Ta có:

$$\begin{cases} x \equiv r_1 \pmod{m_1} \\ x \equiv r_2 \pmod{m_2} \end{cases} \Leftrightarrow \begin{cases} (x-r) - k_1 d \vdots dd_1 \\ (x-r) - k_2 d \vdots dd_2 \end{cases}$$

$$\Leftrightarrow \begin{cases} \dfrac{x-r}{d} \equiv k_2 \pmod{d_1} \\ \dfrac{x-r}{d} \equiv k_2 \pmod{d_2} \end{cases} \quad (6.13)$$

Do $(d_1, d_2) = 1$ nên theo định lí Thặng dư Trung Hoa, tồn tại một số dương $\overline{x}$ sao cho $\overline{x} \equiv k_1 \pmod{d_1}$; $\overline{x} \equiv k_2 \pmod{d_2}$. Vì $\overline{x}$ và $\dfrac{x-r}{d}$ là hai nghiệm của phương trình $\begin{cases} x \equiv k_1 \pmod{d_1} \\ x \equiv k_2 \pmod{d_2} \end{cases}$ nên $\dfrac{x-r}{d} \equiv \overline{x} \pmod{d_1 d_2}$ hay $x \equiv \overline{x} d + r \pmod{dd_1 d_2}$.
Do $m = LCM(m_1, m_2) = dd_1 d_2$ nên theo định lí Thặng dư Trung Hoa, hệ có nghiệm duy nhất module m.
Giả sử định lí đúng đến $n-1$. Ta sẽ chứng minh định lí đúng đến n.
Đặt $m_1' = LCM(m_1, m_2, ..., m_{n-1})$; $m_2' = m_n$; $r_2' = r_n$. Vì $r_i \equiv r_j (\text{mod} GCD(m_i, m_j))$ với mọi $1 \le i < j \le n$ nên theo giả thiết quy nạp, hệ phương trình $\begin{cases} x \equiv r_i \pmod{m_i} \\ i = \overline{1, n-1} \end{cases}$ có duy nhất nghiệm $x \equiv r_1' \pmod{m_1'}$.
Mặt khác từ $r_i \equiv r_j (\text{mod } GCD(m_i, m_j))$ với mọi $1 \le i < j \le n$ suy ra $r_1' \equiv r_2' \pmod{GCD(m_1', m_2')}$.
Theo chứng minh trên cho trường hợp $n = 2$ ta có hệ phương trình $\begin{cases} x \equiv r_1' \pmod{m_1'} \\ x \equiv r_2' \pmod{m_2'} \end{cases}$ có nghiệm duy nhất theo module

$$m = LCM(m_1', m_2') = LCM(m_1, m_2, ..., m_n)$$

. Theo nguyên lí quy nạp ta có điều phải chứng minh. ■

Nhận xét. Đây chính là định lí Thặng dư Trung Hoa dạng mở rộng, nó hoàn toàn chứng minh dựa trên cơ sở định lí Thặng dư Trung Hoa. Trong bài viết này, ta sẽ không đi sâu vào tìm hiểu định lí dạng mở rộng mà chỉ đi sâu vào các ứng dụng của định lí Thặng dư Trung Hoa (dạng thường).

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 thể 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.* △

điều kiện quan hệ, chia hết,..., hay đếm số nghiệm của phương trình đồng dư. Việc sử dụng hợp lý các bộ và (trong định lý) cho ta rất nhiều kết quả thú vị và từ đó có thể đưa ra nhiều bài toán hay và khó.

Ví dụ 6.12. *Cho* $m_1, m_2, ..., m_n$ *là các số nguyên dương,* $r_1, r_2, ..., r_n$ *là các số nguyên bất kì. Chứng minh rằng điều kiện cần và đủ để hệ phương trình đồng dư*

$$\begin{aligned} x &\equiv r_1 \pmod{m_1} \\ x &\equiv r_2 \pmod{m_2} \\ &... \\ x &\equiv r_n \pmod{m_n} \end{aligned}$$

có nghiệm là $r_i \equiv r_j \pmod{GCD\,(m_i, m_j)};\ \forall 1 \le i < j \le n.$

Nếu x_0 *và* x_1 *là hai nghiệm thỏa mãn hệ phương trình trên thì* $x_0 \equiv x_1 \pmod m$ *với* $m = LCM(m_1, m_2, ..., m_n)$. *Tức là hệ phương trình đã cho có nghiệm duy nhất theo module* m. △

Lời giải. Trước hết ta giả sử hệ phương trình đã cho có nghiệm x_0. Đặt $GCD\,(m_i, m_j) = d$, ta có:

$$\begin{cases} x_o - r_i \equiv 0 \pmod{m_i} \\ x_o - r_j \equiv 0 \pmod{m_j} \end{cases}$$

Suy ra $r_i \equiv r_j \bmod (GCD\,(m_i, m_j))$. Do i, j tùy chọn nên $r_i \equiv r_j \pmod{GCD(m_i, m_j)}, \forall 1 \le i < j \le n$. Đây là điều kiện cần để hệ phương trình có nghiệm.
Ngược lại, ta sẽ chứng minh bằng quy nạp theo n rằng nếu điều kiện trên được thỏa mãn thì hệ phương trình luôn có nghiệm duy nhất theo module m với $m = LCM\,(m_1, m_2, ..., m_n)$.
Với trường hợp $n = 2$, đặt $GCD\,(m_1, m_2) = d \Rightarrow m_1 = dd_1;\ m_2 = dd_2$ với $GCD\,(d_1, d_2) = 1$.
Suy ra $r_i \equiv r_j \equiv r \pmod d$. Đặt $r_1 = r + k_1 d;\ r_2 = r + k_2 d$.

Số nguyên b thỏa mãn $b \equiv a_i \pmod{n_i}, \forall i = \overline{1,k}$ *khi và chỉ khi* $b \equiv a \pmod{n}$ *với* $n = n_1 n_2 ... n_k$. □

Lời giải. • Đặt $n = n_1 n_2 ... n_k$ và đặt $N_i = \dfrac{n}{n_i}$.

Do $(n_i, n_j) = 1, \forall i \neq j$ nên suy ra $(N_i, n_i) = 1 \ \forall i = \overline{1;k}$.

Do $(N_i, n_i) = 1, \forall i = \overline{1;k}$ nên với mỗi $i (1 \leq i \leq k)$ tồn tại b_i sao cho

$$N_i b_i \equiv 1 \pmod{n_i} \tag{6.10}$$

Như vậy ta có bộ $b_1, b_2, ..., b_k$. Do $N_j \equiv 0 \pmod{n_i}$ khi $i \neq j$, từ đó dĩ nhiên suy ra

$$N_j b_j \equiv 0 \pmod{n_i} \tag{6.11}$$

Đặt $a = \sum_{j=1}^{k} N_j b_j a_j$.

Với mỗi i $(1 \leq i \leq k)$ ta có

$$a = N_i b_i a_i + \sum_{j=1; j \neq i}^{k} N_j b_j a_j \tag{6.12}$$

Từ (6.10),(6.11),(6.12) suy ra $a \equiv a_i \pmod{n_i}, \forall i = \overline{1,k}$.

- Dễ thấy, vì $n_1, n_2, ..., n_k$ đôi một nguyên tố cùng nhau nên ta có kết luận sau: Số nguyên b thỏa mãn $b \equiv a_i \pmod{n_i}, \forall i = \overline{1,k}$ khi và chỉ khi $b \equiv a \pmod{n}$ với $n = n_1 n_2 ... n_k$. ■

Nhận xét. 1. Ngoài cách chứng minh trên, ta còn có thể sử dụng phép quy nạp để chứng minh định lí thặng dư Trung Hoa.

2. Định lí Thặng dư Trung Hoa khẳng định về sự tồn tại duy nhất của một lớp thặng dư các số nguyên thỏa mãn đồng thời nhiều đồng dư tuyến tính. Do đó có thể dùng định lí để giải quyết những bài toán về sự tồn tại và đếm các số nguyên thỏa mãn một hệ các

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

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

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:

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

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

- Trường hợp 3: q là số chẵn, p là số lẻ. Tương tự trường hợp 2, ta có:

$$\left[\begin{array}{l} \begin{cases} p = 2m + 1 (m \in \mathbb{P}) \\ q = 2 \end{cases} \\ \begin{cases} p = 3 \\ q = n + 1 (n \in \mathbb{P}, n \triangleq 2 \pmod 3) \end{cases} \end{array} \right. \quad (6.9)$$

Từ (6.8) và (6.9) ta có các cặp số p, q cần tìm. ■

Ví dụ 6.11. *Cho a, b, c là các số nguyên dương thỏa mãn $a \le b \le c$ và $(a, b, c) = 1$. Chứng minh rằng nếu $n > ac + b$ thì phương trình $n = ax + by + cz$ có nghiệm nguyên dương.* △

Lời giải. Gọi $(a, c) = d \Rightarrow (b, d) = 1 \Rightarrow A = \{bi\}_{i=1}^{d}$ là HĐĐ mod d

$\Rightarrow \exists\, y \in \{1, 2, ..., d\}$ sao cho $by \equiv n \pmod{d} \Leftrightarrow (n - by) \vdots d$.
Do $(a, c) = d \Rightarrow a = a_1 d$; $c = c_1 d$ $(a_1, c_1 \in Z^+)$; $(a_1, c_2) = 1) \Rightarrow B = \{a_1 j\}_{j=1}^{c_1}$ là HĐĐ mod c_1.

$\Rightarrow \exists x \in \{1, 2, ..., c_1\}$ sao cho $a_1 x \equiv \frac{n - by}{d} \pmod{c_1} \Rightarrow \exists z \in \mathbb{Z}$ sao cho $\frac{n - by}{d} = a_1 x + c_1 z$.
Mặt khác, ta có:

$$\frac{n - by}{d} > \frac{ac + b - by}{d} = (d - 1)\frac{ca_1 - b}{d} + a_1 c_1 \ge a_1 c_1 \ge a_1 x \Rightarrow z \in \mathbb{Z}^+$$

Từ đây suy ra $n - by = ax + cz \Leftrightarrow n = ax + by + cz$.
Vậy nếu $n > ac + b$ thì phương trình $n = ax + by + cz$ có nghiệm nguyên dương. ■

6.3 Định lí thặng dư Trung Hoa

6.3.1 Kiến thức cơ bản

Định lý 6.1– *Cho k số nguyên dương $n_1, n_2, ..., n_k$ đôi một nguên tố cùng nhau và k số nguyên bất kì $a_1, a_2, ..., a_k$. Khi đó tồn tại số nguyên a thỏa mãn $a \equiv a_i \pmod{n_i}, \forall i = \overline{1, k}$.*

Thật vậy, ngược lại, giả sử $\exists\ i,j \in \{1;2;...;p-1\}, i<j$ mà $r_i = r_j$

$$\Rightarrow \begin{cases} 1 \le j-i \le p-2 \\ (j-i)q \vdots p \end{cases} \Leftrightarrow \begin{cases} \le j-i \le p-2 \\ j-i \vdots p \end{cases} \text{ (vô lý)}$$

Ta có:

$$\frac{r_1}{p}+\frac{r_2}{p}+...+\frac{r_{p-1}}{p} = \frac{1+2+...+p-1}{p} = \frac{p-1}{2}$$

$$\Rightarrow S = \frac{(p-1)(q-1)}{2} \quad (6.7)$$

b. Từ (6.7) suy ra để S là số nguyên tố cần có $p,q>1$ và ít nhất một trong hai số p,q lẻ.

- Trường hợp 1: p,q cùng lẻ $\Rightarrow p,q \ge 3, p \ne q$ (do (p,q)=1), kết hợp với (6.7) $\Rightarrow S$ là số chẵn lớn hơn 2 $\Rightarrow S$ không phải là số nguyên tố.
- Trường hợp 2: p là số chẵn, q là số lẻ

$$S \in \mathbb{P} \Leftrightarrow \left[\begin{array}{l} \begin{cases} (p,q)=1 \\ p-1=1 \\ \dfrac{q-1}{2} \in \mathbb{P} \end{cases} \\ \begin{cases} (p,q)=1 \\ p-1 \in P \\ \dfrac{q-1}{2}=1 \end{cases} \end{array}\right.$$

$$\Leftrightarrow \left[\begin{array}{l} \begin{cases} p=2 \\ q=2h+1\ (h \in \mathbb{P}) \end{cases} \\ \begin{cases} q=3 \\ p=t+1\ (t \in P,\ t \triangleq 2 \pmod 3) \end{cases} \end{array}\right. \quad (6.8)$$

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:

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

Vậy nghiệm của hệ là:

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

Hệ đã cho tương đương với:

$$\begin{cases} x \equiv 242 \pmod{900} \\ x \equiv 11 \pmod{231} \end{cases}$$

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 với1 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. ■

Do $B = \{1,3,5,7,9\}$ là một HĐĐ mod 5 cho nên

$$B^* = \{1.2^n+1; 3.2^n+a; 5.2^n+a; 7.2^n+a; 9.2^n+a\}$$

cũng là HĐĐ mod 5 nên tồn tại duy nhất một số trong $B*$ chia hết cho 5.
$\Rightarrow$ Trong 5 số $a_1; a_2; a_3; a_4; a_5$ có duy nhất một số chia hết cho $5(n+1)$ mà số này gồm $n+1$ chữ số lẻ. Vậy mệnh đề đúng với $n+1$.
Theo nguyên lí quy nạp, mệnh đề đúng với mọi n nguyên dương. Vậy với mọi số nguyên dương n, luôn tồn tại một số tự nhiên gồm n chữ số đều lẻ và chia hết cho $5n$. ■

Trong một số dạng toán Số học khác

Ngoài các ứng dụng nêu trên, hệ thặng dư còn được dùng trong nhiều dạng toán số học khác, đơn biểu như trong các bài toán liên quan tới tính tổng, giải phương trình nghiệm nguyên (phương trình Diophant bậc nhất). Sau đây xin nêu ra một số ví dụ.

Ví dụ 6.10. *Với mỗi cặp số nguyên tố cùng nhau (p,q), đặt*

$$S = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + ... + \left[\frac{(p-1)q}{p}\right]$$

a. Chứng minh rằng: $S = \dfrac{(p-1)(q-1)}{2}$

b. Xác định giá trị của p,q để S là số nguyên tố △

Lời giải. *a.* Ta có $\left\{\dfrac{kq}{p}\right\} = \dfrac{r_k}{q}$, ở đây r_k là số dư trong phép chia q cho p $(0 \leq r_k \leq p-1)$.
Ta có:

$$S = \frac{q}{p} + \frac{2q}{p} + ... + \frac{(p-1)q}{p} - \left(\frac{r_1}{p} + \frac{r_2}{p} + ... + \frac{r_{p-1}}{p}\right)$$

Vì $(p,q) = 1 \Rightarrow r_k \neq 0 \ \forall \ k = 1,2,...,p-1$, từ đó ta thấy tập $A = \{r_1; r_2; ...; r_{p-1}\}$ chính là một hoán vị của tập $A = \{1; 2; ...; p-1\}$.

- Vì $\Phi(p) = p - 1 = |A|$ nên điều kiện (iii) thỏa mãn. ■

Vậy A là một HTG mod p.

b. Vì $B = \{1; 2; 3; ...; p-1\}$ là một HTG mod p. Mà A cũng là một HTG mod p (theo phần a.) nên ta có:

$$\begin{aligned} & \prod_{i=2}^{p} (i^3 - 1) \equiv (p-1)! \pmod{p} \\ \Leftrightarrow \quad & \prod_{i=2}^{p} (i^2 + i + 1) \equiv 1 \pmod{p} \\ \Leftrightarrow \quad & \prod_{i=1}^{p} (i^2 + i + 1) \equiv 3 \pmod{p} \end{aligned}$$

Nhận xét. Ta có thể mở rộng Ví dụ 6.7 như sau:

Ví dụ 6.8. *Cho p là số nguyên tố lẻ có dạng $mk + 2$ (m, k là các số nguyên dương, $m > 2$). Tìm số dư của phép chia*

$$T = \prod_{t=1}^{p} (t^{m-1} + t^{m-2} + ... + t + 1)$$

cho p. △

Ví dụ 6.9. *Chứng minh rằng với mọi số nguyên dương n, tồn tại số tự nhiên n gồm n chữ số đều lẻ và nó chia hết cho $5n$.* △

Lời giải. Xét số $x_n = \overline{a_1 a_2 ... a_n} = 5^n.a$ thỏa mãn (với $a_i \in \mathbb{Z}^+$ lẻ với mọi $i = 1, 2, ..., n$ và $a \in \mathbb{Z}^+$)
Ta sẽ chứng minh bài toán bằng phương pháp quy nạp toán học.

Với $n = 1 \Rightarrow \exists a_1 = 5 \vdots 5^1$. Vậy mệnh đề đúng với $n = 1$.
Giả sử mệnh đề đúng với n $\Leftrightarrow x_n = \overline{a_1 a_2 ... a_n} = 5^n.a$, cần chứng minh mệnh đề đúng với $n + 1$.
Xét 5 số sau đây:

$$\begin{aligned} a_1 &= \overline{1a_1 a_2 ... a_n} = 5^n (1.2^n + a) \\ a_2 &= \overline{3a_1 a_2 ... a_n} = 5^n (3.2^n + a) \\ a_3 &= \overline{5a_1 a_2 ... a_n} = 5^n (5.2^n + a) \\ a_4 &= \overline{7a_1 a_2 ... a_n} = 5^n (7.2^n + a) \\ a_5 &= \overline{9a_1 a_2 ... a_n} = 5^n (9.2^n + a) \end{aligned}$$

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 $f(x) = a_0 x^n + a_1 x^{n-1} + ... + a_n, a_i \in \mathbb{N}, i = 0, 1, ..., n$*
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 $\varphi(p) = p-1; \varphi(p^n) = p^n - p^{n-1}(n>1)$

Từ hai điều trên suy ra tồn tại chỉ số $j(1 \le j \le k)$ sao cho $a_k b_{k,j} \notin \{b_{k,1}, b_{k,2}, ..., b_{k,k}\}$.
Xét tập $\{b_{k,1}, b_{k,2}, ..., b_{k,k}, a_k b_{k,j}\}$.
Sau khi đánh số lại các phần tử ta thu được tập

$$\{b_{k+1,1}, b_{k+1,2}, ..., b_{k+1,k}, b_{k+1,k+1}\}$$

. Ta thấy tập này có $k+1$ phần tử thỏa mãn hai tính chất trên nên theo nguyên lí quy nạp, bổ đề được chứng minh. ■

Quay lại bài toán, áp dụng bổ đề 6.3, xét tập $\{b_{p-1,1}, b_{p-1,2}, ..., b_{p-1,p-1}\}$, ta thấy tập này là một HTG mod p nên nó chứa đúng một phần tử đồng dư với 2 mod p. Vì phần tử này khác 1 nên nó phải đồng dư với tích của một số a_k. Suy ra đpcm. ■

Trong tập con tập số nguyên dương, bài toán số học chia hết

Ví dụ 6.7. *Cho $p>3$ là số nguyên tố có dạng $3k+2$.*

a. Chứng minh rằng tập $A = \{2^3-1; 3^3-1; 4^3-1; ...; p^3-1\}$ là HTG mod p.

b. Chứng minh rằng $\prod_{i=1}^{p} (i^2+i+3) \equiv 3 (\mathrm{mod} p)$. △

Lời giải. *a.* Ta sẽ chứng minh tập A thỏa mãn 3 điều kiện đã nêu ở Định nghĩa 6.2.

- Hiển nhiên mỗi phần tử của A đều không chia hết cho p (thỏa mãn điều kiện (i)).
- Giả sử tồn tại $1 \le i < j \le p-1$ sao cho

$$\begin{aligned} & i^3 - 1 \equiv j^3 - 1 \pmod p \\ \Rightarrow\ & i^3 \equiv j^3 \pmod p \\ \Rightarrow\ & i^{3k} \equiv j^{3k} \pmod p \end{aligned}$$

Mặt khác, theo định lí Ferma, ta có: $i^{3k+1} \equiv j^{3k+1} \pmod p$
Từ đó suy ra $i \equiv j \pmod p \Rightarrow i = j$ (mâu thuẫn). Vậy A thỏa mãn điều kiện (ii).

Ta chứng minh đa thức $Q(x) = R(x)+p^m(1-e)$ là đa thức cần tìm.Thật vậy,

$$a_n = (p+1)^n + Q(n) = (p+1)^n + R(n) + p^m(1-e)$$
$$= u_n + p^m(1-e) \vdots p^m, \ \forall n = 1,2,3... \quad (6.6)$$

Mặt khác

$$a_1 = (p+1) + Q(1) = p+1+R(1)+p^m(1-e) = ep^m + p^m(1-e) \vdots p^m$$

Do đó p^m là ƯCLN của a_n với mọi $n = 1,2,3...$ ■

Ví dụ 6.6. *Cho $p \geq 3$ là một số nguyên tố và $a_1, a_2, ..., a_{p-2}$ là một dãy các số nguyên dương sao cho p không là ước số của a_k và ${a_k}^k - 1$ với mọi $k = 1,2,3,...,p-2$. Chứng minh rằng tồn tại một số phần tử trong dãy $a_1, a_2, ..., a_{p-2}$ có tích đồng dư với 2 module p.* △

Lời giải. Ta có bổ đề sau:

Bổ đề 6.3– *Với mỗi số nguyên $k = 1,2,...,p-1$ tồn tại một tập các số nguyên $\{b_{k,1}, b_{k,2}, ..., b_{k,k}\}$ thỏa mãn hai điều kiện sau:*

1. *Mỗi $b_{k,j}$ hoặc bằng 1, hoặc bằng tích của một số phần tử trong dãy $a_1, a_2, ..., a_{p-2}$,*
2. *$b_{k,i} \triangleq b_{k,j} \pmod p$ với $1 \leq i \neq j \leq k$.* □

Chứng minh. Với k=2 chọn $b_{21} = 1; b_{22} = a_1 \triangleq 1 \pmod p$ (do $a_1^1 - 1$ không chia hết cho p).
Giả sử với $2 \leq k \leq p-2$ ta đã chọn được tập $\{b_{k,1}, b_{k,2}, ..., b_{k,k}\}$ thỏa mãn hai tính chất trên.
Vì $a_k \not\vdots p$ nên hai phần tử khác nhau bất kì trong tập

$$\{a_k b_{k,1}, a_k b_{k,2}, ..., a_k b_{k,k}\}$$

là phân biệt theo mod p.

$$a_k^k \triangleq 1 (\mathrm{mod} p) \Rightarrow (a_k b_{k,1})(a_k b_{k,2})...(a_k b_{k,k}) \triangleq b_{k,1} b_{k,2} ... b_{k,k} \pmod p$$

- 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–

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

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 $m_1; m_2; ... m_k$ và chúng nguyên tố với nhau từng đôi một. Đặt $M = m_1.m_2...m_k = m_i t_i$ với $i = 1,2,3...,k$ ta có*

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

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

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

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

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

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 $m_1; m_2; ... m_k$ 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:

Lời giải. Ta có bổ đề sau:

BỔ ĐỀ 6.2– *$\forall k\in\mathbb{N}, k<m$ thì tồn tại $b_k\in\mathbb{Z}$ sao cho $b_kp^m+p^k\vdots k!$* □

Chứng minh. Giả sử $k!=p^{\alpha_k}M_k$ với $(M_k;p)=1$.
Khi e chạy trong tập $\{0;1;...;M_k-1\}$ thì các số $\{ep^{m-k}\}$ lập thành một HĐD modM_k, thành thử tồn tại $b_k\in\mathbb{Z}$ sao cho $b_kp^{m-k}\equiv -1 \pmod{M_k}$

$$\Leftrightarrow \quad (b_kp^{m-k}+1)\vdots M_k$$
$$\Leftrightarrow \quad (b_kp^m+p^k)\vdots p^k.M_k$$

Mặt khác

$$\alpha_k\sum_{i=1}^{\infty}\left[\frac{k}{p^i}\right]<\sum_{i=1}^{\infty}\frac{k}{p^i}<k$$

Vậy $(b_kp^m+p^k)\vdots p^{\alpha_k}.M_k=k!$. Bổ đề được chứng minh. ■

Trở về bài toán.
Đặt $f_i(x)=\dfrac{x(x-1)...(x-i+1)}{i!}$ thì $f_i(n)=\begin{cases}C_n^i\ (\text{nếu } n\geq i)\\ 0\ (\text{nếu } n<i)\end{cases}$.
Đặt $R(x)=-\sum\limits_{i=0}^{m-1}f_i(x)(b_ip^m+p^i)$ thì theo Bổ đề 6.2, $R(x)$ là đa thức có hệ số nguyên.
Ta có:

$$u_n=(p+1)^n+R(n)=\sum_{i=0}^{n}C_n^ip^i-\sum_{i=1}^{m-1}f_i(n)p^i-p^m\sum_{i=0}^{m-1}f_i(n)b_i$$

$$\equiv \sum_{i=0}^{\infty}f_i(n)p^i-\sum_{i=1}^{m-1}f_i(n)p^i \pmod{p^m}$$
$$\equiv \sum_{i=0}^{\infty}f_i(n)p^i\equiv 0 \pmod{p^m}\ \forall n=1,2,3...$$

Đặc biệt $u_1=(p+1)+R(1)=ep^m$

Theo định lí Ferma:

$$x^{p-1} = x^{3k+1} \equiv 1 \pmod p$$
$$y^{p-1} = y^{3k+1} \equiv 1 \pmod p$$
$$\Rightarrow x^{3k+1} \equiv y^{3k+1} \pmod p \quad (6.5)$$

Mà theo giả thiết, $x^3 \equiv y^3 \bmod p \Rightarrow x^{3k} \equiv y^{3k} \pmod p$.

Từ đó suy ra $x \equiv y \pmod p$. Vậy bổ đề được chứng minh. ■

Trở lại bài toán, ta sẽ chứng minh $P(n_1) \equiv P(n_2) \pmod{191}$ với $n_1; n_2 \in \mathbb{Z}$ thì $n_1 \equiv n_2 \pmod{191}$.
Thật vậy, vì

$$27P(n_1) = (3n_1 - 11)^3 - 11.191.n_1 + 11^3 + 27m$$
$$27P(n_2) = (3n_2 - 11)^3 - 11.191.n_2 + 11^3 + 27m$$

nên

$$\begin{aligned}
& P(n_1) \equiv P(n_2) && \pmod{191} \\
\Leftrightarrow & 27P(n_1) \equiv 27P(n_2) && \pmod{191} \\
\Leftrightarrow & (3n_1 - 11)^3 \equiv (3n_2 - 11)^3 && \pmod{191} \\
\Leftrightarrow & 3n_1 - 11 \equiv 3n_2 - 11 && \pmod{191} \text{(suy ra từ bổ đề)} \\
\Leftrightarrow & n_1 \equiv n_2 && \pmod{191}
\end{aligned}$$

Với mọi $n_1, n_2 \in A = \{1; 2; 3; ...; 1991\}$ (A là một HĐĐ mod 191), $n_1 \neq n_2$ ta có $P(n_1) \triangleq P(n_2) \pmod{191}$
$\Rightarrow A^* = \{P(1); P(2); ...; P(191)\}$ là một HĐĐ mod 191.
Từ đó suy ra $\exists n \in A = \{1; 2; 3; ...; 191\}$ sao cho

$$P(n) \equiv 191 \pmod{191} \Leftrightarrow P(n) \vdots 191$$

. ■

Ví dụ 6.5. *Cho p là một số nguyên tố. Chứng minh rằng với mọi số m nguyên không âm bất kì, luôn tồn tại một đa thức $Q(x)$ có hệ số nguyên sao cho p^m là ước chung lớn nhất của các số $a_n = (p+1)^n + Q(n)$; $n = 1, 2, 3...$* △

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

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

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

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

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

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

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:*

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

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

$$m_1^{1+\varphi(t_1)} + m_2^{2+\varphi(t_2)} + ... + m_k^{1+\varphi(t_k)} \equiv m_1 + m_2 + ... + m_k \pmod M \quad (5.15)$$
$$\Rightarrow t_i^{1+\varphi(m_i)} \equiv t_i \pmod M, i = \overline{1,k} \quad (5.16)$$

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:*

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

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:*

$$t_1^n + t_2^n + ... + t_k^n \equiv (t_1 + t_2 + ... + t_k)^n \pmod M \quad (5.18)$$

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 $(x;y) = (14;30)$ ■

Kết hợp với (6.4) suy ra

$$(u - v)((p-1).p.u^{p-1} - 1) \equiv 0 \pmod{p^p} \Rightarrow u - v \equiv 0 \pmod{p^p}$$

Điều này mâu thuẫn với giả sử $u \triangleq v \pmod{p^p}$. Vậy nhận xét được chứng minh.

- Từ nhận xét trên suy ra $H = \{Q(1); Q(2); ...; Q(p^p)\}$ là một HĐĐ mod p^p. Từ đó suy ra trong tập số $\{1; 2; ...; p^p\}$ gồm p^p số thì tồn tại duy nhất một số a sao cho $Q(a) \equiv 0 \pmod{p^p}$ hay $Q(a) \vdots p^p$.
- Ta xét dãy số hạng $a_k = a + k.p^p$ với $k = 0, 1, 2...$, dễ thấy rằng:

  $$Q(a^p) \equiv Q(a) \equiv 0 \pmod{p^p}.$$

  Nghĩa là tồn tại vô hạn số a_k $(k = 0, 1, 2, ...)$ thỏa mãn $Q(a_k) \vdots p^p$. ■

Ví dụ 6.4. *Cho đa thức $P(x) = x^3 - 11x^2 - 87x + m$. Chứng minh rằng với mọi số nguyên m, tồn tại số nguyên n sao cho $P(n)$ chia hết cho 191.* △

Lời giải. Ý tưởng cũng tương tự Ví dụ 6.3, ta sẽ sử dụng HĐĐ. Trước hết ta đưa ra bổ đề sau:

Bổ đề 6.1– *Cho p là số nguyên tố, $p \equiv 2 \pmod 3$. Khi đó,với mọi số nguyên x, y mà $x^3 \equiv y^3 \pmod p \Rightarrow x \equiv y \pmod p$* □

Chứng minh. Thật vậy:

- Nếu $x \equiv 0 \pmod p \Rightarrow y^3 \equiv 0 \pmod p \Rightarrow y \equiv 0 \pmod p \Leftrightarrow x \equiv y (\mathrm{mod} p)$
- Nếu x, y cùng không chia hết cho p, do $p \equiv 2(\mathrm{mod} 3) \Rightarrow p = 3k + 2 (k \in \mathbb{Z})$.

Tương tự, tồn tại duy nhất $a \in A$ để $x \equiv na \pmod{m}$.

Từ đó suy ra $x \equiv na + mb \pmod{n}$ và $x \equiv na + mb \pmod{m}$. Từ đó kết hợp với $(m, n) = 1$ suy ra $x \equiv na + mb \pmod{mn}$. ■

Nhận xét. Từ đây, ta có thể suy ra công thức tính hàm Ơle $\Phi(n)$.

6.2.2 Ứng dụng

Trong các bài toán về đa thức, dãy số

Ví dụ 6.3. *[THTT, số 340] Cho p là số nguyên tố lẻ và đa thức $Q(x) = (p-1)x^p - x - 1$. Chứng minh rằng tồn tại vô hạn số nguyên dương a sao cho $Q(a)$ chia hết cho p^p.* △

Lời giải. Thay cho việc chứng minh tồn tại vô hạn số nguyên dương a sao cho $Q(a)$ chia hết cho p^p, ta sẽ chứng minh tập

$$H = \{Q(1); Q(2); ...; Q(p^p)\}$$

là một HĐĐ mod p^p.
Ta có nhận xét sau: trong tập số $\{1; 2; ...; p^p\}$ gồm p^p số, giả sử có hai số u, v khác nhau thì $Q(u) \triangleq Q(v) \pmod{p^p}$.
Ta chứng minh điều này bằng phản chứng. Giả sử có $Q(u) \equiv Q(v) \pmod{p^p}$

$$\Leftrightarrow (p-1)u^p - u - 1 \equiv (p-1)v^p - v - 1 \pmod{p^p}$$

$$\Leftrightarrow (p-1)(u^p - v^p) - (u - v) \equiv 0 \pmod{p} \tag{6.3}$$

Theo định lí Ferma nhỏ thì $u^p \equiv u \pmod{p}$ và $v^p \equiv vp \pmod{p}$ với p là số nguyên tố nên $u^p - v^p \equiv u - v \pmod{p}$.
Từ (6.3) suy ra

$$(p-2)(u-v) \equiv 0 \pmod{p} \Rightarrow u \equiv v \pmod{p} \tag{6.4}$$

Cũng từ (6.3) ta có:

$$(u-v)((p-1)(u^{p-1} + u^{p-2}v + ... + uv^{p-2} + v^{p-1}) - 1) \equiv 0 \pmod{p^p}$$

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

Ví dụ 6.2. *Cho hai số nguyên dương m, n với $(m;n) = 1$. Giả sử $A = \{a_1, a_2, ..., a_h\}; B = \{b_1, b_2, ..., b_k\}$ tương ứng là các hệ thu gọn mod m và mod n. Xét tập hợp $C = \{a_i n + b_j m\}; 1 \le i \le h; 1 \le j \le k$.. Chứng minh rằng C là một hệ thu gọn HTG mod mn.* △

Lời giải. + Ta chứng minh $(a_i n + b_j m, mn) = 1 \ \forall i = \overline{1,h};\ j = \overline{1,k}$ (điều kiện (i)).

Giả sử tồn tại i, j và số nguyên tố p là ước chung của $a_i n + b_j m$ và mn.

Ta có $a_i n + b_j m \vdots p$ và $mn \vdots p$.

Do $mn \vdots p$ mà $(m, n) = 1$ nên có thể giả sử $n \vdots p$, suy ra

$$a_i n \vdots p \Rightarrow b_j m \vdots p \Rightarrow b_j \vdots p$$

Vậy p là ước nguyên tố chung của n và b_j. Điều này mâu thuẫn với giả thiết. Nên điều giả sử là sai. Vậy $(a_i n + b_j m, mn) = 1 \ \forall i = \overline{1,h};\ j = \overline{1,k}$.

+ Chứng minh điều kiện (ii).

Giả sử tồn tại $a \in A;\ b \in B$ sao cho $an + bm \equiv a'n + b'm \pmod{mn}$

$$\Rightarrow an \equiv a'n \pmod{m} \Rightarrow a \equiv a' \pmod{m} \text{ (do } (m,n) = 1)$$

(điều này mâu thuẫn).

Vậy $an + bm \triangleq a'n + b'm \pmod{mn}$.

+ Chứng minh điều kiện (iii').

Giả sử $(x, mn) = 1 \Rightarrow (x, m) = 1; (x, n) = 1$.

Vì $(m, n) = 1$ nên tập $B = \{mb_1, mb_2, ..., mb_k\}$ là một HTG mod n.

Vậy tồn tại duy nhất $b \in B$ để $x \equiv mb \pmod{n}$.

b. Xét khi n lẻ: Lúc này chưa thể kết luận gì về tính chất của hệ $A+B$.

Thật vậy, ta xét $n=3$; $A=\{1;2;3\}$; $B=\{4;5;6\}$.

Khi đó $A+B=\{5;7;9\}$ là một HĐĐ mod 3.

Nhưng, xét hệ $\overline{A}=\{1;2;3\}$, $\overline{B}=\{5;4;6\}$.

Khi đó $\overline{A}+\overline{B}=\{6;6;9\}$ không phải là một HĐĐ mod 3. ■

Hệ thặng dư thu gọn

Định nghĩa 6.2 *Cho tập $B=\{b_1;b_2;...;b_k\}$ là một tập hợp gồm k số nguyên và $(b_i;n)=1$ với mọi $i=1;2;...;k$.*
Giả sử: $b_i=q_in+r_i$ với $1\le r_i<n$. Khi đó dễ thấy $(r_i;n)=1$.
Nếu tập $\{r_1;r_2;...;r_n\}$ bằng tập K gồm tất cả các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n thì B được gọi là hệ thặng dư thu gọn mod n, gọi tắt là HTG $\pmod n$. △

Nhận xét. Ta có thể rút ra hai nhận xét:

▷ Dễ thấy tập $B=\{b_1;b_2;...;b_k\}$ gồm k số nguyên lập thành một HTG khi và chỉ khi

i. $(b_i;n)=1$

ii. $b_i\neq b_j \pmod n$ với $1\le i\neq j\le k$

iii. $|B|=\Phi(n)$

Điều kiện (iii) tương đương với (iii'): với mọi $x\in\mathbb{Z}; (x;n)=1$ tồn tại duy nhất $b_i\in B$ sao cho $x\equiv b_i \pmod n$.

▷ Từ định nghĩa ta suy ra: cho tập $B=\{b_1;b_2;...;b_k\}$ là HTG mod n và $c\in\mathbb{Z}; (c;n)=1$ thì tập $cB=\{cb_1;cb_2;...;cb_n\}$ cũng là HTG mod n.

Chương

6 Hệ thặng dư và định lý Thặng dư Trung Hoa

Nguyễn Đình Tùng (tungc3sp)

Bài viết này trình bày về Hệ thặng dư và định lý Thặng dư Trung Hoa. Một số kí hiệu sử dụng được phác họa trong Phần 6.1. Phần 6.2 giới thiệu đến bạn đọc một số kiến thức cơ bản về Hệ thặng dư đầy đủ và Hệ thặng dư thu gọn kèm theo bài tập ứng dụng. Định lý Thặng dư Trung Hoa kèm ứng dụng của nó giúp giải quyết một số dạng toán được trình bày trong Phần 6.3. Phần 6.4 kết thúc bài viết bao gồm một số bài tập đề nghị kèm gợi ý hoặc đáp số.

6.1 Một số kí hiệu sử dụng trong bài viết

- $[x,y]$: bội chung nhỏ nhất của hai số nguyên dương x,y (nếu không nói gì thêm).
- (x,y) : ước chung lớn nhất của hai số nguyên x,y.
- $x\triangleq y \pmod p$: x không đồng dư với y theo module p.
- HĐĐ: hệ thặng dư đầy đủ.

- HTG: hệ thặng dư thu gọn.
- $\mathbb{P}$: tập các số nguyên tố.
- $\Phi(n)$: hàm Ơle của n.
- $|A|$: số phần tử của tập A.
- $\{x\}$: phần lẻ của số thực x, được xác định như sau: $\{x\} = x - [x]$, trong đó $[x]$ là phần nguyên của số thực x (là số nguyên lớn nhất không vượt quá x).
- $\prod_{i=1}^{n} p_i = p_1 p_2 ... p_n$

6.2 Hệ thặng dư

6.2.1 Kiến thức cơ bản

Hệ thặng dư đầy đủ

Định nghĩa 6.1 *Cho tập $A = \{a_1; a_2; ...; a_n\}$. Giả sử r_i, $0 \le r_i \le n-1$ là số dư khi chia $a_i$cho n. Nếu tập số dư $\{r_1; r_2; ...; r_n\}$ trùng với tập $\{0; 1; 2; ...; n-1\}$ thì ta nói A là một hệ thặng dư đầy đủ (gọi tắt là HĐD)* mod n.

Nhận xét. Từ định nghĩa, dễ thấy:

▷ Nếu $A = \{a_1; a_2; ...; a_n\}$ lập thành HĐD $\pmod n$ nếu và chỉ nếu: $i \ne j \Rightarrow a_i \ne a_j \pmod n$.

▷ Nếu $A = \{a_1; a_2; ...; a_n\}$ là HĐD $\pmod n$ thì từ định nghĩa dễ dàng suy ra:

– Với mọi $m \in \mathbb{Z}$, tồn tại duy nhất $a_i \in A$ sao cho $a_i \equiv m \pmod n$.

– Với mọi $a \in \mathbb{Z}$, tập $a + A = \{a + a_1; a + a_2; ...; a + a_n\}$ là một HĐD $\pmod n$.

– Với mọi $c \in \mathbb{Z}$ và $(c; n) = 1$; tập $cA = \{ca_1; ca_2; ...; ca_n\}$ là một HĐD $\pmod n$.

Chú ý: tập $A^* = \{0; 1; 2; 3; ...; n-1\}$ là một HĐD $\pmod n$ không âm nhỏ nhất. Số phần tử của tập A là $|A| = n$.

Ví dụ 6.1. *Cho hai HĐD $\pmod n$: $A = \{a_1; a_2; ...; a_n\}$ và $B = \{b_1; b_2; ...; b_n\}$.*

a. Chứng minh rằng: Nếu n chẵn thì tập $A + B = \{a_1 + b_1; a_2 + b_2; ...; a_n + b_n\}$ không hợp thành HĐD $\pmod n$

b. Kết luận ở câu a. sẽ thế nào nếu n là số lẻ △

Lời giải. *a.* Ta có một điều kiện cần sau đây đối với HĐD $\pmod n$, khi n chẵn. Giả sử $C = \{c_1; c_2; ...; c_n\}$ là một HĐD $\pmod n$. Khi đó theo định nghĩa ta có:

$$c_1 + c_2 + ... + c_n \equiv (1 + 2 + ... + (n-1)) \equiv \frac{n(n+1)}{2} \pmod n$$

Do n chẵn nên $n = 2k$, suy ra:

$$\frac{n(n+1)}{2} = k(2k+1) \not\vdots n \Rightarrow k(2k+1) \triangleq 0 \pmod n$$

$$\Rightarrow c_1 + c_2 + ... + c_n \triangleq 0 \pmod n \quad (6.1)$$

Ta có:

$$\begin{aligned} A + B &= \{a_1 + b_1; a_2 + b_2; ...; a_n + b_n\} \\ &\equiv \{(a_1 + a_2 + ... + a_n) + (b_1 + b_2 + ... + b_n)\} \pmod n \\ &\equiv \left\{\frac{n(n+1)}{2} + \frac{n(n+1)}{2}\right\} \pmod n \\ &\equiv [n(n+1)] \pmod n \end{aligned}$$

$$\Rightarrow A + B \equiv 0 \pmod n \quad (6.2)$$

(Ở đây ta cũng sử dụng giả thiết A và B là hai HĐD mod n).

Từ (6.1) và (6.2) ta suy ra đpcm.