Chương

5 Phương trình đồng dư

Trần Trung Kiên (ISPECTORGADGET)
Nguyễn Đình Tùng (TUNGC3SP)

5.1 Phương trình đồng dư tuyến tính

Định nghĩa 5.1 *Phương trình đồng dư dạng* $ax \equiv b \pmod{m}$ *được gọi là phương trình đồng dư tuyến tính với* a, b, m *là các số đã biết.*
x_0 *là một nghiệm của phương trình khi và chỉ khi* $ax_0 \equiv b \pmod{m}$.
Nếu x_0 *là một nghiệm của phương trình thì các phần tử thuộc lớp* $\overline{x_0}$ *cũng là nghiệm.* △

Ví dụ 5.1. *Giải phương trình đồng dư sau:* $12x \equiv 7 \pmod{23}$
Lời giải. *Do* $(12; 23) = 1$ *nên phương trình luôn có nghiệm duy nhất. Ta tìm một số nguyên sao cho* $7 + 23k$ *chia hết cho 12. Chọn* $k = 7$ *suy ra* $12x \equiv 7.24 \pmod{23} \Rightarrow x \equiv 14 \pmod{23}$ ■

Ví dụ 5.2. *Giải phương trình* $5x \equiv 2 \pmod 7$ △

Lời giải. Vì $(5;2) = 1$ nên tồn tại số $k = 4$ sao cho $2 + 7k$ chia hết cho 5. Khi ấy $5x \equiv 2 + 6.7 \pmod 7$ ta được nghiệm $x \equiv \dfrac{30}{5} \equiv 6 \pmod 7$ hay $x = 6 + 7k$ ■

Ví dụ 5.3. *Giải phương trình:* $5x \equiv 4 \pmod{11}$ △

Lời giải. Ta có:

$$\begin{cases} 5x \equiv 4 \pmod{11} \\ 4 \equiv 4 \pmod{11} \end{cases}$$

Áp dụng tính chất bắc cầu ta có: $5x \equiv 4 \pmod{11} \Rightarrow 5x = 11t + 4$
Ta có thế lấy $t = 1; x = 3$. Từ đó phương trình có nghiệm duy nhất là $x \equiv 3 \pmod{11}$ ■

Nhận xét. Cách xác định nghiệm này là đơn giản nhưng chỉ dùng được trong trường hợp a là một số nhỏ hoặc dễ thấy ngay số k.

5.2 Phương trình đồng dư bậc cao

Ví dụ 5.4. *Giải phương trình* $2x^3 + 4 \equiv 0 \pmod 5$ △

Lời giải. Ta thấy $x = 2$ suy ra $2x^3 \equiv -4 \pmod 5$.
Nên $x = 2$ là nghiệm duy nhất của phương trình đã cho. ■

5.3 Hệ phương trình đồng dư bậc nhất một ẩn

Định nghĩa 5.2 *Hệ phương trình có dạng sau được gọi là hệ phương trình đồng dư bậc nhất một ẩn*

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ .... \\ x \equiv b_k \pmod{m_k} \end{cases}$$

Với $m_1; m_2; ...m_k$ *là những số nguyên lớn hơn 1 và* $b_1; b_2; ...; b_k$ *là những số nguyên tùy ý.* △

Nhận xét. • Trong trường hợp tổng quát, chúng ta có thể chứng minh được rằng: Điều kiện cần và đủ để hệ phương trình (5.2) có nghiệm là $UCLN(m_i; m_j)$ chia hết $b_i - b_j$ với $i \neq j (1 \leq i, j \leq k)$.

- Giả sử $m = p_1^{\alpha 1} p_2^{\alpha a_2} ... p_k^{\alpha k}$ là phân tích tiêu chuẩn của m. Khi ấy phương trình đồng dư $f(x) \equiv 0 \pmod{m}$ tương đương với hệ phương trình đồng dư $f(x) \equiv 0 \pmod{p_i^{\alpha 1}}, i = 1, 2, ..., k$. Từ đó suy ra rằng nếu $x \equiv b_1 \pmod{p_1^{\alpha 1}}$ là một nghiệm của phương trình $f(x) \equiv 0 \pmod{p_i}, i = 1, 2, ..., k$ thì nghiệm của hệ phương trình của hệ phương trình đồng dư

$$\begin{cases} x \equiv b_1 \left(\mathrm{mod} p_1^{\alpha_1}\right) \\ x \equiv b_2 \left(\mathrm{mod} p_2^{\alpha_2}\right) \\ \quad ... \\ x \equiv b_k \left(\mathrm{mod} p_k^{\alpha_k}\right) \end{cases}$$

cho ta nghiệm của phương trình $f(x) \equiv 0 (mod m)$.

Vậy trong • *Trường hợp tổng quát giải một phương trình đồng dư dẫn đến giải hệ trên. Với các module $m_1, m_2, ..., m_k$ đôi một nguyên tố cùng nhau.*

Phương pháp chung để giải:

- Trường hợp 1: hệ 2 phương trình

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$$

Với giả thiết $d = (m_1, m_2)$ chia hết cho $b_1 - b_2$. Trước tiên ta nhận xét rằng, mọi số $x = b_1 + m_1 t, t \in \mathbb{Z}$ là nghiệm của phương trình thứ nhất. Sau đó ta tìm cách xác định t sao cho x nghiệm đúng phương trình thứ hai, nghĩa là hệ hai phương trình trên tương đương với hệ phương trình

$$\begin{cases} x = b_1 + m_1 t \\ b_1 + m_1 t \equiv b_2 \pmod{m_2} \end{cases}$$

Vì giả thiết $d = (m_1, m_2)$ là ước $b_1 - b_2$ nên phương trình: $b_1 + m_1 t \equiv b_2 \pmod{m_2}$ tương đương với phương trình:

$$\frac{m_1}{d} t \equiv \frac{b_2 - b_1}{d} \pmod{\frac{m_2}{d}}$$

Nhưng $(\frac{m_1}{d}, \frac{m_2}{d}) = 1$ nên phương trình đồng dư này cho ta nghiệm $t \equiv t_0 \pmod{\frac{m_2}{d}}$, là tập hợp tất cả các số nguyên

$$t = t_0 + \frac{m_2}{d} u, u \in \mathbb{Z}$$

Thay biểu thức của t vào biểu thức tính x ta được tập hợp các giá trị của x nghiệm đúng cả hai phương trình đồng dư đang xét là:
$x = b_1 + m_1(t_0 + \frac{m_2}{d} u) = b_1 + m_1 t_0 + \frac{m_1 m_2}{d} u$, hay $x = x_0 + m_u$ với $x_0 = b_1 + m_1 t_0, m = BCNN(m_1, m_2)$.

Vậy $x \equiv x_0 \pmod{m}$ là nghiệm của hệ hai phương trình đồng dư đang xét.

- Trường hợp 2: Hệ gồm n phương trình. Đầu tiên giải hệ hai phương trình nào đó của hệ đã cho, rồi thay trong hệ hai phương trình đã giải bằng nghiệm tìm thấy, ta sẽ được một hệ gồm $n-1$ phương trình tương đương với với hệ đã cho. Tiếp tục như vậy sau $n-1$ bước ta sẽ được nghiệm cần tìm.

Ví dụ 5.5. *Giải hệ phương trình:* $\begin{cases} x \equiv 26 \pmod{36} \\ x \equiv 62 \pmod{60} \\ x \equiv 92 \pmod{150} \\ x \equiv 11 \pmod{231} \end{cases}$ △

Lời giải. Hệ hai phương trình:

$$\begin{cases} x \equiv 26 \pmod{36} \\ x \equiv 62 \pmod{60} \end{cases} \Leftrightarrow \begin{cases} x = 26 + 36t \\ 26 + 36t \equiv 62 \end{cases}, t \in \mathbb{Z}.$$

$$\begin{aligned} 26 + 36t &\equiv 62 \pmod{60} \\ \Leftrightarrow 36t &\equiv 36 \pmod{60} \\ \Leftrightarrow t &\equiv 1 \pmod{5} \end{aligned}$$

Vậy nghiệm của hệ là: $x \equiv 26 + 36.1 \pmod{180}$ hay $x \equiv 62 \pmod{180}$
Do đó hệ phương trình đã cho tương đương với hệ:

$$\begin{cases} x \equiv 62 \pmod{180} \\ x \equiv 92 \pmod{150} \\ x \equiv 11 \pmod{231} \end{cases}$$

Ví dụ 5.6. *Giải hệ phương trình*

$$\begin{cases} x \equiv 62 \pmod{180} \\ x \equiv 92 \pmod{150} \end{cases} \Leftrightarrow \begin{cases} x = 62 + 180t \\ 62 + 180t \equiv 92 \pmod{150} \end{cases}, t \in \mathbb{Z}.$$

Lời giải. Ta có:

$$\begin{aligned} & 62 + 180t \equiv 92 \pmod{1)50} \\ \Leftrightarrow & 180t \equiv 30 \pmod{150} \\ \Leftrightarrow & 6t \equiv 1 \pmod{5} \Leftrightarrow t \equiv 1 \pmod{5} \end{aligned}$$

Vậy nghiệm của hệ là:

$$x \equiv 62 + 180.(1+) \pmod{900} \Leftrightarrow x \equiv 242 \pmod{900}$$

Hệ đã cho tương đương với:

$$\begin{cases} x \equiv 242 \,(\mathrm{mod} 900) \\ x \equiv 11 \,(\mathrm{mod} 231) \end{cases}$$

Hệ này có nghiệm $x \equiv 242 \pmod{69300}$, và đây cũng là nghiệm của hệ đã cho cần tìm. ■

Ví dụ 5.7. *Tìm số nguyên dương nhỏ nhất thỏa tính chất: chia 7 dư 5, chia 11 dư 7 và chia 13 dư 3.* △

Lời giải. Ta có: $n_1 = 7; N_1 = 11.13 = 143; n_2 = 11; N_2 = 7.13 = 91; n_3 = 13; N_3 = 7.11 = 77$.
Ta có $N_1 b_1 \equiv 3b_1 \equiv 1 \pmod{7} \to b_1 = -2$. Tương tự $b_2 = 4; b_3 = -1$
Vậy $a = 143(-2)5 + (91)(4)(7) + (77)(-1)(3) = -1430 + 2548 - 231 = 887$ vậy các số cần tìm có dạng $b = 877 + 1001k$.
Vậy 877 là số cần tìm. ■

Ví dụ 5.8 (Chọn đội tuyển KHTN). *Xét hệ đồng dư gồm 3 phương trình:*

$$xy \equiv -1 \pmod{z} \quad (5.1)$$
$$yz \equiv 1 \pmod{x} \quad (5.2)$$
$$xz \equiv 1 \pmod{y} \quad (5.3)$$

Hãy tìm số bộ (x, y, z) nguyên dương phân biệt với 1 trong 3 số là 19. △

Lời giải. Từ ba phương trình, theo tính chất đồng dư ta lần lượt có $xy + 1 \vdots z$ và $yz - 1 \vdots x$ và $zx - 1 \vdots y$
Suy ra

$$(xy+1)(yz-1)(zx-1) \vdots xyz$$
$$\Rightarrow x^2y^2z^2 - x^2yz - xy^2z + xyz^2 + xy - yz - zx + 1 \vdots xyz$$
$$\Rightarrow xy - yz - zx + 1 \vdots xyz$$

Nhận thấy do x, y, z nguyên dương cho nên $xyz \geq 1$. Suy ra $xy - yz - zx + 1 \leq 2xyz$
Mặt khác $yz + zx - xy - 1 \leq 2xyz \Rightarrow -(yz + zx - xy - 1) \geq -2xyz$
Do đó ta có bất phương trình kép $-2xyz \leq xy - yz - zx + 1 \leq 2xyz$
Mà $xy-yz-zx+1 \vdots xyz \Rightarrow xy-yz-zx+1 = 2xyz, 1xyz, 0, -1xyz, -2xyz$
• Trường hợp 1: $xy - yz - zx + 1 = 2xyz \Rightarrow xy \equiv -1 \pmod{z}, yz \equiv 1 \pmod{x}, zx \equiv 1 \pmod{y}$
Cho nên ta chỉ cần tìm nghiệm của $xy - yz - zx + 1 = 2xyz$ là xong.
Vì x, y, z có một số bằng 19 nên ta thay lần lượt vào.
Nếu $x = 19 \Rightarrow 19y - yz - 19z + 1 = 38yz \Rightarrow 39yz - 19y + 19z = 1$
$\Rightarrow (39y + 19)(39z - 19) = -322$ Với $y = 19$ hoặc $z = 19$ thì tương tự.
• Trường hợp 2,3,4,5: $xy-yz-zx+1 = 1xyz, 0, -1xyz, -2xyz$ làm hoàn toàn tương tự, ta đẩy được về phương trình có dạng $au+bv = ab+uv+x$ với x là hằng số.
Đưa về $(a - v)(b - u) = x$ và giải kiểu phương trình ước số. Bài toán hoàn tất. ■

Nhận xét. Bài toán này mà không cho điều kiện một số bằng 19 thì không đưa được dạng $au + bv = ab + uv + x \leftrightarrow (a - v)(b - u) = x$ lúc đó suy ra vô hạn nghiệm.

5.4 Bậc của phương trình đồng dư

Định nghĩa 5.3 *Xét phương trình đồng dư* $f(x) = 0 \pmod m$ *với* $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n, a_i \in \mathbb{N}, i = 0, 1, ..., n$
Nếu a_0 *không đồng dư* $0 \pmod m$ *thì ta nói* n *là bậc của phương trình đồng dư.* △

Ví dụ 5.9. *Xác định bậc của phương trình* $15x^6 - 8x^4 + x^2 + 6x + 8 \equiv 0 \pmod 3$ △

Lời giải. Ta thấy $15 \equiv 0 \pmod 3$ nên bậc của phương trình không phải là bậc 6. Phương trình trên tương đương với $-8x^4 + x^2 + 2 \equiv 0 \pmod 3$
Vì $-8 \not\equiv 0 \pmod 3$ nên bậc phương trình là $n = 4$. ■

5.5 Bài tập

Bài 1. Giải các phương trình sau: a) $7x \equiv 6 \pmod{13}$ b) $(a + b)x \equiv a^2 + b^2 \pmod{ab}$ với $(a, b) = 1$ c) $17x \equiv 13 \pmod{11}$ d) $x^2 + x - 2 \equiv 1 \pmod 3$

Bài 2. Giải các hệ phương trình: a) $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 4 \pmod 4 \\ x \equiv 2 \pmod 7 \\ x \equiv 9 \pmod{11} \end{cases}$

b) $\begin{cases} 5x \equiv 1 \pmod{12} \\ 5x \equiv 2 \pmod 8 \\ 7x \equiv 3 \pmod{11} \end{cases}$

Bài 3. Tìm a nguyên để hệ phương trình sau có nghiệm

a) $\begin{cases} x \equiv 3 \pmod 3 \\ x \equiv 1 \pmod 4 \\ x \equiv 11 \pmod 7 \\ x \equiv a \pmod{11} \end{cases}$

b) $\begin{cases} 2x \equiv a \pmod 3 \\ 3x \equiv 4 \pmod{10} \end{cases}$

Bài 4. Một lớp gồm 40 học sinh đứng thành vòng tròn và quay mặt và trong vòng tròn để chơi bóng. Mỗi học sinh nhận được bóng phải ném qua mặt 6 bạn ở bên tay trái mình. Chứng minh rằng tất cả học sinh trong lớp đều nhận được bóng ném tới mình sau 40 lần ném bóng liên tiếp.

5.6 Ứng dụng định lý Euler để giải phương trình đồng dư

Qua bài viết này tôi xin giới thiệu một phương pháp để giải phương trình đồng dư bằng cách khai thác định lý Euler

Trước hết, xin nhắc lại vài kiến thức quen thuộc.

Định nghĩa 5.4 *Hàm Euler $\varphi(m)$ với số nguyên dương m là các số tự nhiên nhỏ hơn m là các số nguyên tố với m.* △

5.6.1 Định lý Euler.

Định lý 5.1 (Euler)– *Cho m là số nguyên dương và $(a, m) = 1$ thì $a^{\varphi(m)} \equiv 1 \pmod m$*

Hàm φ có tính chất sau:

- $\varphi(mn) = \varphi(m)\varphi(n)$ với $(m; n) = 1$
- Nếu p nguyên tố $\varphi(p) = p - 1; \varphi(p^n) = p^n - p^{n-1}(n > 1)$

- Nếu $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha^k}, p_i$ là các số nguyên tố thì

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right)$$

Bây giờ ta xét $m = a.b$ trong đó $(a; b) = 1$ thì có các kết quả sau

Định lý 5.2–

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab} \tag{5.4}$$

Chứng minh. Theo định lý Euler ta có: $a^{\varphi(b)} \equiv 1 \pmod{b}$ mà $b^{\varphi(a)} \equiv 0 \pmod{b}$
Nên $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{b}$.
Tương tự ta có:$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{a}$
Theo tính chất đồng dư thì : $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$ ■

Định lý 5.3– *Giả sử có $k(k \geq 2)$ số nguyên dương $m_1; m_2; \ldots m_k$ và chúng nguyên tố với nhau từng đôi một. Đặt $M = m_1.m_2 \ldots m_k = m_i t_i$ với $i = 1, 2, 3 \ldots, k$ ta có*

$$t_1^{\varphi(m_1)} + t_2^{\varphi(m_2)} + ... + t_k^{\varphi(m_k)} \equiv 1 \pmod{M} \tag{5.5}$$

Chứng minh. Từ giả thiết ta có $(m_i, t_i) = 1$ với mỗi $i = 1, 2, \ldots, k$ nên theo định lý Euler thì

$$t_1^{\varphi(m_1)} \equiv 1 \pmod{m_i} \tag{5.6}$$

Mặt khác với $i; j$ thuộc tập 1;2;...;k và $i \neq j$ thì t_j chia hết cho m_j nên $(t_j; m_i) = m_i$ hay

$$t_j^{\varphi(m_i)} \equiv 0 \pmod{m_i} \tag{5.7}$$

Đặt $S = t_1^{\varphi(m_1)} + t_2^{\varphi(m_2)} + ... + t_k^{\varphi(m_k)}$
Từ (5.6) và (5.7) có $S \equiv t_i^{\varphi m_i} \equiv 1 \pmod{m_i}$
Vì $m_1; m_2; \ldots m_k$ nguyên tố với nhau từng đôi một, nên theo tính chất đồng dư thức có
$S - 1 \equiv 0 \pmod{m_1.m_2...m_k} \Leftrightarrow S \equiv 1 \pmod{M}$, tức là có (5.5). ■

Khi mở rộng (5.4) theo hướng nâng lên lũy thừa các số hạng ta có kết quả sau.

Định lý 5.4– *Với $(a,b)=1$ và n,v là hai số nguyên dương nào đó thì*

$$a^{n\varphi(b)}+b^{v\varphi(a)}\equiv 1 \pmod{ab} \tag{5.8}$$

Chứng minh. Để tiện lập luận đặt $x=a^{\varphi(b)}$.
Theo định lý Euler thì $x=a^{\varphi(b)}\equiv 1 \pmod b \Leftrightarrow x-1\equiv 0 \pmod b$
Đồng thời $x=a^{\varphi(b)}\equiv 0 \pmod a$.
Từ đó có $x(x-1)\equiv 0 \pmod a$ và $x(x-1)\equiv 0 \pmod b$ nên $x(x-1)\equiv 0 \pmod{ab}$
Từ đó $x^3\equiv x^2.x\equiv x.x\equiv x^2\equiv x \pmod{ab}$ và cứ lập luận như thế có $x^n\equiv x \pmod{ab}$ hay $a^{n\varphi(b)}\equiv a^{\varphi(b)} \pmod{ab}$
Tương tự ta có: $b^{v\varphi(a)}\equiv b^{\varphi(a)} \pmod{ab}$ nên theo (5.4) có $a^{n\varphi(b)}+b^{v\varphi(a)}\equiv b^{\varphi(a)}+a^{\varphi(b)}\equiv 1 \pmod{ab}$.
(5.8) được chứng minh. ■

Hệ quả 5.1– *Với $(a;b)=1$ thì $a^{n\varphi(b)}+b^{n\varphi(a)}\equiv 1 \pmod{ab}$* □

Hệ quả này có thể chứng minh trực tiếp khi nâng hai vế của hệ thức (5.4) lên lũy thừa bậc n (sử dụng khi triển nhị thức Newton) và chú ý rằng $ab\equiv 0 \pmod{ab}$. Nên lưu ý rằng trong đồng dư thức thì $a\not\equiv 0 \pmod{ab}$!

Với kí hiệu như ở định lý 5.3 ta có $t_i.t_j\equiv 0 \pmod M$ với i khác j và mọi $i;j$ thuộc tập 1,2,...,k (nhưng $t\not\equiv 0 \pmod M$ với mọi $i=1,2,3,...k$)

Từ đó khi nâng hai vế của (5.5) lên lũy thừa bậc n ta có kết quả sau.

Định lý 5.5– *Với các giả thiết như định lý 5.3 ta có:*

$$t_1^{n\varphi(m_1)}+t_2^{n\varphi(m_2)}+...+t_k^{n\varphi(m_k)}\equiv 1 \pmod M \tag{5.9}$$

Với các kí hiệu như trên ta đặt $a=m_i$ và $b=t_i$ thì theo (5.4) có

$$m_i^{n\varphi(t_i)}+t_i^{n\varphi(m_i)}\equiv 1 \pmod M \tag{5.10}$$

Cộng từng vế của k đồng thức dạng (5.10) và sử dụng (5.5) ta được kết quả sau:

Định lý 5.6– *Với các giả thiết ở định lý 5.3 ta có:*

$$m_1^{\varphi(t_1)} + m_2^{\varphi(t_2)} + ... + m_k^{n\varphi(t_k)} \equiv k - 1 \pmod{M} \tag{5.11}$$

Khi nhân 2 vế của (??) với m_i ta được

$$m_1^{1+\varphi(t_i)} + m_i.t_i^{\varphi(m_i)} + \equiv m_i \pmod{M} \tag{5.12}$$

Do $m_i.t_i^{\varphi(m_i)} = m_i.t_i.t_i^{\varphi(m_i)-1} = M.t_i^{(m_i)-1}$ nên

$$m_i^{1+\varphi(t_1)} \equiv m_i \pmod{M}, i = \overline{1,k} \tag{5.13}$$

Cộng từng vế k đồng thức dạng (5.13) ta được kết quả sau:

Định lý 5.7– *Với các giả thiết như định lý 5.3 ta có:*

$$m_1^{1+\varphi(t_1)} + m_2^{2+\varphi(t_2)} + ... + m_k^{1+\varphi(t_k)} \equiv m_1 + m_2 + ... + m_k \pmod{M} \tag{5.14}$$

Khi nhân 2 vế của (5.10) với t_i ta được

$$m_1^{1+\varphi(t_1)} + m_2^{2+\varphi(t_2)} + ... + m_k^{1+\varphi(t_k)} \equiv m_1 + m_2 + ... + m_k \pmod{M} \tag{5.15}$$

$$\Rightarrow t_i^{1+\varphi(m_i)} \equiv t_i \pmod{M}, i = \overline{1,k} \tag{5.16}$$

Cộng từng vế của k đồng dư dạng (5.16) ta được kết quả sau

Định lý 5.8– *Với các giả thiết như định lý 5.3 ta có:*

$$t_1^{1+\varphi(m_1)} + t_2^{1+\varphi(m_2)} + ... + t_k^{1+\varphi(m_k)} \equiv t_1 + t_2 + ... + t_k \pmod{M} \tag{5.17}$$

Chú ý rằng $t_i.t_j \equiv 0 \pmod{M}$ nên khi nâng lên lũy thừa bậc n của tổng $t_1 + t_2 + ... + t_k$ ta có kết quả sau.

Định lý 5.9– *Với các giả thiết như định lý 5.3 ta có:*

$$t_1^n + t_2^n + ... + t_k^n \equiv (t_1 + t_2 + ... + t_k)^n \pmod{M} \tag{5.18}$$

Khả năng tìm ra các hệ thức đồng dư mới chưa phải đã hết mời bạn đọc nghiên cứu thêm. Để nắm rõ được những phần trên ta tìm hiểu qua một số ví dụ sau đây.

Ví dụ 5.10. *Tìm ít nhất bốn nghiệm của phương trình đồng dư:*

$$x^3 + y^7 \equiv 1 \pmod{30} \tag{5.19}$$

Lời giải. Do $30 = 5.6$ và $(6;5) = 1$ nên theo (5.4) có $5^{\varphi(6)} + 6^{\varphi(5)} \equiv 1 \pmod{30}$
vì $\varphi(6) = \varphi(2).\varphi(3) = 2$ và $\varphi(5) = 4; 6^2 \equiv 6 \pmod{30}$.
Tương tự ta có: $25^7 \equiv 25 \pmod{30}$ và $6^3 \equiv 6 \pmod{30}$ nên $6^3 + 25^7 \equiv 26 + 6 \equiv 1 \pmod{30}$
Nếu phân tích $30 = 3.10$ với $(3;10) = 1$ thì theo (5.4) có $3^{\varphi(10)} + 10^{\varphi(3)} \equiv 1 \pmod{30}$. Tính toán tương tự như trên ta có $3^4 + 10^2 \equiv 1 \pmod{30}$.
Vì $3^4 = 81 \equiv 21 \pmod{30}$ và $10^2 \equiv 10 \pmod{30}$ nên theo (5.8) có $(3^4)^3 + (10^2)^7 \equiv 1 \pmod{30}$ và $(3^4)^7 + (10^2)^3 \equiv 1 \pmod{30}$
Suy ra phương trình trên có ít nhất bốn nghiệm $(x;y)$ là $(25;6); (6;25); (21;10); (10;21)$. ■

Ví dụ 5.11. *Chứng minh rằng phương trình đồng dư sau có nghiệm $(x;y;z;t)$ khác $(0;0;0;0)$:*

$$x^4 + y^4 + z^4 + t^4 \equiv t^3 \pmod{60}.$$

Lời giải. $60 = 3.4.5$ và $(5;3) = 1; (5;4) = 1; (3;4) = 1$ nên đặt $m_1 = 3; m_2 = 4; m_3 = 5; t_1 = 15; t_2 = 1; t_3 = 20$ theo (5.18)

$$15^4 + 12^4 + 20^4 \equiv (15 + 20 + 12)^4 \equiv 1 \pmod{60}$$

Ví dụ 5.12. *Tìm ít nhất một nghiệm của phương trình đồng dư $x^{17} + y^{19} \equiv 1 \pmod{35}$* △

Lời giải. Ta có: $35 = 5.7$ mà $(5;7) = 1$ nên theo (5.4): $5^{\varphi^7} + 7^{\varphi^5} \equiv 1 \pmod{35}$)
Vì $\varphi(5) = 4; \varphi(7) = 6$ nên $5^4 + 7^6 \equiv 1 \pmod{35}$
Theo (5.8): $14^{17} + 30^{19} \equiv 14 + 30 \equiv 1 \pmod{35}$
Vậy phương trình đồng dư có ít nhất một nghiệm $(x;y) = (14;30)$ ■

5.7 Bài tập

Bài 1. Chứng minh rằng phương trình đồng dư sau có nghiệm $(x; y; z; t)$ khác $(0; 0; 0; 0)$:

a) $x^3 + y^3 + z^3 \equiv t^3 \pmod{210}$

b) $x^5 + y^5 + z^5 \equiv t^5 \pmod{1155}$

Bài 2. Tìm ít nhất một nghiệm của phương trình đồng dư sau:

$$x^{11} + y^{13} \equiv 1 \pmod{45}$$

Bài 3. Chứng tỏ rằng mỗi phương trình sau có nghiệm nguyên dương.

a) $2^x + 3^y + 5^z + 7^t \equiv 3 \pmod{210}$

b) $3^x + 5^y + 7^z \equiv 2 \pmod{105}$