03

Chuyên đề Số học

HỆ THẶNG DƯ

Residue System

Ban chuyên môn Toán
The Gifted Battlefield

Mục lục

Định lý Fermat nhỏ
Định lý Euler
Định lý Wilson

Định lý Fermat nhỏ*

Cho số nguyên tố p. Khi đó, với mọi số nguyên dương a sao cho $(a, p) = 1$ thì

$$a^{p-1} \equiv 1 \ (mod \ p)$$

Hàm phi (φ) Euler

Hàm phi Euler của số nguyên dương n là số các số nguyên dương m không vượt quá n sao cho $(m, n) = 1$.

Các tính chất:

Nếu p là số nguyên tố thì $\varphi(p) = p - 1$.
Nếu p là số nguyên tố thì $\varphi(p^k) = p^{k-1}(p - 1)$
Nếu $n = p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_k^{\alpha_k}$ thì

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right).\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)$$

Nếu $(a, b) = 1$ thì $\varphi(ab) = \varphi(a).\varphi(b)$ (Hàm phi Euler là một hàm nhân tính)

Định lý Euler*

Nếu $(a, m) = 1$ thì $a^{\varphi(m)} \equiv 1 \ (mod \ m)$.

Định lý Wilson*

Số nguyên dương p là số nguyên tố
$\Leftrightarrow (p - 1)! \equiv -1 \ (mod \ p)$

*Chứng minh trong phần tiếp theo!

Hệ thặng dư

Hệ thặng dư đầy đủ mod n

Tập hợp các số nguyên A= $\{a_1; a_2; \dots; a_n\}$ được gọi là hệ thặng dư đầy đủ mod n khi và chỉ khi hai số bất kì trong tập hợp không đồng dư nhau theo mod n, hay tập số dư r_i của a_i khi chia cho n trùng với tập $\{0;\ 1; \dots;\ n-1\}$.

Nhận xét:

- ✓ Nếu $A = \{a_1; a_2; \dots; a_n\}$ là một hệ thặng dư đầy đủ mod n thì với mọi số nguyên m thì tồn tại duy nhất $a_i \in A$ để $a_i \equiv m\ (mod\ n)$.
- ✓ Với mọi số nguyên a, k thỏa $(k, n) = 1$ thì $A' = \{a + ka_1, a + ka_2, \dots, a + ka_n\}$ cũng là một hệ thặng dư đầy đủ mod n. Trong các bài toán về hệ thặng dư, ta thường sử dụng tính chất này để phát hiện/xây dựng một hệ thặng dư đầy đủ.

Chứng minh:

Giả sử tồn tại $i \neq j$ thỏa $1 \leq i, j \leq n$ và $a + ka_i \equiv a + ka_j\ (mod\ n)$. Khi đó ta có $ka_i \equiv ka_j\ (mod\ n) \Leftrightarrow a_i \equiv a_j\ (mod\ n)$ (vì $(k, n) = 1$) vô lý do $a_i \not\equiv a_j\ (mod\ n)$).

Mà A' có n phần tử nên A' là một hệ thặng dư đầy đủ mod n.

Hệ thặng dư thu gọn mod n

Tập hợp $B = \{b_1, b_2, \dots, b_{\varphi(n)}\}$ được gọi là một hệ thặng dư thu gọn mod n khi và chỉ khi $(b_i, n) = 1,\ i = \overline{1, \varphi(n)}$ và hai phần tử bất kì trong tập hợp không đồng dư nhau theo mod n.

Nhận xét:

✓ Nếu $B = \{b_1; b_2; \dots; b_{\varphi(n)}\}$ là một hệ thặng dư thu gọn mod n và c là số nguyên sao cho $(c, n) = 1$ thì tập $B' = \{cb_1; cb_2; \dots; cb_{\varphi(n)}\}$ cũng là một hệ thặng dư thu gọn mod n.

Chứng minh:

Giả sử tồn tại $i \neq j$ thỏa $1 \leq i, j \leq \varphi(n)$ thỏa $cb_i \equiv cb_j (mod\ n)$.

Khi đó ta có $b_i \equiv b_j\ (mod\ n)$ (vì $(c, n) = 1$) (vô lý do $b_i \not\equiv b_j\ (mod\ n)$).

Mà B' có $\varphi(n)$ phần tử $\Rightarrow B'$ là một hệ thặng dư thu gọn mod n.

✓ Cho số nguyên dương n. Tập hợp $\{1; 2; \dots; n-1\}$ là một hệ thặng dư thu gọn mod n khi và chỉ khi n là số nguyên tố hoặc $n = 1$.

Chứng minh:

Khi $n = 1$, bài toán hiển nhiên.

Xét $n \geq 2$.

+) Nếu n là số nguyên tố thì với mọi $i = \overline{1, n-1}$, ta có: $(i, n) = 1$.

$\Rightarrow$ Tập hợp $\{1,2, \dots, n-1\}$ là một hệ thặng dư thu gọn mod n.

+) Nếu tập $\{1,2, \dots, n-1\}$ là một hệ thặng dư thu gọn mod n.

$\Rightarrow n$ không chia hết cho bất cứ số nào khác 1 nhỏ hơn nó.

$\Rightarrow n$ là số nguyên tố.

✓ $|B| = \varphi(n)$

Bổ đề 1

Cho hai số nguyên dương a, n thỏa mãn $(a, n) = 1$. Khi đó, tồn tại duy nhất số nguyên k theo mod n sao cho $ak \equiv 1$.

Chứng minh:

Gọi $S = \{a_1; a_2; \dots; a_l\}$ là một hệ thặng dư thu gọn mod n.
⇒ Tập hợp $\{aa_1; aa_2; \dots; aa_l\}$ cũng là một hệ thặng dư thu gọn mod n
Do đó, tồn tại số nguyên i sao cho $aa_i \equiv 1 \ (mod\ n)$.

Từ ý tưởng trên, ta có thể chứng mình được các định lý ở mục I bao gồm định lý Wilson, định lý Fermat nhỏ và định lý Euler (chứng minh ở trang sau).

Bổ đề 2

Cho hai số nguyên dương $a, b; (a, n) = (b, n) = 1$ thỏa mãn

$$\begin{cases} a^m \equiv b^m \ (mod\ n) \\ a^l \equiv b^l \ (mod\ n) \end{cases} \Rightarrow a^{(m,l)} \equiv b^{(m,l)} \ (mod\ n)$$

Bổ đề này là một kết quả cơ bản của phần cấp của một số nên xin phép chỉ đề cập đến đây và không chứng mình.

Chứng minh các định lý

Định lý Wilson

☜ Chiều đảo:

Nếu $(p-1)! \equiv -1 \ (mod\ p)$ thì hiển nhiên ta có p là số nguyên tố

☞ Chiều thuận: Ta chỉ xét $p \geq 5$.

Với mỗi số nguyên dương $k \leq p-1$, tồn tại duy nhất số nguyên dương $l \leq p-l$ sao cho $kl \equiv 1 \ (mod\ p)$.

Hơn nữa, nếu $k \neq 1$ và $k \neq p-1$ thì $k \neq l$.

Nghĩa là các số $2, 3, \dots, p-2$ có thể chia thành các cặp rời nhau, tích của mỗi cặp đều đồng dư 1 mod p.

Vậy, $(p-1)! \equiv 1.(p-1).1^{\frac{p-3}{2}} \equiv -1 \ (mod\ p)$.

Định lý Fermat nhỏ

Xét tập hợp $\{a; 2a; \dots; (p-1)a\}$ là một hệ thặng dư thu gọn mod p do $(a,p) = 1$. Vì $\{1; 2; \dots; p-1\}$ cũng là một hệ thặng dư thu gọn nên

$$a.(2a) \dots (p-1)a \equiv 1.2 \dots (p-1) \ (mod\ p)$$

Hay ta có

$$a^{p-1} \equiv 1 \ (mod\ p)$$

Định lý Euler

Xét tập hợp S $= \{a_1; a_2; \dots; a_k\}$ là một hệ thặng dư thu gọn nhỏ nhất mod n (nghĩa là các phần tử trong hệ thặng dư đó đều bé hơn hoặc bằng n). Khi đó, $\{aa_1; aa_2; \dots; aa_k\}$ cũng là một hệ thặng dư thu gọn mod n.

$$\Rightarrow a^{\varphi(n)}.a_1.a_2 \dots a_k \equiv a_1.a_2 \dots a_k \ (mod\ n)$$

$$\Rightarrow a^{\varphi(n)} \equiv 1 \ (mod\ n)$$

Ghi chú 1: Để xử lý các bài toán chia hết, ta có thể làm xuất hiện hệ thặng dư đầy đủ mod n. Khi đó, nếu $A = \{a_1, a_2, \dots, a_n\}$ là một hệ thặng dư đầy đủ mod n thì:

i. $a_1 + a_2 + \cdots + a_n \equiv 0 + 1 + \cdots + n \equiv \frac{n(n-1)}{2} \ (mod\ n)$

ii. A có một phần tử chia hết cho n (có thể sử dụng khi cần chứng minh tồn tại một số chia hết cho n).

Ví dụ 1: Tìm tất cả số nguyên dương n để tồn tại hai hệ thặng dư đầy đủ theo mod n là $(a_1, a_2, \dots, a_n)$ và $(b_1, b_2, \dots, b_n)$ sao cho $(a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$ cũng là hệ thặng dư đầy đủ.

Ví dụ 2 *(Poland 2010)*: Cho p là số nguyên tố lẻ có dạng $3k + 2$. Chứng minh rằng:

$$\prod_{k=1}^{p-1}(k^2 + k + 1) \equiv 3(mod\ p) \qquad (*)$$

Ví dụ 1: Do $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n)$ và $(a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$ là hệ thặng dư đầy đủ mod n nên:

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \equiv \sum_{i=1}^{n} a_i + b_i \equiv \sum_{i=1}^{n} i \equiv 2\sum_{i=1}^{n} i \equiv n(n-1) \equiv \frac{n(n-1)}{2} \equiv 0\ (mod\ n)$$

Suy ra $\frac{n(n-1)}{2} : n$ tức là $n - 1$ chia hết cho 2 và n lẻ.

Với n lẻ, ta xét hai bộ hệ thặng dư đầy đủ mod n là $(1, 2, \dots, n)$.

Khi đó, bộ $(1 + 1, 2 + 2, \dots, n + n)$ cũng là một hệ thặng dư đầy đủ mod n.

Vậy n lẻ thỏa yêu cầu bài toán.

Ví dụ 2:

Sử dụng định lý Wilson ta có :

$(p-1)! \equiv -1\ (mod\ p)$ (#)

Ta chứng mình $\{2^3-1; 3^3-1; \dots; p^3-1\}$ là hệ thặng dư rút gọn mod p (với p có dạng $3k+2$)

Nhận thấy hệ trên có $p-1$ phần tử, vì vậy nếu hai phần tử bất kỳ không đồng dư nhau theo mod p thì đây là một hệ thặng dư thu gọn mod p.

Giả sử tồn tại x, y nguyên dương phân biệt trong $\{1; 2; \dots; p-1\}$ thoả mãn :

$$x^3 \equiv y^3\ (mod\ p) \qquad (1)$$

Sử dụng bổ đề 2 kết hợp với $x^{p-1} \equiv y^{p-1}\ (mod\ p)$ và $(p-1, 3) = 1 \Rightarrow x \equiv y\ (mod\ p)$.

Mà x, y thuộc $\{1,2, \dots, p-1\} \Rightarrow x-y = 0$ (vô lý). Vậy điều giả sử sai.

Nhân $(*)$ và (#) với nhau ta chứng minh:

$$3(\mathrm{p}-1).\prod_{k=2}^{p-1}(k^3-1) \equiv -3(mod\ p)$$

Do $\mathrm{p}-1 \equiv \mathrm{p}^3-1\ (\mathrm{mod\ p})$

Đồng nghĩa :

$$\mathrm{VT} \equiv 3(\mathrm{p}-1)! \equiv -3\ (\mathrm{mod\ p})$$

Như vậy $(*)$ đúng.

Bài tập VD1.

Bài 1: Tìm số nguyên dương n sao cho tồn tại 3 hệ thặng dư đầy đủ mod n là A, B, C thỏa $A+B,\ B+C,\ C+A,\ A+B+C$ đều là các hệ thặng dư đầy đủ mod n, trong đó $X = \{x_1, x_2 \dots, x_n\}, Y = \{y_1, y_2 \dots, y_n\}$ thì $X+Y = \{x_1+y_1, x_2+y_2, \dots, x_n+y_n\}$.

Bài 2: Chứng minh rằng $\{1^n, 2^n, 3^n, \dots, (p-1)^n\}$ là một hệ thặng dư thu gọn mod p với $(n, p-1) = 1$ và p là số nguyên tố.

Bài 3: Cho p là số nguyên tố lẻ. Chứng minh:

$$1!.2!\dots(p-1)! \equiv (-1)^{\frac{p^2-1}{8}}.\left(\frac{p-1}{2}\right)!\ (mod\ p)$$

Bài 4: Cho p là một số nguyên tố lẻ. Xét đa thức $P(x) = (p-1)x^p - x - 1$. Chứng minh rằng tồn tại vô số số nguyên a sao cho $p^p \mid P(a)$.

Bài 5: Cho p là số nguyên tố dạng $3k+2$. Xét hàm số

$$f(x) = 3x^{\frac{2p-1}{3}} + 3x^{\frac{p+1}{3}} + x + 1$$

Kí hiệu $f_i(x) = f(f(\dots(x)\dots)$ (i lần f). Chứng minh $(1 + \prod_{i=1}^{p-1} f_i(0)) \vdots p$

Bài 6: Cho số nguyên tố p lẻ, ta gọi 1 bộ gồm p số $(a_1, a_2, \dots, a_p)$ là một bộ tốt nếu thỏa mãn cả ba điều kiện sau:

i. $0 \le a_i \le p-1\ \forall i \in \{1,2,\dots,p-1\}$

ii. $p \nmid \sum_{i=1}^{p} a_i$

iii. $p \mid \sum_{i=1}^{p} a_i^2$

Đếm tất cả số bộ tốt theo p.

Ghi chú 2: Để tính tổng trong một số bài toán Số học, ta thường làm xuất hiện hệ thặng dư đầy đủ mod n (không âm nhỏ nhất). Khi đó, các số hạng trong hệ thặng dư đó là một hoán vị của $\{0; 1; \dots; n-1\}$.

Ví dụ 3: Tính tổng sau:

$$S = \left[\frac{m}{n}\right] + \left[\frac{2m}{n}\right] + \cdots + \left[\frac{mn}{n}\right]$$

Đặt $d = (m,n), m = pd, n = qd \Rightarrow (p,q) = 1.$

Lúc này

$$S = \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \cdots + \left[\frac{dqp}{q}\right] = \sum_{i=0}^{d-1}\sum_{j=1}^{q}\left([(iq+j)\frac{p}{q}]\right)$$

$$= \sum_{i=0}^{d-1}\sum_{j=1}^{q}\left(i + \left[\frac{pj}{q}\right]\right) = \sum_{i=0}^{d-1} qi + \sum_{i=0}^{d-1}\sum_{j=1}^{q}\left(\left[\frac{pj}{q}\right]\right) = \frac{qd(d-1)}{2} + dT$$

Với $T = \sum_{j=1}^{q}([pj/q])$

Nhận xét: Với $(p,q) = 1$ thì $\{pj;\ j \in \{1,2,\dots,q\}\}$ là hệ thặng dư đầy đủ mod q, do đó tập hợp các số là phần lẻ của các số $\frac{pj}{q}$ trùng với tập $\left\{\frac{1}{q}; \frac{2}{q}; \dots; 0\right\}$.

Do đó $T = \sum_{j=1}^{q}\frac{pj}{q} - \sum_{j=0}^{q-1}\frac{j}{q} = \frac{p(q+1)}{2} - \frac{q-1}{2}$

Vậy $S = \frac{qd(d-1)}{2} + \frac{dp(q+1)}{2} - \frac{d(q-1)}{2}$. Thay $d = (m,n), p = \frac{m}{(m,n)}, q = \frac{n}{(m,n)}$ ta có đáp số.

Nhận xét: *Bài toán gốc (tính S) là mở rộng cho bài toán phụ (tính T) khi không có giả thiết $(m,n) = 1$. Để có thể sử dụng tính chất của hệ thặng dư đầy đủ (thuận tiện cho việc tính tổng) thì ta đặt thêm $d = (m,n)$ để đưa về bài toán tính T, từ đó có các bước như trên.*

Bài tập VD2.

Bài 1: Cho m, n nguyên dương sao cho $(m, n) = 1$ và m chẵn. Tính tổng sau:

$$S = \sum_{k=1}^{n-1} (-1)^{\left\lfloor \frac{mk}{n} \right\rfloor} \cdot \left\{ \frac{mk}{n} \right\}$$

Bài 2: Cho $a \in \mathbb{R}$, $k, n \in \mathbb{N}^*$ thoả $(k, n) = 1$. Giả sử $\lfloor x \rfloor$ là số nguyên lớn nhất nhỏ hơn x. Chứng minh rằng:

$$\lfloor a \rfloor + \left\lfloor a + \frac{k}{n} \right\rfloor + \left\lfloor a + \frac{2k}{n} \right\rfloor + \cdots + \left\lfloor a + \frac{(n-1)k}{n} \right\rfloor = \lfloor na \rfloor + \frac{(n-1)(k-1)}{2}$$

Bài tập tổng hợp.

Bài 1: Tìm số dư của phép chia $T = \prod_{x=1}^{37} (1 + x + x^2 + x^3 + x^4)$ khi chia cho 37.

Bài 2: Cho đa thức $P(x)$ hệ số nguyên thỏa $P(x_1), P(x_2), \ldots, P(x_n)$ không chia hết cho n với $n \in \mathbb{N}^*$ và $\{x_1, x_2, \ldots, x_n\}$ là hệ thặng dư đầy đủ mod n. Khi đó $P(x)$ có nghiệm nguyên không?

Bài 3: Xét n = 20192020 số nguyên dương phân biệt và S là tập hợp tất cả các tổng của từng cặp hai số trong chúng. Hỏi số dư của các số trong S khi chia cho $\frac{n(n-1)}{2}$ có thể đôi một phân biệt nhau hay không?

Bài 4: Cho dãy số (u_n) có $u_0 = a$ $(a \in \mathbb{N}^*)$, $u_n = u_{n-1} + u_{\left\lfloor \frac{n}{k} \right\rfloor}$ với $n \in \mathbb{N}^*$, $k \in \mathbb{N}^*$ là hằng số. Giả sử tồn tại $x \in \mathbb{N}^*$ thoả $u_x, u_{x+1}, \ldots, u_{x+k}$ chia $k^2 + k + 1$ có cùng số dư và $k^2 + k + 1$ là số nguyên tố, chứng minh có vô số số $x \in \mathbb{N}^*$ thoả $u_x, u_{x+1}, \ldots, u_{x+k}$ chia $k^2 + k + 1$ có cùng số dư. ($\lfloor a \rfloor$: phần nguyên của a).

Bài tập tổng hợp (tt).

Bài 5: Cho $n \in N^*$. Tồn tại hoán vị $\{a_1; a_2; \ldots; a_n\}$ của $\{1; 2; \ldots; n\}$ sao cho $\{a_1 + 1;\ a_2 + 2; \ldots;\ a_n + n\}$ là hệ thặng dư đầy đủ mod n. Chứng minh rằng n lẻ.

Bài 6: Cho 2 hệ thặng dư đầy đủ theo mod n: $A = \{a_1; a_2; \ldots; a_n\}$ và $B = \{b_1; b_2; \ldots; b_n\}$. Chứng minh rằng nếu n chẵn thì tập $C = \{a_1 + b_1; a_2 + b_2; \ldots; a_n + b_n\}$ không là hệ thặng dư đầy đủ mod n.

Bài 7 *(IMO 2005)*: Cho 1 dãy các số nguyên $a_1, a_2, \ldots, a_n$ thỏa mãn 2 điều kiện:

a) $\{a_1, a_2, \ldots, a_n\}$ là 1 hệ thặng dư đầy đủ mod n với $n \geq 1$.

b) Có vô số số hạng dương và vô số số hạn âm xuất hiện trong dãy.

Chứng minh rằng mỗi số nguyên xuất hiện đúng 1 lần trong dãy.

Bài 8 *(Balkan 1999)*: Cho số nguyên tố $p > 2$ thoả p chia 3 dư 2. Chứng minh tập hợp $A = \{y^2 - x^3 - 1 \mid x, y \in Z^+, x < p, y < p\}$ có nhiều nhất $p - 1$ phần tử chia hết cho p.

Bài 9: 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.

Bài 10: Gọi a, b, c là các số nguyên dương sao cho $\frac{a^2 + b^2 + c^2}{ab + bc + ca}$ là 1 số nguyên. Chứng minh số này không bao giờ là bội của 3.

Bài 11: Cho số nguyên tố $p > 3$ và m, n là 2 số nguyên tố cùng nhau thỏa mãn $\frac{m}{n} = \sum_{i=1}^{p-1} \frac{1}{i^2}$. Chứng minh rằng m chia hết cho p.

Bài 12: Cho số nguyên tố $p > 3$. Chứng minh rằng số dư của phép chia $\prod_{j=1}^{p}(j^2 + 1)$ cho p chỉ có thể là 0 hoặc 4.

Lời giải tham khảo của nhóm

Bài tập Ví dụ 1, 2

Bài 1: Tìm số nguyên dương n sao cho tồn tại 3 hệ thặng dư đầy đủ mod n là A, B, C thỏa $A+B,\ B+C,\ C+A,\ A+B+C$ đều là các hệ thặng dư đầy đủ mod n, trong đó $X=\{x_1, x_2 \dots, x_n\}, Y=\{y_1, y_2 \dots, y_n\}$ thì $X+Y=\{x_1+y_1, x_2+y_2, \dots, x_n+y_n\}$.

Đặt $A=\{a_1, a_2, \dots, a_n\},\ B=\{b_1, b_2, \dots, b_n\},\ C=\{c_1, c_2, \dots, c_n\}, s=\frac{n(n+1)}{2}$.

Khi đó: do $A, A+B$ là các hệ thặng dư đầy đủ mod n nên:

$$\sum_{i=1}^{n}(a_i+b_i) \equiv \sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} i \equiv s \ (mod\ n)$$

$$\Rightarrow s \equiv \sum_{i=1}^{n}(a_i+b_i) \equiv 2s \ (mod\ n)$$

$$\Rightarrow n \equiv s = \frac{n(n+1)}{2} \Rightarrow 2 \nmid n$$

Đặt $p=\frac{n(n+1)(2n+1)}{6}=\sum_{i=1}^{n} i^2$, do $A, B, C, A+B,\ B+C,\ C+A,\ A+B+C$ đều là các hệ thặng dư đầy đủ mod n nên ta có:

$$4p \equiv \sum_{i=1}^{n}\left[(a_i+b_i+c_i)^2+a_i^2+b_i^2+c_i^2\right]$$

$$\equiv \sum_{i=1}^{n}[(a_i+b_i)^2+(b_i+c_i)^2+(a_i+c_i)^2] \equiv 3p \ \ (mod\ n)$$

$$\Rightarrow n \mid p = \frac{n(n+1)(2n+1)}{6} \Rightarrow 3 \nmid n$$

Vậy $(n, 6)=1$.

Với $(n, 6)=1$: ta xét $A=\ B=C=\{1,2, \dots, n\}$ thỏa yêu cầu bài toán.

Bài 2: Chứng minh rằng $\{1^n, 2^n, 3^n, \ldots, (p-1)^n\}$ là một hệ thặng dư thu gọn mod p với $(n, p-1) = 1$ và p là số nguyên tố.

Để chứng minh yêu cầu bài toán, ta chỉ cần chứng minh:

Với hai số i, j bất kì ($i \neq j$ và $i, j \in \{1,2,\ldots,p-1\}$) thì $i^n \not\equiv j^n \ (mod\ p)$

Giả sử tồn tại $i, j \in \{1, 2, \ldots, p-1\}$ và $i \neq j$ sao cho $i^n \equiv j^n \ (mod\ p)$ (1)

Do p là số nguyên tố và $j \neq 0$ nên tồn tại k sao cho $jk \equiv 1 \ (mod\ p)$

Nhân k^n vào 2 vế của (1) ta được $(ik)^n \equiv 1 \ (mod\ p)$

Do $i \not\equiv j \ (mod\ p)$ nên $ik \not\equiv jk \ (mod\ p)$

Suy ra $ik \not\equiv 1 \ (mod\ p)$ (2)

Mà ta có $\begin{cases} (ik)^n \equiv 1 \ (mod\ p) \\ (ik)^{p-1} \equiv 1 \ (mod\ p) \end{cases}$

Suy ra $(ik)^{(n,p-1)} \equiv 1 \ (mod\ p)$

Mà $(n, p-1) = 1$ nên $ik \equiv 1 \ (mod\ p)$ (mâu thuẫn với (2))

Nên ta có điều giả sử là sai.

Vậy với hai số i, j bất kì ($i \neq j$ và $i, j \in \{1,2,\ldots,p-1\}$) thì $i^n \not\equiv j^n \ (mod\ p)$

Nói cách khác, $\{1^n, 2^n, 3^n, \ldots, (p-1)^n\}$ là một hệ thặng dư thu gọn modulo p.

Bài 3: Cho p là số nguyên tố lẻ. Chứng minh:

$$1!.2!\dots(p-1)! \equiv (-1)^{\frac{p^2-1}{8}}.\left(\frac{p-1}{2}\right)!\ (mod\ p)$$

Ta có

$$\begin{cases} (p-1)! \equiv (p-1)! \equiv -1\ (mod\ p) \\ 1!\,(p-2)! \equiv -(p-1)(p-2)! \equiv (-1)^1(p-1)! \equiv (-1)^2\ (mod\ p) \\ 2!\,(p-3)! \equiv [-(p-1)][-(p-2)](p-3)! \equiv (-1)^2(p-1)! \equiv (-1)^3\ \ (mod\ p) \\ \dots \\ \left(\frac{p-3}{2}\right)!\left(\frac{p+1}{2}\right)! \equiv (-1)^{\frac{p-1}{2}} \end{cases}$$

$$\Rightarrow 1!.2!\dots(p-1)!$$

$$= (p-1)!\,[1!\,(p-2)!][2!\,(p-3)!]\dots\left[\left(\frac{p-3}{2}\right)!\left(\frac{p+1}{2}\right)!\right]\left(\frac{p-1}{2}\right)!$$

$$\equiv (-1)^1.(-1)^2\dots(-1)^{\frac{p-1}{2}}.\left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right)}{2}}.\left(\frac{p-1}{2}\right)!$$

$$\equiv (-1)^{\frac{p^2-1}{8}}.\left(\frac{p-1}{2}\right)!\ (mod\ p)$$

Nhận xét: *Đây là một ví dụ điển hình cho việc sử dụng phương pháp nhóm các nhân tử để lấy đồng dư và kết hợp với định lý Wilson.*

Bài 4: Cho p là một số nguyên tố lẻ. Xét đa thức $P(x) = (p-1)x^p - x - 1$. Chứng minh rằng tồn tại vô số số nguyên a sao cho $p^p \mid P(a)$.

Đặt $A = \{P(1), P(2), \dots, P(p^p)\}$.

Ta chứng minh A là một hệ thặng dư đầy đủ mod p^p.

Giả sử tồn tại 2 số nguyên dương phân biệt $a, b \in \overline{1, p^p}$ sao cho $p^p \mid P(a) - P(b)$

$$\Rightarrow p^p \mid [(p-1)a^p - a - 1] - [(p-1)b^p - b - 1]$$
$$\Rightarrow p^p \mid (p-1)(a^p - b^p) - (a-b) \qquad (*)$$

Mà $a^p \equiv a,\ b^p \equiv b \pmod p$ nên $p \mid (p-1-1)(a-b) \Rightarrow p \mid a-b$

$\Rightarrow a^i b^{p-1-i} \equiv a^{p-1} \pmod p$ với mọi $i \in \overline{0, p-1}$

$$\Rightarrow (a^{p-1} + a^{p-2}b + \cdots + b^{p-1}) \equiv pa^{p-1} \equiv 0 (mod\ p) \quad (**)$$

Mà từ $(*)$ ta có:

$$p^p \mid (a-b)[(p-1)(a^{p-1} + a^{p-2}b + \cdots + b^{p-1}) - 1]$$

Rõ ràng $a, b \in \overline{1, p^p}$ mà $a \neq b$ nên $p^p \nmid a - b$

$$\Rightarrow p \mid [(p-1)(a^{p-1} + a^{p-2}b + \cdots + b^{p-1}) - 1]$$

Điều này vô lý do $(**)$.

Vậy A là một hệ thặng dư đầy đủ mod p^p nên tồn tại số nguyên a sao cho $p^p \mid P(a)$, chọn $x \equiv a \pmod{p^p}$ thì $p^p \mid P(x)$. Vậy có vô số số x thỏa.

Bài 5: Cho p là số nguyên tố dạng $3k+2$. Xét hàm số

$$f(x) = 3x^{\frac{2p-1}{3}} + 3x^{\frac{p+1}{3}} + x + 1$$

Kí hiệu $f_i(x) = f(f(\dots(x)\dots)$ (i lần f). Chứng minh $(1 + \prod_{i=1}^{p-1} f_i(0)) \vdots p$

Cho a $\in Z$. Ta có:

$$f(a^3) = 3a^{2p-1} + 3a^{p+1} + a^3 + 1 \equiv 3a + 3a^2 + a^3 + 1$$
$$\equiv (a+1)^3 \ (mod\ p)$$

(do $a^{2p-1} = a^p . a^{p-1} \equiv a \ (mod\ p)$; $a^{p+1} \equiv a^2 \ (mod\ p)$ (định lý nhỏ Fermat)

$$\Rightarrow f(0) \equiv 1^3 \ (mod\ p)\ ;\ f\big(f(0)\big) \equiv f(1^3) \equiv 2^3 \ (mod\ p);$$

$$f\Big(f\big(f(0)\big)\Big) \equiv f(2^3) \equiv 3^3 \ (mod\ p); \dots \qquad (1)$$

Xét hệ thặng dư $\{1^3\ ;2^3\ ;\dots;(p-1)^3\}$ (có $p-1$ phần tử)

Từ bổ đề, ta suy ra hệ thặng dư $\{1^3\ ;2^3\ ;\dots;(p-1)^3\}$ là hệ thặng dư thu gọn mod p.

$(1) \Rightarrow \{f(0)\ ;f_2(0)\ ;\dots;f_{p-1}(0)\}$ là hệ thặng dư thu gọn mod p

$\Rightarrow \big(1 + \prod_{i=1}^{p-1} f_i(0)\big) \vdots p$ (định lý Wilson)

Bài 6: Cho số nguyên tố p lẻ, ta gọi 1 bộ gồm p số $(a_1, a_2, \ldots, a_p)$ là một bộ tốt nếu thỏa mãn cả ba điều kiện sau:

i. $0 \le a_i \le p-1 \; \forall i \in \{1,2,\ldots,p-1\}$

ii. $p \nmid \sum_{i=1}^{p} a_i$

iii. $p \mid \sum_{i=1}^{p} a_i^2$

Đếm tất cả số bộ tốt theo p.

Trước hết, ta gọi S là tập hợp các bộ $B = (b_1, b_2, \ldots, b_p)$ sao cho $p \nmid \sum_{i=1}^{p} b_i$, ta đếm số bộ của S.

Ta thấy mỗi số từ b_1 đến b_{p-1} có đúng p cách chọn và ta cần chọn số b_p sao cho $b_p \not\equiv -\sum_{i=1}^{p-1} b_i \pmod p$, dễ thấy có đúng $p-1$ cách chọn b_p thỏa mãn điều kiện trên.

Vậy có đúng $p^{p-1}(p-1)$ cách chọn các bộ B thỏa điều kiện (i) và (ii) hay $|S| = p^{p-1}(p-1)$

Với mỗi bộ B, ta định nghĩa $S_B = \{B_1, B_2, B_3, \ldots, B_p\}$ là 1 lớp tương đương của B.

Với $B_i = (b_{i_1}, b_{i_2}, \ldots, b_{i_p})$ trong đó $b_{i_j} \equiv b_j - b_1 + i \pmod p$ $(i, j \in \{1,2 \ldots, p\})$

Ta có $\sum_{j=1}^{p} b_{i_j} \equiv \sum_{i=1}^{p} b_i + pi - pb_1 \not\equiv 0 \pmod p$.

Vậy ta dễ thấy $B_1, B_2, B_3, \ldots, B_p \in S$

Ta có phần tử đầu tiên của B_i là i nên các bộ này là các bộ phân biệt

Để ý thấy $B = B_{b_1}$ nên B cũng sẽ thuộc S_B

Bây giờ ta chứng minh 2 điều:

1. Mỗi phần tử của S thuộc đúng 1 lớp tương đương.
2. Trong mỗi lớp tương đương có đúng 1 phần tử thỏa mãn (iii).

❑ ***Chứng minh điều 1:***

Giả sử $A \in S_C, S_D, (C \neq D)$ ta chứng minh $S_C = S_D$.

Tồn tại k, q sao cho $\begin{cases} a_i \equiv c_i - c_1 + k \ (mod\ p) \\ a_i \equiv d_i - d_1 + q \ (mod\ p) \end{cases}$ với mọi $i \in \{1,2,\dots \text{p}\}$

(trong đó $A = (a_1, a_2, \dots, a_p), C = (c_1, c_2, \dots, c_p), D = (d_1, d_2, \dots, d_p)$)

Không mất tính tổng quát, ta giả sử $q \geq k$

Vậy ta có

$c_i - c_1 + k \equiv d_i - d_1 + q \ (mod\ p)$ với mọi i $\in \{1,2,\dots \text{p}\}$

$$\Leftrightarrow c_i \equiv d_i - d_1 + (q - k + c_1) \ (mod\ p)$$

Vậy C sẽ là phần tử thứ $q - k + c_1$ của S_D, vậy nên mọi phần tử của S_C sẽ thuộc S_D, mà

$|S_C| = |S_D| = p$ từ đó ta có $S_C = S_D$.

❑ ***Chứng minh điều 2:***

Với mỗi $B_i \in S_B$, ta đặt $n_i = i - b_1$, khi đó ta có $B_i = (b_1 + n_i, b_2 + n_i, \dots, b_p + n_i)$

Ta đặt $k = \sum_{i=1}^{p} b_i$, $q = \sum_{i=1}^{p} b_i^2$

Ta có $(b_1 + n_i)^2 + (b_2 + n_i)^2 + \dots + (b_p + n_i)^2 = q + 2n_i.k + p.n_i^2 \equiv q + 2n_i.k \ (mod\ p)$

Do $\{1, 2, \dots, \text{p}\}$ một hệ thặng dư đầy đủ mod p nên ta có $\{1 - b_1, 2 - b_1, \dots, p - b_1\} = \{n_1, n_2, \dots, n_p\}$ cũng là một hệ đầy đủ mod p.

Lại có $2\ k = 2 \sum_{i=1}^{p} b_i \not\equiv 0 \ (mod\ p)$nên $(2k, p) = 1$ vậy $\{2kn_1, 2kn_2, \dots, 2kn_p\}$ cũng là một hệ thặng dư đầy đủ mod p.

Khi đó tồn tại duy nhất 1 số trong các số trong tập trên có số dư là p - q, hay tồn tại duy nhất x sao cho

$$(b_1 + n_x)^2 + (b_2 + n_x)^2 + \dots + (b_p + n_x)^2 \equiv 0 \ (mod\ p)$$

Vậy trong mỗi lớp tương đương có duy nhất 1 bộ số thỏa yêu cầu bài toán.

⇒ Từ 2 điều vừa chứng minh, kết hợp với việc tập S là hợp của tất cả các lớp tương đương, ta có số bộ số thỏa mãn yêu cầu bài toán là

$$\frac{p^{p-1}(p-1)}{p} = p^{p-2}(p-1)$$

Nhận xét:

- *Bài toán tuy không có kỹ thuật quá nặng nhưng lại yêu cầu sự tư duy ở mức độ cao, việc đặt ra định nghĩa cho tập S và các lớp tương đương là rất sáng tạo, đòi hỏi nhiều sự nhạy bén và kinh nghiệm.*
- *Trong bài toán trên, ta đã gián tiếp chứng minh một bổ đề khá quan trọng và được sử dụng nhiều: cho a,n là 2 số nguyên dương sao cho* $(a,n) = 1$ *thì tồn tại duy nhất b (mod n) sao cho* $ab \equiv 1 \pmod n$.

Bài tập Ví dụ 3

Bài 1: Cho m,n nguyên dương sao cho $(m,n) = 1$ và m chẵn. Tính tổng sau:

$$S = \sum_{k=1}^{n-1} (-1)^{\left\lfloor \frac{mk}{n} \right\rfloor} . \left\{ \frac{mk}{n} \right\}$$

Đặt $r_k = mk - n.\left\lfloor \frac{mk}{n} \right\rfloor$ với mọi $k \in \overline{1,n-1}$. $\Rightarrow \left\{ \frac{mk}{n} \right\} = \frac{r_k}{n}$

Rõ ràng $A = \{ mk \mid k \in \overline{0,n-1} \}$ là hệ thặng dư đầy đủ mod n. (do $(m,n) = 1$)

$$\Rightarrow \left\{ \frac{r_k}{n} \mid k \in \overline{1,n-1} \right\} = \left\{ \left\{ \frac{mk}{n} \right\} \mid k \in \overline{1,n-1} \right\} = \left\{ \frac{k}{n} \mid k \in \overline{1,n-1} \right\}$$

Mà $2 \mid m, 2 \nmid n$ nên $r_k = mk - n.\left\lfloor \frac{mk}{n} \right\rfloor \equiv \left\lfloor \frac{mk}{n} \right\rfloor \pmod 2$

Vậy:

$$S = \sum_{k=1}^{n-1} (-1)^{\left\lfloor \frac{mk}{n} \right\rfloor} . \left\{ \frac{mk}{n} \right\} = \sum_{k=1}^{n-1} (-1)^{r_k} . \frac{r_k}{n} = \sum_{k=1}^{n-1} (-1)^k . \frac{k}{n} = \frac{n-1}{2n}$$

Bài 2: Cho $a \in \mathbb{R}, k, n \in \mathbb{N}^*$ thoả $(k, n) = 1$. Giả sử $\lfloor x \rfloor$ là số nguyên lớn nhất nhỏ hơn x. Chứng minh rằng:

$$\lfloor a \rfloor + \left\lfloor a + \frac{k}{n} \right\rfloor + \left\lfloor a + \frac{2k}{n} \right\rfloor + \cdots + \left\lfloor a + \frac{(n-1)k}{n} \right\rfloor = \lfloor na \rfloor + \frac{(n-1)(k-1)}{2}$$

Ta kí hiệu $\{x\} = x - \lfloor x \rfloor$. Gọi $b = \{a\}$, ta có:

$VT = na + \frac{k(n-1)}{2} - \{a\} - \left\{a + \frac{k}{n}\right\} - \left\{a + \frac{2k}{n}\right\} - \ldots - \left\{a + \frac{(n-1)k}{n}\right\}$

Mà $\{0;\ k;\ 2k;\ \ldots;\ (n-1)k\}$ là hệ thặng dư đầy đủ mod n (Do $\gcd(k\ ;\ n) = 1$)

$\Rightarrow VT$

$$= na + \frac{k(n-1)}{2} - \{b\} - \left\{b + \frac{1}{n}\right\} - \left\{b + \frac{2}{n}\right\} - \cdots - \left\{b + \frac{(n-1)}{n}\right\}$$

$$= na + \frac{k(n-1)}{2} - nb - \frac{n-1}{2} + \lfloor b \rfloor + \left\lfloor b + \frac{1}{n} \right\rfloor + \left\lfloor b + \frac{2}{n} \right\rfloor + \cdots + \left\lfloor b + \frac{(n-1)}{n} \right\rfloor$$

Trong nửa khoảng $[0\ ;\ nb)$ có $\lfloor nb \rfloor$ số dạng $nb - y$ $(y \in N^*, y \leq n)$

$\Rightarrow$ Trong nửa khoảng $[n\ ;\ nb + n)$ có $\lfloor nb \rfloor$ số dạng $nb + n - y$

$\Rightarrow$ Trong nửa khoảng $[1\ ;\ b + 1)$ có $\lfloor nb \rfloor$ số dạng $b + \frac{n-y}{n}$.

Mà $b = \{a\} \Rightarrow 0 \leq b < 1 \Rightarrow$ Trong n số $\lfloor b \rfloor$, $\left\lfloor b + \frac{1}{n} \right\rfloor$, $\left\lfloor b + \frac{2}{n} \right\rfloor$, …, $\left\lfloor b + \frac{(n-1)}{n} \right\rfloor$ có $\lfloor nb \rfloor$ số có giá trị bằng 1, $n - \lfloor nb \rfloor$ số có giá trị bằng 0.

$\Rightarrow \lfloor b \rfloor + \left\lfloor b + \frac{1}{n} \right\rfloor + \left\lfloor b + \frac{2}{n} \right\rfloor + \cdots + \left\lfloor b + \frac{(n-1)}{n} \right\rfloor = \lfloor nb \rfloor$.

$\Rightarrow VT = na - nb + \frac{(k-1)(n-1)}{2} + \lfloor nb \rfloor = na - \{nb\} + \frac{(k-1)(n-1)}{2} = na - \{na\} + \frac{(k-1)(n-1)}{2} = \lfloor na \rfloor + \frac{(n-1)(k-1)}{2} = VP$. (điều phải chứng minh)

Bài tập Tổng hợp

Bài 1: Tìm số dư của phép chia $T = \prod_{x=1}^{37}(1 + x + x^2 + x^3 + x^4)$ khi chia cho 37.

Ta chứng minh: nếu $a^5 \equiv b^5 \ (mod\ 37)$ thì $a \equiv b \ (mod\ 37)$.

Theo định lí Fermat nhỏ thì $a^{36} \equiv b^{36} \ (mod\ 37)$.

Mà $a^5 \equiv b^5 \ (mod\ 37) \Rightarrow a^{35} \equiv b^{35} \ (mod\ 37)$, vậy $a \equiv b \ (mod\ 37)$.

Do đó, các số trong tập $\{2^5 - 1, 3^5 - 1, \dots, 36^5 - 1\}$ là hệ thu gọn mod 37.

Áp dụng Wilson:

$$\prod_{x=2}^{37}(x^5 - 1) \equiv -1 \ (mod\ 37)$$

$$\Leftrightarrow \prod_{x=2}^{37}(x - 1) . \prod_{x=2}^{37}(1 + x + x^2 + x^3 + x^4) \equiv -1 \ (mod\ 37)$$

Mà cũng theo wilson thì

$$\prod_{x=2}^{37}(x - 1) \equiv -1 \ (mod\ 37)$$

Nên

$$\prod_{x=2}^{37}(1 + x + x^2 + x^3 + x^4) \equiv 1 \ (mod\ 37)$$

Nhân thêm biểu thức khi x=1 vào, ta có $T \equiv 5 \ (mod\ 37)$.

Nhận xét: *Đánh giá đầu bài còn có thể phát biểu dưới dạng tổng quát : Cho p là số nguyên tố có dạng m.k + 2. Khi đó* $a^m \equiv b^m \ (mod\ p)$ *thì* $a \equiv b \ (mod\ p)$. *Cách chứng minh kết quả này hoàn toàn tương tự.*

Bài 2: Cho đa thức $P(x)$ hệ số nguyên thỏa $P(x_1),\ P(x_2), \dots ,\ P(x_n)$ không chia hết cho n với $n \in \mathbb{N}^*$ và $\{x_1, x_2, \dots, x_n\}$ là hệ thặng dư đầy đủ mod n. Khi đó $P(x)$ có nghiệm nguyên không?

Giả sử $P(x)$ có nghiệm nguyên (gọi là $a \in \mathbb{Z}$)

Theo định lý Bézout, khi đó $P(x) = (x - a).Q(x)$

Mặt khác, vì $\{x_1, x_2, \dots, x_n\}$ là hệ thặng dư đầy đủ mod n nên $\exists i$ thỏa $x_i \equiv a\ (mod\ n)\ \ (1 < i < n)$

$\Rightarrow P(x_i) \vdots n$ (Vô lý do $P(x_1),\ P(x_2), \dots ,\ P(x_n)$ không chia hết cho n với $n \in \mathbb{N}^*$)

Vậy đa thức $P(x)$ không có nghiệm nguyên.

Bài 3: Xét n = 20192020 số nguyên dương phân biệt và S là tập hợp tất cả các tổng của từng cặp hai số trong chúng. Hỏi số dư của các số trong S khi chia cho $\frac{n(n-1)}{2}$ có thể đôi một phân biệt nhau hay không?

Giả sử trong các số ban đầu, có a số chẵn, b số lẻ với $a + b = n$. Khi đó, việc tính tổng các số trong n số đó sẽ sinh ra: ab số lẻ và $\frac{n(n-1)}{2} - ab = \frac{a^2 + b^2 - a - b}{2}$ số chẵn.

Vì $4|n$ nên $\frac{n(n-1)}{2}$ là số chẵn, để có được hệ đầy đủ như đề bài thì:

$$ab = \frac{a^2 + b^2 - a - b}{2} \Leftrightarrow (a - b)^2 = a + b = n$$

Dễ thấy n không là số chính phương vì n chia hết 5 mà không chia hết 25 nên từ đây suy ra điều kiện trên không thoả.

Bài 4: Cho dãy số (u_n) có $u_0 = a$ $(a \in \mathbb{N}^*)$, $u_n = u_{n-1} + u_{\lfloor \frac{n}{k} \rfloor}$ với $n \in \mathbb{N}^*$, $k \in \mathbb{N}^*$ là hằng số. Giả sử tồn tại $x \in \mathbb{N}^*$ thoả $u_x, u_{x+1}, \ldots, u_{x+k}$ chia $k^2 + k + 1$ có cùng số dư và $k^2 + k + 1$ là số nguyên tố, chứng minh có vô số số $x \in \mathbb{N}^*$ thoả $u_x, u_{x+1}, \ldots, u_{x+k}$ chia $k^2 + k + 1$ có cùng số dư. ($\lfloor a \rfloor$: phần nguyên của a).

Giả sử tồn tại $x \in \mathbb{N}^*$ là số lớn nhất thoả $u_x, u_{x+1}, \ldots, u_{x+k}$ chia $k^2 + k + 1$ có cùng số dư r $(r \in \mathbb{N}^*, 0 \leq r < k^2 + k + 1)$.

$\Rightarrow u_{kx-1} \equiv u_{kx-1} \ (mod\ k^2 + k + 1)$;

$u_{kx} \equiv u_{kx-1} + u_x \equiv u_{kx-1} + r \ (mod\ k^2 + k + 1)$;

$u_{kx+1} \equiv u_{kx} + u_x \equiv u_{kx-1} + 2r \ (mod\ k^2 + k + 1)$;

...;

$u_{kx+k} \equiv u_{kx+k-1} + u_{x+1} \equiv u_{kx-1} + (k+1)r \ (mod\ k^2 + k + 1)$;

...;

$u_{kx+k^2+k-1} \equiv u_{kx+k^2-k-2} + u_{x+k} \equiv u_{kx-1} + (k^2+1)r \ (mod\ k^2 + k + 1)$.

Nếu $r = 0 \Rightarrow u_{kx-1}, u_{kx}, \ldots, u_{kx+k^2+k-1}$ chia $k^2 + k + 1$ có cùng số dư. (trái giả thiết)

Nếu $r > 0 \Rightarrow (u_{kx-1}, u_{kx}, \ldots, u_{kx+k^2+k-1})$ là một hệ thặng dư đầy đủ mod $k^2 + k + 1$. (do $\gcd(r;\ k^2 + k + 1) = 1$)

$\Rightarrow$ Tồn tại $m \in \{-1;\ 0;\ \ldots;\ k^2 + k - 1\}$ thoả $u_{kx+k} \vdots k^2 + k + 1$.

$\Rightarrow u_{k^2x+km} = u_{k^2x+km-1} + u_{kx+m} \equiv u_{k^2x+km-1} \ (mod\ k^2 + k + 1)$;

$u_{k^2x+km+1} = u_{k^2x+km} + u_{kx+m} \equiv u_{k^2x+km} \ (mod\ k^2 + k + 1)$;

...;

$u_{k^2x+km+k-1} = u_{k^2x+km+k-2} + u_{kx+m} \equiv u_{k^2x+km+k-2} \ (mod\ k^2 + k + 1)$;

Đặt $y = k^2x + km - 1 \Rightarrow y \in \mathbb{N}^*, y > x$ và $u_y, u_{y+1}, \ldots, u_{y+k}$ chia $k^2 + k + 1$ có cùng số dư. (trái giả thiết)

Bài 5: Cho $n \in N^*$. Tồn tại hoán vị $\{a_1; a_2; \ldots; a_n\}$ của $\{1; 2; \ldots; n\}$ sao cho $\{a_1 + 1; a_2 + 2; \ldots; a_n + n\}$ là hệ thặng dư đầy đủ mod n. Chứng minh rằng n lẻ.

Ta có:

$$a_1 + a_2 + \cdots + a_n = \frac{n(n+1)}{2}$$

$$\Rightarrow (a_1 + 1) + (a_2 + 2) + \cdots + (a_n + n) = n(n+1)$$

Mặt khác, do $\{a_1 + 1; a_2 + 2; \ldots; a_n + n\}$ là hệ thặng dư đầy đủ mod n nên $(a_1 + 1) + (a_2 + 2) + \cdots + (a_n + n) \equiv \frac{n(n+1)}{2} \pmod{n}$ (1)

(1) $\Rightarrow \frac{n(n+1)}{2} : n \Rightarrow n$ là số lẻ.

Bài 6: Cho 2 hệ thặng dư đầy đủ theo mod n: $A = \{a_1; a_2; \dots; a_n\}$ và $B = \{b_1; b_2; \dots; b_n\}$. Chứng minh rằng nếu n chẵn thì tập $C = \{a_1 + b_1; a_2 + b_2; \dots; a_n + b_n\}$ không là hệ thặng dư đầy đủ mod n.

Xét 1 tập X bất kỳ gồm n phần tử $x_1, x_2, \dots, x_n$ là 1 hệ thặng dư đầy đủ theo mod n.

Khi đó, vì $\{0;\ 1;\ 2;\ \dots;\ n-1\}$ cũng là hệ thặng dư đầy đủ theo mod n, nên:

$$\sum_{i=1}^{n} x_i \equiv \sum_{j=0}^{n-1} j = \frac{n(n-1)}{2} \ (mod\ n)$$

Nếu n chẵn, đặt $n = 2k, k \in \mathbb{N}^*$, khi đó

$$\frac{n(n\ -\ 1)}{2} = k.(2k-1) \not\equiv 0\ (mod\ 2k) \qquad (1)$$

Vì $A = \{a_1;\ a_2;\ \dots;\ a_n\}$ và $B = \{b_1;\ b_2;\ \dots;\ b_n\}$ là 2 hệ thặng dư đầy đủ theo mod n, nên: $\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \equiv \frac{n(n-1)}{2}\ (mod\ n)$

Giả sử $C = \{a_1 + b_1;\ a_2 + b_2;\ \dots;\ a_n + b_n\}$ là hệ thặng dư đầy đủ mod n với n chẵn, ta có: $\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i \not\equiv 0\ (mod\ n)$ (theo (1)).

Nhưng $\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i \equiv 2.\frac{n(n-1)}{2} = n(n-1) \equiv 0\ (mod\ n)$ (vô lí), vậy điều giả sử là sai, suy ra điều phải chứng minh.

Nhận xét: *Với những bài toán về hệ thặng dư có giả thiết mang tính "mơ hồ" như vậy, việc tìm những yếu tố bất biến là điều quan trọng giúp ta có cơ sở để suy luận.*

Bài 7 *(IMO 2005)*: Cho 1 dãy các số nguyên $a_1, a_2, \dots, a_n$ thỏa mãn 2 điều kiện:
a) $\{a_1, a_2, \dots, a_n\}$ là 1 hệ thặng dư đầy đủ mod n với $n \geq 1$.
b) Có vô số số hạng dương và vô số số hạn âm xuất hiện trong dãy.
Chứng minh rằng mỗi số nguyên xuất hiện đúng 1 lần trong dãy.

Ta sẽ đưa về chứng minh là mọi dãy $a_1, a_2, \dots, a_n$ là các số nguyên liên tiếp với mọi $n \geq 1$.

Ta sẽ chứng minh điều này bằng quy nạp.

Với $n = 1$, điều trên là hiển nhiên.

Với bước quy nạp, ta giả sử dãy $a_1, a_2, \dots, a_n$ là các số nguyên liên tiếp tức là $a_i, a_i + 1, \dots, a_i + n - 1 = a_j$ với $1 \leq i, j \leq n$.

$\Rightarrow$ Rõ ràng a_{n+1} không thể là 1 trong các số của $a_1, a_2, \dots, a_n$ (vì ngược lại thì $a_1, a_2, \dots, a_{n+1}$ không là hệ thặng dư đầy đủ mod $n + 1$).

+ Nếu $a_{n+1} > a_i + n$: Khi đó ta đặt $N = a_{n+1} - a_i \geq n + 1$.
  Khi đó do $a_{n+1} \equiv a_i \ (mod\ N)$ nên $a_1, a_2, \dots, a_N$ không phải là 1 hệ thặng dư đầy đủ mod N (vô lí).
+ Tương tự nếu $a_{n+1} < a_i - 1$: Khi đó ta đặt $N = a_j - a_{n+1} \geq n + 1$ và $a_{n+1} \equiv a_j \ (mod\ N)$, cũng vô lí.

$\Rightarrow a_{n+1}$ phải là $a_i - 1$ hoặc $a_i + n = a_j + 1$.

Từ cả 2 trường hợp này ta thấy rằng $a_1, a_2, \dots, a_{n+1}$ là 1 hệ thặng dư đầy đủ mod $n + 1$.

Vậy khẳng định cũng đúng với $n + 1$.

Vậy theo nguyên lí quy nạp toán học, ta có điều phải chứng minh.

Nhận xét: *Đây là một bài khá khó khi cách đặt N cho 2 trường hợp là không quá tự nhiên và ta cần quan sát nhiều hơn để có thể cảm nhận bài toán và việc đưa bài toán về 1 giả thiết khác dễ dàng hơn giúp ta dễ xử lí bài toán hơn rất nhiều từ một bài toán tưởng chừng như rất khó giải được.*

Bài 8 *(Balkan 1999)*: Cho số nguyên tố $p > 2$ thoả p chia 3 dư 2. Chứng minh tập hợp $A = \{y^2 - x^3 - 1 \mid x, y \in Z^+, x < p, y < p\}$ có nhiều nhất $p-1$ phần tử chia hết cho p.

Giả sử tồn tại 2 số $a, b \in \mathbb{Z}^+$, $a, b < p$, $a \neq b$ thoả $a^3 - b^3 \vdots p \Rightarrow a^3 \equiv b^3 \ (mod\ p)$ và $a \not\equiv b \ (mod\ p)$.

Áp dụng đồng nhất Bezout, tồn tại 2 số $k, n \in \mathbb{Z}$ thoả $ka + np = 1$. (Do $a < p$, p là số nguyên tố nên $\gcd(a;\ p) = 1) \Rightarrow ka \equiv 1 \ (mod\ p) \Rightarrow (ka)^3 \equiv 1 \ (mod\ p) \Rightarrow (kb)^3 \equiv 1 \ (mod\ p)$.

Áp dụng định lí Fermat nhỏ: $(kb)^{p-1} \equiv 1 \ (mod\ p)$. (Do $b < p$, $ka + np = 1$, p là số nguyên tố nên $\gcd(kb;\ p) = 1$)

Gọi $h = ord_p(kb) \Rightarrow 3 \vdots h$ và $p - 1 \vdots h \Rightarrow h \in \{1;\ 3\}$ và $p - 1 \vdots h$.

Mà p chia 3 dư 2 $\Rightarrow p - 1$ chia 3 dư 1 $\Rightarrow\ h = 1 \Rightarrow kb \equiv 1 \equiv ka \ (mod\ p)$

$\Rightarrow k(b - a) \vdots p \Rightarrow b - a \vdots p$. (trái giả thiết)

Vậy không tồn tại 2 số a, b thoả giả sử trên $\Rightarrow \{1^3, 2^3, \dots, (p-1)^3\}$ là hệ thặng dư thu gọn mod $p \Rightarrow$ Với mỗi giá trị y, có nhiều nhất 1 giá trị x thoả $y^2 - x^3 - 1 \vdots p$. (Do $0 < x < p$)

Mà trong tập hợp A có $p - 1$ giá trị của $y \Rightarrow$ Tập hợp A có nhiều nhất $p - 1$ phần tử chia hết cho p. (điều phải chứng minh)

Nhận xét: *Ta thấy với trường hợp $y = 1$ và $y = p - 1$ thì $y^2 - 1 \vdots p$ nên sẽ không tồn tại $x < p$ thoả $y^2 - x^3 - 1 \vdots p$. Vì vậy ta có thể làm chặt bài toán hơn thành tập A có nhiều nhất $p - 3$ phần tử chia hết cho p.*

Bài 9: 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.

Dễ thấy với x, y nguyên mà $x^3 \equiv y^3 \ (mod\ 191) \Rightarrow x \equiv y \ (mod\ 191)$.

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

Thật vậy, vì :

$$27P(n_1) = (3n_1 - 11)^3 - 18.191.n_1 + 1331 + 27m$$
$$27P(n_2) = (3n_2 - 11)^3 - 18.191.n_2 + 1331 + 27m$$

Nên:

$$P(n_1) \equiv P(n_2) \ (mod\ 191)$$
$$\Leftrightarrow 27P(n_1) \equiv 27\ P(n_2) \ (mod\ 191)$$
$$\Leftrightarrow (3n_1 - 11)^3 \equiv (3n_2 - 11)^3 \ (mod\ 191)$$
$$\Rightarrow 3n_1 - 11 \equiv 3n_2 - 11 \ (mod\ 191)$$
$$\Leftrightarrow n_1 \equiv n_2 \ (mod\ 191)$$

Với mọi $n_1, n_2 \in A = \{1;\ 2;\ 3;\ \ldots;\ 191\}$ (A là một hệ đầy đủ mod 191), $n_1 \neq n_2$ ta có $P(n_1) \not\equiv P(n_2) \ (mod\ 191)$.

$\Rightarrow B = \{P(1);\ P(2);\ \ldots;\ P(191)\}$ là một hệ đầy đủ mod 191.

Từ đó suy ra $\exists n \in A = \{1; 2; 3; \ldots; 191\}$ sao cho:

$P(n) \equiv 191 \ (mod\ 191) \Leftrightarrow 191 \mid P(n)$.

Bài 10: Gọi a, b, c là các số nguyên dương sao cho $\frac{a^2 + b^2 + c^2}{ab + bc + ca}$ là 1 số nguyên. Chứng minh số này không bao giờ là bội của 3.

Ta giả sử $a^2 + b^2 + c^2 = 3n(ab + bc + ca)$ với n là số nguyên dương.

$\Rightarrow (a + b + c)2 = (3n + 2)(ab + bc + ca).$

Ta chia a, b, c cho (a, b, c) nên ta có thể giả sử $(a, b, c) = 1.$

Đặt $3n + 2 = p_1^{a_1}.p_2^{a_2} \ldots p_k^{a_k}$ là phân tích tiêu chuẩn của số $3n + 2.$

$\Rightarrow$ Tồn tại p_i để $p_i \equiv 2 \ (mod\ 3)$ và a_i lẻ (do ngược lại thì$p_i^{a_i} \equiv 1 \ (mod\ 3)$ với mọi i chạy từ 1 đến n nên $3n + 2 \equiv 1 \ (mod\ 3)$ (vô lí))

Ta cố định i ở trên $\Rightarrow a + b + c$ chia hết p_i mà lũy thừa của p_i trong phân tích tiêu chuẩn của $a + b + c$ là chẵn nhưng phân tích tiêu chuẩn của p_i trong $3n + 2$ là lẻ

$\Rightarrow ab + bc + ca$ chia hết $p_i.$

$\Rightarrow ab + bc + ca \equiv ab + c(a + b) \equiv ab - (a + b)^2 = -(a^2 + ab + b^2) \equiv 0 \ (mod\ p)$

$\Rightarrow a \vdots p, b \vdots p$ nên $c \vdots p$ (vô lí do $(a, b, c) = 1$).

Vậy ta có điều phải chứng minh.

Bài 11: Cho số nguyên tố $p > 3$ và m, n là 2 số nguyên tố cùng nhau thỏa mãn $\frac{m}{n} = \sum_{i=1}^{p-1} \frac{1}{i^2}$. Chứng minh rằng m chia hết cho p.

Trước khi giải bài toán, ta cần hiểu về khái niệm số hữu tỉ đồng dư:
Cho số nguyên dương n, ta định nghĩa tập con $\mathbb{Z}_{(n)}$ của $\mathbb{Q}$ như sau: $\mathbb{Z}_{(n)} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, (b, n) = 1\right\}$.
Hai số hữu tỉ x, y thuộc $\mathbb{Z}_{(n)}$ gọi là đồng dư theo mod n nếu $x - y = n.z$ với z là 1 số hữu tỉ nào đó thuộc $\mathbb{Z}_{(n)}$, kí hiệu là $x \equiv y \ (mod\ n)$ trong $\mathbb{Z}_{(n)}$.
Quay trở lại bài toán, với $\{0;\ 1;\ 2;\ 3;\ \ldots;\ p-1\}$ là hệ thặng dư đầy đủ theo mod p, xét 2 số i, j bất kì thuộc $\{1;\ 2;\ 3;\ \ldots\ ; p-1\}$ sao cho $i.j \equiv 1 \ (mod\ p)$.
Khi đó theo khái niệm về số hữu tỉ đồng dư, ta có thể viết thành $i \equiv \frac{1}{j} \ (mod\ p)$.
Kéo theo $\left\{0; \frac{1}{1}; \frac{1}{2}; \ldots; \frac{1}{p-1}\right\}$ cũng là hệ thặng dư đầy đủ theo mod p, vì thế:

$$\sum_{i=1}^{p-1} \frac{1}{i^2} \equiv \sum_{i=1}^{p-1} i^2 = \frac{p(p-1)(2p-1)}{6} \equiv 0 \ (mod\ p)$$

(vì $p > 3$ nên $(p;\ 6) = 1$) $(*)$
Với $(p-1)!^2 . \sum_{i=1}^{p-1} \frac{1}{i^2}$ là 1 số tự nhiên, ta có $(p-1)!^2 . \sum_{i=1}^{p-1} \frac{1}{i^2}$ chia hết cho p.
$\Rightarrow (p-1)!^2 . \frac{m}{n} \vdots p$, theo định lý Wilson, $(p-1)!^2 \equiv (-1)^2 \equiv 1 \ (mod\ p)$, do vậy m chia hết cho p.

Nhận xét:

- Ta có thể thay số 2 trong đề và đánh giá $(*)$ thành 1 số k bất kì thỏa $1 \leq k < p-1$, có thể chứng minh điều này bằng số hữu tỉ đồng dư và căn nguyên thủy.

- Đối với những bài toán chứa biểu thức tổng của các phân số($\sum_{i=1}^{p-1} \frac{1}{i^2}$ là 1 ví dụ), việc sử dụng hệ thặng dư để đưa về dạng đánh giá trên số nguyên cũng là 1 hướng thường nghĩ đến.

Bài 12: Cho số nguyên tố $p > 3$. Chứng minh rằng số dư của phép chia $\prod_{j=1}^{p}(j^2+1)$ cho p chỉ có thể là 0 hoặc 4.

Xét các lớp thặng dư $\mathbb{Z}_p$ và mở rộng trường $\mathbb{Z}_p$ thành trường $\mathbb{Z}_p(\alpha)$ với $\alpha^2 = -1$.

Ta có: $\prod_{j=1}^{p}(j^2+1) = \prod_{j=1}^{p}(j-\alpha).\prod_{j=1}^{p}(j+\alpha)$ $(*)$

Xét đa thức $f(x) = \prod_{j=1}^{p}(x+j)$ và đa thức $G(x) = x^p - x - f(x)$, nhận xét rằng $deg G(x) \le p-1$ (1)

Theo định lý Fermat nhỏ, ta có $x^p - x \vdots p$ với mọi x thuộc $\overline{1,p}$, đồng thời $f(x) \equiv p! \equiv 0 \ (mod\ p)$ với mọi x thuộc $\overline{1,p}$.

Do vậy, phương trình đồng dư $G(x) \equiv 0 \ (mod\ p)$ có p nghiệm $1,2,\dots,p$, cùng với nhận xét (1), ta có: $G(x) \equiv 0 \ (mod\ p)$, hay $f(x) = \prod_{j=1}^{p}(x+j) \equiv x^p - x \ (mod\ p)$ $(**)$

Từ đánh giá $(*)$, ta có:

$$\prod_{j=1}^{p}(j^2+1) \equiv (\alpha^p - \alpha)\left((-\alpha)^p + \alpha\right) \equiv \left((-1)^{\frac{p-1}{2}} - 1\right)^2 \ (mod\ p)$$

Vậy số dư của phép chia $\prod_{j=1}^{p}(j^2+1)$ cho p chỉ có thể là 0 hoặc 4.

Nhận xét:

Việc đánh giá bằng số phức cũng là 1 công cụ hữu hiệu giúp ta giảm thiểu những sai số khi đánh giá các bài toán về hệ thặng dư, bên cạnh công cụ đồng dư đa thức như đánh giá $(**)$.

IV

Tài liệu tham khảo

[1] Ứng dụng hệ thặng dư đầy đủ - Gặp Gỡ Toán Học 2019

[2] https://tailieu.vn/doc/chuong-6-he-thang-du-va-dinh-ly-thang-du-trung-hoa-1457704.html

[3] https://pdfcoffee.com/thang-du-day-du-pdf-free.html

[4] https://artofproblemsolving.com/community/c13_contest_collections

[5] Tham khảo tài liệu của một số thầy cô khác.

[6] Lại là một link feedback khác đây: *link feedback here*