

Chương II. Đồng dư

Bài 1. Đồng dư thức

A. Tóm tắt lý thuyết

1.1. Định nghĩa.

a) Cho số nguyên dương m . Hai số nguyên a và b được gọi là đồng dư với nhau theo môđun m nếu chúng có cùng số dư trong phép chia cho m , và kí hiệu bởi $a \equiv b \pmod{m}$.

b) Định nghĩa trên là tương đương với một trong hai phát biểu sau:

- $m \mid (a - b)$.

- Tồn tại số nguyên t sao cho $a = b + mt$.

1.2. Tính chất.

a) Có thể cộng hoặc trừ từng vế nhiều đồng dư thức theo cùng một môđun với nhau.

b) Có thể nhân từng vế nhiều đồng dư thức theo cùng một môđun với nhau.

B. Một số dạng bài toán thường gặp

Dạng 1. Chứng minh đồng dư thức

Phương pháp:

- Sử dụng định nghĩa và tính chất của đồng dư thức

Ví dụ 1. Chứng minh rằng nếu $ac \equiv bd \pmod{m}$, $a \equiv b \pmod{m}$ và $\text{ƯCLN}(a, m) = 1$ thì $c \equiv d \pmod{m}$.

Giải

Ta có:

$$ac - bd = (ac - ad) + (ad - bd) = a(c - d) + (a - b)d.$$

Do $ac - bd$ và $a - b$ chia hết cho m nên $a(c - d)$ chia hết cho m .

Do $\text{ƯCLN}(a, m) = 1$ nên $(c - d) \vdots m$, nghĩa là $c \equiv d \pmod{m}$.

Ví dụ 2. Chứng minh rằng với mọi $n \in \mathbb{N}$ ta có: $2^{2n} + 15n - 1 \equiv 0 \pmod{9}$.

Giải

- Với $n = 0$, điều phải chứng minh là hiển nhiên.

- Với mọi $n > 0$ ta có:

$$2^{2n} + 15n - 1 \equiv 2^{2n} - 1 - 3n \pmod{9}$$

và

$$2^{2n} - 1 - 3n = 4^n - 1 - 3n = 3 \left[(4^{n-1} + \dots + 4 + 1) - n \right].$$

Điều phải chứng minh tương đương với

$$4^{n-1} + \dots + 4 + 1 \equiv n \pmod{3}.$$

Điều này luôn luôn đúng vì $4 \equiv 1 \pmod{3}$.

Dạng 2. Chứng minh chia hết

Phương pháp:

- Sử dụng định nghĩa và tính chất của đồng dư thức

Ví dụ 1. Chứng minh rằng: $2222^{5555} + 5555^{2222}$ chia hết cho 7.

Giải

Trước hết ta có $2222 \equiv 3 \pmod{7}$ và $5555 \equiv 4 \pmod{7}$.

Do $3^2 = 9 \equiv 2 \pmod{7}$ nên $3^3 \equiv 6 \equiv -1 \pmod{7}$.

Từ đó theo môđun 7 ta có

$$2222^{5555} \equiv 3^{3 \cdot 1851} \cdot 3^2 \equiv (-1)^{1851} \cdot 2 \equiv -2 \pmod{7}. \quad (1)$$

Mặt khác, $4^2 \equiv 2 \pmod{7}$ nên $4^3 \equiv 1 \pmod{7}$. Do đó

$$5555^{2222} \equiv 4^{3 \cdot 740} \cdot 4^2 \equiv 1^{740} \cdot 2 \equiv 2 \pmod{7}. \quad (2)$$

Từ (1) và (2) suy ra điều phải chứng minh.

Ví dụ 2. Chứng minh rằng $2a + 11b$ chia hết cho 19 khi và chỉ khi $5a + 18b$ chia hết cho 19, ở đó $a, b \in \mathbb{Z}$.

Giải

$$\begin{aligned} 2a + 11b : 19 &\Leftrightarrow 2a + 11b \equiv 0 \pmod{19} \\ &\Leftrightarrow 5(2a + 11b) \equiv 0 \pmod{19} \text{ (do } \text{ƯCLN}(5, 19) = 1) \\ &\Leftrightarrow 10a + 55b \equiv 0 \pmod{19} \\ &\Leftrightarrow 10a + (19b + 36b) \equiv 0 \pmod{19} \\ &\Leftrightarrow 10a + 36b \equiv 0 \pmod{19} \\ &\Leftrightarrow 2(5a + 18b) \equiv 0 \pmod{19} \\ &\Leftrightarrow 5a + 18b \equiv 0 \pmod{19} \text{ (do } \text{ƯCLN}(2, 19) = 1) \\ &\Leftrightarrow 5a + 18b : 19 \end{aligned}$$

Dạng 3. Tìm số dư

Phương pháp:

- Sử dụng định nghĩa và tính chất của đồng dư thức

Ví dụ 1. Tìm phép dư trong các phép chia: $1532^5 - 1$ chia cho 9

Giải

Ta có:

$$1532 \equiv 2 \pmod{9}$$

nên

$$532^5 - 1 \equiv 2^5 - 1 \equiv 4 \pmod{9}.$$

Vậy số dư phải tìm là $r = 4$.

Ví dụ 2. Tìm số dư trong phép chia a cho 73, biết rằng: $a^{100} \equiv 2 \pmod{73}$ và $a^{101} \equiv 69 \pmod{73}$.

Giải

Gọi r là số dư trong phép chia a cho 73, $0 \leq r < 73$.

Khi đó $r^{100} \equiv 2 \pmod{73}$ và $r^{101} \equiv 69 \pmod{73}$.

Suy ra $69 \equiv r^{101} = r^{100} \cdot r \equiv 2r \pmod{73} \Rightarrow 2r = 73t + 69, t \in \mathbb{Z}$.

- Nếu $t = 0$ phương trình $2r = 69$ không có nghiệm nguyên.

- Nếu $t = 1$ thì $r = \frac{73 + 69}{2} = 71$.

- Nếu $t = 3$ thì $r = \frac{2 \cdot 73 + 69}{2} > 73$ (loại)

- Nếu $t = -1$ thì $r = \frac{-73 + 69}{2} < 0$.

Vậy $r = 71$.