

Chương IV. Phương trình đồng dư bậc nhất một ẩn

A. Tóm tắt lý thuyết

1. Phương trình đồng dư một ẩn

$$ax \equiv b \pmod{m} \quad (1)$$

có nghiệm khi và chỉ khi $d = \text{ƯCLN}(a, m)$ là ước của b . Khi ấy phương trình có d nghiệm. Trường hợp $d = 1$ ta có thể nêu hai cách giải (1).

Cách 1:

- Nếu a chia hết b thì $x \equiv \frac{b}{a} \pmod{m}$.
- Nếu a không chia hết b thì do $(a, m) = 1$ nên tồn tại $u, v \in \mathbb{Z}$ để:

$$au + mv = 1$$

$$\Rightarrow a(ub) + m(vb) = b$$

$$\Rightarrow a(ub) \equiv b \pmod{m}$$

Từ đó nghiệm của (1) là $x \equiv ub \pmod{m}$.

Cách 2:

Theo định lý Ôle ta có:

$$\text{ƯCLN}(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Từ đó $a[ba^{\varphi(m)-1}] \equiv b \pmod{m}$.

Suy ra nghiệm của (1) là $x \equiv ba^{\varphi(m)-1} \pmod{m}$.

Trường hợp $d \neq 1$, chia cả hai vế và môđun m cho d ta được:

$$a_1 x \equiv b_1 \pmod{m_1} \quad (2).$$

Phương trình (2) có nghiệm duy nhất $x_0 \pmod{m_1}$. Khi đó phương trình (1) có d nghiệm:

$$\overline{x_0, x_0 + m_1, \dots, x_0 + (d-1)m_1}$$

lấy theo môđun m .

2. Hệ phương trình đồng dư bậc nhất một ẩn

Hệ phương trình:

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots\dots\dots \\ x \equiv b_k \pmod{m_k} \end{cases} \quad (1)$$

được gọi là hệ phương trình đồng dư bậc nhất một ẩn. Nếu x_0 là một số nguyên nghiệm đúng hệ thì mọi số nguyên thuộc lớp $\overline{x_0} \pmod{m}$, trong đó m là BCNN của m_1, m_2, \dots, m_k , cũng nghiệm đúng hệ.

- Nếu hệ (1) có nghiệm thì nghiệm là duy nhất.

- Nếu các số m_1, m_2, \dots, m_k đôi một nguyên tố cùng nhau thì hệ (1) có nghiệm.

- Một cách tổng quát, điều kiện cần và đủ để hệ (1) có nghiệm là $d_{ij} = (m_i, m_j)$ chia hết $b_i - b_j$ ($1 \leq i, j \leq k$).

- Nếu $m > 1$ có dạng phân tích tiêu chuẩn

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

và $f(x) \in \mathbb{Z}[x]$ thì phương trình đồng dư

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

tương đương với hệ phương trình đồng dư

$$f(x) \equiv 0 \pmod{p_i^{a_i}}, \quad (i = 1, 2, \dots, k)$$

Cách thực hành để tìm nghiệm của hệ (1)

Trước hết ta hãy giải hệ hai phương trình nào đó của hệ (1). Với nghiệm tìm được cùng với một phương trình của hệ (1) ta được hệ hai phương trình. Giải hệ này và tiếp tục làm như trên sau $k - 1$ bước ta sẽ được nghiệm của hệ (1).

Đối với trường hợp m_1, m_2, \dots, m_k nguyên tố cùng nhau ta có thể giải hệ (1) như sau:

Đặt

$$m = m_1 m_2 \dots m_k = M_i m_i \quad (i = 1, 2, \dots, k).$$

Sau đó tìm các số nguyên N_i nghiệm đúng các phương trình

$$M_i N_i \equiv 1 \pmod{m_i}.$$

Khi đó $x_0 = M_1 N_1 b_1 + M_2 N_2 b_2 + \dots + M_k N_k b_k$ nghiệm đúng hệ đã cho.

B. Một số dạng bài toán thường gặp

Dạng 1. Giải phương trình đồng dư bậc nhất một ẩn

Ví dụ 1. Giải phương trình đồng dư sau: $3x \equiv 7 \pmod{8}$

Giải

Ta có:

$$\text{ƯCLN}(3, 8) = 1 \Rightarrow 3 \cdot 3 - 8 = 1 \Rightarrow 3(3 \cdot 7) - 8 \cdot 7 = 7 \Rightarrow x \equiv 21 \equiv 5 \pmod{8}.$$

Vậy nghiệm của phương trình đã cho là:

$$x \equiv 5 \pmod{8}.$$

Ví dụ 2. Giải phương trình đồng dư sau: $7x \equiv 6 \pmod{13}$.

Giải

Theo định lý Ô-le ta có:

$$\text{ƯCLN}(7, 13) = 1 \Rightarrow 7^{\varphi(13)} = 7^{12} \equiv 1 \pmod{13} \Rightarrow x \equiv 7^{11} \cdot 6 \equiv -6^{12} \equiv -(-3)^6 \equiv -27^2 \equiv -1 \pmod{13}$$

Vậy nghiệm của phương trình đã cho là:

$$x \equiv -1 \pmod{13}.$$

Ví dụ 3. Giải và biện luận phương trình đồng dư sau: $(a+1)x \equiv a^2 - 1 \pmod{m}$, trong đó a là một số nguyên cho trước.

Giải

- Nếu $\text{ƯCLN}(a+1, m) = 1$ thì $x \equiv a-1 \pmod{m}$

- Nếu $\text{ƯCLN}(a+1, m) = d \neq 1$ thì

$$\frac{a+1}{d} x \equiv \frac{a^2-1}{d} \pmod{\frac{m}{d}};$$

$$x \equiv a-1 \pmod{\frac{m}{d}}.$$

Suy ra phương trình đã cho có d nghiệm theo môđun m

$$x \equiv a-1, x \equiv a-1 + \frac{m}{d}, \dots, x \equiv a-1 + \frac{(d-1)m}{d} \pmod{m}.$$

Dạng 2. Giải phương trình Di-ô-phăng

Ví dụ 1. Giải phương trình Di-ô-phăng sau: $31x - 43y = 5$.

Giải

Ta xét phương trình đồng dư

$$-43y \equiv 5 \pmod{31},$$

hay

$$12y \equiv -5 \equiv -36 \pmod{31}.$$

Do $\text{UCLN}(12, 31) = 1$ nên

$$y \equiv -3 \pmod{31}.$$

Suy ra

$$\begin{cases} y = -3 + 31t \\ x = -4 + 43t \end{cases}, t \in \mathbb{Z}$$

là nghiệm nguyên của phương trình đã cho.

Ví dụ 2. Giải và biện luận theo số nguyên m phương trình sau: $12x + 8y = 3m + 2$.

Giải

Do $\text{UCLN}(12, 8) = 4$ nên phương trình có nghiệm khi và chỉ khi $3m + 2$ chia hết cho 4, hay

$$\begin{aligned} 3m &\equiv -2 \pmod{4} \\ \Rightarrow 3m &\equiv 6 \pmod{4} \\ \Rightarrow m &\equiv 2 \pmod{4}. \end{aligned}$$

nghĩa là $m = 4k + 2, k \in \mathbb{Z}$. Khi đó phương trình đã cho có dạng

$$3x + 2y = 3k + 2.$$

Phương trình có nghiệm riêng $x_0 = k, y_0 = 1$. Suy ra nghiệm tổng quát là

$$\begin{cases} x = k + 2t \\ y = 1 - 3t \end{cases}$$

Kết luận:

- Nếu $m \equiv 2 \pmod{4}$: phương trình đã cho có nghiệm nguyên là

$$\begin{cases} x = k + 2t \\ y = 1 - 3t \end{cases}, k \in \mathbb{Z}$$

- Nếu $m \not\equiv 2 \pmod{4}$: phương trình đã cho không có nghiệm nguyên.

Dạng 3. Chứng minh không chia hết

Ví dụ. Chứng minh rằng với mọi số nguyên a ta có $a^2 + 1$ không chia hết cho 7

Giải

Xét phương trình đồng dư

$$x^2 + 1 \equiv 0 \pmod{7}.$$

Cho x chạy qua hệ thặng dư đầy đủ môđun 7

$$\{0, \pm 1, \pm 2, \pm 3\}$$

thì $x^2 + 1$ chạy qua tập $\{1, 2, 5, 10\}$.

Do đó phương trình trên không có nghiệm, nghĩa là $a^2 + 1$ không chia hết cho 7 với mọi $a \in \mathbb{Z}$.

Dạng 4. Giải hệ phương trình đồng dư bậc nhất một ẩn

Ví dụ 1. Giải hệ phương trình đồng dư sau: $\begin{cases} 5x \equiv 4 \pmod{11} \\ 11x \equiv 8 \pmod{13} \end{cases}$

Giải

Ta có:

$$\begin{aligned} &\begin{cases} 5x \equiv 4 \pmod{11} \\ 11x \equiv 8 \pmod{13} \end{cases} \\ \Leftrightarrow &\begin{cases} 5x \equiv 15 \pmod{11} \\ -2x \equiv 8 \pmod{13} \end{cases} \end{aligned}$$

$$\Leftrightarrow \begin{cases} x \equiv 3 \pmod{11} \\ x \equiv -4 \pmod{13} \end{cases}$$

$$\Leftrightarrow \begin{cases} x = -4 + 13t \\ -4 + 13t \equiv 3 \pmod{11} \end{cases}$$

Phương trình cuối cùng tương đương với

$$2t \equiv 7 \equiv -4 \pmod{11} \Rightarrow t \equiv -2 \pmod{11}.$$

Vậy

$$x = -4 + 13(-2 + 11k) = -30 + 143k, k \in \mathbb{Z}.$$

hay

$$x \equiv -30 \pmod{143}$$

là nghiệm của hệ đã cho.

Ví dụ 2. Giải hệ phương trình đồng dư sau:
$$\begin{cases} x \equiv a \pmod{3} \\ x \equiv b \pmod{5} \\ x \equiv c \pmod{7} \end{cases}$$

Giải

Ta có $3 \cdot 5 \cdot 7 = 3 \cdot 35 = 5 \cdot 21 = 7 \cdot 15$.

Từ đó xét các phương trình

$$35x \equiv 1 \pmod{3} \Rightarrow x \equiv 2 \pmod{3}.$$

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

$$15x \equiv 1 \pmod{7} \Rightarrow x \equiv 1 \pmod{7}.$$

Suy ra nghiệm của hệ là

$$\begin{aligned} x &\equiv 2 \cdot 35a + 1 \cdot 21b + 1 \cdot 15c \pmod{105} \\ &\equiv 70a + 21b + 15c \pmod{105}. \end{aligned}$$

Dạng 5. Tìm số nguyên thoả mãn điều kiện cho trước

Ví dụ. Tìm số tự nhiên nhỏ nhất sao cho khi chia nó cho 3, 5, 7 và 11 ta được số dư tương ứng là 1; 2; 3 và 9.

Giải

Gọi số phải tìm là x ($x \in \mathbb{N}$) ta có hệ

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 9 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv -2 \pmod{11} \end{cases}$$

Xét các phương trình

$$5 \cdot 7 \cdot 11x \equiv 1 \pmod{3} \Rightarrow x \equiv 1 \pmod{3}$$

$$3 \cdot 7 \cdot 11x \equiv 1 \pmod{5} \Rightarrow x \equiv 1 \pmod{5}$$

$$3 \cdot 5 \cdot 11x \equiv 1 \pmod{7} \Rightarrow x \equiv 2 \pmod{7}$$

$$3 \cdot 5 \cdot 7x \equiv 1 \pmod{11} \Rightarrow x \equiv 2 \pmod{11}$$

Suy ra nghiệm của hệ là

$$x \equiv 385 \cdot 1 \cdot 1 + 231 \cdot 1 \cdot 2 + 165 \cdot 2 \cdot 3 + 105 \cdot 2 \cdot (-2) \equiv 262 \pmod{1155}.$$

Bởi vậy $x = 262$ là số cần tìm.