

SỞ GIÁO DỤC VÀ ĐÀO TẠO ĐẮK LẮK  
TRƯỜNG THPT PHAN ĐÌNH PHÙNG

\*\*\*\*\*

HÀ DUY NGHĨA

ỨNG DỤNG LÝ THUYẾT ĐỒNG DƯ  
TRONG CÁC BÀI TOÁN CHIA HẾT

CHUYÊN ĐỀ BỒI DƯỠNG HSG

# MỤC LỤC

<b>Mục lục</b>	<b>i</b>
<b>Chương 1 ĐỒNG DƯ VÀ ÁP DỤNG</b>	<b>1</b>
1.1 Đồng dư thức . . . . .	1
1.1.1 Một số khái niệm và tính chất cơ bản . . . . .	1
1.1.2 Ứng dụng của lý thuyết đồng dư để tìm dấu hiệu chia hết . . . . .	4
1.2 Phương trình đồng dư . . . . .	10
1.2.1 Phương trình đồng dư bậc nhất một ẩn . . . . .	10
1.2.2 Hệ phương trình đồng dư đồng dư bậc nhất một ẩn . . . . .	11
1.2.3 Ứng dụng . . . . .	11
1.3 Các hàm số học . . . . .	12
1.3.1 Phi hàm Öle $\varphi(t)$ . . . . .	12
1.3.2 Hàm Möbius $\mu n$ . . . . .	15
1.3.3 Hàm tổng các ước dương $\sigma(n)$ . . . . .	15
1.3.4 Ứng dụng . . . . .	17
1.4 Bài tập tự luyện . . . . .	18
<b>Chương 2 MỘT SỐ BÀI TOÁN TRONG CÁC KỲ THI HỌC SINH GIỎI</b>	<b>20</b>
2.1 Các bài toán trong các kỳ thi Olympic . . . . .	20
2.2 Các bài toán trong kỳ thi học sinh giỏi Quốc gia . . . . .	22
<b>Tài liệu tham khảo</b>	<b>28</b>

# Chương 1

## LÝ THUYẾT ĐỒNG DƯ VÀ ÁP DỤNG

### 1.1 Đồng dư thức

#### 1.1.1 Một số khái niệm và tính chất cơ bản

**Định nghĩa 1.1.1.** Cho  $a, b, m$  là các số nguyên,  $m \neq 0$ . Số  $a$  được gọi là *đồng dư* với  $b$  theo môđun  $m$  nếu  $m$  là ước của  $(b - a)$ .

Nếu  $a$  đồng dư với  $b$  theo môđun  $m$  thì viết  $a \equiv b \pmod{m}$ . Ngược lại, nếu  $a$  không đồng dư với  $b$  theo môđun  $m$  thì ta viết  $a \not\equiv b \pmod{m}$ .

Ví dụ  $2 \equiv 5 \pmod{3}$  vì  $3 \mid (5 - 2)$ .

Nếu  $a \equiv b \pmod{m}$  thì  $b$  gọi là một *thặng dư* của  $a$  theo môđun  $m$ .

Nếu  $0 \leq b \leq m - 1$  thì  $b$  gọi là một *thặng dư bé nhất* của  $a$  theo môđun  $m$ .

**Mệnh đề 1.1.2.** Cho  $a, b, c, m$  là những số nguyên  $m \neq 0$ . Khi đó, ta có

(i)  $a \equiv a \pmod{m}$ ,

(ii) Nếu  $a \equiv b \pmod{m}$  thì  $b \equiv a \pmod{m}$ ,

(iii) Nếu  $a \equiv b \pmod{m}$  và  $b \equiv c \pmod{m}$  thì  $a \equiv c \pmod{m}$ .

*Chứng minh.* Mệnh đề (i), (ii) là hiển nhiên, ta chứng minh mệnh đề (iii). Thật vậy, ta có  $a \equiv b \pmod{m}, b \equiv c \pmod{m}$  suy ra  $m \mid (b - a)$  và  $m \mid (c - b)$ . Do đó  $m \mid (b - a + c - b)$ , hay  $m \mid (c - a)$ . Vậy  $a \equiv c \pmod{m}$ .  $\square$

Tiếp theo, ký hiệu  $\bar{a}$  là tập hợp tất cả các số nguyên đồng dư với  $a$  theo môđun  $m$ ,  $\bar{a} = \{n \in \mathbb{Z} \mid n \equiv a \pmod{m}\}$ . Nói cách khác,  $\bar{a}$  là tập hợp các số nguyên có dạng  $\{a + km\}$ . Từ đó, ta có định nghĩa sau.

**Định nghĩa 1.1.3.** Một tập gồm các phần tử dạng  $\bar{a} = \{a + km, k \in \mathbb{Z}\}$  gọi là một *lớp đồng dư* của  $a$  theo môđun  $m$ .

Ví dụ với  $m = 2$ , ta có lớp  $\bar{0}$  là tập các số nguyên chẵn, lớp  $\bar{1}$  là tập các số nguyên lẻ.

**Mệnh đề 1.1.4.** Cho  $a, b, m$  là những số nguyên  $m \neq 0$ . Khi đó, ta có

(i)  $\bar{a} = \bar{b}$  khi và chỉ khi  $a \equiv b \pmod{m}$ ,

(ii)  $\bar{a} \neq \bar{b}$  khi và chỉ khi  $\bar{a} \cap \bar{b} = \emptyset$ ,

(iii) Có đúng  $m$  lớp đồng dư phân biệt theo môđun  $m$ .

*Chứng minh.* (i) Giả sử  $\bar{a} = \bar{b}$ , ta xét  $a \in \bar{a} = \bar{b}$ . Do đó,  $a \equiv b \pmod{m}$ . Ngược lại, nếu  $a \equiv b \pmod{m}$  thì  $a \in \bar{b}$ . Ngoài ra, nếu  $c \equiv a \pmod{m}$  thì  $c \equiv b \pmod{m}$ . Điều này chứng tỏ rằng  $\bar{a} \subseteq \bar{b}$ . Hơn nữa, từ  $a \equiv b \pmod{m}$  ta suy ra  $b \equiv a \pmod{m}$ , hay  $\bar{b} \subseteq \bar{a}$ . Từ đó suy ra  $\bar{a} = \bar{b}$ .

(ii) Dễ thấy rằng, nếu  $\bar{a} \cap \bar{b} = \emptyset$  thì  $\bar{a} \neq \bar{b}$ . Ngược lại, ta cần chứng tỏ rằng nếu  $\bar{a} \cap \bar{b} \neq \emptyset$  thì  $\bar{a} = \bar{b}$ . Thật vậy, giả sử  $\bar{a} \cap \bar{b} \neq \emptyset$  gọi  $c \in \bar{a} \cap \bar{b}$ . Khi đó, ta có  $c \equiv a \pmod{m}$  và  $c \equiv b \pmod{m}$ . Điều này suy ra  $a \equiv b \pmod{m}$ . Do đó, theo (i) ta suy ra  $\bar{a} = \bar{b}$ .

(iii) Để chứng minh phần này, ta chứng minh tập  $\{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$  là  $m$  lớp đồng dư phân biệt theo môđun  $m$ . Thật vậy, giả sử tồn tại  $0 \leq k < l < m$  sao cho  $\bar{k} = \bar{l}$ . Khi đó, theo (i) ta có  $k \equiv l \pmod{m}$ , hay  $m \mid (l - k)$ . Điều này mâu thuẫn với giả thiết  $0 < l - k < m$ . Do đó,  $\bar{k} \neq \bar{l}$ . Ngoài ra, với mỗi  $a \in \mathbb{Z}$  luôn tồn tại cặp số nguyên  $q, r$  sao cho  $a = qm + r$ ,  $0 \leq r < m$ , suy ra  $a \equiv r \pmod{m}$  hay  $\bar{a} = \bar{r}$ .  $\square$

**Định nghĩa 1.1.5.** Tập gồm  $m$  phần tử  $\{A = a_1, a_2, \dots, a_m\}$  gọi là một hệ thặng dư đầy đủ theo môđun  $m$  nếu  $\{B = \bar{a}_1, \bar{a}_2, \bar{a}_3, \dots, \bar{a}_m\}$  là tập gồm  $m$  lớp đồng dư phân biệt theo môđun  $m$ .

Từ định nghĩa ta thấy rằng, hệ thặng dư đầy đủ theo môđun  $m$  là không duy nhất. Ví dụ các tập  $\{0, 1, 2, 3\}$ ,  $\{4, 9, 14, -1\}$ ,  $\{0, 1, -2, -1\}$  là những hệ thặng dư đầy đủ theo môđun 4.

**Mệnh đề 1.1.6.** Nếu  $a \equiv c \pmod{m}$  và  $b \equiv d \pmod{m}$  thì  $a + b \equiv c + d \pmod{m}$  và  $ab \equiv cd \pmod{m}$ .

*Chứng minh.* Dễ dàng suy ra từ định nghĩa.  $\square$

**Mệnh đề 1.1.7.** Cho  $a, b, c, m$  là các số nguyên,  $m > 0$ ,  $ac \equiv bc \pmod{m}$  và  $d = (c, m)$ . Khi đó, ta có

$$a \equiv b \pmod{\frac{m}{d}}.$$

*Chứng minh.* Giả sử  $ac \equiv bc \pmod{m}$ . Ta có  $m \mid (bd - ac)$ , suy ra tồn tại số nguyên  $k$  sao cho  $c(b - a) = km$ . Khi đó, chia hai vế cho  $d$  ta được  $\frac{c}{d}(b - a) = k\frac{m}{d}$ . Ngoài ra, theo giả thiết ta có  $d = (c, m)$ , suy ra  $\frac{c}{d}, \frac{m}{d} = 1$ . Do đó, ta có  $\frac{m}{d} \mid (b - a)$  hay

$$a \equiv b \pmod{\frac{m}{d}}. \quad \square$$

**Mệnh đề 1.1.8.** Cho  $a, b, m_1, \dots, m_k$  là các số nguyên,  $m_1, \dots, m_k > 0$ ,  $a \equiv b \pmod{m_1}$ ,  $a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$ . Khi đó, ta có

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

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

*Chứng minh.* Suy ra trực tiếp từ định nghĩa. □

**Mệnh đề 1.1.9.** Nếu  $a \equiv b \pmod{n}$  thì  $a^n \equiv b^n \pmod{n^2}$ .

*Chứng minh.* Từ  $a \equiv b \pmod{n}$  suy ra  $a = b + nq$ . Do đó, theo công thức khai triển nhị thức ta có

$$\begin{aligned} a^n - b^n &= (b + nq)^n - b^n \\ &= \binom{n}{1} b^{n-1} q n + \binom{n}{2} b^{n-2} q^2 n^2 + \dots + \binom{n}{n} q^n n^n \\ &= n^2 \left( b^{n-1} q + \binom{n}{2} b^{n-2} q^2 + \dots + \binom{n}{n} q^n n^{n-2} \right). \end{aligned}$$

Từ đó suy ra  $a^n \equiv b^n \pmod{n^2}$ .

Điều ngược lại không đúng, ví dụ như  $3^4 \equiv 1^4 \pmod{4^2}$  nhưng  $3 \not\equiv 1 \pmod{4}$ . □

**Mệnh đề 1.1.10.** Nếu  $a, b$  là các số nguyên và  $p$  là số nguyên tố thì

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

*Chứng minh.* Theo công thức khai triển nhị thức ta có

$$(a + b)^p = a^p + b^p + \binom{p}{1} a^{p-1} b + \dots + \binom{p}{p-1} a b^{p-1}.$$

Do đó, để chứng minh mệnh đề ta chỉ cần chứng minh  $p \mid \binom{p}{k}$ , ( $1 \leq k \leq p-1$ ). Thật vậy, ta có

$$\binom{p}{k} = \frac{p!}{k!(p-k)!},$$

suy ra

$$\begin{aligned} k \binom{p}{k} &= \frac{p!}{(k-1)!(p-k)!} \\ &= p \frac{(p-1)!}{(k-1)!(p-k)!} = p \binom{p-1}{k-1}. \end{aligned}$$

Từ đó,  $p \mid k \binom{p}{k}$ . Ngoài ra, do  $\text{ƯCLN}(p, k) = 1$  nên  $p \mid \binom{p}{k}$ .  $\square$

### 1.1.2 Ứng dụng của lý thuyết đồng dư để tìm dấu hiệu chia hết

**Ví dụ 1.1.2.1.** Tìm dấu hiệu chia hết cho  $2^k, 3, 5^k, 7, 11, 13, 37$ .

**Lời giải:** Xét số tự nhiên  $a = \overline{a_n a_{n-1} \dots a_0}$ . Tức là  $a$  được viết dưới dạng

$$a = a_n \cdot 10^n + \dots + a_1 \cdot 10 + a_0, (0 \leq a_i \leq 9).$$

- *Dấu hiệu chia hết cho  $2^k$ .*

Vì  $10 \equiv 0 \pmod{2}$  nên  $10^k \equiv 0 \pmod{2^k}$ . Từ đó suy ra

$$a \equiv a_{k-1} \cdot 10^{k-1} + \dots + a_0 \pmod{2^k}.$$

Do đó, số  $a$  chia hết cho  $2^k$  khi số  $b = a_{k-1} \cdot 10^{k-1} + \dots + a_0 \equiv 0 \pmod{2^k}$ , tức là  $b$  chia hết cho  $2^k$ . Nói cách khác, số tự nhiên  $a$  chia hết cho  $2^k$  khi số tự nhiên  $b$  được lập từ  $k$  chữ số tận cùng của  $a$  chia hết cho  $2^k$ .

Tương tự, ta cũng có  $10 \equiv 0 \pmod{5}$  và  $10^k \equiv 0 \pmod{5^k}$ . Do đó, số  $a$  chia hết cho  $5^k$  khi số  $b$  lập từ  $k$  chữ số tận cùng của  $a$  chia hết cho  $5^k$ .

- *Dấu hiệu chia hết cho 3 và 9.*

Ta có  $10 \equiv 1 \pmod{3}$  suy ra  $10^k \equiv 1 \pmod{3}$ . Do đó  $a_i \cdot 10^k \equiv a_i \pmod{3}$ . Từ đó suy ra  $a = a_n \cdot 10^n + \dots + a_1 \cdot 10 + a_0 \equiv a_n + \dots + a_0 \pmod{3}$ . Vậy, số  $a$  chia hết cho 3 khi tổng các chữ số của nó chia hết cho 3.

Tương tự ta cũng có  $10 \equiv 1 \pmod{9}$  và  $a_i \cdot 10^k \equiv a_i \pmod{9}$ . Vậy, số  $a$  chia hết cho 9 khi tổng các chữ số của nó chia hết cho 9.

- *Dấu hiệu chia hết cho 7*

Ta có

$$\begin{aligned}
 a_0 &\equiv a_0 \pmod{7} && \Rightarrow a_0 \equiv a_0 \pmod{7} \\
 10 &\equiv 3 \pmod{7} && \Rightarrow 10a_1 \equiv 3a_1 \pmod{7} \\
 10^2 &\equiv 2 \pmod{7} && \Rightarrow 10^2a_2 \equiv 2a_2 \pmod{7} \\
 10^3 &\equiv -1 \pmod{7} && \Rightarrow 10^3a_3 \equiv -1a_3 \pmod{7} \\
 &\dots &&
 \end{aligned}$$

Từ đó, ta có bảng đồng dư theo môđun 7 tương ứng như sau

$a_0$	$10a_1$	$10^2a_2$	$10^3a_3$	$10^4a_4$	$10^5a_5$	$10^6a_6$	$10^7a_7$	$10^8a_8$	$10^9a_9$	$10^{10}a_{10}$	$10^{11}a_{11}$	...	$10^{6t-1}a_{6t-1}$
$a_0$	$3a_1$	$2a_2$	$-a_3$	$-3a_4$	$-2a_5$	$a_6$	$3a_7$	$2a_8$	$-a_9$	$-3a_{10}$	$-2a_{11}$	...	$-2a_{6t-1}$

Bảng 1.1:

Do đó, số  $a = \overline{a_n a_{n-1} \dots a_1 a_0}$  chia hết cho 7 khi tổng dạng

$$(a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + \dots) + \dots - (a_{6t-3} + 3a_{6t-2} + 2a_{6t-1}) \equiv 0 \pmod{7}$$

Ngoài ra, với mọi số  $x, y, z$  ta đều có

$$x \quad 3y \quad 2z \equiv 100z + 10y + x \pmod{7} \equiv \overline{zyx} \pmod{7}.$$

Từ đó suy ra, số  $a = \overline{a_n a_{n-1} \dots a_1 a_0}$  chia hết cho 7 khi tổng dạng

$$\overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \overline{a_{11} a_{10} a_9} + \dots, \text{ chia hết cho 7}$$

- *Dấu hiệu chia hết cho 11*

Tương tự dấu hiệu chia hết cho 7, ta cũng có

$$\begin{aligned}
 a_0 &\equiv a_0 \pmod{11} && \Rightarrow a_0 \equiv a_0 \pmod{11} \\
 10 &\equiv -1 \pmod{11} && \Rightarrow 10a_1 \equiv -a_1 \pmod{11} \\
 10^2 &\equiv 1 \pmod{11} && \Rightarrow 10^2a_2 \equiv a_2 \pmod{11} \\
 10^3 &\equiv -1 \pmod{11} && \Rightarrow 10^3a_3 \equiv -1a_3 \pmod{11} \\
 &\dots &&
 \end{aligned}$$

$a_0$	$10a_1$	$10^2a_2$	$10^3a_3$	$10^4a_4$	$10^5a_5$	$10^6a_6$	$10^7a_7$	$10^8a_8$	$10^9a_9$	$10^{10}a_{10}$	$10^{11}a_{11}$	...	$10^{2t-1}a_{2t-1}$
$a_0$	$-a_1$	$a_2$	$-a_3$	$a_4$	$-a_5$	$a_6$	$-a_7$	$a_8$	$-a_9$	$a_{10}$	$-a_{11}$	...	$-a_{2t-1}$

Bảng 1.2:

Do đó, số  $a = \overline{a_n \cdot a_{n-1} \dots a_1 a_0}$  chia hết cho 11 khi tổng dạng

$$a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + a_6 + \dots - a_{2t-1} \equiv 0 \pmod{11}$$

Nói cách khác, số  $a = \overline{a_n \cdot a_{n-1} \dots a_1 a_0}$  chia hết cho 11 khi tổng đan dấu

$$a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + a_6 + \dots - a_{2t-1} \text{ chia hết cho 11}$$

- *Dấu hiệu chia hết cho 13*

Ta có

$$\begin{aligned} 10^0 &\equiv 1 \pmod{13} && \Rightarrow 10^0 a_0 \equiv 1 a_0 \pmod{13} \\ 10^1 &\equiv -3 \pmod{13} && \Rightarrow 10^1 a_1 \equiv -3 a_1 \pmod{13} \\ 10^2 &\equiv 4 \pmod{13} && \Rightarrow 10^2 a_2 \equiv 4 a_2 \pmod{13} \\ 10^3 &\equiv 1 \pmod{13} && \Rightarrow 10^3 a_3 \equiv 1 a_3 \pmod{13} \\ &\dots && \dots \end{aligned}$$

Tương tự ta cũng có bảng các lớp đồng dư theo môđun 13 (Bảng 1.3)

$a_0$	$10a_1$	$10^2a_2$	$10^3a_3$	$10^4a_4$	$10^5a_5$	$10^6a_6$	$10^7a_7$	$10^8a_8$	$10^9a_9$	$10^{10}a_{10}$	$10^{11}a_{11}$	...	$10^{6t-1}a_{6t-1}$
$a_0$	$-3a_1$	$-4a_2$	$-a_3$	$3a_4$	$4a_5$	$a_6$	$-3a_7$	$-4a_8$	$-a_9$	$3a_{10}$	$4a_{11}$	...	$4a_{6t-1}$

Bảng 1.3:

Từ bảng 1.3 ta suy ra rằng, số  $a = \overline{a_n \cdot a_{n-1} \dots a_1 a_0}$  chia hết cho 13 khi tổng dạng

$$(a_0 - 3a_1 - 4a_2) - 3(a_3 - 3a_4 - 4a_5) + \dots - a_6(-3 - 3a_{6t-2} - 4a_{6t-1}) \equiv 0 \pmod{13}$$

Ngoài ra, với mọi số  $x, y, z$  ta đều có

$$x - 3y - 4z \equiv 100z + 10y + x \pmod{13} \equiv \overline{zyx} \pmod{13}.$$

Từ đó suy ra, số  $a = \overline{a_n \cdot a_{n-1} \dots a_1 a_0}$  chia hết cho 13 khi tổng dạng

$$\overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \overline{a_{11} a_{10} a_9} + \dots \text{ chia hết cho 13.}$$



- *Dấu hiệu chia hết cho 33*

Ta có

$$\begin{aligned}
 a_0 &\equiv a_0 \pmod{33} && \Rightarrow a_0 \equiv a_0 \pmod{33} \\
 10 &\equiv 10 \pmod{33} && \Rightarrow 10a_1 \equiv 10a_1 \pmod{33} \\
 10^2 &\equiv 1 \pmod{33} && \Rightarrow 10^2 a_2 \equiv a_2 \pmod{33} \\
 10^3 &\equiv 10 \pmod{33} && \Rightarrow 10^3 a_3 \equiv 10a_3 \pmod{33} \\
 &\dots &&
 \end{aligned}$$

$a_0$	$10a_1$	$10^2 a_2$	$10^3 a_3$	$10^4 a_4$	$10^5 a_5$	$10^6 a_6$	$10^7 a_7$	$10^8 a_8$	$10^9 a_9$	$10^{10} a_{10}$	$10^{11} a_{11}$	...	$10^{2t} a_{2t}$
$a_0$	$10a_1$	$a_2$	$10a_3$	$a_4$	$10a_5$	$a_6$	$10a_7$	$a_8$	$10a_9$	$a_{10}$	$10a_{11}$	...	$a_{2t}$

Bảng 1.4:

Từ bảng 1.4 ta suy ra rằng, số  $a = \overline{a_n a_{n-1} \dots a_1 a_0}$  chia hết cho 33 khi tổng dạng

$$(a_0 + a_2 + \dots + a_{2t}) + 10(a_1 + a_3 + \dots + a_{2t+1}) \equiv 0 \pmod{33}$$

Ngoài ra, với mọi số  $x, y$  ta đều có

$$x - 10y \equiv 10y + x \pmod{33} \equiv \overline{yx} \pmod{33}.$$

Từ đó suy ra, số  $a = \overline{a_n a_{n-1} \dots a_1 a_0}$  chia hết cho 33 khi tổng dạng

$$\overline{a_1 a_0} \quad \overline{a_3 a_2} \quad \overline{a_5 a_4} \quad \overline{a_6 a_5} \quad \dots \text{chia hết cho } 33.$$

Ngoài ra, ta có  $33 = 11 \cdot 3$  nên ta suy ra được một dấu hiệu khác nữa của số chia hết cho 11; 3 là tổng dạng

$$\overline{a_1 a_0} \quad \overline{a_3 a_2} \quad \overline{a_5 a_4} \quad \overline{a_6 a_5} \quad \dots, \text{ chia hết cho } 11; 3.$$

- *Dấu hiệu chia hết cho 37*

Ta có

$$\begin{aligned}
 a_0 &\equiv a_0 \pmod{37} && \Rightarrow a_0 \equiv a_0 \pmod{37} \\
 10 &\equiv 10 \pmod{37} && \Rightarrow 10a_1 \equiv 10a_1 \pmod{37} \\
 10^2 &\equiv -11 \pmod{37} && \Rightarrow 10^2 a_2 \equiv -11a_2 \pmod{37}
 \end{aligned}$$

$$\begin{aligned}
10^3 &\equiv 1 \pmod{37} && \Rightarrow 10^3 a_3 \equiv 1a_3 \pmod{37} \\
10^4 &\equiv 10 \pmod{37} && \Rightarrow 10^4 a_3 \equiv 10a_3 \pmod{37} \\
10^5 &\equiv -11 \pmod{37} && \Rightarrow 10^5 a_3 \equiv -11a_3 \pmod{37} \\
&\dots &&
\end{aligned}$$

$a_0$	$10a_1$	$10^2 a_2$	$10^3 a_3$	$10^4 a_4$	$10^5 a_5$	$10^6 a_6$	$10^7 a_7$	$10^8 a_8$	$10^9 a_9$	$10^{10} a_{10}$	$10^{11} a_{11}$	...	$10^{2t} a_{3t}$
$a_0$	$10a_1$	$-11a_2$	$a_3$	$10a_4$	$-11a_5$	$a_6$	$10a_7$	$-11a_8$	$a_9$	$10a_{10}$	$-a_{11}$	...	$-11a_{3t}$

Bảng 1.5:

Từ bảng 1.5 ta suy ra rằng, số  $a = \overline{a_n a_{n-1} \dots a_1 a_0}$  chia hết cho 37 khi tổng dạng

$$(a_0 + a_3 + \dots + a_{3t}) + 10(a_1 + a_4 + \dots + a_{3t+1}) - 11(a_2 + a_5 + \dots + a_{3t+2}) \equiv 0 \pmod{37}$$

Ngoài ra, với mọi số  $x, y, z$  ta đều có

$$x - 10y - 11z \equiv 100z + 10y + x \pmod{37} \equiv \overline{zyx} \pmod{37}.$$

Từ đó suy ra, số  $a = \overline{a_n a_{n-1} \dots a_1 a_0}$  chia hết cho 37 khi tổng dạng

$$\overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \dots, \text{ chia hết cho 37.}$$

**Ví dụ 1.1.2.2.** Chứng minh rằng

- $4^{4021} + 3^{2012}$  chia hết cho 13,
- $6^{2023} + 8^{2023}$  chia hết cho 49,
- $220^{119^{69}} + 119^{69^{220}} + 69^{220^{119}}$  chia hết cho 102,
- $2222^{5555} + 5555^{2222}$  chia hết cho 7.

**Lời giải** a) Ta có

$$\begin{aligned}
4^{4021} - 3^{2012} &= 4 \cdot 16^{2010} - 9 \cdot 3^{2010} \\
&\equiv 4(16^{2010} - 3^{2010}) \pmod{13} \\
&= (16 - 3)(16^{2009} + 16^{2008} \cdot 3 + \dots + 3^{2009}) \pmod{13} \\
&\equiv 0 \pmod{13}.
\end{aligned}$$

Vậy,  $4^{4021} \cdot 3^{2012}$  chia hết cho 13.

b) Ta có  $6^{2023} \cdot 8^{2023} = (6+8)(6^{2022} - 6^{2021}8 + 6^{2020}8^2 + \dots + 8^{2022}) = 14M$ , trong đó

$$M = (6^{2022} - 6^{2021}8 + 6^{2020}8^2 + \dots + 8^{2022}).$$

Hơn nữa,  $M \equiv \underbrace{(-1)^{2022} + 1^{2021} - \dots - 1^{2022}}_{2023 \text{ số hạng}} \equiv 2023 \equiv 0 \pmod{7}$ , hay  $7|M$ . Từ đó

suy ra,  $49|14M$  hay  $6^{2023} + 8^{2023}$  chia hết cho 49.

c) Ta có

$$\begin{aligned} 220 &\equiv 0 \pmod{2} \Rightarrow 220^{119^{69}} \equiv 0 \pmod{2} \\ 119 &\equiv 1 \pmod{2} \Rightarrow 119^{220^{69}} \equiv 1 \pmod{2}, \\ 69 &\equiv 1 \pmod{2} \Rightarrow 69^{220^{119}} \equiv 1 \pmod{2}. \end{aligned}$$

Do đó,  $A = 220^{119^{69}} + 119^{69^{220}} + 69^{220^{119}}$  chia hết cho 2.

Tương tự ta cũng chứng minh được  $A$  chia hết cho 3, 17. Vì các số  $\{2, 3, 17\}$  là những số đôi một nguyên tố cùng nhau nên ta suy ra  $A$  chia hết cho 102.

d) Ta có  $2222 \equiv 3 \pmod{7}$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv -1 \pmod{7}$ . Do đó

$$2222^{5555} \equiv 3^{3 \cdot 1851 + 2} \equiv -2 \pmod{7}.$$

Tương tự, ta cũng có  $5555 \equiv 4 \pmod{7}$ ,  $4^3 \equiv 1 \pmod{7}$ ,  $4^2 \equiv 2 \pmod{7}$  nên

$$5555^{2222} \equiv 4^{3 \cdot 740 + 2} \equiv 2 \pmod{7}.$$

Từ đó suy ra,  $2222^{5555} \cdot 5555^{2222} \equiv 0 \pmod{7}$  hay  $2222^{5555} + 5555^{2222} \equiv 0 \pmod{7}$ .

**Ví dụ 1.1.2.3.** Tìm số dư của số  $1234356789^4$  khi chia cho 8.

**Lời giải:** Vì  $8 = 2^3$  nên số dư của phép chia  $1234356789^4$  cho 8 cũng chính là số dư của  $789^4$  khi chia cho 8. Do đó, ta có

$$1234356789^4 \equiv 789^4 \equiv 5^4 \equiv 1 \pmod{8}.$$

Từ đó suy ra số dư của phép chia  $1234356789^4$  cho 8 là 1.

## 1.2 Phương trình đồng dư

### 1.2.1 Phương trình đồng dư bậc nhất một ẩn

**Định nghĩa 1.2.1.** Phương trình đồng dư tuyến tính một ẩn số là phương trình dạng  $ax \equiv b \pmod{m}$ , trong đó  $a, b, m \in \mathbb{Z}, m \neq 0, a \not\equiv 0 \pmod{m}$ .

Một nghiệm của phương trình là số nguyên  $x_0$  thỏa mãn  $ax_0 \equiv b \pmod{m}$ .

Ví dụ 3, 8, 13 là những nghiệm của phương trình  $6x \equiv 3 \pmod{15}$ . Số 18 cũng là nghiệm, nhưng  $18 \equiv 3 \pmod{15}$ .

**Mệnh đề 1.2.2.** Gọi  $d = \text{ƯCLN}(a, m)$ . Khi đó, phương trình đồng dư  $ax \equiv b \pmod{m}$  có nghiệm nếu và chỉ nếu  $d|b$ . Hơn nữa, nếu  $x_0$  là nghiệm thì phương trình có đúng  $d$  nghiệm không đồng dư theo môđun  $m$ .

*Chứng minh.* Nếu  $x_0$  là nghiệm thì  $ax_0 - b = my_0$  với mỗi số nguyên  $y_0$ . Do đó,  $ax_0 - my_0 = b$ . Ngoài ra, ta có  $d = \text{ƯCLN}(a, m)$  suy ra  $d|(ax_0 - my_0 = b)$ .

Ngược lại, giả sử  $d|b$ , khi đó tồn tại hai số nguyên  $x_0, y_0$  sao cho  $d = ax_0 - my_0$ . Đặt  $c = \frac{b}{d}$ , nhân cả hai vế phương trình trên cho  $c$  ta được  $a(x_0c) - m(y_0c) = b$ . Điều này suy ra  $x = x_0c$  là nghiệm của phương trình  $ax \equiv b \pmod{m}$ .

Tiếp theo, ta chứng minh phương trình này có đúng  $d$  nghiệm không đồng dư theo môđun  $m$ . Thật vậy, giả sử  $x_1, x_2$  là hai nghiệm của phương trình. Khi đó,  $a(x_1 - x_0) \equiv 0 \pmod{m}$  suy ra  $m|a(x_1 - x_0)$ . Hơn nữa, ta có  $d = \text{ƯCLN}(a, m)$  nên đặt  $m' = \frac{m}{d}, a' = \frac{a}{d}$  ta cũng có  $m'|a'(x_1 - x_0)$  suy ra  $m'|(x_1 - x_0)$  hay  $x_1 = x_0 + km'$  với mỗi số nguyên  $k$ . Do đó, mọi nghiệm của phương trình đều có dạng  $x_0 + km', k \in \mathbb{Z}$ . Ngoài ra, do với hai số nguyên  $k, d$  luôn tồn tại hai số nguyên  $q, r$  sao cho  $k = qd + r, 0 \leq r < d$  khi đó  $x_1 = x_0 + qdm' + rm' = x_0 + qm + rm'$  nghiệm này đồng dư với nghiệm  $x_0 + rm'$ . Điều này chứng tỏ các nghiệm không đồng dư của phương trình là  $x_0, x_0 + m', \dots, x_0 + (d-1)m'$ .  $\square$

Quay lại ví dụ xét ở trên, phương trình  $6x \equiv 3 \pmod{15}$  có  $d = \text{ƯCLN}(15, 3) = 3$ ,  $m' = 5$ , và  $x_0 = 3$  là nghiệm, các nghiệm tiếp theo là 8, 13.

**Định nghĩa 1.2.3.** Cho  $a, m$  là các số nguyên,  $m > 1$ . Nghiệm của phương trình đồng dư  $ax \equiv 1 \pmod{m}$  được gọi là nghịch đảo của  $a$  theo môđun  $m$ .

## 1.2.2 Hệ phương trình đồng dư đồng dư bậc nhất một ẩn

**Định nghĩa 1.2.4.** Hệ phương trình dạng

$$\left\{ \begin{array}{l} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots \\ x \equiv b_n \pmod{m_n} \end{array} \right.$$

gọi là hệ phương trình đồng dư bậc nhất một ẩn. Nếu một số nguyên  $x_0$  là nghiệm của hệ thì các số nguyên thuộc lớp đồng dư với  $x_0$  theo môđun  $m$  cũng là nghiệm của hệ, ( $m$  là BCNN của  $m_1, m_2, \dots, m_n$ ).

**Định lý 1.2.5** (Chinese Remainder Theorem). *Giả sử  $m = m_1.m_2\dots m_t$  và các số  $m_1, m_2, \dots, m_t$  đôi một nguyên tố cùng nhau. Khi đó hệ phương trình đồng dư*

$$\left\{ \begin{array}{l} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots \\ x \equiv b_n \pmod{m_n} \end{array} \right.$$

*có nghiệm duy nhất theo môđun  $m$ .*

*Chứng minh.* Đặt  $n_i = \frac{m}{m_i}$ , ta được  $(m_i, n_i) = 1$ . Khi đó, tồn tại số nguyên  $r_i, s_i$  sao cho  $r_i m_i + s_i n_i = 1$ . Gọi  $e_i = s_i n_i$  suy ra  $e_i \equiv 1 \pmod{m_i}$  và  $e_i \equiv 0 \pmod{m_j}, j \neq i$ . Tiếp tục đặt  $x_0 = \sum_{i=1}^n b_i e_i$  ta được  $x_0 \equiv b_i e_i \pmod{m_i}$  dẫn đến  $x_0 \equiv b_i \pmod{m_i}$ . Vậy  $x_0$  là một nghiệm của hệ. Hơn nữa, giả sử  $x_1$  là một nghiệm khác của hệ. Ta có  $x_1 - x_0 \equiv 0 \pmod{m_i}, (i = 1, 2, \dots, n)$  hay  $m_1, m_2, \dots, m_n$  chia hết cho  $x_1 - x_0$ . Điều này chứng tỏ  $x_1 \equiv x_0 \pmod{m}$ .  $\square$

## 1.2.3 Ứng dụng

**Ví dụ 1.2.3.1.** Tìm một số chia hết cho 11 nhưng khi chia cho 2, 3, 5, 7 đều dư 1.

**Lời giải:** Gọi số phải tìm là  $x$ . Khi đó, ta có hệ phương trình đồng dư sau

$$\begin{cases} x \equiv 0 \pmod{11} \\ x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} \\ x \equiv 1 \pmod{7} \end{cases}$$

Đặt  $m = 11 \cdot 2 \cdot 3 \cdot 5 \cdot 7 = 2310$ , ta có các bộ số  $n_i, m_i, r_i, s_i$  tương ứng như sau

$m_i$	$r_i$	$n_i$	$s_i$
2	578	1155	-1
3	257	770	-1
5	-277	462	3
7	-47	330	1
11	0	210	0

Bảng 1.6:

( $2r - 1155s = 1 \Rightarrow 2r = 1 - 1155s = 2 - 1144s - s - 1$ , vì  $r$  nguyên nên ta chọn  $s = 1, \dots$ , dẫn đến ta có cặp  $(r, s)$  như bảng (1.6).)

Áp dụng Định lý 1.2.5, ta có nghiệm của hệ trên là

$$x \equiv 1155(-1) - 770(-1) - 462(3) - 330(1) - 210 \cdot 0 \pmod{2310} \equiv -209 \pmod{2310}.$$

## 1.3 Các hàm số học

### 1.3.1 Phi hàm Ôle $\varphi(n)$

**Định nghĩa 1.3.1.** Cho  $n$  là số nguyên dương. Phi hàm Ôle  $\varphi(n)$  (Euler's function  $\varphi(n)$ ) là số các số nguyên dương không vượt quá  $n$  và nguyên tố cùng nhau với  $n$ .

Ví dụ với  $n = 4$ , ta có  $\varphi(4) = 3$ .

Phi hàm Ôle là hàm *nhân tính*, tức là với hai số  $m, n$  nguyên tố cùng nhau ta có  $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ . Với kết quả này, ta có mệnh đề sau đây cho ta cách tính  $\varphi(n)$ .

**Mệnh đề 1.3.2.** Giả sử số tự nhiên  $n$  được phân tích thành tích các thừa số nguyên tố  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ . Khi đó

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

*Chứng minh.* Xem [1, tr.60-61]. □

**Mệnh đề 1.3.3.** Cho  $n$  là một số nguyên dương. Khi đó,

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

trong đó tổng được lấy theo mọi ước của  $n$ .

*Chứng minh.* Xét  $n$  số hữu tỉ  $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$ . Rút gọn mỗi phân số sao cho mỗi phân số đều tối giản. Khi đó, tất cả các mẫu số của những phân số này đều là ước của  $n$ . Do đó, nếu  $d$  là ước của  $n$  thì có chính xác  $\varphi(d)$  phân số có mẫu số là  $d$ . Từ đó suy ra

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

**Định nghĩa 1.3.4.** Một tập gồm  $\varphi(n)$  số nguyên mà mỗi phân tử của tập đều nguyên tố cùng nhau với  $n$  và hai phân tử khác nhau của tập không đồng dư theo môđun  $n$  được gọi là một *hệ thặng dư thu gọn* theo môđun  $n$ .

**Định lý 1.3.5** (Euler's theorem). Cho  $m$  là số nguyên dương và  $a$  là số nguyên với  $(a, m) = 1$ . Khi đó, ta có  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

*Chứng minh.* Giả sử  $\{r_1, r_2, \dots, r_{\varphi(m)}\}$  là một hệ thặng dư thu gọn theo môđun  $m$ . Khi đó, ta có  $\{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$  cũng là một hệ thặng dư thu gọn theo môđun  $m$ . Do đó

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

tức là

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

Ngoài ra, ta có  $\text{ƯCLN}(r_1 r_2 \dots r_{\varphi(m)}, m) = 1$  nên suy ra  $a^{\varphi(m)} \equiv 1 \pmod{m}$ . □

**Hệ quả 1.3.6.** Cho  $a, m$  là các số nguyên, với  $m > 0$ ,  $\text{ƯCLN}(a, m) = 1$  và  $n, k$  là hai số tự nhiên thỏa  $n \equiv k \pmod{\varphi(m)}$ . Khi đó

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

*Chứng minh.* Ta có  $n \equiv k \pmod{\varphi(m)}$ .  $\Rightarrow n = k + t \cdot \varphi(m), t \in \mathbb{Z}$ . Do đó,

$$a^n = a^{k+t \cdot \varphi(m)} = a^k \cdot (a^{\varphi(m)})^t \equiv a^k \pmod{m}. \quad \square$$

**Định lý 1.3.7** (Fermat's little theorem). *Nếu  $p$  là số nguyên tố thì với mỗi số nguyên  $a$  ta đều có  $a^p \equiv a \pmod{p}$ .*

*Chứng minh.* Suy ra trực tiếp từ Định lý Euler.  $\square$

**Định lý 1.3.8** (Wilson's theorem). *Số nguyên  $n > 1$  là số nguyên tố nếu và chỉ nếu  $(n-1)! \equiv -1 \pmod{n}$ .*

*Chứng minh.* Giả sử  $n$  là số nguyên tố. Nếu  $n = 2, 3$  thì định lý đúng. Nếu  $n > 3$ , thì với mỗi số nguyên  $a$  luôn tồn tại duy nhất số nguyên  $b$  sao cho  $a \cdot b \equiv 1 \pmod{n}$ . Ta chứng minh  $2 \leq b \leq p-2$ . Thật vậy, theo Mệnh đề 1.2.2 về sự tồn tại nghiệm của phương trình đồng dư ta có  $1 \leq b \leq p-1$ . Ngoài ra, nếu  $b = 1$  thì  $a = 1$ . Nếu  $b = n-1$  thì  $a = n-1$ . Điều này mâu thuẫn. Do đó, các phần tử của tập  $A = \{2, 3, \dots, n-2\}$  chia thành  $\frac{n-3}{2}$  cặp  $(a, b)$  như trên. Từ đó suy ra

$$2 \cdot 3 \dots (n-2) \equiv 1 \pmod{p}$$

hay

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

Ngược lại, giả sử  $(n-1)! \equiv -1 \pmod{n}$ . Ta chứng minh  $n$  là số nguyên tố. Thật vậy, giả sử  $n$  là hợp số, tức là  $n = a \cdot b$  trong đó  $1 < a \leq b < n$ . Khi đó  $a | (n-1)!$ . Ngoài ra theo giả thiết, ta có  $(n-1)! \equiv -1 \pmod{n}$  tức là  $a | ((n-1)! + 1)$ . Từ đó suy ra  $a | 1$ . Điều này mâu thuẫn. Vậy  $n$  là số nguyên tố.  $\square$

**Mệnh đề 1.3.9.** *Gọi  $p^t$  là lũy thừa của số nguyên tố lẻ,  $m$  là số nguyên tố cùng nhau với cả  $p$  và  $p-1$  và  $a, b$  nguyên tố cùng nhau với  $p$ . Khi đó*

$$a^m \equiv b^m \pmod{p^t} \text{ nếu và chỉ nếu } a \equiv b \pmod{p^t}.$$

*Chứng minh.* Vì  $(a-b) | (a^m - b^m)$  nên từ giả thiết là  $a \equiv b \pmod{p^t}$  ta suy ra

$$a^m \equiv b^m \pmod{p^t}.$$

Ngược lại, giả sử  $a^m \equiv b^m \pmod{p^t}$  và  $a, b$  nguyên tố cùng nhau với  $p$  ta chứng minh  $a \equiv b \pmod{p^t}$ . Thật vậy, vì  $m$  nguyên tố cùng nhau với  $p$  và  $p-1$  nên



$\text{UCLN}(m, (p-1)p^{t-1}) = 1$ . Do đó, tồn tại số nguyên dương  $k$  sao cho  $mk \equiv 1 \pmod{\varphi(p^t)}$ . Từ đó suy ra

$$a \equiv a^{mk} \equiv (a^m)^k \equiv (b^m)^k \equiv b \pmod{p^t}. \quad \square$$

### 1.3.2 Hàm Möbius $\mu(n)$

**Định nghĩa 1.3.10.** Hàm số học Möbius  $\mu(n)$  là hàm cho bởi công thức

$$\mu(n) \begin{cases} 1 & \text{nếu } n = 1, \\ 0 & \text{nếu } n \text{ không chính phương,} \\ (-1)^k & \text{nếu } n \text{ là số chính phương và } k \text{ là số các ước nguyên tố của } n. \end{cases}$$

**Mệnh đề 1.3.11.** Nếu  $n > 1$  thì  $\sum_{d|n} \mu(d) = 0$ .

*Chứng minh.* Nếu  $n > 1$  thì  $n$  được phân tích thành tích các thừa số nguyên tố  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_l^{\alpha_l}$ . Khi đó,  $\sum_{d|n} \mu(d) = \sum_{\epsilon_1, \dots, \epsilon_l} \mu(p_1^{\epsilon_1} \dots p_l^{\epsilon_l})$  trong đó  $\epsilon_i$  là 0 hoặc 1. Do đó,

$$\sum_{d|n} \mu(d) = 1 - l + \binom{l}{2} - \binom{l}{3} + \dots + (-1)^l \binom{l}{l} = (1-1)^l = 0. \quad \square$$

### 1.3.3 Hàm tổng các ước dương $\sigma(n)$

**Định nghĩa 1.3.12.** Hàm số học  $\sigma(n)$  là hàm nhận giá trị tại  $n$  là tổng các ước dương của  $n$ . Ta có thể viết gọn định nghĩa trên như sau

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

Hàm  $\sigma(n)$  là hàm nhân tính. Nếu  $p$  là số nguyên tố thì  $\sigma(p) = p + 1$ .

Nếu  $\sigma(n) = 2n$  thì  $n$  được gọi là số *hoàn hảo* (perfect), ví dụ số 6, 28 là những số hoàn hảo.

**Định lý 1.3.13.** Nếu số tự nhiên  $n$  được phân tích thành tích các thừa số nguyên tố  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_l^{\alpha_l}$  thì

$$\sigma(n) = \prod_{i=1}^l \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

*Chứng minh.* Ta có các ước của  $p^{\alpha_i}$  là  $1, p, p^2, \dots, p^{\alpha_i}$ , nên

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

Từ đó suy ra,

$$\sigma(n) = \prod_{i=1}^l \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}. \quad \square$$

**Mệnh đề 1.3.14.** Nếu  $m$  là số hoàn hảo lẻ và  $m$  có phân tích cơ sở  $m = \prod p_i^{\alpha_i}$  thì

$$1) \text{ Tồn tại duy nhất một chỉ số } i \text{ sao cho } \begin{cases} \alpha_i \text{ lẻ} \\ p_i \equiv 1 \pmod{4} \end{cases}$$

2) Với mọi  $j \neq i, \alpha_j$  chẵn.

*Chứng minh.* Ta có  $\sigma(m) = 2m \Rightarrow \prod \left( \sum_{j=1}^{\alpha_i} p_i^j \right) = 2 \prod p_i^{\alpha_i}$ . Suy ra, tồn tại duy nhất một số  $i$  sao cho  $\alpha_i$  lẻ và do  $2|\sigma(m)$  nên ứng với  $\alpha_i$  lẻ ta có  $p_i \equiv 1 \pmod{4}$ .

Ngoài ra, với các chỉ số  $j \neq i$  ta xét  $\sigma(p_j^{\alpha_j}) = 1 + p_j + p_j^2 \dots + p_j^{\alpha_j}$ . Khi đó từ  $\sigma(p_j^{\alpha_j})$  là số lẻ nên  $\alpha_j$  phải chia hết cho 2.  $\square$

**Mệnh đề 1.3.15.**  $n$  là số hoàn hảo chẵn khi và chỉ khi  $n = 2^{m-1}(2^m - 1)$ , trong đó  $2^m - 1$  là số nguyên tố Mersene.

*Chứng minh.* Giả sử  $n = 2^s q, s \geq 1, q = 2t + 1$ , ta có

$$2^{s+1}q = \sigma(2^s q) = (2^{s+1} - 1)\sigma(q).$$

Suy ra  $q$  chia hết cho  $2^{s+1} - 1$ . Tiếp theo, ta đặt  $q = (2^{s+1} - 1)k$ . Khi đó, nếu  $k > 1$  ta có

$$2^{s+1}k(2^{s+1} - 1) = \sigma((2^{s+1} - 1)k)(2^{s+1} - 1).$$

Suy ra  $k2^{s+1} = \sigma((2^{s+1} - 1)k) > k(2^{s+1} - 1) \quad k, (\text{mâu thuẫn})$ . Vậy  $k = 1$  hay  $q = 2^{s+1} - 1$  và  $q$  là số nguyên tố Mersene.

Ngược lại, giả sử  $n = 2^{m-1}(2^m - 1)$  trong đó  $2^m - 1$  là số nguyên tố. Khi đó,

$$\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1) = 2^{m-1}2^m = 2n.$$

Vậy  $n$  là số hoàn hảo.  $\square$

### 1.3.4 Ứng dụng

**Ví dụ 1.3.4.1.** Tìm số dư trong các phép chia sau

a)  $123^{345}$  chia cho 14,

b)  $35^{150}$  chia cho 425, (Chọn HSGQG-Daklak-2011).

**Lời giải:** a) Ta có  $123 \equiv -3 \pmod{14}$ ,  $345 \equiv 3 \pmod{6}$  và  $\text{ƯCLN}(123, 14) = 1$ ,  $\varphi(14) = 6$  nên áp dụng Hệ quả 1.3.6 ta có

$$123^{345} \equiv 123^3 \equiv (-3)^3 \equiv 1 \pmod{14}.$$

Vậy số dư trong phép chia  $123^{345}$  chia cho 14 là 1.

b) Vì  $\text{ƯCLN}(35^{150}, 425) = 25$  nên

$$35^{150} \equiv r \pmod{425} \Leftrightarrow 5^{158} \cdot 7^{150} \equiv x \pmod{17}.$$

Ta có  $\varphi(17) = 16$ ,  $148 \equiv 6 \pmod{16}$ ,  $\text{ƯCLN}(148, 17) = 1$  nên suy ra

$$5^{148} \equiv 5^6 \equiv (5^3)^2 \equiv 6^2 \equiv 2 \pmod{17}.$$

Tương tự, ta cũng có

$$7^{150} \equiv 7^8 \equiv (7^2)^4 \equiv (-2)^4 \equiv -1 \pmod{17}.$$

Từ đó suy ra  $5^{158} \cdot 7^{150} \equiv -2 \equiv 15 \pmod{17}$  hay  $35^{150} \equiv 375 \pmod{425}$ .

Vậy số dư khi chia  $35^{150}$  cho 425 là 375.

**Ví dụ 1.3.4.2.** Chứng minh rằng nếu  $\text{ƯCLN}(a, 5) = 1$  thì  $a^{8n} + 3a^{4n} - 4$  chia hết cho 100.

**Lời giải:** Đặt  $A = a^{8n} + 3a^{4n} - 4 = (a^{4n} - 1)(a^{4n} + 4)$ . Theo công thức Euler ta có  $a^4 \equiv 1 \pmod{5}$  suy ra  $a^{4n} \equiv 1 \pmod{5}$ . Do đó  $a^{4n} + 4$  chia hết cho 5 và  $a^{4n} - 1$  cũng chia hết cho 5, hay  $A$  chia hết cho 25. Điều này dẫn đến bài toán trở thành chứng minh  $A$  chia hết cho 4. Thật vậy, ta viết trở lại

$$a^{8n} + 3a^{4n} - 4 = a^{4n}(a^{4n} + 3) - 4 = B$$

và ta xét hai trường hợp sau:

$a$  chẵn, tức là  $a = 2k$  ta có  $a^{4n} = 2^{4n} a^{4n} : 4$  suy ra  $B : 4$

••• lẻ, tức là  $a = 2k + 1$  ta có

$$\begin{aligned} a^{4n} - 3 &= (2k + 1)^{4n} - 3 \\ &= \sum_{k=0}^{4n} \binom{4n}{k} (2k)^{4n-k} \cdot 1^k - 3 : 4 \end{aligned}$$

Từ đó suy ra  $a^{8n} - 3a^{4n} - 4$  chia hết cho 100.

**Ví dụ 1.3.4.3.** Tìm số tự nhiên  $n$  sao cho hai số  $n - 1$  và  $\frac{n(n+1)}{2}$  là hai số số hoàn hảo.

**Lời giải:** Vì  $n$  là số tự nhiên nên  $n$  chia hết cho 2 hoặc không chia hết cho 2. Trước hết ta xét trường hợp  $n$  chia hết cho 2. Khi đó:

a) Với  $n = 4k$ , ta có  $n - 1 = 4k - 1 \equiv 3 \pmod{4}$ . Điều này mâu thuẫn ( $n \equiv 1 \pmod{4}$ ).

b) Với  $n = 4k + 2$  ta có  $\frac{n(n+1)}{2} = (2k + 1)(4k + 3)$  là số hoàn chỉnh lẻ và  $\frac{n(n+1)}{2} \equiv 3 \pmod{4}$  Điều này mâu thuẫn.

Trường hợp tiếp theo, với  $n$  không chia hết cho 2, ta có:

a)  $n = 3k + 3 \Rightarrow -1, \frac{n(n+1)}{2}$  đều là số hoàn hảo chẵn. Do đó  $n - 1 = 2^{p-1}(2^p - 1)$ ,  $\frac{n(n+1)}{2} = 2^{q-1}(2^q - 1)$ . Ngoài ra,  $(n - 1, \frac{n(n+1)}{2}) = 2$  nên  $q = 2$  hoặc  $p = 2$  suy ra  $n = 7$ .

b)  $n = 4k + 1$  suy ra  $\frac{n(n+1)}{2}$  là số hoàn hảo lẻ và  $n - 1$  là số hoàn hảo chẵn. Do đó,

$$n - 1 = 2^{p-1}(2^p - 1) \Rightarrow \frac{n(n + 1)}{2} = (2^{2p-2} - 2^{p-2} + 1)(2^{2p-1} - 2^{p-1} + 1).$$

Suy ra  $(2^{2p-2} - 2^{p-2} + 1)$ , hoặc  $(2^{2p-1} - 2^{p-1} + 1)$  là những số chính phương. Điều này mâu thuẫn.

Vậy chỉ có  $n = 7$  thỏa điều kiện.

## 1.4 Bài tập tự luyện

**Bài tập 1.4.1.** Chứng minh rằng với mọi số tự nhiên  $n \geq 1$  ta có

a)  $3^{2^{4n+1}} + 2$  chia hết cho 11,

b)  $2^{2^{10n+1}} + 19$  chia hết cho 23,

c)  $2^{2^{6n+2}} + 21$  chia hết cho 37.

**Bài tập 1.4.2.** Tìm số dư trong phép chia

a)  $6^{592}$  chia cho 11,

b)  $3^{40}$  chia cho 83,

c)  $51200^{2^{100}}$  chia cho 41.

**Bài tập 1.4.3.** Chứng minh rằng  $0,3.(1983^{1983} - 1917^{1917})$  là số nguyên.

**Bài tập 1.4.4.** Chứng minh rằng  $\sum_{k=1}^{26} k \cdot 10^{3k}$ ,  $k \in \mathbb{N}$  chia hết cho 13.

**Bài tập 1.4.5.** Tìm các số tự nhiên  $n$  để  $n^{n+1}(n+1)^n$  chia hết cho 5.

HD: Xét  $n = 5k + r$ ,  $r \in \{0, 1, 2, 3, 4\}$ .

**Bài tập 1.4.6.** Cho số nguyên  $a$ , chứng minh rằng  $a^2 - 1$  không có ước nguyên tố dạng  $4k - 3$ , từ đó suy ra các phương trình sau không có nghiệm nguyên dương.

a)  $4xy - x - y = z^2$ ,

b)  $x^2 - y^3 = 7$ .

**Bài tập 1.4.7.** Cho  $k, t$  là các số tự nhiên lớn hơn 1. Với giá trị nào của  $k$  thì với mọi số tự nhiên  $n$  ta luôn có

$$n^k \equiv n \pmod{10^t} \Rightarrow n^2 \equiv n \pmod{10^t}.$$

**Bài tập 1.4.8.** Cho  $n$  là số tự nhiên,  $p$  là số nguyên tố,  $n \geq p$ . Chứng minh rằng

$$\binom{n}{p} \equiv \left[ \frac{n}{p} \right] \pmod{p},$$

trong đó  $[x]$  là phần nguyên của  $x$ .

**Bài tập 1.4.9.** Giả sử  $p$  là số nguyên tố có dạng  $3n - 2$ . Chứng minh rằng không tồn tại số nguyên  $x$  sao cho  $x^2 - 3$  chia hết cho  $p$ .

# Chương 2

## MỘT SỐ BÀI TOÁN TRONG CÁC KỲ THI HỌC SINH GIỎI

### 2.1 Các bài toán trong các kỳ thi Olympic

**Bài toán 2.1.1** (CHINA, 2004). Hãy xác định ba chữ số tận cùng của số  $n$  với

$$n = 3 \times 7 \times 11 \times 15 \times \cdots \times 2011. \quad (2.1)$$

**Lời giải:** Dễ thấy rằng  $n$  là số lẻ. Gọi  $x$  là 3 chữ số tận cùng của  $n$ . Khi đó  $n \equiv x \pmod{1000}$ . Vì 15, 35, 55 là 3 số hạng trong tích (2.1) nên  $n$  chia hết cho 125, và  $1000 = 125 \cdot 8$  ta suy ra  $x$  cũng chia hết cho 125. Do đó,  $x$  chỉ có thể là những số 125, 375, 625, 875.

Từ đó suy ra,  $1000 \mid (n - x) \Leftrightarrow 8 \mid (n - x) \Rightarrow n \equiv x \pmod{8}$ . Tiếp theo lấy môđun 8 các số hạng của  $n$  ta được

$$\begin{aligned} n &= 3(4.1 + 3)(4.2 + 3)\dots(4.502 + 3) \equiv \underbrace{(3.7)(3.7)\dots(3.7)}_{251 \text{ cặp}} 3.3 \equiv \underbrace{5.5\dots5}_{251 \text{ cặp}}.3 \pmod{8} \\ &\equiv \underbrace{1.1\dots1}_{125 \text{ cặp}}.5.3 \equiv 7 \pmod{8} \end{aligned}$$

Hơn nữa, trong các số 125, 375, 625, 875 chỉ có duy nhất số 375 là đồng dư với 7 theo môđun 8 nên 375 là 3 chữ số tận cùng của  $n$ .

**Bài toán 2.1.2.** (IMO-1964). a) Tìm tất cả các số nguyên dương  $n$  sao cho  $2^n - 1$  chia hết cho 7.

b) Chứng minh rằng không có số tự nhiên  $n$  nào để  $2^n - 1$  chia hết cho 7.

**Lời giải:** Vì  $n$  là số nguyên dương nên ta xét các trường hợp của  $n$  như sau:

- Với  $n = 3k, k \in \mathbb{Z}$  ta có

$$2^n - 1 = (2^3)^k - 1 \equiv 1^k - 1 \equiv 0 \pmod{7}.$$

Do đó, với  $n$  là bội của 3 thỏa yêu cầu bài toán.

- Với  $n = 3k + r, k \in \mathbb{Z}, r = 1, 2$  ta có

$$2^n - 1 = 2^{3k} \cdot 2^r - 1 \equiv 2^r - 1 \equiv \begin{cases} 1 \pmod{7}, & r = 1 \\ 3 \pmod{7}, & r = 2 \end{cases}$$

Từ đó suy ra,  $n = 3k, k \in \mathbb{Z}$  ta luôn có  $7 | (2^n - 1)$ .

b) Theo trên ta có  $2^n \equiv 1, 2, 4 \pmod{7}$  với mọi số tự nhiên  $n$ . Do đó  $2^n + 1 \not\equiv 0 \pmod{7}$  với mọi số nguyên dương  $n$ .

**Bài toán 2.1.3.** (MOSCOW-1982). Tìm tất cả các số tự nhiên  $n$  sao cho  $n \cdot 2^n - 1$  chia hết cho 3.

**Hướng dẫn:** Xét số tự nhiên  $n$  dạng  $n = 6k + r, k \in \mathbb{Z}, 0 \leq r < 6$ .

**Bài toán 2.1.4.** (Olympic10-30/4-2008) Tìm tất cả các số nguyên dương  $m$  thỏa điều kiện

$$\forall a, b \in \mathbb{Z}, a^2 \equiv b^2 \pmod{m} \Rightarrow a \equiv \pm b \pmod{m} \quad (2.2)$$

**Lời giải:** Trước hết, nhận thấy rằng nếu  $m = 1$  hoặc  $m$  là số nguyên tố thì với mọi  $a, b \in \mathbb{Z}, a^2 \equiv b^2 \pmod{m} \Rightarrow a \equiv \pm b \pmod{m}$ . Thật vậy,

Nếu  $m = 1$  thì (2.2) đúng.

Xét  $m$  là số nguyên tố, với  $a, b \in \mathbb{Z}$  thỏa  $a^2 \equiv b^2 \pmod{m}$ . Ta có

$$(a - b)(a + b) = a^2 - b^2 \equiv 0 \pmod{m},$$

điều này suy ra  $a - b \equiv 0 \pmod{m}$  hoặc  $a + b \equiv 0 \pmod{m}$ . Do đó,  $a \equiv \pm b \pmod{m}$ .

Tiếp theo, ta xét với  $m \neq 1$  và  $m$  không nguyên tố, ta chứng minh số  $m$  cần tìm là  $m = 2p$  trong đó  $p$  là số nguyên tố lẻ. Thật vậy, giả sử (2.2) đúng. Vì  $m$  là số nguyên tố lẻ nên ta có  $m = x \cdot y, x, y \neq 1$ , đặt  $a = x + y, b = x - y$ . Khi đó ta có  $a^2 - b^2 = 4xy = 4m \equiv 0 \pmod{m}$  suy ra,  $a \equiv \pm b \pmod{m}$  hay  $2y = a - b \equiv 0 \pmod{m}$ , hoặc  $2x = a + b \equiv 0 \pmod{m}$ . Do đó  $2x \equiv 0 \pmod{m}$  hoặc  $2y \equiv 0 \pmod{m}$  với  $m = xy$ , suy ra,  $x = 2$  hoặc  $y = 2$  hay  $m = 2n, n \neq 1$ . Hơn nữa, nếu  $n$  là hợp số thì  $n = k \cdot t$  suy ra  $m = 2kt, k, t \neq 1$  theo trên ta suy ra  $t = 2$  hay  $m = 4k$  mâu thuẫn với (2.2), (Chọn  $a = 2k, b = 0$ ). Vậy  $n = p$  là số nguyên tố. Hơn nữa, nếu  $p = 2$  thì  $m = 4$  (2.2) không thỏa. Vậy  $p$  là số nguyên tố lẻ.

Ngược lại, giả sử  $m = 2p$  với  $p$  là số nguyên tố lẻ. Khi đó, theo giả thiết ta có  $a^2 - b^2 \cdot 2p$  suy ra  $(a - b)(a + b) \cdot 2$ , và  $(a - b)(a + b) \cdot p$ . Do đó  $a - b \cdot 2p, a + b \cdot 2p$  hay  $a \equiv \pm b \pmod{m}$ .

Vậy với  $m = 1, m = 2p$  hoặc  $m$  nguyên tố là những giá trị cần tìm.

## 2.2 Các bài toán trong kỳ thi học sinh giỏi Quốc gia

**Bài toán 2.2.1.** (HSGQG-1975) Tìm tất cả các số hạng của cấp số cộng  $-1, 18, 37, \dots$ , có các chữ số đều là chữ số 5.

**Lời giải:** Ta có số hạng đầu của cấp số cộng là  $a_1 = -1$  và công sai  $d = 19$  nên số hạng tổng quát là  $a_n = 19n - 20, n \geq 1$ . Do đó, bài toán trở thành tìm tất cả số  $n$  thỏa

$$19n - 20 = \underbrace{55\dots5}_{k \text{ số}} = 5 \cdot \frac{10^k - 1}{9}, k \geq 1$$

Điều này tương đương với  $5 \cdot 10^k \equiv -4 \pmod{19}$ , hay

$$5 \cdot 10^k \equiv 15 \pmod{19} \Leftrightarrow 10^k \equiv 3 \pmod{19}.$$

Ngoài ra, ta có

$$10^0 \equiv 1, 10^1 \equiv 10, 10^2 \equiv 5, 10^3 \equiv 12, 10^4 \equiv 6, 10^5 \equiv 3, 10^6 \equiv 11, \dots, 10^{18} \equiv 1.$$

Suy ra  $10^{18l+5} \equiv 3 \pmod{19}, l \geq 0$ , do đó suy ra số  $k$  cần tìm có dạng  $k = 18l + 5$ .

Ngược lại, Nếu  $k = 18l + 5$  ta có  $10^k \equiv 3 \pmod{19}$ . Do đó,  $5 \cdot 10^k \equiv -4 \pmod{19}$  tức là  $5 \cdot 10^k = 19s - 4 \Leftrightarrow 5 \cdot (10^k - 1) = 19s - 9$ , với mỗi số nguyên  $s$ . Từ đây, nhận thấy rằng vế trái của biểu thức trên chia hết cho 9, do đó vế phải của nó cũng chia hết cho 9, tức là  $s = 9r$ . Khi đó ta có

$$19r - 1 = 5 \cdot \frac{10^k - 1}{9} = \underbrace{55 \dots 5}_{k \text{ số}}.$$

Từ đó suy ra, các số hạng cần tìm của dãy có dạng  $\underbrace{55 \dots 5}_{18l \text{ số}}$  với mỗi số tự nhiên  $l$ .

**Bài toán 2.2.2.** (HSGQG-1987) Cho hai dãy  $(x_n), (y_n)$  xác định bởi

$$x_0 = 365, x_{n+1} = x_n(x_n^{1986} + 1) \quad 162\cancel{2}, \forall n \geq 0,$$



$$y_0 = 16, y_{n+1} = y_n(y_n^3 + 1) - 1952, \forall n \geq 0.$$

Chứng minh rằng  $|x_n - y_k| > 0, \forall k, n \geq 1$ .

**Lời giải:** Dễ thấy rằng  $(x_n), (y_n)$  là những số nguyên dương.

Ta có  $y_1 - y_0 = y_0^4 - 1952 = 63584 = 32 \cdot 1987$  do đó,  $y_1 \equiv y_0 \pmod{1987}$ . Ngoài ra, ta có  $y_2 - y_1 = y_1^4 - 1952 \equiv y_0^4 - 1952 \pmod{1987} \equiv 0 \pmod{1987}$  nên suy ra  $y_2 \equiv y_1 \pmod{1987}$ . Tương tự, ta chứng minh được

$$y_k \equiv y_0 \pmod{1987}, \forall k \geq 1.$$

Mặt khác, đối với dãy  $(x_n)$  ta cũng có

$$x_1 - x_0 = x_0^{1987} + 1622 = (365^{1987} - 365) \pmod{1987}.$$

Nhưng theo định lý Fermat nhỏ ta có  $365^{1987} \equiv 365 \pmod{1987}$  suy ra

$$x_1 \equiv x_0 \pmod{1987}$$

Hơn nữa,

$$x_2 - x_1 = x_1^{1987} + 1622 = x_0^{1987} - 1622 \equiv 0 \pmod{1987}.$$

Do đó,

$$x_2 \equiv x_0 \pmod{1987}.$$

Tương tự, ta chứng minh được

$$x_n \equiv x_0 \pmod{1987} \equiv 365 \pmod{1987}, \forall n \geq 1.$$

Từ đó suy ra, với mọi  $k, n \geq 1$  ta luôn có  $|y_k - x_n| > 0$ . (Vì 365 và 16 không đồng dư theo môđun 1987).

**Bài toán 2.2.3.** (HSGQG-1999B) Cho hai dãy  $(x_n, y_n)$  xác định bởi :

$$x_1 = 1, y_1 = 2, x_{n+1} = 22y_n - 15x_n, y_{n+1} = 17y_n - 12x_n, \forall n \geq 1.$$

1. Chứng minh rằng các số hạng của cả hai dãy  $(x_n), (y_n)$  đều khác không, và có vô hạn số hạng dương và vô hạn số hạng âm.
2. Hỏi số hạng thứ 1999<sup>1945</sup> của hai dãy có chia hết cho 7 không? Giải thích.

**Lời giải:** 1) Ta có,

$$\begin{aligned}x_{n-2} &= 22y_{n+1} - 15x_{n+1} = 22(17y_n - 12x_n) - 15x_n + 1 \\ &= 17(x_{n+1} + 15x_n) - 22 \cdot 12x_n - 15x_{n+1} \\ &= 2x_{n+1} - 9x_n, \forall n.\end{aligned}$$

Do đó,  $x_{n-2} \equiv 2x_{n+1} \pmod{3}$ . Hơn nữa ta có,  $x_1 = 1, x_2 = 29$  suy ra  $x_n$  không chia hết cho 3, hay  $x_n \neq 0, \forall n$ . Tiếp theo, ta chứng minh  $x_n$  có vô hạn số hạng dương và vô hạn số hạng âm. Thật vậy, từ trên ta có

$$x_{n-3} = 2x_{n+2} - 9x_{n+1} = -5x_{n+1} - 18x_n$$

hay

$$x_{n-3} - 5x_{n-1} - 18x_n = 0, \forall n. \quad (2.3)$$

Do đó, nếu giả sử rằng trong dãy  $x_n$  có hữu hạn các số hạng dương (hữu hạn các số hạng âm), ta gọi  $x_{n_j}$  là số hạng dương lớn nhất của dãy. Khi đó, với mọi  $n \geq n_j$  ta có  $x_n < 0$ , điều này mâu thuẫn với (2.3).

Tương tự, ta cũng chứng minh được dãy  $y_{n-2} = 2y_{n+1} - 9y_n, \forall n$ . thỏa yêu cầu bài toán.

2) Từ trên, ta có  $x_{n-4} = -28x_{n+1} - 45x_n$ , nên

$$x_n \equiv 0 \pmod{7} \Leftrightarrow x_{n+4} \equiv 0 \pmod{7} \Leftrightarrow x_{4k+n} \equiv 0 \pmod{7}.$$

Ngoài ra, từ  $1999^{1945} \equiv (-1)^{1945} \pmod{4} \equiv 3 \pmod{4}$  và  $x_3 = 49$ . nên ta suy ra

$$x_{1999^{1945}} \equiv 0 \pmod{7}.$$

Tương tự, ta cũng có

$$y_n \equiv 0 \pmod{7} \Leftrightarrow y_{4k+n} \equiv 0 \pmod{7}.$$

Nhưng  $y_3 = 26 \not\equiv 0 \pmod{7}$  nên  $y_{1999^{1945}} \not\equiv 0 \pmod{7}$ .

**Bài toán 2.2.4.** (HSGQG-2005A) Tìm tất cả các bộ 3 số tự nhiên  $(x, y, n)$  thỏa mãn hệ thức

$$\frac{x! - y!}{n!} = 3^n.$$

**Lời giải:** Từ hệ thức của đề, ta viết lại

$$x! \cdot y! = 3^n \cdot n! \quad (2.4)$$

Giả sử  $(x, y, n)$  là bộ các số tự nhiên thỏa mãn (2.4). Dễ dàng suy ra  $n \geq 1$ , và không mất tính tổng quát của bài toán, ta giả sử  $x \leq y$ . Khi đó xảy ra hai trường hợp:

1) **Trường hợp 1:**  $x \leq n$ . Phương trình (2.4) tương đương

$$1 \cdot \frac{y!}{x!} = 3^n \cdot \frac{n!}{x!}. \quad (2.5)$$

Suy ra  $1 \cdot \frac{y!}{x!} \equiv 0 \pmod{3}$ . Do đó  $x < y$  và  $y < x + 2$  ( Vì nếu  $y > x + 2$  thì  $\frac{y!}{x!} \equiv 0 \pmod{3}$ , mâu thuẫn). Vì vậy ta chỉ cần xét hai giá trị của  $y$  như sau:

1. Nếu  $y = x + 2$  thì từ (2.5) ta suy ra rằng

$$1 \cdot (x + 1)(x + 2) = 3^n \cdot \frac{n!}{x!} \quad (2.6)$$

Dễ thấy, vế trái của 2.6 không chia hết cho 2 nên vế phải cũng vậy, tức là  $n \leq x + 1$ . Nếu  $n = x$ , thì  $1 + (x + 1)(x + 2) = 3^x$  hay  $x^2 + 3x + 3 = 3^x$ , điều này suy ra,  $x \equiv 0 \pmod{3}$ . Do đó,  $x \geq 3$  và  $-3 = x^2 + 3x - 3^x \equiv 0 \pmod{9}$ . Điều này vô lý, chứng tỏ  $n \neq x$ . Với  $n = x + 1$ , từ 2.6 ta có,  $1 + (x + 1)(x + 2) = 3^n(x + 1)$  chứng tỏ  $x - 1$  là ước nguyên dương của 1. Do đó,  $x = 1$  dẫn đến  $y = 2, n = 1$ .

2. Nếu  $y = x + 1$  thì từ (2.5) ta có

$$x + 2 = 3^n \cdot \frac{n!}{x!} \quad (2.7)$$

Vì  $n \geq 1$  nên suy ra  $x \geq 1$ . Trong trường hợp này ta viết  $x + 2 \equiv 1 \pmod{(x + 1)}$ . Khi đó từ 2.7 ta suy ra  $n = x$  ( Nếu không, vế phải của (2.7) chia hết cho  $x + 1$  còn vế trái thì không). Do đó,

$$x + 2 = 3^x.$$

Dễ thấy rằng, nếu  $x \geq 2$  thì  $3^x > x + 2$ . suy ra có duy nhất giá trị  $x = 1$  thỏa mãn, trong trường hợp này ta chọn được bộ số tự nhiên thỏa yêu cầu của đề bài là  $(0, 2, 1)$  hoặc  $(1, 2, 1)$ .

2) **Trường hợp 2:**  $x > n$ . Khi đó (2.4) tương đương

$$\frac{x!}{n!} = \frac{y!}{n!} = 3^n. \quad (2.8)$$

Chú ý rằng,  $n-1, n-2$  không thể đồng thời là lũy thừa của 3 nên từ (2.8) ta suy ra  $x = n+1$ . Khi đó

$$(n-1) \frac{y!}{x!} = 3^n. \quad (2.9)$$

Vì từ,  $y \geq x, y \geq n+1$ . Ta đặt  $M = \frac{y!}{(n+1)!}$ . Khi đó, (2.9) có thể viết lại

$$(n+1)(M+1) = 3^n. \quad (2.10)$$

Rõ ràng, nếu  $y \geq 4$  thì  $M \equiv 0 \pmod{3}$  vì thế,  $M+1$  không thể là một lũy thừa của 3. Do đó từ (2.10) ta có

$$(n+1)(1 + \frac{y!}{(n+1)!}) = 3^n$$

hay  $(n+2)^3 - 1 = 3^n$ . Điều này suy ra  $n > 2$  và  $n+2 \equiv 1 \pmod{3}$ . Đặt  $n+2 = 3k+1, k \geq 2$ . Ta có

$$9k(3k^2 + 3k + 1) = 3^{3k-1}.$$

Suy ra  $3k^2 + 3k + 1$  là lũy thừa của 3, (điều này vô lý). Chứng tỏ  $y \neq n+3$ .

- Nếu  $y = n+2$  thì  $M = n+2$ , do đó ta có,  $(n+1)(n+3) = 3^n$ . Vì  $n-1, n-3$  không thể đồng thời là lũy thừa của 3 nên không tồn tại số  $n$  thỏa  $(n+1)(n+3) = 3^n$ . Do đó  $y \neq n+2$

- Với  $y = n+1$ , ta có  $A = 1$ . Do đó, từ (2.10) ta có  $2(n+1) = 3^n$ . Rõ ràng không tồn tại  $n$  thỏa hệ thức vừa nêu. Do vậy  $y \neq n+1$ .

Như vậy, nếu bộ số tự nhiên  $(x, y, n)$  với  $x \geq y$  thỏa yêu cầu bài toán thì không thể có  $x > n$ .

Tóm lại, nếu bộ số tự nhiên  $x, y, n$  thỏa (2.4) thì  $(x, y, n)$  là  $(0, 2, 1); (2, 0, 1); (1, 2, 1); (2, 1, 1)$ . Ngược lại, kiểm tra trực tiếp ta thấy bốn bộ số trên thỏa mãn.

Vậy bộ số thỏa yêu cầu là  $(0, 2, 1); (2, 0, 1); (1, 2, 1); (2, 1, 1)$ .

**Bài toán 2.2.5.** (HSGQG-2011) Cho dãy số nguyên  $(a_n)$  xác định bởi

$$a_0 = 1, a_1 = -1, a_n = 6a_{n-1} + 5a_{n-2}, \forall n \geq 2 \quad (2.11)$$

Chứng minh rằng  $a_{2012} - 2010$  chia hết cho 2011.

**Lời giải:** Xét dãy số nguyên  $(b_n)$  xác định bởi

$$b_0 = 1, b_1 = -1, b_n = 6b_{n-1} + 2016b_{n-2}, \forall n \geq 2.$$

Dễ dàng tìm được số hạng tổng quát của dãy này là  $b_n = \frac{49 \cdot (-42)^n + 41 \cdot 48^n}{90}, \forall n \geq 0$ .

Vì 2011 là số nguyên tố nên theo định lý Fermat nhỏ ta có:

$$(-42)^{2010} = 48^{2010} \equiv 1 \pmod{2011}.$$

Do đó,

$$90b_{2012} \equiv 49 \cdot (-42)^{2012} + 41 \cdot 48^{2012} \equiv 49(-42)^2 + 41 \cdot 48^2 \equiv 90b_2 \pmod{2011}.$$

Suy ra  $b_{2012} \equiv b_2 \pmod{2011}$ . Vì  $\text{ƯCLN}(90, 2011) = 1$ , mà  $b_2 = 6b_1 + 2016b_0$  nên  $b_{2012} \equiv 2010 \pmod{2011}$ . Ngoài ra, theo (2.11) ta có  $a_n \equiv b_n \pmod{2011}$ .

Từ đó suy ra

$$a_{2012} \equiv 2010 \pmod{2011}.$$

# TÀI LIỆU THAM KHẢO

## A. Tiếng Việt

1. Hà Huy Khoái (2004), *Chuyên đề bồi dưỡng học sinh giỏi toán phổ thông Số học*, Nhà xuất bản Giáo dục.
2. Hà Huy Khoái (2003), *Số học và thuật toán: Cơ sở lý thuyết và tính toán thực hành*, Nhà xuất bản Đại học Quốc Gia Hà Nội.
3. Nguyễn Tiến Quang (2007), *Bài tập số học*, Nhà xuất bản Giáo dục.

## B. Tiếng Anh

4. Cohen, H. (2007), *Number Theory Volume I: Tools and Diophantine Equations*, Springer Science+Business Media, LLC.
5. Ireland K., Rosen M. (1990) *A Classical Introduction to Modern Number Theory*, Springer-Verlag, Berlin.
6. Andreeescu, Titu (2006) *104 Number theory Problems From the Training of the USA IMO Team*, Birkhauser.
7. Chau, Le Hai (2010), *Selected Problems of the Vietnamese Mathematical Olympiad (1962-2009)*, Singapore.
8. Dušan Djukić (2009), *The IMO Compendium A Collection of Problems Suggested for the International Mathematical Olympiad: 1959-2009*, Springer.

## C. Một số tài liệu khác trên mạng Internet