dương, $v$ là số nguyên dương lẻ. Giả sử $m \leq n$. Do $(a,\ b) = 1$ nên $(a,\ d) = (b,\ d) = 1$. Theo Định lí Fermat nhỏ ta có :

$$(a^{3^n.2^{n-m}})^{d-1} \equiv (b^{3^n.2^{n-m}})^{d-1} \equiv 1 \pmod{d}$$

suy ra

$$(a^{6^n})^n \equiv (b^{6^n})^n \equiv 1 \pmod{d}. \qquad (1)$$

Mặt khác,

$$(a^{6^n})^n = (kd - b^{6^n})^n = td - (b^{6^n})^n \equiv -1 \pmod{d} \qquad (2)$$

($t$ là số nguyên nào đó). Mâu thuẫn giữa (1) và (2) suy ra $m \geq n+1$, tức là $d \equiv 1 \pmod{2^{n+1}}$. Nhận xét 1 được chứng minh.

**Nhận xét 2.** Nếu $x \equiv 1 \pmod{c^k}$ thì $x^{c^m} \equiv 1 \pmod{c^{m+k}}$.

*Chứng minh.* Giả sử $x = tc^k + 1$. Khi đó

$$x^{c^m} = (tc^k + 1)^{c^m} = sc^{m+k} + 1 \equiv 1 \pmod{c^{m+k}}.$$

Ta trở lại bài toán. Theo Nhận xét 1, $p^{3^n} \equiv q^{3^n} \equiv 1 \pmod{2^{n+1}}$. Từ Nhận xét 2 suy ra

$$p^{6^n} \equiv q^{6^n} \equiv 1 \pmod{2^{n+1}}. \qquad (3)$$

Do $(a,\ b) = 1$ nên $a^{6^n} + b^{6^n} \not\equiv 0 \pmod{3}$. Suy ra $(p,\ 3) = (q,\ 3) = 1$. Vậy $p^{2^n} \equiv q^{2^n} \equiv 1 \pmod{3}$. Lại do Nhận xét 2,

$$p^{6^n} \equiv q^{6^n} \equiv 1 \pmod{3^{n+1}}. \qquad (4)$$

Từ (3), (4) và do $(2,\ 3) = 1$ ta có

$$p^{6^n} \equiv q^{6^n} \equiv 1 \pmod{6.(12)^n}.$$

Vậy

$$p^{6^n} + q^{6^n} \equiv 2 \pmod{6.(12)^n}.$$

**25.** Ta chứng minh bằng quy nạp theo $n$. Với $n = 1$, ta lấy số $G_1 = A \vdots 2$..

Giả sử ta có $G_k$ là số mà các chữ số $k$ chỉ gồm các chữ số của $A$, $B$ và $G_k \vdots 2^k$.

Nếu $G_k \vdots 2^{k+1}$, $k$ lấy $G_{k+1} = G_k$.

Giả sử $G_k$ không chia hết $2^{k+1}$. Ta lập $F_k$ như sau :

a) Nếu $G_k$ có $k$ chữ số thì lấy $F_k = G_k$

b) Nếu $G_k$ có nhiều hơn $k$ chữ số thì $F_k$ nhận được từ $G_k$ bằng cách bỏ đi các chữ số, từ chữ số đầu tiên cho đến khi chỉ còn $k$ chữ số. Do $G_k \vdots 2^k$ nên $F_k \vdots 2^k$.

c) Nếu $G_k$ có ít hơn $k$ chữ số thì ta viết ghép vào bên trái chính số đó, cho đến khi nhận được số có ít nhất $k$ chữ số. Rõ ràng số này chia hết $G_k$, do đó chia hết cho $2^k$. Ta bỏ đi các chữ số từ chữ số đầu cho đến khi nhận được số $F_k$ có $k$ chữ đó. Rõ ràng $F_k \vdots 2^k$.

Nếu $F_k \vdots 2^{k+1}$, ta đặt $G_{k+1} = F_k$.

Nếu $F_k \not\vdots 2^{k+1}$, ta đặt $G_{k+1} = \overline{BF_k}$.

Ta chứng tỏ $G_{k+1}$ chia hết cho $2^{k+1}$. Thật vậy, giả sử $F_k = 2^k p$, trong đó $p$ lẻ. Khi đó

$$G_{k+1} = 10^k B + 2^k p = 2^k(5^k B + p) \vdots 2^{k+1}.$$

**26.** Giả sử tồn tại các số $a_1, \ldots, a_{2004}$ sao cho với mọi $i \neq j$,

$$P(a_i)P(a_j) \vdots a_i a_j.$$

Rõ ràng $(a_i, P(a_j)) = (a_j, P(a_j)) = 1$. Suy ra $P(a_i) \vdots a_j$ với mọi $i \neq j$. Khi đó, do

$$(a_i^{2003} - a_i^{1000} + 1) \vdots a_j$$

nên suy ra $(a_i, a_j) = 1$ với mọi $i \neq 1$. Không giảm tổng quat, giả sử

$$a_1 < a_2 < \cdots < a_{2004}.$$

Ta có :

$$P(a_1) \vdots a_2 \ldots a_{2004} > a_1^{2003}$$

Mâu thuẫn, vì $P(a_1) < a_1^{2003}$.

**27.** Xét phân tích đa thức sau đây ra thừa số :

$$x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1).$$

Khi $x = 2^{2^{n-1}}$ ta có

$$a_{n+1} = 2^{2^{n+1}} + 2^{2^n} + 1 = (2^{2^n} - 2^{2^{n-1}} + 1)(2^{2^n} + 2^{2^{n-1}} + 1)$$

$$= (2^{2^n} - 2^{2^{n-1}} + 1)a_n.$$

Vậy

$$a_{n+1} \vdots a_n.$$

Mặt khác, các số $a_n$ và $(2^{2^n} - 2^{2^{n-1}} + 1)$ nguyên tố cùng nhau (vì ước chung của chúng chỉ có thể có dạng $2^k$, $k \geq 0$). Do đó, số ước nguyên tố của $a_{n+1}$ lớn hơn số ước nguyên tố của $a_n$. Từ đó suy ra số ước nguyên tố của $a_n$ phải không ít hơn $n$.

**28.** Giả sử $p = mk + r$, $1 \leq r \leq m-1$. Giả sử $x$ là số tự nhiên sao cho

$$(x^{m-1} + x^{m-2} + \cdots + 1) \vdots p.$$

Từ đó suy ra

$$x^m \equiv 1 \pmod{p}. \tag{1}$$

Vậy, $x \not\vdots p$.

Ta chứng minh

$$x^{r-1} \equiv 1 \pmod{p}. \tag{2}$$

Nếu $p < m$ thì (2) đúng do Định lí Fermat.

Giả sử $p > m$. Ta nâng hai vế của (1) lên lũy thừa $k = \dfrac{p-r}{m}$:

$$x^{p-r} \equiv 1 \pmod{p}.$$

Mặt khác, theo Định lí Fermat

$$x^{p-1} \equiv 1 \pmod{p}.$$

Vậy

$$x^{p-r}(x^{r-1} - 1) \equiv 0 \pmod{p}.$$

Từ đó suy ra (2).

Ta cần chứng minh $r = 1$. Giả sử ngược lại, $r > 1$. Khi đó $(m,\ r-1) = 1$. Ta có :

$$(x^m - 1,\ x^{r-1} - 1) = x^{(m,\ r-1)} - 1 = x - 1.$$

Từ (1) và (2) ta được : $p \mid (x^m - 1)$, $p \mid (x^{r-1} - 1)$. Do đó $p \mid (x-1)$, tức là $x \equiv 1 \pmod{p}$. Nhưng khi đó

$$P(x) \equiv m \pmod{p},$$

trái giả thiết $p \mid P(x)$.

**29.** a) Trước tiên ta thấy rằng, nếu $n$ chẵn thì $n^4 \vdots 16$, nếu $n$ lẻ thì

$n^4 \equiv 1 \pmod{16}$. Thật vậy, nếu $n = 2k + 1$ thì

$$n^4 - 1 = (n-1)(n+1)(n^2+1) = 8k(k+1)(2k^2+2k+1),$$

mà $k(k+1)$ chẵn.

Do đó, phần dư của phép chia $a^4 + b^4 + c^4 + d^4$ cho 16 bằng số các số lẻ trong 4 số. Vì phần dư đó trùng với phần dư của $e^4$ cho 16 nên đẳng thức chỉ có thể xảy ra khi hoặc cả 5 số đều chẵn, hoặc $e$ và một trong các số còn lại lẻ.

b) Nếu $n \vdots 5$ thì $n^4 \vdots 5$, nếu $n \not\vdots 5$ thì $n^4 \equiv 1 \pmod{5}$.

Thật vậy, nếu $n = 5k \pm 1$ thì $n^2 - 1 = 5k(5k \pm 2) \vdots 5$. Nếu $n = 5k \pm 2$ thì $n^2 + 1 = 5k(5k \pm 4) + 5 \vdots 5$. Do đó $n^4 - 1 = (n^2-1)(n^2+1) \vdots 5$ trong mọi trường hợp.

Lí luận còn lại hoàn toàn tương tự như trường hợp a).

c) Ta chia ra ba trường hợp

i) $e$ chẵn. Từ a) suy ra các số còn lại cũng chẵn. Từ b) suy ra có ít nhất 3 số trong đó chia hết cho 5, nghĩa là có ít nhất 3 số chia hết cho 10.

ii) $e$ chia hết cho 5. Cũng như trước, các số đều chia hết cho 5, mà ít nhất có 3 số chẵn.

iii) $e$ không chia hết cho 2 và 5. Khi đó từ b) suy ra trong các số $a$, $b$, $c$, $d$ có ba số chẵn, ba số chia hết cho 5 nên có ít nhất hai số chia hết cho 10.

**30.** Một ước chung tùy ý của $(n^a + 1)$ và $(n^b - 1)$ phải là ước của tổng $(n^a + 1) + (n^b - 1) = n^a + n^b$. Giả sử $a > b$. Khi đó, ước chung của $(n^a + 1)$ và $(n^b - 1)$ là ước chung của $n^b - 1$ và $n^{a-b} + 1$. (Tương tự, nếu $a \le b$ thì ta lấy $n^{b-a} + 1$ thay cho $n^{a-b} + 1$). Tiếp tục lí luận trên, ta thấy rằng, ước chung của $(n^a + 1)$ và $(n^b - 1)$ là ước của $n^d + 1$, với $d = (a, b)$.

Giả sử $x = n^d$, khi đó $n^b - 1 = x^{b'} - 1$, trong đó $b' = \dfrac{b}{d}$ là số lẻ theo giả thiết. Ta có : $n^b - 1 = n^{b'd} - 1 = x^{b'} - 1$. Do đó, nếu $n^b - 1 \equiv k \pmod{(n^d + 1)}$ thì $x^{b'} - 1 \equiv k \pmod{(x+1)}$. Rõ ràng $k = -2$, và ta có

$$n^b - 1 \equiv -2 \pmod{(n^d + 1)}.$$

Vậy, ước chung của $(n^a + 1)$ và $(n^b - 1)$ phải là ước của $2$, suy ra

$$(n^a + 1,\ n^b - 1) \le 2.$$

**31.** Từ đồng dư $n^r \equiv n \pmod{10^a}$ không luôn luôn suy ra $n^2 \equiv n \pmod{10^a}$ trong hai trường hợp : hoặc $r$ là số lẻ (khi đó $4^r \equiv 4 \pmod{10}$, trong khi $4^2 \equiv 16$), hoặc $r \equiv 1 \pmod 5$. (Thật vậy, khi $r \equiv 1 \pmod 5$ thì $21^r \equiv 21 \pmod{100}$ vì $21^5 \equiv 1 \pmod{100}$, trong khi đó $21^2 = 441 \not\equiv 1 \pmod{100}$.)

Ta sẽ chứng minh rằng, ngoài hai trường hợp đó, từ đồng dư $n^r \equiv n \pmod{10^a}$ luôn suy ra $n^2 \equiv n \pmod{10^a}$. Như vậy, giả thiết $r$ là số chẵn, $r \not\equiv 1 \pmod 5$, tức là $r$ có tận cùng khác $6$. Khi đó $(r-1)$ nguyên tố cùng nhau với $10$.

Giả sử rằng $\dfrac{n^{r-1} - 1}{n - 1} \vdots 5$. Khi đó $n^{r-1} \equiv 1 \pmod 5$. Mặt khác, theo Định lí Fermat, $n^4 \equiv 1 \pmod 5$. Do $(r-1)$ lẻ nên $r - 1 \equiv \pm 1 \pmod 4$. Từ đó suy ra $n \equiv 1 \pmod 5$, hoặc $n^{-1} \equiv 1 \pmod 5$ (cũng tức là $n \equiv 1 \pmod 5$). Đặt $n = 5m + 1$. Ta có :

$$\frac{n^{r-1} - 1}{n - 1} = \frac{(5m+1)^{r-1} - 1}{5m} = \frac{(5m)^{r-1} + \cdots + 5m(r-1) + 1 - 1}{5m}$$

$$\equiv (r - 1) \pmod 5.$$

Vậy $(r - 1) \equiv 0 \pmod 5$ : mâu thuẫn vì $(r - 1,\ 10) = 1$. Hơn nữa, khi $(r-1)$ lẻ thì $\dfrac{n^{r-1} - 1}{n - 1} = n^{r-2} + \cdots + n + 1$ lẻ với mọi $n$. Suy ra số $\dfrac{n^r - n}{n^2 - n}$ nguyên tố cùng nhau với $10$ (vì không chia hết cho $5$ và $2$), do đó từ $n^r \equiv n \pmod{10^a}$ suy ra $n^2 \equiv n \pmod{10^a}$.

**32.** Giả sử mọi hệ số trong khai triển nhị thức $(a + b)^n$ đều lẻ. Tỉ số giữa hai hệ số nhị thức liên tiếp $C_n^{k+1}$ và $C_n^k$ là $\dfrac{n-k}{k+1}$ $(k = 0, 1, \ldots, n-1)$.

Vậy, dãy phân số

$$\frac{n}{1}, \frac{n-1}{2}, \frac{n-2}{3}, \ldots, \frac{n-k}{k+1}, \ldots, \frac{1}{n} \qquad (1)$$

khi đưa về dạng tối giản phải có tử số và mẫu số đều lẻ. Do $n$ cùng là số lẻ, ta đặt $n = 2^s u - 1$, trong đó $u$ là số lẻ. Khi đó, tỉ số giữa hệ số thứ $(2^s + 1)$ và hệ số thứ $2^s$ là :

$$\frac{n-(2^s-1)}{2^s} = \frac{2^s(u-1)}{2^s} = \frac{u-1}{1}.$$

Như vậy, nếu $u \neq 1$ thì ta có mâu thuẫn vì tử số là số chẵn. Do đó $u = 1$ (và không tồn tại hệ số thứ $2^s + 1$), tức là $n$ có dạng $n = 2^s - 1$.

Ngược lại, giả sử $n = 2^s - 1$. Khi đó, từ tổng quát của dãy (1) có dạng

$$\frac{2^s-(k+1)}{k+1},$$

với $k < n$. Nếu $k+1 = 2^t v$ với $v$ là số lẻ nào đó thì tỉ số là $\dfrac{2^{s-t} - v}{v}$.

Do hệ số đầu tiên là 1 (lẻ) nên suy ra mọi hệ số nhị thức trong trường hợp này đều lẻ.

Vậy, $n$ thỏa mãn bài ra khi và chỉ khi $n$ có dạng $2^s - 1$ với $s$ nguyên dương nào đó.

**33.** a) Với mọi $j$, $0 \leq j \leq n-1$, ta có :

$$\left[\sqrt{\alpha + \frac{j}{n}}\right] \geq [\sqrt{\alpha}].$$

Do đó

$$S_n(\alpha) \geq n[\sqrt{\alpha}].$$

Nếu đẳng thức không xảy ra thì ta phải có

$$\left[\sqrt{\alpha + \frac{n-1}{n}}\right] > [\sqrt{\alpha}].$$

Như vậy, tồn tại số nguyên $k$ thỏa mãn

$$\sqrt{\alpha} < k \leq \sqrt{\alpha + \frac{n-1}{n}} \Rightarrow k^2 + \frac{1}{n} \leq \alpha + 1 < k^2 + 1$$

$$\Rightarrow [\alpha] + 1 = k^2.$$

$$(c+1)(\sqrt{3}-1) < b+1. \tag{3}$$

Từ bất đẳng thức thứ hai trong (1) và bất đẳng thức thứ nhất trong (2) ta nhận được :

$$\frac{b}{2}(\sqrt{3}+1) + \frac{\sqrt{3}-1}{2} < c+1.$$

Nhân hai vế với $(\sqrt{3}-1)$ ta được

$$b + \frac{(\sqrt{3}-1)^2}{2} < (c+1)(\sqrt{3}-1),$$

suy ra

$$b < (c+1)(\sqrt{3}-1). \tag{4}$$

Nhận xét được chứng minh nhờ (3) và (4).

Ta chứng minh bài toán bằng quy nạp theo $n$. Với $n=1$ đẳng thức đúng. Giả sử đẳng thức đúng với $n$, ta chứng minh đẳng thức sau cũng đúng.

$$[(J(n+1)+1)(\sqrt{3}-1)] = J(n). \tag{5}$$

Nhưng khi đó (5) chính là hệ quả của giả thiết quy nạp và nhận xét đã chứng minh : chỉ cần đặt $b = J(n)$, $a = J(n-1)$.

**35.** Khi $n = 0$, thử trực tiếp ta có

$$[1+\sqrt{2}] = [\sqrt{8}] = 2.$$

Xét $n \geq 1$. Đặt

$$x = \sqrt{n} + \sqrt{n+1} + \sqrt{n+2},$$

ta được :

$$x^2 = 3n + 3 + 2\left(\sqrt{n(n+1)} + \sqrt{n(n+2)} + \sqrt{(n+1)(n+2)}\right).$$

Mặt khác, khi $n \geq 1$ ta có :

$$\left(n+\frac{2}{5}\right)^2 < n(n+1) < \left(n+\frac{1}{2}\right)^2,$$

$$\left(n+\frac{7}{10}\right)^2 < n(n+2) < (n+1)^2,$$

Do đó, nếu không có đẳng thức thì $[\alpha]+1$ là số chính phương.

b) Đặt

$$r=[n(\alpha\ -[\alpha])].$$

Khi đó, nếu $[\alpha]+1=k^2$ thì

$$k^2+\frac{r}{n}\le\alpha+1<k^2+\frac{(r+1)}{n}\Rightarrow\sqrt{\alpha+\frac{n-r-1}{n}}<k\le\sqrt{\alpha+\frac{n-r}{n}}.$$

Vậy

$$\left[\sqrt{\alpha+\frac{j}{n}}\right]=\begin{cases}k-1 & \text{nếu} \quad j<n-r\\ k & \text{nếu} \quad j\ge n-r\end{cases}$$

Do đó :

$$S_n(\alpha)=(n-r)(k-1)+rk=n(k-1)+r.$$

Vì

$$(k-1)=[\sqrt{\alpha}]$$

nên suy ra

$$S_n(\alpha)=n[\alpha]+[n(\alpha-[\alpha])].$$

**34.** Trước tiên, ta chứng minh nhận xét sau :

Giả sử $b$ là số nguyên dương, $a=[(b+1)(\sqrt{3}-1)]$, $c=b+\left[\frac{a}{2}\right]$, trong đó $[x]$ là kí hiệu phần nguyên của $x$. Khi đó ta có :

$$b=[(c+1)(\sqrt{3}-1)].$$

*Chứng minh nhận xét* : Do cách đặt $a$, ta có

$$a<(b+1)(\sqrt{3}-1)<a+1. \tag{1}$$

Vì $a$ là số nguyên nên từ định nghĩa $c$ suy ra :

$$b+\frac{a-1}{2}\le c\le b+\frac{a}{2}. \tag{2}$$

Từ bất đẳng thức thứ nhất trong (1) và bất đẳng thức thứ hai trong (2) ta nhận được

$$c+1<\frac{b}{2}(\sqrt{3}+1)+\frac{\sqrt{3}+1}{2}.$$

Nhân hai vế với $(\sqrt{3}-1)$ ta có :

$$\left(n+\frac{7}{5}\right)^2 < (n+1)(n+2) < \left(n+\frac{3}{2}\right)^2.$$

Do đó

$$9n+8 < x^2 < 9n+9.$$

Vậy

$$[x] = [\sqrt{9n+8}].$$

**36.** Ta có

$$\begin{aligned} P &= n(n+1)(n+2)(n+3)(n+4)(n+5)(n+6)(n+7) \\ &= n(n+7)(n+1)(n+6)(n+2)(n+5)(n+3)(n+4) \\ &= (n^2+7n+6-6)(n^2+7n+6)(n^2+7n+6+4)(n^2+7n+6+6) \\ &= (a-6)a(a+4)(a+6) = a^4+4a(a+3)(a-12), \end{aligned}$$

trong đó $a = n^2+7n+6$.

Do $n \geq 1$ nên $a > 12$, suy ra $a^4 < P$. Mặt khác

$$(a+1)^4 - P = 42a^2 + 148a + 1 > 0.$$

Vậy

$$a^4 < P < (a+1)^4,$$

suy ra điều phải chứng minh.

**Nhận xét :** Từ bài toán nói trên suy ra mệnh đề sau : Tích 8 số tự nhiên liên tiếp không phải là lũy thừa bậc 4 của một số nguyên.

**37.** Viết $(n-1)$ dưới dạng cơ số 2 :

$$n-1 = \sum_{m=0}^{\infty} 2^m a_m, \qquad a_m = 0,\ 1,$$

trong đó chỉ có hữu hạn $m$ với $a_m = 1$.

Khi đó ta có :

$$\left[\frac{n-1+2^{k-1}}{2^k}\right] = \left[\frac{n-1}{2^k}+\frac{1}{2}\right] = a_{k-1} + \sum_{r=k}^{\infty} a_r . 2^{r-k}.$$

Từ đó suy ra

$$\sum_{k=1}^{\infty}\left[\frac{n-1+2^{k-1}}{2^k}\right]=\sum_{r=0}^{\infty}a_r+\sum_{r=1}^{\infty}\sum_{k=1}^{r}2^{r-k}a_r=\sum_{r=0}^{\infty}2^r a_r=n-1.$$

Công thức được chứng minh.

**38.** a) Đặt $x=x_1+u$, $y=y_1+v$, trong đó $x_1$, $y_1$ là các số nguyên không âm, $0\le u<1$, $0\le v<1$. Bất đẳng thức cần chứng minh được đưa về dạng sau :

$$x_1+y_1+[5u]+[5v]\ge[3u+v]+[3v+u]. \tag{1}$$

Ta chứng tỏ rằng

$$[5u]+[5v]\ge[3u+v]+[3v+u]. \tag{2}$$

Do vai trò đối xứng của $u$ và $v$, có thể giả thiết rằng $u\ge v$. Từ đó ta có $[5u]\ge[3u+v]$.

Nếu $u\le 2v$ thì $[5v]\ge[3v+u]$ : (2) đúng.

Giả sử $u>2v$. Đặt $5u=a+b$, $5v=c+d$, trong đó $a$ và $c$ là các số nguyên không âm, $0\le b\le 1$, $0\le d<1$. Ta có thể viết lại (2) như sau :

$$a+c\le\left[\frac{3a+c+3b+d}{5}\right]\left[\frac{3c+a+3d+b}{5}\right]. \tag{3}$$

Do $1>u>2v$ nên $5>5u>10v$, suy ra $5>a+b>2c+2d$. Do đó $5>a$, tức là $4\ge a$. Từ bất đẳng thức $a+b>2c+2d$ suy ra $a\ge 2c$, vì nếu ngược lại, $a<2c$ thì $a\le 2c-1\Rightarrow a+1-2c\le 0$ và $a+b-2c<0$. Vậy ta có $4\ge a\ge 2c$. Do đó, chỉ cần xét các trường hợp sau :

| $a$ | 4 | 4 | 4 | 3 | 3 | 2 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|---|
| $c$ | 2 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |

Dễ kiểm tra bất đẳng thức (3) đối với 9 trường hợp này, vì $3b+d<4$, $3d+b<4$.

b) Ta biết rằng, lũy thừa cao nhất của số nguyên tố $p$ chia hết $m!$ được tính bởi công thức

$$\left[\frac{m}{p}\right]+\left[\frac{m}{p^2}\right]+\left[\frac{m}{p^3}\right]+\cdots$$

Do đó, chỉ cần chứng minh rằng

$$\left[\frac{5m}{r}\right]+\left[\frac{5n}{r}\right]\geq\left[\frac{m}{r}\right]+\left[\frac{n}{r}\right]+\left[\frac{3m+n}{r}\right]+\left[\frac{3n+m}{r}\right] \qquad (4)$$

với mọi số nguyên $r\geq 2$.

Viết

$$m=rm_1+x,\qquad n=rn_1+y,$$

trong đó $0\leq x<r$; $0\leq y<r$; $r$, $m_1$, $n_1$ nguyên. Khi đó, (4) trở thành

$$\left[\frac{5x}{r}\right]+\left[\frac{5y}{r}\right]\geq\left[\frac{3x+y}{r}\right]+\left[\frac{3y+x}{r}\right].$$

Bất đẳng thức này suy ra từ phần a).

**Nhận xét :** Dùng phương pháp trên đây có thể chứng minh rằng các số sau đây là số nguyên :

1) $\dfrac{(3m)!(3n)!}{m!n!(m+n)!(m+n)!}$,

2) $\dfrac{(4m)!(4n)!}{m!n!(2m+n)!(2n+m)!}$,

3) $\dfrac{(mnr)!}{m!(n!)^m(r!)^{mn}}$,

4) $\dfrac{(m-1)!\,\delta}{m_1!m_2!\ldots m_r!}$,

trong đó $m=m_1+m_2+\cdots+m_r$; còn $\delta$ là ước chung lớn nhất của $m_1,\ m_2,\ \ldots,\ m_r$.

**39.** Ta dùng quy nạp toán học. Khi $n=1$, bất đẳng thức là rõ ràng, vì $a_1>a_0\geq 1$, $[a_0,\ a_1]\geq 2$. Giả sử bất đẳng thức đúng với $n=k$, ta xét $n=k+1$. Ta chia ra hai trường hợp sau.

a) Giả sử $a_{k+1}\geq 2^{k+1}$, khi đó $[a_k,\ a_{k+1}]\geq a_{k+1}\geq 2^{k+1}$. Theo giả thiết quy nạp, ta có :

$$\frac{1}{[a_0,\ a_1]}+\cdots+\frac{1}{[a_{k-1},\ a_k]}+\frac{1}{[a_k,\ a_{k+1}]}\leq\left(1-\frac{1}{2^k}\right)+\frac{1}{2^{k+1}}=1-\frac{1}{2^{k+1}}.$$

2) Giả sử $a_{k+1}<2^{k+1}$. Kí hiệu $(a,\ b)$ là ước chung lớn nhất của $a$ và

$b$ thì ta có

$$[a,\ b] = \frac{ab}{(a,\ b)}.$$

Do $b \vdots (a,\ b)$ nên suy ra $(a,\ b) = b - a$ khi $b > a$. Từ đó ta có :

$$\frac{1}{[a,\ b]} = \frac{(a,\ b)}{ab} \le \frac{b-a}{ab} = \frac{1}{a} - \frac{1}{b}.$$

Do đó :

$$\frac{1}{[a_0,\ a_1]} + \cdots + \frac{1}{[a_k,\ a_{k+1}]} \le \left(\frac{1}{a_0} - \frac{1}{a_1}\right) + \cdots + \left(\frac{1}{a_k} - \frac{1}{a_{k+1}}\right) =$$

$$= \frac{1}{a_0} - \frac{1}{a_{k+1}} < 1 - \frac{1}{2^{k+1}}.$$

**Nhận xét :** Ước lượng trên đây là chặt : khi $a_0 = 1$, $a_1 = 2$, ... , $a_n = 2^n$, ta có đẳng thức.

**40.** Hiển nhiên nếu $n = 1$ thì $\varphi(n) \mid n$. Ta xét $n > 1$. Giả sử $n$ có phân tích thành thừa số nguyên tố dưới dạng :

$$n = p_1^{k_1} \ldots p_i^{k_i}.$$

Ta có

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_i}\right).$$

Từ điều kiện $\varphi(n) \mid n$, chẳng hạn $n = x\varphi(n)$, suy ra

$$p_1 \ldots p_i = x(p_1 - 1)\ldots(p_i - 1).$$

Như vậy, phải có $p_j$ nào đó bằng 2 (nếu ngược lại thì vô lí, vì vế trái là số lẻ, vế phải là số chẵn). Giả sử $p_1 = 2$, ta có :

$$2p_2 \ldots p_i = x(p_2 - 1)\ldots(p_i - 1).$$

Do $p_2, \ldots, p_i$ khác 2 nên từ đẳng thức trên suy ra rằng $n$ có nhiều nhất là một ước nguyên tố lẻ, chẳng hạn $p_2$.

Đặt

$$p_2 = 2y + 1.$$

Ta có :

$$2p_2 = x(2y).$$

Do $p_2$ nguyên tố nên suy ra $x = p_2$, $y = 1$. Vậy $p_2 = 3$ và $n$ có dạng

$$n = 2^k 3^m, \quad k \geq 1, \quad m \geq 0.$$

Dễ thử lại rằng, các số $n$ có dạng nói trên thỏa mãn điều kiện

$$\varphi(n) \mid n.$$

**41.** Giả sử $m$ là một số hoàn hảo, đồng thời $m$ có $n$ ước nguyên tố khác nhau $p_1 < p_2 < \cdots < p_n$ $(n \geq 2)$. Ta viết $m$ dưới dạng :

$$m = p_1^{\alpha_1} . p_2^{\alpha_2} \ldots p_n^{\alpha_n}.$$

Khi đó tổng các ước của $m$ là

$$\sigma(m) = (1 + p_1 + \cdots + p_1^{\alpha_1}) \cdots (1 + p_n + \cdots + p_n^{\alpha_n}).$$

Nếu mọi ước nguyên tố của $m$ đều lớn hơn $n$ thì $p_1 \geq n + 1$. Suy ra $p_i \geq n + i$ $(i = 1, 2, \ldots, n)$. Ta có :

$$\begin{aligned}
\frac{\sigma(m)}{m} &= \left(1 + \frac{1}{p_1} + \cdots + \frac{1}{p_1^{\alpha_1}}\right) \cdots \left(1 + \frac{1}{p_n} + \cdots + \frac{1}{p_n^{\alpha_n}}\right) \\
&< \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right) \cdots \left(1 + \frac{1}{p_n} + \frac{1}{p_n^2} + \cdots\right) \\
&= \left(1 + \frac{1}{p_1 - 1}\right) \cdots \left(1 + \frac{1}{p_n - 1}\right) \\
&= \left(1 + \frac{1}{n}\right) \cdots \left(1 + \frac{1}{2n - 1}\right) \\
&= \frac{2m}{m} = 2,
\end{aligned}$$

tức là

$$\sigma(m) < 2m,$$

vô lí, vì $m$ là số hoàn hảo.

**42.** Ta chứng minh bằng quy nạp theo $m$.

Với $m = 1$ : dãy luôn nhận giá trị $0$.

Giả sử kết luận đúng đối với mọi cặp số tự nhiên $(a, n)$ với $n < m$. Ta chứng minh kết luận đúng với cặp $(a, m)$, $m$ tùy ý. Xét hai trường hợp

a) $m$ không phải là lũy thừa của một số nguyên tố, tức là phân tích $m$ ra thừa số nguyên tố có dạng :

$$m = p_1^{k_1} \dots p_s^{k_s}, \quad s \geq 2.$$

Với mọi $j = 1, \dots, s$, ta có $p_j^{k_j} < m$. Do đó dãy

$$1,\ a,\ a^a,\ a^{a^a},\ \dots \pmod{p_j^{k_j}}$$

là hằng số từ lúc nào đó (theo giả thiết quy nạp). Vậy, nếu đặt

$$x_j = a^{a^{\cdot^{\cdot^{a}}}} \Big\} n \text{ lần}$$

thì với mọi $j = 1, \dots, s$, tồn tại $b_j$, $n_j$ sao cho khi $n \geq n_j$ ta có

$$x_n \equiv b_j \pmod{p_j^{k_j}}.$$

Như vậy, khi $n \geq \max\{n_1, \dots, n_s\}$, ta có

$$x_n \equiv (b_1 \dots b_s) \pmod{m},$$

nghĩa là kết luận đúng với $m$.

b) $m$ là lũy thừa của một số nguyên tố nào đó : $m = p^\alpha$. Nếu $a \mid p$ thì $x_n \equiv 0 \pmod{m}$ khi $n \geq \alpha$. Nếu $(a, m) = 1$ thì do $\varphi(m) < m$ nên theo giả thiết quy nạp, dãy $x_j \pmod{\varphi(m)}$ là hằng số với $j$ đủ lớn. Chẳng hạn

$$x_j \equiv c \pmod{\varphi(m)} \quad \text{với} \quad j \geq k$$

$$x_j = c + q_j\varphi(m).$$

Khi đó, với $j \geq k$ ta được

$$x_{j+1} = a^{x_j} = a^c.(a^{\varphi(m)})^{q_j}.$$

Do $a^{\varphi(m)} \equiv 1 \pmod{m}$ nên

$$x_{j+1} \equiv a^c \pmod{m}$$

với $j \geq k$. Vậy, dãy $\{x_n \bmod m\}$ từ lúc nào đó chỉ nhận giá trị $a^c \bmod m$.

**43.** Giả sử các ước của $n$ là

$$1 = d_1 < d_2 < \dots < d_k = n.$$

Trong các số tự nhiên không vượt quá $n$, có $\frac{n}{d_i}$ số là bội của $d_i$. Mỗi số không vượt quá $n$ và không nguyên tố cùng nhau với $n$ phải là bội của một ước nào đó $(>1)$ của $n$. Vì thế ta có :

$$n-\varphi(n)\le\frac{n}{d_2}+\frac{n}{d_3}+\cdots+\frac{n}{d_k}.$$

Mặt khác

$$\frac{n}{d_2}+\frac{n}{d_3}+\cdots+\frac{n}{d_k}=d_{k-1}+d_{k-2}+\cdots+d_1=\sigma(n)-n.$$

Vậy

$$n-\varphi(n)\le\sigma(n)-n,$$

tức là

$$\sigma(n)+\varphi(n)\ge 2n.$$

Khi $n$ nguyên tố, ta có đẳng thức

$$\sigma(n)+\varphi(n)=2n.$$

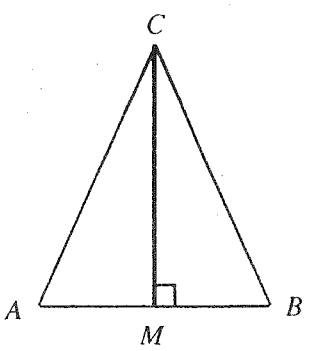
**44.** a) Xét tam giác cân $ABC$ có $AC=BC$, trong đó các đỉnh có tọa độ nguyên và có số đo các cạnh là số nguyên. Không giảm tổng quát, ta có thể xem đỉnh $C$ nằm tại gốc tọa độ, tức là $C=(0,\ 0)$. Các đỉnh còn lại có tọa độ $A=(a_1,\ a_2)$, $B=(b_1,\ b_2)$, cạnh $AC=BC=x$, $AB=y$. Khi đó ta có :

$$x^2=a_1^2+a_2^2=b_1^2+b_2^2, \tag{1}$$

$$y^2=(a_1-b_1)^2+(a_2-b_2)^2=2(x^2-a_1b_1-a_2b_2). \tag{2}$$

Kí hiệu qua $M$ chân đường vuông góc hạ từ đỉnh $C$ xuống cạnh $AB$.

Từ (2) suy ra rằng $y$ là số chẵn, do đó số đo của $AM$ nguyên. Mặt khác, vì $y$ chẵn nên $y^2\equiv 0\ (\mathrm{mod}\,4)$. Từ (2) suy ra $(a_1-b_1)$ và $(a_2-b_2)$ đều là số chẵn, tức là điểm $M=\left(\frac{a_1+b_1}{2},\ \frac{a_2+b_2}{2}\right)$ có các tọa độ nguyên. Chỉ còn phải chứng tỏ rằng, $CM$ có độ dài là số nguyên. Giả sử $a_2\ne b_2$. Từ (1) ta có



$$\frac{a_2 + b_2}{a_1 + b_1} = -\frac{a_1 - b_1}{a_2 - b_2}.$$

Kết hợp với (2) ta được :

$$(CM)^2 = \left(\frac{a_1 + b_1}{2}\right)^2 \left(1 + \left(\frac{a_1 - b_1}{a_2 - b_2}\right)^2\right) = \left(\frac{a_1 + b_1}{2}\right)^2 \cdot \frac{y^2}{(a_2 - b_2)^2}.$$

Như vậy, $(CM)^2$ là bình phương của một số hữu tỉ, và do $(CM)^2$ là số nguyên (vì $AC$, $CM$ có số đo nguyên) nên ta suy ra $(CM)^2$ là số chính phương, tức là $CM$ có độ dài nguyên.

b) Ta chứng tỏ rằng trong không gian không tồn tại các tam giác đều với các đỉnh có tọa độ nguyên và số đo của cạnh là số nguyên. Giả sử ngược lại, tam giác đều $ABC$ có tính chất vừa nêu, đồng thời giả sử $C$ có tọa độ $(0, 0, 0)$, $A$, $B$ có tọa độ lần lượt là $(a_1, a_2, a_3)$; $(b_1, b_2, b_3)$ và cạnh tam giác là $x$.

Không giảm tổng quát, có thể giả thiết $a_1$, $a_2$, $a_3$, $b_1$, $b_2$, $b_3$ không có ước chung lớn hơn 1, đặc biệt, ít nhất một trong các số đó là số lẻ. Ta có

$$\begin{aligned} x^2 &= a_1^2 + a_2^2 + a_3^2 = b_1^2 + b_2^2 + b_3^2 \\ &= (a_1 - b_1)^2 + (a_2 - b_2)^2 + (a_3 - b_3)^2 \\ &= 2(x^2 - a_1b_1 - a_2b_2 - a_3b_3). \end{aligned}$$

Như vậy, $x$ chẵn và

$$a_1^2 + a_2^2 + a_3^2 \equiv b_1^2 + b_2^2 + b_3^2 \equiv 0 \pmod 4.$$

Điều này vô lí vì có ít nhất một trong các số $a_1$, $a_2$, $a_3$, $b_1$, $b_2$, $b_3$ là số lẻ.

**45.** Gọi độ dài các cạnh tam giác là $x - 1$, $x$, $x + 1$, chiều cao hạ xuống cạnh $x$ là $h$, diện tích $S$. Theo công thức Hêrông ta có :

$$S = \frac{hx}{2} = \sqrt{\frac{1}{2}(3x) \cdot \frac{1}{2}(x + 2) \cdot \frac{1}{2}x \cdot \frac{1}{2}(x - 2)} = \frac{1}{4}x\sqrt{3x^2 - 12}.$$

Vì $S$ và $h$ là các số nguyên nên $x$ chẵn. Đặt $x = 2y$. Khi đó $S = hy$ và $h = \sqrt{3(y^2 - 1)}$. Như vậy $h$ phải là số chia hết cho 3, chẳng hạn $h = 3z$. Ta có :

$$S = 3yz, \quad y^2 - 3z^2 = 1. \tag{1}$$

Như vậy, ta nhận được phương trình Pell (1). Để giải phương trình (1), ta xét các quan hệ truy hồi sau :

$$y_{n+1} = 2y_n + 3z_n, \quad z_{n+1} = 2z_n + y_n. \tag{2}$$

Từ (2) suy ra

$$y_n = 2y_{n+1} - 3z_{n+1}, \quad z_n = 2z_{n+1} - y_{n+1}. \tag{3}$$

Nếu các số $(y_n,\ z_n)$ thỏa mãn phương trình (1) thì các số $(y_{n+1},\ z_{n+1})$ cũng thỏa mãn, và ngược lại. Hơn nữa, từ (2) ta có :

$$y_{n+2} = 4y_{n+1} - y_n, \quad z_{n+2} = 4z_{n+1} - z_n. \tag{4}$$

Quan hệ (4) cho ta các nghiệm của (1). Ta sẽ chứng minh rằng, nghiệm tùy ý của (1) được xác định từ (4), và như vậy, ta có tất cả các nghiệm của (1) (do đó, xác định được tất cả các tam giác thỏa mãn bài ra).

Nếu các số $y_n,\ z_n$ không âm, thì từ (2) suy ra rằng $y_{n+1} > y_n$; $z_{n+1} > z_n$. Ngoài ra, nếu $y_{n+1},\ z_{n+1} \in \mathbb{N}$ thỏa mãn (1) thì bất đẳng thức

$$9z_{n+1}^2 = 3y_{n+1}^2 - 3 < 4y_{n+1}^2$$

kéo theo $3z_{n+1} < 2y_{n+1}$. Vậy $y_n > 0$. Tương tự, nếu $z_{n+1} \neq 1$ thì bất đẳng thức

$$y_{n+1}^2 = 3z_{n+1}^2 + 1 < 4z_{n+1}^2$$

kéo theo $y_n < 2z_{n+1}$, tức là $z_n > 0$. Vậy, nếu $(y_{n+1},\ z_{n+1})$ là nghiệm tùy ý của (1) và $z_{n+1} \neq 1$ thì $(y_n,\ z_n)$ xác định bởi (3) cũng thỏa mãn (1), đồng thời $y_n < y_{n+1}$, $z_n < z_{n+1}$. Việc chuyển từ giá trị $(y_{n+1},\ z_{n+1})$ sang $(y_n,\ z_n)$ phải dừng khi $z_n = 1$. Vậy, mọi nghiệm của (1) nhận được từ $y_0 = 1$, $z_0 = 0$, $y_1 = 2$, $z_1 = 1$ và quan hệ (2).

Từ các quan hệ (2), (3) và do $x_n = 2y_n$, ta được :

$$x_{n+2} = 4x_{n+1} - x_n. \tag{5}$$

Vậy, mọi tam giác thỏa mãn đầu bài có cạnh là $x_n - 1$, $x_n$, $x_n + 1$, trong đó các giá trị $x_n$ xác định bởi (5), với $x_1 = 4$, $x_2 = 2y_2 = 14$.

(Như vậy, tam giác nhỏ nhất thỏa mãn bài ra chính là tam giác có các cạnh 3, 4, 5).

**46.** Để giải bài toán, ta cần tìm các nghiệm nguyên dương của phương trình sau :

$$2^m + 3^n = t^2.$$

Do $t^2 \equiv 0$ hoặc $1$ môdulô $3$ nên suy ra $m$ phải là số chẵn, $m \geq 2$. Vậy $t^2$ là số lẻ và $t^2 \equiv 1 \pmod 4$. Suy ra $3^n \equiv 1 \pmod 4$ nên $n$ là số chẵn. Giả sử $n = 2q$ với $q$ là số nguyên dương. Ta có :

$$2^m = t^2 - 3^{2q} = (t + 3^q)(t - 3^q).$$

Vì tổng của hai nhân tử là $2t$, mà $t$ lẻ nên lũy thừa cao nhất của 2 mà là ước của cả hai nhân tử chỉ là 2, tức là :

$$t - 3^q = 2, \quad t + 3^q = 2^{m-1}.$$

Suy ra

$$3^q + 1 = 2^{m-2} \tag{1}$$

Nhưng $m$ chẵn, và rõ ràng $m \neq 2$ nên

$$3^q + 1 \equiv 0 \pmod 4.$$

Vậy $q$ lẻ. Nếu $q > 1$ thì

$$3^q + 1 = (3 + 1)\left(\sum_{k=0}^{q-1} (-1)^k 3^{q-1-k}\right),$$

trong đó tổng gồm $q$ số lẻ nên là một số lẻ. Do (1), tổng chỉ có thể bằng 1, và ta có $2^{m-2} = 4$, tức là $m = 4$. Suy ra $n = 2$, $t = 5$ :

$$2^4 + 3^2 = 5^2.$$

**47.** Ta sẽ chứng minh rằng, phương trình

$$x^y - y^x = x + y \tag{1}$$

chỉ có nghiệm nguyên dương duy nhất $(x,\ y) = (2,\ 5)$. Với mọi $x$, $y$ nguyên dương, vế phải của (1) dương. Trước hết ta tìm $x$, $y$ sao cho

$$x^y > y^x \tag{2}$$

(2) $\Leftrightarrow \dfrac{\ln x}{x} > \dfrac{\ln y}{y}$. Xét hàm số

$$f(x) = \frac{\ln x}{x}.$$

Ta có

$$f'(x) = \frac{1 - \ln x}{x^2}.$$

Như vậy, $f(x)$ là hàm tăng trên khoảng $(1,\ e]$ và giảm khi $x \geq e$. Do $2 < e < 3$ và

$$\frac{\ln 4}{4} = \frac{\ln 2}{2} < \frac{\ln 3}{3}$$

nên ta có các cặp $(x,\ y)$ nguyên dương thỏa mãn (2) như sau :

1) $(x,\ 1),\ x > 1$

2) $(2,\ y),\ y \geq 5$

3) $(3,\ 2)$

4) $(x,\ y),\ 3 \leq x < y.$

Thử trực tiếp cho thấy $(x,\ 1)$, $(3,\ 2)$ không phải là nghiệm, còn $(2,\ 5)$ là một nghiệm.

Khi $y \geq 6$ ta có : $2^y > y^2$ và $2^{y-1} > (y-1)^2$ (vì $2^k > k^2$ nếu $k > 4$). Từ đó suy ra

$$2^y - y^2 = 2.2^{y-1} - y^2 > 2(y-1)^2 - y^2 = y^2 - 4y + 2 > y + 2.$$

Vậy, các cặp $(2,\ y)$ với $y \geq 6$ không thỏa mãn.

Xét các cặp trong 4). Ta cố định $x = a \geq 3$ và xét $a^y - y^a$ như hàm của biến số $y$ với $y \geq a + 1$. Ta có

$$a^y - y^a = \left(a^y + \frac{y^{a+1}}{a+1}\right) + \left(\frac{y^{a+1}}{a+1} - y^a\right).$$

Lấy đạo hàm số hạng thứ nhất ta được

$$\ln a.a^y - y^a = (\ln a - 1)a^y + (a^y - y^a) > 0$$

vì $a \geq 3$ và $a^y - y^a > 0$. Như vậy, số hạng đầu tăng, nên lớn hơn giá trị tại $y = a$, và ta có :

$$a^y - y^a > \left(a^a - \frac{a^{a+1}}{a+1}\right) + y^a\left(\frac{y-a-1}{a+1}\right) =$$

$$= \frac{a^a}{a+1} + \frac{y^a}{a+1}(y-a-1) > a^{a-2} + y^{a-1}(y-a-1)$$

(vì $a^2 > a+1$ với $a \geq 3$, $y \geq a+1$).

Khi $y \geq a+2$ ta có $y-a-1>1$ nên vế phải lớn hơn hoặc bằng $a^{a-2} + y^{a-1} > a + y$ : cặp $(a,\ y)$ không phải là nghiệm.

Khi $y = a+1$, $a \geq 4$ thì $a^{a-2} \geq 4a^{a-3} > 4a > 2a+1 = a+y$ nên cặp $(a,\ a+1)$ với $a \geq 4$ cũng không phải là nghiệm. Chỉ còn phải xét cặp $(a,\ a+1)$ với $a = 3$, tức là cặp $(3,\ 4)$. Thử trực tiếp cho thấy $(3,\ 4)$ không phải là nghiệm.

Vậy, chỉ có cặp nghiệm duy nhất là $(2,\ 5)$.

**48.** Giả sử phương trình có nghiệm nguyên dương $(a,\ b)$, trong đó $1 < a < b$. Ta viết phương trình đã cho dưới dạng

$$a^x = b^y. \tag{1}$$

Rõ ràng các ước nguyên tố của $a$ và $b$ là như nhau. Ta đặt $a = p_1^{\alpha_1} \dots p_t^{\alpha_t}$, $b = p_1^{\beta_1} \dots p_t^{\beta_t}$, $\alpha_i$, $\beta_i$ là các số nguyên dương. Từ (1) suy ra rằng, với $i = 1,\ \dots,\ t$ ta có

$$\alpha_i x = \beta_i y.$$

Đặt

$$z = \frac{x}{y}.$$

Như vậy, với mọi $i = 1,\ \dots,\ t$, ta có

$$\beta_i = \alpha_i z, \quad b = a^z.$$

Ta chỉ ra rằng $z$ là số nguyên. Các số $x$ và $y$ có thể viết dưới dạng

$$x = a^u, \quad y = b^v,$$

trong đó $u$, $v$ nguyên. Khi đó

$$z = p_1^{(\alpha_1 u - \beta_1 v)} \dots p_t^{(\alpha_t u - \beta_t v)}.$$

Các số mũ ở vế phải đều là số nguyên. Nếu chúng dương thì $z$ là số nguyên. Từ phương trình (1) ta có :

$$z = \frac{\log b}{\log a}.$$

Mặt khác, do $a < b$ nên $x > y$, suy ra $a^u > b^v$ và

$$\frac{u}{v} > \frac{\log b}{\log a} = z = \frac{\beta_i}{\alpha_i}.$$

Vậy $\alpha_i u - \beta_i v > 0$ với $i = 1, \ldots, t$, tức là $z$ nguyên.

Từ biểu thức của $z$ ta có : $z = a^w$, trong đó $w = u - zv > 0$. Mặt khác, $u = a^s$ với $s$ nguyên dương nào đó (vì $a < b$ nên suy ra $n \geq 3$, $s \geq 1$). Từ biểu diễn của $w$ ta được

$$w + a^w v = u - a^s. \tag{2}$$

Do $v \geq 1$ nên vế trái $> a^w$, suy ra $s \geq w$. Như vậy từ (2) suy ra $a^w \mid w$ : vô lí nếu $a > 1$.

Vậy, với những điều kiện của bài toán, phương trình đã cho vô nghiệm.

**49.** Rõ ràng $x$, $y$, $z \neq 0$. Ta xét hai trường hợp : một trong các số $x$, $y$, $z$ bằng 1 và các số đều lớn hơn hay bằng 2.

a) Giả sử $x = 1$. Khi đó phương trình đã cho trở thành

$$(\sqrt{y} - 1)(\sqrt{z} - 1) = 4. \tag{1}$$

Ta chứng minh nếu các số nguyên dương không âm $y$, $z$ thỏa mãn phương trình (1) thì chúng phải là các số chính phương. Rõ ràng nếu một trong hai số là chính phương thì số kia cũng là số chính phương. Giả sử cả hai số đều không chính phương. Nhân hai vế của (1) với $(\sqrt{y} + 1)$ ta được

$$4 + 4\sqrt{y} = (1 - y^2) + (y^2 - 1)\sqrt{z}. \tag{2}$$

Giả sử $\sqrt{y} = y_0\sqrt{y_1}$, $\sqrt{z} = z_0\sqrt{z_1}$, trong đó $y_0$, $y_1$, $z_0$, $z_1$ là các số nguyên dương, đồng thời $y_1$, $z_1$ là tích các thừa số nguyên tố khác nhau. Đặt $a = 4y_0$, $b = 1 - y^2$, $c = (y^2 - 1)z_0$ ta có :

$$4 + a\sqrt{y_1} = b + c\sqrt{z_1}. \tag{3}$$

Suy ra

$$(4 - b)^2 = (c\sqrt{z_1} - a\sqrt{y_1})^2 \Rightarrow 16 + b^2 - 8b - c^2 z_1 - a^2 y_1 = -2ac\sqrt{z_1 y_1}.$$

Như vậy $z_1 y_1$ phải là số chính phương, mà do $z_1$, $y_1$ đều là tích các số nguyên tố khác nhau (với số mũ 1) nên suy ra $z_1 = y_1$. Từ (3) ta có

$4 = b = 1 - y^2$ : vô lí. Như vậy $y$, $z$ đều là số chính phương và từ (1) ta được

$$\begin{cases} \sqrt{y} - 1 = 1 \\ \sqrt{z} - 1 = 4 \end{cases} \quad \text{hoặc} \quad \begin{cases} \sqrt{y} - 1 = 2 \\ \sqrt{z} - 1 = 2. \end{cases}$$

Ta nhận được các nghiệm $(x, y, z) = (1, 9, 9)$, $(1, 4, 25)$ (và các hoán vị của chúng).

b) Xét trường hợp $x, y, z \geq 2$. Ta xem $x \leq y \leq z$. Đặt

$$f(x, y, z) = \sqrt{xyz} - \sqrt{x} - \sqrt{y} - \sqrt{z} - 2$$
$$= \sqrt{x}(\sqrt{yz} - 1) - \sqrt{y} - \sqrt{z} - 2.$$

Với $y$, $z$ cố định, $f(x, y, z)$ là hàm tăng theo biến $x$. Ta cũng có điều tương tự khi cố định $x$, $y$ hoặc $x$, $z$. Như vậy, nếu $(x, y, z)$ là một nghiệm thì

$$0 = f(x, y, z) \geq f(z, y, y) \Rightarrow 2\sqrt{y^2} - \sqrt{2} - 2\sqrt{y} - 2 \leq 0$$
$$\Rightarrow y \leq \left(\frac{\sqrt{2}}{2} + \sqrt{\frac{3}{2} + \sqrt{2}}\right)^2 < 5{,}83.$$

Vậy $y \leq 5$.

$$z = \left(\frac{\sqrt{x} + \sqrt{y} + 2}{\sqrt{xy} - 1}\right)^2, \quad 2 \leq x \leq y \leq 5.$$

Thử trực tiếp, ta thấy chỉ có nghiệm $x = y = z = 4$.

**50.** Không giảm tổng quát, giả sử $1 < a < b < c < d$. Đặt

$$x = abcd - 1, \quad y = (a-1)(b-1)(c-1)(d-1).$$

Giả sử $y \mid x$. Nếu một trong các số $a$, $b$, $c$, $d$ chẵn thì $x$ lẻ nên $y$ lẻ, suy ra $a$, $b$, $c$, $d$ đều là chẵn. Vậy các số $a$, $b$, $c$, $d$ cùng chẵn hoặc cùng lẻ.

Trước tiên ta có nhận xét rằng, hàm $\dfrac{t}{t-1}$ là hàm giảm theo $t$. Do đó, nếu $a \geq 5$ thì

$$k = \frac{x}{y} = \frac{abcd - 1}{(a-1)(b-1)(c-1)(d-1)} < \frac{a}{a-1} \cdot \frac{b}{b-1} \cdot \frac{c}{c-1} \cdot \frac{d}{d-1}$$

$$< \frac{5}{4} \cdot \frac{6}{5} \cdot \frac{7}{6} \cdot \frac{8}{7} = 2,$$

suy ra $x = y$ : vô lí.

Khi $a = 4$ (suy ra $b \geq 6$, $c \geq 8$, $d \geq 10$) ta có :

$$k = \frac{x}{y} < \frac{4}{3} \cdot \frac{6}{5} \cdot \frac{8}{7} \cdot \frac{10}{9} < 3.$$

Vậy $k = 2$ : vô lí, vì $x$ lẻ.

Khi $a = 3$ (suy ra $b \geq 5$, $c \geq 7$, $d \geq 9$) ta có :

$$k = \frac{x}{y} < \frac{3}{2} \cdot \frac{5}{4} \cdot \frac{7}{6} \cdot \frac{9}{7} < 3.$$

Vậy $k = 2$. Mặt khác, do $x \equiv -1 \pmod 3$ nên các số $b-1$, $c-1$, $d-1$ không chia hết cho 3. Do đó, nếu $b \neq 5$ thì $b \geq 9$ (và $c \geq 11$, $d \geq 15$). Ta được

$$k < \frac{3}{2} \cdot \frac{9}{8} \cdot \frac{11}{10} \cdot \frac{15}{14} < 2 \text{ : vô lí.}$$

Vậy $b = 5$, và ta nhận được phương trình

$$15cd - 1 = 16(c-1)(d-1) \Rightarrow (c-16)(d-16) = 239 \Rightarrow c = 17$$

$$\Rightarrow (a,\ b,\ c,\ d) = (3,\ 5,\ 17,\ 255).$$

Chỉ còn phải xét trường hợp $a = 2$. Khi đó $(a,\ b,\ c,\ d)$ chẵn, $k = \frac{x}{y}$ lẻ. Ta có :

$$k = \frac{x}{y} < \frac{2}{1} \cdot \frac{4}{3} \cdot \frac{6}{5} \cdot \frac{8}{7} < 4.$$

Vì $k$ lẻ nên suy ra $k = 3$. Do $abcd - 1 = 3y$ nên $b$, $c$, $d$ không chia hết cho 3. Vậy nếu $b \neq 4$ thì $b \geq 8$ (suy ra $c \geq 10$, $d \geq 14$). Ta được

$$k = \frac{x}{y} < \frac{2}{1} \cdot \frac{8}{7} \cdot \frac{10}{9} \cdot \frac{14}{13} < 3.$$

Vô lí vì $k$ lẻ $\neq 1$. Vậy $b = 4$ và ta có phương trình

$$8cd - 1 = 3y = 9(c-1)(d-1) \Rightarrow (c-9)(d-9) = 71$$

$$\Rightarrow (a,\ b,\ c,\ d) = (2,\ 4,\ 10,\ 80).$$

Vậy, các nghiệm của bài toán là

$$(3,\ 5,\ 17,\ 255)\ ;\ (2,\ 4,\ 10,\ 80)$$

và các hoán vị của chúng.

**51.** Đặt

$$F(x,\ y,\ z) = \frac{(x+y+z)^2}{xyz}.$$

Giả sử $n$ là số nguyên dương nào đó sao cho tồn tại bộ số nguyên dương $(x,\ y,\ z)$ để $n = F(x,\ y,\ z)$. Ta giả sử $(x,\ y,\ z)$ là một bộ số như vậy, đồng thời $x \le y \le z$ và $z$ đạt cực tiểu trong tất cả các bộ số thỏa mãn điều kiện $n = F(x,\ y,\ z)$, $x \le y \le z$. Ta có :

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

Từ đó suy ra $z \mid (x+y)^2$. Mặt khác, nếu $(x+y+z)$ thỏa mãn điều kiện đòi hỏi thì

$$F\left(x,\ y,\ \frac{(x+y)^2}{z}\right) = n.$$

Như vậy, nếu $z > (x+y)$ thì $\dfrac{(x+y)^2}{z} < z$, trái với giả thiết về tính cực tiểu của $z$. Từ đó suy ra

$$x + y \ge z.$$

Ta có :

$$\begin{aligned} n &= \frac{x}{yz} + \frac{y}{xz} + \frac{z}{xy} + \frac{2}{x} + \frac{2}{y} + \frac{2}{z} \\ &\le \frac{1}{z} + \frac{1}{x} + \left(\frac{1}{y} + \frac{1}{x}\right) + \frac{2}{x} + \frac{2}{y} + \frac{2}{z} \\ &\le \frac{7}{x} + \frac{3}{z}. \end{aligned}$$

Vậy, $n$ lớn nhất khi $z = 1$ (suy ra $x = y = z = 1$), tức là $n \le 9$. Ta chứng tỏ $n \ne 7$. Giả sử ngược lại,

$$7 = \frac{7}{z} + \frac{3}{z}$$

Khi đó $x \geq 2 \Rightarrow \frac{7}{x} + \frac{3}{z} \leq \frac{7}{2} + \frac{3}{2} = 5$ : vô lí. Tính trực tiếp, ta được :

$F(9, 9, 9) = 1$, $F(4, 4, 8) = 2$, $F(3, 3, 3) = 3$, $F(2, 2, 2) = 4$,

$F(1, 4, 5) = 5$, $F(1, 2, 3) = 6$, $F(1, 1, 2) = 8$, $F(1, 1, 1) = 9$.

**52.** Xét tổng của $y$ số tự nhiên liên tiếp

$$x + (x + 1) + \cdots + (x + y) = \frac{(y + 1)(2x + y)}{2}.$$

Như vậy, một số nguyên dương $S$ biểu diễn được như tổng một số số tự nhiên liên tiếp nếu tồn tại các số nguyên dương $(x, y)$ để

$$S = \frac{(y + 1)(2x + y)}{2} \tag{1}$$

Giả sử $S$ là số tự nhiên có dạng (1). Xét các trường hợp :

a) $y$ chẵn, $y = 2z$. Khi đó (2) trở thành

$$(2z + 1)(x + z) = S. \tag{2}$$

Như vậy, $u = 2z + 1$ là một ước lẻ của $S$, đồng thời $u > 1$. Ngược lại, giả sử $S = uv$, $u > 1$ và $u$ lẻ. Đặt $2s + 1 = u$, $x + z = v$ ta có :

$$z = \frac{1}{2}(u - 1), \quad x = \frac{1}{2}(2v - u + 1).$$

Rõ ràng $(x, z)$ là một nghiệm của (2) và nó cho ta một cách biểu diễn của $S$ nếu và chỉ nếu

$$2v - u \geq 1. \tag{3}$$

b) $y$ lẻ, $y = 2z + 1$. Khi đó (1) trở thành

$$s(2x + 2z - 1) = S \tag{4}$$

$u = 2x + 2z - 1 > 1$ là một ước lẻ của $S$. Ngược lại, giả sử $S = uv$, $u > 1$ lẻ. Đặt $2x + 2z - 1 = u$, $z = v$ ta có $x = \frac{1}{2}(u - 2v + 1)$. Rõ ràng $(x, z)$ là một nghiệm của (4) và cho ta một cách biểu diễn của $S$ nếu và chỉ nếu

$$u - 2v \geq 1. \tag{5}$$

Nếu $u > 1$ là một ước lẻ của $S$, $S = uv$, thì có một và chỉ một trong

các điều kiện (3), (5) thỏa mãn, nên chỉ cho ta một cách biểu diễn $S$.

**53.** Với mọi số nguyên $n$ ta có :

$$n^2 \equiv \begin{cases} 0 \pmod 8 & \text{nếu } n \equiv 0 \pmod 4 \\ 1 \pmod 8 & \text{nếu } n \equiv 1,\ 3 \pmod 4 \\ 4 \pmod 8 & \text{nếu } n \equiv 2 \pmod 4 \end{cases}$$

Như vậy, với mọi số nguyên $m$, ta có:

$$n^2 \equiv \begin{cases} 0,\ 1 \text{ hoặc } 4 \pmod 8 & \text{nếu } n \equiv 0 \pmod 4 \\ 1,\ 2 \text{ hoặc } 5 \pmod 8 & \text{nếu } n \equiv 1,\ 3 \pmod 4 \\ 0,\ 4 \text{ hoặc } 5 \pmod 8 & \text{nếu } n \equiv 2 \pmod 4 \end{cases}$$

Ta có $(x+1)$, $(x+2)$, $(x+3)$, $(x+4)$ lập thành một hệ thặng dư đầy đủ môdulô 4. Nếu phương trình có nghiệm nguyên thì tồn tại số nguyên $n$ sao cho

$$(x+1)^2 + a^2 \equiv (x+2)^2 + b^2 \equiv (x+3)^2 + c^2$$
$$\equiv (x+4)^2 + d^2 \equiv n \pmod 8.$$

Từ nhận xét đã nêu về đồng dư $(n^2 + m^2) \pmod 8$ suy ra rằng :

$$n \in \{0,\ 1,\ 4\} \cap \{1,\ 2,\ 5\} \cap \{0,\ 4,\ 5\}.$$

Nhưng giao ba tập hợp trên bằng rỗng, suy ra không tồn tại $n$. Vậy phương trình đã cho không có nghiệm nguyên.

**54.** Xét phương trình

$$y^2 = 1 + x + x^2 + x^3 + x^4. \tag{1}$$

Từ (1) ta có :

$$y^2 = \left(x^2 + \frac{x}{2} + 1\right)^2 - \frac{5x^2}{4}. \tag{2}$$

Suy ra

$$|y| \le x^2 + \frac{x}{2} + 1. \tag{3}$$

Mặt khác, từ (1) cũng suy ra phương trình sau đây :

$$y^2 = \left(x^2 + \frac{x}{2} + \frac{\sqrt{5}-1}{4}\right)^2 + \frac{5-2\sqrt{5}}{4}\left(x + \frac{3+\sqrt{5}}{2}\right)^2.$$

Suy ra

$$|y| \geq x^2 + \frac{x}{2} + \frac{\sqrt{5}-1}{4}. \tag{4}$$

Từ (3) và (4) ta có :

$$|y| = x^2 + \frac{x+a}{2}, \quad 0 < a \leq 2.$$

Nếu $x$ chẵn thì $a = 2$, nên từ (2) suy ra $x = 0$, $y \neq \pm 1$. Nếu $x$ lẻ thì $a = 1$. Khi đó

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

Từ (1) ta được

$$x^4 + x^3 + x^2 + \left(\frac{x+1}{2}\right)^2 = 1 + x + x^2 + x^3 + x^4.$$

Phương trình cho nghiệm $x = 3$ và $x = -1$. Tương ứng ta được $y = \pm 11$ và $y = \pm 1$.

Vậy, các nghiệm của phương trình là

$$x = 0,\ y = \pm 1\ ;\ x = -1,\ y = \pm 1\ ;\ x = 3,\ y = \pm 11.$$

**55.** Xét hệ phương trình

$$\begin{cases} x + y + z = m & (1) \\ x^2 + y^2 + z^2 = n & (2) \end{cases}$$

trong đó $m$, $n$ là các số nguyên.

Khử $x$ từ hệ phương trình, ta được :

$$2(y^2 + yz + z^2 - my - mz) = n - m^2. \tag{3}$$

Do đó, $n - m^2$ là số chẵn, nên $m$ và $n$ phải cùng chẵn hoặc cùng lẻ. Ta đặt

$$x = \frac{m}{3} - s \tag{4}$$

$$y = \frac{s-t}{2} + \frac{m}{3} \tag{5}$$

$$z = \frac{s+t}{2} + \frac{m}{3} \tag{6}$$

Từ (5) và (6) ta được : $t = z - y$, tức $t$ là số nguyên. Không giảm tổng quát, ta xem $t$ là số nguyên không âm, vì việc đổi dấu $t$ chỉ dẫn đến việc đổi chỗ $y$ và $z$ mà không sinh ra bộ nghiệm nguyên mới của hệ đang xét. Khi $t = 0$, ta có $y = z$, và hệ được đưa về hệ hai phương trình với hai ẩn.

Thay (4), (5), (6) vào (2), ta được :

$$3s^2 + t^2 = 2\left(n - \frac{m^2}{3}\right). \tag{7}$$

Vậy, điều kiện là $n \geq \frac{m^2}{3}$. Xét các trường hợp sau :

• *Trường hợp 1.* $m \vdots 3$. Khi đó, từ (4) suy ra $s$ nguyên. Vì $y$, $z$ nguyên nên từ (5) và (6) suy ra $s$, $t$ cùng chẵn hoặc cùng lẻ. Mỗi cặp $(s, t)$ thỏa mãn (7) sinh ra một bộ $(x, y, z)$ thỏa mãn (1) và (2). Nghiệm $(x, y, z)$ với $s > 0$ khác với nghiệm $(x, y, z)$ tương ứng với giá trị ngược dấu của $s$ (nhưng cùng $|s|$). Khi $s = t$ thì $s$ và $-s$ cho cùng một bộ nghiệm $(x, y, z)$. Các cặp $(s, t)$ khác nhau thỏa mãn (7) không nhất thiết dẫn đến các bộ nghiệm $(x, y, z)$ khác nhau của (1) và (2). Thật vậy do tính đối xứng của $x$, $y$, $z$ trong (1) và (2), nếu giá trị mới của $s$ cho giá trị $x$ trùng với $y$ (hoặc $z$) ứng với giá trị $s$ trước đó, thì giá trị $s$ mới này không cho bộ nghiệm mới. Vì vậy, trừ các trường hợp đặc biệt, mỗi bộ nghiệm $(x, y, z)$ tương ứng với ba cặp giá trị khác nhau của $s$ và $t$.

• *Trường hợp 2.* $a$ không chia hết cho 3.

Khi đó $s$ có dạng $\frac{p}{3}$, trong đó $p$ là số nguyên sao cho $\frac{m - p}{3}$ nguyên. Các cặp $p$ và $t$ dùng để tính $(x, y, z)$ phải thỏa mãn (7), và dấu của $p$ được chọn để thỏa mãn (4). Các số $t$ và $p$ phải cùng chẵn hoặc cùng lẻ.

**Chú ý :** Để hiểu phương pháp giải trên đây một cách cặn kẽ, người đọc nên thử tính toán với $m$, $n$ cụ thể.

Chẳng hạn, với $m = 54$, $n = 1406$ ta được các nghiệm sau :

$$(15, 5, 34),\ (21, 2, 31),\ (10, 9, 35),\ (26, 1, 27).$$

**56.** Giả sử $p$ là số nguyên tố lẻ sao cho

$$x^{2^n} + y^{2^n} \equiv 0 \pmod{p}.$$

Do $(x,\ y) = 1$ nên $x \not\equiv 0 \pmod{p}$, $y \not\equiv 0 \pmod{p}$.

Giả sử $a$ là số nguyên sao cho $ay \equiv 1 \pmod{p}$ ($a$ tồn tại vì $(y,\ p) = 1$). Khi đó ta có

$$(ax)^{2^n} \equiv -1 \pmod{p}.$$

Đặt $u = ax$. Vì $(u,\ p) = 1$ nên

$$u^{p-1} \equiv 1 \pmod{p}.$$

Kí hiệu $d = (p-1,\ 2^n)$. Khi đó ta có

$$(-1)^{\frac{p-1}{d}} \equiv \left(u^{2^n}\right)^{\frac{p-1}{d}} \equiv \left(u^{p-1}\right)^{\frac{2^n}{d}} \equiv 1 \pmod{p}.$$

Vậy $\dfrac{p-1}{d}$ là số chẵn, mà

$$\left(\frac{p-1}{d},\ \frac{2^n}{d}\right) = 1$$

nên suy ra $d = 2^n$. Vậy $(p-1)$ chia hết cho $2^{n+1}$, tức là

$$p = 2^{n+1}m + 1. \tag{1}$$

Một ước lẻ tùy ý của số $x^{2^n} + y^{2^n}$ là tích các số có dạng (1) nên cũng là số có dạng (1).

**57.** Ta có

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Như vậy, ta cần tìm $n > 1$ nhỏ nhất sao cho phương trình

$$(n+1)(2n+1) = 6m^2$$

có nghiệm nguyên.

Dễ thấy rằng, $(n+1)(2n+1)$ chia hết cho 6 khi và chỉ khi $n \equiv 1$ hoặc $5 \pmod{6}$. Ta xét hai trường hợp :

a) $n = 6k + 5$. Khi đó

$$m^2 = (k+1)(12k+11).$$

Do $(k+1)$ và $(12k+11)$ nguyên tố cùng nhau, nên mỗi một trong chúng phải là số chính phương, chẳng hạn

$$k+1 = a^2, \quad 12k+11 = b^2.$$

Suy ra

$$12a^2 = b^2 + 1.$$

Ta có : $12a^2 \equiv 0 \pmod 4$, $b^2 + 1 \equiv 1$ hoặc $2 \pmod 4$. Vậy, phương trình đã cho vô nghiệm.

b) $n = 6k + 1$. Khi đó ta có

$$m^2 = (3k+1)(4k+1).$$

Lí luận tương tự như trường hợp a), ta chỉ ra rằng tồn tại $a$, $b$ tự nhiên sao cho

$$3k+1 = a^2, \quad 4k+1 = b^2.$$

Khi đó $(2a-1)(2a+1) = 3b^2$.

Mọi ước nguyên tố của vế trái, trừ số 3, đều phải tham gia với số mũ chẵn. Ta kiểm tra lần lượt từ $a = 1$ với những $a$ sao cho $(2a-1)$ hoặc $(2a+1)$ có ước nguyên tố khác 3.

Với $a = 1 : b = 1 \Rightarrow n = 1$ (trái giả thiết $n > 1$)

$a = 2$ : Không tồn tại $b$, tương tự cho $a = 3,\ 4,\ \ldots,\ 12$.

Với $a = 13$, ta được $b = 5.3 = 15$. Suy ra $k = 56$, $n = 337$ là số cần tìm.

**58.** Có thể giả thiết $x$, $y$, $z$ không âm. Trước tiên, ta có nhận xét rằng,

$$n^2 \equiv \begin{cases} 0 \pmod 4 \text{ nếu } n \text{ chẵn} \\ 1 \pmod 4 \text{ nếu } n \text{ lẻ} \end{cases}$$

Xét các trường hợp sau :

a) $x$, $y$, $z$ đều lẻ. Khi đó

$$x^2 + y^2 + z^2 \equiv 3 \pmod 4$$

$$x^2y^2 \equiv 1 \pmod 4.$$

Vậy, phương trình không có các nghiệm $x$, $y$, $z$ đều lẻ.

b) Hai trong số các số $x$, $y$, $z$ lẻ, số kia chẵn. Khi đó

$$x^2 + y^2 + z^2 \equiv 2 \pmod 4$$

$$x^2y^2 \equiv 0 \text{ hoặc } 1 \pmod 4.$$

Phương trình không có các nghiệm rơi vào trường hợp này.

c) Hai trong các số $x$, $y$, $z$ chẵn, số kia lẻ. Khi đó

$$x^2 + y^2 + z^2 \equiv 1 \pmod 4$$

$$x^2y^2 \equiv 0 \pmod 4.$$

Phương trình cũng không có nghiệm rơi vào trường hợp này. Vậy, nếu có nghiệm $(x, y, z)$ thì cả ba số phải chẵn. Giả sử $x = 2x_1$, $y = 2y_1$, $z = 2z_1$. Ta được

$$x_1^2 + y_1^2 + z_1^2 = 4x_1^2y_1^2.$$

Mặt khác, $4x_1^2y_1^2 \equiv 0 \pmod 4$ và mỗi một trong các số $x_1^2$, $y_1^2$, $z_1^2$ đồng dư $0$ hoặc $1$ môđulô $4$. Từ đó suy ra $x_1^2 \equiv y_1^2 \equiv z_1^2 \pmod 4$, tức là $x_1$, $y_1$, $z_1$ đều chẵn. Giả sử $x_1 = 2x_2$, $y_1 = 2y_2$, $z_1 = 2z_2$. Ta được phương trình

$$16x_2^2y_2^2 = x_2^2 + y_2^2 + z_2^2.$$

Từ đó, lại suy ra $x_2$, $y_2$, $z_2$ đều chẵn và dẫn đến phương trình

$$64x_3^2y_3^2 = x_3^2 + y_3^2 + z_3^2.$$

trong đó $x = 8x_3$, $y = 8y_3$, $z = 8z_3$.

Tiếp tục quá trình, ta thấy rằng $x$, $y$, $z$ chia hết cho lũy thừa tùy ý của $2$, suy ra $x = y = z = 0$. Đây chính là nghiệm duy nhất của phương trình.

**Nhận xét.** Lời giải trên đây là một ví dụ của phương pháp lùi vô hạn của Fermat. Bằng phương pháp đó, ta có thể chứng minh các phương trình sau chỉ tồn tại nghiệm nguyên tầm thường duy nhất (các số đều bằng $0$):

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

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

3) $x^2 + y^2 + z^2 + w^2 = 2xyzw$.

**59.** Giả sử $n$ là số nguyên dương sao cho phương trình

$$(x + y + u + v)^2 = n^2xyuv$$

có nghiệm nguyên dương. Viết phương trình dưới dạng

$$x^2 + 2(y + u + v)x + (y + u + v)^2 = n^2xyuv. \qquad (1)$$

Giả sử $(x_0,\ y_0,\ u_0,\ v_0)$ là nghiệm nguyên dương của phương trình (1) sao cho $x_0 + y_0 + u_0 + v_0$ đạt giá trị nhỏ nhất. Không giảm tổng quát, giả sử $x_0 \geq y_0 \geq u_0 \geq v_0$. Ta có :

1) $(y_0 + u_0 + v_0)^2$ chia hết cho $x_0$

2) $x_0$ là nghiệm nguyên dương của tam thức bậc hai

$$P(x) = x^2 - n^2y_0u_0v_0x + 2(y_0 + u_0 + v_0)x + (y_0 + u_0 + v_0)^2.$$

Theo Định lí Viét, ngoài nghiệm $x_0$, tam thức $P(x)$ còn có nghiệm nguyên dương

$$x_1 = \frac{(y_0 + u_0 + v_0)^2}{x_0}.$$

Như vậy, $(x_1,\ y_0,\ u_0,\ v_0)$ là một nghiệm nguyên dương của (1). Do cách xác định $(x_0,\ y_0,\ u_0,\ v_0)$ ta có :

$$x_1 \geq x_0 \geq y_0 \geq u_0 \geq v_0 \qquad (2)$$

Theo định lí về dấu của tam thức bậc hai, ta thấy :

$$0 \leq P(y_0) = y_0^2 - n^2y_0^2u_0v_0 + 2(y_0 + u_0 + v_0)y_0 + (y_0 + u_0 + v_0)^2$$
$$\leq 16y_0^2 - n^2y_0^2u_0v_0.$$

Vậy

$$n^2y_0^2u_0v_0 \leq 16y_0^2,$$

suy ra $n^2 \leq n^2u_0v_0 \leq 16$. Như vậy, $n$ chỉ có thể nhận các giá trị 1, 2, 3, 4.

Thử lại ta thấy với các giá trị trên của $n$, phương trình (1) có các nghiệm nguyên dương :

Với $n = 1$, phương trình có nghiệm $x = y = u = v = 4$.

Với $n = 2$, phương trình có nghiệm $x = y = u = v = 2$.

Với $n = 3$, phương trình có nghiệm $x = y = 1$, $u = v = 2$.

Với $n = 4$, phương trình có nghiệm $x = y = u = v = 1$.

Vậy, tất cả các giá trị $n$ cần tìm là $n = 1,\ 2,\ 3,\ 4$.

**60.** a) Ta chỉ ra 11 số liên tiếp thỏa mãn bài ra :

$18^2 + 19^2 + 20^2 + 21^2 + 22^2 + 23^2 + 24^2 + 25^2 + 26^2 + 27^2 + 28^2 = 77^2$.

b) Giả sử $n$ là số tự nhiên sao cho tồn tại $n$ số tự nhiên liên tiếp có tổng các bình phương là một số chính phương. Khi đó, tồn tại các số tự nhiên $x$, $y$ sao cho

$$(x+1)^2 + \cdots + (x+n)^2 = y^2.$$

Ta có

$$nx^2 + n(n+1)x + \frac{n(n+1)(2n+1)}{6} = y^2. \qquad (1)$$

Ta chỉ ra rằng, khi $3 < n \le 10$, phương trình (1) không có nghiệm nguyên, $x \ge 0$, $y \ge 1$.

Nếu (1) thỏa mãn thì số dư của $y^2$ chia $n$ bằng số dư của $\dfrac{n(n+1)(2n+1)}{6} = a$ chia $n$. Khi $n = 3$, 4 hoặc 9 thì số dư tương ứng là 2, 2, 6 ($a = 14,\ 30,\ 15.19$). Rõ ràng khi đó không tồn tại $y$ thỏa mãn.

Xét $n = 5$ hoặc $n = 7$. Khi đó $a \vdots n$ nên $y \vdots n$ (vì trong trường hợp này, $n$ nguyên tố), ta có $y = nz$.

Đặt

$$t = x + \frac{n+1}{2}.$$

Khi đó

$$t^2 + \frac{n^2 - 1}{12} = z^2,$$

tức là

$$z^2 - t^2 = \frac{n^2 - 1}{12}.$$

Phương trình này vô nghiệm

**61.** Giả sử $n$ là giá trị để phương trình

$$x^3 + y^3 + z^3 = nx^2y^2z^2 \tag{1}$$

có nghiệm nguyên dương $x,\ y,\ z$. Không giảm tổng quát, giả sử $x \le y \le z$. Khi đó

$$z = nx^2y^2 - \frac{x^3 + y^3}{z^2} \ge nx^2y^2 - (x + y).$$

Do $x^3 + y^3$ chia hết cho $z^2$ nên

$$x^3 + y^3 \ge z^2 \ge (nx^2y^2 - (x + y))^2.$$

Suy ra

$$n^2x^4y^4 < 2nx^2y^2(x + y) + x^3 + y^3.$$

Chia hai vế cho $nx^3y^3$ ta được

$$nxy < \left(\frac{1}{x} + \frac{1}{y}\right) + \frac{1}{nx^3} + \frac{1}{ny^3}. \tag{2}$$

Nếu $x \ge 2$ thì do $y \ge x$, vế trái $\ge 4$, trong khi vế phải $\le 3$. Vậy $x = 1$.

Thay $x = 1$ vào, ta được :

$$ny < 2 + \frac{2}{y} + \frac{1}{n} + \frac{1}{ny^3} \Rightarrow y \le 3.$$

Mặt khác, $x^3 + y^3 = 1 + y^3 \ \vdots\ z^2$. Do $z \ge y$ nên :

+ $y = 1 \Rightarrow z = 1$

+ $y = 2 \Rightarrow z = 3$

+ $y = 3 \Rightarrow$ không tồn tại $z$.

Vậy, chỉ có các nghiệm (1, 1, 1) và (1, 2, 3). Các nghiệm này ứng với $n = 3$ và $n = 1$.

**62.** Khi $n = 1$, ta có phương trình

$$4x + (x+1)^2 = y^2,$$

suy ra

$$(x+3)^2 - y^2 = 8 \Rightarrow (x+y+3)(x-y+3) = 8.$$

Do $x + y + 3 \geq 5$ nên ta có hệ phương trình

$$\begin{cases} x + y + 3 = 8 \\ x - y + 3 = 1. \end{cases}$$

Hệ không có nghiệm nguyên dương.

Khi $n \geq 3$, giả sử phương trình có nghiệm. Ta có

$$4x^n = (y - x - 1)(y + x + 1).$$

Các nhân tử ở vế phải cùng tính chẵn lẻ nên suy ra chúng đều là số chẵn. Đặt

$$y - x - 1 = 2a \Rightarrow y + x + 1 = 2(a + x + 1) \Rightarrow x^n = a(a + x + 1).$$

Do $a$ và $(a + x + 1)$ nguyên tố cùng nhau (vì nếu $d \mid a$, $d \mid (a + x + 1)$ thì $d \mid x \Rightarrow d \mid 1$) nên tồn tại $u$, $v$ nguyên sao cho

$$a = u^n,\ a + x + 1 = v^n,\ x = uv.$$

Do $n \geq 3$ nên

$$uv + 1 = x + 1 = v^n - u^n = (v - u)(v^{n-1} + v^{n-2}u + \cdots + u^{n-1})$$

$$\geq 1 + uv + v^2.$$

Vô lí, vậy khi $n \geq 3$, phương trình không có nghiệm nguyên dương.

Xét $n = 2$. Ta có phương trình

$$4x^2 + (x+1)^2 = y^2 \Rightarrow 5(x+1)^2 - 5y^2 = -4 \Rightarrow z^2 - 5y^2 = -4, \quad (1)$$

trong đó $z = 5x + 1$.

Phương trình (1) có nghiệm $(z,\ y) = (1,\ 1)$. Mặt khác, nếu $(z,\ y)$ là một nghiệm của (1) thì cặp $(z',\ y')$ với

$$\begin{cases} z' = 161z + 360y \\ y' = 72z + 161y \end{cases}$$

cũng là một nghiệm. Hơn nữa, nếu $z \equiv 1 \pmod 5$ (và do đó tồn tại $x$ nguyên dương để $z = 5x + 1$) thì $z'$ cũng thỏa mãn $z' \equiv 1 \pmod 5$.

Vậy khi $n = 2$, phương trình đã cho có vô số nghiệm.

**63.** Ta chứng minh kết quả tổng quát sau đây :

Giả sử đối với $n \geq 2$, phương trình

$$x^n + y^n = z^n$$

có nghiệm nguyên không tầm thường $(xyz \neq 0)$. Khi đó :

1) Nếu $n = (p-1)k$, $p \geq 3$ là số nguyên tố thì $x$ hoặc $y$ chia hết cho $p$.

2) Nếu $n = \dfrac{(p-1)k}{2}$, $p \geq 5$ là số nguyên tố, thì $x$, $y$ hoặc $z$ chia hết cho $p$.

Như vậy, a) là hệ quả của 1) với $n = 2$, $p = 3$ ; b) là hệ quả của 2) với $n = 2$, $p = 5$.

*Chứng minh 1).* Giả sử $n = (p-1)k$ và $x$, $y$ đều không chia hết cho $p$. Theo Định lí Fermat bé,

$$x^n \equiv y^n \equiv 1 \pmod p.$$

Nếu $z$ cũng không chia hết cho $p$ thì

$$z^n \equiv 1 \pmod p.$$

Nếu $z$ chia hết cho $p$ thì

$$z^n \equiv 0 \pmod p.$$

Trong cả hai trường hợp,

$$x^n + y^n \not\equiv z^n \pmod p.$$

*Chứng minh 2).* Giả sử $n = \dfrac{(p-1)k}{2}$, và các số $x$, $y$, $z$ không chia hết cho $p$. Khi $p \geq 5$, ta có :

$$x^n \equiv \pm 1 \pmod p,\ y^n \equiv \neq 1 \pmod p,\ z^n \equiv \pm 1 \pmod p.$$

Như vậy, $x^n + y^n \equiv 0$ hoặc $\pm 2 \pmod p$, suy ra

$$x^n + y^n \not\equiv z^n \pmod{p}.$$

**64.** a) Giả sử $a$ là số nguyên dương sao cho $a+1$ và $3a+1$ là số chính phương :

$$a+1 = x^2, \quad 3a+1 = y^2.$$

Khi đó ta có

$$y^2 - 3x^2 = -2. \tag{1}$$

Vì $x^2$ và $y^2$ chỉ có thể đồng dư với 0 hoặc 1 môđulô 4, nên từ (1) suy ra rằng $x$, $y$ đều là số lẻ. Ta viết lại phương trình (1) dưới dạng :

$$\left(\frac{3x-y}{2}\right)^2 - 3\left(\frac{y-x}{2}\right)^2 = 1.$$

Ta chỉ xét các nghiệm $x$, $y$ nguyên dương. Khi đó, rõ ràng $x \le y \le 3x$. Đặt

$$u = \frac{3x-y}{2}, \quad v = \frac{y-x}{2}.$$

Ta nhận được phương trình Pell sau đây :

$$u^2 - 3v^2 = 1. \tag{2}$$

Nghiệm nguyên dương nhỏ nhất của phương trình (2) là $(u_1, v_1) = (2, 1)$. Các nghiệm $(u_n, v_n)$ $(n = 2, 3, \ldots)$ khác thỏa mãn :

$$u_n \pm v_n\sqrt{3} = (u_1 \pm v_1\sqrt{3})^n = (2 \pm \sqrt{3})^n.$$

Đặt $\alpha = 2+\sqrt{3}$, $\beta = 2-\sqrt{3}$ ta có :

$$u_n = \frac{\alpha^n + \beta^n}{2}, \quad v_n = \frac{\alpha^n - \beta^n}{2\sqrt{3}}.$$

Bài toán có vô số nghiệm $a_n$ cho bởi :

$$a_n = (u_n + v_n)^2 - 1 = \frac{\alpha^{2n+1} - 4 + \beta^{2n+1}}{6}.$$

b) Nếu $a_1 < a_2 < \cdots$ là dãy nghiệm của phần a), ta có :

$$a_n a_{n+1} + 1 = \left(\frac{\alpha^{2n+2} - 8 + \beta^{2n+2}}{6}\right)^2.$$

Do $(u_n + v_n)$ nguyên nên $a_n$, $a_n a_{n+1}$ đều nguyên, và do đó $a_n a_{n+1} + 1$ là số chính phương.

**65.** Xét dãy $\{c_n\}$ định nghĩa như sau :

$$c_0 = 1,\ c_1 = 1,\ c_{n+2} = nc_{n+1} + c_n \text{ với } n \geq 0.$$

Khi đó ta có :

$$c_{n+3} = (n+1)c_{n+2} + c_{n+1}$$
$$c_n = c_{n+2} - nc_{n+1}.$$

Từ đó suy ra

$$c_{n+3}^2 = (n+1)^2 c_{n+2}^2 + 2(n+1)c_{n+2}c_{n+1} + c_{n+1}^2$$
$$c_n^2 = c_{n+2}^2 + n^2 c_{n+1}^2 - 2nc_{n+2}c_{n+1}.$$

Khử $c_{n+2}c_{n+1}$ từ hai phương trình trên, ta nhận được :

$$c_{n+3}^2 = \frac{(n^2+n+1)(n+1)}{n} c_{n+2}^2 + (n^2+n+1)c_{n+1}^2 - \frac{n+1}{n} c_n^2.$$

Như vậy, dãy $\{c_n^2\}$ thỏa mãn cùng điều kiện hồi quy như dãy $\{x_n\}$, hơn nữa

$$c_0 = x_0 = 0,\ c_1 = x_1 = 1,\ c_2 = x_2 = 0.$$

Do đó, các phần tử của hai dãy trùng nhau, tức là

$$x_n = c_n^2 \text{ với mọi } n.$$

Dễ thấy rằng $c_n$ nguyên với mọi $n$, nên $x_n$ là số chính phương với mọi $n$.

**66.** Đặt

$$v_n = \frac{u_n}{(2n)!}.$$

Khi đó ta có :

$$(n+2)v_{n+2} = (2n+3)v_{n+1} - (n+1)v_n$$
$$\Rightarrow (n+2)(v_{n+2} - v_{n+1}) = (n+1)(v_{n+1} - v_n)$$
$$\Rightarrow (n+2)(v_{n+2} - v_{n+1}) = (v_1 - v_0)$$
$$\Rightarrow v_{n+2} = v_{n+1} + \frac{v_1 - v_0}{n+2}$$

$$\Rightarrow v_n = v_0 + (v_1 - v_0)\left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right)$$

$$\Rightarrow u_n = (2n)!\left(u_0 + \left(\frac{u_1}{2} - u_0\right)\right)\left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right).$$

**67.** Bài toán không thay đổi nếu $a$, $b$ được thay bởi $-a$, $-b$. Vì thế, không giảm tổng quát, ta giả thiết rằng $a \geq b > 0$. Ta sẽ chứng tỏ rằng, các cặp số $(a,\ b)$ thỏa mãn bài toán chính là các cặp

$$(a,\ b) = (F_{2n+1},\ F_{2n-1}),\quad n \geq 0,$$

trong đó $F_n$ là số Fibonacci thứ $n$ (ta quy ước $F_{-1} = 1$, $F_0 = 0$). Từ quan hệ giữa các số Fibonacci

$$F_{2n-1}F_{2n+1} = F_{2n}^2 + 1$$

ta có :

$$F_{2n+1}^2 + F_{2n-1}^2 - 2F_{2n+1}F_{2n-1} = (F_{2n+1} - F_{2n-1})^2 = F_{2n}^2 = F_{2n+1}F_{2n-1} - 1.$$

Vậy,

$$F_{2n+1}^2 + F_{2n-1}^2 + 1 = 3F_{2n+1}F_{2n-1}.$$

Do đó, cặp $(F_{2n+1},\ F_{2n-1})$ thoả mãn bài toán. Điều ngược lại được chứng minh bằng quy nạp theo $a$. Nếu $(a,\ b)$ thỏa mãn bài toán mà $a = b$ thì $a^2 \mid (2a^2 + 1)$. Suy ra $a = b = 1$ : chính là nghiệm đã xét với $n = 0$. Giả sử $a > b$ và $ab \mid (a^2 + b^2 + 1)$, chẳng hạn

$$a^2 + b^2 + 1 = kab.$$

Đặt $a' = b$, $b' = kb - a = \dfrac{b^2 + 1}{a}$. Khi đó

$$(a')^2 + (b')^2 + 1 = kb(kb - a) = ka'b'.$$

Như vậy $(a',b')$ cũng thỏa mãn bài toán. Mặt khác,

$$b' = \frac{b^2 + 1}{a} < \frac{b^2 + 1}{b} \leq b + 1.$$

Do $b'$ nguyên nên từ đó suy ra $b' \leq b = a'$. Vậy $0 \leq b' \leq a' < a$.

Để sử dụng quy nạp, giả thiết rằng với mọi cặp $(a',b')$,

$0 < b' \le a' < a$ và thỏa mãn bài toán, ta có :

$$a' = F_{2n+1},\ b' = F_{2n-1}$$

với $n \ge 0$ nào đó (giả thiết đúng với $a = 2$). Hơn nữa, theo phần chứng minh trên,

$$(a')^2 + (b')^2 + 1 = 3a'b'.$$

Ta có :

$$b = a' = F_{2n+1},\quad b' = 3b - a = F_{2n-1}.$$

Suy ra

$$a = 3F_{2n+1} - F_{2n-1} = 2F_{2n+1} + F_{2n} = F_{2n+1} + F_{2n+2} = F_{2n+3}.$$

tức là

$$(a,\ b) = (F_{2n+3},\ F_{2n+1}).$$

**68.** Giả sử $(a,\ b)$ là một cặp số thỏa mãn bài ra, $1 \le a \le b$ và $a^2 \equiv -1 \pmod b$, $b^2 \equiv -1 \pmod a$, $b > 1$. Đặt $c = \dfrac{a^2+1}{b}$ và xét cặp $T(a,\ b) = (c,\ a)$. Ta có :

$$c^2 = \frac{(a^2+1)^2}{b^2} \equiv -(a^2+1)^2 \equiv -1 \pmod a$$

$$a^2 = bc - 1 \equiv -1 \pmod c.$$

Như vậy, cặp $(c,\ a)$ cũng thỏa mãn bài toán, đồng thời $1 \le c \le a$ và $c = a$ khi và chỉ khi $a = c = 1$. Do đó, ta có thể lặp lại phép toán $T$ cho đến lúc nhận được cặp $T^k(a,\ b) = (1,\ 1)$ với $k > 0$ nào đó. Nhận xét rằng, nếu $T(x,\ y) = (m,\ n)$ thì cặp $(x,\ y)$ chính là cặp $\left(n,\ \dfrac{n^2+1}{m}\right)$. Như vậy, cặp $(x,\ y)$ có $T(x,\ y) = (1,\ 1)$ là cặp $(1,\ 2) = (F_1,\ F_3)$, trong đó $F_n$ là số Fibonacci thứ $n$. Ta sẽ chứng minh rằng, nếu $T^k(a,\ b) = (1,\ 1)$ thì $(a,\ b) = (F_{2k-1},\ F_{2k+1})$, $k \ge 1$. Ta đã thấy khẳng định đúng với $k = 1$. Mặt khác, do nhận xét trên, nếu $T(x,\ y) = (F_{2n-1},\ F_{2n+1})$ thì $x = F_{2n+1}$, $y = \dfrac{F_{2n+1}^2 + 1}{F_{2n-1}} = F_{2n+3}$ nên $(x,\ y) = (F_{2n+1},\ F_{2n+3})$. Do đó :

$$T(1,\ 1) = (F_1,\ F_3);$$

$$T^2(1,\ 1) = (F_3,\ F_5);$$

...

$$T^k(1,\ 1) = (F_{2k-1},\ F_{2k+1}) = (a,\ b).$$

Vậy, các cặp $(m,\ n)$ cần tìm chính là $(F_{2k-1},\ F_{2k+1})$, $k \geq 1$, trong đó $F_n$ là số Fibonacci thứ $n$.

**69.** Lập dãy số $\{x_n\}$ như sau :

$$x_n = ny_n \text{ với mọi } n \geq 2 \ ;\ x_2 = 2,\ x_3 = 3.$$

Khi đó ta có :

$$(n-2)x_{n+1} = (n^2 - n - 1)x_n - (n-1)^2 x_{n-1}$$

với $n \geq 3$. Từ đó suy ra :

$$\frac{x_{n+1} - x_n}{n-1} = (n-1)\frac{x_n - x_{n-1}}{n-1}.$$

Đặt

$$z_n = \frac{x_{n+1} - x_n}{n-1}, \quad n \geq 2.$$

Ta có:

$$z_n = (n-1)!$$

Vậy

$$x_{n+1} - x_n = (n-1)z_n = n! - (n-1)!.$$

Suy ra

$$x_n = x_2 + \sum_{k=2}^{n-1}(x_{k+1} - x_k) = 2 + (n-1)! - 1! = (n-1)! + 1.$$

Do đó

$$y_n = \frac{x_n}{n} = \frac{(n-1)!+1}{n}.$$

Từ Định lí Wilson suy ra rằng, $y_n$ là số nguyên khi và chỉ khi $n$ là số nguyên tố, hoặc $n = 1$ (vì dễ thấy rằng $y_1 = 2$).

**70.** Trước tiên ta chứng minh rằng, nếu $a_n \equiv 0 \pmod p$ thì tồn tại $m > n$

sao cho $a_m \equiv 0 \pmod{p}$.

Thật vậy từ công thức xác định dãy $\{a_n\}$ ta có :

$$a_{3n} = a_{3n-1} + a_n$$

$$a_{3n+1} = a_{3n-1} + 2a_n$$

$$a_{3n+2} = a_{3n-1} + 3a_n.$$

Suy ra $a_{3n-1}$, $a_{3n}$, $a_{3n+2}$ có cùng số dư trong phép chia cho $p$. Gọi số dư đó là $a$.

Nếu $a \equiv 0 \pmod{p}$ : ta có điều cần chứng minh.

Nếu $a \not\equiv 0 \pmod{p}$, ta xét 13 số sau :

$$a_{9n-4} = a_{9n-4} \equiv a_{9n-4} \pmod{p}$$

$$a_{9n-3} = a_{9n-4} + a_{3n-1} \equiv a_{9n-4} + a \pmod{p}$$

$$a_{9n-2} = a_{9n-3} + a_{3n-1} \equiv a_{9n-4} + 2a \pmod{p}$$

$$\ldots$$

$$a_{9n+7} = a_{9n+6} + a_{3n+2} \equiv a_{9n-4} + 11a \pmod{p}$$

$$a_{9n+8} = a_{9n+7} + a_{3n+2} \equiv a_{9n-4} + 12a \pmod{p}.$$

Vì $a \not\equiv 0 \pmod{p}$ nên $p$ số đầu tiên trong 13 số nói trên lập thành hệ thặng dư đầy đủ môđulô $p$. Suy ra có ít nhất một trong 13 số nói trên chia hết cho $p$.

Bằng tính toán trực tiếp, ta có :

$$a_1 = 2 \equiv 0 \pmod{2}$$

$$a_2 = 3 \equiv 0 \pmod{3}$$

$$a_3 = 5 \equiv 0 \pmod{5}$$

$$a_4 = 7 \equiv 0 \pmod{7}$$

$$a_{11} = 33 \equiv 0 \pmod{11}$$

$$a_{20} = 117 \equiv 0 \pmod{13}.$$

Từ chứng minh nói trên suy ra ngay kết luận của bài toán.

**71.** Ta thấy rằng, với mọi $n \geq 1$, $x_n > 0$. Đặt $u_n = \dfrac{2}{x_n}$. Từ công thức xác định dãy $x_n$ ta có :

$$u_1 = 3,\ u_{n+1} = 4(2n+1)u_n,\ n \geq 1.$$

Suy ra :

$$\begin{aligned} u_n &= (u_n - u_{n-1}) + (u_{n-1} - u_{n-2}) + \cdots + (u_2 - u_1) + u_1 \\ &= 4[(2n-1) + (2n-3) + \cdots + 3] + 3 \\ &= (2n-1)(2n+1). \end{aligned}$$

Vậy

$$x_n = \frac{2}{u_n} = \frac{2}{(2n-1)(2n+1)} = \frac{1}{2n-1} + \frac{1}{2n+1}.$$

Do đó

$$\begin{aligned} x_1 + x_2 + \cdots + x_k &= \left(\frac{1}{2k-1} + \frac{1}{2k+1}\right) + \left(\frac{1}{2k-3} + \frac{1}{2k-1}\right) + \cdots + 1 - \frac{1}{3} \\ &= 1 - \frac{1}{2k+1} \cdot \frac{2k}{2k+1}. \end{aligned}$$

**72.** Quan hệ

$$a_{n+2} = 4a_{n+1} + 5a_n + 20 \qquad (1)$$

không phải là quan hệ hồi quy tuyến tính với hệ số hằng. Ta sẽ tìm số $t$ thích hợp cho dãy $\{b_n\}$ xác định bởi $b_n = a_n + t$ thỏa mãn quan hệ tuyến tính với hệ số hằng. Thay công thức của $b_n$ vào (1) ta được

$$b_{n+2} = 4b_{n+1} + 5b_n - 8t + 20.$$

Như vậy, nếu lấy $t = \dfrac{5}{2}$ thì dãy $\{b_n\}$ thỏa mãn quan hệ sau :

$$b_0 = 20 + \frac{5}{2},\ b_1 = 100 + \frac{5}{2},\ b_{n+2} = 4b_{n+1} + 5b_n. \qquad (2)$$

Phương trình đặc trưng của (2) là

$$x^2 - 4x - 5 = 0.$$

Hai nghiệm của phương trình là $5$ và $-1$. Vậy, nghiệm tổng quát của (2) cho bởi :

$$b_n = c_1 5^n + c_2(-1)^n.$$

Ta xác định $c_1$, $c_2$ theo các giá trị $b_0$, $b_1$ :

$$\begin{cases} c_1 + c_2 = 20 + \dfrac{5}{2} \\ 5c_1 - c_2 = 100 + \dfrac{5}{2}. \end{cases}$$

Vậy, $c_1 = \dfrac{125}{6}$, $c_2 = \dfrac{10}{6}$. Ta có công thức

$$\begin{cases} a_n = \dfrac{5}{6}(5^{n+2} - 1) & \text{nếu } n \text{ chẵn} \\ a_n = \dfrac{5}{6}(5^{n+2} - 5) & \text{nếu } n \text{ lẻ.} \end{cases}$$

**73.** Giả sử $(n,\ m)$ là một cặp số nguyên dương thỏa mãn bài ra. Ta có

$$(n^2 - mn - m^2)^2 = 1. \tag{1}$$

Nếu $n = m$ thì $n = m = 1$. Nếu $(n_0,\ m_0)$ là một cặp thỏa mãn (1) và $n_0 > m_0$ thì cặp $(m_0,\ n_0 - m_0)$ cũng thỏa mãn (1). Như vậy, nếu đặt $n_1 = m_0$, $m_1 = n_0 - m_0$ thì ta được cặp $(n_1,\ m_1)$ thỏa mãn (1), đồng thời $n_1 \geq m_1$. Nếu có $n_1 > m_1$ thì ta lại được cặp $(n_2,\ m_2)$ với $n_2 = m_1$, $m_2 = n_1 - m_1$ cũng thỏa mãn (1). Như vậy, sau hữu hạn bước, ta đi đến cặp (1, 1), rõ ràng thỏa mãn (1).

Nếu cặp $(n',\ m')$ nhận được từ cặp $(n,\ m)$ thì

$$n = m' + n',\ m = n. \tag{2}$$

Như vậy, mọi cặp $(n,\ m)$ thỏa mãn (1) đều nhận được từ (1, 1) nhờ quan hệ (2).

Ta có tất cả các cặp thỏa mãn (1) :

$$(1,\ 1),\ (2,\ 1),\ (3,\ 2),\ (5,\ 3),\ (8,\ 5),\ (13,\ 8),\ldots$$

tức là các cặp $(F_{i+1},\ F_i)$, $i = 1,\ 2,\ \ldots,\ F_i$ là số Fibonacci thứ $i$.

**74.** Trước tiên, ta chỉ ra rằng, nếu tồn tại $n$ để

$$\tau(n^2) = k\tau(n) \tag{1}$$

khi $k$ là số lẻ.

Nếu $n = 1$ thì $\tau(n) = \tau(n^2) = 1 \Rightarrow k = 1$.

Giả sử $n > 1$, $n = p_1^{r_1} \dots p_s^{r_s}$ là khai triển $n$ thành thừa số nguyên tố.

Khi đó

$$n^2 = p_1^{2r_1} \dots p_s^{2r_s}.$$

Phương trình (1) cho ta

$$(2r_1 + 1)\dots(2r_s + 1) = k(r_1 + 1)\dots(r_s + 1). \qquad (2)$$

Vậy $k$ là số lẻ.

Ngược lại, giả sử $k = 2m + 1$. Ta chứng minh sự tồn tại $n$ thoả mãn (1) bằng quy nạp theo $m$. Sự tồn tại $n$ tương đương với sự tồn tại $(r_1, \dots, r_s)$ thoả mãn (2).

Với $m = 1$, ta có $2m + 1 = 3 = \dfrac{(2.4 + 1)(2.2 + 1)}{(4 + 1).(2 + 1)}$.

Giả sử với mọi $m < M$, mỗi số $k = 2m + 1$ đều có thể biểu diễn dưới dạng (2). Ta chứng minh $k = 2M + 1$ cũng có dạng đó.

Giả sử $k + 1 = 2^l.t$, trong đó $t$ lẻ. Khi đó ta có

$$t = \frac{k+1}{2^l} \le \frac{k+1}{2} < k,$$

vì $l \ge 1$, $k > 1$. Xét các số $r_1, \dots, r_l$ như sau :

$$r_1 = 2^l.t - 2^0.t - 2^0,$$

$$r_2 = 2^{l+1}.t - 2^1.t - 2^1,$$

$$\dots$$

$$r_l = 2^{l+l-1}.t - 2^{l-1}.t - 2^{l-1}.$$

Xét $n_1 = p_1^{r_1} \dots p_l^{r_l}$. Khi đó ta có

$$k_1 = \frac{\tau(n_1^2)}{\tau(n_1)} = \frac{(2^{l+1}.t - 2^1.t - 2^1 + 1)\cdots(2^{l+l}.t - 2^l.t - 2^l + 1)}{(2^l.t - 2^0.t - 2^0 + 1)\cdots(2^{l+l-1}.t - 2^{l-1}.t - 2^{l-1} + 1)}$$

$$= \frac{2^{2l}.t - 2^l.t - 2^l + 1}{2^l.t - 2^0.t - 2^0 + 1} = \frac{(2^l - 1)(2^l.t - 1)}{(2^l - 1)t} = \frac{2^l.t - 1}{t}.$$

Vì $1 < k$ nên theo giả thiết quy nạp, tồn tại số

$$n_2 = q_1^{a_1} \dots q_s^{a_s}$$

sao cho

$$t = \frac{\tau(n_2^2)}{\tau(n_2)}.$$

Bằng cách chọn các số $q_1, \dots, q_s$, $p_1, \dots, p_l$ là các số nguyên tố khác nhau, và đặt $n = n_1.n_2$, ta có :

$$\frac{\tau(n^2)}{\tau(n)} = \frac{\tau(n_1^2)}{\tau(n_1)} \cdot \frac{\tau(n_2^2)}{\tau(n_2)} = k_1.t = 2^l.t - 1 = k.$$

Chứng minh xong.

**75.** Giả sử $r$, $s$ là nghiệm của phương trình

$$x^2 - x - 1 = 0.$$

Theo Định lí Binê ta có :

$$F_n = \frac{r^n - s^n}{\sqrt{5}}.$$

Đặt $a = 2^n$, ta nhận được :

$$\frac{F_{4a}}{F_{2a}} - \left(\frac{F_{2a}}{F_a}\right)^2 + 2 = \frac{r^{4a} - s^{4a}}{r^{2a} - s^{2a}} - \left(\frac{r^{2a} - s^{2a}}{r^a - s^a}\right)^2 + 2$$

$$= r^{2a} + s^{2a} - (r^a + s^a)^2 + 2 = -2(rs)^a + 2 = 0,$$

vì $rs = -1$.

Vậy, nếu đặt

$$a_k = \frac{F_{2^{k+1}}}{f_{2^k}}$$

thì dãy $\{a_k\}$ thoả mãn quan hệ

$$a_{k+1} = a_k^2 - 2.$$

Mặt khác, $a_1 = \frac{F_4}{F_2} = 3$, nên $a_k = \frac{F_{2^{k+1}}}{F_{2^k}}$ chính là nghiệm của dãy truy hồi xét trong bài toán.

**76.** Trước tiên, với mỗi số nguyên dương $n$ tùy ý, ta xét dãy $\{a_i\}$ xác định

bởi

$$a_i = n + i, \quad i = 1,\ 2,\ \ldots,\ n.$$

Như vậy, dãy $\{a_i\}$ đang xét thỏa mãn giả thiết

$$0 < a_1 < a_2 < \cdots < a_n \leq 2n. \tag{1}$$

Dễ thấy rằng, số chẵn đầu tiên của dãy là số $2\left(\left[\frac{n}{2}\right]+1\right)$. Mặt khác, với $n = 3$ hoặc $n \geq 5$, số $3\left(\left[\frac{n}{2}\right]+1\right)$ cũng thuộc dãy. Vậy, với dãy đặc biệt nói trên ta có :

$$\min[a_i,\ a_j] \leq \text{BCNN của } 2\left(\left[\frac{n}{2}\right]+1\right) \text{ và } 3\left(\left[\frac{n}{2}\right]+1\right).$$

Do đó, với $n \geq 3$ và $n \neq 4$ ta được

$$\min[a_i,\ a_j] \leq 6\left(\left[\frac{n}{2}\right]+1\right).$$

Ta chuyển sang xét dãy tùy ý thỏa mãn điều kiện (1). Với mỗi $i = 1$, $2, \ldots, n$, tồn tại số nguyên $k_i \geq 1$ sao cho

$$n < k_i a_i \leq 2n. \tag{2}$$

Nếu có $i \neq j$ sao cho $k_i a_i = k_j a_j$ thì giá trị chung này là bội số của $a_i$, $a_j$. Từ đó suy ra $[a_i,\ a_j] \leq 2n$, chứng minh xong. Nếu ngược lại,

$$k_i a_i \neq k_j a_j \quad \text{với} \quad i \neq j.$$

Như vậy, dãy $\{k_i,\ a_i\}$, $i = 1,\ 2,\ \ldots,\ n$ là $n$ số nguyên khác nhau thỏa mãn (2). Do đó, $\{k_i,\ a_i\}$ chính là dãy đã xét $\{n+1,\ n+2,\ \ldots,\ 2n\}$ (xếp theo thứ tự nào đó). Như vậy, tồn tại $p,\ q$ để $k_p a_p = 2\left(\left[\frac{n}{2}\right]+1\right)$, $k_q a_q = 3\left(\left[\frac{n}{2}\right]+1\right)$, và dó đó

$$[a_p,\ a_q] \leq 6\left(\left[\frac{n}{2}\right]+1\right).$$

77. Dễ thấy rằng, nếu $f(x,\ y)$ là bội số chung nhỏ nhất của hai số $x$ và $y$ thì hàm $f(x,\ y)$ thỏa mãn các điều kiện của bài toán. Ta chứng tỏ rằng, đó là hàm duy nhất thoả mãn i), ii), iii).

Thật vậy, giả sử tồn tại hai hàm $f_1 \neq f_2$ cùng thoả mãn i), ii), iii). Do $f_1 \neq f_2$ nên tồn tại các cặp số $(x,\ t)$ sao cho

$$f_1(x,\ t) \neq f_2(x,\ t). \qquad (*)$$

Giả sử $(s,\ t)$ là cặp số thỏa mãn (*), đồng thời tích $st$ là nhỏ nhất trong số các tích $xt$ của các cặp thỏa mãn (*). Từ điều kiện ii) suy ra rằng $s \neq t$. Giả sử $s < t$. Do điều kiện iii),

$$f_1(s,\ t) = \frac{[tf_1(s,\ t-s)]}{t-s},$$

$$f_2(s,\ t) = \frac{[tf_2(s,\ t-s)]}{t-s}.$$

Vì $s(t-s) < st$ nên theo cách chọn cặp $(s,\ t)$ ta có :

$$f_1(s,\ t-s) = f_2(s,\ t-s).$$

Vậy,

$$f_1(s,\ t) = f_2(s,\ t),$$

mâu thuẫn.

**78.** Giả sử ngược lại, tồn tại ba số nguyên tố $p$, $q$, $r$ mà căn bậc 3 của chúng là các số hạng của một cấp số cộng:

$$\sqrt[3]{p} = a,\ \sqrt[3]{q} = a + md,\ \sqrt[3]{r} = a + nd,$$

trong đó $m$, $n$ là các số nguyên dương nào đó. Ta có :

$$\frac{\sqrt[3]{q} - \sqrt[3]{p}}{\sqrt[3]{r} - \sqrt[3]{p}} = \frac{m}{n}.$$

Suy ra

$$m\sqrt[3]{r} - n\sqrt[3]{q} = (m-n)\sqrt[3]{p}.$$

Lấy lập phương hai vế ta được

$$m^3 r - n^3 q - 3mn\sqrt[3]{rq}(m\sqrt[3]{r} - n\sqrt[3]{q}) = (m-n)^3 p.$$

Do đó

$$3mn(m-n)\sqrt[3]{pqr} = m^3 r - n^3 q - (n-m)^3 p.$$

Như vậy, $\sqrt[3]{pqr}$ là số hữu tỉ, chẳng hạn

$$\sqrt[3]{pqr} = \frac{x}{y},$$

trong đó $x$, $y$ là các số dương nguyên tố cùng nhau. Ta có

$$y^3pqr = x^3.$$

Do đó $x \vdots (pqr)$, suy ra $y \vdots (pqr)$ : trái với giả thiết $x$, $y$ nguyên tố cùng nhau.

**79.** Mọi số nguyên dương $m \leq n$ đều có thể viết dưới dạng

$$m = p_1^{\alpha_1} \dots p_k^{\alpha_k},$$

trong đó $p_i$ là các số nguyên tố và

$$p_1 < p_2 < \cdots < p_k \leq n.$$

Mặt khác, rõ ràng $k \leq \pi(n)$. Nếu trong dãy $a_1 < a_2 < \cdots < a_m$ không có số $a_i$ nào là ước của tích các số khác thì ít nhất một trong các ước nguyên tố của $a_i$, chẳng hạn $p_j$, tham gia trong khai triển của $a_i$ với số mũ $\alpha_j$ lớn hơn tổng các số mũ của $p_j$ tham gia trong khai triển của các số còn lại. Ta gọi $p_j$ là "đại diện" của $a_i$. Hiển nhiên $p_j \leq n$. Vì mỗi số nguyên tố $\leq n$ chỉ có thể đại diện cho nhiều nhất là một số trong dãy đang xét nên số các phân tử của dãy không vượt quá số các số nguyên tố bé hơn hoặc bằng $n$ : $n \leq \pi(n)$.

Với dãy số sau đây, $m$ đúng bằng $\pi(n)$ :

$$p_1 < p_2 < \cdots < p_{\pi(n)},$$

trong đó $\{p_j\}$, $j \leq \pi(n)$ là các số nguyên tố không vượt quá $n$.

Vậy giá trị lớn nhất có thể của $m$ là $\pi(n)$.

**80.** Giả sử $d$ là số các ước nguyên dương của $n^2$. Ta sẽ chứng tỏ rằng, nếu không để ý đến thứ tự lấy tổng thì đáp số sẽ là :

a) $\dfrac{d+1}{2}$; b) $\dfrac{d-1}{2}$.

Trước tiên ta nhận xét rằng, $d$ là số lẻ. Thật vậy, nếu $k$ là một ước của $n^2$ và $k < n$ thì $\dfrac{n}{k}$ sẽ là một ước của $n^2$ và $\dfrac{n}{k} > n$. Như vậy, ta sẽ có từng cặp ước của $n^2$ như trên, cùng với ước là $n$.

Bây giờ giả sử

$$\frac{1}{n} = \frac{1}{x} + \frac{1}{y},$$

trong đó $x$, $y$ nguyên dương. Như vậy, $x$, $y > n$. Đặt $x = n + k$, $y = n + l$. Khi đó ta có $kl = n^2$. Do không để ý đến thứ tự lấy tổng, ta xem $k \leq n$. Vậy có đúng $\dfrac{d+1}{2}$ cách chọn $k$ (là số các ước dương của $n^2$ không vượt quá $n$).

Nếu

$$\frac{1}{n} = \frac{1}{x} - \frac{1}{y} \qquad x, y \text{ nguyên dương,}$$

thì $x < n$. Ta đặt

$$x = n - k,\ y = l - n,\ 1 \leq k \leq n,\ l > n.$$

Khi đó, từ

$$\frac{1}{n} = \frac{1}{x} - \frac{1}{y}$$

suy ra $kl = n^2$. Số các cách viết như trên sẽ là số các ước dương nhỏ hơn $n$ của $n^2$, tức là $\dfrac{d-1}{2}$.

**81.** Ta chia các số hữu tỉ được chứa trong khoảng $\left(\alpha,\ \alpha + \dfrac{1}{n}\right)$ và thỏa mãn đầu bài thành hai tập hợp :

$$\left\{\frac{u_i}{v_i}\right\},\ i = 1,2,\ldots,r\ ;\ 1 \leq v_i < \frac{n}{2},$$

$$\left\{\frac{x_i}{y_i}\right\},\ i = 1,2,\ldots,s\ ;\ \frac{n}{2} \leq y_i < n.$$

Chú ý rằng, các phân số $\dfrac{u_i}{v_i}$ và $\dfrac{x_i}{y_i}$ đều là phân số tối giản.

Với mỗi số $v_i$, $i = 1,2,\ldots,r$, tồn tại số nguyên dương $c_i$ sao cho

$$\frac{n}{2} \leq c_i v_i \leq n.$$

Đặt

$$y_{s+i} = c_i v_i,\ i = 1,2,\ldots,r,$$

$$x_{s+i} = c_i u_i,\ i = 1,2,\ldots,r.$$

Ta thấy rằng, không có hai số $y_i$ nào $(1 \le i \le s+r)$ bằng nhau. Thật vậy, giả sử ngược lại, tồn tại $i \ne k$ sao cho $y_i = y_k$. Khi đó

$$\left|\frac{x_i}{y_i} - \frac{x_k}{y_k}\right| \ge \frac{1}{y_i} \ge \frac{1}{n}.$$

Vì mọi $y_i$ đều khác nhau và $\ge \frac{n}{2}$ nên ta có

$$r + s \le n - \left[\frac{n}{2}\right] \le \frac{n+1}{2}$$

Vậy số các phân số tối giản thỏa mãn bài ra cùng lắm là $\frac{n+1}{2}$. Ví dụ sau đây chỉ ra rằng, số $\frac{n+1}{2}$ có thể đạt được.

Xét số dương $\varepsilon$ thỏa mãn : $0 < \varepsilon < \frac{1}{n+1} - \frac{1}{n}$. Các số hữu tỉ dạng phân số tối giản với mẫu số $\le n$ và thuộc khoảng $\left(\varepsilon + \frac{1}{n},\ \varepsilon + \frac{2}{n}\right)$ là $\frac{1}{n-1}, \frac{1}{n-2}, \cdots, \frac{1}{\left[\frac{n-1}{2}\right]}$ và $\frac{2}{n}$.

**82.** Theo giả thiết, tồn tại $t$ nguyên để

$$n^2 - 1 \equiv t(m^2 + 1 - n^2).$$

Đặt $k = t + 1$. Rõ ràng $k \ne 0$. Chỉ cần chứng minh rằng $k$ là số chính phương.

Gọi $S_k$ là tập hợp các cặp có thứ tự $(x,\ y)$ các số nguyên thỏa mãn

$$(x+y)^2 = k(1 + 4xy).$$

Khi đó cặp $\left(\frac{m+n}{2},\ \frac{m-n}{2}\right) \in S_k$, nên $S_k$ là tập hợp không rỗng. Ta đặt

$$a = \min\left\{|x| : \exists(x,\ y) \in S_k\right\}.$$

Ta chỉ ra rằng $a = 0$, khi đó $k = y^2$ và $k$ là số chính phương.

Nếu $(x,\ y) \in S$ thì $(-x,\ -y) \in S$ nên có thể xem tồn tại cặp

$(a,\ y) \in S$. Ta có

$$(a+y)^2 = k(1+4ay).$$

Hai nghiệm $b_1$, $b_2$ của phương trình là các số nguyên có trị tuyệt đối $\geq a$ (vì $(a,\ b_i) \in S$ suy ra $(b_i,\ a) \in S$, mà $a$ đạt cực tiểu về giá trị tuyệt đối trong các $x$ để tồn tại $(x,\ y) \in S$). Mặt khác ta có

$$b_1 + b_2 = 4ak - 2a, \quad b_1 b_2 = a^2 - k.$$

Suy ra

$$(a+b_1)(a+b_2) = (4a^2-1)k.$$

Nếu $k < 0$ thì $b_1 b_2 > 0$, $b_1 + b_2 \leq 0$, suy ra $b_1$, $b_2 < 0$. Do $|b_i| > a$ nên $a + b_i < 0$, suy ra $(a+b_1)(a+b_2) > 0$, tức là $(4a^2-1)k > 0$. Do $k < 0$ nên $a = 0$. Bây giờ giả sử $k > 0$ và $a \neq 0$ $(a > 0)$. Khi đó $b_1 + b_2 > 0$, $(a+b_1)(a+b_2) > 0$ nên suy ra $b_1$, $b_2 > 0$. Do cách chọn $a$, ta có $a^2 \leq b_1.b_2$ : mâu thuẫn với đẳng thức $b_1 b_2 = a^2 - k$.

Vậy $a = 0$, chứng minh xong.

**83.** Trước tiên ta nhận xét rằng, nếu $n$ là số tốt thì $2n+8$ và $2n+9$ cũng là các số tốt. Thật vậy, giả sử

$$n = a_1 + a_2 + \cdots + a_k,$$

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_k} = 1.$$

Khi đó

$$\frac{1}{2a_1} + \frac{1}{2a_2} + \cdots + \frac{1}{2a_k} = \frac{1}{2}.$$

Mặt khác, do

$$\frac{1}{2} = \frac{1}{4} + \frac{1}{4} = \frac{1}{3} + \frac{1}{6}$$

nên các bộ số

$$(4,\ 4,\ 2a_1,\ 2a_2,\ \ldots,\ 2a_k) \text{ và } (3,\ 6,\ 2a_1,\ 2a_2,\ \ldots,\ 2a_k)$$

đều có tính chất tổng các nghịch đảo bằng 1. Do tổng các số trong 2 bộ đó tương ứng bằng $2n+8$ và $2n+9$ nên $2n+8$ và $2n+9$ đều là các số tốt.

Như vậy, nếu các số $n,\ n+1,\ \ldots,\ 2n+7$ đều là số tốt thì các số từ $2n+8,\ 2n+9,\ \ldots,\ 2(2n+7)+9$, số tiếp theo $2(2n+8)+8 = 4n+24$ cũng là số tốt. Tiếp tục như vậy, ta suy ra, mọi số lớn hơn $n$ đều là số tốt. Do với $n = 33$, các số từ $n$ đến $2n+7 = 73$ đều là số tốt nên mọi $n \geq 33$ đều là số tốt.

**84.** Theo bài ra, tồn tại các số tự nhiên $x$ và $y$ sao cho

$$(x+1)^3 - x^3 = n = y^2. \tag{1}$$

Ta chứng minh $y$ là tổng bình phương của hai số tự nhiên liên tiếp. Phương trình (1) có thể đưa về dạng :

$$3(2x+1)^2 = (2y-1)(2y+1).$$

Do $(2y-1)$ và $(2y+1)$ nguyên tố cùng nhau, nên chỉ có thể xảy ra các trường hợp sau đây :

a) $2y-1 = 3m^2, \quad 2y+1 = l^2,$

b) $2y-1 = m^2, \quad 2y+1 = 3l^2,$

với $m$, $l$ là các số tự nhiên nào đó.

Trong trường hợp a), ta có :

$$l^2 - 3m^2 = 2.$$

Do $l^2 \equiv 0$ hoặc $1 \pmod 3$ nên trường hợp này không thể xảy ra. Vậy, chỉ còn trường hợp b). Vì $m$ lẻ nên ta đặt $m = 2k+1$. Khi đó

$$2y = 4k^2 + 4k + 2 = 2[(k+1)^2 + k^2],$$

tức là

$$y = k^2 + (k+1)^2.$$

**85.** Do $r$ là số vô tỉ nên không có số hạng nào của hai dãy trên đây là số nguyên. Giả sử $N$ là số nguyên dương tùy ý. Khi đó, có $\left[\dfrac{N}{1+r}\right]$ số hạng của dãy thứ nhất nhỏ hơn $N$ và có $\left[\dfrac{N}{1+\dfrac{1}{r}}\right]$ số hạng của dãy thứ hai nhỏ hơn $N$. Mặt khác,

$$\frac{N}{1+r}+\frac{N}{1+\frac{1}{r}}=N. \qquad (1)$$

Do $r$ vô tỉ nên các phần lẻ $\left\{\frac{N}{1+r}\right\}$, $\left\{\frac{N}{1+\frac{1}{r}}\right\}$ khác $0$, và tổng của chúng bằng $1$ (suy ra từ (1)). Như vậy, tổng các phần nguyên

$$\left[\frac{N}{1+r}\right]+\left[\frac{N}{1+\frac{1}{r}}\right]=N-1.$$

Vậy có đúng $(N-1)$ số hạng thuộc hai dãy nói trên nhỏ hơn $N$. Mặt khác, có đúng $N$ số hạng thuộc hai dãy nói trên và nhỏ hơn $N+1$. Vậy, giữa $N$ và $N+1$ có đúng một số hạng thuộc một trong hai dãy nói trên.

86. a) Trước tiên ta chỉ ra rằng, dãy $\{a_n\}$ giới nội, tức là $\exists M$ sao cho $|a_n| \le M$ với mọi $n$.

Thật vậy, do bậc của $f(x)$ lớn hơn 1 nên

$$\lim_{x\to\infty}\frac{|f(x)|}{|x|}=\infty .$$

Do đó, tồn tại $M$ (có thể giả thiết $M \ge |a_1|$) sao cho khi $|x| \ge M$ thì $|f(x)| \ge |x|$. Ta chứng tỏ $a_n \le M$ với mọi $M$. Giả sử ngược lại, tồn tại $n$ để $|a_n| > M$. Khi đó ta có :

$|a_{n-1}| = |f(a_n)| \ge |a_n| > M,$

$|a_{n-2}| = |f(a_{n-1})| \ge |a_{n-1}| > M, \ \ldots$

$|a_1| > M$ : trái giả thiết.

b) Ta tìm số tự nhiên $N$ để $Na_n$ nguyên với mọi $n$. Do $f(x)$ có hệ số hữu tỉ, có thể viết $f(x)$ dưới dạng :

$$f(x)=\frac{b_d x^d+\cdots+b_0}{c},$$

trong đó $b_0, \ldots, b_d, c$ nguyên. Giả sử $a_1=\frac{r}{s}$ với $r, s$ nguyên. Đặt

$N = sb_d$. Khi đó $Na_1 = rb_d$ nguyên. Ta chứng minh bằng quy nạp rằng $Na_n$ nguyên với mọi $n$.

Giả sử $Na_n$ nguyên với $n$ nào đó. Xét $Na_{n+1}$. Lập đa thức

$$P(x) = \frac{cN^d}{b_d}\left(f\left(\frac{x}{N}\right) - a_n\right).$$

Dễ thấy rằng $P(x)$ là đa thức hệ số nguyên, với hệ số của bậc cao nhất của $x$ bằng 1. Hơn nữa, do $f(a_{n+1}) = a_n$ nên $P(Na_{n+1}) = 0$. Như vậy $Na_{n+1}$ là nghiệm hữu tỉ của $P(x)$, và do đó là nghiệm nguyên.

Dãy $\{a_n\}$ là dãy giới nội, mỗi phần tử đều là một bội nào đó của $\frac{1}{N}$. Từ đó suy ra dãy $\{a_n\}$ chỉ nhận hữu hạn giá trị khác nhau, chẳng hạn $m$ giá trị khác nhau.

Xét dãy $a_1, a_2, \ldots, a_{m+1}$. Do $\{a_n\}$ chỉ nhận $m$ giá trị khác nhau nên tồn tại $i_1$, $k_1$ sao cho $1 \le i_1 < i_1 + k_1 \le m+1$ và $a_{i_1} = a_{i_1+k_1}$. Tương tự, tồn tại các $k_j$ cho mỗi đoạn $(m+1)$ số hạng tiếp theo. Do các $k_j$ chỉ nhận hữu hạn giá trị nên tồn tại $k = k_j$ với vô hạn giá trị $j$. Ta chứng tỏ rằng $k$ là chu kì của dãy $\{a_n\}$.

Thật vậy, giả sử tồn tại $n$ sao cho $a_{n+k} \ne a_n$. Lấy $n_j$ đủ lớn sao cho $a_{n_j} = a_{n_j+k}$. Khi đó

$$a_{n_j+k-1} = P(a_{n_j+k}) = P(a_{n_j}) = a_{n_j-1}.$$

Tiếp tục như vậy ta được

$$a_{n+k} = P(a_{n+k+1}) = P(a_{n+1}) = a_n.$$

mâu thuẫn.

**87.** Giả sử $m \mid (n!)$. Xét đa thức

$$f(x) = (x+1)\cdots(x+n).$$

Khi đó $f(x)$ có hệ số nguyên, đồng thời với mọi $j$ nguyên dương,

$$f(j) = n!\,C_{n+j}^{n}.$$

Do $m \mid (n!)$ nên $f(j) \vdots m$. Mặt khác, hệ số của $x^n$ là 1 nên điều kiện

$(a^0,\ a_1,\ \ldots,\ a_n,\ m) = 1$ thỏa mãn.

Ngược lại, giả sử tồn tại đa thức $f(x)$ thỏa mãn điều kiện bài toán. Ta viết đa thức $f(x)$ dưới dạng

$$f(x) = b_0 + \sum_{k=1}^{n} b_k\,[x(x-1)\cdots(x-k+1)]. \qquad (1)$$

Với đa thức $f(x)$ đã xác định, các số $b_k$, $(k = 0,\ 1,\ldots,\ n)$ được xác định duy nhất.

Trước tiên ta nhận xét rằng

$$(b_0,\ldots,\ b_n) = (a_0,\ldots,\ a_n).$$

Thật vậy, $p$ là một ước của $(b_0,\ldots,\ b_n)$ khi và chỉ khi $p$ là ước của $f(j)$ với mọi $j$ nguyên, tức là khi và chỉ khi $p$ là ước của $(a_0,\ldots,\ a_n)$.

Do $f(j) \equiv 0 \pmod m$ với $j = 0,\ 1,\ldots,\ n$, ta có :

$b_0 = f(0) \equiv 0 \pmod m$, $f(1) = b_0 + b_1 \equiv 0 \pmod m \Rightarrow b_1 \equiv 0 \pmod m$,

$f(2) = b_0 + 2b_1 + 2b_2 \equiv 0 \pmod m \Rightarrow 2b_2 \equiv 0 \pmod m$,... ta được

$$j!\,b_j \equiv 0 \pmod m. \qquad (2)$$

Do $(b_0,\ldots,\ b_n,\ m) = (a_0,\ a_1,\ldots,\ a_n,\ m) = 1$ nên tồn tại các số nguyên $c_0,\ c_1,\ldots,\ c_n,\ D$ sao cho :

$$c_0b_0 + c_1b1 + \cdots + c_nb_n + Dm = 1 \Rightarrow n!(c_0b_0 + \cdots + c_nb_n) + Dmn! = n!$$

Từ (2) ta suy ra $m \mid (n!)$.

**88.** Nếu $m \le n$ thì hiển nhiên đúng. Xét trường hợp $m > n$. Giả sử $m$ không biểu diễn được dưới dạng tích $k$ số không vượt quá $n$. Ta viết $m$ dưới dạng tích các số nguyên tố :

$$m = p_1p_2\ldots p_r,\quad p_1 \le p_2 \le \cdots \le p_r.$$

Xác định hai bộ số $A_1,\ A_2,\ldots,\ A_k$ và $r_1,\ r_2,\ldots,\ r_k$ như sau :

$$A_1 = p_1\ldots p_{r_1-1} \le n,\quad p_{r_1}A_1 > n$$

$$A_2 = p_{r_1}\ldots p_{r_2-1} \le n,\quad p_{r_2}A_2 > n$$

$$\ldots$$

$$A_k = p_{k_1}\ldots p_{r_k-1} \le n,\quad p_{r_k}A_k > n.$$

Việc làm nói trên có nghĩa là ta tách $p_1 \dots p_r$ thành từng đoạn dài nhất có thể với tích trong mỗi đoạn $\le n$. Do $m$ không biểu diễn được dưới dạng tích $k$ số $\le n$ (theo giả thiết phản chứng) nên hai bộ số trên tồn tại. Rõ ràng ta có :

$$A_{j+1} \ge p_{r_j}, \quad j = 1, 2, \dots, k-1$$

$$m \ge A_1 A_2 \dots A_k p_{r_k}.$$

Suy ra

$$m^2 \ge (A_1 \dots A_k p_{r_k})^2 = (A_1 A_2)(A_2 A_3) \dots (A_{k-1} A_k)(A_k p_{r_k})(A_k p_{r_k})$$

$$\ge (A_1 p_{r_1})(A_2 p_{r_2}) \dots (A_{k-1} p_{r_{k-1}})(A_k p_{r_k})^2 > n^{k+1},$$

tức là

$$m > n^{\frac{k+1}{2}}.$$

Mâu thuẫn với giả thiết.

**89.** Ta có nhận xét sau: nếu cặp số $(m,\ m+1)$ có tính chất đòi hỏi thì cặp số $(4m(m+1),\ 4m(m+1)+1)$ cũng có tính chất đó. Thật vậy, $4m(m+1) = 2^2 m(m+1)$, $4m(m+1)+1 = (2m+1)^2$. Mặt khác, cặp $(8,\ 9) = (2^3,\ 3^2)$ rõ ràng là cặp có tính chất đòi hỏi.

Vậy, có thể tìm vô hạn cặp $(m,\ m+1)$ thỏa mãn bài ra.

Chú ý rằng, câu hỏi sau đây cho đến nay vẫn chưa được trả lời : Tồn tại hay không bộ ba số tự nhiên $(m,\ m+1,\ m+2)$ sao cho mọi ước nguyên tố của mỗi số trong bộ đều tham gia trong khai triển với số mũ lớn hơn 1.

**90.** Giả sử $\alpha$ và $\beta$ là các nghiệm của phương trình

$$x^2 - ax + a = 0.$$

Do $a > 4$ nên phương trình trên có hai nghiệm thực $\alpha$, $\beta$. Giả sử $\alpha < \beta$.

Khi đó $\alpha + \beta = a$, $\alpha\beta = a$, $\frac{1}{\alpha} + \frac{1}{\beta} = 1$, $1 < \alpha \le 2$, $2 \le \beta$. Ngoài ra, các nghiệm $\alpha$, $\beta$ đều vô tỉ, vì nếu chúng hữu tỉ thì chúng phải nguyên. Từ đó $\alpha = 2$, $\beta = 2$ và $a = 4$ : trái giả thiết.

Vậy $1 < \alpha < 2$, và $[\alpha] = 1$ (1)

Nếu $n \geq 1$ thì

$$[\beta n] = [(a - \alpha)n] = na - 1 - [\alpha n]. \quad (2)$$

Nếu $[\alpha n] = [\beta n] = k$ với $m$, $n$ tự nhiên nào đó, thì $\alpha n = k + r$, $\beta m = k + s$, $0 < r < 1$, $0 < s < 1$. Do đó

$$n + m = k\left(\frac{1}{\alpha} + \frac{1}{\beta}\right) + \frac{r}{\alpha} + \frac{s}{\beta} = k + \frac{r}{\alpha} + \frac{s}{\beta}.$$

Nhưng

$$0 < \frac{r}{\alpha} + \frac{s}{\beta} < 1$$

nên đẳng thức trên không thể xảy ra. Vậy với mọi $m$, $n$ tự nhiên,

$$[\alpha n] \neq [\beta m] \quad (3)$$

Hơn nữa,

$$[\alpha(n+1)] \geq [\alpha n] + 1, \quad [\beta(n+1)] \geq [\beta n] + 2 > [\alpha n] + 1. \quad (3')$$

Mặt khác, với $k$ là số nguyên dương tùy ý, ta có :

- Nếu $n > \dfrac{k}{\alpha}$ thì $k < \alpha n < \dfrac{\alpha(k+1)}{\alpha} = k + 1$ và $[\alpha n] = k$.

- Nếu $n < \dfrac{k}{\alpha}$ thì

$$\beta(k - n) > \beta k - \frac{\beta}{\alpha} k = \beta k\left(1 - \frac{1}{\alpha}\right) = k,$$

$$\beta(k - n) < \beta k - \beta\left(\frac{k+1}{\alpha} - 1\right) = k + 1,$$

tức là $[\beta(k - n)] = k$.

Kết hợp với (3) và $(3')$ ta thấy rằng, với mỗi số nguyên dương $k$ được gặp một và chỉ một lần ở một trong hai dãy

$$[\alpha n], \quad [\beta n] \quad (3'')$$

Từ $(3'')$ và $(3')$ suy ra rằng $[\alpha(n+1)]$ là số tự nhiên nhỏ nhất khác với $[\alpha]$, $[\alpha 2]$, ..., $[\alpha n]$, $[\beta]$, $[\beta 2]$, ..., $[\beta n]$. Như vậy, dãy $[\alpha n]$, $[\beta n]$

cũng thỏa mãn mọi tính chất như $f(n)$, $g(n)$, nên ta có

$$f(n) = [\alpha n], \quad g(n) = [\beta n].$$

**91.** Xét các số hạng của dãy đã cho mà không là ước của bất kì số hạng nào khác thuộc dãy. Nếu tồn tại vô hạn số hạng như vậy thì ta được dãy con vô hạn của dãy đã cho, mà trong dãy con này, không có số hạng nào là bội của số hạng khác.

Giả sử số các số hạng có tính chất trên đây chỉ là hữu hạn. Ta loại các số hạng đó và các ước của chúng (nếu thuộc dãy) ra khỏi dãy đang xét. Như vậy, ta vẫn còn lại một dãy vô hạn. Trong dãy này, mỗi số hạng là ước của một số hạng khác nào đó. Rõ ràng từ dãy còn lại này, ta có thể chọn ra dãy vô hạn mà mỗi số hạng đều là bội của số hạng đứng trước nó.

**92.** Lập dãy đa thức $Q_k$ như sau : bậc của $Q_k \le k$,

$$Q_0 = -1,$$

$$Q_{k+1}(x) = b^{k+1}(x-1)Q_k(bx) - a(b^{k+1}x - 1)Q_k(x),$$

với mọi $k \ge 0$. Ta có :

$$Q_{k+1}(0) = (a - b^{k+1})Q_k(0).$$

Từ đó suy ra

$$Q_k(0) = -(a-b^k)(a-b^{k-1})\ldots(a-b).$$

Như vậy, bài toán sẽ được giải nếu tồn tại $k$ sao cho $Q_k(0) = 0$. Giả sử ngược lại, tức là với mọi $j$ nguyên dương, $a \ne b^j$. Ta chỉ ra mâu thuẫn bằng cách chứng tỏ rằng, tồn tại $k$ để $Q_k(x) \equiv 0$.

Với mọi $n$ nguyên dương, đặt

$$r_{0,n} = \frac{a^n - 1}{b^n - 1}.$$

Theo bài ra, $r_{0,n}$ nguyên. Với mọi $k \ge 0$,

$$r_{k+1,n} = b^{k+1}r_{k,n+1} - ar_{k,n};$$

$$p_0 = 1, \quad p_{k+1} = a(1 - b^{k+1})p_k.$$

Bằng quy nạp theo $k$, dễ chứng minh được rằng, với mọi $k \ge 0$, $n \ge 1$ ta có

$$r_{k,n} = \frac{p_k a^n + Q_k(b^n)}{(b^{n+k}-1)(b^{n+k-1}-1)\dots(b^n-1)}$$

Giả sử $a \neq b^k$ với mọi $k$. Khi đó tồn tại $k$ sao cho

$$b^k < a < b^{k+1}.$$

Vì

$$(b^n-1)(b^{n+1}-1)\cdots(b^{n+1}-1) = b^{n(k+1)}\left(1-\frac{1}{b^n}\right)\left(b-\frac{1}{b^n}\right)\cdots\left(b^k-\frac{1}{b^n}\right)$$

$$\geq \frac{b^{n(k+1)}}{2}$$

nên ta có

$$|r_{k,n}| \leq \frac{|p_k a^n + Q_k(b^n)|}{\frac{b^{n(k+1)}}{2}} \leq 2\left(|p_k|\left(\frac{a}{b^{k+1}}\right)^n + \frac{|Q_k(b^n)|}{(b^n)^{k+1}}\right). \quad (1)$$

Do $a < b^{k+1}$ và bậc của $Q_k$ nhỏ hơn $(k+1)$ nên vế phải của (1) giới nội bởi 1 khi $n$ đủ lớn. Mặt khác, $r_{k,n}$ nguyên với mọi $n$ nên suy ra $r_{k,n} = 0$ với $n$ đủ lớn. Như vậy, với mọi $n$ đủ lớn ta có :

$$p_k a^n + Q_k(b^n) = 0 \quad (2)$$

suy ra :

$$p_k\left(\frac{a}{b^k}\right)^n + \frac{Q_k(b^n)}{(b^n)^k} = 0. \quad (3)$$

Do $a > b^k$ nên $\left(\frac{a}{b^k}\right)^n \to \infty$ khi $n \to \infty$. Mặt khác, do bậc của $Q_k$ không vượt quá $k$ nên $\frac{Q_k(b^n)}{(b^n)^k}$ giới nội khi $n \to \infty$. Vậy (3) chứng tỏ rằng $p_k = 0$. Nhưng khi đó từ (2) suy ra rằng

$$Q_k(b^n) = 0 \text{ với mọi } n \text{ đủ lớn.}$$

Do $Q_k(x)$ là đa thức nên điều này chỉ có thể xảy ra khi $Q_k(x) \equiv 0$.

**93.** Xét phần dư khi chia cho 9 của các số thuộc tập hợp số nói trên. Ta thấy phần dư đó bằng phần dư của phép chia $1+2+\cdots+7 = 28$ cho 9, tức là bằng 1. Lũy thừa bậc 7 của các số đó chia 9 cũng dư 1. Rõ ràng

không thể chia 7 số đó thành hai nhóm sao cho tổng các lũy thừa bậc 7 của các số thuộc hai nhóm bằng nhau.

**94.** Giả sử $n$ là số tự nhiên lẻ, $p$ là một ước nguyên tố của $n$. Ta viết $n$ dưới dạng

$$n = 2r + 1 = sp^i, \quad \text{với } i > 0, \quad s \not\vdots p. \tag{1}$$

Nếu $n$ số tự nhiên liên tiếp có trung bình cộng là $m$ thì các số đó là

$$m - r,\ m - r + 1,\ \ldots,\ m + r - 1,\ m + r. \tag{2}$$

Tổng các số của dãy (2) là $mr$, tích của chúng là $m$ nhân với tích của hai bộ số tự nhiên liên tiếp :

$$(m - r)(m - r + 1)\ldots(m - 1) \quad \text{và} \quad (m + 1)(m + 2)\cdots(m + r).$$

Giả sử

$$\frac{r}{p} = a + \frac{b}{p}, \quad 0 < b < p.$$

Khi đó

$$2r + 1 = 2ap + 2b + 1 = sp^i.$$

Từ đó suy ra

$$2b + 1 = p, \quad a = \frac{sp^{i-1} - 1}{2}.$$

Vậy

$$\frac{r}{p} > a = \frac{sp^{i-1} - 1}{2} \geq \frac{p^{i-1} - 1}{2}$$

với mọi $i \geq 2$ $(p \geq 3)$.

Mặt khác, mỗi một trong hai bộ $r$ số tự nhiên liên tiếp từ $(m - r)$ đến $(m - 1)$ và $(m + 1)$ đến $(m + r)$ chứa $a$ bộ đầy đủ của $p$ số tự nhiên liên tiếp, vì thế tích của các số thuộc mỗi một trong hai bộ đó chia hết cho $p^a$. Vậy, nếu đặt $P$ là tích của $n$ số tự nhiên liên tiếp đang xét thì $\dfrac{P}{m} \vdots p^{2a}$. Do đó $\dfrac{P}{m} \vdots p^i$.

**95.** Giả sử $a_1, \ldots, a_n$ là các số đã cho, $b_1 = \{a_1\}$, $b_2 = \{a_1 + a_2\}$, ... , $b_n = \{a_1 + \cdots + a_n\}$, trong đó $\{x\}$ kí hiệu phần lẻ của $x$. Các số $b_1, \ldots, b_n$ thỏa mãn

$$0 \le b_j < 1, \quad j = 1, \ldots, n.$$

Chia đoạn $[0, 1)$ thành $(n+1)$ khoảng độ dài bằng nhau :

$$\Delta_0 = \left[0, \frac{1}{n+1}\right), \quad \Delta_1 = \left[\frac{1}{n+1}, \frac{2}{n+1}\right), \quad \ldots, \quad \Delta_n = \left[\frac{n}{n+1}, 1\right).$$

Nếu ít nhất một trong các số $b_j$ rơi vào một trong các đoạn tận cùng $\Delta_0$ hoặc $\Delta_n$ thì khẳng định của bài toán là đúng (chỉ cần chọn $a_1, \ldots, a_j$). Nếu ngược lại, $(n-1)$ đoạn $\Delta_1, \ldots, \Delta_{n-1}$ sẽ chứa các số $b_1, \ldots, b_n$. Như vậy, có ít nhất một đoạn trong chúng chứa hai điểm nào đó $b_k$, $b_l$. Giả sử $k > l$, khi đó

$$a_{l+1} + a_{l+2} + \cdots + a_k = (a_1 + \cdots + a_k) - (a_1 + \cdots + a_l) = M + (b_k - b_l),$$

trong đó $M$ là số nguyên nào đó. Vậy bộ $a_{l+1}, \ldots, a_k$ chính là các số cần tìm, vì

$$|b_k - b_l| < \frac{1}{n+1}.$$

Dễ thấy rằng, số $\dfrac{1}{n+1}$ không thể làm nhỏ hơn: chỉ cần lấy mọi số bằng $\dfrac{1}{n+1}$.

**96.** Trước tiên ta nhận xét rằng, nếu $m = kl$ với $l$ lẻ, $l > 2k+1$ thì $M \le (k+1)l$. Thật vậy, xét

$$T = \left\{kl,\ k(l+1),\ \left(k+\frac{1}{2}\right)(l-1),\ \left(k+\frac{1}{2}\right)(l+1),\ (k+1)(l-1),\ (k+1)l\right\}.$$

Khi đó $m(T) = kl = m$, $M(T) = (k+1)l$ và $P(T)$ chính phương. Chú ý rằng, 4 số hạng ở giữa không nhất thiết đã được sắp theo thứ tự tăng dần. Hơn nữa, có thể có cặp số bằng nhau chẳng hạn

$$k(l+1) = \left(k+\frac{1}{2}\right)(l-1).$$

Khi đó, ta loại cặp nói trên và vẫn được tập hợp có các tính chất đòi hỏi. Vậy $M \le M(T) = (k+1)l$.

Theo bài ra, $m$ có ước nguyên tố $p > \sqrt{2m} + 1$. Như vậy, $p$ chỉ xuất hiện trong khai triển của $m$ thành thừa số nguyên tố với số mũ 1. Mặt

khác,

$$p > 2 \cdot \frac{m}{p} + 1$$

nên $M \le \left(\frac{m}{p} + 1\right) = m + p$ (theo nhận xét) (2). Do $p$ chỉ có số mũ 1 trong khai triển $m$ nên để $P(T)$ chính phương, $T$ phải chứa số lớn hơn $m$ và chia hết cho $p$. Số nhỏ nhất có tính chất đó là $m + p$. Vậy $M(T) \ge m + p$, tức là $M \ge m + p$. (3). Từ (2) và (3) suy ra $M = m + p$.

Từ nhận xét, ta xây dựng được tập $T$ có $M_T = m + p$.

**97.** Số các số nguyên chia hết cho 3 trong tập hợp các số $\{1,2,...,N\}$ là $\left[\frac{N}{3}\right]$ ([ ] là kí hiệu phần nguyên). Tương tự, số các số nguyên trong tập hợp đó chia hết cho 5, 7 là $\left[\frac{N}{5}\right]$ và $\left[\frac{N}{7}\right]$. Có cả thảy $\left[\frac{N}{35}\right]$ số chia hết cho 5 và 7, nên số các số chia hết cho 5 hoặc 7 là $\left[\frac{N}{5}\right] + \left[\frac{N}{7}\right] - \left[\frac{N}{35}\right]$.

Theo bài ra, ta cần tìm số $N$ lớn nhất sao cho

$$\left[\frac{N}{3}\right] = \left[\frac{N}{5}\right] + \left[\frac{N}{7}\right] - \left[\frac{N}{35}\right],$$

tức là

$$\left[\frac{N}{3}\right] + \left[\frac{N}{35}\right] = \left[\frac{N}{5}\right] + \left[\frac{N}{7}\right]. \quad (1)$$

Nếu $N$ thoả mãn (1) thì ta có :

$$\frac{N-2}{3} + \frac{N-34}{35} \le \frac{N}{5} + \frac{N}{7},$$

suy ra $N \le 86$.

Mặt khác, nếu $70 \le N \le 86$ thì từ (1) ta có :

$$\frac{N-2}{3} + \frac{N-16}{35} \le \frac{N}{5} + \frac{N}{7},$$

suy ra $N \le 59$, mâu thuẫn với $N \ge 70$. Vậy số $N$ cùng lắm chỉ là 69.

Thử trực tiếp (1) cho $N \le 69$ ta được :

- Khi $N = 69$ : (1) trở thành $23 + 1 = 13 + 9$ : sai

- Khi $N = 68,\ 67,\ 66$ : (1) trở thành $22 + 1 = 13 + 9$ : sai

- Khi $N = 65$ : (1) trở thành $21 + 1 = 13 + 9$ : đúng.

Vậy số $N$ lớn nhất cần tìm là $N = 65$.

**98.** Ta sẽ chứng minh bằng quy nạp (theo số chữ số của $n$). Đẳng thức

$$n = S(n) + 9T(n). \tag{1}$$

Nếu $n$ chỉ gồm một chữ số thì đẳng thức hiển nhiên đúng. Giả sử đẳng thức đúng với mọi số nguyên dương $n$ có $k$ chữ số. Ta thấy rằng, mọi số $m$ có $(k+1)$ chữ số đều có thể viết dưới dạng

$$m = 10n + a,$$

trong đó $n$ là số có $k$ chữ số. Rõ ràng là :

$$T(m) = n + T(n), \quad S(m) = S(n) + a.$$

Do đó

$$\begin{aligned} m - S(m) &= 10n + a + S(n) - a \\ &= 10n - S(n) \\ &= (n - S(n)) + 9n \\ &= 9T(n) + 9n \\ &= 9T(n). \end{aligned}$$

Đẳng thức (1) được chứng minh cho $m$.

**99.** Ta đặt $a_r = 2^{b_r}.c_r$, trong đó $c_r$ $(r = 1,\ldots,n)$ là các số lẻ. Do không có hai số $a_r$, $a_s$ nào chia hết cho nhau $(r \neq s)$ nên các $c_r$ đều khác nhau. Vậy, $\{c_1,\ c_2,\ \ldots,\ c_n\}$ là một phép thế nào đó của $\{1,\ 3,\ \ldots,\ 2n-1\}$.

Ta xét dãy con $\{a_r\}$ mà các từ $c_r$ có dạng $1,\ 3,\ \ldots,\ 3^k$. Các số của dãy sẽ có dạng

$$2^{s_i}3^i, \quad i = 0,\ 1,\ 2,\ldots,\ k,$$

đồng thời $s_i > s_{i+1}$, vì các số không chia hết cho nhau. Vậy :

$$s_i > s_{i+1} > \cdots > s_1 \geq 0,$$

suy ra $s_i \geq k - i$. Do đó

$$2^s.3^t \geq 2^{k-t}3^t \geq 2^k.$$

Nếu $a_1$ thuộc dãy con đang xét thì $a_1 \geq 2^k$, chứng minh xong.

Giả sử $a_1$ không thuộc dãy con đang xét. Khi đó ta có $a_1 = 2^{b_1}.c_1$, với $c_1 \geq 5$. Ta chứng minh $a_1 \geq 2^k$ bằng phản chứng. Giả sử ngược lại, $2^{b_1}.c_1 < 2^k$. Khi đó $5 \leq c_1 < 2^{k-b_1}$, suy ra $k - b_1 \geq 3$.

Theo chứng minh trên, $c_r$ là các số lẻ khác nhau và nhỏ hơn $2n$. Do đó, các số $c_1 3^{t-1}$ với $t = 1, 2, \ldots, n+2$, thuộc bộ số $\{c_r\}$ đang xét, vì số lớn nhất là

$$c_1 3^{b_1+1} < 2^{k-b_1}.3^{b_1+1} < 3^2.2^{k-b_1-3}.3^{b_1+1} < 3^k < 2n.$$

Như vậy, các số $\{c_1 3^{t-1},\ t = 1, 2, \ldots, b_1 + 2\}$ cho ta một dãy con của dãy xuất phát

$$a_t = c_1 3^{t-1}.2^{b_t},\ t = 1, 2, \ldots, b_1 + 2. \qquad (1)$$

Trong dãy này sẽ có hai số chia hết cho nhau. Thật vậy, nếu $b_{t_1} = b_{t_2}$ nào đó thì rõ ràng $a_{t_1}$ chia hết cho $a_{t_2}$ (nếu $t_1 > t_2$). Nếu các $b_t$ khác nhau đôi một thì dãy $\{b_t\}$ nhận $b_1 + 2$ giá trị nguyên không âm khác nhau, mỗi số không vượt quá $b_1$ (vì từ (1), do các $a_t$ không chia hết cho nhau nên $b_1 \geq b_2 \geq \cdots$). Mâu thuẫn này kết thúc chứng minh.

**100.** Giả sử đa thức $P(x)$ bậc $n$, có dạng,

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Không giảm tổng quát, có thể xem $P(x)$ có hệ số nguyên, và hệ số của $x^n$ bằng 1, tức là

$$P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

trong đó $a_0, a_1, \ldots, a_{n-1}$ là các số nguyên.

Rõ ràng là, với mọi số $p$ nguyên tố, đa thức

$$Q(x) = P(x) - p - a_0$$

cũng có tính chất đã nêu. Mặt khác, do $Q(0) < 0$, $Q(x) \to \infty$ khi $x \to \infty$ nên $Q(x)$ có nghiệm thực, tức là tồn tại $x_0$ để $Q(x_0) = 0$. Do $Q(x)$ nhận giá trị hữu tỉ khi và chỉ khi $x$ hữu tỉ nên suy ra $x_0$ là số hữu tỉ.

Giả sử $x = \frac{r}{s}$ là một nghiệm hữu tỉ tùy ý của $Q(x)$. Khi đó ta có

$$P\left(\frac{r}{s}\right) - a_0 = p,$$

$$r^n + a_{n-1}sr^{n-1} + \cdots + a_1 s^{n-1} r = p.$$

Như vậy, $r \mid p$, suy ra $r = \pm 1$ hoặc $r = \pm p$. Do $x_0$ là nghiệm hữu tỉ của $Q(x)$ nên $x_0 = \pm 1$ hoặc $x_0 = \pm p$. Vì $p$ có thể lớn tùy ý nên nếu lấy $p$ đủ lớn thì rõ ràng $Q(\pm 1) < 0$. Mặt khác, nếu bậc của $Q(x)$ là $n \geq 2$ thì khi $p$ đủ lớn, $|Q(\pm p)| > 0$. Suy ra bậc $Q(x)$ bằng 1, và do đó $P(x) = ax + b$ với $a$, $b$ hữu tỉ nào đó. Rõ ràng các đa thức như vậy thỏa mãn bài ra.

**101.** Ta gọi một số là "tốt" nếu nó đồng dư với 0, 1 hoặc 4 môđulô 5, là "xấu" nếu nó đồng dư với 2, 3 môđulô 5.

Dễ thấy rằng lũy thừa của một số tốt là số tốt.

Như vậy, người thứ hai sẽ có chiến lược để thắng, không tùy thuộc cách chơi của người thứ nhất. Thật vậy, mỗi lần đến lượt mình, người thứ hai luôn xóa số tốt $a$, số xấu $b$, và thay vào đó số tốt $a^b$ (chừng nào còn có thể). Như vậy, mỗi lần, số các số xấu bị giảm đi một. Vì các số xấu ít hơn một nửa các số nên đến lúc nào đó, trên bảng chỉ còn lại toàn số tốt. Do đó, số cuối cùng còn lại trên bảng là số tốt, tức là số đồng dư $0$, $1$ hoặc $4$ môđulô 5. Số này có chữ số tận cùng là 0, 1, 4, 6 hoặc 9. Vậy với cách chơi đó, người thứ hai sẽ thắng.

**102.** a) Ta chỉ ra một cấp số cộng với công sai 12 có tính chất đã nêu : 1, 13, 25.

Ta có : $5^2 + 1 = 13.2$, $7^2 + 1 = 25.2$.

Vậy $(35)^2 + 1 \vdots 13.25$.

b) Xét 3 số hạng đầu của cấp số cộng tùy ý công sai 10 :

$$a, \quad a + 10, \quad a + 20.$$

Trong ba số hạng đó phải có số hạng chia hết cho 3, trong khi $(n^2 + 1)$ không chia hết cho 3 với mọi $n$. Vậy không tồn tại cấp số cộng công sai 10 thỏa mãn tính chất đã nêu.

Lí luận tương tự cho trường hợp công sai 11.

c) Dễ thử lại rằng, với mọi $n$, số $(n^2+1)$ không chia hết cho 7. Nếu tồn tại cấp số cộng công sai 12 có không ít hơn 7 số hạng, thì từ 7 số hạng đầu tiên, ta tìm được số hạng chia hết cho 7 hoặc hai số hạng có hiệu chia hết cho 7. Nếu cấp số cộng đó thỏa mãn bài ra thì không có số hạng nào chia hết cho 7, do đó tồn tại $k$, $0<k<7$ mà $12k \vdots 7$. Vô lí. Vậy, cấp số cộng công sai 12 thoả mãn bài ra có cùng lắm là 6 số hạng.

Ta chỉ ra cấp số cộng gồm 6 số hạng sau đây thỏa mãn bài ra :

$$5,\ 17,\ 29,\ 41,\ 53,\ 65.$$

Cần chứng minh tồn tại $n$ sao cho

$$n^2+1 \vdots 5.17.29.41.53.65 = (25).17.29.41.53.13. \qquad (1)$$

Mỗi một số trong 6 số ở vế phải của (1) có tính chất đòi hỏi. Thật vậy,

$(7+25x)^2+1 \vdots 25$, $\qquad$ $(4+17y)^2+1 \vdots 17$,

$(12+29z)^2+1 \vdots 29$, $\qquad$ $(9+414u)^2+1 \vdots 41$,

$(23+53v)^2+1 \vdots 53$, $\qquad$ $(5+13w)^2+1 \vdots 13$,

trong đó $x,\ y,\ z,\ u,\ w$ là các số nguyên tùy ý. Như vậy, chỉ cần tìm $n$ thỏa mãn hệ đồng dư sau :

$$\begin{aligned} n &\equiv 7 \pmod{25} \\ &\equiv 4 \pmod{17} \\ &\equiv 12 \pmod{19} \\ &\equiv 9 \pmod{41} \\ &\equiv 23 \pmod{53} \\ &\equiv 5 \pmod{13}. \end{aligned}$$

Sự tồn tại của $n$ suy ra từ Định lí Trung quốc về phần dư.

**103.** Bất đẳng thức đúng với $n=1,\ 2$. Ta giả sử $n \geq 3$. Đặt $k = [\sqrt{2n}]+1$,

$$A_k = \left\{\frac{n}{1}\right\} - \left\{\frac{n}{2}\right\} + \cdots - (-1)^{k-1}\left\{\frac{n}{k-1}\right\}$$

$$B_k = \left\{\frac{n}{k}\right\} - \left\{\frac{n}{k+1}\right\} + \cdots + (-1)^{n-k}\left\{\frac{n}{k}\right\}.$$

Rõ ràng

$$A \le \left\{\frac{n}{1}\right\} + \left\{\frac{n}{3}\right\} + \cdots,$$

tổng gồm $\left[\frac{k}{2}\right]$ số hạng (xem số hạng thứ nhất bằng 0). Mặt khác

$$A \ge -\left\{\frac{n}{2}\right\} - \left\{\frac{n}{4}\right\} - \cdots,$$

gồm $\left[\frac{k-1}{2}\right]$ số hạng. Với số tự nhiên $m < k$ ta có

$$\left\{\frac{n}{m}\right\} \le \frac{m-1}{m} \le \frac{k-2}{k-1},$$

do đó

$$|A| \le \left[\frac{k-1}{2}\right] \cdot \frac{k-2}{k-1} \le \frac{k-2}{2}.$$

Vì với mọi số thực $x$, $\{x\} = x - [x]$ nên ta có

$$B = C - D,$$

trong đó

$$C = \frac{n}{k} - \frac{n}{k+1} + \cdots + (-1)^{n-k}\frac{k}{n},$$

$$D = \left[\frac{n}{k}\right] - \left[\frac{n}{k+1}\right] + \cdots + (-1)^{n-k}\left[\frac{n}{n}\right].$$

Mặt khác,

$$0 \le \left(\frac{k}{n} - \frac{n}{k+1}\right) + \left(\frac{n}{k+2} - \frac{n}{k+3}\right) + \cdots = C =$$

$$= \frac{n}{k} - \left(\frac{n}{k+1} - \frac{n}{k+2}\right) - \cdots \le \frac{n}{k}.$$

Vậy,

$$0 \le C \le \frac{n}{k}.$$

Tương tự,

$$0 \le D \le \left[\frac{n}{k}\right] \le \frac{n}{k}.$$

Do đó

$$|B| = |C - D| \leq \frac{n}{k}.$$

Ta được

$$\begin{aligned}\left|\left\{\frac{n}{1}\right\} - \left\{\frac{n}{2}\right\} + \left\{\frac{n}{3}\right\} - \cdots - (-1)^n \left\{\frac{n}{n}\right\}\right| &= \left|A - (-1)^k B\right| \\ &\leq \frac{k-2}{2} + \frac{n}{k} \\ &< \frac{\sqrt{2n}-1}{2} + \sqrt{\frac{n}{2}} \\ &< \sqrt{2n}\,.\end{aligned}$$

# MỤC LỤC

*Chịu trách nhiệm xuất bản :*
Chủ tịch HĐQT kiêm Tổng Giám đốc NGÔ TRẦN ÁI
Phó Tổng Giám đốc kiêm Tổng biên tập VŨ DƯƠNG THỤY

*Biên tập nội dung :*
TRẦN PHƯỚC CHƯƠNG

*Trình bày bìa :*
TRỊNH THANH SƠN

*Sửa bản in :*
HÀ HUY KHOÁI

---

**CHUYÊN ĐỀ BỒI DƯỠNG HỌC SINH GIỎI TOÁN TRUNG HỌC PHỔ THÔNG : SỐ HỌC**

In 5.000 bản, khổ 17 x 24 cm tại Xí nghiệp In Chuyên Dùng TTHuế. Giấy phép xuất bản số: 276/41 - 04/CXB do Cục Xuất bản cấp ngày 15 tháng 03 năm 2004. In xong và nộp lưu chiểu tháng 6 năm 2004.