Mai Xuân Việt – Email: xuanviet15@gmail.com – Tel : 01678336358 – 0938680277 – 0947572201

GIỚI THIỆU VỀ ĐỒNG DƯ VÀ HỆ ĐỒNG DƯ

Đồng dư và phương trình đồng dư được sử dụng khá nhiều trong chương trình phổ thông, đặc biệt là các cuộc thi HSG các cấp. Nhưng không ít học sinh còn mơ hồ về khái niệm này. Sau đây, tôi xin có vài lời giới thiệu về đồng dư thức và phương trình đồng dư để mọi các bạn cùng tham khảo.

I-Giới thiệu về đồng dư.

Đồng dư là khái niệm cực kì cơ bản và đầy sức mạnh trong lý thuyết số. Khái niệm này do nhà toán học Đức Gauss (1777-1855), được mạnh danh là ông vua toán học, một t rong những nhà toán học lỗi lạc của nhân loại đưa ra. Nó được trình bày trong tác phẩm "Disquistiones Arthmeticcate" của ông xuất bàn năm 1801 khi ông mới 24 tuổi.

1/ Định nghĩa: Cho số nguyên dương n. Hai số nguyên $a,b\in\mathbb{Z}$ được gọi là đồng dư theo mol n và khi đó ta kí hiệu $a\equiv b\,(\mathrm{mod}\,n)$ nếu khi chia cho n chúng cho cùng một số dư. Từ đó ta có: $a-b\vdots n$ hay $a=b+kn\ (k\in\mathbb{Z})$.

2/ Tính chất: Ký hiệu $\equiv$ nhằm nhấn mạnh rằng đồng dư có nhiều tính chất giống với đẳng thức.

a) Nếu $a\equiv b\,(\mathrm{mod}\,n)$, $c\equiv d\,(\mathrm{mod}\,n)$ thì $a\pm c\equiv b\pm d\,(\mathrm{mod}\,n)$, $ac\equiv bd\,(\mathrm{mod}\,n)$.

b) Với $\forall k\in\mathbb{Z}^*, a\equiv b\,(\mathrm{mod}\,n)\Rightarrow a^k\equiv b^k\,(\mathrm{mod}\,n)$

c) Nếu $ac\equiv bc\,(\mathrm{mod}\,n), (c,n)=1$ thì $a\equiv b$.

3/ Hệ thặng dư.

a) **Hệ thặng dư đầy đủ.** Cho tập hợp $A=\{a_1,a_2,...,a_n\}$. Giả sử r_i với $0\le r_i\le n-1$ là số dư khi chia a_i cho r_i. Nếu tập các số dư trùng với tập $\{0,1,2,....,n-1\}$ thì ta A là hệ thặng dư đầy đủ (gọi tắt là HĐĐ) theo mod n. Dễ thấy: Tập A lập thành một HĐĐ (mod n) nếu và chỉ nếu $i\ne j$ thì $a_{\partial i}\ne a_j$ (mod n). Từ định nghĩa ta suy ra một số tính chất sau:

- ☞ Với $\forall m\in\mathbb{Z}, \exists! a_i\in A$ sao cho $a_i\equiv m\,(\mathrm{mod}\,n)$
- ☞ Với $\forall a\in\mathbb{Z}$ thì tập A+a $=\{a_1+a,a_2+a,....,a_n+a\}$ cũng lập thành một HĐĐ theo mod n.
- ☞ Nếu $c\in\mathbb{Z},(c,n)=1$ thì tập cA $=\{ca_1,ca_2,.....,ca_n\}$ cũng lập thành HĐĐ.

b) **Hệ thặng dư thu gọn.** Cho $B=\{b_1,b_2,...,b_k\}$ là một tập gồm k số nguyên và $(b_i,n)=1$ với $i=\overline{1,k}$. Giả sử $b_i=q_in+r_i$,$1\le r_i<n$. Khi đó dễ thấy $(r_i,n)=1$. Nếu tập $\{r_1,r_2,....,r_k\}$ bằng tập K gồm tất cả các số nguyên dương bé hơn n và nguyên tố với n thì B gọi là hệ thặng dư thu gọn mod n, gọi tắt là hệt thu mod n. Dễ thấy một tập hợp $B=\{b_1,b_2,...,b_m\}$ gồm m số nguyên lập thành một hệ thu gọn khi và chỉ khi:

- ☞ $(b_i,n)=1$
- ☞ $b_i\equiv b_j\ (\mathrm{mod}\,n)$
- ☞ Số phần tử của B là $\phi(n)$ trong đó $\phi(n)$ là hàm Euler.

c) **Hàm Euler.** Đây là hàm đếm số các số nguyên tố cùng nhau với số n cho trước, kí hiệu là $\phi(n)$. Dễ dàng chứng minh được hàm Euler có tính nhân tính, tức là $\phi(mn)=\phi(m).\phi(n)$.

Ta sẽ đi tìm công thức tính của hàm Euler như sau:

Giả sử ta phân tích n ra thừa số nguyên tố là $n=\prod_{i=1}^{k}p_i^{s_i}=p_1^{s_1}.p_2^{s_2}....p_k^{s_k}$.

Ta chú ý rằng nếu p là một số nguyên tố và một số i bất sao cho $(p,i)=1$ thì i không chia hết cho p. Số các số chia hết cho p mà không vượt quá p^s là p^{s-1}. Khi đó ta có $\phi(p^s)=p^s-p^{s-1}=p^s\left(1-\frac{1}{p}\right)$. Lúc đó

$$\phi(n)=\phi\left(p_1^{s_1}.p_2^{s_2}.....p_k^{s_k}\right)=\phi\left(p_1^{s_1}\right).\phi\left(p_2^{s_2}\right).....\phi\left(p_k^{s_k}\right)=p_1^{s_1}\left(1-\frac{1}{p_1}\right).p_2^{s_2}\left(1-\frac{1}{p_2}\right).....p_k^{s_k}\left(1-\frac{1}{p_k}\right)=n.\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).$$

4/ Một số định lý về đồng dư.

❶ Định lý Euler. Cho n là số nguyên và a$\in\mathbb{Z}$ sao cho $(a,n)=1$. Khi đó, ta có $a^{\phi(n)}\equiv 1\ (\mathrm{mod}\,n)$, tổng quát với nọi số nguyên $a\in\mathbb{Z}$, ta có $a^n\equiv a^{n-\phi(n)}\ (\mathrm{mod}\,n)$

❷ Định lý Fecma nhỏ. Nếu p là một số nguyên tố và $a\in\mathbb{Z}$ sao cho $(a,p)=1$. Khi đó $a^{p-1}\equiv 1\,(\mathrm{mod}\,p)$. Thực chất đây cũng là một hệ quả của định lý Euler vì $\phi(p)=p-1$.

❸ Định lý Wilson. Cho n>1 là số nguyên dương. Khi đó n là số nguyên tố khi và chỉ khi $(n-1)!\equiv -1\ (\mathrm{mod}\,n)$.

❹ Định lý thặng dư Trung Hoa. Cho k số nguyên dương $n_1,n_2,....,n_k$ đôi một nguyên tố cùng nhau và k số nguyên bất kì $a_1,a_2,.....,a_k$. Khi đó tồn tại nguyên a thoả mãn $a\equiv a_i\ (\mathrm{mod}\,n)\quad\forall i=1,2,...,k\quad(1)$

Số nguyên b thoả mãn (1) khi và chỉ khi $b \equiv a \pmod{n}$ ở đó $n = n_1.n_2...n_k$.

5/ Số chính phương (mod n). Cho số nguyên dương n. Số nguyên a gọi là số chính phương mod n nếu tồn tại $x \in \mathbb{Z}$ sao cho $x^2 \equiv a \pmod{n}$. Rõ ràng một số chính phương sẽ là số chính phương mod n với mọi n vì luôn tồn tại $x = \sqrt{a}$ thoả đề. Ví dụ : 2 là một số chính phương mod 7 vì $3^2 \equiv 2 \pmod{7}$.

⊕Trường hợp n = p là một số nguyên tố.

Hiển nhiên nếu $p \mid a \Leftrightarrow a \equiv 0 \pmod{p}$ thì a là một số chính phương mod p, ta chỉ xét $(a, p) = 1$.

Một số định lý:

❖ Nếu p=2 thì mọi số a lẻ đều là số chính phương (mod 2)

❖ Nếu p > 2, khi đó a là số chính phương (mod p) khi và chỉ khi $a^{(p-1)/2} \equiv 1 \pmod{p}$, a không chính phương (mod p) khi và chỉ khi $a^{(p-1)/2} \equiv -1 \pmod{p}$.

❖ Nếu p là một số nguyên tố lẻ thì :

- Tích của hai số chính phương (mod p) là số chính phương (mod p)
- Tích của hai số không chính phương (mod p) là số chính phương (mod p)
- Tích của một số không chính phương (mod p) với một số chính phương (mod p) là một số không chính phương (mod p).
- (-1) là một số chính phương (mod p) khi và chỉ khi p = 4k+1.
- Trong tập $S = \{1, 2, ..., p-1\}$ có $(p-1)/2$ số chính phương (mod p) và $(p-1)/2$ số không chính phương (mod p).
- Gọi n là số các số chẵn nằm trong khoảng $(p/2; p)$, khi đó $2^{(p-1)/2} \equiv (-1)^n \pmod{p}$.

❖ Cho $p = 4k \pm 1$ là một số nguyên tố lẻ. Khi đó $2^{(p-1)/2} \equiv (-1)^k \pmod{p}$, từ đó suy ra 2 là số chính phương mod p khi và chỉ khi $p = 8k \pm 1$.

❖ Cho p là số nguyên tố lẻ $(p, 3) = 1$. Gọi n là số các số là bội của 3 trong khoảng $(p/2; p)$. Khi đó $3^{(p-1)/2} \equiv (-1)^n \pmod{p}$. Từ đây ta cũng có hệ quả: Nếu $p = 6k \pm 1$ là số nguyên tố. Khi đó $3^{(p-1)/2} \equiv (-1)^k \pmod{p}$, suy ra 3 là số chính phương (mod p) khi và chỉ khi $p = 12t \pm 1$.

❖ ***(Luật tương hỗ Gauss).*** Cho p, q là hai số nguyên tố lẻ phân biệt. Khi đó:

❶ Nếu có ít nhất 1 trong 2 số có dạng 4k+1 thì p là số chính phương (mod q) khi và chỉ khi q là số chính phương (mod p).

❷ Nếu cả hai số có dạng 4k+3 thì p là số chính phương (mod q) khi và chỉ khi q là số không chính phương (mod p)

Kí hiệu Legendre. Giả sử p là một số nguyên tố lẻ, a là số nguyên không âm. Kí hiệu Legendre $\left(\frac{a}{p}\right)$ được định nghĩa như sau : $\left(\frac{a}{p}\right) = \begin{cases} 1 & neu\ a\ la\ so\ chinh\ phuong \bmod p \\ -1 & neu\ a\ la\ so\ khong\ chinh\ phuong \bmod p \end{cases}$.

Với kí hiệu này ta có thể viết các định lý trên một cách ngắn gọn là:

①. $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$

②. Nếu $a \equiv b \pmod{p}$ thì $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

③. $\left(\frac{a}{p}\right).\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

④. $\left(\frac{a^2}{p}\right) = 1$.

⑤. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

⑥. $\left(\frac{2}{p}\right) = (-1)^{(p^2-p)/8}$

⑦. (Luật tương hỗ). Nếu a=q là số nguyên tố lẻ thì $\left(\frac{q}{p}\right).\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$.

⊕Trường hợp n là hợp số. Phân tích n ra thừa số nguyên tố ta được $n = \prod_{i=1}^{k} p_i^{s_i}$.

Bổ đề: Số nguyên a với (a, n) = 1 là số chính phương (mod p) khi và chỉ khi với mỗi p_i, a là số chính phương (mod p).

Chứng minh: Giả sử a là số chính phương (mod n). Khi đó tồn tại $x \in \mathbb{Z}$ sao cho $x^2 \equiv a \pmod{n} \Rightarrow x^2 \equiv a \pmod{p_i^{s_i}}$. Vậy a là số chính phương (mod $p_i^{s_i}$). Đảo lại giả sử với mỗi số i=1,2,...,k a là số chính phương (mod $p_i^{s_i}$). Khi đó tồn tại $x \in \mathbb{Z}$ soa cho $x_i^2 \equiv a \pmod{p_i^{s_i}}$. Theo định lý thặng dư Trung Hoa tồn tại $x \in \mathbb{Z}$ sao cho $x \equiv x_i \pmod{p_i^{s_i}}$ với mỗi i = 1,2,....,k . Thành thử $x^2 \equiv x_i^2 \equiv a \pmod{p_i^{s_i}}$. Suy ra $x^2 \equiv a \pmod{n}$. Vậy a là số chính phương mod n.

❖ **Định lý 1:** Giả sử $n = 2^s$, s>1 và a là số nguyên lẻ. Khi đó a là số chính phương (mod n) khi và chỉ khi:

i) $a \equiv 1 \pmod{4}$ nếu s = 2.

ii) $a \equiv 1 \pmod{8}$ nếu $s \geq 3$.

❖ **Định lý 2:** Giả sử $n = p^s$ với p là số nguyên tố lẻ. Khi đó a là số chính phương mod n khi và chỉ khi a là số chính phương mod p.

Kí hiệu Jacobi: là ký hiệu mở rộng của ký hiệu Lagendre. Cho n là một số nguyên dương lẻ với phân tích tiêu chuẩn $n = \prod_{i=1}^{k} p_i^{s_i}$ (p_i là các số nguyên tố khác nhau). Với (a, n)=1 ta định nghĩa Jacobi như sau: $\left(\frac{a}{n}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)$.

Dễ thấy rằng nếu a là số chính phương mod n thì $\left(\frac{a}{p_i}\right) = 1, \forall i \Rightarrow \left(\frac{a}{n}\right) = 1$ nhưng ngược lại không đúng.

6/ Phương trình đồng dư. Cho $f(x)$ là đa thức với hệ số nguyên và m là một số nguyên dương. Số nguyên a được gọi là nghiệm của phương trình đồng dư $f(x) \equiv 0 \pmod{m}$ nếu $f(a) \equiv 0 \pmod{m}$.

❖ **Định lý 1:** Cho đa thức $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ có hệ số nguyên. Xét phương trình đồng dư $f(x) \equiv 0 \pmod{p}$ (*), trong đó m=p là một số nguyên tố. Nếu pt (*) có n+1 nghiệm phân biệt (mod p) thì mọi hệ số $a_i, i = \overline{1,n}$ đều chia hết cho p. Nói riêng khi đó $f(a) \equiv 0 \pmod{p}, \forall a \in \mathbb{Z}$.

❖ **Định lý 2:** Giả sử $m = m_1 m_2 .....m_k$ và các số m_i đôi một nguyên tố cùng nhau, khi đó:

i) a là nghiệm của pt (*) khi và chỉ khi với mọi i = 1,2,....,k là nghiệm của pt $f(x) \equiv 0 \pmod{m_i}$ (**).

ii) Kí hiệu $N(m), N(m_i)$ tương ứng là số nghiệm phân biệt (mod m) của nghiệm phân biệt (mod m_i) của (**) thì khi đó ta có $N(m) = N(m_1).N(m_2).....N(m_k)$.

II- Một số bài toán ứng dụng.

✪**Bài 1:** ***(Vietnam MO 2004, Bảng A).*** Kí hiệu $S(n)$ là tổng tất cả các chữ số của n trong cơ sở 10. Xét tất cả các số nguyên dương m thoả mãn m là bội của 2003, tìm giá trị bé nhất có thể có của $S(m)$.

Giải: Đặt p = 2003, p là số nguyên tố. Rõ ràng $S(n) > 1$ vì 10^k không chia hết cho p. Giả sử tồn tại n là bội của p và $S(n) = 2$. Suy ra tồn tại k để $10^k \equiv -1 \pmod{p}$. Chú ý rằng $2^{10} = 1024 \equiv 10^7 \pmod{p}$ nên $\left(2^{5k}\right)^2 = 2^{10k} \equiv 10^{7k} \equiv \left(10^k\right)^7 \equiv -1 \pmod{p}$. Vậy -1 là số chính phương mod p. Mâu thuẫn vì p không có dạng 4k+1. Tiếp theo ta chứng minh tồn tại n là bội của 3 mà $S(n) = 3$. Ta có $10^7 \equiv 2^{10} \Rightarrow 2.10^{700} \equiv 2^{1001} = 2^{(p-1)/2} \equiv -1 \pmod{p}$ vì $p \neq 8t \pm 1$. Vậy $n = 2.10^{700} + 1$ là bội của p và $S(n) = 3$. Vậy giá trị nhỏ nhất của $S(n) = 3$.

✪**Bài 2:** Xét số Fecma $F = F_n = 2^{2^n} + 1, n \geq 1$. Chứng minh rằng F là số nguyên tố khi và chỉ khi $3^{(F-1)/2} + 1 \vdots F$.

Giải: Dễ thấy F không có dạng $12k \pm 1$. Do đó nếu F là số nguyên tố thì 3 là số không chính phương (mod F). Vậy $3^{(F-1)/2} \equiv -1 \pmod{F}$ tức là $3^{(F-1)/2} + 1 \vdots F$.

Đảo lại giả sử $3^{(F-1)/2} \equiv -1 \pmod{F}$. Gọi h là cấp của 3 (mod F). Khi đó $h \mid (F-1) = 2^{2^n}$. Vậy $h = 2^t, t \leq 2^n$. Nếu $t \leq 2^n - 1$ thì $h \mid (F-1)/2$ do đó $3^{(F-1)/2} \equiv 1 \pmod{F}$, mau thuẫn với điều dã giả sử. Vậy $t = 2^n \Leftrightarrow h = F - 1$. Vì $h \mid \phi(F)$ nên $(F-1) \mid \phi(F) \Rightarrow F - 1 = \phi(F)$. Vậy F là số nguyên tố.

✪**Bài 3:** Giải phương trình $f(x) = x^4 + 2x^3 + 8x + 9 \equiv 0 \pmod{35}$.

Giải: Phương trình $f(x) \equiv 0 \pmod{5}$ có tập nghiệm là $C_1 = \{1;4\}$. Phương trình $f(x) \equiv 0 \pmod{7}$ có tập nghiệm $C_2 = \{3;5;6\}$. Ta phải giải hệ $\begin{cases} a \equiv a_1 \pmod{5} \\ a \equiv a_2 \pmod{5} \end{cases}$. Từ định lý thặng dư Trung Hoa ta tìm được a = $21a_1 + 15a_2$. Từ đó lần lượt cho $a_1 \in C_1, a_2 \in C_2$ ta tìm được $A = \{6;19;24;26;31;34\}$.

Name : **Mai Xuân Việt**
Address : **Đội II – thôn Dương Quang – Xã Đức Thắng – Huyện Mộ Đức – Tỉnh Quảng Ngãi .**
Email : xuanviet15@gmail.com
Tel : **01678336358 – 0938680277 – 0947572201**