Chuyên đề - ĐS 7: Phép toán đồng dư

Nguyễn Thành Phát

Lớp 9 (chuyên) - Trung tâm Thành Nhân

12/2022

Cho các số nguyên a, b, m trong đó $m \neq 0$. Ta nói a đồng dư với b theo modulo m và kí hiệu

$$a \equiv b \pmod{m} \iff a - b \,\vdots\, m.$$

Ví dụ

$$2022 \equiv 2 \pmod{4}$$
$$11^3 \equiv 1 \pmod{10}$$
$$a^n \equiv b^n \pmod{a-b}$$

Tính chất 1

Cho các số nguyên a, b, c, m trong đó $m \neq 0$.

- $a \equiv a \pmod{m}$,
- $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$,
- $a \equiv b \pmod{m} \implies a^k \equiv b^k \pmod{m}$ với mọi $k \in \mathbb{N}$,
- $\begin{cases} a \equiv b \pmod{m} \\ b \equiv c \pmod{m} \end{cases} \implies a \equiv c \pmod{m}$.

Tính chất 2

Cho các số nguyên a_1, a_2, b_1, b_2, m trong đó $m \neq 0$ thỏa mãn

$$a_1 \equiv a_2 \pmod m \quad \text{và} \quad b_1 \equiv b_2 \pmod m.$$

Khi đó

- $a_1 + a_2 \equiv b_1 + b_2 \pmod m$,
- $a_1 - a_2 \equiv b_1 - b_2 \pmod m$,
- $a_1 a_2 \equiv b_1 b_2 \pmod m$.

Định lí Fermat nhỏ

Cho số nguyên tố p và a nguyên dương, khi đó

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

Ngoài ra nếu $a \not\vdots\, p$ thì $a^{p-1} \equiv 1 \pmod p$.

Ví dụ

$3^{17} \equiv 3 \pmod{17}$

Ví dụ 1

Tìm số dư của phép chia 1532^5 cho 9.

Lời giải.

Ta có $1532 \equiv 2 \pmod 9$ nên

$$1532^5 \equiv 2^5 \pmod 9.$$

Mặt khác $2^5 = 32 \equiv 5 \pmod 9$ nên $1532^5 \equiv 5 \pmod 9$. $\square$

Ví dụ 2

Tìm chữ số tận cùng của số 3^{9^8} (chú ý $3^{9^8} \neq (3^9)^8 = 3^{72}$)

Ý tưởng: Tìm số k sao cho $3^k \equiv 1 \pmod{10}$.

Lời giải.

Ta có $3^4 = 81 \equiv 1 \pmod{10}$, do vậy cần tìm số dư của 9^8 cho 4.

$$9^8 \equiv 1^8 = 1 \pmod{4} \implies 9^8 = 4m + 1.$$

Có

$$\begin{aligned} 3^{9^8} = 3^{4m+1} &= 3 \cdot 3^{4m} \\ &\equiv 3 \cdot 1 \pmod{10} \\ &= 3 \pmod{10} \end{aligned}$$

Vậy 3^{9^8} có chữ số tận cùng là 3. $\square$

Ví dụ 3

Tìm số nguyên tố p biết rằng $2^{p-1} + 9 \vdots p$.

Lời giải.

Vì $2^{p-1} + 9$ lẻ nên p lẻ. Vì $2 \not\vdots\, p$ nên theo định lí Fermat nhỏ thì

$$2^{p-1} \equiv 1 \pmod{p} \implies 2^{p-1} + 9 \equiv 10 \pmod{p}.$$

Như vậy $10 \vdots p$, mà p lẻ nên $p = 5$ (thỏa mãn). □