

**ĐẠI HỌC QUỐC GIA HÀ NỘI  
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN  
KHỐI THPT CHUYÊN TOÁN - TIN**

---

**NGUYỄN VŨ LƯƠNG (Chủ biên)  
NGUYỄN LƯU SƠN - NGUYỄN NGỌC THẮNG - PHẠM VĂN HÙNG**

# **CÁC BÀI GIẢNG VỀ SỐ HỌC**

**ĐỒNG DƯ, PHƯƠNG TRÌNH NGHIỆM NGUYÊN, HÀM SỐ HỌC**

# Mục Lục

<b>1 Các định lý cơ bản về đồng dư</b>	<b>3</b>
1 Định lý nhỏ của Fermat, định lý Wilson . . . . .	3
2 Phương trình đồng dư . . . . .	16
2.1 Phương trình đồng dư . . . . .	16
2.2 Phương trình đồng dư tuyến tính . . . . .	18
2.3 Phương trình đồng dư modulo một số nguyên tố .	19
3 Định lý thặng dư Trung Hoa . . . . .	32
4 Cấp của một số nguyên . . . . .	46
4.1 Cấp của một số nguyên . . . . .	46
4.2 Căn nguyên thuỷ . . . . .	48
5 Thặng dư toàn phương . . . . .	73
5.1 Thặng dư toàn phương . . . . .	73
5.2 Luật thuận nghịch bình phương . . . . .	78
<b>2 Phương trình nghiệm nguyên</b>	<b>81</b>
1 Phương trình Pythagore . . . . .	81
2 Phương trình Pell . . . . .	86
2.1 Công thức nghiệm . . . . .	87
2.2 Phương trình $x^2 - dy^2 = -1$ . . . . .	97
3 Các bài toán khác . . . . .	107
<b>3 Hàm số học</b>	<b>121</b>
1 Phần nguyên . . . . .	121
2 Một số hàm số học . . . . .	141
3 Hàm Möbius . . . . .	155

# Chương 1

## Các định lý cơ bản về đồng dư

### 1 Định lý nhỏ của Fermat, định lý Wilson

#### Định lý 1.1.1 (Định lý nhỏ của Fermat)

Cho  $p$  là một số nguyên tố,  $a$  là một số nguyên thoả mãn  $a \not\equiv p$ . Khi đó,

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

Đối với số nguyên  $a$  bất kì,  $a^p \equiv a \pmod{p}$ .

#### Định lý 1.1.2 (Định lý Euler)

Cho  $a, m$  là các số nguyên,  $(a, m) = 1$ . Khi đó,

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

#### Chứng minh

Gọi  $(r_1, r_2, \dots, r_{\phi(m)})$  là một hệ thặng dư thu gọn modulo  $m$ . Vì  $(a, m) = 1$  nên  $(ar_1, ar_2, \dots, ar_{\phi(m)})$  cũng là một hệ thặng dư thu gọn modulo  $m$ .

Từ định nghĩa của hệ thặng dư thu gọn, ứng với mỗi  $i$ ,  $1 \leq i \leq \phi(m)$  tồn tại duy nhất  $1 \leq j \leq \phi(m)$  sao cho  $r_i \equiv ar_j \pmod{m}$  và ngược lại, với mỗi  $j$ ,  $1 \leq j \leq \phi(m)$  tồn tại duy nhất  $1 \leq i \leq \phi(m)$  sao cho  $ar_j \equiv r_i \pmod{m}$ .

mod  $m$ . Từ đó,

$$\prod_{j=1}^{\phi(m)} (ar_j) = a^{\phi(m)} \prod_{j=1}^{\phi(m)} r_j \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}.$$

Do  $(r_i, m) = 1$  với  $i = 1, 2, \dots, \phi(m)$  nên ta có  $a^{\phi(m)} \equiv 1 \pmod{m}$ .  
Định lý được chứng minh.

### Chứng minh định lý 1.1.1

Do  $p$  là số nguyên tố nên  $(1, 2, 3, \dots, p-1)$  là một hệ thặng dư thu gọn modulo  $p$ , từ đó suy ra  $\phi(p) = p-1$ .

Nếu  $a \not\equiv p$  thì  $(a, p) = 1$ , do đó áp dụng định lý Euler ta có

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

Từ đó dễ dàng suy ra trong trường hợp  $a$  bất kì ta luôn có  $a^p \equiv a \pmod{p}$ .  
Định lý được chứng minh.

### Định lý 1.1.3

Cho  $a, m$  là các số nguyên,  $(a, m) = 1$ . Khi đó, tồn tại một số nguyên  $x$  sao cho  $ax \equiv 1 \pmod{m}$ .

Nếu  $x_1, x_2$  thoả mãn  $ax_1 \equiv ax_2 \equiv 1 \pmod{m}$  thì  $x_1 \equiv x_2 \pmod{m}$ .

### Chứng minh

Vì  $(a, m) = 1$  nên tồn tại các số nguyên  $x, y$  sao cho  $ax + my = 1$ .  
Từ đó suy ra phương trình  $ax \equiv 1 \pmod{m}$  có nghiệm.

Ngược lại, nếu tồn tại số nguyên  $x$  thoả mãn  $ax \equiv 1 \pmod{m}$  thì đồng thời tồn tại số nguyên  $y$  sao cho  $ax + my = 1$ . Suy ra  $(a, m) = 1$ .

Nếu  $ax_1 \equiv ax_2 \equiv 1 \pmod{m}$  thì ta có  $(a, m) = 1$ , từ đó suy ra  $x_1 \equiv x_2 \pmod{m}$ . Định lý được chứng minh.

Giả sử  $(r_1, r_2, \dots, r_{\phi(m)})$  là một hệ thặng dư thu gọn modulo  $m$ ,  $a$  là một số nguyên thoả mãn  $(a, m) = 1$ . Khi đó, từ định nghĩa hệ thặng dư thu gọn và định lý 1.1.3 ta có

- Với mỗi  $i$ ,  $1 \leq i \leq \phi(m)$  tồn tại duy nhất  $j$ ,  $1 \leq j \leq \phi(m)$  thoả mãn

$$r_i r_j \equiv 1 \pmod{m}.$$

Trong trường hợp này, lớp thặng dư  $r_j$  được gọi là nghịch đảo của lớp thặng dư  $r_i$ , kí hiệu bởi  $\bar{r}_i$ . Theo định lý Euler,

$$\bar{r}_i = r_i^{\phi(m)-1}.$$

- Với mỗi cặp  $(i, j)$ ,  $1 \leq i, j \leq \phi(m)$  tồn tại duy nhất  $k$ ,  $1 \leq k \leq \phi(m)$  thoả mãn

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

Giống như đối với phép nhân thông thường (nếu  $ab = c$  thì  $a^{-1}b^{-1} = c^{-1}$ ,  $a = (a^{-1})^{-1}$ ), ta luôn có

$$\bar{r}_i \bar{r}_j \equiv \bar{r}_k \pmod{m}, \quad r_i \equiv \bar{r}_i \pmod{m}.$$

- Với mỗi cặp  $(i, j)$ ,  $1 \leq i, j \leq \phi(m)$  tồn tại duy nhất  $l$ ,  $1 \leq l \leq \phi(m)$  thoả mãn

$$r_i r_l \equiv r_j \pmod{m}.$$

Dễ thấy, trong trường hợp này,  $r_l = \bar{r}_i r_j$ .

#### Bổ đề 1.1.4

Cho  $p$  là một số nguyên tố. Khi đó,  $x^2 \equiv 1 \pmod{p}$  nếu và chỉ nếu  $x \equiv \pm 1 \pmod{p}$ .

#### Chứng minh

Ta có  $x^2 \equiv 1 \pmod{p}$  nếu và chỉ nếu  $x^2 - 1 = (x - 1)(x + 1) \vdots p$ . Do  $p$  là số nguyên tố,  $(x - 1)(x + 1) \vdots p$  nếu và chỉ nếu  $x - 1 \vdots p$  hoặc  $x + 1 \vdots p$ , tức là  $x \equiv \pm 1 \pmod{p}$ . Bổ đề được chứng minh.

Từ bổ đề trên, nếu  $p$  là một số nguyên tố thì trong hệ thặng dư thu gọn  $R = \{r_1, r_2, \dots, r_{p-1}\}$  có đúng 2 lớp thặng dư thoả mãn phương trình

$$\bar{r}_i \equiv r_i \pmod{p}$$

là  $r_i \equiv \pm 1 \pmod{p}$ . Giả sử 2 lớp thặng dư đó là  $r_1$  và  $r_{p-1}$ . Đặt  $A = \{r_1, r_{p-1}\}$ .

Nếu  $\bar{r}_i \not\equiv r_i \pmod{p}$  thì tồn tại duy nhất  $j \neq i$  sao cho  $\bar{r}_i \equiv r_j \pmod{p}$ . Như vậy, tập hợp  $\{r_2, r_3, \dots, r_{p-2}\}$  có thể chia được thành  $(p-3)/2$  cặp phân biệt có dạng  $(r_i, \bar{r}_i)$ .

Xét các tập  $B$  và  $C$  sao cho với mỗi cặp như vậy,  $r_i \in B$  và  $\bar{r}_i \in C$ . Khi đó ta có

$$B \cap C = \emptyset, \quad B = \{j \in R \setminus A : \bar{j} \in C\}, \quad C = \{k \in R \setminus A : \bar{k} \in B\}.$$

### **Định lý 1.1.5 (Định lý Wilson).**

Cho  $p$  là một số nguyên tố. Khi đó,

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

### **Chứng minh**

Chia tập  $R = \{1, 2, \dots, p-1\}$  thành 3 tập  $A, B, C$  rời nhau thỏa mãn

$$A = \{i \in R : \bar{i} \equiv i \pmod{p}\}, \quad B = \{j \in R \setminus A : \bar{j} \in C\},$$

$$C = \{k \in R \setminus A : \bar{k} \in B\}.$$

Theo nhận xét trên ta có  $A = \{1, p-1\}$ . Từ đó và cách định nghĩa của  $B, C$  ta có

$$\begin{aligned} (p-1)! &= \prod_{i \in A} i \prod_{j \in B} j \prod_{k \in C} k \\ &= \prod_{i \in A} i \prod_{j \in B} j \prod_{k \in B} \bar{k} \\ &\equiv 1(p-1) \prod_{j \in B} (j\bar{j}) \\ &\equiv -1 \pmod{p}. \end{aligned}$$

Định lý được chứng minh.

### **Định lý 1.1.6**

Cho  $p$  là một số nguyên tố. Khi đó phương trình  $x^2 \equiv -1 \pmod{p}$

có nghiệm nếu và chỉ nếu  $p = 2$  hoặc  $p \equiv 1 \pmod{4}$ .

### Chứng minh

Nếu  $p = 2$ , phương trình có nghiệm  $x = 1$ .

Nếu  $p \equiv 1 \pmod{4}$  thì  $(p-1)/2$  là số chẵn. Đặt

$$x = 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}.$$

Ta có

$$1 \equiv -(p-1), 2 \equiv -(p-2), 3 \equiv -(p-3), \dots, (p-1)/2 \equiv -(p+1)/2 \pmod{p}$$

nên

$$x \equiv (-1)^{(p-1)/2} (p-1)(p-2)(p-3) \cdots \left(\frac{p+1}{2}\right) \pmod{p}.$$

Từ đó, do  $(p-1)/2$  là số chẵn và theo định lý Wilson ta có

$$\begin{aligned} x^2 &\equiv \left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right) \left((p-1)(p-2)(p-3) \cdots \left(\frac{p+1}{2}\right)\right) \\ &\equiv \left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right) \left(\frac{p+1}{2} \frac{p+3}{2} \cdots (p-1)\right) \\ &\equiv (p-1)! \\ &\equiv -1 \pmod{p}. \end{aligned}$$

Ngược lại, giả sử  $p$  là một số nguyên tố lẻ và tồn tại số nguyên  $x$  sao cho  $x^2 \equiv -1 \pmod{p}$ , khi đó theo định lý nhỏ của Fermat,

$$x^{p-1} \equiv (x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \equiv 1 \pmod{p}$$

Do  $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$  suy ra  $(p-1)/2$  là một số chẵn, tức là  $p \equiv 1 \pmod{4}$ . Định lý được chứng minh.

### Định lý 1.1.7

Cho  $p$  là một số nguyên tố,  $p \equiv 1 \pmod{4}$ . Khi đó tồn tại các số nguyên dương  $x, y$  sao cho

$$x^2 + y^2 = p.$$

### Bổ đề 1.1.8

Cho  $a, b$  là các số nguyên,  $q$  là một ước số nguyên tố của  $a^2 + b^2$ . Khi đó, nếu  $q \equiv 3 \pmod{4}$  thì  $a \nmid q$  và  $b \nmid q$ .

Từ bổ đề trên có thể chứng minh được định lý sau. Chứng minh xin dành cho độc giả.

### Định lý 1.1.9 (Fermat).

Cho  $n$  là một số nguyên có biểu diễn chuẩn tắc như sau

$$n = 2^\alpha \prod_{\substack{p \text{ nguyên tố} \\ p \equiv 1 \pmod{4}}} p^\beta \prod_{\substack{q \text{ nguyên tố} \\ q \equiv 3 \pmod{4}}} q^\gamma.$$

Khi đó,  $n$  có thể biểu diễn dưới dạng tổng của hai số chính phương khi và chỉ khi các số mũ  $\gamma$  là chẵn.

**Ví dụ 1.1.1.** Tìm tất cả các số nguyên dương  $n$  sao cho  $n$  là ước số của  $3^{12} - 1$  nhưng  $n$  không là ước số của  $3^i - 1$  với mọi  $i = 1, 2, 3, \dots, 11$ . Có bao nhiêu số chẵn và bao nhiêu số  $n$  lẻ?

### Giải

Giả sử  $n$  là một số nguyên tố lẻ thoả mãn điều kiện đề bài, do

$$3^{12} - 1 = (3^6 - 1)(3^2 + 1)(3^4 - 3^2 + 1)$$

và  $3^4 - 1 \vdash 3^2 + 1$  nên  $n$  phải là ước số của  $3^4 - 3^2 + 1 = 73$ . Do 73 là một số nguyên tố nên theo định lý nhỏ của Fermat,  $3^{72} \equiv 1 \pmod{73}$ . Kiểm tra với những  $i = 2, 3, 4, 8, 9$  (các ước số không vượt quá 11 của 72) ta thấy  $n = 73$  thoả mãn. Từ đó suy ra tất cả các số  $n$  thoả mãn điều kiện đề bài là  $73d$  với  $d$  là một ước số của  $(3^6 - 1)(3^2 + 1)$ .

**Ví dụ 1.1.2.** Cho dãy số  $(x_n)_{n \geq 1}$  được xác định như sau

$$x_1 = 2, \quad x_{n+1} = 2^{x_n} \quad \text{với mọi } n \geq 1.$$

Chứng minh rằng  $x_n \equiv x_{n-1} \pmod{n}$  với mọi  $n \geq 2$ .

**Giải**

Ta sẽ chứng minh bằng quy nạp theo  $n$  rằng

$$x_{n-1} \equiv x_n \equiv x_{n+1} \equiv \cdots \pmod{n} \quad \text{với mọi } n \geq 1.$$

Với  $n = 1$  và  $n = 2$  khẳng định đúng. Giả sử khẳng định đúng đến  $n - 1$ . Cần chứng minh khẳng định đúng đến  $n$ . Giả sử  $n > 2$ ,  $n = 2^a b$  với  $b$  là một số lẻ. Cần chứng minh

$$x_{n-1} \equiv x_n \equiv x_{n+1} \equiv \cdots \pmod{2^a} \quad \text{và} \pmod{b}.$$

Bằng quy nạp dễ chứng minh được  $x_{n-1} > n$  nên  $x_{n-2} \geq a$ , từ đó suy ra

$$x_{n-1} \equiv x_n \equiv x_{n+1} \equiv \cdots \pmod{2^a}.$$

Theo định lý Euler, để chứng minh  $x_{n-1} \equiv x_n \equiv x_{n+1} \equiv \cdots \pmod{b}$  điều kiện đủ là

$$x_{n-2} \equiv x_{n-1} \equiv x_n \equiv \cdots \pmod{\phi(b)}.$$

Mặt khác, do  $\phi(b) \leq n - 1$  nên theo giả thiết quy nạp,  $x_{n-2} \equiv x_{n-1} \equiv x_n \equiv \cdots \pmod{\phi(b)}$ . Từ đó suy ra khẳng định đúng với  $n$ . Theo nguyên lý quy nạp ta có điều phải chứng minh.

**Ví dụ 1.1.3.** Chứng minh rằng với mọi số nguyên tố  $p$ , tồn tại vô số số nguyên dương  $n$  thoả mãn

$$2^n - n \vdots p.$$

**Giải**

Nếu  $p = 2$  thì mọi  $n$  chẵn đều thoả mãn điều kiện đề bài nên không mất tính tổng quát nếu ta giả sử  $p > 2$ . Khi đó theo định lý nhỏ của Fermat,

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

Lấy  $n = m(p - 1)$  với  $m \equiv -1 \pmod{p}$  ta có  $n = m(p - 1) \equiv 1 \pmod{p}$  và

$$2^n - n \equiv 2^n - 1 \equiv 0 \pmod{p}.$$

Do có vô số số nguyên dương  $m$  sao cho  $m \equiv -1 \pmod{p}$  nên tồn tại vô số số nguyên dương  $n$  thoả mãn điều kiện đã cho. Điều phải chứng minh.

**Ví dụ 1.1.4.** Tìm tất cả các số nguyên tố  $p$  sao cho

$$5^{p^2} + 1 \equiv 0 \pmod{p^2}.$$

### Giải

Giả sử số nguyên tố  $p$  thoả mãn điều kiện đã cho. Khi đó

$$5^{2p^2} \equiv 1 \pmod{p}.$$

Mặt khác, vì  $p^2 - 1 : p - 1$  nên theo định lý nhỏ của Fermat ta có

$$5^{2(p^2-1)} \equiv 1 \pmod{p}.$$

Từ đó suy ra  $5^2 \equiv 1 \pmod{p}$  nên  $p$  chỉ có thể bằng 2 hoặc 3. Kiểm tra trực tiếp suy ra  $p = 3$  thoả mãn điều kiện đề bài.

**Ví dụ 1.1.5.** Cho  $a, b$  là các số nguyên dương nguyên tố cùng nhau. Chứng minh rằng tồn tại các số nguyên dương  $m, n$  sao cho

$$a^m + b^n - 1 : ab.$$

### Giải

Lấy  $m = \phi(b)$ ,  $n = \phi(a)$ , vì  $(a, b) = 1$  nên theo định lý Euler ta có

$$a^m - 1 = a^{\phi(b)} - 1 : b, \quad b^{\phi(a)} - 1 : a.$$

Từ đó suy ra

$$a^m + b^n - 1 : ab.$$

Điều phải chứng minh.

**Ví dụ 1.1.6.** Cho  $a, b, m$  là các số nguyên dương. Chứng minh rằng các khẳng định sau tương đương:

- i, Tồn tại số nguyên dương  $n$  để  $(a^n - 1)b : m$ ,
- ii,  $(ab, m) = (b, m)$ .

**Giải**

Đặt  $(b, m) = d$ ,  $b = kd$ ,  $m = qd$ . Khi đó  $(q, k) = 1$  và

$$\begin{aligned} \text{ii}, \Leftrightarrow (a, q) = 1 &\Leftrightarrow \text{tồn tại số nguyên dương } n \text{ sao cho } a^n - 1 \mid d, \\ &\Leftrightarrow \text{tồn tại số nguyên dương } n \text{ sao cho } (a^n - 1)b \mid m. \end{aligned}$$

Từ đó ta có điều phải chứng minh.

**Ví dụ 1.1.7.** Cho  $n$  là một số nguyên dương lẻ,  $n \geq 5$  và có các ước số nguyên tố là  $p_1, p_2, \dots, p_k$ . Chứng minh rằng  $2^{\phi(n)} - 1$  có ước số nguyên tố không thuộc tập  $\{p_1, p_2, \dots, p_k\}$ .

**Giải**

Đặt

$$n = \prod_{i=1}^k p_i^{\alpha_i}, \quad m = \phi(n) = \prod_{i=1}^k (p_i^{\alpha_i-1}(p_i - 1)) = 2u.$$

Khi đó  $u \mid p_i - 1$  và  $2^u \mid p_i$  với mọi  $i = 1, 2, \dots, k$ . Mặt khác ta có

$$2^{2u} - 1 = (2^u - 1)(2^u + 1), \quad (2^u - 1, 2^u + 1) = 1$$

nên suy ra  $(2^u + 1, p_i) = 1$  với mọi  $i = 1, 2, \dots, k$ , tức là  $2^u + 1$  có ước số nguyên tố không thuộc tập  $\{p_1, p_2, \dots, p_k\}$ . Từ đó ta có  $2^{\phi(n)} - 1$  có ước số nguyên tố không thuộc tập  $\{p_1, p_2, \dots, p_k\}$ .

## BÀI TẬP

**Bài 1.** Chứng minh rằng không tồn tại một dãy vô hạn tăng các số nguyên tố  $\{p_n\}_n$  thoả mãn

$$|p_{n+1} - 2p_n| = 1, \quad \text{với mọi } n \geq 1.$$

**Bài 2.** Cho  $p$  là một số nguyên tố,  $\{r_1, r_2, \dots, r_p\}$  và  $\{s_1, s_2, \dots, s_p\}$  là các hệ thặng dư đầy đủ modulo  $p$ . Hỏi tập hợp  $\{r_1s_1, r_2s_2, \dots, r_ps_p\}$  có phải là một hệ thặng dư đầy đủ modulo  $p$  không?

**Bài 3.** Chứng minh rằng nếu  $p$  là một số nguyên tố thì  $(p-2)! - 1 : p$  nhưng nếu  $p > 5$  thì  $(p-2)! - 1$  không phải là một luỹ thừa của  $p$ .

**Bài 4.** Chứng minh rằng tồn tại vô số số nguyên dương  $n$  sao cho  $n! - 1$  có ít nhất hai ước số nguyên tố.

**Bài 5.** Cho  $n$  là một số nguyên dương. Tìm  $(n! + 1, (n+1)!)$ .

**Bài 6 (Estonia 2000).** Chứng minh rằng không thể chia một tập hợp gồm 18 số nguyên dương liên tiếp thành hai tập con rời nhau  $A$  và  $B$  sao cho tích các phân tử của tập  $A$  bằng tích các phân tử của tập  $B$ .

**Bài 7.** Cho  $p > 3$  là số nguyên tố,  $n = (2^{2p} - 1)/3$ . Chứng minh rằng

$$2^n - n : n.$$

**Bài 8.** Tìm tất cả các số nguyên dương  $m$  sao cho nếu tồn tại số nguyên dương  $n$  thoả mãn

Nếu  $m^n \equiv 1 \pmod{n}$  thì  $m \equiv 1 \pmod{n}$ .

**Bài 9.** Cho  $n$  là một số nguyên dương, xét tập hợp

$$A_n = \{1 \leq a \leq n : (a, n) = (a+1, n) = 1\}.$$

Chứng minh rằng

$$\prod_{x \in A_n} x \equiv 1 \pmod{n},$$

## LỜI GIẢI

### Bài 1.

Giả sử  $(p_k, k \geq 1)$  là một dãy vô hạn các số nguyên tố thoả mãn điều kiện đề bài. Theo giả thiết, với mỗi  $k$ ,  $p_{k+1} = 2p_k - 1$  hoặc  $2p_k + 1$ . Vì  $p_{k+1}$  là một số nguyên tố nên khi xét số dư khi chia cho 3 ta có

- Nếu  $p_k \equiv -1 \pmod{3}$  thì  $p_{k+1} = 2p_k + 1 = 6l - 1$ .
- Nếu  $p_k \equiv 1 \pmod{3}$  thì  $p_{k+1} = 2p_k - 1 = 6l + 1$ .

Do đó chỉ có thể xảy ra hai khả năng sau

Nếu  $p_1 = p \equiv -1 \pmod{3}$  thì

$$p_k = 2^{k-1}p + 2^{k-1} - 1 \quad \text{với mọi } k \geq 1.$$

Chọn  $k = p$ , theo định lý Fermat ta có  $p_p \equiv 2^{p-1} - 1 \equiv 0 \pmod{p}$ . Vô lý.

Nếu  $p_k \equiv 1 \pmod{3}$  thì

$$p_k = 2^{k-1}p - (2^{k-1} - 1) \quad \text{với mọi } k \geq 1.$$

Chọn  $k = p$ , theo định lý Fermat ta có  $p_p \equiv -(2^{p-1} - 1) \equiv 0 \pmod{p}$ . Vô lý.

Vậy không tồn tại dãy vô hạn  $(p_k, k \geq 1)$  thoả mãn điều kiện đề bài.

### Bài 2.

Ta sẽ chứng minh  $\{r_1s_1, r_2s_2, \dots, r_ps_p\}$  không phải là một hệ thặng dư đầy đủ modulo  $p$ . Phản chứng, giả sử  $\{r_1s_1, r_2s_2, \dots, r_ps_p\}$  là một hệ thặng dư đầy đủ modulo  $p$ . Giả sử  $r_i \equiv s_j \equiv 0 \pmod{p}$ .

Nếu  $i \neq j$  thì  $r_i s_i \equiv r_j s_j \equiv 0 \pmod{p}$  nên tập hợp  $\{r_1s_1, r_2s_2, \dots, r_ps_p\}$  không thể là một hệ thặng dư đầy đủ modulo  $p$ . Từ đó suy ra  $i = j$ , không mất tính tổng quát nếu ta giả sử  $i = j = p$ . Khi đó  $\{r_1s_1, r_2s_2, \dots, r_{p-1}s_{p-1}\}$  là một hệ thặng dư thu gọn modulo  $p$  và theo định lý Wilson ta có

$$r_1s_1 \cdot r_2s_2 \cdot \dots \cdot r_{p-1}s_{p-1} \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \equiv -1 \pmod{p}.$$

Mặt khác, do  $\{r_1, r_2, \dots, r_{p-1}\}$  và  $\{s_1, s_2, \dots, s_{p-1}\}$  là các hệ thặng dư thu gọn modulo  $p$  nên theo định lý Wilson,

$$r_1.r_2.\dots.r_{p-1} \equiv s_1.s_2.\dots.s_{p-1} \equiv 1.2.\dots.(p-1) \equiv -1 \pmod{p}.$$

Từ đó suy ra

$$\begin{aligned} r_1s_1.r_2s_2.\dots.r_{p-1}s_{p-1} &= \\ &= (r_1.r_2.\dots.r_{p-1})(s_1.s_2.\dots.s_{p-1}) \equiv (-1)^2 \equiv 1 \pmod{p}. \end{aligned}$$

Vô lý. Vậy điều giả sử là sai và ta có điều phải chứng minh.

### Bài 3.

Ta có  $(p-1)! \equiv -1 \pmod{p}$  nên  $(p-2)! \equiv 1 \pmod{p}$ , từ đó suy ra  $(p-2)! - 1 \mid p$ . Giả sử  $p > 5$  và  $(p-2)! - 1 = p^m$ , khi đó vì  $(p-2)! \mid p-1$  nên  $p^m + 1 = (p^m - 1) + 2 \mid p-1$ , suy ra  $2 \mid p-1$  vô lý. Vậy với  $p > 5$  thì  $(p-2)! - 1$  không phải là một luỹ thừa của  $p$ . Điều phải chứng minh.

### Bài 4.

Theo ví dụ trên, với mọi  $n = p-1$  với  $p$  là một số nguyên tố đều thoả mãn ta có đề bài. Do đó tồn tại vô số số nguyên dương  $n$  sao cho  $n! - 1$  có ít nhất hai ước số nguyên tố.

### Bài 5.

Đặt

$$f(n) = (n! + 1, (n+1)!).$$

Dễ thấy  $f(3) = (7, 24) = 1$ . Nếu  $n+1 > 4$  không phải là một số nguyên tố thì  $n! \mid n+1$  nên

$$\begin{aligned} f(n) &= (n! + 1, (n+1)!) = (n! + 1, (n+1)(n! + 1) - (n+1)) = \\ &= (n! + 1, n+1) = 1. \end{aligned}$$

Nếu  $n+1$  là một số nguyên tố thì theo định lý Wilson,  $n! + 1 \mid n+1$ .

Do đó  $f(n) = 1$ . Vậy

$$(n! + 1, (n+1)!) = \begin{cases} 1 & \text{nếu } n+1 \text{ không phải là một số nguyên tố,} \\ n+1 & \text{nếu } n+1 \text{ là một số nguyên tố.} \end{cases}$$

**Bài 6 (Estonia 2000).**

Phản chứng. Giả sử có thể chia tập hợp  $S = \{n, n + 1, \dots, n + 17\}$  gồm 18 số nguyên dương liên tiếp thành hai tập rời nhau  $A$  và  $B$  sao cho

$$\prod_{a \in A} a = \prod_{b \in B} b.$$

Vì  $S = \{n, n + 1, \dots, n + 17\}$  chứa 18 số nguyên dương liên tiếp và 19 là một số nguyên tố nên chỉ có thể xảy ra 1 trong 2 khả năng sau

- Trong  $S$  có đúng một số chia hết cho 19.
- $S$  là một hệ thặng dư thu gọn modulo 19.

Nếu trong  $S$  có duy nhất một số chia hết cho 19 thì trong hai số  $\prod_{a \in A} a, \prod_{b \in B} b$  có đúng 1 số chia hết cho 19, do đó chúng không thể bằng nhau. Vô lý.

Nếu  $S$  là một hệ thặng dư thu gọn modulo 19 thì

$$\prod_{s \in S} s = \prod_{a \in A} a \prod_{b \in B} b = \left( \prod_{a \in A} a \right)^2 \equiv 18! \pmod{19}.$$

Theo định lý Wilson,  $18! \equiv -1 \pmod{19}$  nên suy ra  $-1$  là một số chính phương modulo 19. Vô lý vì  $19 = 4 \cdot 4 + 3$  là một số nguyên tố có dạng  $4k + 3$ .

Vậy điều giả sử là sai và ta có điều phải chứng minh.

## 2 Phương trình đồng dư

### 2.1 Phương trình đồng dư

Trong toàn bộ tiết này, ta chỉ xét các đa thức với các hệ số nguyên. Tương tự việc giải các phương trình đại số có rất nhiều câu hỏi được đặt ra một cách tự nhiên cho phương trình đồng dư. Chẳng hạn, liên hệ giữa số nghiệm của một phương trình đồng dư và bậc của nó. Tiết này được trình bày nhằm giải quyết một số câu hỏi như vậy. Giả sử  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_0$  là một đa thức (với các hệ số nguyên). Số nguyên  $x_0$  được gọi là nghiệm của phương trình đồng dư  $f(x) \equiv 0 \pmod{m}$  nếu  $f(x_0) \equiv 0 \pmod{m}$ .

Vì, nếu  $x_1 \equiv x_0 \pmod{m}$  thì  $x_1$  cũng là nghiệm của phương trình  $f(x) \equiv 0 \pmod{m}$  nên thay vì nói  $x_0$  là một nghiệm của phương trình  $f(x) \equiv 0 \pmod{m}$ , ta nói rằng  $x \equiv x_0 \pmod{m}$  là một nghiệm của phương trình  $f(x) \equiv 0 \pmod{m}$ . Từ đó dẫn đến định nghĩa sau

#### Định nghĩa 1.2.1.

Cho  $r_1, r_2, \dots, r_m$  là một hệ thăng dư đầy đủ modulo  $m$ . Số nghiệm của phương trình  $f(x) \equiv 0 \pmod{m}$  được định nghĩa là số các  $r_i$  thoả mãn  $f(r_i) \equiv 0 \pmod{m}$ .

Dễ thấy rằng, với cùng một đa thức  $f(x)$  số nghiệm của phương trình  $f(x) \equiv 0 \pmod{m}$  phụ thuộc vào  $m$ .

Chẳng hạn, xét phương trình

$$x^2 + 1 \equiv 0 \pmod{m}$$

với  $m$  là một số nguyên tố. Khi đó nếu  $m = 2$  hoặc  $m \equiv 1 \pmod{4}$  thì phương trình có nghiệm, nếu  $m \equiv 3 \pmod{4}$  thì phương trình vô nghiệm.

#### Định nghĩa 1.2.2.

Cho đa thức  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_0$ . Khi đó, bậc của phương trình  $f(x) \equiv 0 \pmod{m}$  được định nghĩa là số nguyên  $j$  lớn nhất,  $j \leq n$  sao cho  $a_j \not\equiv 0 \pmod{m}$ .

Nếu không tồn tại số nguyên  $j$  như vậy, phương trình được coi như không có bậc.

Theo các định nghĩa trên, ta có các nhận xét sau:

- Khi xét phương trình  $f(x) \equiv 0 \pmod{m}$ , tất cả các nghiệm đều được xét theo modulo  $m$ . Ví dụ, xét phương trình

$$x^2 - 1 \equiv 0 \pmod{4} \quad ((x-1)(x+1) \equiv 0 \pmod{4})$$

có 2 nghiệm là  $x \equiv \pm 1 \pmod{4}$ . Phương trình

$$x^2 - 1 \equiv 0 \pmod{6} \quad ((x-1)(x+1) \equiv 0 \pmod{6})$$

có 2 nghiệm là  $x \equiv \pm 1 \pmod{6}$ .

- Với cùng một đa thức  $f(x)$ , khi xét các phương trình  $f(x) \equiv 0 \pmod{m}$  với các số nguyên  $m$  khác nhau các phương trình có thể có bậc khác nhau. Chẳng hạn, xét đa thức

$$f(x) = 25x^3 + 16x^2 + 9x + 4.$$

Khi đó, phương trình  $f(x) \equiv 0 \pmod{5}$  có bậc 2, trong khi phương trình  $f(x) \equiv 0 \pmod{3}$  có bậc 3.

- Khác với phương trình đại số, một phương trình đồng dư có thể có số nghiệm lớn hơn số bậc. Chẳng hạn phương trình bậc 2

$$x^2 - 1 \equiv 0 \pmod{8}$$

có 4 nghiệm là  $x \equiv \pm 1, \pm 3 \pmod{8}$ .

Tuy nhiên, khi  $m$  là một số nguyên tố, số nghiệm của một phương trình đồng dư sẽ không vượt quá số bậc của nó.

### **Định lý 1.2.1.**

Cho  $d$  là một ước số của  $m$ ,  $x_0$  là một nghiệm của phương trình đồng dư  $f(x) \equiv 0 \pmod{m}$ . Khi đó,  $x_0$  cũng là một nghiệm của phương trình đồng dư  $f(x) \equiv 0 \pmod{d}$ .

### **Chứng minh**

Suy ra từ định nghĩa và định lý 1.2.1.

## 2.2 Phương trình đồng dư tuyến tính

Xét phương trình đồng dư

$$ax + b \equiv 0 \pmod{m}$$

Mục đích của phần này là tìm điều kiện cần và đủ của  $a$  và  $b$  (theo  $m$ ) để phương trình có nghiệm.

Theo nhận xét sau định lý 1.1.3, nếu  $(a, m) = 1$  thì tồn tại số nguyên  $\bar{a}$ ,  $(\bar{a}, m) = 1$  thoả mãn phương trình  $a\bar{a} \equiv 1 \pmod{m}$ . Do đó, khi nhân cả 2 vế của phương trình đang xét với  $\bar{a}$  ta thấy nó luôn có nghiệm

$$x \equiv -\bar{a}b \pmod{m}.$$

Do  $(a, m) = 1$ , dễ dàng chứng minh được nghiệm này là duy nhất. Như vậy trong trường hợp  $(a, m) = 1$ , phương trình luôn có duy nhất nghiệm với mọi  $b$ . Vì vậy ta chỉ cần xét trường hợp  $(a, m) = d > 1$ . Ta có định lý sau

**Định lý 1.2.2** Cho  $a, m$  là các số nguyên,  $m > 0$ ,  $d = (a, m)$ . Khi đó, điều kiện cần và đủ để phương trình

$$ax + b \equiv 0 \pmod{m}$$

có nghiệm là  $b : d$ .

Nếu điều kiện này được thoả mãn, phương trình sẽ có  $d$  nghiệm phân biệt và các nghiệm lập thành một cấp số cộng với công sai  $m/d$ .

### Chứng minh

Giả sử phương trình có nghiệm  $x_0$ . Khi đó tồn tại số nguyên  $k$  sao cho  $ax_0 + b = mk$ , hay  $b = mk - ax_0$ . Do cả  $a$  và  $m$  cùng chia hết cho  $d$  nên suy ra  $b$  cũng chia hết cho  $d$ .

Ngược lại, giả sử  $b : d$ , đặt  $a = da_1, b = db_1, m = dm_1$ . Do  $(a, m) = d$  nên  $(a_1, m_1) = 1$ . Ta có phương trình đã cho tương đương với phương trình sau

$$a_1x + b_1 \equiv 0 \pmod{m_1},$$

trong đó  $(a_1, m_1) = 1$ . Theo định lý 1.1.3 tồn tại duy nhất  $\bar{a}_1$  modulo  $m_1$  thoả mãn  $\bar{a}_1 a_1 \equiv 1 \pmod{m_1}$ . Sau khi nhân cả hai vế của phương trình trên với  $\bar{a}_1$  ta tìm được nghiệm

$$x \equiv -b_1 \bar{a}_1 \pmod{m_1}.$$

Do đó, nghiệm của phương trình đã cho là các số lập thành một cấp số cộng có dạng  $-b_1 \bar{a}_1 + km_1$ . Với  $k = 0, 1, \dots, d-1$  ta thu được  $d$  giá trị phân biệt modulo  $m$ . Vậy phương trình đã cho có đúng  $d$  nghiệm lập thành một cấp số cộng với công sai là  $m_1 = m/d$ .

## 2.3 Phương trình đồng dư modulo một số nguyên tố

Trong phần tiếp theo ta xét các phương trình đồng dư  $f(x) \equiv 0 \pmod{m}$  trong trường hợp  $m = p$  là một số nguyên tố. Định lý quan trọng nhất của phần này khẳng định rằng mọi phương trình đồng dư modulo một số nguyên tố sẽ có số nghiệm không vượt quá số bậc và chỉ ra điều kiện cần và đủ để một phương trình có số nghiệm bằng số bậc. Chẳng hạn, xét phương trình

$$25x^2 + 10x - 5 \equiv 0 \pmod{5}.$$

Để thấy phương trình này có 5 nghiệm modulo 5 và bậc cao nhất của đa thức  $f(x)$  là 2. Tuy nhiên, theo định nghĩa 1.2.2, phương trình đồng dư này không có bậc (vì tất cả các hệ số của đa thức  $f(x)$  đều chia hết cho 5 nên sự kiện này không mâu thuẫn với khẳng định của định lý 1.2.3).

### **Định lý 1.2.3.**

Với  $p$  là một số nguyên tố, phương trình đồng dư bậc  $n$

$$f(x) \equiv 0 \pmod{p}$$

có không quá  $n$  nghiệm.

### Chứng minh

Ta chứng minh bằng quy nạp. Với  $n = 0$ , phương trình có bậc 0 tức là  $f(x) \equiv a_0 : p$ . Khi đó phương trình  $f(x) \equiv 0 \pmod{p}$  vô nghiệm.

Giả sử khẳng định đúng với mọi phương trình đồng dư có bậc nhỏ hơn  $n$ . Ta chứng minh nó đúng với phương trình đồng dư có bậc  $n$ . Xét đa thức  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$  với  $a_n : p$ . Giả sử phương trình

$$f(x) \equiv 0 \pmod{p}$$

có  $n + 1$  nghiệm phân biệt modulo  $p$  là  $x_0, x_1, \dots, x_n$ . Khi đó đa thức

$$g(x) = f(x) - a_n(x - x_1)(x - x_2) \cdots (x - x_n)$$

có bậc bé hơn hoặc bằng  $n - 1$ .

Nếu phương trình  $g(x) \equiv 0 \pmod{p}$  có bậc thì bậc đó bé hơn  $n$ . Tuy nhiên phương trình này có  $n$  nghiệm phân biệt modulo  $p$  là  $x_1, x_2, \dots, x_n$ . Mâu thuẫn trái với giả thiết quy nạp.

Nếu phương trình  $g(x) \equiv 0 \pmod{p}$  không có bậc, tức là mọi hệ số của  $g(x)$  đều chia hết cho  $p$  hay  $g(x) \equiv 0 \pmod{p}$  với mọi số nguyên  $x$ , ta chọn  $x = x_0$ . Khi đó

$$g(x_0) = f(x_0) - a_n(x_0 - x_1)(x_0 - x_2) \cdots (x_0 - x_n) \equiv 0 \pmod{p}.$$

Mâu thuẫn vì  $f(x_0) \equiv 0 \pmod{p}$  còn  $a_n(x_0 - x_1)(x_0 - x_2) \cdots (x_0 - x_n) \not\equiv 0 \pmod{p}$  do  $x_0, x_1, \dots, x_n$  là phân biệt modulo  $p$ .

Vậy điều giả sử là sai, theo nguyên lý quy nạp ta có điều phải chứng minh.

Từ định lý nhỏ của Fermat ta thấy phương trình

$$x^p - x \equiv 0 \pmod{p}$$

luôn có  $p$  nghiệm với mọi số nguyên tố  $p$ . Do đó, với đa thức  $f(x) = (x^p - x)q(x) + r(x)$  trong đó  $\deg r < p$ , hai phương trình

$$f(x) \equiv 0 \pmod{p} \quad \text{và} \quad r(x) \equiv 0 \pmod{p}$$

có cùng một tập hợp nghiệm. Vì lý do đó, ta có định lý sau

### Định lý 1.2.4.

Cho phương trình đồng dư  $f(x) \equiv 0 \pmod{p}$  có bậc  $n \geq p$ . Khi đó chỉ có 2 khả năng sau

- 1, Mọi số nguyên đều là nghiệm của phương trình.
- 2, Tồn tại đa thức  $g(x)$  có  $\deg g < p$  với hệ số cao nhất bằng 1 sao cho phương trình

$$f(x) \equiv 0 \pmod{p} \quad \text{và} \quad g(x) \equiv 0 \pmod{p}.$$

có cùng tập hợp nghiệm.

### Chứng minh

Giả sử  $f(x) = (x^p - x)q(x) + r(x)$  trong đó  $\deg r < p$ .

Nếu  $r(x) \equiv 0$  hoặc mọi hệ số của  $r(x)$  đều chia hết cho  $p$  thì ta có mọi số nguyên đều là nghiệm của phương trình  $f(x) \equiv 0 \pmod{p}$ .

Nếu  $r(x)$  có ít nhất một hệ số không chia hết cho  $p$ , giả sử  $\deg r = n < p$ , gọi  $a_m$  là hệ số bậc cao nhất không chia hết cho  $p$ . Khi đó  $r(x)$  có dạng

$$r(x) = p(b_n x^n + b_{n-1} x^{n-1} + \cdots + b_{m+1} x^{m+1}) + a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0.$$

Dễ thấy

$$f(x) \equiv r(x) \equiv a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0 \pmod{p}, \quad \forall x \in Z.$$

Do  $(a_m, p) = 1$  nên theo định lý 1.1.3 tồn tại số nguyên  $\bar{a}_m$  sao cho  $\bar{a}_m a_m \equiv 1 \pmod{p}$ .

Đặt

$$\bar{a}_m a_m = pk + 1, g(x) = \bar{a}_m(a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0) - pkx^m$$

Dễ thấy hệ số cao nhất (bậc  $m < p$ ) của  $g(x)$  là  $\bar{a}_m a_m - pk = 1$ , và  $g(x) \equiv 0 \pmod{p}$  nếu và chỉ nếu  $f(x) \equiv 0 \pmod{p}$ . Định lý được chứng minh.

Định lý sau đây cho ta điều kiện cần và đủ để một phương trình đồng dư modulo một số nguyên tố có số nghiệm bằng với số bậc. Từ định lý 1.2.4, ta chỉ cần xét các đa thức  $f(x)$  có bậc bé hơn  $p$  và có hệ số cao nhất bằng 1.

**Định lý 1.2.5.**

Cho đa thức  $f(x)$  có bậc  $n$  với hệ số cao nhất  $a_n = 1$ . Khi đó phương trình  $f(x) \equiv 0 \pmod{p}$  có  $n$  nghiệm nếu và chỉ nếu ta có biểu diễn

$$x^p - x = f(x)q(x) + ps(x),$$

trong đó,  $q(x), s(x)$  là các đa thức có hệ số nguyên,  $\deg q = p-n$ ,  $\deg s < n$  và  $q(x)$  có hệ số cao nhất bằng 1.

**Chứng minh**

Giả sử phương trình  $f(x) \equiv 0 \pmod{p}$  có  $n$  nghiệm, khi đó  $n \leq p$ . Chia  $x^p - x$  cho  $f(x)$  được thương là  $q(x)$  và dư là  $r(x)$ . Ta có

$$x^p - x = f(x)q(x) + r(x), \quad \deg r < n.$$

Do phương trình  $x^p - x \equiv 0 \pmod{p}$  có  $p$  nghiệm,  $f(x) \equiv 0 \pmod{p}$  có  $n$  nghiệm, nên phương trình  $r(x) \equiv 0 \pmod{p}$  cũng có  $n$  nghiệm. Vì  $\deg r < n$  nên nếu phương trình  $r(x) \equiv 0 \pmod{p}$  có bậc thì bậc bé hơn  $n$  và có  $n$  nghiệm, tức là số nghiệm lớn hơn bậc, vô lý. Vậy phương trình  $r(x) \equiv 0 \pmod{p}$  không có bậc, tức là  $r(x)$  có dạng  $r(x) = ps(x)$ . Do đó ta có,

$$x^p - x = f(x)q(x) + ps(x),$$

Ngược lại, nếu  $f(x)$  có biểu diễn như trên thì

$$f(x)q(x) = (x^p - x) - ps(x),$$

tức là phương trình  $f(x)q(x) \equiv 0 \pmod{p}$  có  $p$  nghiệm. Gọi số nghiệm của các phương trình  $f(x) \equiv 0$ ,  $g(x) \equiv 0$ ,  $f(x)g(x) \equiv 0 \pmod{p}$  lần lượt là  $n_f, n_g, n_{fg}$ . Ta có  $n_{fg} \leq n_f + n_g$ . Do  $\deg f = n$ ,  $\deg g = p - n$  nên  $n_f \leq n, n_g \leq p - n$ , do đó

$$n_{fg} \leq n_f + n_g \leq n + (p - n) = p.$$

Vì phương trình  $f(x)q(x) \equiv 0 \pmod{p}$  có  $p$  nghiệm nên  $n_{fg} = p$ , suy ra phương  $n_f = n, n_g = p - n$ , tức là trình  $f(x) \equiv 0 \pmod{p}$  phải có đủ  $n$  nghiệm. Định lý được chứng minh.

Chú ý rằng trong định lý trên, giả thiết  $f(x)$  có hệ số cao nhất bằng 1 là cần thiết, vì với giả thiết ấy ta mới có thể thực hiện phép chia  $x^p - x$

cho  $f(x)$ . Tuy nhiên theo định lý 1.2.4, giả thiết này không phải là một hạn chế lớn.

Bằng cách tương tự như chứng minh định lý trên, ta có thể chứng minh được các khẳng định sau

- Nếu  $f(x)$  là một đa thức có hệ số nguyên, hệ số cao nhất bằng 1 và phương trình  $f(x) \equiv 0 \pmod{p}$  có số nghiệm bằng  $\deg f$  thì với mọi phân tích  $f(x) = g(x)h(x)$ , trong đó  $g(x), h(x)$  là các đa thức với hệ số nguyên, các phương trình  $g(x) \equiv 0, h(x) \equiv 0 \pmod{p}$  lần lượt có số nghiệm là  $\deg g, \deg h$ .

Tức là, nếu  $f(x)$  là một đa thức có hệ số nguyên, hệ số cao nhất bằng 1 và phương trình  $f(x) \equiv 0 \pmod{p}$  có số nghiệm bằng bậc của  $f$  thì với mọi đa thức  $g(x)$  là ước của  $f(x)$ , phương trình  $g(x) \equiv 0 \pmod{p}$  cũng có số nghiệm bằng bậc của  $g$ .

- Xét đa thức  $f(x) = x^{p-1} - 1$  có bậc  $p-1$  với các hệ số nguyên và hệ số cao nhất bằng 1. Theo định lý Fermat, phương trình  $x^{p-1} - 1 \equiv 0 \pmod{p}$  có  $p-1$  nghiệm. Với mọi ước số  $d$  của  $p-1$ , ta có

$$x^{p-1} - 1 = (x^d - 1)h(x)$$

với  $h(x)$  là đa thức có hệ số nguyên. Do đó, từ nhận xét trên, nếu  $d|(p-1)$  thì phương trình

$$x^d - 1 \equiv 0 \pmod{p}$$

luôn có  $d$  nghiệm.

**Ví dụ 1.2.1.** Có thể tìm được số tự nhiên  $n$  để  $n^2 + n + 1$  chia hết cho 1995 hay không?

### Giải

Nếu  $n = 5k$  ta có  $n^2 + n + 1 = 5k(5k+1) + 1 \equiv 1 \pmod{5}$

$n = 5k + 1$  ta có  $n^2 + n + 1 = (5k+1)(5k+2) + 3 \equiv 3 \pmod{5}$

$n = 5k + 2$  ta có  $n(n+1) + 1 = (5k+2)(5k+3) + 1 \equiv 2 \pmod{5}$

$n = 5k + 3$  ta có  $n(n+1) + 1 = (5k+3)(5k+4) + 1 \equiv 3(mod5)$

$n = 5k + 4$  ta có  $n(n+1) + 1 = (5k+4)(5k+5) + 1 \equiv 1(mod5)$ .

Vậy  $n^2 + n + 1$  không chia hết cho 5 nên không chia hết cho 1955.

**Ví dụ 1.2.2.** Chứng minh rằng  $5^{3^n} + 7$  chia hết cho 12 với mọi số tự nhiên  $n$ .

### Giải

Ta có

$$5^k + 7 = (4+1)^k + 7 \equiv 0(mod4)$$

$$5^k + 7 = (6-1)^k + 7 \equiv 0(mod3)$$

với  $k$  lẻ.

Vì  $3^n$  lẻ suy ra  $5^{3^n} + 7$  chia hết cho 12 (đpcm).

**Ví dụ 1.2.3.** Tìm tất cả các số nguyên  $n$  sao cho  $n2^n + 1$  chia hết cho 3.

### Giải

- Xét  $n = 6k$  ta có

$$6k(3-1)^{6k} + 1 \equiv 1(mod3)$$

- Xét  $n = 6k + 1$  ta có

$$(6k+1)(3-1)^{6k+1} + 1 \equiv -6k - 1 + 1(mod3) \equiv 0(mod3)$$

- Xét  $n = 6k + 2$  ta có

$$(6k+2)(3-1)^{6k+2} + 1 \equiv 6k + 2 + 1(mod3) \equiv 0(mod3)$$

- Xét  $n = 6k + 3$  ta có

$$(6k+3)(3-1)^{6k+3} + 1 \equiv -6k - 3 + 1(mod3) \equiv 1(mod3)$$

- Xét  $n = 6k + 4$  ta có

$$n2^n + 1 = (6k+4)(3-1)^{6k+4} + 1 \equiv 6k+4+1 \pmod{3} \equiv 2 \pmod{3}$$

- Xét  $n = 6k + 5$  ta có

$$n2^n + 1 = (6k+5)(3-1)^{6k+5} + 1 \equiv -6k-5+1 \pmod{3} \equiv 2 \pmod{3}.$$

**Đáp số:** Để  $n2^n + 1$  chia hết cho 3 thì các số tự nhiên n có dạng  $n = 6k + 1$ ,  $n = 6k + 2$ .

**Ví dụ 1.2.4.** Xét những số tự nhiên  $m, n, k$  thoả mãn  $m^n : n^m$ ,  $n^k : k^n$ .  
Chứng minh rằng  $m^k : k^m$ .

### Giải

Từ giả thiết của bài toán suy ra

$$m^n = A_n^m, \quad n^k = Bk^n$$

Ta có

$$\begin{aligned} (m^k)^n &= (m^n)^k = (An^m)^k = A^k(n^m)^k \\ &= A^k(n^k)^m = A^k(Bk^n)^m \\ &= A^k B^m (k^m)^n \end{aligned}$$

Suy ra:  $(m^k)^n : (k^m)^n \Rightarrow m^k : k^m$  (đpcm).

**Ví dụ 1.2.5.** Với các số tự nhiên  $m, n$ , chứng minh rằng  $2^n - 1$  chia hết cho  $(2^m - 1)^2$  khi và chỉ khi  $n$  chia hết cho  $m(2^m - 1)$ .

### Giải

có

$$2^{kn} - 1 = (2^n - 1)(2^{n(k-1)} + \dots + 1)$$

ra  $2^{kn} - 1$  chia hết cho  $2^n - 1$ .

vậy

$$2^{kn+d} - 1 = 2^d(2^{kn} - 1) + 2^d - 1$$

Vậy  $2^n - 1$  chia hết cho  $2^m - 1$  khi và chỉ khi  $n$  chia hết cho  $m$ .

Với  $n = km$  ta có  $\frac{2^{km} - 1}{2^m - 1} = 2^{m(k-1)} + \dots + 2 + 1$ .

Suy ra

$$\frac{2^{km} - 1}{2^m - 1} \equiv k \pmod{2^n - 1}$$

Ta có  $k = \frac{n}{m}$  chia hết cho  $2^m - 1$  khi và chỉ khi  $n$  chia hết cho  $m(2^m - 1)$ .

**Ví dụ 1.2.6.** Chứng minh rằng nếu  $p$  là một số nguyên tố thì

$$C_p^k : p \quad \text{với mọi } k = 1, 2, \dots, p-1.$$

### Giải

Đặt

$$f(x) = \sum_{k=1}^{p-1} C_p^k x^k = (x+1)^p - (x^p + 1).$$

Theo định lý nhỏ của Fermat ta có

$$(x+1)^p \equiv x+1 \equiv x^p + 1 \pmod{p} \quad \text{với mọi số nguyên } x$$

nên phương trình

$$f(x) \equiv 0 \pmod{p}$$

có  $p$  nghiệm. Do  $\deg f = p-1$  nên  $f$  không có bậc modulo  $p$ , tức là mọi hệ số của  $f$  đều chia hết cho  $p$ . Từ đó ta có điều phải chứng minh.

**Ví dụ 1.2.7.** Chứng minh rằng nếu  $p$  là một số nguyên tố thì

$$C_{p-1}^k \equiv (-1)^k \pmod{p} \quad \text{với mọi } 1 \leq k \leq p-1.$$

### Giải

Xét đa thức

$$f(x) = (x+1)^{p-1} - \frac{x^p + 1}{x+1}.$$

Để thấy bậc của  $f$  modulo  $p$  không quá  $p-2$  hoặc không có bậc. Mặt khác, theo định lý nhỏ của Fermat, phương trình

$$f(x) \equiv 0 \pmod{p}$$

có  $p - 1$  nghiệm modulo  $p$  là  $0, 1, 2, \dots, p - 2$ . Từ đó suy ra mọi hệ số của  $f(x)$  đều chia hết cho  $p$ . Do đó,

$$C_{p-1}^k \equiv (-1)^k \pmod{p} \quad \text{với mọi } 1 \leq k \leq p - 1.$$

Điều phải chứng minh.

**Ví dụ 1.2.8 (Định lý Wolstenholme).** Cho  $p$  là một số nguyên tố, gọi  $\sigma_1, \sigma_2, \dots, \sigma_{p-1}$  là các số nguyên thoả mãn

$$(x - 1)(x - 2) \cdots (x - p + 1) = x^{p-1} - \sigma_1 x^{p-2} + \sigma_2 x^{p-3} - \cdots + \sigma_{p-1}.$$

Chứng minh rằng nếu  $p \geq 5$  thì

a,  $\sigma_{p-1} \equiv -1 \pmod{p}$ .

b,  $\sigma_{p-2} \equiv 0 \pmod{p^2}$ .

c,  $\sigma_{p-2} \equiv p\sigma_{p-3} \pmod{p^3}$ .

### Giải

a, Đặt

$$f(x) = (x - 1)(x - 2) \cdots (x - p + 1).$$

Xét đa thức

$$g(x) = x^p - x - xf(x).$$

Hiển nhiên nếu  $g$  có bậc modulo  $p$  thì bậc không vượt quá  $p - 1$ . Mặt khác, theo định lý nhỏ của Fermat, phương trình

$$g(x) \equiv 0 \pmod{p}$$

có đủ  $p$  nghiệm modulo  $p$ . Do đó mọi hệ số của  $g$  đều chia hết cho  $p$ . Xét hệ số của  $x^1$  ta có  $\sigma_{p-1} \equiv -1 \pmod{p}$ . Xét hệ số của  $x^i$ ,  $p - 1 \geq i \geq 2$  ta có  $\sigma_{p-i} : p$  với mọi  $i = 2, 3, \dots, p - 1$ :

b, Ta có  $f(p) = (p - 1)! = \sigma_{p-1}$ , mặt khác

$$f(p) = p^{p-1} - \sigma_1 p^{p-2} + \sigma_2 p^{p-3} - \cdots + \sigma_{p-3} p^2 - \sigma_{p-2} p + \sigma_{p-1}.$$

Trừ cả hai vế cho  $(p - 1)!$  sau đó chia cả hai vế cho  $p$  ta được

$$p^{p-2} - \sigma_1 p^{p-3} + \sigma_2 p^{p-4} - \cdots + \sigma_{p-3} p - \sigma_{p-2} = 0$$

Từ phần trên ta có  $\sigma_i \vdots p$  với mọi  $i = 1, 2, \dots, p - 2$ . Do đó,

$$\sigma_{p-2} = p^{p-2} - \sigma_1 p^{p-3} + \sigma_2 p^{p-4} - \dots + \sigma_{p-3} p \vdots p^2,$$

điều phải chứng minh.

c, Hiển nhiên, do  $\sigma_i \vdots p$  với mọi  $i = 1, 2, \dots, p - 2$  nên

$$\sigma_{p-2} - \sigma_{p-3} p = p^{p-2} - \sigma_1 p^{p-3} + \sigma_2 p^{p-4} - \dots + \sigma_{p-4} p^2 \vdots p^3,$$

điều phải chứng minh.

## BÀI TẬP

**Bài 1 (Định lý Lucas).** Cho  $p$  là một số nguyên tố,  $n, k$  là các số nguyên không âm có biểu diễn trong cơ sở  $p$  như sau

$$n = n_0 + n_1p + \cdots + n_tp^t, \quad k = k_0 + k_1p + \cdots + k_tp^t.$$

Chứng minh rằng

$$C_n^k \equiv C_{n_0}^{k_0} C_{n_1}^{k_1} \cdots C_{n_t}^{k_t} \pmod{p}.$$

**Bài 2 (Nordic 1998).** Cho  $n$  là một số nguyên dương. Chứng minh rằng số các số  $k \in \{0, 1, 2, \dots, n\}$  thoả mãn  $C_n^k$  lẻ là một luỹ thừa của 2.

**Bài 3.** Chứng minh rằng với mọi số nguyên tố  $p$  tồn tại một số nguyên dương  $n > 1$  sao cho

$$C_n^i : p \quad \text{với mọi } i = 1, 2, \dots, n-1.$$

Hơn nữa,  $n$  thoả mãn điều kiện trên khi và chỉ khi tồn tại một số nguyên dương  $m$  sao cho  $n = p^m$ .

**Bài 4.** Cho  $p$  là một số nguyên tố,  $G = \{r_1, r_2, \dots, r_k\}$  thoả mãn tính chất sau

$$0 < r_i < p, \quad r_i r_j \in G \quad \text{với mọi } i, j = 1, 2, \dots, k.$$

Đặt  $a = \prod_{i=1}^k r_i, b = \prod_{0 < r_j < p/2} r_j$ . Chứng minh rằng

a,  $a \equiv (-1)^{k+1} \pmod{p}$ .

b, Nếu  $k = 2h$ ,  $h$  lẻ thì  $b \equiv \pm 1 \pmod{p}$ .

c, Nếu  $1 \leq r_i \leq (p-1)/2$  với mọi  $1 \leq i \leq k$  thì  $a \equiv 1 \pmod{p}$ .

d, Nếu  $k = 2h$ ,  $h \geq 2$  thì tử số của phân số

$$\frac{1}{r_1} + \frac{1}{r_2} + \cdots + \frac{1}{r_k}$$

chia hết cho  $p^2$ .

**Bài 5.** Cho  $p$  là một số nguyên tố,  $k$  là một số tự nhiên thoả mãn  $2k \leq p - 1$ . Chứng minh rằng

a, Tử số của phân số

$$1 + \frac{1}{2^{2k-1}} + \cdots + \frac{1}{(p-1)^{2k-1}}$$

chia hết cho  $p^2$ .

b, Tử số của phân số

$$1 + \frac{1}{2^{2k}} + \cdots + \frac{1}{(p-1)^{2k}}$$

chia hết cho  $p$ .

## LỜI GIẢI

### Bài 1 (Định lý Lucas).

Ta có

$$(a+b)^{p^r} \equiv a^{p^r} + b^{p^r} \pmod{p} \text{ với mọi } r \geq 0.$$

Do đó

$$\begin{aligned} (1+x)^n &\equiv (1+x)^{n_0+n_1p+\cdots+n_tp^t} \\ &\equiv (1+x)^{n_0}(1+x)^{n_1p}\cdots(1+x)^{n_tp^t} \\ &\equiv (1+x)^{n_0}(1+x^p)^{n_1}\cdots(1+x^{p^t})^{n_t} \\ &\equiv \left(\sum_{i_0=0}^{n_0} C_{n_0}^{i_0} x^{i_0}\right) \left(\sum_{i_1=0}^{n_1} C_{n_1}^{i_1} x^{i_1p}\right) \cdots \left(\sum_{i_t=0}^{n_t} C_{n_t}^{i_t} x^{i_tp^t}\right) \pmod{p}. \end{aligned}$$

Vì  $k$  có biểu diễn duy nhất trong cơ sở  $p$ ,  $k = k_0 + k_1p + \cdots + k_tp^t$  nên hệ số của  $x^k$  trong biểu thức cuối cùng là

$$C_{n_0}^{k_0} C_{n_1}^{k_1} \cdots C_{n_t}^{k_t}.$$

Từ đó ta có

$$C_n^k \equiv C_{n_0}^{k_0} C_{n_1}^{k_1} \cdots C_{n_t}^{k_t} \pmod{p}.$$

Điều phải chứng minh.

### Bài 2 (Nordic 1998).

Xét hai biểu diễn nhị phân của  $n$  và  $k$ ,

$$\begin{aligned} n &= 2^0 n_0 + 2^1 n_1 + \cdots + 2^m n_m, \quad n_i \in \{0, 1\}, \\ k &= 2^0 k_0 + 2^1 k_1 + \cdots + 2^m k_m, \quad k_i \in \{0, 1\}. \end{aligned}$$

Theo định lý Lucas,

$$C_n^k \equiv C_{n_0}^{k_0} C_{n_1}^{k_1} \cdots C_{n_m}^{k_m} \pmod{2}.$$

Do đó,  $C_n^k$  lẻ nếu và chỉ nếu  $k_i \leq n_i$  với mọi  $i$ . Đặt

$$L = \{0 \leq i \leq m | n_i = 1\}, \quad |L| = l.$$

Khi đó, nếu  $i \in L$  thì  $k_i$  có thể nhận 2 giá trị là 0 hoặc 1, nếu  $i \notin L$  thì  $k_i$  chỉ có duy nhất 1 cách chọn là  $k_i = 0$ .

Vậy số các số  $k$  thoả mãn  $C_n^k$  lẻ là  $2^l$ . Điều phải chứng minh.

### Bài 3.

Giả sử trong biểu diễn cơ sở  $p$  ta có

$$\begin{aligned} n &= n_0 + n_1 p + \cdots + n_m p^m, \quad 0 \leq n_0, n_1, \dots, n_m \leq p-1, \quad n_m \neq 0, \\ i &= i_0 + i_1 p + \cdots + i_m p^m, \quad 0 \leq i_0, i_1, \dots, i_m \leq p-1 \text{ (có thể } i_m = 0). \end{aligned}$$

Khi đó theo định lý Lucas,

$$C_n^i \equiv \prod_{j=0}^m C_{n_j}^{i_j} \pmod{p}.$$

Nếu  $n = p^m$  thì  $n_0 = n_1 = \cdots = n_{m-1} = 0$ . Vì  $1 \leq i \leq n-1$  nên  $i_m = 0$  và tồn tại một chỉ số  $j$  sao cho  $i_j \neq 0$ . Khi đó  $C_{n_j}^{i_j} = 0$  nên  $C_n^i \equiv 0 \pmod{p}$ .

Nếu  $n \neq p^m$  với mọi  $m$ . Giả sử  $n_m > 1$ , đặt  $i = p^m < n$  ta có

$$C_n^i \equiv n_m \cdot 1 \cdot 1 \cdots 1 \equiv n_m \not\equiv 0 \pmod{p}.$$

Do đó ta có điều phải chứng minh.

### 3 Định lý thặng dư Trung Hoa

Tương tự với hệ phương trình bậc nhất, ta có thể đặt bài toán cho phương trình đồng dư như sau:

Cho  $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n, m_1, m_2, \dots, m_n$  là các số nguyên,  $m_i > 0$  với mọi  $i = 1, 2, \dots, n$ . Khi nào hệ phương trình sau có nghiệm

$$\begin{aligned} a_1x + b_1 &\equiv 0 \pmod{m_1}, \\ a_2x + b_2 &\equiv 0 \pmod{m_2}, \\ &\dots \\ a_nx + b_n &\equiv 0 \pmod{m_n}. \end{aligned}$$

Trước tiên, ta xét trường hợp  $m_1, m_2, \dots, m_n$  đôi một nguyên tố cùng nhau. Để hệ phương trình này có nghiệm, trước hết mỗi phương trình đồng dư tuyến tính  $a_i x + b_i \equiv 0 \pmod{m_i}$  trong hệ phải có nghiệm. Vì vậy ta có thể đưa hệ phương trình trên về dạng sau đây

$$\begin{aligned} x &\equiv r_1 \pmod{m_1}, \\ x &\equiv r_2 \pmod{m_2}, \\ &\dots \\ x &\equiv r_n \pmod{m_n}. \end{aligned}$$

trong đó  $x \equiv r_i \pmod{m_i}$  là nghiệm của phương trình  $a_i x + b_i \equiv 0 \pmod{m_i}$ . Định lý sau đây là định lý quan trọng nhất trong tiết này, lần đầu tiên được biết đến tại Trung Hoa vào thế kỉ đầu tiên sau công nguyên.

#### Định lý 1.3.1

Cho  $m_1, m_2, \dots, m_n$  là các số nguyên dương đôi một nguyên tố cùng nhau,  $r_1, r_2, \dots, r_n$  là các số nguyên bất kì. Khi đó hệ phương trình đồng dư trên luôn có nghiệm chung.

Nếu  $x_0$  và  $x_1$  là hai nghiệm thoả mãn hệ phương trình trên thì  $x_0 \equiv x_1 \pmod{m}$  với  $m = m_1 m_2 \cdots m_n$ . Tức là hệ phương trình đồng dư trên luôn có nghiệm duy nhất modulo  $m$ .

#### Chứng minh

Đặt  $s_i = m/m_i$ , do giả thiết  $m_1, m_2, \dots, m_n$  là các số nguyên dương đôi một nguyên tố cùng nhau nên ta có  $(s_i, m_i) = 1$  với mọi  $i = 1, 2, \dots, n$ .

Do đó với mỗi  $i$  tồn tại một số nguyên  $\bar{s}_i$  thoả mãn  $\bar{s}_i s_i \equiv 1 \pmod{m_i}$ .  
Đặt

$$x_0 = s_1 \bar{s}_1 r_1 + s_2 \bar{s}_2 r_2 + \cdots + s_n \bar{s}_n r_n.$$

Vì  $s_j$  chia hết cho  $m_i$  nếu  $j \neq i$  nên  $x_0 \equiv s_i \bar{s}_i r_i \equiv r_i \pmod{m_i}$  với mọi  $1 \leq i \leq n$ . Tức là hệ phương trình đồng dư đã cho có nghiệm chung.

Giả sử  $x_1$  là một nghiệm khác của hệ phương trình đồng dư trên. Khi đó ta có  $x_1 - x_0 \equiv 0 \pmod{m_i}$  hay  $x_1 - x_0 \mid m_i$  với mọi  $i = 1, 2, \dots, n$ . Do  $m_1, m_2, \dots, m_n$  là các số đôi một nguyên tố cùng nhau nên từ đó suy ra  $x_1 - x_0 \mid m_1 m_2 \cdots m_n$ . Định lý được chứng minh.

Trong trường hợp  $m_1, m_2, \dots, m_n$  là các số nguyên dương tùy ý, điều kiện để hệ phương trình đồng dư có nghiệm là bất cứ hai phương trình đồng dư tuyến tính nào trong hệ cũng có nghiệm chung. Ta có định lý sau

### Định lý 1.3.2.

Cho  $m_1, m_2, \dots, m_n$  là các số nguyên dương,  $r_1, r_2, \dots, r_n$  là các số nguyên bất kì. Khi đó điều kiện cần và đủ để hệ phương trình đồng dư trên có nghiệm chung là

$$r_i \equiv r_j \pmod{(m_i, m_j)}, \quad \forall 1 \leq i < j \leq n.$$

Nếu  $x_0$  và  $x_1$  là hai nghiệm thoả mãn hệ phương trình trên thì  $x_0 \equiv x_1 \pmod{m}$  với  $m = [m_1, m_2, \dots, m_n]$ . Tức là hệ phương trình đồng dư trên có nghiệm thì nghiệm đó là duy nhất modulo  $m$ .

### Chứng minh

Trước hết, giả sử hệ phương trình đã cho có nghiệm  $x_0$ . Đặt  $(m_i, m_j) = d$ , ta có

$$x_0 - r_i \equiv 0 \pmod{m_i}, \quad x_0 - r_j \equiv 0 \pmod{m_j}$$

nên  $x_0 - r_i \equiv x_0 - r_j \equiv 0 \pmod{d}$  hay  $r_i \equiv r_j \pmod{(m_i, m_j)}$ . Do  $i, j$  được chọn tùy ý nên

$$r_i \equiv r_j \pmod{(m_i, m_j)} \quad \text{với mọi } 1 \leq i < j \leq n.$$

là điều kiện cần để hệ phương trình có nghiệm.

Ngược lại, ta sẽ chứng minh bằng quy nạp theo  $n$  rằng nếu điều kiện trên được thoả mãn thì hệ phương trình luôn có duy nhất nghiệm modulo

$m$  với  $m = [m_1, m_2, \dots, m_n]$ .

Với trường hợp  $n = 2$ , đặt

$$(m_1, m_2) = d, \quad m_1 = dd_1, \quad m_2 = dd_2$$

suy ra  $(d_1, d_2) = 1$  và  $r_i \equiv r_j \pmod{d}$ . Đặt

$$r_1 = r + k_1 d, \quad r_2 = r + k_2 d.$$

Ta có

$$\begin{aligned} \begin{cases} x \equiv r_1 \pmod{m_1}, \\ x \equiv r_2 \pmod{m_2} \end{cases} &\Leftrightarrow \begin{cases} (x - r) - k_1 d \mid dd_1, \\ (x - r) - k_2 d \mid dd_2 \end{cases} \\ &\Leftrightarrow \begin{cases} (x - r)/d \equiv k_1 \pmod{d_1}, \\ (x - r)/d \equiv k_2 \pmod{d_2} \end{cases} \end{aligned}$$

Do  $(d_1, d_2) = 1$  nên theo định lý Thăng dư Trung Hoa tồn tại một số nguyên dương  $\bar{x}$  sao cho

$$\bar{x} \equiv k_1 \pmod{d_1}, \quad \bar{x} \equiv k_2 \pmod{d_2}.$$

Từ chứng minh trên,  $x$  là nghiệm của hệ

$$\begin{cases} x \equiv k_1 \pmod{d_1}, \\ x \equiv k_2 \pmod{d_2} \end{cases}$$

khi và chỉ khi  $(x - r)/d \equiv \bar{x} \pmod{d_1 d_2}$  hay  $x \equiv \bar{x}d + r \pmod{dd_1 d_2}$

Do  $m = [m_1, m_2] = dd_1 d_2$  nên từ định lý Thăng dư Trung Hoa suy ra hệ phương trình có nghiệm duy nhất modulo  $m$ .

Giả sử định lý đúng đến  $n - 1$ . Ta sẽ chứng minh định lý đúng đến  $n$ . Đặt

$$m'_1 = [m_1, m_2, \dots, m_{n-1}], \quad m'_2 = m_n, \quad r'_2 = r_n.$$

Vì

$$r_i \equiv r_j \pmod{(m_i, m_j)} \quad \text{với mọi } 1 \leq i < j \leq n$$

nên theo giả thiết quy nạp, hệ phương trình

$$\begin{cases} x \equiv r_i \pmod{m_i}, \\ i = 1, 2, \dots, n-1 \end{cases}$$

có duy nhất nghiệm  $x \equiv r'_1 \pmod{m'_1}$ . Mặt khác từ  $r_i \equiv r_j \pmod{(m_i, m_j)}$  với mọi  $1 \leq i < j \leq n$  suy ra  $r'_1 \equiv r'_2 \pmod{(m'_1, m'_2)}$ . Theo chứng minh trên cho trường hợp  $n = 2$  ta có hệ phương trình

$$\begin{cases} x \equiv r'_1 \pmod{m'_1}, \\ x \equiv r'_2 \pmod{m'_2} \end{cases}$$

có nghiệm duy nhất modulo  $m = [m'_1, m'_2] = [m_1, m_2, \dots, m_n]$ . Vậy định lý đúng với  $n$ . Theo nguyên lý quy nạp ta có điều phải chứng minh.

### Định lý 1.3.3.

Cho  $m_1, m_2$  là hai số nguyên dương nguyên tố cùng nhau. Khi đó  $\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$ .

Nếu  $m$  có phân tích chính tắc thành tích các thừa số nguyên tố  $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$  thì

$$\phi(m) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1} (p_1 - 1)(p_2 - 1) \cdots (p_k - 1).$$

### Chứng minh

Đặt  $m = m_1 m_2$ . Giả sử  $\{a_1, a_2, \dots, a_k\}$  là một hệ thặng dư thu gọn modulo  $m_1$ ,  $\{b_1, b_2, \dots, b_l\}$  là một hệ thặng dư thu gọn modulo  $m_2$ .

Gọi  $a$  là một số nguyên dương bất kỳ sao cho  $(a, m) = 1$ . Khi đó  $(a, m_1) = (a, m_2) = 1$  nên tồn tại duy nhất  $a_i, b_j$  sao cho  $a \equiv a_i \pmod{m_1}$  và  $a \equiv b_j \pmod{m_2}$ . Như vậy, mỗi lớp thặng dư thu gọn modulo  $m$  đều ứng với một cặp  $\{a_i, b_j\}$ .

Ngược lại với một bộ  $\{a_i, b_j\}$  bất kỳ, theo định lý Thặng dư Trung Hoa, tồn tại duy nhất một lớp thặng dư  $a$  thoả mãn  $a \equiv a_i \pmod{m_1}$  và  $a \equiv b_j \pmod{m_2}$ . Do  $(a_i, m_1) = (b_j, m_2) = 1$  nên  $(a, m_1) = (a, m_2) = 1$  và  $(a, m) = 1$ . Do đó, mỗi cặp  $\{a_i, b_j\}$  đều ứng với một lớp thặng dư thu gọn modulo  $m$ . Từ đó suy ra có một tương ứng một-một giữa các cặp  $\{a_i, b_j\}$  với các lớp thặng dư thu gọn modulo  $m$ , tức là  $\phi(m) = kl = \phi(m_1)\phi(m_2)$ .

Hiển nhiên nếu  $p$  là một số nguyên tố thì  $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ . Từ

đó ta có

$$\phi(m) = \prod_{i=1}^k \phi(p_i^{\alpha_i}) = \prod_{i=1}^k p_i^{\alpha_i - 1}(p_i - 1).$$

Điều phải chứng minh.

**Ví dụ 1.3.1.** Cho  $p$  là một số nguyên tố,  $\alpha_1 < \alpha_2 < \dots < \alpha_n$  là một dãy các số nguyên dương. Chứng minh rằng hệ phương trình đồng dư

$$\begin{cases} x \equiv r_i \pmod{p^{\alpha_i}} \\ i = 1, 2, \dots, n. \end{cases}$$

có nghiệm khi và chỉ khi  $r_i \equiv r_k \pmod{p^{\alpha_i}}$  với mọi  $i = 1, 2, \dots, k$ .

### Giải

Giả sử  $m$  là một số nguyên dương thoả mãn  $x \equiv r_i \pmod{p^{\alpha_i}}$  với mọi  $i = 1, 2, \dots, n$ . Khi đó ta có  $m \equiv r_k \pmod{p^{\alpha_k}}$ . Vì  $\alpha_1 < \alpha_2 < \dots < \alpha_n$  nên  $m \equiv r_k \pmod{p^{\alpha_i}}$  với mọi  $i = 1, 2, \dots, k$ , suy ra

$$r_i \equiv m \equiv r_k \pmod{p^{\alpha_i}} \text{ với mọi } i = 1, 2, \dots, k.$$

Ngược lại, giả sử  $r_i \equiv r_k \pmod{p^{\alpha_i}}$  với mọi  $i = 1, 2, \dots, k$ . Đặt  $m = r_n$ , ta có

$$m \equiv r_n \equiv r_i \pmod{p^{\alpha_i}} \text{ với mọi } i = 1, 2, \dots, n$$

suy ra  $m$  là một nghiệm của hệ phương trình đã cho, tức là hệ phương trình đã cho có nghiệm. Điều phải chứng minh.

**Ví dụ 1.3.2.** Cho  $m_1, m_2, \dots, m_n$  là các số nguyên dương,  $r_1, r_2, \dots, r_n$  là các số nguyên bất kì. Khi đó điều kiện cần và đủ để hệ phương trình đồng dư trên có nghiệm chung là

$$r_i \equiv r_j \pmod{(m_i, m_j)}, \quad \text{với mọi } 1 \leq i < j \leq n.$$

Nếu  $x_0$  và  $x_1$  là hai nghiệm thoả mãn hệ phương trình trên thì  $x_0 \equiv x_1 \pmod{m}$  với  $m = [m_1, m_2, \dots, m_n]$ . Tức là hệ phương trình đồng dư trên có nghiệm thì nghiệm đó là duy nhất modulo  $m$ .

**Giải**

Trước hết, giả sử hệ phương trình đã cho có nghiệm  $x_0$ . Đặt  $(m_i, m_j) = d$ , ta có

$$x_0 - r_i \equiv 0 \pmod{m_i}, \quad x_0 - r_j \equiv 0 \pmod{m_j}$$

nên  $x_0 - r_i \equiv x_0 - r_j \equiv 0 \pmod{d}$  hay  $r_i \equiv r_j \pmod{(m_i, m_j)}$ . Do  $i, j$  được chọn tùy ý nên

$$r_i \equiv r_j \pmod{(m_i, m_j)} \quad \text{với mọi } 1 \leq i < j \leq n.$$

là điều kiện cần để hệ phương trình có nghiệm.

Ngược lại, ta sẽ chứng minh bằng quy nạp theo  $n$  rằng nếu điều kiện trên được thoả mãn thì hệ phương trình luôn có duy nhất nghiệm modulo  $m$  với  $m = [m_1, m_2, \dots, m_n]$ .

Với trường hợp  $n = 2$ , đặt

$$(m_1, m_2) = d, \quad m_1 = dd_1, \quad m_2 = dd_2$$

suy ra  $(d_1, d_2) = 1$  và  $r_i \equiv r_j \equiv r \pmod{d}$ . Đặt

$$r_1 = r + k_1d, \quad r_2 = r + k_2d.$$

Ta có

$$\begin{aligned} \begin{cases} x \equiv r_1 \pmod{m_1}, \\ x \equiv r_2 \pmod{m_2} \end{cases} &\Leftrightarrow \begin{cases} (x - r) - k_1d \vdots dd_1, \\ (x - r) - k_2d \vdots dd_2 \end{cases} \\ &\Leftrightarrow \begin{cases} (x - r)/d \equiv k_1 \pmod{d_1}, \\ (x - r)/d \equiv k_2 \pmod{d_2} \end{cases} \end{aligned}$$

Do  $(d_1, d_2) = 1$  nên theo định lý thăng dư Trung Hoa tồn tại một số nguyên dương  $\bar{x}$  sao cho

$$\bar{x} \equiv k_1 \pmod{d_1}, \quad \bar{x} \equiv d_2 \pmod{m_2}.$$

Từ chứng minh trên,  $x$  là nghiệm của hệ

$$\begin{cases} x \equiv k_1 \pmod{d_1}, \\ x \equiv k_2 \pmod{d_2} \end{cases}$$

khi và chỉ khi  $(x - r)/d \equiv \bar{x} \pmod{d_1 d_2}$  hay  $x \equiv \bar{x}d + r \pmod{d d_1 d_2}$ . Do  $m = [m_1, m_2] = d d_1 d_2$  nên từ định lý Thăng dư Trung Hoa suy ra hệ phương trình có nghiệm duy nhất modulo  $m$ .

Giả sử bài toán đúng đến  $n - 1$ . Ta sẽ chứng minh bài toán đúng đến  $n$ . Đặt

$$m'_1 = [m_1, m_2, \dots, m_{n-1}], \quad m'_2 = m_n, \quad r'_2 = r_n.$$

Vì

$$r_i \equiv r_j \pmod{(m_i, m_j)} \quad \text{với mọi } 1 \leq i < j \leq n$$

nên theo giả thiết quy nạp, hệ phương trình

$$\begin{cases} x \equiv r_i \pmod{m_i}, \\ i = 1, 2, \dots, n-1 \end{cases}$$

có duy nhất nghiệm  $x \equiv r'_1 \pmod{m'_1}$ . Mặt khác từ  $r_i \equiv r_j \pmod{(m_i, m_j)}$  với mọi  $1 \leq i < j \leq n$  suy ra  $r'_1 \equiv r'_2 \pmod{(m'_1, m'_2)}$ . Theo chứng minh trên cho trường hợp  $n = 2$  ta có hệ phương trình

$$\begin{cases} x \equiv r'_1 \pmod{m'_1}, \\ x \equiv r'_2 \pmod{m'_2} \end{cases}$$

có nghiệm duy nhất modulo  $m = [m'_1, m'_2] = [m_1, m_2, \dots, m_n]$ . Vậy bài toán đúng với  $n$ . Theo nguyên lý quy nạp ta có điều phải chứng minh.

**Ví dụ 1.3.3.** Với mỗi số nguyên dương  $n$  kí hiệu  $f(n)$  là tổng của các số nguyên dương bé hơn  $n$  và nguyên tố cùng nhau với  $n$ .

- a, Chứng minh rằng  $f(n) = n\phi(n)/2$ .
- b, Chứng minh rằng nếu  $f(m) = f(n)$  thì  $m = n$ .

### Giải

a, Xét các cặp  $\{d, n - d\}$ , dễ thấy nếu  $(d, n) = 1$  thì  $(n - d, n) = 1$  và ngược lại. Chia tập tất cả các số nguyên dương bé hơn  $n$  và nguyên tố cùng nhau với  $n$  thành các cặp có dạng  $\{d, n - d\}$  ta có

$$f(n) = n\phi(n)/2.$$

b, Từ giả thiết và phần a, ta có  $m\phi(m) = n\phi(n)$ . Gọi  $p$  là ước số nguyên tố lớn nhất của  $m$ ,  $\alpha$  là số mũ của  $p$  trong phân tích  $m$  thành tích các thừa số nguyên tố,  $m = p^\alpha m_1$ . Ta có

$$m\phi(m) = p^{2\alpha-1}l\phi(l) = n\phi(n).$$

Từ đó suy ra  $p$  cũng là ước số nguyên tố lớn nhất của  $n$  và số mũ của  $p$  trong phân tích  $m$  thành tích các thừa số nguyên tố là  $\alpha$ . Đặt  $n = p^\alpha n_1$ , ta có  $m_1\phi(m_1) = n_1\phi(n_1)$ ,  $m_1 < m$  và  $n_1 < n$ . Lặp lại lập luận trên ta có  $m = n$ .

**Ví dụ 1.3.4.** Cho  $n$  là một số nguyên dương,  $d$  là một ước số của  $n$ ,  $0 < d < n$ . Chứng minh rằng

$$n - \phi(n) > d - \phi(d).$$

### Giải

Ta có  $n - \phi(n)$  là số các số nguyên dương không vượt quá  $n$  và không nguyên tố cùng nhau với  $n$ ,  $d - \phi(d)$  là số các số nguyên dương không vượt quá  $d$  và không nguyên tố cùng nhau với  $d$ . Do  $d$  là một ước số của  $n$  nên nếu một số không nguyên tố cùng nhau với  $d$  thì cũng không nguyên tố cùng nhau với  $n$ . Từ đó suy ra điều phải chứng minh.

**Ví dụ 1.3.5.** Chứng minh rằng với mọi số nguyên dương  $m$ ,

$$a^m \equiv a^{m-\phi(m)} \pmod{m} \quad \text{với mọi số nguyên } a.$$

### Giải

Giả sử  $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ . Ta có

- Nếu  $a : p_i$  thì từ  $m > m - \phi(m) > \alpha_i$  suy ra  $a^m \equiv a^{m-\phi(m)} \equiv 0 \pmod{p_i^{\alpha_i}}$ .
- Nếu  $(a, p_i) = 1$  thì từ  $\phi(m) : \phi(p_i^{\alpha_i})$  suy ra  $a^{\phi(m)} \equiv 1 \pmod{p_i^{\alpha_i}}$  và

$$a^m = a^{m-\phi(m)} \cdot a^{\phi(m)} \equiv a^{m-\phi(m)} \pmod{p_i^{\alpha_i}}.$$

Do đó,

$$a^m \equiv a^{m-\phi(m)} \pmod{p_i^{\alpha_i}}$$

với mọi  $i = 1, 2, \dots, k$ .

Vì các số  $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$  đôi một nguyên tố cùng nhau nên theo định lý Thăng dư Trung Hoa ta có

$$a^m \equiv a^{m-\phi(m)} \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}}.$$

Điều phải chứng minh.

**Ví dụ 1.3.6.** Cho  $m$  là một số nguyên dương. Tìm số nghiệm của phương trình

$$x^2 \equiv x \pmod{m}.$$

### Giải

Giả sử  $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ . Ta có  $x^2 \equiv x \pmod{m}$  khi và chỉ khi

$$x^2 \equiv x \pmod{p_i^{\alpha_i}} \quad \text{với mọi } i = 1, 2, \dots, k$$

hay

$$x(x-1) \equiv 0 \pmod{p_i^{\alpha_i}} \quad \text{với mọi } i = 1, 2, \dots, k.$$

Vì  $(x, x-1) = 1$  nên phương trình  $x(x-1) \equiv 0 \pmod{p_i^{\alpha_i}}$  có hai nghiệm modulo  $p_i^{\alpha_i}$  là  $x \equiv 0 \pmod{p_i^{\alpha_i}}$  hoặc  $x \equiv 1 \pmod{p_i^{\alpha_i}}$ .

Theo định lý Thăng dư Trung Hoa, với mỗi bộ  $r_1, r_2, \dots, r_k$ , hệ phương trình

$$\begin{cases} x \equiv r_i \pmod{p_i^{\alpha_i}} \\ i = 1, 2, \dots, k \end{cases}$$

luôn có một nghiệm duy nhất modulo  $m$ . Do mỗi phương trình  $x(x-1) \equiv 0 \pmod{p_i^{\alpha_i}}$  đều có hai nghiệm modulo  $p_i^{\alpha_i}$  nên phương trình đã cho có  $2^k$  nghiệm.

## BÀI TẬP

**Bài 1 (Nordic 1998).**

a, Tìm các số nguyên dương  $n$  sao cho tồn tại dãy  $\{x_1, x_2, \dots, x_n\} = \{1, 2, \dots, n\}$  thoả mãn

$$x_1 + x_2 + \dots + x_k \vdots k \quad \text{với mọi } k = 1, 2, \dots, n.$$

b, Tồn tại hay không một dãy vô hạn  $\{x_1, x_2, \dots\} = \{1, 2, \dots\}$  sao cho  $x_i \neq x_j$  với mọi  $i \neq j$  và

$$x_1 + x_2 + \dots + x_k \vdots k \quad \text{với mọi } k = 1, 2, \dots, n?$$

**Bài 2 (Czech-Slovak 1997).** Chứng minh rằng tồn tại một dãy tăng  $\{a_n\}_{n=1}^{\infty}$  các số tự nhiên sao cho với mọi  $k \geq 0$ , dãy  $\{k + a_n\}$  chỉ chứa hữu hạn các số nguyên tố.

**Bài 3 (Korea 1999).** Tìm tất cả các số nguyên dương  $n$  sao cho  $2^n - 1 \vdots 3$  và  $(2^n - 1)/3$  là ước số của một số nguyên có dạng  $4m^2 + 1$ .

**Bài 4 (Balkan 2000).** Cho  $A$  là một tập khác rỗng các số nguyên dương. Chứng minh rằng tồn tại một số nguyên dương  $m$  sao cho mọi phân tử của  $mA$  đều là luỹ thừa.

**Bài 5.** Cho  $n$  là một số nguyên dương, xét tập hợp

$$A_n = \{1 \leq a \leq n : (a, n) = (a+1, n) = 1\}.$$

Chứng minh rằng

$$|A_n| = n \prod_{p|n, p \text{ nguyên tố}} \left(1 - \frac{2}{p}\right).$$

**Bài 6.** Tìm tất cả các số nguyên dương  $n$  thoả mãn tính chất sau:

$$\text{Nếu } (x, n) = 1 \text{ thì } x^2 \equiv 1 \pmod{n}.$$

**Bài 7.** Tìm tất cả các số nguyên dương  $m > 1$  sao cho tồn tại đa thức  $P(x)$  với các hệ số nguyên thoả mãn:

- i, Với mỗi  $a$  nguyên,  $f(a) \equiv 0$  hoặc  $1 \pmod{m}$ .  
ii, Tồn tại  $u, v$  nguyên sao cho  $f(u) \equiv 0, f(v) \equiv 1 \pmod{m}$ .

**Bài 8.** Cho  $n$  là một số nguyên dương. Chứng minh rằng luôn tồn tại  $n$  số nguyên dương liên tiếp sao cho trong chúng không có số nào là lũy thừa của một số nguyên tố.

## LỜI GIẢI

**Bài 1 (Nordic 1998).**

a, Các số nguyên dương  $n$  thoả mãn điều kiện đã cho là 1 và 3, trong đó các dãy tương ứng là 1 và 1, 3, 2.

Giả sử  $n$  là một số nguyên dương thoả mãn điều kiện đề bài. Khi đó ta có

$$x_1 + x_2 + \cdots + x_n = 1 + 2 + \cdots + n = \frac{n(n+1)}{2} : n$$

nên  $n$  là một số lẻ. Giả sử  $n \geq 5$ , đặt  $m = (n+1)/2$ . Theo giả thiết,

$$x_1 + x_2 + \cdots + x_{n-1} = nm - x_n : n - 1$$

nên

$$x_n \equiv nm \equiv m \pmod{n-1}, \quad 1 \leq x_n \leq n$$

suy ra  $x_{n-1} = m$ . Tương tự,

$$x_1 + x_2 + \cdots + x_{n-2} = (n-1)m - x_{n-1} : n - 2$$

nên

$$x_{n-1} \equiv (n-1)m \equiv m \pmod{n-2}, \quad 1 \leq x_{n-1} \leq n$$

suy ra  $x_{n-1} = m = x_n$  vô lý. Vậy chỉ có  $n = 1$  hoặc  $n = 3$  thoả mãn điều kiện đề bài.

b, Ta sẽ xây dựng một dãy  $(x_n)_n$  thoả mãn điều kiện đề bài. Lấy  $x_1 = 1, x_2 = 3, x_3 = 2$ .

Giả sử  $x_1, x_2, \dots, x_N$  là một dãy thoả mãn  $x_1 + x_2 + \dots + x_k \vdots k$  với mọi  $k = 1, 2, \dots, N$ . Đặt

$$s = x_1 + x_2 + \dots + x_N.$$

Gọi  $n$  là số nguyên dương bé nhất không nằm trong dãy  $x_1, x_2, \dots, x_N$ . Do  $(N+1, N+2) = 1$  nên theo định lý thặng dư Trung Hoa tồn tại một số nguyên  $m > x_1, x_2, \dots, x_N$  thoả mãn

$$m \equiv -s \pmod{N+1}, \quad m \equiv -s - n \pmod{N+2}.$$

Đặt  $x_{N+1} = m$ ,  $x_{N+2} = n$  ta có dãy  $x_1, x_2, \dots, x_N, x_{N+1}, x_{N+2}$  thoả mãn

$$x_1 + x_2 + \dots + x_{N+1} = s + m \vdots N+1,$$

$$x_1 + x_2 + \dots + x_{N+2} = s + m + n \vdots N+2$$

và

$$x_1 + x_2 + \dots + x_k \vdots k \quad \text{với mọi } k = 1, 2, \dots, N.$$

Do đó,

$$x_1 + x_2 + \dots + x_k \vdots k \quad \text{với mọi } k = 1, 2, \dots, N+2.$$

Hiển nhiên dãy  $(x_n)_n$  được xây dựng như trên thoả mãn điều kiện đã cho.

### Bài 2 (Czech-Slovak 1997).

Gọi  $p_k$  là số nguyên tố thứ  $k$ ,  $k \geq 1$ . Theo định lý thặng dư Trung Hoa tồn tại dãy số  $\{a_n\}_{n=1}^{\infty}$  thoả mãn

$$a_1 = 2, \quad a_n \equiv -k \pmod{p_{k+1}}, \quad \forall k \leq n.$$

Với mọi  $k \geq 0$  ta có  $k + a_n \equiv 0 \pmod{p_{k+1}}$  với mọi  $n \geq k + 1$ . Do đó, có nhiều nhất  $k + 1$  số trong dãy  $\{k + a_n\}$  là số nguyên tố, các số từ thứ  $k + 2$  trở đi sẽ chia hết cho  $p_{k+1}$  và do đó là hợp số. Từ đó suy ra điều phải chứng minh.

### Bài 3 (Korea 1999).

Tất cả các số nguyên dương  $n$  cần tìm đều có dạng  $n = 2^k$  với  $k$  là một số nguyên dương bất kỳ.

Do  $2^n \equiv 1 \pmod{3}$  nên  $n$  phải là một số chẵn. Giả sử  $n$  có một ước số lẻ  $l$ . Ta có  $2^n - 1 : 2^l - 1$  nên  $2^l - 1$  là một ước số của  $4m^2 + 1$ . Vì  $2^l - 1 \equiv -1 \pmod{4}$  nên tồn tại một ước số nguyên tố  $p$  của  $2^l - 1$  có dạng  $p = 4r + 3$ . Do đó,  $4m^2 + 1 : p$  hay  $-1 \equiv (2m)^2 \pmod{p}$ , tức là  $-1$  là một số chính phương modulo  $p$  với  $p = 4r + 3$ , vô lý. Vậy điều giả sử là sai nên  $n$  không có ước số lẻ, suy ra tồn tại một số nguyên dương  $k$  sao cho  $n = 2^k$ .

Với  $n = 2^k$  ta có

$$\frac{2^n - 1}{3} = (2^{2^1} + 1)(2^{2^2} + 1)(2^{2^3} + 1) \cdots (2^{2^{k-1}} + 1).$$

Mặt khác với mọi số nguyên dương  $a < b$  ta có

$$2^{2^b} - 1 : 2^{2^{a+1}} - 1 \quad \text{và} \quad 2^{2^{a+1}} - 1 = (2^{2^a} + 1)(2^{2^a} - 1)$$

nên  $2^{2^b} - 1 : 2^{2^a} + 1$ , do đó

$$(2^{2^a} + 1, 2^{2^b} + 1) = (2^{2^a} + 1, 2^{2^b} - 1 + 2) = (2^{2^a} + 1, 2) = 1,$$

suy ra các số  $2^{2^1} + 1, 2^{2^2} + 1, 2^{2^3} + 1, \dots, 2^{2^{k-1}} + 1$  đều chia hết cho nhau.

Theo định lý thặng dư Trung Hoa, tồn tại một số nguyên dương  $c$  chẵn thoả mãn

$$c \equiv 2^{2^{i-1}} \pmod{2^{2^i} + 1}, \quad \text{với mọi } i = 1, 2, \dots, k-1.$$

Đặt  $c = 2m$  ta có  $4m^2 + 1 : (2^n - 1)/3$ , tức là mọi số nguyên dương  $n = 2^k$  đều thoả mãn điều kiện đã cho.

#### Bài 4 (Balkan 2000).

Giả sử  $A = \{a_1, a_2, \dots, a_k\}$ . Gọi  $p_1, p_2, \dots, p_N$  là tất cả các ước số nguyên tố của  $\prod_{i=1}^k a_i$ . Với mỗi  $i = 1, 2, \dots, k$  tồn tại các số nguyên không âm  $\alpha_{i,j}$  sao cho

$$a_i = \prod_{j=1}^N p_j^{\alpha_{i,j}}$$

Gọi  $q_1, q_2, \dots, q_k$  là các số nguyên tố phân biệt. Theo định lý thăng dù Trung Hoa, với  $j = 1, 2, \dots, N$  tồn tại  $\beta_j$  sao cho

$$\beta_j \equiv -\alpha_{i,j} \pmod{q_i} \quad \text{với mọi } i = 1, 2, \dots, k.$$

Đặt  $m = \prod_{j=1}^N p_j^{\beta_j}$ . Khi đó với  $i = 1, 2, \dots, k$ ,

$$ma_i = \prod_{j=1}^N p_j^{\alpha_{i,j} + \beta_j} = \left( \prod_{j=1}^N p_j^{(\alpha_{i,j} + \beta_j)/q_i} \right)^{q_i}$$

là một luỹ thừa.

## 4 Cấp của một số nguyên

### 4.1 Cấp của một số nguyên

#### Định nghĩa 1.4.1.

Cho  $m$  là một số nguyên dương và  $a$  là một số nguyên bất kỳ thoả mãn  $(a, m) = 1$ . Số nguyên dương  $h$  nhỏ nhất sao cho  $a^h \equiv 1 \pmod{m}$  được gọi là cấp của  $a$  modulo  $m$ .

Ví dụ, cấp của 2 modulo 3 là 2, modulo 5 là 4, cấp của 4 modulo 5 là 2. Để thấy rằng nếu  $a$  có cấp  $h$  modulo  $m$  và  $k$  là một bội số bất kỳ của  $h$ ,  $k = qh$  thì

$$a^k \equiv a^{qh} \equiv (a^h)^q \equiv 1^q \equiv 1 \pmod{m}.$$

Bổ đề sau (gồm các tính chất cơ bản của cấp) cho thấy điều ngược lại cũng đúng.

#### Bổ đề 1.4.1.

- i) Nếu  $a$  có cấp  $h$  modulo  $m$  thì số nguyên  $k$  thoả mãn  $a^k \equiv 1 \pmod{m}$  nếu và chỉ nếu  $k$  là bội của  $h$ .
- ii) Nếu  $a$  có cấp  $h$  modulo  $m$  thì  $a^k$  có cấp  $h/(h, k)$  modulo  $m$ .
- iii) Nếu  $a$  có cấp  $h$  modulo  $m$ ,  $b$  có cấp  $k$  modulo  $m$  và  $(h, k) = 1$  thì  $ab$  có cấp  $hk$  modulo  $m$ .

#### Chứng minh

- i) Chứng minh trên ta thấy nếu  $k$  là bội của  $h$  thì  $a^k \equiv 1 \pmod{m}$ . Do đó chỉ cần chứng minh phần ngược lại.

Giả sử  $a^k \equiv 1 \pmod{m}$  với  $k = qh + r$ ,  $0 \leq q, 0 \leq r < h$ . Khi đó

$$1 \equiv a^k = a^{qh+r} = (a^h)^q a^r \equiv 1^q a^r \equiv a^r \pmod{m}.$$

Do  $0 \leq r < h$  và  $h$  là số nguyên dương nhỏ nhất thoả mãn  $a^h \equiv 1 \pmod{m}$  nên suy ra  $r = 0$ , tức là  $k$  là bội của  $h$ . Bổ đề được chứng minh.

- ii) Theo phần i,  $(a^k)^j \equiv 1 \pmod{m}$  nếu và chỉ nếu  $kj \vdash h$ . Mặt khác,  $kj \vdash h$  khi và chỉ khi  $kj/(h, k) \vdash h/(h, k)$ . Do  $(k/(h, k), h/(h, k)) = 1$

nên  $kj \vdash h$  nếu và chỉ nếu  $j \vdash h/(h, k)$ . Do đó, số nguyên dương  $j$  nhỏ nhất thoả mãn  $(a^k)^j \equiv 1 \pmod{m}$  là  $j = h/(h, k)$ . ii, được chứng minh.

iii) Gọi  $r$  là cấp của  $ab \pmod{m}$ . Do  $(ab)^{hk} \equiv (a^h)^k(b^k)^h \equiv 1 \pmod{m}$  nên từ i, suy ra  $r$  là ước số của  $hk$ . Vì vậy, để chứng minh  $r = hk$  ta chỉ cần chứng minh  $r \vdash hk$ . Ta có

$$b^{rh} \equiv (a^h)^r b^{rh} = (ab)^{rh} \equiv 1 \pmod{m}$$

nên theo i, có  $rh \vdash k$ . Vì  $(h, k) = 1$  nên  $r \vdash k$ . Hoàn toàn tương tự ta cũng có  $r \vdash h$ . Từ đó và  $(h, k) = 1$  suy ra  $r \vdash hk$ , tức là  $r = hk$ .

Từ bổ đề 1.4.1 ta có các nhận xét sau:

- Phần ii, là một mở rộng của i,. Khẳng định i, chính là khẳng định của ii, trong trường hợp  $k$  là bội của  $h$ , tức là khi  $h/(h, k) = 1$ .
- Phần iii, sẽ không còn đúng nếu thiếu giả thiết  $(h, k) = 1$ . Ví dụ, 2 và 3 cùng có cấp là 2 modulo 5, nhưng  $6 = 2 \cdot 3$  có cấp 1 ( $\neq 2, 2$ ) modulo 5.
- Trong trường hợp  $(h, k) > 1$ , dù không suy ra được cấp của  $ab$  modulo  $m$  là  $r = hk$  nhưng ta có thể dễ dàng chứng minh được  $r$  là ước số của  $hk$ .

Thật vậy, ta có

$$(ab)^{hk} = (a^h)^k(b^k)^h \equiv 1 \pmod{m}$$

nên từ i, suy ra  $hk \vdash r$ .

Tính chất sau là một trong những tính chất quan trọng nhất của phần này khi làm các bài tập

- Nếu  $p$  là một số nguyên tố,  $a, m > 1$  là các số nguyên dương thoả mãn  $(a, m) = 1$ ,  $a \not\equiv 1 \pmod{m}$  và  $a^p \equiv 1 \pmod{m}$  thì cấp của  $a$  modulo  $m$  là  $p$ .

Thật vậy, gọi  $h$  là cấp của  $a$  modulo  $m$ . Từ bổ đề 1.4.1, ta có  $h/p, h \neq 1$ . Do  $p$  là một số nguyên tố nên  $h = p$ .

Từ định lýthagoras Trung Hoa ta có tính chất sau

- Nếu  $a, m, n$  là các số nguyên đôi một nguyên tố cùng nhau,  $a$  có cấp  $h$  modulo  $m$  và có cấp  $k$  modulo  $n$  thì  $a$  có cấp  $[h, k]$  modulo  $mn$ .

Thật vậy, gọi  $r$  là cấp của  $a$  modulo  $mn$ , ta có  $a^r \equiv 1 \pmod{m}$  và  $a \equiv 1 \pmod{n}$ . Theo bổ đề 1.4.1 ta có  $r : h$  và  $r : k$ , tức là  $r : [h, k]$ . Để chứng minh  $r = [h, k]$  chỉ cần chứng minh  $[h, k] : r$ .

Giả sử  $[h, k] = hk_1 = h_1k$ . Ta có

$$a^{[h,k]} = (a^h)^{k_1} \equiv 1^{k_1} \equiv 1 \pmod{m},$$

$$a^{[h,k]} = (a^k)^{h_1} \equiv 1^{h_1} \equiv 1 \pmod{n}.$$

Theo định lý thặng dư Trung Hoa suy ra  $a^{[h,k]} \equiv 1 \pmod{(mn)}$ , từ bổ đề 1.1.4 suy ra  $[h, k] : r$ , tức là  $r = [h, k]$ .

Theo định lý Euler, nếu  $(a, m) = 1$  thì  $a^{\phi(m)} \equiv 1 \pmod{m}$  nên từ bổ đề trên ta có ngay hệ quả sau.

### Hệ quả 1.4.2

- Nếu  $(a, m) = 1$  thì cấp của  $a$  modulo  $m$  là một ước số của  $\phi(m)$ .
- Nếu  $p$  là một số nguyên tố,  $(a, p) = 1$  thì cấp của  $a$  modulo  $p$  là một ước số của  $p - 1$ .

## 4.2 Căn nguyên thuỷ

Từ bổ đề 1.4.1 ta đã biết cấp của một số nguyên  $a$  modulo  $m$  luôn là một ước số của  $\phi(m)$ . Trong nhiều trường hợp cụ thể của  $m$ , tồn tại những số nguyên  $a$  sao cho cấp của  $a$  modulo  $m$  đúng bằng  $\phi(m)$ . Khi đó, ta có thể biểu diễn hệ thặng dư thu gọn modulo  $m$  dưới dạng sau

$$\{1, a, a^2, \dots, a^{\phi(m)}\}.$$

Biểu diễn này đem lại rất nhiều thuận lợi khi xét tích các phân tử trong hệ thặng dư thu gọn, ta có thể quy phép nhân các phân tử trong hệ thặng dư thu gọn trên về phép cộng modulo  $\phi(m)$ . Cụ thể hơn, ta có thể tương ứng phân tử  $a^i, a^j$  trong hệ thặng dư với các phân tử  $i, j$  trong tập

$\{1, 2, \dots, \phi(m)\}$ . Khi đó, tích  $a^i \cdot a^j$  được tương ứng với phân tử  $i + j$ . Vì lý do đó, người ta đưa ra định nghĩa sau.

### Định nghĩa 1.4.2.

Nếu số nguyên dương  $g$  có cấp là  $\phi(m)$  modulo  $m$  thì  $g$  được gọi là một căn nguyên thuỷ modulo  $m$ .

Kết quả quan trọng nhất trong mục này khẳng định rằng mỗi số nguyên tố  $p$  đều có đúng  $\phi(p - 1)$  căn nguyên thuỷ. Để đi đến kết quả đó ta cần bổ đề sau

### Bổ đề 1.4.3.

Cho  $p$  và  $q$  là hai số nguyên tố sao cho  $(p - 1) : q^\alpha$  với  $\alpha \geq 1$ . Khi đó có đúng  $q^\alpha - q^{\alpha-1}$  lớp thặng dư phân biệt có cấp  $q^\alpha$  modulo  $p$ .

### Chứng minh

Xét phương trình

$$x^{q^\alpha} - 1 \equiv 0 \pmod{p}.$$

Phương trình này có đúng  $q^\alpha$  nghiệm phân biệt modulo  $p$ . Vì  $q$  là một số nguyên tố nên từ bổ đề 1.4.1, mỗi nghiệm cho ta một lớp thặng dư có cấp là  $q^\beta$  trong đó  $\beta$  là một số nguyên nhỏ hơn hoặc bằng  $\alpha$ . Như vậy, một lớp thặng dư  $a$  có cấp  $q^\alpha$  modulo  $p$  nếu nó là nghiệm của phương trình trên và  $a^{q^{\alpha-1}} \not\equiv 1 \pmod{p}$ , tức là nó không là nghiệm của phương trình

$$x^{q^{\alpha-1}} - 1 \equiv 0 \pmod{p}.$$

Mỗi nghiệm trong số  $q^{\alpha-1}$  nghiệm của phương trình dưới đây đều là nghiệm của phương trình trên, do đó số lớp thặng dư phân biệt có cấp  $q^\alpha$  modulo  $p$  là  $q^\alpha - q^{\alpha-1}$ .

Định lý sau là kết quả quan trọng nhất của mục này.

### Định lý 1.4.4.

Nếu  $p$  là một số nguyên tố thì có đúng  $\phi(p - 1)$  căn nguyên thuỷ modulo  $p$ .

### Chứng minh

Trước hết ta đi chứng minh tồn tại một căn nguyên thuỷ modulo  $p$ .  
Giả sử có phân tích chính tắc

$$p - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Theo bổ đề 1.4.3, với mỗi  $i$  tồn tại một lớp thặng dư  $a_i$  (modulo  $p$ ) sao cho  $a_i$  có cấp  $p^{\alpha_i}$  modulo  $p$ . Do các số  $\{p_i^{\alpha_i}, i = 1, 2, \dots, k\}$  là đôi một nguyên tố cùng nhau nên theo bổ đề 1.4.3, ta có  $g = a_1 a_2 \cdots a_k$  có cấp  $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p - 1$  modulo  $p$ . Vậy  $g$  là một căn nguyên thuỷ modulo  $p$ .

Tiếp theo ta sẽ chứng minh có đúng  $\phi(p - 1)$  căn nguyên thuỷ modulo  $p$ . Xét căn nguyên thuỷ  $g$  như trên, khi đó tập hợp  $\{g^1, g^2, \dots, g^{p-1}\}$  lập thành một hệ thặng dư thu gọn modulo  $p$ . Theo bổ đề 1.4.3,  $g^k$  có cấp  $(p - 1)/(k, p - 1)$  modulo  $p$ . Do đó,  $g^k$  là một căn nguyên thuỷ nếu và chỉ nếu  $(k, p - 1) = 1$ . Từ định nghĩa của hàm Euler suy ra có đúng  $\phi(p - 1)$  căn nguyên thuỷ modulo  $p$ .

### Định lý 1.4.5.

Nếu  $p$  là một số nguyên tố lẻ thì  $p^2$  có đúng  $\phi(\phi(p^2))$  căn nguyên thuỷ. Hơn nữa, nếu  $g$  là một căn nguyên thuỷ modulo  $p$  thì trong  $p$  số  $g + kp$ ,  $k = 0, 1, \dots, p - 1$  có đúng  $p - 1$  số là căn nguyên thuỷ modulo  $p^2$ .

### Chứng minh

Trước hết, ta đi chứng minh có không quá  $\phi(p(p - 1)) = \phi(\phi(p^2))$  căn nguyên thuỷ modulo  $p^2$ . Thật vậy, nếu  $p^2$  có căn nguyên thuỷ  $g$  thì tập

$$\{1, g, g^2, g^3, \dots, g^{p(p-1)-1}\}$$

lập thành một hệ thặng dư thu gọn modulo  $p^2$ . Theo bổ đề 1.4.3, phân tử  $g^k$  là một căn nguyên thuỷ nếu và chỉ nếu  $(k, p(p - 1)) = 1$ . Do đó, theo định nghĩa của hàm Euler, có đúng  $\phi(p(p - 1))$  số như vậy. Vậy nếu  $p^2$  có căn nguyên thuỷ thì sẽ có đúng  $\phi(p(p - 1))$  căn nguyên thuỷ.

Tiếp theo, ta đi chứng minh  $p^2$  có căn nguyên thuỷ.

Gọi  $g$  là một căn nguyên thuỷ của  $p$ . Xét các số  $\{g + kp : 0 \leq k \leq p - 1\}$ .

Ta sẽ chứng minh rằng trong tập hợp này có đúng  $p - 1$  căn nguyên thuỷ modulo  $p^2$ . Gọi  $h = h(k)$  là cấp của  $g + kp$  modulo  $p^2$ , khi đó  $h$  là ước số của  $\phi(p^2) = p(p - 1)$ . Mặt khác, do

$$(g + kp)^h \equiv 1 \pmod{p^2}$$

nên  $(g + kp)^h \equiv g^h \equiv 1 \pmod{p}$ , từ đó suy ra  $h : p - 1$  (vì  $g$  là căn nguyên thuỷ modulo  $p$ ). Vậy  $h$  chỉ có thể nhận một trong hai giá trị là  $p - 1$  hoặc  $p(p - 1)$ .

Nếu  $h = p(p - 1)$  thì  $g + kp$  là một căn nguyên thuỷ modulo  $p^2$ , nên ta chỉ cần chứng minh có đúng  $p - 1$  giá trị của  $k$  sao cho  $h(k) = p(p - 1)$ . Xét đa thức

$$f(x) = x^{p-1} - 1.$$

Điều kiện cần và đủ để  $h(k) = p - 1$  là  $g + kp$  phải là nghiệm của phương trình

$$f(x) \equiv 0 \pmod{p^2}.$$

Vì vậy, ta chỉ cần chứng minh có duy nhất một số  $k$  trong tập hợp  $\{0, 1, \dots, p - 1\}$  sao cho  $f(g + kp) \equiv 0 \pmod{p^2}$ . Đặt  $g^{p-1} - 1 = pN$ , ta có

$$\begin{aligned} f(g + kp) &= (g + kp)^{p-1} - 1 \equiv g^{p-1} - 1 + (p - 1)g^{p-2}kp \\ &= p(N + (p - 1)kg^{p-2}) \pmod{p^2}. \end{aligned}$$

Tức là,  $f(g + kp) \equiv 0 \pmod{p^2}$  khi và chỉ khi

$$N + (p - 1)kg^{p-2} \equiv 0 \pmod{p}.$$

Do  $((p - 1)g^{p-2}, p) = 1$ , nên suy ra có duy nhất  $k \in \{0, 1, \dots, p - 1\}$  là nghiệm của phương trình

$$(p - 1)g^{p-2}x + N \equiv 0 \pmod{p}.$$

Từ đó ta có điều phải chứng minh.

Từ chứng minh định lý trên, nếu  $g < p$  là một căn nguyên thuỷ của  $p$  thì trong tập hợp  $\{g + kp : 0 \leq k \leq p - 1\}$  có đúng  $p - 1$  căn nguyên thuỷ modulo  $p^2$ . Do đó, trong hai số  $g$  và  $g + p$  phải có ít nhất một số là căn nguyên thuỷ modulo  $p^2$ . Có nhiều số nguyên tố  $p$  và căn nguyên thuỷ  $g < p$  modulo  $p$  sao cho  $g$  không phải là căn nguyên thuỷ modulo  $p$ . Chẳng hạn  $(p, g) = (29, 14), (37, 18), (71, 11), (487, 10), \dots$

Ta có định lý sau, chúng minh dành cho bạn đọc.

### Định lý 1.4.6.

Nếu  $p$  là một số nguyên tố lẻ và  $g$  là một căn nguyên thuỷ modulo  $p^2$  thì  $g$  cũng là căn nguyên thuỷ modulo  $p^n$  với  $n \geq 3$ .

Tiếp theo, ta sẽ xét câu hỏi: Những số nguyên dương nào có căn nguyên thuỷ? Câu trả lời được cho trong định lý sau.

### Định lý 1.4.7.

Cho  $m$  là một số nguyên,  $m > 1$ . Khi đó,  $m$  có căn nguyên thuỷ khi và chỉ khi  $m$  có một trong 4 dạng sau

$$2, 4, p^\alpha, 2p^\alpha$$

trong đó  $p$  là một số nguyên tố lẻ.

### Chứng minh

Trước hết, ta đi chứng minh rằng, nếu  $m$  có một trong 4 dạng trên thì  $m$  có căn nguyên thuỷ. Bằng kiểm tra trực tiếp, ta thấy ngay 2 và 4 có căn nguyên thuỷ.

$$1^{\phi(2)-1} \equiv 1 \pmod{2}, \quad 3^{\phi(4)-1} = 3^2 \equiv 1 \pmod{4}.$$

Từ đó và định lý 1.4.6, ta chỉ cần chứng minh nếu  $m = 2p^\alpha$  thì  $m$  có căn nguyên thuỷ. Ta có

$$\phi(2p^\alpha) = \phi(2)\phi(p^\alpha) = \phi(p^\alpha).$$

Giả sử  $g$  là một căn nguyên thuỷ modulo  $p^\alpha$ , khi đó

$$\{1, g, g^2, \dots, g^{\phi(p^\alpha)-1}\} = \{1, g, g^2, \dots, g^{\phi(2p^\alpha)-1}\}$$

lập thành một hệ thặng dư thu gọn modulo  $p^\alpha$ . Ta có thể giả sử  $g$  lẻ vì nếu trái lại, thay vì xét  $g$ , ta có thể xét  $g + p^\alpha$  là một số lẻ và cũng là một căn nguyên thuỷ modulo  $p^\alpha$ . Vì  $g$  lẻ nên tập hợp  $\{1, g, g^2, \dots, g^{\phi(2p^\alpha)-1}\}$  chứa  $\phi(2p^\alpha)$  phần tử phân biệt modulo  $2p^\alpha$  và mỗi phần tử đều nguyên tố

cùng nhau với  $2p^\alpha$ . Do đó,  $\{1, g, g^2, \dots, g^{\phi(2p^\alpha)-1}\}$  đồng thời cũng là hệ thặng dư thu gọn modulo  $2p^\alpha$ , tức là  $g$  là một căn nguyên thuỷ modulo  $2p^\alpha$ . Vậy phần đảo của định lý được chứng minh.

Ngược lại, ta sẽ chứng minh rằng nếu  $m$  không có một trong 4 dạng trên thì nó không có căn nguyên thuỷ. Để thấy, nếu  $m$  không có một trong 4 dạng trên thì nó chỉ có thể có một trong hai dạng:  $m = 2^\alpha$  với  $\alpha > 2$ , hoặc  $m = m_1m_2$  với  $m_1, m_2 > 2$ ,  $(m_1, m_2) = 1$ .

Trước hết, ta chứng minh cho rằng nếu  $m = 2^\alpha$  với  $\alpha > 2$  thì  $m$  không có căn nguyên thuỷ. Nhận xét rằng nếu  $g$  là một số nguyên lẻ thì  $g^2 \equiv 1 \pmod{8}$ . Mặt khác,

$$g^{2^{n+1}} - 1 = (g^{2^n} + 1)(g^{2^n} - 1)$$

với  $g^{2^n} + 1$  là một số chẵn nên tồn tại một số nguyên dương  $k_n$  sao cho

$$g^{2^{n+1}} = 2k_n(g^{2^n} - 1).$$

Từ đó, bằng quy nạp ta có  $g^{2^{\alpha-2}} = g^{(\phi(2^\alpha)-1)/2} \equiv 1 \pmod{2^\alpha}$ . Do đó,  $2^\alpha$  không thể có căn nguyên thuỷ nếu  $\alpha > 2$ .

Tiếp theo, ta chứng minh cho rằng nếu  $m = m_1m_2$  với  $m_1, m_2 > 2$  là các số nguyên tố cùng nhau thì  $m$  không có căn nguyên thuỷ. Thật vậy, do  $m_1, m_2 > 2$  nên  $\phi(m_1), \phi(m_2) : 2$ , do đó

$$[\phi(m_1), \phi(m_2)] =$$

$$= \frac{\phi(m_1)\phi(m_2)}{(\phi(m_1), \phi(m_2))} \leq \frac{\phi(m_1)\phi(m_2)}{2} < \phi(m_1)\phi(m_2) = \phi(m).$$

Đặt  $h = [\phi(m_1), \phi(m_2)]$ , khi đó  $h : \phi(m_1)$  và  $h : \phi(m_2)$ . Theo định lý Euler, với mỗi số nguyên dương  $a$  thoả mãn  $(a, m) = 1$  ta có

$$a^h \equiv 1 \pmod{m_1}, \quad a^h \equiv 1 \pmod{m_2}.$$

Từ định lý thặng dư Trung Hoa suy ra  $a^h \equiv 1 \pmod{m}$  với mọi số nguyên dương  $a$ ,  $(a, m) = 1$ . Từ đó suy ra  $m$  không thể có căn nguyên thuỷ. Định lý được chứng minh.

**Ví dụ 1.4.1.** Cho  $p$  là một số nguyên tố,  $a, n$  là các số nguyên dương,  $(a, n) = 1$ . Chứng minh rằng

a, Phương trình  $x^n \equiv a \pmod{p}$  hoặc có  $(n, p - 1)$  nghiệm hoặc vô nghiệm, tuỳ theo

$$a^{(p-1)/(n,p-1)} \equiv 1 \pmod{p} \text{ hay không.}$$

b, Nếu  $(n, p - 1) = 1$  thì phương trình  $x^n \equiv a \pmod{p}$  có đúng một nghiệm.

### Giải

a, Giả sử  $g$  là một căn nguyên thuỷ của  $p$ ,  $a \equiv g^k \pmod{p}$ . Nếu tồn tại số nguyên  $x$  sao cho  $x^n \equiv a \pmod{p}$  thì  $(x, p) = 1$ , do đó tồn tại một số nguyên dương  $u$  sao cho  $x \equiv g^u \pmod{p}$ . Khi đó,

$$g^{nu} \equiv g^k \pmod{p} \text{ hay } nu \equiv k \pmod{p-1}.$$

Đặt  $d = (n, p - 1)$ , khi đó phương trình  $nu \equiv k \pmod{p-1}$  có  $d$  nghiệm nếu  $k : d$  và vô nghiệm nếu  $k \nmid d$ .

Nếu  $k : d$  thì  $k(p - 1)/d \equiv 0 \pmod{p - 1}$  nên

$$a^{(p-1)/d} \equiv g^{k(p-1)/d} \equiv (g^{p-1})^{k/d} \equiv 1 \pmod{p}$$

Nếu  $k \nmid d$  thì  $k(p - 1)/d \not\equiv 0 \pmod{p - 1}$  nên

$$a^{(p-1)/d} \equiv g^{k(p-1)/d} \not\equiv 1 \pmod{p}$$

Điều phải chứng minh.

b, Là trường hợp riêng của a, với  $(n, p - 1) = 1$ .

### Ví dụ 1.4.2.

a. Cho  $p$  là một số nguyên tố. Chứng minh rằng các số  $1^k, 2^k, \dots, (p - 1)^k$  lập thành một hệ thặng dư thu gọn modulo  $p$  nếu và chỉ nếu  $(k, p - 1) = 1$ .

b. Cho  $r_1, r_2, \dots, r_n$  là một hệ thặng dư thu gọn modulo  $m$ . Chứng minh rằng các số  $r_1^k, r_2^k, \dots, r_n^k$  lập thành một hệ thặng dư thu gọn modulo  $m$  nếu và chỉ nếu  $(k, \phi(m)) = 1$ .

### Giải

a. Gọi  $g$  là một căn nguyên thuỷ của  $p$ , khi đó  $g, g^2, g^3, \dots, g^{p-1}$  là một

hệ thặng dư thu gọn modulo  $p$ . Ta có  $g^{r_1}, g^{r_2}, g^{r_3}, \dots, g^{r_{p-1}}$  là một hệ thặng dư thu gọn modulo  $p$  khi và chỉ khi  $r_1, r_2, \dots, r_{p-1}$  là một hệ thặng dư đầy đủ modulo  $p - 1$ . Do đó, để  $1^k, 2^k, \dots, (p-1)^k$  lập thành một hệ thặng dư thu gọn modulo  $p$ , điều kiện cần và đủ là  $g^k, g^{2k}, g^{3k}, \dots, g^{(p-1)k}$  là một hệ thặng dư thu gọn modulo  $p$  hay  $k, 2k, \dots, (p-1)k$  là một hệ thặng dư đầy đủ modulo  $p - 1$ . Hiển nhiên  $k, 2k, \dots, (p-1)k$  là một hệ thặng dư đầy đủ modulo  $p - 1$  nếu và chỉ nếu  $(k, p - 1) = 1$ . Từ đó ta có điều phải chứng minh.

b. Giả sử  $m = \prod_i p_i^{\alpha_i}$ . Khi đó, theo định lý thặng dư Trung Hoa, điều kiện cần và đủ để  $r_1^k, r_2^k, \dots, r_n^k$  lập thành một hệ thặng dư thu gọn modulo  $m$  là với mỗi ước số nguyên tố  $p_i$  của  $m$ ,  $s_1^k, s_2^k, \dots, s_l^k$  lập thành một hệ thặng dư thu gọn modulo  $p_i^{\alpha_i}$  với mọi hệ thặng dư thu gọn  $s_1, s_2, \dots, s_l$  của  $p_i^{\alpha_i}$ . Gọi  $g$  là một căn nguyên thuỷ của  $p_i^{\alpha_i}$ , khi đó  $g^{t_1}, g^{t_2}, g^{t_3}, \dots, g^{t_{\phi(p_i^{\alpha_i})}}$  là một hệ thặng dư thu gọn modulo  $p_i^{\alpha_i}$  khi và chỉ khi  $t_1, t_2, \dots, t_{\phi(p_i^{\alpha_i})}$  là một hệ thặng dư đầy đủ modulo  $\phi(p_i^{\alpha_i})$ . Từ đó, tương tự phần a, suy ra điều kiện cần và đủ để  $s_1^k, s_2^k, \dots, s_l^k$  lập thành một hệ thặng dư thu gọn modulo  $p_i^{\alpha_i}$  là  $(k, \phi(p_i^{\alpha_i})) = 1$  với mọi ước số nguyên tố  $p_i$  của  $m$  hay  $(k, \phi(m)) = 1$ . Điều phải chứng minh.

**Ví dụ 1.4.3 (Balkan 1999).** Cho  $p$  là một số nguyên tố có dạng  $3l + 2$ .  
Đặt

$$S = \{y^2 - x^3 - 1 \mid x, y \text{ là các số nguyên, } 0 \leq x, y \leq p - 1\}.$$

Chứng minh rằng có nhiều nhất  $p$  phần tử trong  $S$  chia hết cho  $p$ .

### Giải

Trước hết, từ ví dụ trên ta có nhận xét sau: Nếu  $p$  là một số nguyên tố,  $k, x, y$  là các số nguyên dương thỏa mãn  $(k, p - 1) = 1$  và  $x^k \equiv y^k \pmod{p}$  thì  $x \equiv y \pmod{p}$ .

Theo giả thiết ta có  $(3, p - 1) = 1$  nên  $\{1^3, 2^3, \dots, p^3\}$  là một hệ thặng dư đầy đủ modulo  $p$ . Do đó, với mỗi  $0 \leq y \leq p - 1$  tồn tại duy nhất số nguyên  $x$ ,  $0 \leq x \leq p - 1$  sao cho  $x^3 \equiv y^2 - 1 \pmod{p}$ , tức là trong tập  $S$  có nhiều nhất  $p$  số chia hết cho  $p$ . Điều phải chứng minh.

**Ví dụ 1.4.4.** Cho  $g$  là một căn nguyên thuỷ của số nguyên tố  $p$ , số

nguyên dương  $a \equiv g^k \pmod{p}$  có cấp  $h$  modulo  $p$  và  $a\bar{a} \equiv 1 \pmod{p}$ .  
 Chứng minh rằng  $\bar{a}$  cũng có cấp  $h$  modulo  $p$  và

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

### Giải

Hiển nhiên  $a\bar{a} \equiv g^k \bar{a} \equiv 1 \equiv g^{p-1} \pmod{p}$  nên  $\bar{a} \equiv g^{p-1-k} \pmod{p}$ .

Gọi  $k$  là cấp của  $\bar{a}$  modulo  $p$ .

Vì  $a^h \equiv 1 \pmod{p}$  nên  $\bar{a}^h \equiv (a\bar{a})^h \equiv 1^h = 1 \pmod{p}$ , từ đó suy ra  $h \mid k$ .

Vì  $\bar{a}^k \equiv 1 \pmod{p}$  nên  $a^k \equiv (a\bar{a})^k \equiv 1^k = 1 \pmod{p}$ , từ đó suy ra  $k \mid h$ .

Do  $h \mid k$  và  $k \mid h$  nên  $h = k$ , tức là cấp của  $\bar{a}$  là  $h$ . Điều phải chứng minh.

### Ví dụ 1.4.5. Chứng minh rằng

a, 2 là một căn nguyên thuỷ của  $3^n$  với mọi  $n \leq 1$ .

b, 2 là một căn nguyên thuỷ của 101.

### Giải

a, Ta có  $\phi(9) = 6$ ,  $2^1 \equiv 2 \not\equiv 1 \pmod{9}$ ,  $2^2 \equiv 4 \not\equiv 1 \pmod{9}$ ,  $2^3 \equiv 8 \not\equiv 1 \pmod{9}$ ,  $2^6 \equiv 64 \equiv 1 \pmod{9}$  nên 2 là một căn nguyên thuỷ modulo 9.  
 Theo định lý 1.4.6 suy ra 2 là căn nguyên thuỷ của  $3^n$  với mọi  $n \geq 1$ .

b, Ta có  $\phi(101) = 100$ . Mặt khác,

$$\begin{aligned} 2^{10} &= 1024 \equiv 14 \pmod{101}, \\ 2^{20} &\equiv 14^2 \equiv -6 \pmod{101}, \\ 2^{40} &\equiv (-6)^2 \equiv 36 \pmod{101}, \\ 2^{50} &\equiv 14 \cdot 36 \equiv -1 \pmod{101} \end{aligned}$$

nên suy ra 2 là một căn nguyên thuỷ modulo 101. Điều phải chứng minh.

### Ví dụ 1.4.6. Cho $p, q$ là hai số nguyên tố lẻ thoả mãn $p = 2q + 1$ . Chứng minh rằng $-a^2$ luôn là một căn nguyên thuỷ modulo $p$ với mọi số nguyên dương $a$ , $1 < a \leq q$ .

**Giải**

Giả sử  $q = 2k + 1$ , suy ra  $p = 2q + 1 = 4k + 3$  nên  $-1$  không phải là một số chính phương modulo  $p$ . Gọi  $g$  là một căn nguyên thuỷ modulo  $p$ , khi đó tồn tại các số nguyên dương  $s, t$ ,  $1 \leq s, t \leq p - 1$  sao cho  $-1 \equiv g^s, a \equiv g^t \pmod{p}$ . Do  $-1$  không là số chính phương modulo  $p$  nên  $s$  lẻ, do đó  $(s + 2t)q$  là một số lẻ và không chia hết cho  $p - 1$ . Từ đó,

$$(-a^2)^q \equiv (g^s g^{2t})^q \equiv g^{(s+2t)q} \not\equiv 1 \pmod{p}.$$

Mặt khác, vì  $1 < a \leq q$  nên  $a^2 \not\equiv 1 \pmod{p}$ , do đó

$$(-a^2)^2 \equiv a^4 \not\equiv 1 \pmod{p}.$$

Gọi cấp của  $-a^2$  modulo  $p$  là  $h$ . Khi đó  $h|(p - 1)$  nên  $h$  chỉ có thể nhận các giá trị là  $2, q$  hoặc  $2q$ . Từ chứng minh trên suy ra  $h = 2q = p - 1$ . Vậy  $-a^2$  là một căn nguyên thuỷ modulo  $p$ . Điều phải chứng minh.

**Ví dụ 1.4.7.** Chứng minh rằng

- a, Nếu  $a^k + 1$  là một số nguyên tố với  $a > 1$  thì  $k$  là một luỹ thừa của 2.
- b, Nếu số nguyên tố  $p$  thoả mãn  $p|(a^{2^n} + 1)$  thì  $p = 2$  hoặc  $p \equiv 1 \pmod{2^{n+1}}$ .

**Giải**

- a, Nếu  $k$  có một ước số lẻ  $l$  thì  $a^k + 1 = (a^{k/l})^l + 1 : a^{k/l} + 1$  nên  $a^k + 1$  không phải là một số nguyên tố. Vô lý. Vậy  $k$  không có ước số lẻ, tức là  $k$  là một luỹ thừa của 2.

- b, Gọi  $h$  là cấp của  $a$  modulo  $p$ . Ta có  $a^{2^n} \equiv -1 \pmod{p}$  và  $a^{2^{n+1}} \equiv 1 \pmod{p}$  nên  $h|2^{n+1}$  và  $h > 2^n$ , suy ra  $h = 2^{n+1}$ . Do  $h|(p - 1)$  nên  $p \equiv 1 \pmod{h}$ , tức là  $p \equiv 1 \pmod{2^{n+1}}$ . Điều phải chứng minh.

**Ví dụ 1.4.8.** Chứng minh rằng

- a, Nếu  $g$  và  $g'$  là hai căn nguyên thuỷ phân biệt modulo  $p$  thì  $gg'$  không phải là một căn nguyên thuỷ.
- b, Nếu  $g$  là một căn nguyên thuỷ modulo  $p^2$  thì  $g$  là một căn nguyên thuỷ modulo  $p$ .
- c, Hãy chứng minh định lý Wilson dựa vào căn nguyên thuỷ.

**Giải**

a, Giả sử  $g' \equiv g^k \pmod{p}$ . Do  $g'$  là một căn nguyên thuỷ nên  $(k, p - 1) = 1$ , suy ra  $k$  là một số lẻ. Do  $k$  lẻ nên  $k + 1 \vdots 2$  và  $(k + 1)(p - 1)/2 \vdots p - 1$ , từ đó ta có

$$(gg')^{(p-1)/2} = (g^{(k+1)/2})^{(p-1)} \equiv g^{p-1} \equiv 1 \pmod{p}.$$

Từ đó suy ra  $gg'$  không phải là một căn nguyên thuỷ.

b, Gọi cấp của  $g$  modulo  $p$  là  $h$ , khi đó  $h|(p - 1)$ . Do  $g^h \equiv 1 \pmod{p}$  nên tồn tại một số nguyên dương  $q$  sao cho  $g^h = pq + 1$ .

Ta có

$$\begin{aligned} g^{ph} &= (pq + 1)^p = (pq)^p + C_p^{p-1}(pq)^{p-1} + C_p^{p-2}(pq)^{p-2} + \dots \\ &\quad \dots + C_p^2(pq)^2 + C_p^1(pq) + 1. \end{aligned}$$

Do  $C_p^1 = p$  nên  $g^{ph} \equiv 1 \pmod{p^2}$ . Từ đó,  $ph \vdots \phi(p^2)$  tức là  $ph \vdots p(p - 1)$  hay  $h \vdots p - 1$ . Vì  $h|(p - 1)$  nên  $h = p - 1$ , suy ra  $g$  là một căn nguyên thuỷ của  $p$ . Điều phải chứng minh.

c, Vì  $g^1, g^2, g^3, \dots, g^{p-1}$  là một hệ thặng dư thu gọn modulo  $p$  nên  $(p - 1)! \equiv g^1 \cdot g^2 \cdot g^3 \cdots \cdot g^{p-1} \equiv g^{p(p-1)/2} \equiv g^{(p-1)/2} \equiv -1 \pmod{p}$ .

Điều phải chứng minh.

**Ví dụ 1.4.9.**

Cho  $a$  có cấp 3 modulo  $p$ . Tìm cấp của  $a + 1$  modulo  $p$ .

**Giải**

Ta có

$$a \not\equiv 1 \pmod{p}, \quad a^2 \not\equiv 1 \pmod{p}$$

nên từ  $a^3 - 1 = (a - 1)(a^2 + a + 1) \equiv 0 \pmod{p}$  suy ra  $a + 1 \equiv -a^2 \pmod{p}$ . Do  $a$  có cấp 3 modulo  $p$ ,  $-1$  có cấp 2 modulo  $p$  nên  $-a^2$  có cấp 6 modulo  $p$ .

Vậy cấp của  $a + 1$  modulo  $p$  là 6.

**Ví dụ 1.4.10.**

a, Cho  $a$  và  $n > 1$  là các số nguyên dương thoả mãn  $a^{n-1} \equiv 1 \pmod{n}$  và  $a^d \not\equiv 1 \pmod{n}$  với mọi ước  $d$  số của  $n - 1$ . Chứng minh rằng  $n$  là một số nguyên tố.

b, Cho  $n$  là một số nguyên dương, chứng minh rằng số các lớp thặng dư thu gọn  $a$  modulo  $n$  thoả mãn  $a^{n-1} \equiv 1 \pmod{n}$  là  $\prod_{p|n} (p-1, n-1)$ .

c, Chứng minh rằng số nguyên dương  $n$  có tính chất  $a^{n-1} \equiv 1 \pmod{n}$  với mọi lớp thặng dư thu gọn  $a$  modulo  $n$  nếu và chỉ nếu  $n$  không có ước số chính phương và  $(p-1)|(n-1)$  với mọi ước số nguyên tố  $p$  của  $n$ .

d, Chứng minh rằng số nguyên dương  $n$  có tính chất như phần c, nếu và chỉ nếu  $a^n \equiv a \pmod{n}$  với mọi số nguyên  $a$ .

**Giải**

a, Gọi  $h$  là số nguyên dương nhỏ nhất thoả mãn  $a^h \equiv 1 \pmod{n}$ . Đặt  $n-1 = hq+r$ ,  $0 \leq r < h$ , khi đó

$$a^r \equiv a^r a^{hq} = a^{hq+r} = a^n \equiv 1 \pmod{p}.$$

Từ cách đặt  $h$  suy ra  $r = 0$ , tức là  $h$  là ước của  $n-1$ . Theo giả thiết suy ra  $h = n-1$ .

Do  $(a, n) = 1$  nên theo định lý Euler,  $a^{\phi(n)} \equiv 1 \pmod{n}$ . Làm tương tự như trên đối với  $(h, n) = (n-1, \phi(n))$  ta có  $n-1$  là ước của  $\phi(n)$ . Từ đó suy ra  $n$  là một số nguyên tố.

b, Giả sử  $n = \prod_{p|n} p^\alpha$ , khi đó  $(n-1, p) = 1$  nên  $(n-1, \phi(p^\alpha)) = (n-1, p-1)$ . Gọi  $N(p)$  là số các lớp thặng dư thu gọn  $a$  modulo  $p^\alpha$  sao cho  $a^{n-1} \equiv 1 \pmod{p^\alpha}$ . Theo định lý thặng dư Trung Hoa ta có số các lớp thặng dư thu gọn modulo  $n$  thoả mãn  $a^{n-1} \equiv 1 \pmod{n}$  là  $\prod_{p|n} N(p)$ . Do đó, chỉ cần chứng minh rằng  $N(p) = (p-1, n-1)$ .

Gọi  $g$  là một căn nguyên thuỷ modulo  $p^\alpha$ , giả sử  $a \equiv g^u \pmod{p^\alpha}$ . Khi đó phương trình  $a^{n-1} \equiv 1 \pmod{p^\alpha}$  tương đương với  $g^{u(n-1)} \equiv 1 \pmod{p^\alpha}$  hay  $u(n-1) \equiv 0 \pmod{\phi(p^\alpha)}$ . Hiển nhiên phương trình  $u(n-1) \equiv 0 \pmod{\phi(p^\alpha)}$  có  $(n-1, \phi(p^\alpha))$  nghiệm modulo  $\phi(p^\alpha)$  nên phương trình  $a^{n-1} \equiv 1 \pmod{p^\alpha}$  có số nghiệm là  $N(p) = (n-1, \phi(p^\alpha)) = (n-1, p-1)$ .

c, Giả sử  $n$  thoả mãn  $a^{n-1} \equiv 1 \pmod{n}$  với mọi lớp thặng dư thu gọn  $a$  modulo  $n$ . Đặt  $n = \prod_{p|n} p^\alpha$ . Khi đó  $a^{n-1} \equiv 1 \pmod{p^\alpha}$  với mọi lớp thặng dư thu gọn  $a$  modulo  $p^\alpha$ . Gọi  $g$  là một căn nguyên thuỷ của  $p^\alpha$ , khi đó  $g^{n-1} \equiv 1 \pmod{p^\alpha}$  nên  $n - 1 \mid \phi(p^\alpha)$ . Do  $\phi(p^\alpha) = p^{\alpha-1}(p - 1)$  và  $(n - 1, p) = 1$  nên  $\alpha = 0$  và  $n - 1 \mid p - 1$ . Vậy  $n$  không có ước số chính phương và  $(p - 1)|(n - 1)$  với mọi ước số nguyên tố  $p$  của  $n$ .

Ngược lại, giả sử  $n$  không có ước số chính phương và  $(p - 1)|(n - 1)$  với mọi ước số nguyên tố  $p$  của  $n$ . Giả sử  $(a, n) = 1$ . Gọi  $p$  là một ước số nguyên tố bất kỳ của  $n$ , khi đó  $n - 1 \mid p - 1$  nên  $a^{n-1} \equiv 1 \pmod{p}$ . Vì  $n$  không có ước số chính phương và  $a^{n-1} \equiv 1 \pmod{p}$  với mọi ước số nguyên tố  $p$  của  $n$  nên theo định lý thặng dư Trung Hoa ta có  $a^{n-1} \equiv 1 \pmod{n}$ . Từ đó suy ra  $a^{n-1} \equiv 1 \pmod{n}$  với mọi lớp thặng dư thu gọn  $a$  modulo  $n$ .

d, Giả sử  $n$  thoả mãn điều kiện đề bài. Gọi  $a$  là một số nguyên dương bất kỳ,  $p$  là một ước số nguyên tố của  $n$ . Khi đó, theo phần c,  $n \mid p^2$  và  $n - 1 \mid p - 1$  nên

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

Vậy  $a^n \equiv a \pmod{p}$  với mọi ước số nguyên tố  $p$  của  $n$ . Vì  $n$  không có ước số chính phương nên theo định lý thặng dư Trung Hoa ta có

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

Tức là  $a^n \equiv a \pmod{n}$  với mọi số nguyên  $a$ . Điều phải chứng minh.

**Ví dụ 1.4.11.** Chứng minh rằng dãy số  $1^1, 2^2, 3^3, \dots$  xét theo modulo  $p$  tuân hoà với chu kì nhỏ nhất là  $p(p - 1)$ .

### Giải

Hiển nhiên dãy đã cho tuân hoà với chu kì  $p(p - 1)$  vì

$$n^n \equiv (n + p(p - 1))^{n+p(p-1)} \pmod{p} \quad \text{với mọi } n \geq 1.$$

Ta sẽ chứng minh  $p(p - 1)$  là chu kì nhỏ nhất. Gọi  $h$  là một chu kì của dãy trên. Khi đó ta có

$$n^n \equiv (n + ph)^{n+ph} \pmod{p}.$$

Do  $n^n \equiv (n + ph)^n \pmod{p}$  nên phải có  $(n + ph)^{ph} \equiv 1 \pmod{p}$  với mọi  $(n, p) = 1$ . Chọn  $n$  là một căn nguyên thuỷ suy ra  $ph \mid p - 1$ , tức là  $h \mid p - 1$ .

Mặt khác, vì  $h$  là chu kì nên

$$n^n \equiv (n + h)^{n+h} \pmod{p}.$$

Chọn  $n \equiv 0 \pmod{p}$  suy ra  $h \equiv 0 \pmod{p}$ . Vậy  $h \mid p$  và  $p - 1$  nên  $h \mid p(p - 1)$ , tức là  $p(p - 1)$  là chu kì bé nhất. Điều phải chứng minh.

#### Ví dụ 1.4.12.

- a, Cho  $a, k$  là các số nguyên dương,  $a \geq 2$ . Chứng minh rằng  $k \mid \phi(a^k - 1)$ .
- b, Cho  $m$  là một số nguyên dương,  $p$  là một số nguyên tố sao cho  $p \mid \phi(m)$  và  $p \nmid m$ . Chứng minh rằng tồn tại ít nhất một ước số nguyên tố  $q$  của  $m$  sao cho  $q \equiv 1 \pmod{p}$ .
- c, Cho  $p$  là một số nguyên tố. Chứng minh rằng tồn tại vô số các số nguyên tố có dạng  $pk + 1$ .

#### Giải

a, Đặt  $m = a^k - 1$ . Ta có  $a^k \equiv 1 \pmod{m}$  và  $1 < a^h < m$  với mọi  $h < k$  nên  $k$  là cấp của  $a$  modulo  $m$ . Từ đó suy ra  $k \mid \phi(m)$  hay  $k \mid \phi(a^k - 1)$ .

b, Giả sử  $m = \prod_i p_i^{\alpha_i}$ . Khi đó  $\phi(m) = \prod_i [p_i^{\alpha_i-1}(p_i - 1)]$ . Do  $p \mid \phi(m)$  và  $p \nmid m$  nên  $p \mid \prod_i (p_i - 1)$ , tức là tồn tại một chỉ số  $i$  sao cho  $p_i - 1 \mid p$  hay  $p_i \equiv 1 \pmod{p}$ .

c, Giả sử có hữu hạn các số nguyên tố có dạng  $pk + 1$  là  $p_1, p_2, \dots, p_n$ .

Đặt

$$a = p \cdot p_1 \cdot p_2 \cdots p_n, \quad m = a^p - 1.$$

theo phần a, ta có  $p \mid \phi(m)$ . Mặt khác, vì  $a \nmid p$  nên  $m \nmid p$ . Từ đó, theo phần b, tồn tại một ước số nguyên tố  $q$  của  $m$  sao cho  $q \equiv 1 \pmod{p}$ . Vì  $(p_i, p) = 1$  với mọi  $i = 1, 2, \dots, n$  nên  $q \neq p_i$  với mọi  $i = 1, 2, \dots, n$ , tức là tồn tại một số nguyên tố  $q$  có dạng  $pk + 1$  không nằm trong tập  $\{p_1, p_2, \dots, p_n\}$ . Vô lý. Vậy điều giả sử là sai và ta có điều phải chứng minh.

**Ví dụ 1.4.13.** Cho  $n$  là một số nguyên dương,  $n > 1$ . Chứng minh rằng  $n \nmid 2^n - 1$ .

**Giải**

Giả sử tồn tại một số nguyên dương  $n$  sao cho  $2^n - 1 \mid n$ . Gọi  $p$  là ước số nguyên tố bé nhất của  $n$ . Vì  $2^n - 1 \mid n$  nên  $2^n - 1 \mid p$ . Gọi cấp của 2 modulo  $p$  là  $h$ , khi đó ta có  $h|(p-1)$  và  $h|n$ . Mặt khác, vì  $p$  là ước số nguyên tố bé nhất của  $n$  nên  $(p-1, n) = 1$ , suy ra  $h = 1$ . Vô lý vì  $2^1 = 2 \not\equiv 1 \pmod{2^n - 1}$ . Vậy điều giả sử là sai và ta có điều phải chứng minh.

**Ví dụ 1.4.14.**

- a, Cho  $p$  và  $q$  là các số nguyên tố sao cho tồn tại một số nguyên  $b$  thoả mãn  $1 < b < q$  và  $b^p \equiv 1 \pmod{q}$ . Chứng minh rằng  $q - 1 \mid p$ .
- b, Cho  $b$  là một số nguyên,  $p$  là một số nguyên tố. Chứng minh rằng mọi ước số nguyên tố của  $b^p - 1$  đều lớn hơn  $p$ .

**Giải**

- a, Gọi  $h$  là cấp của  $b$  modulo  $q$ . Hiển nhiên  $h > 1$  và  $q - 1 \mid h$ . Do  $b^p - 1 \mid q$  nên theo tính chất của cấp ta có  $p \mid h$ . Vì  $p$  là một số nguyên tố và  $h > 1$  nên  $p = h$ , do đó  $p$  là ước số của  $q - 1$ .
- b, Gọi  $q$  là một ước số nguyên tố bất kỳ của  $b^p - 1$ , khi đó  $b^p \equiv 1 \pmod{q}$  nên theo phần a, ta có  $q \equiv 1 \pmod{p}$ , tức là  $q > p$ . Vì  $q$  được chọn bất kỳ nên suy ra mọi ước số nguyên tố của  $b^p - 1$  đều lớn hơn  $p$ . Điều phải chứng minh.

## BÀI TẬP

**Bài 1.** Cho  $p, q$  là các số nguyên tố khác nhau sao cho tồn tại một số nguyên dương  $b$  thoả mãn

$$b^{q-1} + b^{q-2} + \cdots + 1 \vdots p.$$

Chứng minh rằng  $p \equiv 1 \pmod{q}$ .

**Bài 2.** Cho  $b$  là một số nguyên. Chứng minh rằng tồn tại vô số cặp số nguyên tố  $(p, q)$  thoả mãn

$$\frac{q-1}{p} = k \in \mathbb{Z}, \quad b \text{ là luỹ thừa bậc } k \pmod{p}.$$

**Bài 3.** Cho  $b, t, k$  là các số nguyên dương lớn hơn 1. Chứng minh rằng điều kiện cần và đủ để tồn tại một số nguyên dương  $n$  thoả mãn

$$b^{t-1} \leq n < b^t, \quad n^k \equiv n \pmod{b^t}$$

là một trong hai điều sau xảy ra

i,  $b$  không là luỹ thừa của một số nguyên tố,

ii,  $(k-1, \phi(b^t)) > 1$ .

**Bài 4.** Cho  $p$  là một số nguyên tố,  $h > 1$  là một ước số của  $p-1$ .

a, Chứng minh rằng có  $\phi(h)$  phân tử có cấp  $h$  theo modulo  $p$ . (gọi là  $r_1, r_2, \dots, r_{\phi(h)}$ )

b, Chứng minh rằng

$$r_1 + r_2 + \cdots + r_{\phi(h)} \equiv \mu(h) \pmod{p},$$

trong đó  $\mu(h)$  là hàm Möbius.

c, Chứng minh rằng

$$r_1^k + r_2^k + \cdots + r_{\phi(h)}^k \equiv \sum_{d|(h,k)} d\mu(h/d) \pmod{p}.$$

**Bài 5.** Tìm tất cả các số nguyên  $n > 1$  sao cho

$$a^{25} - a \vdots n \quad \text{với mọi } a \in \mathbb{Z}^+.$$

**Bài 6.** Tìm tất cả các cặp số nguyên tố  $p, q$  sao cho

$$pq|(5^p - 2^p)(5^q - 2^q).$$

**Bài 7.** Tìm tất cả các cặp số nguyên tố  $p, q$  thoả mãn

$$\alpha^{3pq} \equiv \alpha \pmod{3pq} \quad \forall \alpha \in \mathbb{Z}.$$

**Bài 8.** Tìm tất cả các số nguyên  $n > 1$  sao cho  $\frac{2^n + 1}{n^2}$  là một số nguyên.

**Bài 9.** Với mỗi số nguyên  $a$  đặt

$$n_a = 101a - 100 \cdot 2^a.$$

Chứng minh rằng nếu  $0 \leq a, b, c, d \leq 99$ ,  $n_a + n_b \equiv n_c + n_d \pmod{10100}$  thì  $\{a, b\} = \{c, d\}$ .

**Bài 10 (Russia 2000).** Với mỗi số nguyên dương  $n$  gọi  $\pi(n)$  là ước số nguyên tố nhỏ nhất của  $n$ . Chứng minh rằng nếu  $p$  là một số nguyên tố,  $y$  là một số nguyên dương thoả mãn

$$2^y + 1 \vdots p, \quad p < \pi(y)$$

thì  $p = 3$ .

**Bài 11 (Russia 2000).** Có tồn tại hay không các số nguyên dương đôi một nguyên tố cùng nhau  $a, b, c$  thoả mãn

$$2^a + 1 \vdots b, \quad 2^b + 1 \vdots c, \quad 2^c + 1 \vdots a.$$

**Bài 12 (Romania 2000).** Cho trước biểu diễn nhị phân của một số nguyên dương lẻ  $a$ , tìm một thuật toán đơn giản để xác định số nguyên dương  $n$  nhỏ nhất sao cho  $a^n - 1 \vdots 2^{2000}$

**Bài 13.** Cho  $b$  là một số nguyên dương thoả mãn  $b + 1 = q$  là số nguyên tố. Với mỗi số nguyên  $y$  kí hiệu  $\pi(y)$  là ước số nguyên tố nhỏ nhất của  $y$ . Chứng minh rằng nếu tồn tại một số nguyên dương  $y$  và một số nguyên tố  $p \leq \pi(y)$  sao cho  $b^y + 1 : p$  thì  $p = q$ .

**Bài 14.** Cho  $b$  là một số nguyên dương thoả mãn  $b + 1 = q \geq 5$  là số nguyên tố. Gọi  $p$  là ước số nguyên tố lớn nhất của  $b^y + 1$ ,  $q$  là ước số nguyên tố nhỏ nhất của  $y$ . Chứng minh rằng

$$p \geq q + 2.$$

## LỜI GIẢI

### Bài 1.

Ta có

$$b^{q-1} + b^{q-2} + \cdots + 1 = \frac{b^q - 1}{b - 1}.$$

Nếu  $b \equiv 1 \pmod{p}$  thì  $b^{q-1} + b^{q-2} + \cdots + 1 \equiv q \pmod{p}$ , suy ra  $q : p$ . Vì lý do  $p, q$  là các số nguyên tố khác nhau. Vậy  $b \not\equiv 1 \pmod{p}$ . Từ đẳng thức trên ta có  $b^q - 1 : p$ . Theo ví dụ 1.4.14 suy ra  $p \equiv 1 \pmod{q}$ , điều phải chứng minh.

### Bài 2.

Chọn  $p$  là một số nguyên tố tuỳ ý. Xét số nguyên tố  $q$  thoả mãn  $q|(b^p - 1)$ , theo ví dụ 1.4.14 ta có  $p|(q - 1)$  nên tồn tại một số nguyên dương  $k$  sao cho  $q - 1 = kp$ . Gọi  $g$  là một căn nguyên thuỷ của  $q$ , khi đó tồn tại một số nguyên dương  $h$  sao cho  $b \equiv g^h \pmod{q}$ . Do  $p$  là một số nguyên tố và  $q|(b^p - 1)$  nên cấp của  $b$  modulo  $q$  là  $p$ . Mặt khác, vì  $b \equiv g^h \pmod{q}$  nên cấp của  $b$  modulo  $q$  là  $(q - 1)/(h, p - 1)$ . Từ đó ta có

$$p = \frac{q - 1}{(h, p - 1)} \quad \text{hay} \quad (h, p - 1) = \frac{q - 1}{p} = k,$$

tức là  $h : k$ . Vậy  $b$  là một luỹ thừa bậc  $k$  modulo  $p$ . Do  $p$  được chọn tuỳ ý nên suy ra có vô số cặp số nguyên tố  $(p, q)$  thoả mãn điều kiện đề bài. Điều phải chứng minh.

**Bài 3.**

Giả sử  $b^{t-1} \leq n < b^t$ ,  $n^k \equiv n \pmod{b^t}$  và  $b = p^c$  là luỹ thừa của một số nguyên tố. Vì  $n^k - n = n(n^{k-1} - 1) : p^{ct}$  và  $n < b^t = p^{ct}$  nên  $n^{k-1} - 1 \nmid p^{ct}$ . Gọi  $h$  là cấp của  $n$  modulo  $p^{ct}$ , khi đó  $h|(k-1)$  và  $h|\phi(p^{ct})$  nên

$$1 < (k-1, \phi(b^t)) = (k-1, \phi(p^{ct})) \leq h.$$

Giả sử  $b$  không phải là luỹ thừa của một số nguyên tố, theo định lý thặng dư Trung Hoa tồn tại một số nguyên  $m$ ,  $0 \leq m \leq b^t$ ,  $m \not\equiv 0, 1 \pmod{b^t}$  sao cho  $m^2 \equiv m \pmod{b^t}$ . Khi đó ta có

$$m^k \equiv m \pmod{b^t} \quad \text{và} \quad (1-m)^2 \equiv (1-m) \pmod{b^t},$$

suy ra

$$(b^t + 1 - m)^k \equiv (b^t + 1 - m) \pmod{b^t}.$$

Chọn  $n = \max\{m, b^t + 1 - m\}$  ta có  $b^{t-1} \leq n < b^t$  và  $n^k \equiv n \pmod{b^t}$ .

Giả sử  $b = p^c$  là luỹ thừa của một số nguyên tố và tồn tại một ước số nguyên tố  $q$  chung của  $k-1$  và  $\phi(b^t) = p^{ct-1}(p-1)$ .

Nếu  $p = q$  thì  $n = 1 + p^{ct-1}$  thoả mãn  $b^{t-1} \leq n < b^t$  và  $n^k \equiv n \pmod{b^t}$ . Nếu  $p \neq q$  gọi  $a$  là một thặng dư có cấp  $q$  modulo  $p^{ct}$ , ta có  $(a, p) = 1$  và

$$a^q - 1 = (a-1)(a^{q-1} + a^{q-2} + \cdots + 1) : p^{ct}.$$

nên

$$a^{q-1} + a^{q-2} + \cdots + 1 \nmid p^{ct}.$$

Từ đó suy ra có ít nhất một số  $a^i \equiv n \pmod{p^{ct}}$  với  $(p^{ct}-1)/(p-1) \leq n \leq p^{ct} = b^t$ . Vì  $q < p$  nên

$$\frac{p^{ct} - 1}{q - 1} > \frac{p^{ct} - 1}{p - 1} > p^{ct-1} \geq p^{c(t-1)} = b^{t-1}.$$

Do đó,  $n$  thoả mãn  $b^{t-1} \leq n < b^t$  và  $n^k \equiv n \pmod{b^t}$ . Điều phải chứng minh.

**Bài 4.**

a, Giả sử  $g$  là một căn nguyên thuỷ của  $p$ . Khi đó, mỗi lớp thặng

dư có cấp  $h$  modulo  $p$  đều có dạng  $g^{[(p-1)/h]t}$  với  $1 \leq t \leq h$  và  $(t, h) = 1$ . Từ đó suy ra số các phương trình có cấp  $h$  là  $\phi(h)$ .

b, Gọi  $F(h)$  là tổng của  $h$  thặng dư phân biệt thoả mãn phương trình  $x^h \equiv 1 \pmod{p}$ . Với  $h = 1$  ta có  $F(1) = 1$ . Với  $h > 1$ , vì  $F(h)$  là tổng các nghiệm của  $P(x) = x^h - 1 \equiv 0 \pmod{p}$  nên theo định lý Viète,  $F(h)$  đồng dư với số đối của hệ số của  $x^{h-1}$  trong đa thức  $P(x)$ . Do đó  $F(h) \equiv 0 \pmod{p}$  với mọi  $h > 1$ .

Gọi  $f(h)$  là tổng của  $\phi(h)$  thặng dư có cấp  $h$  modulo  $p$ . Ta có

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

Từ chứng minh trên và theo công thức ngược ta có

$$f(h) = \sum_{d|h} F(d) \equiv \mu\left(\frac{h}{l}\right) F(1) \equiv \mu(h) \pmod{p}$$

c, Tương tự câu b.,

### Bài 5.

Đặt  $N = 2.3.5.7.13$ . Ta chứng minh  $n$  thoả mãn điều kiện đề bài khi và chỉ khi  $n$  là một ước số của  $N$ .

Bằng định lý Fermat, dễ kiểm tra

$$a^{25} - a = a(a^{24} - 1) : N \quad \text{với mọi } a \in Z^+.$$

Do đó mọi ước số của  $N$  đều thoả mãn tính chất đề bài.

Giả sử tồn tại một số nguyên dương  $n$  không là ước số của  $N$  thoả mãn điều kiện đề bài.

Nếu  $n$  có một ước số nguyên tố  $p$  không là ước số của  $N$ , thì tồn tại một số nguyên  $a$  là căn nguyên thuỷ của  $p$ . Khi đó,  $a^{25} - a = a(a^{24} - 1) : p$  khi và chỉ khi  $24 : p - 1$ . Vô lý.

Nếu  $n$  có một ước số chính phương  $p^2$ , xét  $a = 2$  ta có

$$2^{24} - 1 = 2.3^2.5.7.13.241$$

nên  $p$  chỉ có thể bằng 3. Xét  $a = 3$  suy ra vô lý. Vậy  $n$  phải là một ước số của  $N$ .

**Bài 6.**

Giả sử  $p, q$  là hai số nguyên tố thoả mãn điều kiện đề bài và  $p \leq q$ .

Nếu  $p|(5^p - 2^p)$  thì  $p = 3$  vì theo định lý Fermat,  $5^p - 2^p \equiv 5 - 2 = 3 \pmod{p}$ . Khi đó  $q = 3$  hoặc  $q = 13$ .

Nếu  $p|(5^q - 2^q)$  và  $q|(5^p - 2^p)$  thì tồn tại các số nguyên dương  $a, b$  sao cho  $5 \equiv 2a \pmod{p}$ ,  $2 \equiv 5b \pmod{q}$ . Khi đó

$$a^q \equiv 1 \pmod{p} \quad \text{và} \quad b^p \equiv 1 \pmod{q}.$$

Do  $p, q$  là các số nguyên tố nên  $q$  là cấp của  $a$  modulo  $p$ ,  $p$  là cấp của  $b$  modulo  $q$ . Do đó  $p - 1 : q$  và  $q - 1 : p$ . Vô lý.

Vậy có hai cặp  $(p, q) = (3, 3), (3, 13)$  thoả mãn điều kiện đề bài.

**Bài 7.**

Giả sử  $p \leq q$  là các số thoả mãn điều kiện đề bài.

Do  $\alpha^{3pq} \equiv \alpha \pmod{3}$  với mọi số nguyên  $\alpha$  nên nếu chọn  $\alpha = -1$  suy ra cả  $p$  và  $q$  đều là các số lẻ.

Do  $\alpha^{3pq} \equiv \alpha \pmod{p}$  với mọi số nguyên  $\alpha$  nên nếu chọn  $\alpha$  là một căn nguyên thuỷ của  $p$  ta có  $3pq - 1 : p - 1$ .

Do  $\alpha^{3pq} \equiv \alpha \pmod{q}$  với mọi số nguyên  $\alpha$  nên nếu chọn  $\alpha$  là một căn nguyên thuỷ của  $q$  ta có  $3pq - 1 : q - 1$ .

Vậy  $3pq - 1 : p - 1$  và  $3pq - 1 : q - 1$ . Do  $3pq - 1 = 3q(p - 1) + 3q - 1 = 3p(q - 1) + 3p - 1$  nên  $3p - 1 : q - 1$  và  $3q - 1 : p - 1$ .

Nếu  $p = q$  thì  $3p - 1 : p - 1$  nên suy ra  $p = q = 3$ . Thay vào không thoả mãn vì  $4^{27} \equiv 1 \pmod{27}$ .

Nếu  $q \geq p + 2$  thì  $(3p - 1)/(q - 1) < 3$  nên  $3p - 1 = 2(q - 1)$  hay  $2q = 3p + 1$ , do đó

$$3q - 1 = \frac{9p + 1}{2} : p - 1 \quad \text{và} \quad (9p + 1) - (9p - 9) = 10 : p - 1$$

suy ra  $p = 11$ ,  $q = 17$ . Thay vào thấy thoả mãn điều kiện đề bài.

**Bài 8.**

Giả sử  $n > 1$  thoả mãn  $(2^n + 1)/n^2$  là một số nguyên, khi đó  $2^n + 1 : n^2$ .

Do  $2^n + 1$  lẻ nên  $n$  phải là một số lẻ. Gọi  $p$  là ước số nguyên tố nhỏ nhất của  $n$  và  $h$  là cấp của 2 modulo  $p$ . Ta có  $2^n \equiv -1 \pmod{p}$  nên  $2^{2n} \equiv 1 \pmod{p}$ . Từ đó suy ra  $2n : h$  và  $p - 1 : h$  hay  $(2n, p - 1) : h$ . Do  $p$  là ước

số nguyên tố nhỏ nhất của  $n$  nên  $(n, p-1) = 1$ , tức là  $(2n, p-1) = 2 : h$ , suy ra  $h = 2$  và  $p = 3$ .

Giả sử  $n = 3^k d$  với  $(d, 3) = 1$ . Vì  $2^n + 1 \vdots n^2$  nên  $2^{2n} \equiv 1 \pmod{3^{2k}}$ . Do 2 là một căn nguyên thuỷ của  $3^{2k}$  nên  $2n \vdash \phi(3^{2k})$  hay  $2 \cdot 3^k \cdot d \vdash 2 \cdot 3^{2k-1}$ , suy ra  $k \geq 2k-1$  hay  $k \leq 1$ . Vậy  $k = 1$ ,  $n = 3d$  với  $(d, 3) = 1$ .

Giả sử  $d > 1$ . Gọi  $q$  là ước số nguyên tố nhỏ nhất của  $d$ , khi đó do  $(3, d) = 1$  nên  $q \leq 5$ . Gọi  $k$  là cấp của 2 modulo  $q$ . Ta có  $2^n \equiv -1 \pmod{q}$  nên  $2^{2n} \equiv 1 \pmod{q}$ . Từ đó suy ra  $2n = 6d \vdash k$  và  $q-1 \vdash k$  hay  $(6d, q-1) \vdash k$ . Do  $q$  là ước số nguyên tố nhỏ nhất của  $d$  nên  $(d, q-1) = 1$ , tức là  $(6d, q-1) = 2 \vdash k$ , suy ra  $k = 2$  và  $2^2 = 4 \equiv 1 \pmod{q}$  với  $q > 5$ . Vô lý. Vậy điều giả sử là sai nên  $d = 1$  và  $n = 3$ . Thủ lại thấy  $n = 3$  đúng.

### Bài 9.

Giả sử  $a, b, c, d$  là các số nguyên thoả mãn  $0 \leq a, b, c, d \leq 99$  và  $n_a + n_b \equiv n_c + n_d \pmod{10100}$ . Theo định lý thặng dư Trung Hoa ta có

$$a + b \equiv c + d \pmod{100} \quad \text{và} \quad 2^a + 2^b \equiv 2^c + 2^d \pmod{101}.$$

Theo định lý Fermat, từ  $a + b \equiv c + d \pmod{100}$  ta có  $2^a 2^b \equiv 2^c 2^d \pmod{101}$ . Do  $2^b \equiv 2^c + 2^d - 2^a \pmod{101}$  nên

$$2^a (2^c + 2^d - 2^a) \equiv 2^c 2^d \pmod{101} \quad \text{hay} \quad (2^a - 2^c)(2^a - 2^d) \equiv 0 \pmod{101}.$$

Do 2 là một căn nguyên thuỷ modulo 101 nên  $(2^a - 2^c)(2^a - 2^d) \equiv 0 \pmod{101}$  khi và chỉ khi  $a \equiv c \pmod{100}$  hoặc  $a \equiv d \pmod{100}$ . Vì  $0 \leq a, b, c, d \leq 99$  nên suy ra  $a = c$  hoặc  $a = d$ . Từ cả hai trường hợp này đều suy ra điều phải chứng minh.

### Bài 10 (Russia 2000).

Gọi  $h$  là cấp của 2 modulo  $p$ . Vì  $h \leq p-1$  nên  $h < \pi(y)$  và  $(h, y) = 1$ .  
Mặt khác,

$$2^{2y} - 1 = (2^y - 1)(2^y + 1) \vdash p$$

nên  $2y \vdash h$ . Vì  $(h, y) = 1$  nên  $2 \vdash h, h > 1$ , suy ra  $h = 2$ , tức là  $2^2 - 1 = 3 \vdash p$ . Vậy  $p = 3$ , ta có điều phải chứng minh.

**Bài 11 (Russia 2000).**

Ta sẽ chứng minh không tồn tại các số nguyên dương  $a, b, c$  thoả mãn điều kiện đề bài. Phản chứng, giả sử tồn tại các số nguyên dương đôi một nguyên tố cùng nhau  $a, b, c \geq 1$  thoả mãn

$$2^a + 1 \mid b, \quad 2^b + 1 \mid c, \quad 2^c + 1 \mid a.$$

Khi đó cả ba số  $a, b, c$  đều lẻ. Vì  $a, b, c$  đôi một nguyên tố cùng nhau nên  $\pi(a), \pi(b), \pi(c)$  là ba số nguyên phân biệt. Không mất tính tổng quát ta có thể giả sử

$$\pi(b), \pi(c) > \pi(a).$$

Theo ví dụ trên với  $(p, y) = (\pi(a), c)$  ta có  $\pi(a) = 3$ .

Đặt  $a = 3a_0$ , ta sẽ chứng minh  $a_0 \mid 3$ . Thực vậy:

Nếu  $a_0 \nmid 3$  thì  $2^c + 1 \mid 9$ , suy ra  $2^{2c} - 1 \mid 9$  hay  $2c \mid 6$  và  $c \mid 3$ . Từ đó suy ra  $(a, c) \mid 3$ , mâu thuẫn với giả thiết  $(a, c) = 1$  nên điều giả sử là sai.

Vậy  $(a_0, 3) = 1$ .

Đặt  $q = \pi(a_0bc)$ , ta có  $q = \pi(q) \leq \min\{\pi(b), \pi(c)\}$ . Ta sẽ chứng minh  $b \mid q$ .

- Nếu  $a_0 \mid q$ , áp dụng ví dụ trên với  $(p, y) = (q, c)$  ta có  $q = 3$ , tức là  $a_0 \mid 3$ . Vô lý.
- Nếu  $c \mid q$  thì do  $(b, c) = 1$ ,  $q = \pi(c) < \pi(b)$ . Do đó, áp dụng ví dụ trên với  $(p, y) = (q, b)$  ta có  $q = 3$ , vô lý.

Vậy  $b \mid q$ , tức là  $2^a + 1 \mid q$ . Gọi  $h$  là cấp của 2 modulo  $q$  ta có  $h \leq q - 1$  nên  $\pi(a_0) > q > h$  và  $(a_0, h) = 1$ . Do

$$2^{2a} - 1 = (2^a - 1)(2^a + 1) \mid q$$

nên  $2a \mid h$ , tức là  $6a_0 \mid h$ . Vì  $(a_0, h) = 1$  nên  $6 \mid h$ , suy ra  $2^6 - 1 = 63 \mid q$  nên  $q = 7$ . Mặt khác

$$2^a + 1 = (2^3)^{a_0} + 1 \equiv 8^{a_0} + 1 \equiv 2 \pmod{7},$$

vô lý. Vậy điều giả sử là sai và ta có điều phải chứng minh.

**Bài 12 (Romania 2000).**

Vì  $a$  lẻ nên  $(a, 2^k) = 1$  với mọi  $k \geq 0$ , theo định lý Euler

$a^{2^{k-1}} \equiv a^{\phi(2^k)} \equiv 1 \pmod{2^k}$  với mọi  $k \geq 0$ . Do đó, cấp  $n$  của  $a$  modulo  $2^{2000}$  là một ước số của  $2^{2000-1} = 2^{1999}$ .

Nếu  $a \equiv 1 \pmod{2000}$  thì  $n = 1$ , nên có thể giả sử  $a \not\equiv 1 \pmod{2000}$ . Với mỗi số nguyên dương  $m$  ta có

$$a^{2^m} - 1 = (a - 1)(a + 1)(a^2 + 1)(a^{2^2} + 1) \cdots (a^{2^{m-1}} + 1).$$

Do  $a$  lẻ,  $a^{2^k} \equiv 1 \pmod{4}$  với mọi  $k \geq 1$  nên ước số lớn nhất của  $(a^2 + 1)(a^{2^2} + 1) \cdots (a^{2^{m-1}} + 1)$  có dạng luỹ thừa của 2 là  $2^{m-1}$ .

Nếu trong biểu diễn nhị phân  $a$  có tận cùng dạng

$$\underbrace{100 \cdots 01}_{k \text{ chữ số}}$$

thì luỹ thừa lớn nhất của 2 là ước số của  $a - 1$  là  $2^k$ , luỹ thừa lớn nhất của 2 là ước số của  $a + 1$  là 2.

Nếu trong biểu diễn nhị phân  $a$  có tận cùng dạng

$$\underbrace{011 \cdots 1}_{k \text{ chữ số}}$$

thì luỹ thừa lớn nhất của 2 là ước số của  $a - 1$  là 2, luỹ thừa lớn nhất của 2 là ước số của  $a + 1$  là  $2^k$ .

Trong mọi trường hợp, ta đều xác định được ước số lớn nhất của  $a^{2^m} - 1$  là  $2^{m+k}$ .

Nếu  $k < 2000$  thì số nguyên  $m$  nhỏ nhất sao cho  $a^{2^m} - 1 : 2^{2000}$  là  $2000 - k$ , khi đó  $n = 2^{2000-k}$ .

Nếu  $k \geq 2000$  thì số nguyên  $m$  nhỏ nhất sao cho  $a^{2^m} - 1 : 2^{2000}$  là 1 (do ta đang xét  $a \not\equiv 1 \pmod{2^{2000}}$ ), khi đó  $n = 2$ .

### Bài 13.

Gọi  $h$  là cấp số của  $b$  modulo  $p$

- Vì  $h|(p-1)$  nên  $h < \pi(p)$  và  $(h, p) = 1$ .

- Vì  $b^y + 1 \vdots p$  nên  $b^{2y} \equiv 1 \pmod{p}$  suy ra  $2y \vdash h$  (theo tính chất của cấp).

Từ đó suy ra  $h = 2$ , tức là  $b^2 - 1 = q(q-2) \vdash p$ . Mặt khác, do  $b$  chẵn nên  $(b^y - 1, b^y + 1) = 1 = (b-1, b^y + 1) = (q-2, b^y + 1) = (q-2, p)$ . Vậy ta có  $q(q-2) \vdash p$  và  $(q-2, p) = 1$  nên suy ra  $q \vdash p$ . Vì  $p, q$  là các số nguyên tố nên  $p = q$ .

#### Bài 14.

Từ ví dụ trên, nếu  $p \leq q$  thì mọi ước số của  $b^y + 1$  đều bằng  $q$ , tức là tồn tại số nguyên dương  $n$  sao cho

$$b^y + 1 = q^n \quad \text{hay} \quad (q-1)^y + 1 = q^n.$$

Dễ thấy  $y$  lẻ và  $(q-1)^{2y} \equiv 1 \pmod{q^n}$  nên  $2y \vdash ord_{q^n}(q-1)$ , ở đây  $ord_{q^n}(q-1)$  là bậc số của  $(q-1)$  modulo  $q^n$ . Mặt khác,  $ord_q(q-1) = 2$  nên  $ord_{q^n}(q-1) = 2q^{n-1}$ . Do đó,  $2y \vdash 2q^{n-1}$  hay  $y \vdash q$ . Vì  $y$  lẻ,  $(q-1)^y + 1 \vdash (q-1)^q + 1$  nên tồn tại số nguyên dương  $m$  sao cho

$$(q-1)^q + 1 = q^m.$$

Vì  $q \geq 5$  thì  $(q-1)^q + 1 \geq (q-1)^5 \geq q^3$  nên  $m \geq 3$ . Xét theo modulo  $q^3$  ta có

- $(q-1)^q + 1 = \sum_{i=1}^q C_q^i (-1)^i q^{q-i} \equiv q^2 \pmod{q^3}$  do  $C_q^i \vdash q$  với mọi  $i = 1, 2, \dots, q-1$ .
- $q^m \equiv 0 \pmod{q^3}$ .

Vô lý. Vậy điều giả sử là sai và ta có điều phải chứng minh.

## 5 Thặng dư toàn phương

Mục đích chính của phần này là trả lời câu hỏi khi nào thì phương trình  $x^2 \equiv a \pmod{m}$  có nghiệm. Nhờ định lý thặng dư Trung Hoa, ta có thể đưa câu hỏi này về dạng đơn giản hơn là khi nào thì phương trình  $x^2 \equiv q \pmod{p}$  có nghiệm, trong đó  $p, q$  là các số nguyên tố. Kết quả quan trọng nhất của phần này là Luật thuận nghịch bình phương, khẳng định rằng hai phương trình

$$x^2 \equiv q \pmod{p}, \quad x^2 \equiv p \pmod{q}$$

luôn cùng có nghiệm, hoặc cùng không có nghiệm, trừ trường hợp cả  $p$  và  $q$  cùng có dạng  $4k + 3$ . Trong trường hợp đó, có đúng một trong hai phương trình trên có nghiệm.

### 5.1 Thặng dư toàn phương

#### Định nghĩa 1.5.1.

Số nguyên dương  $a$  thoả mãn  $(a, m) = 1$  được gọi là một thặng dư toàn phương modulo  $m$  nếu phương trình  $x^2 \equiv a \pmod{m}$  có nghiệm.

Để thấy rằng  $a$  là một thặng dư toàn phương modulo  $m$  nếu và chỉ nếu  $a + m$  là thặng dư toàn phương modulo  $m$ , tức là nếu một phân tử của một lớp thặng dư (modulo  $m$ ) là thặng dư toàn phương modulo  $m$  thì mọi phân tử của lớp thặng dư đó đều là thặng dư toàn phương modulo  $m$ . Do đó, khi xét các thặng dư toàn phương modulo  $m$  ta chỉ cần xét các lớp thặng dư thu gọn modulo  $m$ . Chẳng hạn 1, 4 là các thặng dư toàn phương modulo 5; 2, 3 không là thặng dư toàn phương modulo 5.

#### Định nghĩa 1.5.2.

Cho  $a$  là một số nguyên,  $p$  là một số nguyên tố lẻ, ta định nghĩa kí hiệu Legendre như sau

$$\left[ \frac{a}{p} \right] = \begin{cases} 1 & \text{nếu } a \text{ là một thặng dư toàn phương modulo } p, \\ -1 & \text{nếu } a \text{ không là một thặng dư toàn phương modulo } p, \\ 0 & \text{nếu } a \vdots p. \end{cases}$$

**Định lý 1.5.1.**

Cho  $p$  là một số nguyên tố. Khi đó

$$1. \left[ \begin{matrix} a \\ p \end{matrix} \right] \equiv a^{(p-1)/2} \pmod{p},$$

$$2. \left[ \begin{matrix} a \\ p \end{matrix} \right] \left[ \begin{matrix} b \\ p \end{matrix} \right] = \left[ \begin{matrix} ab \\ p \end{matrix} \right].$$

**Chứng minh**

1. Nếu  $\left[ \begin{matrix} a \\ p \end{matrix} \right] = 1$  thì phương trình  $x^2 \equiv a \pmod{p}$  có nghiệm, gọi  $x_0$  là một nghiệm của phương trình. Khi đó

$$a^{(p-1)/2} \equiv (p-1)! \equiv -1 \equiv \left[ \begin{matrix} a \\ p \end{matrix} \right] \pmod{p}.$$

Phân 1 của định lý được chứng minh.

2. Trực tiếp suy ra từ 1,. Ta có

$$\left[ \begin{matrix} a \\ p \end{matrix} \right] \left[ \begin{matrix} b \\ p \end{matrix} \right] \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv (ab)^{(p-1)/2} \equiv \left[ \begin{matrix} ab \\ p \end{matrix} \right] \pmod{p}.$$

Định lý được chứng minh.

**Định lý 1.5.2 (Bổ đề Gauss).**

Cho  $a$  là một số nguyên,  $p$  là một số nguyên tố lẻ. Xét các số nguyên

$$a, 2a, 3a, \dots, \frac{(p-1)a}{2}$$

và các lớp thặng dư dương nhỏ nhất của chúng. Gọi  $n$  là số các lớp thặng dư vượt quá  $p/2$ . Khi đó

$$\left[ \begin{matrix} a \\ p \end{matrix} \right] = (-1)^n.$$

**Chứng minh**

Gọi  $r_1, r_2, \dots, r_n$  là các thặng dư lớn hơn  $p/2$ ,  $s_1, s_2, \dots, s_k$  là các thặng dư còn lại. Ta có các số  $r_1, r_2, \dots, r_n, s_1, s_2, \dots, s_k$  phân biệt và

$$n+k = (p-1)/2.$$

Ta sẽ chứng minh rằng

$$\{p-r_1, p-r_2, \dots, p-r_n, s_1, s_2, \dots, s_k\} = \{1, 2, \dots, \frac{p-1}{2}\}.$$

Do các phần tử của tập hợp  $\{p-r_1, p-r_2, \dots, p-r_n, s_1, s_2, \dots, s_k\}$  đều nằm trong tập  $\{1, 2, \dots, (p-1)/2\}$  và  $n+k = (p-1)/2$  nên ta chỉ cần chứng minh các phần tử của tập hợp  $\{p-r_1, p-r_2, \dots, p-r_n, s_1, s_2, \dots, s_k\}$  phân biệt. Thật vậy, ta có

- $r_1, r_2, \dots, r_n, s_1, s_2, \dots, s_k$  phân biệt.
- Nếu tồn tại  $i, j$  sao cho  $p-r_i = s_j$  thì tồn tại hai số nguyên  $l_i, m_j$  thoả mãn  
 $r_i = l_i a, s_j = m_j a, \quad 0 \leq l_i \neq m_j \leq (p-1)/2$  và  
 $p = r_i + s_j = (l_i + m_j)a$ , tức là  $p \vdots l_i + m_j$ . Vô lý.

Từ đó suy ra  $\{p-r_1, p-r_2, \dots, p-r_n, s_1, s_2, \dots, s_k\} = \{1, 2, \dots, \frac{p-1}{2}\}$  và

$$(p-r_1)(p-r_2) \cdots (p-r_n)s_1s_2 \cdots s_k = \left(\frac{p-1}{2}\right)!.$$

Do đó,

$$\begin{aligned} (-r_1)(-r_2) \cdots (-r_n)s_1s_2 \cdots s_k &\equiv \left(\frac{p-1}{2}\right)! \pmod{p}, \\ (-1)^n r_1 r_2 \cdots r_n s_1 s_2 \cdots s_k &\equiv \left(\frac{p-1}{2}\right)! \pmod{p}, \\ (-1)^n \left(\frac{p-1}{2}\right)! a^{(p-1)/2} &\equiv \left(\frac{p-1}{2}\right)! \pmod{p}. \end{aligned}$$

Từ đó suy ra,

$$(-1)^n \equiv a^{(p-1)/2} = \begin{bmatrix} a \\ p \end{bmatrix} \pmod{p}.$$

Định lý được chứng minh.

Từ định lý trên ta có ngay hệ quả sau

**Hệ quả 1.5.3.**

Cho  $p$  là một số nguyên tố lẻ. Khi đó

$$\begin{bmatrix} -1 \\ p \end{bmatrix} = (-1)^{(p-1)/2}.$$

Tức là

$$\begin{bmatrix} -1 \\ p \end{bmatrix} = \begin{cases} 1 & \text{nếu } p \equiv 1 \pmod{4}, \\ -1 & \text{nếu } p \equiv 3 \pmod{4}. \end{cases}$$

### Chứng minh

Suy ra trực tiếp từ định lý 1.5.1.

### Định lý 1.5.4.

Cho  $p$  là một số nguyên tố lẻ. Khi đó

$$\begin{bmatrix} 2 \\ p \end{bmatrix} = (-1)^{(p^2-1)/8}.$$

Tức là

$$\begin{bmatrix} 2 \\ p \end{bmatrix} = \begin{cases} 1 & \text{nếu } p \equiv 1 \text{ hoặc } 7 \pmod{8}, \\ -1 & \text{nếu } p \equiv 3 \text{ hoặc } 5 \pmod{8}. \end{cases}$$

### Chứng minh

Nếu  $p \equiv 1$  hoặc  $5 \pmod{8}$  thì ta có

$$\begin{aligned} 2^{(p-1)/2} \left( \frac{p-1}{2} \right)! &\equiv 2 \cdot 4 \cdot 6 \cdots (p-1) \\ &\equiv 2 \cdot 4 \cdot 6 \cdots \left( \frac{p-1}{2} \right) \cdot \left( -\frac{p-3}{2} \right) \cdots (-5) \cdot (-3) \cdot (-1) \\ &\equiv (-1)^{(p-1)/4} \left( \frac{p-1}{2} \right)! \pmod{p}. \end{aligned}$$

Do đó, với mọi số nguyên tố  $p \equiv 1$  hoặc  $5 \pmod{8}$ ,

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

Theo định lý 1.5.2 ta có

$$\begin{bmatrix} 2 \\ p \end{bmatrix} = 1 \text{ nếu } p \equiv 1 \pmod{8}, \quad \begin{bmatrix} 2 \\ p \end{bmatrix} = -1 \text{ nếu } p \equiv 5 \pmod{8}.$$

Tương tự, nếu  $p \equiv 3$  hoặc  $7 \pmod{8}$  ta có

$$\begin{aligned} 2^{(p-1)/2} \left(\frac{p-1}{2}\right)! &\equiv 2.4.6.\dots.(p-1) \\ &\equiv 2.4.6.\dots.\left(\frac{p-3}{2}\right).\left(-\frac{p-1}{2}\right).\dots.(-5).(-3).(-1) \\ &\equiv (-1)^{(p+1)/4} \left(\frac{p-1}{2}\right)! \pmod{p}. \end{aligned}$$

Do đó, với mọi số nguyên tố  $p \equiv 3$  hoặc  $7 \pmod{8}$ ,

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

Theo định lý 1.5.2 ta có

$$\left[\frac{2}{p}\right] = 1 \text{ nếu } p \equiv 7 \pmod{8}, \quad \left[\frac{2}{p}\right] = -1 \text{ nếu } p \equiv 3 \pmod{8}.$$

Trong chứng minh trên có thể sử dụng trực tiếp định lý 1.5.2 với  $a = 2$ . Khi đó, số  $n$  trong định lý 1.5.2 chính là số các số chẵn nằm trong khoảng  $(p/2, p)$  và ta có:

Nếu  $p \equiv 1$  hoặc  $5 \pmod{8}$  thì  $(p-1)/2$  là một số chẵn, nên số các số chẵn nằm trong khoảng  $(p/2, p)$  là

$$\frac{(p-1) - \frac{p-1}{2}}{2} = \frac{p-1}{4}.$$

Nếu  $p \equiv 3$  hoặc  $7 \pmod{8}$  thì  $(p-3)/2$  là một số chẵn, nên số các số chẵn nằm trong khoảng  $(p/2, p)$  là

$$\frac{(p-1) - \frac{p-3}{2}}{2} = \frac{p+1}{4}.$$

Từ đó theo định lý 1.5.2

$$\begin{aligned} 2^{(p-1)/2} &\equiv (-1)^{(p-1)/4} \pmod{p} \text{ nếu } p \equiv 1 \text{ hoặc } 5 \pmod{8}, \\ 2^{(p-1)/2} &\equiv (-1)^{(p+1)/4} \pmod{p} \text{ nếu } p \equiv 3 \text{ hoặc } 7 \pmod{8}. \end{aligned}$$

## 5.2 Luật thuận nghịch bình phương

**Định lý 1.5.5.**

Cho  $a$  là một số nguyên lẻ,  $p$  là một số nguyên tố lẻ thoả mãn  $(a, 2p) = 1$ . Khi đó

$$\left[ \begin{matrix} a \\ p \end{matrix} \right] = (-1)^t, \quad \text{với } t = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor.$$

### Chứng minh

Sử dụng các kí hiệu trong định lý 1.5.2. Vì

$$ja \equiv ja - p \left\lfloor \frac{ja}{p} \right\rfloor \pmod{p}, \quad 0 \leq ja - p \left\lfloor \frac{ja}{p} \right\rfloor \leq p - 1$$

nên  $ja - p \left\lfloor \frac{ja}{p} \right\rfloor$  là số dư trong phép chia  $ja$  cho  $p$ . Do đó,

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^n r_j + \sum_{j=1}^k s_j.$$

Mặt khác, từ chứng minh định lý 1.5.2 ta có

$$\{p - r_1, p - r_2, \dots, p - r_n, s_1, s_2, \dots, s_k\} = \{1, 2, \dots, \frac{p-1}{2}\} \text{ nên}$$

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^n (p - r_j) + \sum_{j=1}^k s_j = np - \sum_{j=1}^n r_j + \sum_{j=1}^k s_j.$$

Trừ vế với vế của hai đẳng thức trên ta thu được

$$(a-1) \sum_{j=1}^{(p-1)/2} j = p \left( \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor - n \right) + 2 \sum_{j=1}^n r_j.$$

Do  $a$  lẻ và

$$\sum_{j=1}^{(p-1)/2} j = \frac{p^2 - 1}{8}$$

nên

$$(a-1) \frac{p^2 - 1}{8} \equiv \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor - n \equiv 0 \pmod{2}.$$

Suy ra  $n \equiv \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor = t \pmod{2}$ . Từ định lý 1.5.2 ta có điều phải chứng minh.

### **Định lý 1.5.6 (Luật thuận nghịch bình phương Gauss).**

Cho  $p, q$  là hai số nguyên tố lẻ khác nhau. Khi đó

$$\begin{bmatrix} p \\ q \end{bmatrix} \begin{bmatrix} q \\ p \end{bmatrix} = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

### **Chứng minh**

Từ định lý 1.5.5, định lý sẽ được chứng minh nếu ta chứng minh được rằng

$$\sum_{j=1}^{(p-1)/2} \left\lfloor \frac{qj}{p} \right\rfloor + \sum_{j=1}^{(q-1)/2} \left\lfloor \frac{pj}{q} \right\rfloor = \frac{p-1}{2} \frac{q-1}{2}.$$

Đặt

$$S = \{(x, y) : 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}\}.$$

Khi đó,  $S$  có  $(p-1)(q-1)/4$  phân tử và không có phân tử  $(x, y) \in S$  thoả mãn  $qx = py$ . Xét phân hoạch  $S = S_1 \cup S_2$  với

$$S_1 = \{(x, y) \in S : py < qx\}, \quad S_2 = \{(x, y) \in S : qx < py\}.$$

Ta có

$$S_1 = \{(x, y) : 1 \leq x \leq \frac{p-1}{2}, 1 \leq y < \frac{qx}{p}\} = \{(x, y) : 1 \leq x \leq \frac{p-1}{2},$$

$$1 \leq y \leq \left\lfloor \frac{qx}{p} \right\rfloor\},$$

$$S_2 = \{(x, y) : 1 \leq y \leq \frac{q-1}{2}, 1 \leq x < \frac{py}{q}\} = \{(x, y) : 1 \leq y \leq \frac{q-1}{2},$$

$$1 \leq x \leq \left\lfloor \frac{py}{q} \right\rfloor\}.$$

Do đó,

$$|S_1| = \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor, \quad |S_2| = \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor.$$

Vì  $|S| = |S_1| + |S_2|$  nên ta có

$$|S| = \frac{p-1}{2} \frac{q-1}{2} = |S_1| + |S_2| = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{qj}{p} \right\rfloor + \sum_{j=1}^{(q-1)/2} \left\lfloor \frac{pj}{q} \right\rfloor.$$

Tức là ta có điều phải chứng minh.

# Chương 2

## Phương trình nghiệm nguyên

### 1 Phương trình Pythagore

Trong mục này ta sẽ tìm tất cả các nghiệm nguyên dương của phương trình sau

$$x^2 + y^2 = z^2.$$

Dễ thấy nếu  $(x_0, y_0, z_0)$  là một nghiệm của phương trình thì với mọi số nguyên dương  $k$ , bộ  $(kx_0, ky_0, kz_0)$  cũng là một nghiệm. Ngược lại, nếu  $(x_0, y_0, z_0)$  là một nghiệm của phương trình trên và  $d = (x_0, y_0, z_0)$  thì  $(x_0/d, y_0/d, z_0/d)$  cũng là một nghiệm. Do đó ta chỉ cần xét các nghiệm nguyên  $(x, y, z)$  của phương trình thoả mãn  $(x, y, z) = 1$ . Một nghiệm như thế được gọi là một bộ ba số Pythagore nguyên thuỷ. Hiển nhiên, nếu  $(x, y, z)$  là một bộ Pythagore nguyên thuỷ thì  $x, y, z$  đều là một số nguyên tố cùng nhau. Thật vậy, nếu hai trong ba số cùng chia hết cho một số nguyên dương  $d$  thì từ phương trình  $x^2 + y^2 = z^2$  suy ra số còn lại cũng chia hết cho  $d$ . Vì một số chính phương lẻ luôn chia 4 dư 1, và một số chính phương chẵn luôn chia hết cho 4 nên  $z$  là một số lẻ, và hai số  $x, y$  khác tính chẵn lẻ. Định lý sau đây cho phép tìm tất cả các bộ Pythagore nguyên thuỷ.

**Định lý 2.1.1.**

Giả sử  $(x, y, z)$  là một bộ Pythagore nguyên thuỷ với  $x$  chẵn. Khi đó tồn tại hai số nguyên dương nguyên tố cùng nhau  $m, n$  thoả mãn

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2.$$

Ngược lại, nếu tồn tại hai số nguyên dương nguyên tố cùng nhau  $m, n$  sao cho

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2.$$

thì  $(x, y, z)$  là một bộ Pythagore nguyên thuỷ.

### Chứng minh

Giả sử  $(x, y, z)$  là một bộ Pythagore nguyên thuỷ với  $x$  chẵn, ta có

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

Vì  $(z, y) = 1$  nên

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

do đó tồn tại hai số nguyên dương nguyên tố cùng nhau  $m, n$  sao cho

$$\frac{z+y}{2} = m^2, \quad \frac{z-y}{2} = n^2.$$

Từ đó suy ra

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2.$$

Ngược lại, nếu tồn tại hai số nguyên dương nguyên tố cùng nhau  $m, n$  sao cho

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2.$$

thì dễ dàng kiểm tra  $(x, y, z)$  là một bộ Pythagore. Cần chứng minh  $(x, y, z)$  là một bộ Pythagore nguyên thuỷ. Đặt  $(y, z) = d$ , vì  $y, z$  lẻ nên  $d$  lẻ. Mặt khác ta có

$$y + z = 2m^2 : d, \quad z - y = 2n^2 : d$$

nên  $m^2, n^2 : d$ . Vì  $(m, n) = 1$  nên  $d = 1$ , tức là  $(y, z) = 1$ . Từ đó suy ra  $(x, y) = 1$  và  $(x, z) = 1$ . Điều phải chứng minh.

**Ví dụ 2.1.1 (Bulgaria 1998).** Chứng minh rằng phương trình

$$x^4 - y^4 = z^2$$

không có nghiệm nguyên dương.

**Giải**

Phản chứng, giả sử phương trình đã cho có nghiệm nguyên dương. Gọi  $(a, b, c)$  là nghiệm nguyên dương của phương trình có  $a$  nhỏ nhất. Khi đó ta có

$$(b, c) = (c, a) = (a, b) = (a, b, c) = 1.$$

Xét hai trường hợp sau

Trường hợp 1:  $c$  là một số chẵn. Khi đó, vì  $(a, c) = (b, c) = 1$  nên  $a, b$  là các số lẻ và  $a^2 + b^2 \equiv 2 \pmod{4}$ . Vì  $(a, b) = 1$  nên

$$(a^2 + b^2)(a^2 - b^2) = c^2, \quad (a^2 + b^2, a^2 - b^2) = 2.$$

Từ đó suy ra

$$u = \sqrt{\frac{a^2 + b^2}{2}} \quad \text{và} \quad v = \sqrt{\frac{a^2 - b^2}{2}}$$

là các số nguyên thoả mãn

$$a > b > u, \quad u^4 - v^4 = (ab)^2.$$

Vậy  $(u, v, ab)$  là cặp nghiệm nguyên dương thoả mãn  $u < a$ , mâu thuẫn với cách chọn trên.

Trường hợp 2:  $c$  là một số lẻ. Khi đó,  $c^2 \equiv 1 \pmod{4}$ . Vì  $a^4, b^4$  chỉ có thể có hai số dư là 0 hoặc 1 khi chia cho 4 nên suy ra  $a$  lẻ,  $b$  chẵn. Ta có  $a, b, c$  thoả mãn phương trình Pythagore

$$(a^2)^2 = (b^2)^2 + c^2$$

nên tồn tại các số nguyên dương nguyên tố cùng nhau  $r, s$  sao cho

$$a^2 = r^2 + s^2, \quad b^2 = 2rs, \quad c = r^2 - s^2.$$

Vì  $b$  chẵn nên  $b^2 \vdots 4$  suy ra trong  $r, s$  có đúng một số lẻ. Trong chứng minh tiếp theo, không cần dùng đến đẳng thức  $c = r^2 - s^2$  nên có thể coi  $r, s$  bình đẳng và giả sử  $r$  chẵn. Khi đó tồn tại các số nguyên dương  $u, v$  sao cho  $r/2 = u^2, s = v^2$ . Suy ra  $a, u, v$  thoả mãn phương trình Pythagore

$$a^2 = (2u^2)^2 + (v^2)^2.$$

Đó là tồn tại các số nguyên dương nguyên tố cùng nhau  $m, n$  sao cho

$$a = m^2 + n^2, \quad 2u^2 = 2mn, \quad v^2 = m^2 - n^2.$$

Vì  $u^2 = mn$  và  $(m, n) = 1$  nên  $m = p^2, n = q^2$  và  $p, q, v$  thỏa mãn phương trình

$$v^2 = m^2 - n^2 = p^4 - q^4.$$

Để thấy  $(p, q, v)$  là một nghiệm nguyên dương của phương trình  $x^4 - y^4 = z^2$  với

$$p = \sqrt{m} \leq u = \sqrt{r/2} < r \leq a$$

nên mâu thuẫn với cách chọn nghiệm  $(a, b, c)$ .

Vậy điều giả sử là sai, suy ra phương trình đã cho vô nghiệm.

**Ví dụ 2.1.2 (Bulgaria 1998).** Chứng minh rằng phương trình

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

không có nghiệm nguyên dương.

### Giải

Phản chứng, giả sử phương trình đã cho có nghiệm nguyên dương  $(x_0, y_0, z_0)$ . Ta có phương trình trên tương đương với phương trình bậc 2 đối với  $z^2$  sau

$$(z^2)^2 - (x^2 + y^2)z^2 - x^2y^2 = 0.$$

Đặt  $a = x_0^2 + y_0^2, b = 2x_0^2y_0^2$ . Vì với  $(x, y) = (x_0, y_0)$  phương trình trên có nghiệm nguyên nên

$$\Delta = (x_0^2 + y_0^2)^2 + 4x_0^2y_0^2 = a^2 + b^2$$

phải là một số chính phương.

Giả sử  $a^2 + b^2 = S^2$ , khi đó

$$a^4 - b^4 = (a^2 + b^2)(a^2 - b^2) = S^2(x_0^2 - y_0^2)^2 = \left(S(x_0^2 - y_0^2)\right)^2$$

nên  $(a, b, S(x_0^2 - y_0^2))$  là một nghiệm nguyên dương của phương trình  $x^4 - y^4 = z^2$ . Vô lý, vì phương trình  $x^4 - y^4 = z^2$  không có nghiệm nguyên dương. Vậy điều giả sử là sai và ta có điều phải chứng minh.

**Ví dụ 2.1.3 (Bulgaria 1998).** Giải phương trình nghiệm nguyên dương

$$x^2 + y^2 = 1997(x - y).$$

### Giải

Ta có phương trình đã cho tương đương với các phương trình sau

$$\begin{aligned} x^2 + y^2 + (x^2 + y^2 - 2 \cdot 1997(x - y)) &= 0 \\ (x + y)^2 + (1997 - x + y)^2 &= 1997^2. \end{aligned}$$

Do  $x, y$  là các số nguyên dương nên  $0 < x + y, 1997 - x + y < 1997$  và phương trình đã cho trở thành phương trình Pythagore sau

$$a^2 + b^2 = 1997^2.$$

Vì 1997 là một số nguyên tố nên  $(a, b) = 1$ . Theo công thức nghiệm của phương trình Pythagore tồn tại các số nguyên dương nguyên tố cùng nhau  $m > n$  thoả mãn

$$1997 = m^2 + n^2, \quad a = 2mn, \quad b = m^2 - n^2.$$

- Vì  $m^2, n^2 \equiv 0, \pm 1 \pmod{5}$  và  $1997 \equiv 2 \pmod{5}$  nên  $m, n \equiv \pm 1 \pmod{5}$ .
- Vì  $m^2, n^2 \equiv 0, 1 \pmod{3}$  và  $1997 \equiv 2 \pmod{3}$  nên  $m, n \equiv \pm 1 \pmod{3}$ .

Từ đó suy ra  $m, n \equiv 1, 4, 11, 14 \pmod{15}$ . Do  $m > n$  nên  $1997/2 < m^2 < 1997$ , suy ra  $m$  chỉ có thể nhận các giá trị 34, 41, 44. Thay vào tìm được  $(m, n) = (34, 29)$  và  $(a, b) = (1972, 315)$ . Từ công thức trên tìm được hai nghiệm

$$(x, y) = (170, 145) \quad \text{hoặc} \quad (1827, 145).$$

## 2 Phương trình Pell

Trong mục này ta xét các phương trình nghiệm nguyên có dạng

$$x^2 - dy^2 = 1,$$

trong đó  $d$  là một số nguyên dương không phải là số chính phương. Phương trình này có tên gọi là phương trình Pell.

Trong trường hợp  $d = h^2$  là một số chính phương, phương trình trên tương đương với phương trình sau

$$(x - hy)(x + hy) = 1.$$

Hiển nhiên phương trình này chỉ có nghiệm  $(x, y) = (\pm 1, 0)$ .

Đối với phương trình Pell, dễ thấy rằng  $(x, y) = (\pm 1, 0)$  luôn là nghiệm (ta coi các nghiệm này là các nghiệm tầm thường), và nếu  $(x, y)$  là một nghiệm của nó thì  $(\pm x, \pm y)$  cũng là các nghiệm. Vì lý do đó, ta chỉ xét trường hợp  $d$  không phải là một số chính phương và tìm tất cả các nghiệm nguyên dương của phương trình Pell.

Thật ra Largange mới là người đầu tiên chứng minh được rằng phương trình Pell luôn luôn có vô số nghiệm, còn John Pell đóng góp không nhiều trong nghiên cứu phương trình trên, nhưng do sơ suất của Euler phương trình vẫn được mang tên Pell.

Mục đích chính của mục này là đưa ra công thức nghiệm của phương trình Pell. Trước hết, dễ thấy rằng

- Nếu  $(x_i, y_i)$  và  $(x_j, y_j)$  là các nghiệm nguyên dương của phương trình  $x^2 - dy^2 = 1$  thì  $x_i > x_j$  tương đương với  $y_i > y_j$ .

Do đó, ta có thể giả sử

$$(x_0, y_0), (x_1, y_1), (x_2, y_2), \dots$$

là tất cả các nghiệm nguyên không âm của phương trình  $x^2 - dy^2 = 1$  thoả mãn

$$1 = x_0 < x_1 < x_2 < \dots ; \quad 0 = y_0 < y_1 < y_2 < \dots .$$

Khi đó,

- $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n$  với mọi  $n = 0, 1, 2, \dots$ .
- $(x_{n+1}, y_{n+1})$  sẽ được xác định (duy nhất) thông qua  $(x_n, y_n)$  và  $(x_{n-1}, y_{n-1})$ . Nói cách khác,  $(x_n, n \geq 1)$  và  $(y_n, n \geq 1)$  là các dãy truy hồi cấp 2.

## 2.1 Công thức nghiệm

Trong phần này ta sẽ đưa ra công thức nghiệm (nguyên dương) cho phương trình Pell, dựa trên nghiệm nguyên dương nhỏ nhất. Trước hết, ta thừa nhận định lý sau-khẳng định rằng nếu  $d$  không là một số chính phương thì phương trình Pell luôn có nghiệm không tầm thường.

**Định lý 2.2.1.** Cho  $d$  là một số nguyên dương không phải là một số chính phương. Khi đó phương trình Pell

$$x^2 - dy^2 = 1$$

luôn luôn có nghiệm nguyên dương.

**Định lý 2.2.2.**

Giả sử  $(x_1, y_1)$  là nghiệm nguyên dương nhỏ nhất của phương trình Pell

$$x^2 - dy^2 = 1.$$

Khi đó điều kiện cần và đủ để  $(\bar{x}, \bar{y})$  là một nghiệm nguyên dương của phương trình là tồn tại một số nguyên dương  $n$  sao cho

$$\bar{x} + \sqrt{d}\bar{y} = (x_1 + \sqrt{d}y_1)^n.$$

### Chứng minh

Giả sử tồn tại một số nguyên dương  $n$  sao cho  $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n$ . Ta sẽ chứng minh bằng quy nạp rằng  $x_n - \sqrt{d}y_n = (x_1 - \sqrt{d}y_1)^n$  và  $(x_n, y_n)$  cũng là một nghiệm của phương trình  $x^2 - dy^2 = 1$ .

Với  $n = 1$  hiển nhiên khẳng định đúng. Giả sử khẳng định đúng với  $n$ , ta sẽ chứng minh nó đúng với  $n + 1$ . Ta có

$$\begin{aligned} (x_1 + \sqrt{d}y_1)^{n+1} &= (x_1 + \sqrt{d}y_1)^n(x_1 + \sqrt{d}y_1) = (x_n + \sqrt{d}y_n)(x_1 + \sqrt{d}y_1) \\ &= x_n x_1 + d y_n y_1 + \sqrt{d}(y_n x_1 + x_n y_1) \\ &= x_{n+1} + \sqrt{d}y_{n+1}. \end{aligned}$$

Do đó

$$x_{n+1} = x_n x_1 + d y_n y_1 > 0, \quad y_{n+1} = y_n x_1 + x_n y_1 > 0.$$

Mặt khác

$$\begin{aligned}(x_1 - \sqrt{d}y_1)^{n+1} &= (x_1 - \sqrt{d}y_1)^n(x_1 - \sqrt{d}y_1) = (x_n - \sqrt{d}y_n)(x_1 - \sqrt{d}y_1) \\ &= x_n x_1 + d y_n y_1 - \sqrt{d}(y_n x_1 + x_n y_1) \\ &= x_{n+1} - \sqrt{d}y_{n+1}.\end{aligned}$$

Tức là khẳng định đúng với  $n + 1$ . Theo nguyên lý quy nạp ta có

$$x_n \pm \sqrt{d}y_n = (x_1 \pm \sqrt{d}y_1)^n \text{ với mọi } n \geq 0.$$

Do  $(x_1, y_1)$  là nghiệm của phương trình  $x^2 - dy^2 = 1$  nên

$$\begin{aligned}x_n^2 - dy_n^2 &= (x_n + \sqrt{d}y_n)(x_n - \sqrt{d}y_n) = (x_1 + \sqrt{d}y_1)^n(x_1 - \sqrt{d}y_1)^n = \\ &= (x_1^2 - dy_1^2)^n = 1.\end{aligned}$$

Vậy  $(x_n, y_n)$  là nghiệm của phương trình  $x^2 - dy^2 = 1$ .

Ngược lại, ta sẽ chứng minh bằng phản chứng rằng nếu  $(\bar{x}, \bar{y})$  là một nghiệm của phương trình  $x^2 - dy^2 = 1$  thì tồn tại một số nguyên dương  $n$  sao cho  $\bar{x} + \sqrt{d}\bar{y} = (x_1 + \sqrt{d}y_1)^n$ .

Giả sử  $\bar{x} + \sqrt{d}\bar{y} \neq (x_1 + \sqrt{d}y_1)^n$  với mọi  $n$ . Vì  $x_1 + \sqrt{d}y_1 > 1$  nên tồn tại một số nguyên dương  $m$  sao cho

$$(x_1 + \sqrt{d}y_1)^m < \bar{x} + \sqrt{d}\bar{y} < (x_1 + \sqrt{d}y_1)^{m+1}.$$

Do  $x_1 - \sqrt{d}y_1 = 1/(x_1 + \sqrt{d}y_1) > 0$  nên sau khi nhân cả hai vế của bất đẳng thức trên với  $(x_1 - \sqrt{d}y_1)^m$  ta được

$$1 < (\bar{x} + \sqrt{d}\bar{y})(x_1 - \sqrt{d}y_1)^m < x_1 + \sqrt{d}y_1.$$

Mặt khác, theo phần trên ta có

$$(\bar{x} + \sqrt{d}\bar{y})(x_1 - \sqrt{d}y_1)^m = (\bar{x} + \sqrt{d}\bar{y})(x_m - \sqrt{d}y_m) = s + \sqrt{dt}$$

với  $s = \bar{x}x_m - d\bar{y}y_m$ ,  $t = x_m\bar{y} - \bar{x}y_m$ . Do đó kết hợp với bất đẳng thức ở trên ta có

$$1 < s + \sqrt{dt} < x_1 + \sqrt{d}y_1.$$

Ta sẽ chứng minh  $(s, t)$  cũng là một nghiệm nguyên dương của phương trình

$$x^2 - \sqrt{d}y^2 = 1.$$

Thật vậy,

$$\begin{aligned}s^2 - dt^2 &= (\bar{x}x_m - d\bar{y}y_m)^2 - d(x_m\bar{y} - \bar{x}y_m)^2 \\&= x_m^2(\bar{x}^2 - d\bar{y}^2) - dy_m^2(\bar{x}^2 - d\bar{y}^2) \\&= x_m^2 - dy_m^2 = 1.\end{aligned}$$

Do  $\bar{x} > \sqrt{dy}$ ,  $x_m > \sqrt{dy_m}$  nên  $s = \bar{x}x_m - d\bar{y}y_m > 0$ . Mặt khác, do

$$s^2 - dt^2 = (s - \sqrt{dt})(s + \sqrt{dt}) = 1, \quad \text{và} \quad s + \sqrt{dt} > 1$$

nên  $0 < s - \sqrt{dt} < 1$ , suy ra

$$0 < s - \sqrt{dt} < 1 < s + \sqrt{dt}.$$

Tức là  $t > 0$ . Vậy  $(s, t)$  là một nghiệm nguyên dương của phương trình  $x^2 - dy^2 = 1$ . Do  $1 < s + \sqrt{dt} < x_1 + \sqrt{dy_1}$  nên nghiệm này nhỏ hơn nghiệm  $(x_1, y_1)$ . Vô lý. Vậy điều giả sử là sai và ta có điều phải chứng minh.

Từ 2 định lý trên suy ra mọi phương trình Pell  $x^2 - dy^2 = 1$  đều có vô số nghiệm và dãy tất cả các nghiệm nguyên dương

$$(x_n, y_n), \quad 1 = x_0 < x_1 < x_2 < \dots, \quad 0 = y_0 < y_1 < y_2 < \dots$$

của nó thoả mãn đẳng thức

$$x_n \pm \sqrt{dy_n} = (x_1 \pm \sqrt{dy_1})^n \quad \text{với mọi } n = 0, 1, 2, \dots$$

Từ hai đẳng thức này có thể tính được  $x_n, y_n$  theo  $n, d, x_1, y_1$  như sau

$$x_n = \frac{(x_1 + \sqrt{dy_1})^n + (x_1 - \sqrt{dy_1})^n}{2}, \quad y_n = \frac{(x_1 + \sqrt{dy_1})^n - (x_1 - \sqrt{dy_1})^n}{2\sqrt{d}}$$

Mặt khác, ta có thể chứng minh được rằng hai dãy  $(x_n, n \geq 0)$  và  $(y_n, n \geq 0)$  đều là dãy truy hồi tuyến tính cấp hai. Ta có hệ quả sau.

### Hệ quả 2.2.3.

Giả sử  $(x_n, y_n)_{n>0}$ ,  $1 = x_0 < x_1 < x_2 < \dots, 0 = y_0 < y_1 < y_2 < \dots$  là dãy tất cả các nghiệm nguyên dương của phương trình Pell

$$x^2 - dy^2 = 1.$$

Khi đó,  $(x_n, n \geq 0)$  và  $(y_n, n \geq 0)$  là hai dãy truy hồi tuyến tính cấp 2 thoả mãn công thức

$$\begin{aligned}x_{n+1} &= 2x_1x_n - x_{n-1}, \\y_{n+1} &= 2x_1y_n - y_{n-1}, \quad \text{với mọi } n = 1, 2, \dots\end{aligned}$$

### Chứng minh

Theo định lý trên ta có

$$x_{n+1} = x_1x_n + dy_1y_n, \quad y_{n+1} = x_ny_1 + x_1y_n \quad \text{với mọi } n > 0.$$

Suy ra  $x_n = x_1x_{n-1} + dy_1y_{n-1}$  hay  $dy_1y_{n-1} = x_n - x_1x_{n-1}$ . Do đó,

$$\begin{aligned}x_{n+1} &= x_1x_n + dy_1y_n \\&= x_1x_n + dy_1(x_{n-1}y_1 + x_1y_{n-1}) \\&= x_1x_n + dy_1^2x_{n-1} + x_1(dy_1y_{n-1}) \\&= x_1x_n + dy_1^2x_{n-1} + x_1(x_n - x_1x_{n-1}) \\&= 2x_1x_n + (dy_1^2 - x_1^2)x_{n-1} \\&= 2x_1x_n - x_{n-1}.\end{aligned}$$

Tương tự ta có  $y_n = x_{n-1}y_1 + x_1y_{n-1}$  hay  $x_{n-1}y_1 = y_n - x_1y_{n-1}$ , do đó

$$\begin{aligned}y_{n+1} &= x_ny_1 + x_1y_n \\&= (x_1x_{n-1} + dy_1y_{n-1})y_1 + x_1y_n \\&= x_1(x_{n-1}y_1) + dy_1^2y_{n-1} + x_1y_n \\&= x_1(y_n - x_1y_{n-1}) + dy_1^2y_{n-1} + x_1y_n \\&= 2x_1y_n - (x_1^2 - dy_1^2)y_{n-1} \\&= 2x_1y_n - y_{n-1}.\end{aligned}$$

Hệ quả được chứng minh.

**Ví dụ 2.2.1.** Cho  $d$  là một số nguyên dương không phải là số chính phương,  $k$  là một số nguyên dương bất kỳ. Chứng minh rằng tồn tại vô số cặp các số nguyên dương  $(x, y)$  thoả mãn

$$\begin{cases} x^2 - dy^2 = 1, \\ y : k. \end{cases}$$

**Giải**

Đặt  $d_1 = k^2d$ . Vì  $d$  không phải là một số chính phương nên  $d_1$  cũng không phải là số chính phương, do đó, theo định lý trên phương trình Pell

$$x^2 - d_1 y^2 = 1$$

có vô số nghiệm nguyên dương. Giả sử các nghiệm đó là  $(x_n, y_n)_{n \geq 1}$ . Khi đó,  $(x_n, ky_n)_{n \geq 1}$  sẽ là nghiệm của phương trình Pell

$$x^2 - dy^2 = 1$$

Hiển nhiên các nghiệm này thoả mãn

$$\begin{cases} x_n^2 - d(ky_n)^2 = 1, \\ (ky_n) : k. \end{cases} \quad \text{với mọi } n \geq 1.$$

Từ đó suy ra điều phải chứng minh.

**Ví dụ 2.2.2.**

a, Tìm các số nguyên dương thoả mãn phương trình

$$(x+1)^3 - x^3 = y^2.$$

b, Chứng minh rằng phương trình

$$x^2 + y^2 + z^2 + 2xyz = 1$$

có vô số nghiệm nguyên.

**Giải**

a, Do  $(x+1)^3 - x^3 = 3x^2 + 3x + 1$  nên phương trình đã cho trở thành  $3x^2 + 3x + 1 = y^2$  và tương đương với

$$(2y)^2 - 3(2x+1)^2 = 1.$$

Đặt  $u = 2y, v = 2x+1$  ta có phương trình Pell

$$u^2 - 3v^2 = 1$$

với nghiệm nguyên dương nhỏ nhất là  $(u_1, v_1) = (2, 1)$ . Do đó theo công thức nghiệm của phương trình Pell, nghiệm ta có phương trình  $u^2 - 3v^2 = 1$  có các nghiệm nguyên dương  $u_n, v_n$  thoả mãn

$$\begin{aligned} u_0 &= 1, u_1 = 2, \quad u_{n+1} = 4u_n - u_{n-1}, \\ v_0 &= 0, v_1 = 1, \quad v_{n+1} = 4v_n - v_{n-1}. \end{aligned}$$

từ đó suy ra phương trình  $(x+1)^3 - x^3 = y^2$  có các nghiệm không âm  $(x_n, y_n)$  thoả mãn

$$\begin{aligned} x_0 &= 0, x_1 = 0, \quad x_{n+1} = 4x_n - x_{n-1} + 1, \\ y_0 &= 1, y_1 = 1, \quad y_{n+1} = 4y_n - y_{n-1}. \end{aligned}$$

b, Phương trình đã cho tương đương với

$$x^2 + y^2 + (z + xy)^2 - x^2y^2 - 1 = 0,$$

hay

$$(x^2 - 1)(y^2 - 1) = (z + xy)^2.$$

Vì vế phải của phương trình là một số chính phương nên ta cần biểu diễn

$$x^2 - 1 = r^2q, \quad y^2 - 1 = s^2q,$$

trong đó  $r, s, q$  là các số nguyên dương,  $q$  không có ước số chính phương. Do  $q$  không có ước số chính phương nên hai phương trình Pell

$$x^2 - qr^2 = 1, \quad \text{và} \quad y^2 - qs^2 = 1$$

có vô số nghiệm nguyên dương  $(x, r)$  và  $(y, s)$ . Với mỗi nghiệm này đều tìm được giá trị của  $z$  để

$$(z + xy)^2 = (qrs)^2$$

nên suy ra phương trình đã cho có vô số nghiệm.

Ta cũng có thể chỉ được ngay phương trình có vô số nghiệm nguyên, ít nhất là các nghiệm  $(x, y, z) = (k, k, -1)$  ( $k \in \mathbb{Z}$ ).

**Ví dụ 2.2.3.** Cho hai dãy số nguyên dương  $(x_n)_{n \geq 0}, (y_n)_{n \geq 0}$  được xác định như sau

$$\begin{aligned} x_0 &= 0, x_1 = 1, \quad x_{n+1} = 4x_n - x_{n-1}, \\ y_0 &= 1, y_1 = 2, \quad y_{n+1} = 4y_n - y_{n-1}. \end{aligned}$$

Chứng minh rằng với mọi  $n \geq 0$ ,

$$y_n^2 = 3x_n^2 + 1.$$

Ví dụ này có thể chứng minh bằng quy nạp, nhưng thực chất hai dãy đã cho chính là dãy các nghiệm của một phương trình Pell.

### Giải

Ta có  $(x, y) = (1, 2)$  là nghiệm nguyên dương nhỏ nhất của phương trình Pell

$$y^2 - dx^2 = 1.$$

Do đó, theo công thức nghiệm của phương trình Pell, tất cả các nghiệm nguyên dương  $(x_n, y_n)_{n \geq 1}$  của phương trình trên thoả mãn

$$\begin{aligned} x_0 &= 0, x_1 = 1, & x_{n+1} &= 4x_n - x_{n-1}, \\ y_0 &= 1, y_1 = 2, & y_{n+1} &= 4y_n - y_{n-1}. \end{aligned}$$

Đây chính là hai dãy đã cho nên suy ra điều phải chứng minh.

**Ví dụ 2.2.4.** Tìm tất cả các số nguyên dương  $m$  sao cho

$$\frac{m(m+1)}{3}$$

là một số chính phương.

### Giải

Theo đề bài, cần xác định tất cả các số nguyên dương  $m, v$  sao cho

$$m(m+1) = 3v^2.$$

Phương trình trên tương đương với

$$(2m+1)^2 - 12v^2 = 1.$$

Đặt  $u = 2m+1$  ta có phương trình Pell

$$u^2 - 12v^2 = 1$$

với nghiệm nguyên dương nhỏ nhất là  $u_1 = 5, v_1 = 2$ . Theo công thức nghiệm của phương trình Pell ta có

$$\begin{aligned} u_0 &= 1, u_1 = 5, \quad u_{n+1} = 10u_n - u_{n-1} \\ v_0 &= 0, v_1 = 2, \quad v_{n+1} = 10v_n - v_{n-1}. \end{aligned}$$

Do đó, tập tất cả các số  $m$  cần tìm là một dãy truy hồi tuyến tính cấp 2 thoả mãn

$$m_1 = 2, m_2 = 24, \quad m_{n+1} = 10m_n - m_{n-1} + 4.$$

**Ví dụ 2.2.5.** Chứng minh rằng tồn tại vô số cặp các số nguyên dương liên tiếp  $(n, n + 1)$  thoả mãn tính chất sau:

Nếu một số nguyên tố bất kỳ  $p$  là ước số của  $n$  hoặc  $n + 1$  thì  $p^2$  cũng là ước số của số ấy.

### Giải

Trước hết ta chứng minh rằng nếu  $n + 1 = x^2, n = 2y^2$  với  $x, y$  là các số nguyên dương thì cặp  $(n, n + 1)$  thoả mãn tính chất đề bài.

Thật vậy, vì

$$x^2 - 2y^2 = (n + 1) - n = 1 \equiv 1 \pmod{4}$$

nên  $x$  lẻ và  $x^2 \equiv 1 \pmod{4}$ , do đó  $2y^2 \equiv 0 \pmod{4}$ , suy ra  $y$  phải là một số chẵn.

- Nếu số nguyên tố  $p$  là ước số của  $n + 1 = x^2$ , hiển nhiên  $p^2$  cũng là ước số của  $n + 1$ .
- Nếu  $p > 3$  là ước số của  $n = 2y^2$  thì  $p$  là ước số của  $y^2$  nên  $p^2$  cũng là ước số của  $n$ .
- Với  $p = 2$  hiển nhiên  $p^2 = 4$  là ước số của  $n$  do  $y$  là một số chẵn.

Tóm lại, nếu  $n + 1 = x^2, n = 2y^2$  với  $x, y$  là các số nguyên dương thì cặp  $(n, n + 1)$  thoả mãn tính chất đề bài.

Tiếp theo ta sẽ chứng minh có vô số cặp  $(n, n + 1)$  có biểu diễn như vậy. Ta có phương trình Pell

$$x^2 - 2y^2 = 1$$

có vô số nghiệm nguyên dương  $(x_k, y_k)_{k \geq 0}$ . Theo chứng minh trên, với mỗi số nguyên  $k > 0$ , cặp số nguyên dương  $(n, n+1) = (\lfloor x_k^2 \rfloor, \lfloor x_k^2 \rfloor)$  luôn thoả mãn tính chất đề bài. Từ đó suy ra có vô số cặp  $(n, n+1)$  thoả mãn tính chất đề bài.

**Ví dụ 2.2.6.** Cho hai đa thức  $P(x), Q(x)$  với các hệ số nguyên có hệ số cao nhất cùng dấu,  $\deg P = n, \deg Q = m$  thoả mãn

$$P^2(x) = (x^2 - 1)Q^2(x) + 1.$$

Chứng minh rằng

$$P'(x) = nQ(x).$$

### Giải

Để thấy  $m = n - 1$ . Đặt  $P = P_n, Q = Q_n$ , với mỗi số nguyên dương  $x$ ,  $P_n(x), Q_n(x)$  là các nghiệm nguyên của phương trình Pell (ẩn  $u, v$ )

$$u^2 - (x^2 - 1)v^2 = 1.$$

Do  $P_n(x), Q_n(x)$  có hệ số cao nhất cùng dấu nên không mất tính tổng quát ta có thể giả sử hai hệ số này dương, khi đó  $P_n(x), Q_n(x) > 0$  nếu  $x$  đủ lớn. Tức là với  $x$  là một số nguyên dương đủ lớn thì  $P_n(x), Q_n(x)$  là hai nghiệm nguyên dương của phương trình  $u^2 - (x^2 - 1)v^2 = 1$ . Phương trình này luôn có nghiệm nguyên dương nhỏ nhất là  $(u, v) = (x, 1)$ . Từ công thức nghiệm của phương trình Pell và giả thiết  $\deg P_n = n$  suy ra  $(P_n(x), Q_n(x))$  là nghiệm nguyên dương thứ  $n$  của phương trình  $u^2 - (x^2 - 1)v^2 = 1$  và thoả mãn công thức

$$\begin{aligned} P_n(x) &= \frac{(x + \sqrt{(x^2 - 1)})^n + (x - \sqrt{(x^2 - 1)})^n}{2} \\ Q_n(x) &= \frac{(x + \sqrt{(x^2 - 1)})^n - (x - \sqrt{(x^2 - 1)})^n}{2\sqrt{(x^2 - 1)}}. \end{aligned}$$

Bằng cách lấy đạo hàm trực tiếp suy ra điều phải chứng minh.

**Ví dụ 2.2.7.** Tìm tất cả các cặp số nguyên không âm  $(m, n)$  thoả mãn

$$9^m = 2n^2 + 1.$$

### Giải

Các giá trị của  $m$  để phương trình có nghiệm là  $m = 0, 1$ , khi ấy ta có các nghiệm  $(m, n) = (0, 0), (1, 2)$ . Ta sẽ chứng minh rằng nếu  $m > 1$  thì phương trình đã cho vô nghiệm.

Giả sử phương trình đã cho có một nghiệm  $m > 1$ . Đặt  $x = 3^m$  ta có  $x : 9$  và  $(x, n)$  là nghiệm của phương trình Pell

$$x^2 - 2n^2 = 1.$$

Gọi  $(x_k, n_k)_{k \geq 0}$  là dãy tất cả các nghiệm của phương trình theo thứ tự tăng dần. Ta có

$$x_0 = 1, x_1 = 3, \quad x_{k+1} = 6x_k - x_{k-1} \text{ với mọi } k > 0.$$

Gọi  $r_k$  là số dư trong phép chia  $x_k$  cho 9. Ta có

$$r_0 = 1, r_1 = 3, \quad r_{k+1} \equiv 6r_k - r_{k-1} \pmod{9} \text{ với mọi } k > 0.$$

Bằng cách tính trực tiếp,

$$\begin{aligned} r_0 &= 1, r_1 = 3, r_2 = 8, r_3 = 0, r_4 = 1, r_5 = 6, \\ r_6 &= 8, r_7 = 6, r_8 = 1, r_9 = 0, r_{10} = 8, r_{11} = 3, \\ r_{12} &= 1, r_{13} = 3. \end{aligned}$$

Do  $r_0 = r_{12}, r_1 = r_{13}$  nên dãy  $(r_k)_k$  tuần hoàn với chu kỳ 12. Do  $x = 3^a \equiv 0 \pmod{9}$  nên  $x = x_k$  với  $k \equiv 3$  hoặc  $9 \pmod{12}$ . Ta có  $x_2 = 17, x_3 = 99$ , tức là  $x_3 : 11$ .

Gọi  $s_k$  là số dư của  $x_k$  trong phép chia cho 11. Ta có

$$s_0 = 1, s_1 = 3, \quad s_{k+1} \equiv 6s_k - s_{k-1} \pmod{11} \text{ với mọi } k > 0.$$

Bằng cách tính trực tiếp,

$$\begin{aligned} s_0 &= 1, s_1 = 3, s_2 = 6, s_3 = 0, s_4 = 5, s_5 = 8, \\ s_6 &= 10, s_7 = 8, s_8 = 5, s_9 = 0, s_{10} = 6, s_{11} = 3, \\ s_{12} &= 1, s_{13} = 3. \end{aligned}$$

Do  $s_0 = r_{12}, s_1 = r_{13}$  nên dãy  $(s_k)_k$  tuần hoàn với chu kỳ 12. Từ đó suy ra với  $k \equiv 3$  hoặc  $9 \pmod{12}$  thì  $s_k = 0$ , tức là  $x = x_k : 11$ , mâu thuẫn với  $x = 3^m$ . Vậy điều giả sử là sai, tức là phương trình đã cho chỉ có hai

nghiệm  $(m, n) = (t, t^3 + 1, 2)$ .

**Ví dụ 2.2.8 (Bulgaria 1999).** Chứng minh rằng phương trình

$$x^3 + y^3 + z^3 + t^3 = 1999$$

có vô số nghiệm nguyên.

### Giải

Ta có

$$(m - n)^3 + (m + n)^3 = 2m^3 + 6mn^2.$$

Ta tìm nghiệm có dạng

$$(x, y, z, t) = (a - b, a + b, \frac{c}{2} - \frac{d}{2}, \frac{c}{2} + \frac{d}{2})$$

với  $a, b, c, d$  là các số nguyên. Để thấy  $(x, y, z, t) = (10, 10, -1, 0)$  là một nghiệm. Ta sẽ tìm nghiệm với  $a = 10$  và  $c = -1$  cố định. Để thấy

$$(x, y, z, t) = (10 - b, 10 + b, \frac{-1}{2} - \frac{d}{2}, \frac{-1}{2} + \frac{d}{2})$$

là nghiệm của phương trình đã cho khi và chỉ khi

$$(2000 + 60b^2) - \frac{1 + 3d^2}{4} = 1999 \quad \text{hay} \quad d^2 - 80b^2 = 1.$$

Để thấy phương trình Pell  $d^2 - 80b^2 = 1$  có nghiệm nguyên dương nhỏ nhất là  $(d_1, b_1) = (9, 1)$ . Do phương trình Pell có vô số nghiệm nên phương trình đã cho cũng có vô số nghiệm. Điều phải chứng minh.

Ví dụ sau cho thấy ứng dụng của phương trình Pell để tìm nghiệm của các phương trình bậc hai tổng quát hơn.

## 2.2 Phương trình $x^2 - dy^2 = -1$

Xét phương trình

$$x^2 - dy^2 = -1$$

trong đó  $d$  không phải là một số chính phương.

Khác với phương trình Pell, phương trình này không phải lúc nào cũng có nghiệm nguyên. Chẳng hạn, xét phương trình sau đây

$$x^2 - dy^2 = -1 \text{ với } d \equiv 3 \pmod{4}.$$

Phương trình này không có nghiệm nguyên. Thật vậy, giả sử phương trình này có một nghiệm nguyên  $(x_0, y_0)$ . Khi đó,

$$x_0^2 - dy_0^2 = -1 \equiv x_0^2 + y_0^2 \pmod{4}.$$

Tức là  $x_0^2 + y_0^2 \equiv 3 \pmod{4}$ , vô lý. Tương tự, ta có thể chứng minh được: Nếu  $d = k^2 - 1$  hoặc  $d$  có một ước số nguyên tố  $p$ ,  $p \equiv 3 \pmod{4}$  thì phương trình

$$x^2 - dy^2 = -1$$

cũng không có nghiệm nguyên.

Tuy nhiên, có rất nhiều giá trị của  $d$  để phương trình  $x^2 - dy^2 = -1$  có nghiệm. Ta có ví dụ sau.

**Ví dụ 2.2.9.** Nếu  $d = p \equiv 1 \pmod{4}$  là một số nguyên tố thì phương trình

$$x^2 - dy^2 = -1$$

luôn có nghiệm.

Trong trường hợp phương trình  $x^2 - dy^2 = -1$  có nghiệm, tương tự như phương trình Pell (định lý 2.2.2), ta có định lý sau đây mô tả nghiệm của nó thông qua nghiệm nguyên dương nhỏ nhất.

#### Định lý 2.2.4.

Giả sử phương trình  $x^2 - dy^2 = -1$  có nghiệm nguyên dương với  $(x_1, y_1)$  là nghiệm nguyên dương nhỏ nhất. Khi đó

i, Các số nguyên dương  $(x_2, y_2)$  được xác định bởi

$$x_2 + \sqrt{d}y_2 = (x_1 + \sqrt{d}y_1)^2$$

là nghiệm nguyên dương nhỏ nhất của phương trình  $x^2 - dy^2 = 1$ .

ii, Tất cả các nghiệm nguyên dương của phương trình  $x^2 - dy^2 = -1$  đều có dạng  $(x_n, y_n)$  với  $n$  lẻ, tất cả các nghiệm nguyên dương của phương trình  $x^2 - dy^2 = 1$  đều có dạng  $(x_n, y_n)$  với  $n$  chẵn, trong đó  $(x_n, y_n)$  là các số nguyên dương được xác định bởi

$$x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n.$$

Định lý này có thể chứng minh bằng cách toán tương tự định lý 2.2.

### Ví dụ 2.2.10 (Việt Nam 1999).

Cho hai dãy số  $(x_n)_{n \geq 0}$  và  $(y_n)_{n \geq 0}$  được xác định như sau

$$x_0 = 1, \quad x_1 = 4, \quad x_{n+1} = 3x_n + x_{n-1}, \quad \text{với mọi } n \geq 1,$$

$$y_0 = 1, \quad y_1 = 2, \quad y_{n+1} = 3y_n - y_{n-1}, \quad \text{với mọi } n \geq 1.$$

a, Chứng minh rằng  $x_n^2 - 5y_n^2 + 4 = 0$  với mọi số tự nhiên  $n$ .

b, Chứng minh rằng nếu  $(a, b)$  là hai số nguyên dương thoả mãn phương trình

$$a^2 - 5b^2 + 4 = 0$$

thì tồn tại một số tự nhiên  $k$  sao cho  $a = x_k, b = y_k$ .

### Giải

Trước hết, ta chứng minh bằng quy nạp theo  $n$  rằng

$$(x_{n+1}, y_{n+1}) = \left( \frac{3x_n + 5y_n}{2}, \frac{x_n + 3y_n}{2} \right) \quad \text{với mọi } n \geq 0.$$

Với  $n = 0, n = 1$  khẳng định đúng vì

$$(4, 2) = \left( \frac{3+5}{2}, \frac{1+3}{2} \right), \quad (11, 5) = \left( \frac{12+10}{2}, \frac{4+6}{2} \right).$$

Giả sử khẳng định đúng với  $n = k$  và  $n = k+1$ . Cần chứng minh khẳng định đúng với  $n = k+2$ . Ta có

$$\begin{aligned} & (x_{k+3}, y_{k+3}) \\ &= (3x_{k+2} - x_{k+1}, 3y_{k+2} - y_{k+1}) \\ &= \left( \frac{3}{2}(3x_{k+1} - x_k) + \frac{5}{2}(3y_{k+1} - y_k), \frac{1}{2}(3x_{k+1} - x_k) + \frac{3}{2}(3y_{k+1} - y_k) \right) \\ &= \left( \frac{3x_{k+2} + 5y_{k+2}}{2}, \frac{x_{k+2} + 3y_{k+2}}{2} \right). \end{aligned}$$

Do đó khẳng định đúng với  $n = k+2$ . Theo nguyên lý quy nạp ta có khẳng định đúng với mọi số tự nhiên  $n$ .

a, Ta sẽ chứng minh  $x_n^2 - 5y_n^2 + 4 = 0$  bằng quy nạp theo  $n$ . Với  $n = 0$  hiển nhiên khẳng định đúng. Giả sử khẳng định đúng với  $n$ . Ta có

$$\begin{aligned} x_{n+1}^2 - 5y_{n+1}^2 &= \left( \frac{3x_n + 5y_n}{2} \right)^2 - 5 \left( \frac{x_n + 3y_n}{2} \right)^2 \\ &= \frac{4x_n^2 + 20y_n^2}{4} - x_n^2 - 3y_n^2 = \frac{1}{4}. \end{aligned}$$

Tức là khẳng định đúng với  $n + 1$ . Theo nguyên lý quy nạp ta có khẳng định đúng với mọi số tự nhiên  $n$ .

b, Giả sử trái lại, tồn tại hai số nguyên dương  $a, b$  thoả mãn  $a^2 - 5b^2 + 4 = 0$  nhưng không tồn tại  $k$  sao cho  $(x_k, y_k) = (a, b)$ . Chọn  $a, b$  sao cho tổng  $a + b$  đạt giá trị nhỏ nhất. Đặt

$$(a', b') = \left( \frac{3a - 5b}{2}, \frac{3b - a}{2} \right).$$

Ta sẽ chứng minh rằng  $a', b'$  là các số nguyên dương. Thật vậy, ta có  $0 \equiv a^2 - 5b^2 + 4 \equiv a - b \pmod{2}$  nên  $a', b'$  là các số nguyên. Mặt khác, do  $a^2 - 5b^2 + 4 = 0$  nên  $a > 2$ ,  $a^2 > 5$ . Do đó,

- $a^2 = 5b^2 - 4 < 9b^2$  nên  $a < 3b$ .
- $0 = 5a^2 - 25b^2 + 20 < 5a^2 - 25b^2 + 4a^2$  nên  $3a > 5b$ .

Từ đó suy ra  $a', b'$  là các số nguyên dương. Từ cách xác định  $a', b'$  ta có

$$(a')^2 - 5(b')^2 = \left( \frac{3a - 5b}{2} \right)^2 - 5 \left( \frac{3b - a}{2} \right)^2 = \frac{4a^2 - 20b^2}{4} = a^2 - 5b^2 = -4.$$

Mặt khác,  $a' + b' = a - b < a + b$ . Vô lý, trái với cách chọn tổng  $a + b$  nhỏ nhất. Vậy điều giả sử là sai và ta có điều phải chứng minh.

**BÀI TẬP**

**Bài 1.** Tìm cặp  $(k, n)$  các số nguyên dương thỏa mãn

$$1 + 2 + \cdots + k = k + 1 + k + 2 + \cdots + n.$$

**Bài 2.** Tìm các số tự nhiên  $m$  sao cho  $\frac{m(m+1)}{3}$  là bình phương đúng.

**Bài 3.** Tìm số tự nhiên  $n$  sao cho  $\frac{n(n+1)}{2}$  là bình phương đúng.

**Bài 4.** Tìm nghiệm nguyên dương của phương trình

$$(x+1)^3 - x^3 = y^2.$$

**Bài 5.** Tìm tất cả các số nguyên dương  $n$  sao cho  $2n+1$  và  $3n+1$  là bình phương đúng. Chứng minh rằng các số tự nhiên như vậy chia hết cho 40.

**Bài 6.** Chứng minh rằng nếu  $n$  là số nguyên dương sao cho  $3n+1$  và  $4n+1$  là bình phương đúng, khi đó  $n$  chia hết cho 56.

**Bài 7.** Chứng minh rằng tất cả các phân tử của dãy

$$a_1 = 1, a_{n+1} = 2a_n + \sqrt{3a_n^2 - 2}$$

là số nguyên.

**Bài 8.** Chứng minh phương trình

$$x^2 + y^2 + z^2 + 2xyz = 1$$

có vô số nghiệm nguyên.

## LỜI GIẢI

### Bài 1.

Phương trình đã cho tương đương với

$$\begin{aligned} \frac{k(k+1)}{2} &= \frac{n(n+1)}{2} - \frac{k(k+1)}{2} \\ \Leftrightarrow 2k(k+1) &= n(n+1) \\ \Leftrightarrow (2n+1)^2 - 2(2k+1)^2 &= -1 \end{aligned}$$

Nghiệm của phương trình được viết dưới dạng

$$(2n+1) + (2k+1)\sqrt{2} = (1+\sqrt{2})^{2t+1} \quad t = 1, 2, \dots$$

Suy ra

$$\begin{aligned} n &= \frac{(1+\sqrt{2})^{2t+1} + (1-\sqrt{2})^{2t+1} - 2}{4} \\ k &= \frac{(1+\sqrt{2})^{2t+1} - (1-\sqrt{2})^{2t+1} - 2\sqrt{2}}{4\sqrt{2}}. \end{aligned}$$

### Bài 2.

$\frac{m(m+1)}{3}$  là số nguyên  $\Leftrightarrow m = 3k, m = 3k+2$ .

\*) Xét trường hợp  $m = 3k$ .

Ta có  $k(3k+1) = t^2$  với  $t \in N$ .

Vì  $(k, 3k+1) = 1$  suy ra  $3k+1 = u^2$  và  $k = v^2$ . Khi đó ta nhận được phương trình Pell  $u^2 - 3v^2 = 1$ .

Nghiệm của phương trình được xác định bởi công thức

$$u_n + v_n\sqrt{3} = (2+\sqrt{3})^n, \quad n = 1, 2, 3, \dots$$

Suy ra

$$v_n = \frac{1}{2\sqrt{3}}[(2+\sqrt{3})^n - (2-\sqrt{3})^n]$$

Từ đó thu được dãy các giá trị của  $m$  thoả mãn yêu cầu của bài toán

$$m = \frac{1}{4} [(2+\sqrt{3})^n + (2-\sqrt{3})^n]$$

Kết trường hợp  $k+1 \equiv l^2 \pmod{3}$

Chúng ta có  $(k+1) - (l^2 + 1) \equiv l^2 \pmod{l \in \mathbb{N}}$

$$\Leftrightarrow [3(k+1) - 1](l^2 + 1) \equiv l^2.$$

Vì  $k+1$  và  $3(k+1)-1$  là nguyên tố cùng nhau, ta suy ra

$$k+1 = x^2, 3(k+1)-1 = y^2$$

Suy ra  $x, y$  thoả mãn phương trình  $3x^2 - y^2 = 1$ .

Phương trình vô nghiệm vì  $(y^2 + 1) \equiv 1, 2 \pmod{3}$ , còn  $3x^2 \equiv 0 \pmod{3}$ .

### Bài 3.

Ta có

$$\begin{aligned} n(n+1) &= 2m^2 \\ \Leftrightarrow 4n^2 + 4n &= 8m^2 \\ \Leftrightarrow (2n+1)^2 - 2(2m)^2 &= 1. \end{aligned}$$

Đặt  $x = 2n+1, y = 2m$  và thu được phương trình Pell  $x^2 - 2y^2 = 1$ .

Nghiệm  $(x_k, y_k)$  của phương trình được cho bởi công thức

$$x_k + y_k\sqrt{2} = (3 + 2\sqrt{2})^{k+1}$$

$$\text{và } x_k - y_k\sqrt{2} = (3 - 2\sqrt{2})^{k+1}$$

( $x_k$  lẻ,  $y_k$  chẵn).

$$\text{Thu được } 2n+1 = \frac{(3+2\sqrt{2})^k + (3-2\sqrt{2})^k}{2} \quad (k \in \mathbb{N}).$$

### Bài 4.

Chúng ta đưa phương trình đã cho về phương trình Pell.

Vậy phương trình đã cho tương đương với

$$\begin{aligned} 3x^2 + 3x + 1 &= y^2 \\ \Leftrightarrow 12x^2 + 12x + 4 &= 4y^2 \\ \Leftrightarrow (2y)^2 - 3(2x+1)^2 &= 1 \end{aligned}$$

Đặt  $u = 2y, v = 2x+1$  ta thu được phương trình

$$u^2 - 3v^2 = 1$$

Với nghiệm  $(u_n, v_n)$  thoả mãn  $u_n + \sqrt{3}v_n = (2 + \sqrt{3})^n$ .

Suy ra họ nghiệm của phương trình ban đầu là

$$x_0 = 0, y_0 = 1, x_n = 7x_{n-1} + 4y_{n-1} + 3, y_n = 7y_{n-1} + 12x_{n-1} + 6.$$

### Bài 5.

Đặt  $2n + 1 = x^2, 3n + 1 = y^2$ . Suy ra

$$6n + 3 = 3x^2$$

$$6n + 2 = 2y^2$$

Trừ hai phương trình trên ta thu được phương trình Pell

$$3x^2 - 2y^2 = 1$$

Nghiệm nhỏ nhất của phương trình này là  $x = y = 1$ .

Công thức tổng quát của họ nghiệm là

$$x_m\sqrt{3} + y_m\sqrt{2} = (\sqrt{3} + \sqrt{2})^{2m+1}$$

$$x_m\sqrt{3} - y_m\sqrt{2} = (\sqrt{3} - \sqrt{2})^{2m+1}$$

Suy ra

$$x_m = \frac{1}{2\sqrt{3}} \left[ (\sqrt{3} + \sqrt{2})^{2m+1} + (\sqrt{3} - \sqrt{2})^{2m+1} \right]$$

$$y_m = \frac{1}{2\sqrt{2}} \left[ (\sqrt{3} + \sqrt{2})^{2m+1} - (\sqrt{3} - \sqrt{2})^{2m+1} \right]$$

Ta có

$$\begin{aligned} n &= y_m^2 - x_m^2 \\ &= \left( \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{3}} \right) (\sqrt{3} + \sqrt{2})^{2m+1} - \left( \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} \right) (\sqrt{3} - \sqrt{2})^{2m+1} \end{aligned}$$

Ta có  $x^2 = 2n + 1 \equiv 0, 1, 4 \pmod{8}$

$$\Rightarrow 2n \equiv -1, 0, 3 \pmod{8}$$

Vì  $2n$  chẵn  $\Rightarrow 2n \equiv 0 \pmod{8}$ .

Mặt khác  $y^2 = 3n + 1 \equiv 0, 1, 4 \pmod{8}$

Suy ra  $3n \equiv -1, 0, 3 \pmod{8}$

Vì  $n \equiv 0, 4 \pmod{8}$  suy ra  $n \equiv 0 \pmod{8}$  (n chia hết cho 8).

Ta có

$$x^2 = 2n + 1 \equiv 0, 1, 4 \pmod{5}$$

Sử dụng  $3n \equiv -1, 0, 3 \pmod{5} \Rightarrow n \equiv 2, 0, 4 \pmod{5}$ .

Nếu  $n$  chia  $3n^2 + 3n + 1 = 0, 1, 4 \pmod{5}$ , suy ra

$$3n \equiv -1, 0, 3 \pmod{5}$$

Vì  $n \equiv 2, 0, 4 \pmod{5}$ , suy ra  $n \equiv 0 \pmod{5}$  ( $n$  chia hết cho 5).

Vậy  $n$  chia hết cho 40.

### Bài 6.

Đặt  $3n + 1 = p^2, 4n + 1 = q^2$  suy ra

$$12n + 4 = 4p^2, 12n + 3 = 3q^2$$

và nhận được  $(2p)^2 - 3q^2 = 1$ .

Khi đó  $2p$  và  $q$  là nghiệm của phương trình  $x^2 - 3y^2 = 1$ .

Nghiệm nhỏ nhất  $x = 2, y = 1$  (tương đương với  $n = 0$ ).

Nghiệm tổng quát cho bởi công thức

$$x_m + y_m\sqrt{3} = (2 + \sqrt{3})^m$$

Suy ra

$$2p_n + q_n\sqrt{3} = [(2 + \sqrt{3})^2]^n = (7 + 4\sqrt{3})^n$$

Suy ra

$$p_{k+1} = 7p_k + 6q_k$$

$$q_{k+1} = 7q_k + 8p_k$$

Vậy  $p_{k+1}^2 \equiv q_k^2 \pmod{7}$  và  $q_{k+1}^2 \equiv p_k^2 \pmod{7}$ .

Từ đó chúng ta nhận được  $q^2 \equiv 1 \pmod{7}$ .

Suy ra  $n$  chia hết cho 7 và dễ dàng chứng minh được  $n$  chia hết cho 8.

Vậy  $n$  chia hết cho 56.

### Bài 7.

Công thức truy hồi được viết dưới dạng

$$(a_{n+1} - 2a_n)^2 - 3a_n^2 = -2$$

Đặt  $b_n = a_{n+1} - 2a_n$ , khi đó  $(a_n, b_n)$  là nghiệm của phương trình Pell

$$x^2 - 3y^2 = -2$$

Khi đó

$$b_n + \sqrt{3}a_n = (2 + \sqrt{3})^n(1 + \sqrt{3})$$

Ta cộng hai đẳng thức

$$b_{n+1} + \sqrt{3}a_{n+1} = (2 + \sqrt{3})^{n+1}(1 + \sqrt{3})$$

$$-2b_n - 2\sqrt{3}a_n = -2(2 + \sqrt{3})^n(1 + \sqrt{3})$$

Thu được

$$(b_{n+1} - 2b_n) + \sqrt{3}(a_{n+1} - 2a_n) = \sqrt{3}(2 + \sqrt{3})^n(1 + \sqrt{3}) = \sqrt{3}(b_n + \sqrt{3}a_n)$$

Đồng nhất hệ số của  $\sqrt{3}$  ở 2 vế ta thu được

$$b_n = a_{n+1} - 2a_n$$

### Bài 8.

Phương trình đã cho được viết dưới dạng

$$x^2 + y^2 + (z + xy)^2 - x^2y^2 - 1 = 0$$

$$\Leftrightarrow (x^2 - 1)(y^2 - 1) = (z + yz)^2$$

Để vế trái là bình phương đúng ta phải có

$x^2 - 1 = p^2q$  và  $y^2 - 1 = r^2q$  với  $p, q, r$  nguyên,  $q$  không là ước của  $p^2$  hoặc  $r^2$ .

Cố định  $q$  ta thu nhận được các phương trình Pell

$$x^2 - qp^2 = 1$$

$$\text{và } y^2 - qr^2 = 1$$

Những phương trình này có vô số nghiệm và mỗi nghiệm này ta suy ra được nghiệm của phương trình ban đầu với  $z = pqr - xy$ .

### 3 Các bài toán khác

**Ví dụ 2.3.1.** Cho  $m$  là một số nguyên dương. Tìm tất cả các số nguyên dương  $x, y, n$  thoả mãn phương trình

$$(x^2 + y^2)^m = (xy)^n.$$

#### Giải

Giả sử  $(x, y)$  là một nghiệm nguyên dương của phương trình. Từ giả thiết và bất đẳng thức  $(x^2 + y^2)^m \geq 2^m(xy)^m$  ta có  $n > m$  và

$$x^{2m} : y, \quad y^{2m} : x,$$

tức là  $x, y$  có cùng tập các ước số nguyên tố.

Giả sử  $x = p^\alpha s, y = p^\beta t$  với  $p$  là một số nguyên tố lẻ và  $s, t$  là các số nguyên dương sao cho  $(p, s) = (p, t) = 1$ . Khi đó,

- Số mũ của  $p$  trong phân tích tiêu chuẩn của  $(x^2 + y^2)^m$  là  $\min\{2m\alpha, 2m\beta\}$
- Số mũ của  $p$  trong phân tích tiêu chuẩn của  $(xy)^n$  là  $n(\alpha + \beta)$ .

Do đó ta có  $\min\{2m\alpha, 2m\beta\} = n(\alpha + \beta)$ . Mặt khác, do  $n > m$  nên

$$n(\alpha + \beta) \geq \min\{2n\alpha, 2n\beta\} \geq \min\{2m\alpha, 2m\beta\}.$$

Dấu đẳng thức chỉ xảy ra khi  $\alpha = \beta = 0$ . Vậy  $x, y$  không có ước số lẻ, tức là tồn tại các số nguyên  $\alpha, \beta$  sao cho  $x = 2^\alpha, y = 2^\beta$ .

Bằng cách tương tự ta suy ra  $\alpha = \beta = k$ , tức là

$$(x^2 + y^2)^m = 2^{m(2k+1)} = (xy)^n = 2^{2kn}$$

hay  $m(2k+1) = 2kn$ .

Vậy, nếu  $m/n$  có dạng  $2k/(2k+1)$  thì phương trình có nghiệm nguyên dương duy nhất  $x = y = 2^k$ . Nếu  $m/n$  không có dạng  $2k/(2k+1)$  thì phương trình không có nghiệm nguyên dương.

**Ví dụ 2.3.2 (Vietnam 95).** Tìm tất cả các số nguyên  $a, b, n$  lớn hơn 1 thoả mãn điều kiện

$$(a^3 + b^3)^n = 4(ab)^{1995}.$$

### Giải

Nếu  $n = 1$  dễ thấy phương trình không có nghiệm nguyên. Xét  $n > 1$ , ta có

$$4(ab)^{1995} = (a^3 + b^3)^n \geq 2^n(ab)^{3n/2} \geq 4(ab)^{3n/2},$$

nên  $1995 \geq 3n/2$  hay  $2.1995 \geq 3n$  hoặc  $n \leq 1330$ .

Tương tự ví dụ trên suy ra  $a, b$  có cùng tập các ước số nguyên tố. Giả sử  $a = p^\alpha s, b = p^\beta t$  với  $p$  là một số nguyên tố lẻ và  $s, t$  là các số nguyên dương sao cho  $(p, s) = (p, t) = 1$ . Khi đó,

- Số mũ của  $p$  trong phân tích tiêu chuẩn của  $(x^3 + y^3)^n$  là  $\min\{3n\alpha, 3n\beta\}$
- Số mũ của  $p$  trong phân tích tiêu chuẩn của  $4(xy)^{1995}$  là  $1995(\alpha + \beta)$ .

Do đó ta có  $\min\{3n\alpha, 3n\beta\} = n(\alpha + \beta)$ . Mặt khác, do  $2.1995 \geq 3n$  nên

$$1995(\alpha + \beta) \geq \min\{2.1995\alpha, 2.1995\beta\} \geq \min\{3n\alpha, 3n\beta\}.$$

Dấu đẳng thức chỉ xảy ra khi  $\alpha = \beta$  và  $n = 1330$ . Do đó chỉ có thể xảy ra hai trường hợp sau:

Trong trường hợp 1:  $n < 1330$ . Khi đó  $a$  và  $b$  không có ước số chung lẻ lớn hơn 1 nên tồn tại các số nguyên dương  $u, v$  để  $a = 2^u, b = 2^v$ . Vì  $4(ab)^{1995}$  không có ước số lẻ lớn hơn 1 nên suy ra  $u = v = k$ . Khi đó so sánh hệ số của 2 trong cả hai vế của phương trình ta có

$$(3k + 1)n = 2 + 1995.2k,$$

hay

$$n = \frac{2(1995k + 1)}{3k + 1} = 2 \frac{665(3k + 1) - 664}{3k + 1} = 1330 - \frac{2^4 \cdot 83}{3k + 1}.$$

Từ đó suy ra  $3k + 1$  chỉ có thể nhận các giá trị là 4, 16, 166, 664 hay  $k$  chỉ có thể nhận các giá trị là 1, 5, 55, 221. Vậy nếu  $n = 998$  ( $k = 1$ ),

$1247$  ( $k = 5$ ),  $1322$  ( $k = 55$ ),  $1328$  thì phương trình có các nghiệm tương ứng là  $a = b = 2^1, 2^5, 2^{55}, 2^{221}$ . Với các giá trị bé hơn  $1330$  còn lại của  $n$  phương trình vô nghiệm.

Trong trường hợp  $2$ :  $n = 1330$ . Khi đó số mũ của mọi số nguyên tố lẻ trong phân tích chính tắc của  $a$  và  $b$  đều bằng nhau nên tồn tại các số nguyên không âm  $u, v, l$  thoả mãn

$$a = 2^u l, \quad b = 2^v l, \quad l \text{ là một số lẻ.}$$

Ta có

$$(a^3 + b^3)^n = l^{3 \cdot 1330} (2^{3u} + 2^{3v})^{1330} = 4(ab)^{1995} = l^{2 \cdot 1995} 2^{2+1995(u+v)},$$

tức là

$$(2^{3u} + 2^{3v})^{1330} = 2^{2+1995(u+v)}.$$

Do vế phải không có ước số lẻ nên suy ra  $u = v = k$ . Thay vào ta có

$$1330(3k + 1) = 2(1995k + 1).$$

Phương trình này tương đương với

$$\frac{1995k + 1}{3k + 1} = 665 \quad \text{hay} \quad 1995k + 1 = 1995k + 665$$

Vô lý. Với  $n = 1330$  phương trình vô nghiệm.

**Ví dụ 2.3.3 (Greece 1997).** Tìm tất cả các nghiệm nguyên dương của phương trình

$$\frac{13}{x^2} + \frac{1996}{y^2} = \frac{z}{1997}.$$

**Giải**

Đặt  $d = (x, y)$ ,  $x = dx_1, y = dy_1$  khi đó phương trình tương đương với

$$1997 \cdot 13 \cdot y_1^2 + 1997 \cdot 1996 \cdot x_1^2 = d^2 z x_1^2 y_1^2.$$

Vì  $(x_1, y_1) = 1$  nên ta có

$$x_1^2 \mid 1997 \times 13, \quad y_1^2 \mid 1997 \times 1996.$$

Do  $(1997, 13) = (1997, 1996) = 1, 13$  và  $1997$  không có ước số chính phương, hơn nữa  $1996 = 2^2 \cdot 499$  với  $499$  không có ước số chính phương nên  $(x_1, y_1) = (1, 1)$  hoặc  $(x_1, y_1) = (1, 2)$ . Xét 2 trường hợp sau

Trường hợp 1:  $(x_1, y_1) = (1, 1)$ . Khi đó,

$$d^2 z = (13 + 1996)1997 = 1997 \cdot 7^2 \cdot 41.$$

Do  $(1997, 13) = (1997, 41)$  nên  $d = 1$  hoặc  $7$ . Từ đó có 2 nghiệm sau

$$(x, y, z) = (1, 1, 4011973), (7, 7, 81877).$$

Trường hợp 2:  $(x_1, y_1) = (1, 2)$ . Khi đó,

$$d^2 z = (13 + 499)1997 = 1997 \cdot 2^9.$$

Do đó  $d = 1, 2, 4, 8, 16$ , tương ứng với các nghiệm là

$$\begin{aligned} (x, y, z) = & (1, 2, 1022464), (2, 4, 255616), (4, 8, 63904), \\ & (8, 16, 15976), (16, 32, 3994). \end{aligned}$$

**Ví dụ 2.3.4 (Hungary 1997).** Tìm tất cả các nghiệm nguyên của phương trình

$$x^3 + (x+1)^3 + (x+2)^3 + \cdots + (x+7)^3 = y^3.$$

### Giải

Đặt

$$P(x) = x^3 + (x+1)^3 + (x+2)^3 + \cdots + (x+7)^3 = 8x^3 + 84x^2 + 420x + 784.$$

Nếu  $x > 0$  ta có:

$$\begin{aligned} (2x+7)^3 &= 8x^3 + 84x^2 + 294x + 343 \\ &< P(x) \\ &< (8x^3 + 120x^2 + 600x + 1000) \\ &= (2x+10)^3. \end{aligned}$$

Do đó,  $2x+7 < y < 2x+10$ , tức là  $y$  chỉ có thể bằng  $2x+8$  hoặc  $2x+9$ . Tuy nhiên cả hai phương trình

$$P(x) - (2x+8)^3 = -12x^2 + 36x + 272 = 0,$$

$$P(x) - (2x+9)^3 = -24x^2 - 66x - 55 = 0$$

đều không có nghiệm nguyên nên phương trình không có nghiệm nguyên.

Nếu  $x < 0$ , nhận xét rằng

$$P(-x - 7) = -P(x)$$

nên nếu  $(x, y)$  là một nghiệm thì  $(-x - 7, -y)$  cũng là một nghiệm. Từ đó suy ra phương trình không có nghiệm  $x \leq -7$ . Xét  $-6 \leq x \leq -1$  ta thấy có các nghiệm

$$(x, y) = (-2, 6), (-3, 4), (-4, -4), (-5, -6).$$

**Ví dụ 2.3.5 (Ireland 1997).** Tìm tất cả các cặp số nguyên  $(x, y)$  thoả mãn

$$1 + 1996x + 1998y = xy.$$

### Giải

Ta có

$$(x - 1998)(y - 1996) = xy - 1998y - 1996x + 1996 \cdot 1998 = 1997^2.$$

Do 1997 là số nguyên tố nên ta có

$$x - 1998 = \pm 1, \pm 1997, \pm 1997^2.$$

Từ đó suy ra 6 nghiệm sau

$$(x, y) = (1999, 1997^2 + 1996), (1997, -1997^2 + 1996), (3995, 3993), \\ (1, -1), (1997^2 + 1998, 1997), (-1997^2 + 1998, 1995).$$

**Ví dụ 2.3.6 (Korea 1997).** Tìm tất cả các số nguyên  $x, y, z$  thoả mãn

$$x^2 + y^2 + z^2 - 2xyz = 0.$$

### Giải

Ta chứng minh phương trình đã cho chỉ có nghiệm  $(x, y, z) = (0, 0, 0)$ .

Giả sử  $(x, y, z)$  là nghiệm của phương trình đã cho. Đã thấy  $xyz$  không thể cùng lẻ nên  $xyz \vdots 2$ . Từ đó suy ra  $x^2 + y^2 + z^2 = 2xyz \vdots 4$ .

Do mỗi số chính phương khi chia cho 4 chỉ có thể có số dư là 0 hoặc 1 nên ta có cả ba số  $x, y, z$  đều chẵn. Đặt  $x = 2x_1, y = 2y_1, z = 2z_1$ , ta có

$$x_1^2 + y_1^2 + z_1^2 = 4x_1y_1z_1.$$

Tương tự như trên ta có cả ba số  $x_1, y_1, z_1$  đều chẵn. Từ đó có thể đặt  $x_1 = 2x_2, y_1 = 2y_2, z_1 = 2z_2$ , với  $x_2, y_2, z_2$  thoả mãn phương trình

$$x_2^2 + y_2^2 + z_2^2 = 8x_2y_2z_2.$$

Giả sử  $x, y, z$  đồng thời chia hết cho  $2^n$ , với  $n$  là một số nguyên dương nào đó. Khi đó,  $x = 2^n x_n, y = 2^n y_n, z = 2^n z_n$  với  $x_n, y_n, z_n$  thoả mãn phương trình

$$x_n^2 + y_n^2 + z_n^2 = 2^{n+1} x_n y_n z_n.$$

Tiếp tục xét đồng dư modulo 4 ta có cả ba số  $x_n, y_n, z_n$  đều chẵn. Do đó  $x, y, z$  đồng thời chia hết cho  $2^{n+1}$ . Theo quy nạp ta có  $x, y, z$  đồng thời chia hết cho  $2^n$  với mọi  $n$ , từ đó suy ra  $(x, y, z) = (0, 0, 0)$ .

**Ví dụ 2.3.7 (Taiwan 1998).** Tồn tại hay không các số nguyên dương  $x, y, z, u, v > 1998$  thoả mãn phương trình sau:

$$x^2 + y^2 + z^2 + u^2 + v^2 = xyzuv - 65.$$

### Giải

Ta có phương trình

$$x^2 + y^2 + z^2 + u^2 + v^2 = xyzuv - 65.$$

có nghiệm nguyên dương  $(x, y, z, u, v) = (1, 2, 3, 4, 5)$  và  $(1, 1, 3, 8, 10)$ .

Ta sẽ xây dựng bằng quy nạp các nghiệm  $(x_n, y_n, z_n, u_n, v_n)$  của phương trình thoả mãn

$$x_n \leq y_n \leq z_n \leq u_n \leq v_n \quad x_n < u_n \quad v_n < v_{n+1}$$

với mọi  $n \geq 1$ .

Với  $n = 1$  chọn  $(x_1, y_1, z_1, u_1, v_1) = (1, 2, 3, 4, 5)$ . Giả sử đã xây dựng được nghiệm  $(x_n, y_n, z_n, u_n, v_n)$  với  $x_n < v_n$ . Xét phương trình bậc hai

$$x^2 - (y_n z_n u_n v_n)x + (y_n^2 + z_n^2 + u_n^2 + v_n^2 + 65) = 0$$

có  $x = x_n$  là một nghiệm. Theo định lý  $\epsilon$  ta có nghiệm còn lại là

$$x = \bar{x}_n = y_n z_n u_n v_n = v_n$$

là một số nguyên. Lại có

$$x_n \bar{x}_n = y_n^2 + z_n^2 + u_n^2 + v_n^2 + 65 > v_n^2$$

nên  $\bar{x}_n > v_n^2 > x_n$ . Hiển nhiên  $(y_n, z_n, u_n, v_n, \bar{x}_n)$  cũng là nghiệm của phương trình đã cho. Chọn  $(x_{n+1}, y_{n+1}, z_{n+1}, u_{n+1}, v_{n+1}) = (y_n, z_n, u_n, v_n, \bar{x}_n)$  ta có  $x_{n+1} = y_n \leq v_n < \bar{x}_n = v_{n+1}$  nên

$$x_{n+1} \leq y_{n+1} \leq z_{n+1} \leq u_{n+1} \leq v_{n+1} \quad x_{n+1} < v_{n+1} \quad v_n < v_{n+1}.$$

Tức là xây dựng được nghiệm  $(x_{n+1}, y_{n+1}, z_{n+1}, u_{n+1}, v_{n+1})$ .

Từ cách xây dựng nghiệm như trên, sau một số hữu hạn lần xây dựng ta có  $x_n > 1998$ , từ đó suy ra phương trình đã cho có nghiệm nguyên  $x, y, z, u, v > 1998$ .

**Ví dụ 2.3.8 ( Balkan 1998).** Chứng minh rằng phương trình

$$y^2 = x^5 - 4$$

không có nghiệm nguyên.

### Giải

Xét phương trình theo modulo 11. Ta có

$$(x^5)^2 = x^{10} \equiv 0 \text{ hoặc } 1 \pmod{11}, \quad \forall x.$$

Do đó,  $x^5 \equiv -1, 0 \text{ hoặc } 1 \pmod{11}$ , suy ra về phải đồng dư với 6, 7 hoặc 8 modulo 11. Mặt khác, vì một số chính phương chỉ có thể có số dư là 0, 1, 3, 4, 5 hoặc 9 modulo 11 nên phương trình đã cho không có nghiệm nguyên.

**Ví dụ 2.3.9 (Bulgaria 1999).** Tìm tất cả các số nguyên  $(x, y)$  sao cho

$$x^3 = y^3 + 2y^2 + 1.$$

**Giải**

Giả sử  $(x, y)$  là các số nguyên thoả mãn phương trình đã cho. Nếu  $y^2 + 3y > 0$  thì

$$y^3 < x^3 = y^3 + 2y^2 + 1 < y^3 + 2y^2 + (y^2 + 3y) + 1 = (y + 1)^3,$$

Vô lý, vì  $x, y$  là các số nguyên thì không thể xảy ra  
 $y < x < y + 1 \Leftrightarrow y^3 < x^3 < (y + 1)^3$ . Vậy  $y^2 + 3y \leq 0$ , tức là  
 $y = -3, -2, -1$  hoặc  $0$ . Từ đó suy ra các nghiệm

$$(x, y) = (1, 0), (1, -2), (-2, -3).$$

**Ví dụ 2.3.10 (Italy 1999).** Tìm tất cả các số nguyên dương  $(x, k, n)$  thoả mãn

$$3^k - 1 = x^n.$$

**Giải**

Ta sẽ chứng minh rằng tất cả các số nguyên dương thoả mãn đều có dạng  $(3^k - 1, k, 1)$  với  $k$  là một số nguyên dương, hoặc  $(2, 2, 3)$ .

Với  $n = 1$  hiển nhiên  $(x, k, n) = (3^k - 1, k, 1)$ . Xét  $n > 1$ , nếu  $n$  là một số chẵn thì

$$3^k = x^n + 1 = (x^{n/2})^2 + 1 \equiv 1 \pmod{2}$$

vô lý. Hiển nhiên  $x > 1$ . Vậy  $n > 2$ ,  $n$  lẻ và  $x \geq 2$ . Ta có

$$3^k = x^n + 1 = (x + 1)(1 - x + x^2 - x^3 + \cdots + (-1)^{n-1}x^{n-1})$$

nên cả  $x + 1$  và  $1 - x + x^2 - x^3 + \cdots + (-1)^{n-1}x^{n-1}$  đều là các luỹ thừa của 3. Vì

$$x + 1 < x^2 - x + 1 < 1 - x + x^2 - x^3 + \cdots + (-1)^{n-1}x^{n-1}$$

nên  $x + 1$  là một ước số của  $1 - x + x^2 - x^3 + \cdots + (-1)^{n-1}x^{n-1}$ , do đó

$$0 \equiv 1 - x + x^2 - x^3 + \cdots + (-1)^{n-1}x^{n-1} \equiv n \pmod{x + 1}.$$

Suy ra  $n \mid x + 1$  nên  $n \mid 3$ .

Đặt  $y = x^{(n-k)/3}$ .

$$3^k = y^3 + 1 = (y+1)(y^2 - y + 1).$$

Tương tự chứng minh trên ta có  $y+1$  phải là lũy thừa của 3. Đặt  $y+1 = 3^l$ . Nếu  $l > 1$  ta có

$$3^{3l-1} < 3^k = y^3 + 1 = (3^l - 1)^3 + 1 = 3^{3l} - 3^{2l+1} + 3^{l+1} < 3^{3l}.$$

Vô lý. Vậy  $l = 1$ ,  $y = 2$ ,  $k = 2$ , suy ra  $(x, k, n) = (2, 2, 3)$ .

## BÀI TẬP

**Bài 1 (Italy 1999).** Chứng minh rằng với mỗi số nguyên tố  $p$ , phương trình

$$2^p + 3^p = a^n$$

không có nghiệm nguyên  $(a, n)$  với  $a, n > 1$ .

**Bài 2 (Taiwan 1999).** Tìm tất cả các số nguyên dương  $(x, y, z)$  thoả mãn

$$(x+1)^{y+1} + 1 = (x+2)^{z+1}.$$

**Bài 3 (UK 1999).** Tìm một hằng số  $c$  sao cho phương trình

$$xy^2 - y^2 - x + y = c$$

có đúng ba nghiệm nguyên dương  $x, y$ .

**Bài 4 (Austrian-Polish 1999).** Tìm tất cả các cặp số nguyên dương  $(x, y)$  thoả mãn phương trình sau

$$x^{x+y} = y^{y-x}.$$

**Bài 5 (Hungary 2000).** Tìm tất cả các số nguyên tố  $p$  sao cho tồn tại các số nguyên dương  $n, x, y$  thoả mãn

$$p^n = x^3 + y^3.$$

**Bài 6 (Romania 2000).** Chứng minh rằng tồn tại vô số bộ 4 số nguyên dương  $(x, y, z, t)$  có ước số chung lớn nhất bằng 1 thoả mãn

$$x^3 + y^3 + z^2 = t^4.$$

**Bài 7 (Belarus 1999).** Tìm tất cả các số nguyên  $x, y$  thoả mãn

$$x^6 + x^2y = y^3 + 2y^2.$$

**Bài 8 (Bulgaria 1999).** Tìm tất cả các số tự nhiên  $(x, y, z)$ ,  $y$  là một số nguyên tố,  $z$  không chia hết cho 3 và  $y$  sao cho

$$x^3 - y^3 = z^2.$$

## LỜI GIẢI

### Bài 1 (Italy 1999).

Với  $p = 2$  ta có  $a^n = 13$  nên phương trình không có nghiệm nguyên  $(a, n)$  với  $a, n > 1$ . Với  $p > 2$ , ta có  $2^p + 3^p \not\equiv 0 \pmod{5}$ , do đó

$$2^p + (5 - 2)^p \equiv 2^p + \left( C_p^1 5(-2)^{p-1} + (-2)^p \right) \equiv 5p2^{p-1} \pmod{25},$$

suy ra  $p \nmid 5$ . Vậy  $p = 5$ , khi đó

$$a^n = 2^5 + 3^5 = 5^2 \cdot 11.$$

Phương trình này không có nghiệm nguyên  $(a, n)$  với  $a, n > 1$ .

Vậy trong mọi trường hợp, phương trình đã cho không có nghiệm nguyên  $(a, n)$  với  $a, n > 1$ , điều phải chứng minh.

### Bài 2 (Taiwan 1999).

Xét  $a = x + 1, b = y + 1, c = z + 1$ , khi đó  $a, b, c \geq 2$  và

$$\begin{aligned} a^b + 1 &= (a+1)^c \\ ((a+1)-1)^b + 1 &= (a+1)^c. \end{aligned}$$

Xét đồng dư modulo  $(a+1)$  ta có  $(-1)^b + 1 \equiv 0 \pmod{a+1}$  nên  $b$  là một số lẻ.

Xét đồng dư modulo  $(a+1)^2$  ta có

$$C_b^1(a+1)(-1)^{b-1} + (-1)^b + 1 \equiv 0 \pmod{(a+1)^2}$$

nên  $b \nmid (a+1)$  nên  $a$  là một số chẵn. Mặt khác, xét đồng dư modulo  $a^2$  ta có

$$1 \equiv C_c^1 a + 1 \pmod{a^2},$$

nên  $c \nmid a$  và  $c$  là một số chẵn. Đặt  $a = 2a_1, c = 2c_1$ . Ta có

$$2^b a_1^b = a^b = (a+1)^c - 1 = ((a+1)^{c_1} - 1)((a+1)^{c_1} + 1).$$

Ta có

$$((a+1)^{c_1} - 1, (a+1)^{c_1} + 1) = 2.$$

Do đó, từ  $(a+1)^{c_1} - 1 \vdots 2a_1$  ta có

$$\begin{aligned}(a+1)^{c_1} - 1 &= 2a_1^b, \\ (a+1)^{c_1} + 1 &= 2^{b-1}.\end{aligned}$$

Suy ra  $2^{b-1} > 2a_1^b$  nên  $a_1 = 1$ . Từ đó ta có  $c_1 = 1, b = 3$ .

Vậy nghiệm duy nhất của phương trình đã cho là  $(x, y, z) = (1, 2, 1)$ .

### Bài 3 (UK 1999).

Ta có phương trình đã cho tương đương với phương trình

$$x = \frac{y(y-1) + c}{(y+1)(y-1)}.$$

Vì

$$y(y-1) + c \equiv (-1)(-2) + c \equiv c + 2 \pmod{y+1},$$

$$y(y-1) + c \equiv c \pmod{y-1}.$$

nên  $c \equiv 0 \pmod{y-1}, c \equiv -2 \pmod{y+1}$ . Từ đó ta có

$$c \equiv y-1 \pmod{[y-1, y+1]}.$$

Nếu  $y$  chẵn ta có  $[y-1, y+1] = y^2 - 1$ . Nếu  $y$  lẻ ta có  $[y-1, y+1] = (y^2 - 1)/2$ .

Với  $y = 2, 3, 11$  ta có  $c \equiv 1 \pmod{3}, c \equiv 2 \pmod{4}, c \equiv 10 \pmod{60}$ .

Chọn  $c = 10$ . Để  $x$  là một số nguyên thì  $10 \mid y-1$  nên  $y = 2, 3, 6$  hoặc  $11$ . Thay vào ta tìm được các giá trị tương ứng của  $x$  là  $4, 2, 2/7, 1$ . Do đó, với  $c = 10$  phương trình có đúng ba nghiệm là

$$(x, y) = (4, 2), (2, 3), (1, 11).$$

Vậy  $x = 10$  là một giá trị thỏa mãn.

### Bài 4 (Austrian-Polish 1999).

Đặt  $a = \frac{b}{c}$ , ta có  $a^b = b^a$ ,  $b = a^{\frac{a}{c}}$ ,  $\gcd(a, b) = 1$  và phương trình

$$(ac)^{c(a+b)} = (a^{\frac{a}{c}})^{c(b+a)}$$

$$(ac)^{a+b} = (b^c)^{a+b}$$

$$a^{a+b}c^{2a} = b^{b+a}.$$

Từ đó suy ra  $b^{b-a} : a^{a+b}$ . Do  $(a, b) = 1$  nên  $a = 1$ , phương trình đã cho trở thành

$$b^{b-1} = c^2$$

là một số chính phương. Vậy  $b$  là một số lẻ hoặc  $b$  là một số chính phương.

Nếu  $b = 2n + 1$  thì  $c = (2n + 1)^n$ .

Nếu  $b = n^2$  thì  $c = n^{n^2-1}$ .

Do đó, phương trình đã cho chỉ có thể có các nghiệm là

$$((2n+1)^n, (2n+1)^{n+1}), \quad (n^{n^2-1}, n^{n^2+1}),$$

trong đó  $n$  là một số tự nhiên tùy ý. Hiển nhiên những cặp  $(x, y)$  như trên thoả mãn phương trình đã cho.

### Bài 5 (Hungari 2000).

Ta có  $p = 2$  hoặc  $p = 3$  thoả mãn điều kiện đã cho vì  $2^1 = 1^3 + 1^3, 3^2 = 1^3 + 2^3$ .

Ta sẽ chứng minh không tồn tại  $p > 3$  thoả mãn điều kiện đề bài.

Phản chứng, giả sử tồn tại số nguyên tố  $p > 3$  và các số nguyên dương  $n, x, y$  thoả mãn  $p^n = x^3 + y^3$ . Chọn bộ  $(n, x, y)$  sao cho  $n$  bé nhất, khi đó ta có  $(x, p) = (y, p) = 1$ .

Vì  $p \neq 2$  nên  $(x, y) \neq (1, 1)$ , do đó  $x+y, x^2-xy+y^2 = (x-y)^2+xy > 1$ . Do  $p$  nguyên tố và  $x^3+y^3 = (x+y)(x^2-xy+y^2) = p^n$  nên đồng thời  $x+y$  và  $x^2-xy+y^2$  chia hết cho  $p$ . Do đó,  $(x+y)^2 - (x^2-xy+y^2) = 3xy : p$  và  $xy : p$  vì  $(p, 3) = 1$ . Như vậy ta có cả  $x+y$  và  $xy$  đều chia hết cho  $p$ , suy ra cả  $x$  và  $y$  đều chia hết cho  $p$ . Mâu thuẫn với cách chọn bộ  $n, x, y$  bé nhất. Vậy điều giả sử là sai, tức là ta có điều phải chứng minh.

### Bài 6 (Romania 2000).

Ta có đẳng thức

$$(a+1)^4 - (a-1)^4 = 8a^3 + 8a.$$

Đặt  $a = k^3$  với  $k$  chẵn, đẳng thức trên trở thành

$$(2k^3)^3 + (2k)^3 + [(k^3 - 1)^2]^2 = (k^3 + 1)^4.$$

Vì  $k^3 + 1$  lẻ nên  $(2k^3, k^3 + 1) = (k^3, k^3 + 1) = 1$ . Do đó mọi bộ 4 số nguyên có dạng

$$(x, y, z, t) = (2k^3, 2k, (k^3 - 1)^2, k^3 + 1), \quad k > 0, \quad k \text{ chẵn}$$

đều thoả mãn điều kiện đã cho. Vậy có vô số bộ 4 số nguyên dương  $(x, y, z, t)$  có ước số chung lớn nhất bằng 1 thoả mãn điều kiện đề bài.

# Chương 3

## Hàm số học

### 1 Phân nguyên

Trong chương 1 ta đã định nghĩa phân nguyên  $[x]$  của một số nguyên  $x$  là số nguyên lớn nhất không vượt quá  $x$ . Tức là  $[x]$  là số nguyên duy nhất thoả mãn  $[x] \leq x < [x] + 1$ . Hiệu  $0 \leq \{x\} = x - [x] < 1$  được gọi là phân lẻ của  $x$ . Các tính chất của hàm  $[x]$  được liệt kê trong định lý sau

#### Định lý 3.1.1.

Cho  $x, y$  là các số thực, khi đó

1.  $[x] \leq x < [x] + 1, \quad x - 1 < [x] \leq x, \quad 0 \leq x - [x] < 1.$
2. Với mọi số nguyên  $m$ ,  $[x + m] = [x] + m$ .
3.  $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$ .
4.  $[x] + [-x] = \begin{cases} 0 & \text{nếu } x \text{ là một số nguyên,} \\ -1 & \text{nếu trái lại.} \end{cases}$
5.  $-[-x]$  là số nguyên nhỏ nhất lớn hơn hoặc bằng  $x$ .
6. Nếu  $m$  là một số nguyên thì  $\left[ \frac{[x]}{m} \right] = \left[ \frac{x}{m} \right]$ .
7. Nếu  $a, m$  là các số nguyên dương thì  $[m/a]$  là số các bội số của  $a$  nằm trong khoảng  $[1, m]$ .

### Chứng minh

1, Hiển nhiên suy ra từ định nghĩa.

2, Chỉ cần chứng minh cho  $0 \leq x < 1$ . Khi đó,  $m \leq x + m < m + 1$  nên theo định nghĩa,  $[x] = 0$ ,  $[x + m] = m = [x] + m$ . Tức là  $[x + m] = [x] + m$ .

3, Do  $f(x) = [x]$  là một hàm không giảm và  $[y] \leq y < [y] + 1$  nên từ 2, ta có

$$[x] + [y] = [x + [y]] \leq [x + y] \leq [x + ([y] + 1)] = [x] + [y] + 1.$$

Tức là  $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$ .

4, Nếu  $x = m$  là một số nguyên thì  $[x] = m$ ,  $[-x] = -m$  nên  $[x] + [-x] = 0$ .

Nếu  $x$  không là một số nguyên,  $x = m + h$  với  $m$  là một số nguyên và  $0 < h < 1$  thì  $-x = -m - 1 + (1 - h)$  với  $0 < 1 - h < 1$  nên theo định nghĩa  $[x] = m$  và  $[-x] = -m - 1$ . Do đó,  $[x] + [-x] = -1$ .

5, Chỉ cần chứng minh cho trường hợp  $x$  không phải là một số nguyên. Giả sử  $x = m + h$  với  $m$  là một số nguyên và  $0 < h < 1$ . Khi đó như chứng minh trên ta có  $[-x] = -m - 1$  nên  $-[-x] = m + 1$  chính là số nguyên nhỏ nhất lớn hơn hoặc bằng  $x$ .

6, Giả sử  $\lfloor x/m \rfloor = k$ . Khi đó,  $k \leq x/m < k + 1$  nên  $km \leq x < k(m + 1)$ . Do  $[x]$  là số nguyên dương lớn nhất không vượt quá  $x$  nên  $km \leq [x] \leq x < k(m + 1)$ . Do đó  $km \leq [x] < k(m + 1)$ , suy ra  $k \leq [x]/m < k + 1$ , tức là

$$\left\lfloor \frac{[x]}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor.$$

7, Giả sử  $a, 2a, \dots, na$  là tất cả các bội số của  $a$  nằm trong khoảng  $[1, m]$ , ta cần chứng minh  $\lfloor m/a \rfloor = n$ . Thật vậy, do  $a, 2a, \dots, na$  là tất cả các bội số của  $a$  nằm trong khoảng  $[1, m]$  nên  $na \leq m < (n + 1)a$ . Do đó,  $n \leq m/a < n + 1$ . Theo định nghĩa ta có  $\lfloor m/a \rfloor = n$ .

Định lý được chứng minh.

**Định lý 3.1.2 (Công thức Polignac).** Cho  $p$  là một số nguyên tố, khi đó

với mỗi lũy thừa  $p^i$  và sao cho  $p^k$  là ước số của  $n!$  là

$$k = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

### Chứng minh

Gọi  $e_i$  là số các số chia hết cho  $p^i$  trong khoảng  $[1, n]$ . Khi đó số các số trong khoảng  $[1, n]$  chia hết cho  $p^i$  mà không chia hết cho  $p^{i+1}$  là  $f_i = e_i - e_{i+1}$  và số mũ lớn nhất  $k$  sao cho  $p^k$  là ước số của  $n!$  có dạng  $k = \sum_{i=1}^{\infty} i f_i$ . Theo định lý 3.1.1 ta có

$$e_i = \left\lfloor \frac{n}{p^i} \right\rfloor, \quad f_i = \left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor.$$

Do đó

$$k = \sum_{i=1}^{\infty} i f_i = \sum_{i=1}^{\infty} i \left( \left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor \right) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Định lý được chứng minh.

**Ví dụ 3.1.1.** Chứng minh rằng với mọi số nguyên  $n$ ,

$$\left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n+4}{4} \right\rfloor + \left\lfloor \frac{n-1}{2} \right\rfloor = n.$$

### Giải

Xét  $n = 4k$  ta có

$$\left\lfloor \frac{n+2}{4} \right\rfloor = k, \quad \left\lfloor \frac{n+4}{4} \right\rfloor = k+1, \quad \left\lfloor \frac{n-1}{2} \right\rfloor = 2k-1,$$

do đó

$$\left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n+4}{4} \right\rfloor + \left\lfloor \frac{n-1}{2} \right\rfloor = n.$$

Xét  $n = 4k+1$  ta có

$$\left\lfloor \frac{n+2}{4} \right\rfloor = k, \quad \left\lfloor \frac{n+4}{4} \right\rfloor = k+1, \quad \left\lfloor \frac{n-1}{2} \right\rfloor = 2k,$$

do đó

$$\left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n+4}{4} \right\rfloor + \left\lfloor \frac{n-1}{2} \right\rfloor = n.$$

Tương tự với  $n = 4k+2, 4k+3$  ta cũng có điều phải chứng minh.

**Ví dụ 3.1.2.** Cho  $M = 19871987$ , dãy  $\{x_n\}_{n \geq 1}$  các số nguyên thoả mãn

$$x_1 = M, \quad x_{n+1} = \left\lfloor \frac{x_n + \left\lfloor \frac{M}{x_n} \right\rfloor}{2} \right\rfloor, \quad \text{với mọi } n = 1, 2, \dots$$

Tính

$$\min \{x_n : 1 \leq n \leq M\}.$$

### Giải

Đặt  $\lfloor \sqrt{M} \rfloor = \alpha$ , khi đó  $\alpha \in \mathbb{Z}^+$  và  $\alpha^2 \leq M < (\alpha+1)^2$ . Ta có

$$\left\lfloor \frac{a + \lfloor b \rfloor}{2} \right\rfloor = \left\lfloor \frac{a + b}{2} \right\rfloor$$

nên

$$x_{n+1} = \left\lfloor \frac{x_n + \frac{M}{x_n}}{2} \right\rfloor \geq \lfloor \sqrt{M} \rfloor = \alpha.$$

Do  $M < (\alpha+1)^2$  nên nếu  $x_n \geq \alpha+1$  thì  $M/x_n < x_n$  và

$$x_{n+1} = \left\lfloor \frac{x_n + \frac{M}{x_n}}{2} \right\rfloor < \left\lfloor \frac{x_n + x_n}{2} \right\rfloor = x_n.$$

Tức là, nếu  $x_n \geq \alpha+1$  thì  $x_{n+1} \leq x_n - 1$ . Từ đó suy ra

$$\min \{x_n : 1 \leq n \leq M\} = \alpha.$$

**Ví dụ 3.1.3.** Cho  $m, n$  là các số nguyên,  $c$  là một số vô tỷ dương và  $d = 1/c$ . Chứng minh rằng

$$\sum_{j=0}^{\lfloor m+nc \rfloor} \lfloor n+1 + (m+j)c \rfloor = \sum_{j=0}^{\lfloor n+md \rfloor} \lfloor m+1 + (n+j)c \rfloor.$$

**Giai**

Trong mặt phẳng  $Oxy$  xét hai điểm  $A(0, m+nc)$  và  $B(n+md, 0)$ . Xét số điểm nguyên nằm trong tam giác  $OAB$  theo hai cách.

Cách thứ nhất, với mỗi số nguyên  $j$ ,  $0 \leq j \leq [n+md]$  ta tính số các số nguyên  $i$  sao cho điểm  $(j, i)$  nằm trong tam giác  $OAB$  (coi  $j$  tương ứng với điểm  $(j, 0)$  trên  $OB$ ). Đặt  $x_0 = n+md$ ,  $y_0 = m+nc$ , khi đó đường thẳng có phương trình  $x = j$  cắt đoạn  $AB$  tại điểm có tung độ bằng

$$\frac{(x_0 - j)y_0}{x_0} = \frac{(n+md - j)(m+nc)}{n+md} = \frac{(n + \frac{m}{c} - j)(n + \frac{m}{c})c}{n + \frac{m}{c}} = m + (n-j)c.$$

Do đó, số các số nguyên  $i$  để điểm  $(j, i)$  nằm trong tam giác  $OAB$  là

$$1 + [m + (n - j)c] = [m + 1 + (n - j)c].$$

Từ đó suy ra số các điểm nguyên  $(j, i)$  nằm trong tam giác  $OAB$  là

$$N = \sum_{0 \leq j \leq [n+md]} [m + 1 + (n - j)c].$$

Cách thứ hai, với mỗi số nguyên  $i$ ,  $0 \leq i \leq [m+nc]$  ta tính số các số nguyên  $j$  sao cho điểm  $(j, i)$  nằm trong tam giác  $OAB$  (coi  $i$  tương ứng với điểm  $(0, i)$  trên  $OA$ ). Bằng cách tính hoàn toàn tương tự ta có số các điểm nguyên  $(j, i)$  nằm trong tam giác  $OAB$  là

$$N = \sum_{0 \leq i \leq [m+nc]} [n + 1 + (m - i)d].$$

Từ đó suy ra điều phải chứng minh.

**Ví dụ 3.1.4.** Tìm số nguyên dương  $n$  lớn nhất sao cho  $2003!$  chia hết cho  $5^n$ .

**Giải**

Hiển nhiên số  $n$  cần tìm chính là số mũ của 5 trong phân tích  $2003!$

Tích các thừa số nguyên tố. Theo công thức Polignac,

$$\begin{aligned} n &= \sum_{i=1}^{\infty} \left\lfloor \frac{2003}{5^i} \right\rfloor \\ &= \left\lfloor \frac{2003}{5} \right\rfloor + \left\lfloor \frac{2003}{25} \right\rfloor + \left\lfloor \frac{2003}{125} \right\rfloor + \left\lfloor \frac{2003}{625} \right\rfloor \\ &= 400 + 80 + 16 + 3 \\ &= 499. \end{aligned}$$

Vậy  $n = 499$  là số cần tìm.

**Ví dụ 3.1.5.** Cho  $n$  là một số nguyên dương thoả mãn  $n!$  có đúng 2002 chữ số 0 đứng tận cùng. Chứng minh rằng  $n \leq 8024$ .

### Giải

Giả sử  $n! = 2^\alpha 5^\beta q$ , trong đó  $(q, 2) = (q, 5) = 1$ . Theo công thức Polignac ta có

$$\alpha = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{2^i} \right\rfloor > \beta = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{5^i} \right\rfloor.$$

Do đó  $n! : 10^\beta$ ,  $n! \vdash 10^{\beta+1}$  nên số chữ số 0 đứng tận cùng trong biểu diễn thập phân của  $n!$  là  $\beta$ . Vậy ta cần tìm  $n$  nhỏ nhất sao cho

$$\beta = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{5^i} \right\rfloor = 2002.$$

Với mỗi  $n$  đặt

$$p(n) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{5^i} \right\rfloor.$$

ta có  $p(n) \leq p(n+1)$  với mọi  $n \geq 1$  và

$$\begin{aligned} p(8024) &= \left\lfloor \frac{8024}{5} \right\rfloor + \left\lfloor \frac{8024}{25} \right\rfloor + \left\lfloor \frac{8024}{125} \right\rfloor + \left\lfloor \frac{8024}{625} \right\rfloor + \left\lfloor \frac{8024}{3125} \right\rfloor \\ &= 1604 + 320 + 64 + 12 + 2 \\ &= 2002. \end{aligned}$$

Do đó  $n \leq 3024$ , điều phải chứng minh.

**Ví dụ 3.1.6 (Canada 1998).** Tìm số các nghiệm thực của phương trình

$$\left\lfloor \frac{a}{2} \right\rfloor + \left\lfloor \frac{a}{3} \right\rfloor + \left\lfloor \frac{a}{5} \right\rfloor = a.$$

### Giải

Vì  $a$  phải là một số nguyên nên  $a$  cũng phải là một số nguyên. Đặt  $a = 30q + r$  trong đó  $p, r$  là các số nguyên,  $0 \leq r \leq 29$ . Ta có phương trình đã cho tương đương với phương trình sau

$$31q + \left\lfloor \frac{r}{2} \right\rfloor + \left\lfloor \frac{r}{3} \right\rfloor + \left\lfloor \frac{r}{5} \right\rfloor = 30q + r,$$

hay

$$q = r - \left( \left\lfloor \frac{r}{2} \right\rfloor + \left\lfloor \frac{r}{3} \right\rfloor + \left\lfloor \frac{r}{5} \right\rfloor \right).$$

Như vậy, với mỗi giá trị của  $r$  tồn tại duy nhất một giá trị của  $q$  sao cho  $a = 30q + r$  thoả mãn phương trình đã cho. Do  $r$  có thể nhận 30 giá trị (từ 0 đến 29) nên phương trình đã cho có 30 nghiệm.

**Ví dụ 3.1.7 (Czech-Slovak 1998).** Tìm tất cả các số thực  $x$  thoả mãn

$$x[x[x[x]]] = 88.$$

### Giải

Đặt  $f(x) = x[x[x[x]]]$  với mọi số thực  $x$ . Trước hết ta chứng minh rằng

$$|f(a)| > |f(b)| \quad \text{với mọi } a, b \in R \text{ thoả mãn } ab > 0, |a| > |b| > 1.$$

Thật vậy, từ  $ab > 0, |a| > |b| > 1$  suy ra  $|\lfloor a \rfloor| \geq |\lfloor b \rfloor| \geq 1$ . Nhân  $|a| > |b| > 1$  vào ta có

$$|a \lfloor a \rfloor| \geq |b \lfloor b \rfloor| \geq 1.$$

Dễ thấy  $a \lfloor a \rfloor$  có cùng dấu với  $b \lfloor b \rfloor$ ,  $a \lfloor a \lfloor a \rfloor \rfloor$  có cùng dấu với  $b \lfloor b \lfloor b \rfloor \rfloor$  nên tương tự như trên ta có

$$|a \lfloor a \lfloor a \rfloor \rfloor| \geq |b \lfloor b \lfloor b \rfloor \rfloor| \geq 1, \quad |a \lfloor a \lfloor a \lfloor a \rfloor \rfloor| \geq |b \lfloor b \lfloor b \lfloor b \rfloor \rfloor| \geq 1.$$

Từ đó suy ra  $|f(a)| > |f(b)|$ .

Tì  $f(x) = 0$  với mọi  $|x| < 1$ ,  $f(\pm 1) = 1$  nên nếu  $f(x_0) = 88$  thì  $|x_0| > 1$ . Xét hai trường hợp sau:

Trường hợp 1:  $x_0 > 1$ . Từ chứng minh trên,  $f(x)$  đơn điệu tăng trên khoảng  $(1, \infty)$  nên nếu tồn tại thì  $x_0$  là duy nhất. Ta có

$$f(3) = 81 < 88 = f(x_0) < f(4) = 256$$

nên  $3 < x_0 < 4$  và  $\lfloor x_0 \rfloor = 3$ . Từ đó,  $f(x_0) = x_0 \lfloor x_0 \lfloor 3x_0 \rfloor \rfloor = 88$ . Mặt khác,

$$f(3) = 81 < 88 = f(x_0) < f\left(\frac{10}{3}\right) = 110$$

nên  $3 < x_0 < 10/3$  suy ra  $\lfloor x_0 \lfloor x_0 \rfloor \rfloor = 9$ . Tiếp tục,

$$f(3) = 81 < 88 = f(x_0) < f\left(\frac{29}{9}\right) = \frac{29^2}{9}$$

nên  $3 < x_0 < 29/9$ , do đó

$$27 < \lfloor x_0 \lfloor x_0 \lfloor x_0 \rfloor \rfloor \rfloor = \lfloor 9x_0 \rfloor < 29 = \left\lfloor 9\frac{29}{9} \right\rfloor$$

suy ra  $\lfloor x_0 \lfloor x_0 \lfloor x_0 \rfloor \rfloor \rfloor = 28$ . Từ đó  $f(x_0) = 28x_0 = 88$  nên  $x_0 = 22/7$ .

Trường hợp 2:  $x_0 < -1$ . Từ chứng minh trên,  $f(x)$  đơn điệu giảm trên khoảng  $(-\infty, -1)$ . Tương tự trường hợp 1 ta có

$$|f(-3)| = 81 < 88 = f(x_0) < \left|f\left(\frac{-112}{37}\right)\right| = 112$$

nên  $-3 > x_0 > -112/37$  và  $\lfloor x_0 \lfloor x_0 \lfloor x_0 \rfloor \rfloor \rfloor = -37$ . Từ đó suy ra  $x = -88/37 > -3$ , vô lý. Vậy không tồn tại nghiệm  $x_0 < -1$ .

Tóm lại, tồn tại duy nhất nghiệm  $x_0 = 22/7$ .

**Ví dụ 3.1.8.** Tìm tất cả các số nguyên dương  $n$  sao cho tập hợp

$$A_n = \{1, 2, \dots, n\}$$

có số các số chia hết cho 3 bằng số các số chia hết cho 5 hoặc 7 hoặc

Gửi

Ta có số các số chia hết cho 3, 5, 7, 35 trong tập hợp  $\mathbb{N}_n$  lần lượt là

$$\left\lfloor \frac{n}{3} \right\rfloor, \quad \left\lfloor \frac{n}{5} \right\rfloor, \quad \left\lfloor \frac{n}{7} \right\rfloor, \quad \left\lfloor \frac{n}{35} \right\rfloor.$$

Do đó, ta cần tìm tất cả các số nguyên dương  $n$  sao cho

$$\left\lfloor \frac{n}{3} \right\rfloor = \left\lfloor \frac{n}{5} \right\rfloor + \left\lfloor \frac{n}{7} \right\rfloor - \left\lfloor \frac{n}{35} \right\rfloor.$$

Đặt  $n = 35k + r$  với  $0 \leq r < 35$  ta có đẳng thức trên tương đương với

$$\left\lfloor \frac{35k + r}{3} \right\rfloor = \left\lfloor 7k + \frac{r}{5} \right\rfloor + \left\lfloor 5k + \frac{r}{7} \right\rfloor - \left\lfloor k + \frac{r}{35} \right\rfloor.$$

Vì  $0 \leq r < 35$  nên  $\lfloor r/35 \rfloor = 0$  và đẳng thức trở thành

$$11k + \left\lfloor \frac{2k + r}{3} \right\rfloor = 11k + \left\lfloor \frac{r}{5} \right\rfloor + \left\lfloor \frac{r}{7} \right\rfloor \quad \text{hay} \quad \left\lfloor \frac{2k + r}{3} \right\rfloor = \left\lfloor \frac{r}{5} \right\rfloor + \left\lfloor \frac{r}{7} \right\rfloor$$

Bằng cách thay trực tiếp  $r = 0, 1, 2, \dots, 34$  và tính vế phải ta tìm được các bộ  $(k, r)$  sau

$$\begin{aligned} (0, 1), \quad (0, 2), \quad (0, 5), \quad (0, 7), \quad (0, 8), \quad (0, 10), \\ (0, 11), \quad (0, 14), \quad (0, 15) \\ (0, 16), \quad (0, 17), \quad (0, 20), \quad (0, 21), \quad (0, 22), \quad (0, 23), \\ (0, 25), \quad (0, 26), \quad (0, 28) \\ (0, 29), \quad (0, 30), \quad (0, 31), \quad (0, 32), \quad (1, 15), \quad (1, 21), \quad (1, 30). \end{aligned}$$

Từ đó suy ra số các số  $n$  cần tìm là

$$\begin{aligned} 1, 2, 5, 7, 8, 10, 11, 14, 15, 16, 17, 20, 21, 22, \\ 23, 25, 26, 28, 29, 30, 31, 32, 40, 56, 65. \end{aligned}$$

**Ví dụ 3.1.9.** Cho  $a_1, a_2, \dots, a_k$  là các số nguyên dương không vượt quá  $n$  thoả mãn điều kiện

$$[a_i, a_j] > n \quad \text{với mọi } 1 \leq i \neq j \leq k.$$

Chứng minh rằng

$$\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_k} < 2.$$

**Giải**

Phân hoạch tập  $S = \{1, 2, \dots, n\}$  thành  $k$  tập  $S_1, S_2, \dots, S_k$  thoả mãn

$$S_i = \{s \in S \mid s : a_i\} \quad \text{với mọi } i = 1, 2, \dots, k.$$

Để thấy

$$|S_i| = \left\lfloor \frac{n}{a_i} \right\rfloor \quad \text{với mọi } i = 1, 2, \dots, k.$$

Ta sẽ chứng minh  $S_i \cap S_j = \emptyset$  với mọi  $1 \leq i \neq j \leq k$ . Thật vậy, giả sử tồn tại  $s \in S_i \cap S_j$  khi đó  $s : a_i$  và  $s : a_j$  nên  $a : [a_i, a_j] > n$  vô lý. Vậy các tập  $S_1, S_2, \dots, S_k$  đôi một rời nhau. Do đó

$$\sum_{i=1}^k |S_i| = \sum_{i=1}^k \left\lfloor \frac{n}{a_i} \right\rfloor < n.$$

Từ đó,

$$\sum_{i=1}^k \frac{n}{a_i} < \sum_{i=1}^k \left( \left\lfloor \frac{n}{a_i} \right\rfloor + 1 \right) < n + k < 2n.$$

Điều phải chứng minh.

**Ví dụ 3.1.10.** Chứng minh rằng với mọi số nguyên dương  $n$ , hiệu

$$\sum_{k=1}^n \left\lfloor \frac{n}{k} \right\rfloor - \lfloor \sqrt{n} \rfloor$$

luôn là một số chẵn.

**Giải**

Ta có

$$\lfloor n/k \rfloor = \{s \in Z^+ : ks \leq n\}$$

nên  $\sum_{k=1}^n \left\lfloor \frac{n}{k} \right\rfloor$  là số các cặp (có tính thứ tự)  $(s, k)$  thoả mãn  $1 \leq s, k \leq n$  và  $ks \leq n$ .

Để thấy  $\lfloor \sqrt{n} \rfloor$  là số các cặp  $(k, k)$  thoả mãn  $1 \leq k \leq n$  và  $k^2 \leq n$  nên hiệu

$$\sum_{k=1}^n \left\lfloor \frac{n}{k} \right\rfloor - \lfloor \sqrt{n} \rfloor$$

chính là số các cặp số (tính thứ tự)  $(s, k)$ , sao cho  $1 \leq s \neq k \leq n$  và  $sk \leq n$ . Hiểu như, nếu cặp  $(s, k)$  thỏa mãn tính chất này thì cặp  $(k, s) \neq (s, k)$  cũng thỏa mãn. Do đó số các cặp thỏa mãn tính chất trên phải là một số chẵn, tức là ta có điều phải chứng minh.

### Ví dụ 3.1.11 (Belarus 2000).

Chứng minh rằng  $\{n\sqrt{3}\} > \frac{1}{n\sqrt{3}}$  với mọi số nguyên dương  $n$ .

Tồn tại hay không tồn tại số nguyên dương  $c > 1$  sao cho  $\{n\sqrt{3}\} > \frac{c}{n\sqrt{3}}$  với mọi số nguyên dương  $n$ .

### Giải

Với  $n = 1$  ta có  $\{\sqrt{3}\} = \sqrt{3} - 1 > \frac{c}{\sqrt{3}}$  nếu và chỉ nếu  $3 - \sqrt{3} > c$ . Do đó, chỉ cần xét hằng số  $c \in [1, \sqrt{3})$ .

Với mỗi  $n$ ,

$$\{n\sqrt{3}\} = n\sqrt{3} - \lfloor n\sqrt{3} \rfloor \geq \frac{c}{n\sqrt{3}} \Leftrightarrow n\sqrt{3} - \frac{c}{n\sqrt{3}} > \lfloor n\sqrt{3} \rfloor.$$

Do  $c < \sqrt{3} < 3n^2$  nên bất đẳng thức trên tương đương với

$$3n^2 - 2c + \frac{c^2}{3n^2} > \lfloor n\sqrt{3} \rfloor^2. \quad (*)$$

Với mỗi  $n$ ,  $3n^2 - 1 \equiv 2 \pmod{3}$  nên không thể là một số chính phương, do đó

$$\lfloor n\sqrt{3} \rfloor = \lfloor \sqrt{3n^2} \rfloor \leq \sqrt{3n^2 - 2},$$

dấu bằng chỉ xảy ra nếu  $3n^2 - 2$  là số chính phương.

Ta sẽ chứng minh rằng có vô số  $n$  thoả mãn  $3n^2 - 2$  là số chính phương. Thật vậy, xét các bộ số  $(m_i, n_i)$ ,  $i \geq 1$  như sau

$$(m_0, n_0) = (1, 1), \quad (m_{i+1}, n_{i+1}) = (2m_i + 3n_i, m_i + 2n_i), \quad \forall i \geq 1.$$

Dễ thấy rằng

$$m_{i+1}^2 - 3n_{i+1}^2 = m_i^2 - 3n_i^2 = \cdots = m_0^2 - 3n_0^2 = -2.$$

Suy ra  $3n_i^2 - 2 = m_i^2$  là một số chính phương. Vậy có vô số  $n$  thoả mãn  $3n^2 - 2$  là số chính phương.

Với  $c = 1$ , ta có điều phải chứng minh, bất đẳng thức đúng do

$$3n^2 - 2c + \frac{c^2}{3n^2} > 3n^2 - 2c = 3n^2 - 2 > [n\sqrt{3}]^2, \quad \forall n.$$

Với  $c > 1$  ta có

$$3n^2 - 2c + \frac{c^2}{3n^2} \leq 3n^2 - 2$$

với  $n$  đủ lớn. Mặt khác, tồn tại vô số  $n$  sao cho  $3n^2 - 2$  là số chính phương nên bất đẳng thức (\*) sai với vô số  $n$ . Từ đó suy ra không tồn tại  $c > 1$  để  $\{n\sqrt{3}\} > \frac{c}{n\sqrt{3}}$  với mọi số nguyên dương  $n$ .

**Ví dụ 3.1.12 (Korea 1997).** Biểu diễn  $\sum_{k=1}^n \lfloor \sqrt{k} \rfloor$  theo  $n$  và  $a = \lfloor \sqrt{n} \rfloor$ .

### Giải

Dễ dàng thấy rằng

$$\lfloor \sqrt{k} \rfloor = \sum_{j=1}^a [j^2 \leq k],$$

vì nếu  $1 \leq k \leq n$  thì  $\lfloor \sqrt{k} \rfloor \leq \lfloor \sqrt{n} \rfloor = a$ . Từ đó ta có

$$\sum_{k=1}^n \lfloor \sqrt{k} \rfloor = \sum_{k=1}^n \sum_{j=1}^a [j^2 \leq k] = \sum_{j=1}^a \sum_{k=1}^n [j^2 \leq k].$$

Vì  $\sum_{k=1}^n [j^2 \leq k]$  chứa số các số  $k \in \{1, 2, \dots, n\}$  thoả mãn  $k \geq j^2$ , và do  $j \leq a$  kéo theo  $j^2 \leq n$  nên số các số này là  $n + 1 - j^2$ . Theo đẳng thức trên ta có

$$\sum_{k=1}^n \lfloor \sqrt{k} \rfloor = \sum_{j=1}^a (n + 1 - j^2) = (n + 1)a - \frac{a(a + 1)(2a + 1)}{6}.$$

**Ví dụ 3.1.13 (Taiwan 1998).** Chứng minh rằng với mọi số nguyên dương  $m$  và  $n$ ,

$$\binom{mn}{m} = 2 \sum_{k=0}^{m-1} \left| \frac{kn}{m} \right| + m + n - mn$$

## Giải

Đặt  $d = (m, n)$ ,  $m = kd'$ ,  $n = dn'$  ta có  $k, d'$ ,  $d'$  là các số nguyên dương nguyên tố cùng nhau. Ta có

$$\left\lfloor \frac{kn}{m} \right\rfloor + \left\lfloor n - \frac{kn}{m} \right\rfloor = \begin{cases} n-1 & \text{nếu } \frac{kn}{m} \text{ không là một số nguyên,} \\ n & \text{nếu } \frac{kn}{m} \text{ là một số nguyên.} \end{cases}$$

Mặt khác,

$$\frac{kn}{m} = \frac{kn'}{m'}$$

là một số nguyên khi và chỉ khi  $k \mid m'$ .

Do đó, trong tập hợp  $\{1, 2, \dots, m-1\}$  có

$$\left\lfloor \frac{m-1}{m'} \right\rfloor = \left\lfloor d - \frac{1}{m'} \right\rfloor = d-1$$

giá trị của  $k$  sao cho  $kn/m$  là một số nguyên. Ta có

$$\begin{aligned} 2 \sum_{k=0}^{m-1} \left\lfloor \frac{kn}{m} \right\rfloor &= 2 \sum_{k=1}^{m-1} \left\lfloor \frac{kn}{m} \right\rfloor \\ &= \sum_{k=1}^{m-1} \left( \left\lfloor \frac{kn}{m} \right\rfloor + \left\lfloor n - \frac{kn}{m} \right\rfloor \right) \\ &= mn - m - n + d. \end{aligned}$$

Suy ra

$$(m, n) = d = 2 \sum_{k=0}^{m-1} \left\lfloor \frac{kn}{m} \right\rfloor + m + n - mn.$$

Điều phải chứng minh.

**BÀI TẬP**

**Bài 1 (Korea 2000).** Cho  $p$  là một số nguyên tố,  $p \equiv 1 \pmod{4}$ . Tính giá trị của biểu thức

$$S = \sum_{k=1}^{p-1} \left( \left\lfloor \frac{2k^2}{p} \right\rfloor - 2 \left\lfloor \frac{k^2}{p} \right\rfloor \right).$$

**Bài 2 (Austrian-Polish 1998).**

Cho  $m, n$  là các số nguyên dương,  $n \geq m$ . Chứng minh rằng

$$\sum_{k=1}^n \lfloor \sqrt[k]{k^m} \rfloor \leq n + m(2^{m/4} - 1).$$

**Bài 3 (Balkan 1998).** Tìm số các số khác nhau trong dãy

$$\left\{ \left\lfloor \frac{k^2}{1998} \right\rfloor : k = 1, 2, \dots, 1997 \right\}.$$

**Bài 4 (Russia 1999).** Chứng minh rằng với mọi số tự nhiên dương  $n$ ,

$$\sum_{k=1}^{n^2} \{\sqrt{k}\} \leq \frac{n^2 - 1}{2}.$$

**Bài 5 (Czeck-Slovak 1999).** Chứng minh rằng với mọi số nguyên dương  $n > 2$ ,

$$[1, 2, 3, \dots, n] \geq 2^{n-1}.$$

**Bài 6.** Chứng minh rằng

$$[\sqrt[3]{72n+1}] = [\sqrt[3]{9n} + \sqrt[3]{9n+1}] = [\sqrt[3]{72n+7}].$$

**Bài 7 (St.Peterburg 1998).** Cho  $n$  là một số nguyên dương, chứng minh rằng tồn tại  $\varepsilon > 0$  sao cho với  $n$  số thực dương  $x_1, x_2, \dots, x_n$  tùy ý luôn tồn tại  $t > 0$  sao cho

$$\varepsilon < \{tu_1\}, \{tu_2\}, \dots, \{tu_n\} < \frac{1}{2}.$$

## LỜI GIẢI

### Bài 1 (Korea 2000).

Ta có  $\lfloor 2k^2/p \rfloor = 2k^2/p - \{2k^2/p\}$ ,  $\lfloor k^2/p \rfloor = k^2/p - \{k^2/p\}$  nên

$$\left\lfloor \frac{2k^2}{p} \right\rfloor - 2 \left\lfloor \frac{k^2}{p} \right\rfloor = 2 \left\{ \frac{k^2}{p} \right\} - \left\{ \frac{2k^2}{p} \right\}.$$

Ta thấy

- Nếu  $\{x\} < 1/2$  thì  $2\{x\} - \{2x\} = 2\{x\} - 2\{x\} = 0$ .
- Nếu  $\{x\} \geq 1/2$  thì  $2\{x\} - \{2x\} = 2\{x\} - (2\{x\} - 1) = 1$ .

Do đó,  $S$  bằng số các số  $k \in [1, p-1]$  sao cho  $\{k^2/p\} \geq 1/2$  hay số các lớp thặng dư  $k$  khác 0 sao cho  $k^2$  đồng dư với một số nằm trong khoảng  $[(p+1)/2, p-1]$  modulo  $p$ .

Do  $p \equiv 1 \pmod{4}$  nên tồn tại số nguyên  $d$  sao cho  $d^2 \equiv -1 \pmod{p}$ . Chia  $p-1$  lớp thặng dư khác 0 thành  $(p-1)/2$  cặp có dạng  $(a, da)$ . Do  $(da)^2 \equiv -a^2 \pmod{p}$  nên trong mỗi cặp có đúng một số có thặng dư bình phương nằm trong khoảng  $[(p+1)/2, p-1]$ . Từ đó suy ra có tất cả  $(p-1)/2$  lớp thặng dư  $k$  khác 0 sao cho  $k^2$  đồng dư với một số nằm trong khoảng  $[(p+1)/2, p-1]$  modulo  $p$ , tức là  $S = (p-1)/2$ .

### Bài 2 (Austrian-Polish 1998).

Với  $k > m$  ta có  $k < 2^k$  suy ra,  $k < 2^{k^2/m}$ , tức là  $k^m < 2^{k^2}$  hay  $\sqrt[m]{k^m} < 2$ . Vì vậy nếu  $k > m$  thì

$$\lfloor \sqrt[m]{k^m} \rfloor = 1.$$

Từ đó, để chứng minh bất đẳng thức đã cho ta chỉ cần chứng minh

$$\sum_{k=1}^m \lfloor \sqrt[m]{k^m} \rfloor \leq m + \sum_{k=1}^m \lfloor \sqrt[m]{k^m} \rfloor.$$

Với  $k = 1, 2, 3$  dễ kiểm tra  $2^{k^2/4} \geq k$  nếu và chỉ nếu  $\sqrt[4]{k^m} \leq 2^{m/4}$ .

Với  $k \geq 4$ ,  $2^{k^2/4} > 2^k > k$ , do đó  $\sqrt[4]{k^m} \leq 2^{m/4}$ . Từ đó ta có điều ph chứng minh.

### Bài 3 (Balkan 1998).

Ta có

$$\left\lfloor \frac{998^2}{1998} \right\rfloor = 498 < 499 = \left\lfloor \frac{999^2}{1998} \right\rfloor$$

nên các số trong hai tập hợp

$$\left\{ \left\lfloor \frac{k^2}{1998} \right\rfloor : k = 1, 2, \dots, 998 \right\} \text{ và } \left\{ \left\lfloor \frac{k^2}{1998} \right\rfloor : k = 999, 1000, \dots, 1997 \right\}$$

phân biệt.

Đi  $k = 1, 2, \dots, 998$  ta có

$$\frac{(k+1)^2}{1998} - \frac{k^2}{1998} = \frac{2k+1}{1998} < 1,$$

khi  $k = 1, 2, \dots, 998$ , tập hợp

$$\left\{ \left\lfloor \frac{k^2}{1998} \right\rfloor : k = 1, 2, \dots, 998 \right\}$$

ít cả các số

$$\left\lfloor \frac{1^2}{1998} \right\rfloor = 0, 1, \dots, 498 = \left\lfloor \frac{998^2}{1998} \right\rfloor.$$

Đi  $k = 999, 1000, \dots, 1997$  ta có

$$\frac{(k+1)^2}{1998} - \frac{k^2}{1998} = \frac{2k+1}{1998} > 1,$$

trong tập hợp

$$\left\{ \left\lfloor \frac{k^2}{1998} \right\rfloor : k = 999, 1000, \dots, 1997 \right\}$$

Từ đó suy ra số các số khác nhau trong dãy

**Bài 4 (Russia 1999).**

Ta sẽ chứng minh bằng quy nạp theo  $n$ . Với  $n = 1$  hiển nhiên khẳng định đúng. Giả sử khẳng định đúng với  $n$ . Ta đi chứng minh khẳng định đúng với  $n + 1$ . Ta có

$$n < \sqrt{n^2 + 1} < \sqrt{n^2 + 2} < \cdots < \sqrt{n^2 + 2n} < n + 1$$

nên với mọi  $i = 1, 2, \dots, 2n$  ta có

$$\{\sqrt{n^2 + i}\} = \sqrt{n^2 + i} - n < \sqrt{n^2 + i + \frac{i^2}{4n^2}} - n = \frac{i}{2n}.$$

Do đó,

$$\begin{aligned} \sum_{k=1}^{(n+1)^2} \{\sqrt{k}\} &= \sum_{k=1}^{n^2} \{\sqrt{k}\} + \sum_{k=n^2+1}^{(n+1)^2} \{\sqrt{k}\} \\ &< \frac{n^2 - 1}{2} + \frac{1}{2n} \sum_{i=1}^{2n} i + 0 \\ &= \frac{n^2 - 1}{2} + \frac{2n + 1}{2} \\ &= \frac{(n+1)^2 - 1}{2}. \end{aligned}$$

Như vậy khẳng định đúng với  $n + 1$ , theo nguyên lý quy nạp ta có điều phải chứng minh.

**Bài 5 (Czech-Slovak 1999).**

Do  $C_{n-1}^k \leq C_{n-1}^{\lfloor(n-1)/2\rfloor}$  với mọi  $n \geq 3$  và  $0 \leq k \leq n$  nên với mọi  $n \geq 3$  ta có

$$2^{n-1} = \sum_{k=0}^{n-1} C_{n-1}^k < \sum_{k=0}^{n-1} C_{n-1}^{\lfloor(n-1)/2\rfloor} = nC_{n-1}^{\lfloor(n-1)/2\rfloor}.$$

Ta đi chứng minh

$$[1, 2, \dots, n] : nC_{n-1}^{\lfloor(n-1)/2\rfloor}.$$

Ta sẽ chứng minh khẳng định tổng quát hơn như sau: Với mọi số nguyên dương  $k < n$ ,

$$[n, n-1, n-2, \dots, n-k] : nC_{n-1}^k.$$

Giả sử  $p$  là một số nguyên tố tuỳ ý, gọi  $\alpha$  là số nguyên lớn nhất sao cho

$$[n, n-1, n-2, \dots, n-k] : p^\alpha.$$

Khi đó tồn tại một số nguyên  $l$  sao cho  $n-l : p^\alpha$  và  $n-l : p^i$  với mọi  $i \leq \alpha$ . Ta có

$$\begin{aligned} \{n, n-1, \dots, n-l+1\} &= \{(n-l)+l, (n-l)+(l-1), \dots, (n-l)+1\}, \\ \{n-l-1, n-l-2, \dots, n-k\} &= \{(n-l)-1, (n-l)-2, \dots, (n-l)-(k-l)\}. \end{aligned}$$

Do đó, với mọi  $i \leq \alpha$ :

- Số các số chia hết cho  $p^i$  trong  $1, 2, \dots, k$  là  $\lfloor k/p^i \rfloor$ .
- Số các số chia hết cho  $p^i$  trong  $n, n-1, n-2, \dots, n-l+1$  là  $\lfloor l/p^i \rfloor$ .
- Số các số chia hết cho  $p^i$  trong  $n-l-1, n-l-2, \dots, n-k$  là  $\lfloor (k-l)/p^i \rfloor$ .

Từ đó suy ra số các số chia hết cho  $p^i$  trong tích

$$n(n-1)(n-2) \cdots (n-l+1)(n-l-1)(n-l-2) \cdots (n-k)$$

là  $\lfloor l/p^i \rfloor + \lfloor (k-l)/p^i \rfloor$ . Mặt khác ta có

$$\left\lfloor \frac{l}{p^i} \right\rfloor + \left\lfloor \frac{k-l}{p^i} \right\rfloor \leq \left\lfloor \frac{k}{p^i} \right\rfloor,$$

nên (chọn  $i = \min\{1, \alpha - 1\}$ )

$$\frac{n(n-1)(n-2) \cdots (n-l+1)(n-l-1)(n-l-2) \cdots (n-k)}{k!} : p.$$

Vì vậy,

$$nC_{n-1}^k = \frac{n(n-1)(n-2) \cdots (n-l+1)(n-l-1)(n-l-2) \cdots (n-k)}{k!}.$$

Nhận thấy

$$nC_{n-1}^k \vdots P_{p-1}^{(x)} \vdots \cdots \vdots P_{p-1}^{(\alpha)} \vdots p^{\alpha+1}.$$

Do số nguyên tố  $p$  được chọn tùy ý nên từ đó ta có

$$[n, n-1, n-2, \dots, n-k] \vdots nC_{n-1}^k.$$

Điều phải chứng minh.

### Bài 6.

Ta có

$$9n = \sqrt[3]{9n \cdot 9n \cdot 9n} < \sqrt[3]{(9n)^2(9n+1)} < \sqrt[3]{9n(9n+1)^2} < 9n+1$$

Suy ra

$$\begin{aligned} 3.9n &< 3\sqrt[3]{(9n)^2(9n+1)} < 3\sqrt[3]{(9n)(9n+1)^2} < 3(9n+1) \\ \Leftrightarrow 6.9n &< 3\sqrt[3]{(9n)(9n+1)}(\sqrt[3]{9n} + \sqrt[3]{9n+1}) < 6(9n+1) \\ \Leftrightarrow 72n+1 &< (\sqrt[3]{9n} + \sqrt[3]{9n+1})^3 < 72n+7 \\ \Leftrightarrow \sqrt[3]{72n+1} &< \sqrt[3]{9n} + \sqrt[3]{9n+1} < \sqrt[3]{72n+7} \end{aligned}$$

Ta có

$$a^3 \equiv 0, 1, 8 \pmod{9}$$

$$k^3 < 72n+1 < (k+1)^3$$

Suy ra

$$9.8n+2 \leq (k+1)^3$$

Vì  $k+1 \neq 9.8n+2$  suy ra  $9.8n+2 < (k+1)^3$

Lại suy ra  $9.8n+3 \leq (k+1)^3$

Vì  $9.8n+3 \neq (k+1)^3$

Ta có  $9.8n+3 < (k+1)^3$

Hoàn toàn tương tự, ta thu được

$$k^3 \leq 72n+1 < 72n+7 < (k+1)^3$$

Suy ra

$$k^3 \leq 72n+1 < (\sqrt[3]{9n} + \sqrt[3]{9n+1})^3 < 72n+7 < (k+1)^3$$

$$\Leftrightarrow k \leq \sqrt[3]{72n+1} < \sqrt[3]{9n} + \sqrt[3]{9n+1} < \sqrt[3]{72n+7} < k+1$$

Suy ra

$$[\sqrt[3]{72n+1}] = [\sqrt[3]{9n} + \sqrt[3]{9n+1}] = [\sqrt[3]{72n+7}]$$

Điều phải chứng minh.

**Bài 7 (St.Peterburg 1998).** Cho  $n$  là một số nguyên dương, chứng minh rằng tồn tại  $\varepsilon > 0$  sao cho với  $n$  số thực dương  $x_1, x_2, \dots, x_n$  tùy ý luôn tồn tại  $t > 0$  sao cho

$$\varepsilon < \{ta_1\}, \{ta_2\}, \dots, \{ta_n\} < \frac{1}{2}.$$

## 2 Một số hàm số học

### Định nghĩa 3.2.1.

Với mỗi số nguyên dương  $n$  ta định nghĩa

1.  $d(n)$  là số các ước số dương của  $n$ .
2.  $\sigma(n)$  là tổng các ước số dương của  $n$ .
3.  $\omega(n)$  là số các ước số nguyên tố của  $n$ .

Ví dụ, với  $n = 18$  ta có

$$d(18) = 6, \quad \sigma(18) = 39, \quad \omega(18) = 2.$$

Để tiện theo dõi, ta dùng các kí hiệu  $\sum_{d|n} f(d)$ ,  $\prod_{d|n} f(d)$  để chỉ tổng và tích các số  $f(d)$  trên tập tất cả các ước số nguyên dương  $d$  của  $n$ . Ta có

$$d(n) = \sum_{d|n} 1, \quad \sigma(n) = \sum_{d|n} d, \quad \omega(n) = \sum_{\substack{p \text{ nguyên tố} \\ p|n}} 1.$$

### Định lý 3.2.1.

Cho  $n$  là một số nguyên dương có phân tích  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ . Khi đó

$$d(n) = \prod_{i=1}^k (\alpha_i + 1).$$

### Chứng minh

Điều kiện cần và đủ để một số nguyên dương  $q$  là ước số của  $n$  là  $q = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$  với  $0 \leq \beta_i \leq \alpha_i$  với mọi  $i = 1, 2, \dots, k$ . Do đó,  $d(n)$  chính là số cách chọn các số  $q$  có dạng trên.

Với  $i = 1, 2, \dots, k$ , mỗi số nguyên tố  $p_i$  có  $\alpha_i + 1$  cách chọn số mũ  $\beta_i$  là  $0, 1, 2, \dots, \alpha_i$ . Theo quy tắc nhân, sẽ có  $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$

cách chọn số  $q$ , vì vậy ta có

$$d(n) = \prod_{i=1}^k (\alpha_i + 1).$$

Định lý được chứng minh.

### Định lý 3.2.2.

Một hàm số học  $f(n)$  được gọi là nhân tính nếu  $f(mn) = f(m)f(n)$  với mọi cặp số nguyên dương  $m, n$  thoả mãn  $(m, n) = 1$ .

Nếu  $f(mn) = f(m)f(n)$  với mọi cặp số nguyên dương  $m, n$  tùy ý thì  $f(n)$  được gọi là hoàn toàn nhân tính.

Đối với hàm  $f$  nhân tính, nếu biết được các giá trị của nó tại các điểm có dạng  $p^\alpha$  với  $p$  là một số nguyên tố và  $\alpha$  là một số nguyên dương thì ta sẽ xác định được toàn bộ các giá trị của nó trên tập  $\mathbb{N}$ . Thật vậy, với mỗi số nguyên  $n$  có phân tích  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$  thì

$$f(n) = \prod_{i=1}^k f(p_i^{\alpha_i}).$$

Vì vậy, nếu biết được các giá trị  $f(p_i^{\alpha_i})$  thì ta sẽ xác định được  $f(n)$ . Định lý sau cho ta một cách xác định một số hàm số học tương tự như cách sử dụng định lý thặng dư Trung Hoa trong các bài toán đồng dư.

### Định lý 3.2.3

Cho  $f(n)$  là một hàm nhân tính, đặt

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

Khi đó  $F(n)$  cũng là một hàm nhân tính.

### Chứng minh

Giả sử  $m = m_1 m_2$  với  $(m_1, m_2) = 1$ . Khi đó, ta có một song ánh giữa các ước số của  $m$  với các cặp  $(d_1, d_2)$  các ước số của  $m_1$  và  $m_2$ .

Thật vậy, gọi  $d$  là một ước số bất kỳ của  $m$ , đặt  $d_1 = (d, m_1), d_2 = (d, m_2)$ , khi đó vì  $(m_1, m_2) = 1$  nên  $(d_1, d_2) = 1$  và  $d = d_1d_2$ . Ngược lại, nếu  $d_1$  là một ước số của  $m_1$  và  $d_2$  là một ước số của  $m_2$  thì  $d = d_1d_2$  là một ước số của  $m$  và  $d_1 = (d, m_1), d_2 = (d, m_2)$ .

Do đó,

$$\begin{aligned} F(m) &= \sum_{d|m} f(d) = \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1d_2) \\ &= \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1)f(d_2) \\ &= \left( \sum_{d_1|m_1} f(d_1) \right) \left( \sum_{d_2|m_2} f(d_2) \right) \\ &= F(m_1)F(m_2). \end{aligned}$$

Định lý được chứng minh.

Ta có thể dùng định lý trên để xác định hàm  $d(n)$  bằng một cách khác với định lý 3.2.1. Vì  $d(n) = \sum_{d|n} 1$  nên nó có dạng  $\sum_{d|n} f(d)$  với  $f(d) \equiv 1$  là một hàm nhân tính, do đó theo định lý trên  $d(n)$  cũng là một hàm nhân tính. Giả sử  $n$  có phân tích  $n = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ , vì  $d(n)$  là một hàm nhân tính nên ta có

$$d(n) = \prod_{i=1}^k d(p_i^{\alpha_i}).$$

Mặt khác với mỗi  $i$ ,  $p_i^{\alpha_i}$  có đúng  $\alpha_i + 1$  ước số là  $1 = p_1^0, p_1^1, p_1^2, \dots, p_1^{\alpha_i}$  nên  $d(p_i^{\alpha_i}) = \alpha_i + 1$ . Từ đó,

$$d(n) = \prod_{i=1}^k d(p_i^{\alpha_i}) = \prod_{i=1}^k (\alpha_i + 1).$$

Tức là ta có kết luận của định lý 3.2.1.

Từ định lý 3.2.1 còn có thể tính được hàm  $\sigma(n)$ . Ta có định lý sau

#### Định lý 3.2.4.

Cho  $n$  là một số nguyên dương có phân tích  $n = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ . Khi

đó

$$\sigma(n) = \prod_{i=1}^k \left( \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right).$$

### Chứng minh

Do hàm  $f(d) = d$  là hàm nhân tính nên theo định lý ??,  $\sigma(n) = \sum_{d|n} d$  cũng là hàm nhân tính và  $\sigma(n) = \prod_{i=1}^k \sigma(p_i^{\alpha_i})$ . Vì  $p_i^{\alpha_i}$  chỉ có các ước số là  $1, p_i, p_i^2, \dots, p_i^{\alpha_i}$  nên

$$\sigma(p_i^{\alpha_i}) = 1 + p_i + p_i^2 + \dots + p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Từ đó,

$$\sigma(n) = \prod_{i=1}^k \sigma(p_i^{\alpha_i}) = \prod_{i=1}^k \left( \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right).$$

Định lý được chứng minh.

Định lý sau được chứng minh bằng cùng phương pháp.

### Định lý 3.2.4.

Cho  $n$  là một số nguyên dương. Khi đó

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

### Chứng minh

Đặt  $F(n) = \sum_{d|n} \phi(d)$ . Hàm  $\phi(d)$  là nhân tính nên từ định lý 3.2.3 suy ra  $F(n)$  cũng là hàm nhân tính. Vì vậy, để chứng minh  $F(n) = n$  với mọi  $n$  ta chỉ cần chứng minh  $F(p^\alpha) = p^\alpha$  với mọi số nguyên tố  $p$  và số nguyên dương  $\alpha$ .

Với  $n = p^\alpha$ , mọi ước số  $d > 1$  của  $n$  đều có dạng  $d = p^\beta$  trong đó  $1 \leq \beta \leq \alpha$ , khi đó  $\phi(d) = \phi(p^\beta) = p^\beta - p^{\beta-1}$ . Do đó

$$F(p^\alpha) = \sum_{d|p^\alpha} \phi(d) = \sum_{\beta=0}^{\alpha} \phi(p^\beta) = 1 + \sum_{\beta=1}^{\alpha} (p^\beta - p^{\beta-1}) = p^\alpha.$$

Định lý được chứng minh.

**Ví dụ 3.2.1 (Germany 1997).** Kí hiệu  $u(k)$  là ước số lẻ lớn nhất của số nguyên  $k$ . Chứng minh rằng

$$\frac{1}{2^n} \sum_{k=1}^{2^n} \frac{u(k)}{k} \geq \frac{2}{3}.$$

### Giải

Gọi  $v(k)$  là luỹ thừa của 2 trong phân tích  $k$  thành tích các số nguyên tố. Để thấy  $u(k)v(k) = k$  với mọi số nguyên dương  $k$ , trong tập hợp  $\{1, 2, \dots, 2^n\}$  có  $2^{n-i-1}$  giá trị của  $k$  sao cho  $v(k) = 2^i$  với mọi số nguyên  $i = 1, 2, \dots, n-1$  và có duy nhất  $k = 2^n$  thoả mãn  $v(k) = 2^n$ . Do đó,

$$\begin{aligned} \frac{1}{2^n} \sum_{k=1}^{2^n} \frac{u(k)}{k} &= \frac{1}{2^n} \sum_{k=1}^{2^n} \frac{1}{v(k)} \\ &= \frac{1}{4^n} + \sum_{i=0}^{n-1} \frac{2^{n-i-1}}{2^{n+i}} \\ &= \frac{1}{4^n} + \frac{2}{3} \left(1 - \frac{1}{4^n}\right) \geq \frac{2}{3}. \end{aligned}$$

**Ví dụ 3.2.2 (Ireland 1997).** Cho  $S = \{3, 5, 7, 9, \dots\}$ . Với  $x \in S$  đặt  $\delta(x)$  là số nguyên dương duy nhất thoả mãn  $2^{\delta(x)} < x < 2^{\delta(x)+1}$ . Với  $a, b \in S$  đặt

$$a * b = 2^{\delta(a)-1}(b-3) + a.$$

a, Chứng minh rằng nếu  $a, b \in S$  thì  $a * b \in S$ .

b, Chứng minh rằng nếu  $a, b, c \in S$  thì  $(a * b) * c = a * (b * c)$ .

### Giải

a, Hiển nhiên.

b, Nếu  $2^m < a < 2^{m+1}$ ,  $2^n < b < 2^{n+1}$ ,  $2^p < c < 2^{p+1}$  thì

$$a * b = 2^{m-1}(b-3) + a \geq 2^{m-1}(2^n - 2) + 2^m + 1 = 2^{m+n-1} + 1$$

và

$$a * b \leq 2^{m-1}(2^{n+1} - 4) + 2^{m+1} - 1 = 2^{m+n} - 1$$

do đó  $\delta(a * b) = m + n - 1$ . Ta có

$$(a * b) * c = (2^{m-1}(b-3) + a) * c = 2^{m+n-2}(c-3) + 2^{m-1}(b-3) + a$$

và

$$a*(b*c) = a*(2^{n-1}(c-3)+b) = 2^{m-1}(2^{n-1}(c-3)+b-3)+a = (a*b)*c.$$

**Ví dụ 3.2.3 (Taiwan 1998).** Với mỗi số nguyên dương  $n$  kí hiệu  $\omega(n)$  là số các ước số nguyên tố phân biệt của  $n$ . Tìm số nguyên dương  $k$  bé nhất sao cho với mọi số nguyên dương  $n$ ,

$$2^{\omega(n)} \leq k\sqrt[4]{n}.$$

### Giải

Đặt  $p_0 = 2 < p_1 < p_2 < \dots$  là dãy tất cả các số nguyên tố. Khi đó, tồn tại một chỉ số  $i$  sao cho

$$p_0 p_1 p_2 \cdots p_{i-1} \leq n < p_0 p_1 p_2 \cdots p_i.$$

Ta có  $\omega(n) \leq i$  và

$$\frac{2^{\omega(n)}}{\sqrt[4]{n}} \leq \frac{2^i}{\sqrt[4]{p_0 p_1 p_2 \cdots p_{i-1}}}.$$

Do đó

$$\begin{aligned} k &= \max \left\{ 0, \left\lfloor \frac{2^2}{\sqrt[4]{2.3}} \right\rfloor, \left\lfloor \frac{2^3}{\sqrt[4]{2.3.5}} \right\rfloor, \left\lfloor \frac{2^4}{\sqrt[4]{2.3.5.7}} \right\rfloor, \dots \right\} \\ &= \left\lfloor \frac{2^6}{\sqrt[4]{2.3.5.7.11.13}} \right\rfloor = 5 \end{aligned}$$

thoả mãn điều kiện đã cho.

Để thấy  $k = 4$  không thoả mãn bất đẳng thức với  $n = 2.3.5.7 = 210$ .

**Ví dụ 3.2.4 (Belarus 1999).** Chứng minh rằng với mọi số nguyên dương  $n > 1$ , tổng  $\sigma(n)$  tất cả các ước số nguyên dương của  $n$  (gồm cả 1 và  $n$ ) thoả mãn bất đẳng thức

$$d(n)\sqrt{n} < \sigma(n) < \sqrt{2d(n)}n,$$

trong đó  $d(n)$  là số các ước số nguyên dương của  $n$ .

### Giải

Giả sử tập tất cả các ước số nguyên dương của  $n$  là  $d_1, d_2, \dots, d_{\psi(n)}$ .  
Đặt  $k = d(n)$  ta có  $d_i d_{k+1-i} = n$  với mọi  $i = 1, 2, \dots, k$ . Do đó, theo  
bất đẳng thức Cauchy,

$$\sigma(n) = \sum_{i=1}^k d_i = \sum_{i=1}^k \frac{d_i + d_{k+1-i}}{2} > \sum_{i=1}^k \sqrt{d_i d_{k+1-i}} = k\sqrt{n}.$$

Đặt  $\sigma_2(n) = \sum_{i=1}^k d_i^2$ , áp dụng bất đẳng thức Bunhiakowski,

$$\frac{\sigma(n)}{k} = \frac{1}{k} \sum_{i=1}^k d_i \leq \sqrt{\frac{1}{k} \sum_{i=1}^k d_i^2} = \sqrt{\frac{\sigma_2(n)}{k}}$$

suy ra  $\sigma(n) \leq \sqrt{k\sigma_2(n)}$  nên

$$\frac{\sigma_2(n)}{n^2} = \sum_{i=1}^k \frac{d_i^2}{n^2} = \sum_{i=1}^k \frac{1}{d_{k+1-i}^2} \leq \sum_{j=1}^{\infty} \frac{1}{j^2} < \frac{\pi^2}{6}.$$

Từ đó,

$$\sigma(n) \leq \sqrt{k\sigma_2(n)} < \sqrt{\frac{kn^2\pi^2}{6}} < \sqrt{2kn}.$$

**Ví dụ 3.2.5 (Belarus 1999).** Cho  $a, b$  là các số nguyên dương thoả mãn  
tích tất cả các ước số nguyên dương của  $a$  (kể cả 1 và  $a$ ) bằng tích tất  
cả các ước số nguyên dương của  $b$  (kể cả 1 và  $b$ ). Chứng minh rằng  $a = b$ .

### Giải

Với mỗi số nguyên dương  $n$ , tích tất cả các ước số nguyên dương của  $n$  là

$$\prod_{k|n} k = \sqrt{\prod_{k|n} k \cdot \prod_{k|n} \frac{n}{k}} = \sqrt{\prod_{k|n} n} = n^{d(n)/2}.$$

Từ đó và giả thiết suy ra  $a^{d(a)} = b^{d(b)}$ . Đặt

$$a^{d(a)} = b^{d(b)} = N, \quad m = [d(a), d(b)].$$

Khi đó, tồn tại một số nguyên dương  $n$  sao cho  $N = n^m$  và  $a = n^{m/d(a)}$ ,  $b = n^{m/d(b)}$ .

Nếu  $a = n^{m/d(a)} > n^{m/d(b)} = b$  thì số ước số của  $a$  lớn hơn số ước số của  $b$ , tức là  $d(a) > d(b)$ . Từ đó suy ra

$$N = a^{d(a)} = (n^{m/d(a)})^{d(a)} > (n^{m/d(b)})^{d(a)} > (n^{m/d(b)})^{d(b)} = b^{d(b)} = N.$$

Vô lý, vậy  $a \leq b$ . Do vai trò của  $a, b$  là như nhau nên suy ra  $b \leq a$  hay  $a = b$ . Điều phải chứng minh.

**Ví dụ 3.2.6 (Ireland 1997).** Tìm tất cả các số nguyên dương  $m$  thỏa mãn

$$m = d(m)^4,$$

trong đó  $d(m)$  là số các ước số nguyên dương của  $m$ .

### Giải

Giả sử số nguyên dương  $m$  thỏa mãn điều kiện đề bài. Khi đó  $m$  là luỹ thừa bậc bốn của một số nguyên dương nên  $m$  có dạng  $m = 2^{4a_2}3^{4a_3}5^{4a_5}\dots$ . Số các ước số của  $m$  bằng

$$(4a_2 + 1)(4a_3 + 1)(4a_5 + 1)\dots$$

là một số lẻ nên  $m$  là một số lẻ, suy ra  $a_2 = 0$ . Theo giả thiết,

$$1 = \frac{4a_3 + 1}{3^{a_3}} \cdot \frac{4a_5 + 1}{5^{a_5}} \cdot \frac{4a_7 + 1}{7^{a_7}} \cdots = x_3x_5x_7\cdots$$

Nếu  $a_3 = 1$  thì  $x_3 = 5/3$ ,  $a_3 = 0$  hoặc  $2$  thì  $x_3 = 1$ . Với  $a_3 > 2$  áp dụng bất đẳng thức Bernoulli ta có

$$3^{a_3} = (8 + 1)^{a_3/2} > 8(a_3/2) + 1 = 4a_3 + 1$$

nên  $x_3 < 1$ .

Nếu  $a_5 = 0$  hoặc  $1$  thì  $x_5 = 1$ . Với  $a_5 \geq 2$  áp dụng bất đẳng thức Bernoulli ta có

$$5^{a_5} = (24 + 1)^{a_5/2} \geq 24(a_5/2) + 1 = 12a_5 + 1$$

nên  $x_5 \leq (4a_5 + 1)/(12a_5 + 1) \leq 9/25$ .

Nếu  $p > 5$ ,  $a_p = 0$  thì  $x_p = 1$ ,  $a_p = 1$  thì  $p^{a_p} = p > 5 = 4a_p + 1$  nên  $x_p < 1$ . Với  $a_p \geq 2$  áp dụng bất đẳng thức Bernoulli ta có

$$p^{a_p} > 5^{a_p} > 12a_p + 1$$

nên  $x_p < 9/25$ .

Nếu  $a_3 \neq 1$  thì  $x_p \leq 1$  với mọi  $p$ . Do  $x_3x_5x_7\cdots = 1$  nên  $x_p = 1$  với mọi  $p$ . Khi đó  $a_3 \in \{0, 2\}$ ,  $a_5 \in \{0, 1\}$  và  $a_7 = a_{11} = a_{13} = \cdots = 0$ . Suy ra

$$m = 1^4, (3^2)^4, 5^4 \text{ hoặc } (3^2 \cdot 5)^4.$$

Nếu  $a_3 = 1$  thì  $3|m = 5^4(4a_5 + 1)^4(4a_7 + 1)^4\cdots$  nên tồn tại một số nguyên tố  $\bar{p} \geq 5$  sao cho  $4a_{\bar{p}} + 1 \mid 3$ , tức là  $a_{\bar{p}} \geq 2$ . Từ chứng minh trên ta có  $x_{\bar{p}} \leq 9/25$  nên

$$x_3x_5x_7\cdots \leq \frac{5}{3} \frac{9}{25} < 1,$$

vô lý. Vậy các số nguyên dương  $m$  thoả mãn điều kiện đề bài là

$$1^4, (3^2)^4, 5^4 \text{ và } (3^2 \cdot 5)^4.$$

**Ví dụ 3.2.7 (Canada 1999).** Tìm tất cả các số nguyên dương  $n$  sao cho  $n = d(n)^2$ .

### Giải

Giả sử  $n$  là một số nguyên dương thoả mãn điều kiện đề bài. Do  $n = d(n)^2$  là một số chính phương nên ta có thể đặt  $n = \prod_{i=1}^k p_i^{2\alpha_i}$ . Khi đó  $d(n) = \prod_{i=1}^k (2\alpha_i + 1)$  và

$$\prod_{i=1}^k \frac{2\alpha_i + 1}{p_i^{\alpha_i}} = 1.$$

Theo bất đẳng thức Bernoulli ta có

$$p_i^{\alpha_i} \geq (p_i - 1)\alpha_i + 1 > 2\alpha_i + 1$$

với mọi ước số nguyên tố  $p_i \geq 5$  của  $n$ .

Mặt khác, luôn có  $3^\alpha \geqslant 2\alpha + 1$  với dấu đẳng thức xảy ra khi  $\alpha \in \{0, 1\}$ . Từ đó suy ra  $n = 1$  và  $n = 9$  là hai số duy nhất thoả mãn điều kiện đề bài.

**Ví dụ 3.2.8 (St.Peterburg 1998).** Gọi  $d(n)$  là số các ước số dương của số tự nhiên  $n$ . Chứng minh rằng dãy  $d(n^2 + 1)$  không thể đơn điệu kể từ một lúc nào đó.

### Giải

Trước hết ta chứng minh rằng nếu  $n$  chẵn thì  $d(n^2 + 1) \leq n$ . Thật vậy, một nửa ước số của  $n^2 + 1$  bé hơn  $n$  và là các số lẻ, do đó  $n^2 + 1$  có không quá  $2.(n/2) = n$  ước số.

Giả sử với  $n \geqslant N$ ,  $d(n^2 + 1)$  đơn điệu. Khi đó, do  $d(k)$  chẵn nếu  $k$  không phải số chính phương nên

$$d((n+1)^2 + 1) \geqslant d(n^2 + 1) + 2, \quad \forall n \geqslant N.$$

Từ đó, với  $n > 2N$ ,

$$d(n^2 + 1) \geqslant d(N^2 + 1) + 2(n - N) > n.$$

Vô lý. Vậy ta có điều phải chứng minh.

**Ví dụ 3.2.9 (Ireland 1998).** Tìm tất cả các số nguyên dương  $n$  có đúng 16 ước số nguyên dương  $d_1, d_2, \dots, d_{16}$  thoả mãn

$$1 = d_1 < d_2 < \dots < d_{16} = n, \quad d_6 = 18, \quad d_9 - d_8 = 17.$$

### Giải

Với số nguyên dương  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$  thì số các ước số nguyên dương của  $n$  là

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_m + 1).$$

Do  $18 = 2^1 \cdot 3^2$  nên 18 có 6 ước số nguyên dương là 1, 2, 3, 6, 9, 18. Từ đó và do  $n$  có 16 ước số nguyên dương nên  $n = 2 \cdot 3^3 \cdot p$  hoặc  $d = 2 \cdot 3^7$  với  $p$  là một số nguyên tố lớn hơn 18.

Nếu  $n = 2 \cdot 3^7$  thì  $d_9 - d_8 = 81 - 54 = 27 \neq 17$ , không thoả mãn điều kiện đã cho. Vậy  $n = 2 \cdot 3^3 \cdot p$  với  $p$  là một số nguyên tố lớn hơn 18.

- Nếu  $p < 27$  thì  $d_7 = p, d_8 = 27, d_9 = 2p = d_8 + 17 = 44$  nên  $p = 22$  không là một số nguyên tố, vô lý.
- Nếu  $27 < p < 54$  thì  $d_7 = 27, d_8 = p, d_9 = 54 = d_8 + 17$  nên  $p = 37$ .
- Nếu  $p > 54$  thì  $d_7 = 27, d_8 = 54, d_9 = d_8 + 17 = 71$  nên  $p = 71$ .

Vậy ta có hai số nguyên dương  $n$  thoả mãn điều kiện đề bài là

$$n = 2 \cdot 3^3 \cdot 37 \quad \text{và} \quad n = 2 \cdot 3^3 \cdot 71.$$

**Ví dụ 3.2.10 (Hungari 2000).** Với mỗi số nguyên dương  $k$  kí hiệu  $e(k)$  là số các ước số nguyên dương chẵn của  $k$ ,  $o(k)$  là số các ước số nguyên dương lẻ của  $k$ . Chứng minh rằng

$$\left| \sum_{k=1}^n e(k) - \sum_{k=1}^n o(k) \right| \leq n, \quad \forall n \geq 1.$$

### Giải

Ta có số các số nguyên dương chia hết cho  $d$  trong tập  $\{1, 2, \dots, n\}$  là  $\lfloor n/d \rfloor$  nên

$$e(k) = \sum_{d \text{ chẵn} \leq n} \lfloor \frac{n}{d} \rfloor, \quad o(k) = \sum_{d \text{ lẻ} \leq n} \lfloor \frac{n}{d} \rfloor.$$

Vì  $\lfloor n/d \rfloor \geq \lfloor n/(d+1) \rfloor$  với mọi số nguyên dương  $n, d$  nên

$$\sum_{k=1}^n o(k) - \sum_{k=1}^n e(k) = \sum_{i=1}^{\infty} \left( \lfloor \frac{n}{2i-1} \rfloor - \lfloor \frac{n}{2i} \rfloor \right) \geq 0,$$

$$\sum_{k=1}^n o(k) - \sum_{k=1}^n e(k) = \lfloor \frac{n}{1} \rfloor + \sum_{i=1}^{\infty} \left( \lfloor \frac{n}{2i} \rfloor - \lfloor \frac{n}{2i+1} \rfloor \right) \leq n.$$

## BÀI TẬP

**Bài 1 (Russia 2000).** Một số nguyên dương  $n$  được gọi là hoàn hảo nếu tổng tất cả các ước số của  $n$  (không kể chính nó) bằng  $n$ . Chứng minh rằng

- (a) Nếu một số hoàn hảo lớn hơn 6 và chia hết cho 3 thì nó chia hết cho 9.
- (b) Nếu một số hoàn hảo lớn hơn 28 và chia hết cho 7 thì nó chia hết cho 49.

**Bài 2 (St. Petersburg 1999).** Chứng minh rằng mỗi số nguyên dương nhỏ hơn  $n!$  đều biểu diễn được dưới dạng tổng của không quá  $n$  ước số nguyên dương của  $n!$ .

**Bài 3 (Iran 1997).** Tìm tất cả các số nguyên dương  $n$  thỏa mãn

$$n = d_1^2 + d_2^2 + d_3^2 + d_4^2,$$

trong đó  $d_1 < d_2 < d_3 < d_4$  là bốn ước số dương nhỏ nhất của  $n$ .

## LỜI GIẢI

### Bài 1 (Russia 2000).

Với mỗi số nguyên dương  $n$  kí hiệu  $\sigma(n)$  là tổng tất cả các ước số nguyên dương của  $n$ . Ta có  $\sigma(ab) = \sigma(a)\sigma(b)$  nếu  $(a, b) = 1$ ,  $\sigma(n) \geq n$  và  $n$  là số hoàn hảo nếu và chỉ nếu  $\sigma(n) = 2n$ .

Giả sử  $p \in \{3, 7\}$  và  $n$  là một số hoàn hảo chia hết cho  $p$  nhưng không chia hết cho  $p^2$ . Đặt  $n = 2^a pm$  với  $a, m$  là các số nguyên,  $a \geq 0$  và  $(m, 2p) = 1$ . Khi đó

$$2^{a+1}pm = 2n = \sigma(n) = \sigma(2^a)\sigma(p)\sigma(m) = (2^{a+1} - 1)(p + 1)\sigma(m).$$

Vì  $p + 1$  là lũy thừa của 2 ( $3 + 1 = 2^2, 7 + 1 = 2^3$ ), nên  $2^{a+1} \geq p + 1$ .

## BÀI TẬP

**Bài 1 (Russia 2000).** Một số nguyên dương  $n$  được gọi là hoàn hảo nếu tổng tất cả các ước số của  $n$  (không kể chính nó) bằng  $n$ . Chứng minh rằng

- (a) Nếu một số hoàn hảo lớn hơn 6 và chia hết cho 3 thì nó chia hết cho 9.
- (b) Nếu một số hoàn hảo lớn hơn 28 và chia hết cho 7 thì nó chia hết cho 49.

**Bài 2 (St. Petersburg 1999).** Chứng minh rằng mỗi số nguyên dương nhỏ hơn  $n!$  đều biểu diễn được dưới dạng tổng của không quá  $n$  ước số nguyên dương của  $n!$ .

**Bài 3 (Iran 1997).** Tìm tất cả các số nguyên dương  $n$  thỏa mãn

$$n = d_1^2 + d_2^2 + d_3^2 + d_4^2,$$

trong đó  $d_1 < d_2 < d_3 < d_4$  là bốn ước số dương nhỏ nhất của  $n$ .

## LỜI GIẢI

### Bài 1 (Russia 2000).

Với mỗi số nguyên dương  $n$  kí hiệu  $\sigma(n)$  là tổng tất cả các ước số nguyên dương của  $n$ . Ta có  $\sigma(ab) = \sigma(a)\sigma(b)$  nếu  $(a, b) = 1$ ,  $\sigma(n) \geq n$  và  $n$  là số hoàn hảo nếu và chỉ nếu  $\sigma(n) = 2n$ .

Giả sử  $p \in \{3, 7\}$  và  $n$  là một số hoàn hảo chia hết cho  $p$  nhưng không chia hết cho  $p^2$ . Đặt  $n = 2^a pm$  với  $a, m$  là các số nguyên,  $a \geq 0$  và  $(m, 2p) = 1$ . Khi đó

$$2^{a+1}pm = 2n = \sigma(n) = \sigma(2^a)\sigma(p)\sigma(m) = (2^{a+1} - 1)(p + 1)\sigma(m).$$

Vì  $p + 1$  là lũy thừa của 2 ( $3 + 1 = 2^2, 7 + 1 = 2^3$ ), nên  $2^{a+1} \geq p + 1$ .

Do đó,

$$\begin{aligned} 2^{a+1}pm &= (2^{a+1} - 1)(p + 1)\sigma m \\ &= \left(2^{a+1}\left(1 - \frac{1}{2^{a+1}}\right)\right)(p + 1)\sigma(m) \\ &\geq 2^{a+1}\left(1 - \frac{1}{p + 1}\right)(p + 1)\sigma(m) = 2^{a+1}p\sigma(m), \end{aligned}$$

dấu đẳng thức xảy ra khi và chỉ khi  $\sigma(m) = m$ , tức là  $m = 1$  và  $2^{a+1} = p + 1$ . Từ đó:

Với  $p = 3$  thì  $(m, a) = (1, 1)$ , suy ra  $n = 2^1 \cdot 3 \cdot 1 = 6$ .

Với  $p = 7$  thì  $(m, a) = (1, 2)$ , suy ra  $n = 2^2 \cdot 7 \cdot 1 = 28$ .

Vậy, nếu một số hoàn hảo lớn hơn 6 (tương ứng, 28) và chia hết cho 3 (tương ứng, 7) thì nó chia hết cho 9 (tương ứng, 49).

### Bài 2 (St. Petersburg 1999).

Cố định  $n$ , đặt

$$a_k = \frac{n!}{k!} \quad \text{với mọi } k = 1, 2, \dots, n.$$

Giả sử số nguyên dương  $m$  thoả mãn  $a_k \leq m < a_{k-1}$ , trong đó  $2 \leq k \leq n$ .

Xét

$$d_1 = a_k \left\lfloor \frac{m}{a_k} \right\rfloor,$$

ta có

$$0 \leq m - d_1 < a_k, \quad s_1 = \left\lfloor \frac{m}{a_k} \right\rfloor < \frac{a_{k-1}}{a_k} = k, \quad \frac{n!}{d_1} = \frac{k!}{s_1} \in \mathbb{N}.$$

Do đó,  $d_1$  là một ước số nguyên dương của  $n!$ . Xét  $m_1 = m - d_1 < a_k$  thay cho  $m$ .

Làm tương tự như trên, sau  $n - k$  bước ta thu được

$$m_{n-k} = m_{n-k-1} - d_{n-k} < a_{n-1} = n,$$

trong đó  $d_{n-k}$  là một ước số nguyên dương của  $n$ . Vì  $m_{n-k} < n$  nên  $m_{n-k}$  cũng là một ước số nguyên dương của  $n!$ . Do  $n-k+1 \leq n-2+1 = n-1$  và

$$m = d_1 + d_2 + \cdots + d_{n-k} + m_{n-k}$$

nên  $m$  có thể biểu diễn dưới dạng tổng của không quá  $n - 1$  ước số nguyên dương của  $n!$ . Điều phải chứng minh.

### Bài 3 (Iran 1997).

Nếu  $n$  là một số lẻ thì  $d_1, d_2, d_3, d_4$  là bốn số lẻ, do đó  $d_1^2 \equiv d_2^2 \equiv d_3^2 \equiv d_4^2 \equiv 1 \pmod{4}$  và

$$n = d_1^2 + d_2^2 + d_3^2 + d_4^2 \equiv 0 \pmod{4},$$

vô lý vì  $n$  là một số lẻ. Vậy  $n$  chỉ có thể là một số chẵn.

Nếu  $n \nmid 4$  thì  $d_1 = 1, d_2 = 2, d_3^2 + d_4^2$  chỉ có thể chia 4 dư 0, 1 hoặc 2. Ta có

$$n \equiv 1 + 0 + d_3^2 + d_4^2 \equiv 0 \pmod{4}$$

nên  $d_3^2 + d_4^2 \equiv 3 \pmod{4}$ , vô lý. Vậy  $n \equiv 2 \pmod{4}$ . Do đó chỉ có thể xảy ra hai khả năng sau

$$\{d_1, d_2, d_3, d_4\} = \{1, 2, p, 2p\}, \quad \text{hoặc} \quad \{d_1, d_2, d_3, d_4\} = \{1, 2, p, q\}$$

với  $p, q$  là các số nguyên tố nào đó.

Trường hợp  $\{d_1, d_2, d_3, d_4\} = \{1, 2, p, q\}$  không xảy ra vì khi đó  $n \equiv 3 \pmod{4}$ . Vậy  $\{d_1, d_2, d_3, d_4\} = \{1, 2, p, 2p\}$  nên

$$n = d_1^2 + d_2^2 + d_3^2 + d_4^2 = 5(1 + p^2),$$

suy ra  $n \nmid 5$  và  $p = 5$ . Từ đó ta có  $n = 130$ .

### 3 Hàm Möbius

**Định nghĩa 3.3.1.**

Với mỗi số nguyên dương  $n$  đặt

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{nếu } n \text{ không có ước số chính phương,} \\ 0 & \text{nếu trái lại.} \end{cases}$$

Hàm  $\mu(n)$  được gọi là hàm Möbius.

**Định lý 3.3.1.**

Hàm  $\mu(n)$  là một hàm nhân tính thỏa mãn

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{nếu } n = 1, \\ 0 & \text{nếu } n > 1. \end{cases}$$

#### Chứng minh

Để thấy  $\mu(n)$  là một hàm nhân tính nên theo định lý 3.2.3 ta có  $F(n) = \sum_{d|n} \mu(d)$  cũng là một hàm nhân tính.

Hiển nhiên  $F(1) = 1$ . Nếu  $p$  là một số nguyên tố và  $\alpha$  là một số nguyên dương thì

$$F(p^\alpha) = \sum_{\beta=0}^{\alpha} \mu(p^\beta) = 1 + \mu(p) = 1 + (-1) = 0.$$

Do đó,  $F(n) = 0$  với mọi  $n > 1$ .

**Định lý 3.3.2 (Công thức ngược Möbius).**

Nếu với mọi số nguyên dương  $n$ ,

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

thì

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

**Chứng minh**

Ta có

$$\begin{aligned} \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{k|(n/d)} f(k) \\ &= \sum_{dk|n} \mu(d) f(k) \\ &= \sum_{k|n} f(k) \sum_{d|(n/k)} \mu(d) \\ &= f(n) \end{aligned}$$

theo định lý 3.3.1.

Chú ý rằng định lý 3.3.2 đảo cũng đúng. Ta có định lý sau.

**Định lý 3.3.3.**

Nếu với mọi số nguyên dương  $n$ ,

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

thì

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

**Chứng minh**

Ta có

$$\begin{aligned} \sum_{d|n} f(d) &= \sum_{d|n} \sum_{k|d} \mu(k) F\left(\frac{d}{k}\right) \\ &= \sum_{d|n} \sum_{k|d} \mu\left(\frac{d}{k}\right) F(k) \\ &= \sum_{k|n} \sum_{r|(n/k)} \mu(r) F(k) \\ &= \sum_{k|n} \left( F(k) \sum_{r|(n/k)} \mu(r) \right) \\ &= F(n) \end{aligned}$$

theo định lý 3.3.1.

Theo định lý 3.2.4 ta có  $\sum_{d|n} \phi(d) = n$ . Từ đó và định lý 3.3.2 suy ra

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Từ đẳng thức này có thể suy ra công thức của  $\phi(n)$ . Thật vậy, do  $\mu(d)/d$  là một hàm nhán tính nên từ định lý 3.2.2,  $\phi(n)$  cũng là một hàm nhán tính. Vì vậy chỉ cần chứng minh rằng có thể suy ra công thức của  $\phi(n)$  với  $n = p^\alpha$  là luỹ thừa của một số nguyên tố. Ta có

$$\sum_{d|n} \frac{\mu(d)}{d} = \sum_{\beta=0}^{\alpha} \frac{\mu(p^\beta)}{p^\beta} = 1 - \frac{1}{p}.$$

Do đó

$$\phi(p^\alpha) = p^\alpha \sum_{d|p^\alpha} \frac{\mu(d)}{d} = p^\alpha - p^{\alpha-1}.$$

Tức là có điều phải chứng minh.

## TÀI LIỆU THAM KHẢO

- [1]. Titu Andreescu, Razvan Gelca  
Mathematical Olympiad Challenges - 2001, Birkhauser Boston, Second printe, United states of America.
- [2]. Titu Andreescu, Bogdan Enescu  
Mathematical Olympiad Treasures - 2004, Birkhauser Boston, USA.
- [3]. H.V.Gorbachôv  
Tuyển tập các đề thi vô địch môn toán - NXB MCNMO - Moskva 2004  
(bản tiếng Nga)
- [4]. Các đề thi vô địch quốc gia, quốc tế môn toán (từ 1995 - 2005).