Đồng Dư Thức

1.Định nghĩa:

Cho số nguyên dương $n>1$. Hai số nguyên a,b được gọi là dồng dư theo modulo n nếu chúng cho cùng số dư khi chia cho n.

Kí hiệu: $a \equiv b \pmod n$

2.Tính chất:

a)Các tính chất:

+Nếu

$$\begin{cases} a \equiv a' \pmod n \\ b \equiv b' \pmod n \end{cases}$$

Thì ta có :

$$a+b \equiv a'+b' \pmod n$$

$$a-b \equiv a'-b' \pmod n$$

$$a.b \equiv a'.b' \pmod n$$

$$a^k \equiv b^k \pmod n$$

Như vậy ta có thể cộng, trừ, nhân, và nâng lên lũy thừa các đồng dư thức theo cùng một modun

b)Luật giản ước:

+Nếu $a.c \equiv a'.c \pmod n$

và $(c,n)=1$

thì $a \equiv a' \pmod n$

Bây giờ chúng ta sẽ đi vào một số vấn đề đồng dư thức có nhiều ứng dụng trong khi giải các bài toán số học

3.Hệ thặng dư đầy đủ

Định nghĩa: Mỗi tập hợp A nào đó được gọi là một hệ thăng dư đầy đủ (mod n) nếu vớI bất kì số x∈ Z tồn tạI duy nhất một a∈ A để $x \equiv a \pmod n$

Chẳng hạn A=$\{0,1,2,.....,n-1\}$ là một hệ thặng dư đầy đủ theo mod n

Dễ thấy :

Một tập A=$\{a_1,a_2,.....,a_n\}$gồm n số sẽ là một hệ thăng dư đầy đủ theo modun n Khi và chỉ khi $a_i \cong a_j \pmod n$ (ta tạm kí hiệu "không đồng dư" là $\cong$) với $i \neq j$ và i,j∈ $\{1,2,.....,n\}$

Thí dụ 1:

Xét dãy $U_k = \dfrac{k(k+1)}{2}$ (k=1,2…) .Chứng minh rằng nếu $n=2^s$ (s>1) thì trong dãy trên có thể chọn được một hệ thăng dư đầy đủ modun n.

Giải:Xét n số $U_{2k-1}(k=1,2,...,n)$

Ta chỉ cần chứng minh với mọi $1 \le i < j \le n$ thì

$U_{2i-1} \cong U_{2j-1} \pmod n$

Giả sử ngược lại ∃ $1 \le i < j \le n$ mà

$U_{2i-1} \equiv U_{2j-1} (\text{mod}\, n)$

$\Leftrightarrow (2i-1)i \equiv (2j-1)j (\text{mod}\, n)$

$\Leftrightarrow (j-i)(2j+2i-1) \equiv 0 (\text{mod}\, n) (1)$

Do $n = 2^s$ (s>1) nên n không có ước lẻ.

Từ (1) $\Rightarrow j \equiv i (\text{mod}\, n)$ (Vô lý)

Thí dụ 2: Cho 2 hệ thặng dư đầy đủ modun n

$A = \{a_1, a_2, ..., a_n\}$

$B = \{b_1, b_2, ..., b_n\}$

Chứng minh rằng:

Nếu n là số chẵn thì tập $A + B = \{a_1 + b_1, a_2 + b_2, ..., a_n + b_n\}$ không là hệ thặng dư đầy đủ modulo n

Giải: Nếu A là hệ thặng dư đầy đủ thì

$$a_1 + a_2 + ... + a_n \equiv 1 + 2 + ... + n \equiv \frac{n(n+1)}{2} (\text{mod}\, n)$$

Vì n chẵn và $(n, n+1) = 1$ nên $\frac{n(n+1)}{2} \cong 0 (\text{mod}\ n)$

Nếu $A + B$ là hệ thặng dư đầy đủ vớI n chẵn thì

$(a_1 + b_1) + (a_2 + b_2) + ... + (a_n + b_n) \cong 0 (\text{mod}\, n)$ nhưng

$$(a_1 + b_1) + (a_2 + b_2) + ... + (a_n + b_n) = (a_1 + a_2 + ... + a_n) + (b_1 + b_2 + ... + b_n)$$

$$\equiv \frac{n(n+1)}{2} + \frac{n(n+1)}{2} = n(n+1) \equiv 0 (\text{mod}\, n)$$

Đây là điều vô lý.

4. Định lý Fermat:

Cho số nguyên tố p.Khi đó với mọi số nguyên a ta đều có:

$$a^p \equiv a (\text{mod}\, p)$$

Ngoài ra nếu (a,p)=1 thì $a^{p-1} \equiv 1 (\text{mod}\, p)$

Chứng minh:

Định lý Fermat có khá nhiều cách chứng minh, ở đây chúng tôi sẽ giới thiệu đến các bạn cách chứng minh không phải ngắn nhất, tuy nhiên ý tưởng trong cách chứng minh là nên học hỏi.

Nếu $a \vdots p$ thì ta có ngay điều phải chứng minh.

Nếu $a \nmid p \Rightarrow (a, p) = 1$.

Trước hết chúng ta nhắc lại một tính chất của số nguyên tố.

" Cho p là một số nguyên tố, khi đó tập các số $ai, i = \overline{1, p-1}$ là hệ thặng dư thu gọn modulo p, trong đó $(a, p) = 1$"

Từ tính chất trên ta suy ra $\prod_{i=1}^{p-1} ai \equiv \prod_{i=1}^{p-1} i \Rightarrow a^{p-1} \equiv 1 (\text{mod}\, p) \Rightarrow a^p \equiv a (\text{mod}\, p)$.

Tóm lại trong mọi trường hợp ta đều có điều cần chứng minh.

5. Định lý Euler:

Cho số nguyên dương n.Gọi $j(n)$ là số các số nguyên dương không vượt quá n và nguyên tố cùng nhau với n. Khi đó với mọi số nguyên dương n,ta có:

$$a^{j(n)} \equiv 1 (\mathrm{mod}\, n)$$

Ý tưởng chứng minh định lý Euler là khá tương tự so với định lý Fermat, các bạn hãy thử sức xem **J**.

6. Định lý Wilson

Cho số nguyên tố p ta có định lý sau :

$$(p-1)!+1 \equiv 0 (\mathrm{mod}\, p)$$

Chứng minh:

Nhận thấy định lý đúng với $p=2$.

Trong trường hợp p là số nguyên tố lẻ .

Xét phương trình đồng dư:

$(x-1)(x-2)...(x-p+1)-(x^{p-1}-1)$.

Nhận thấy rằng phương trình trên có $p-1$ nghiệm theo modulo p. Mà bậc của đa thức trên bé hơn $p-1$ nên đa thức này chia hết cho p với mọi x.

Như vậy các hệ số của đa thức chia hết cho p. Xét hệ số tự do:

$(-1)^{p-1}(p-1)! + 1 \vdots p \Rightarrow (p-1)! + 1 \vdots p$($p-1$ chẵn do p là số nguyên tố lẻ)

7.Bài tập ví dụ:

<u>Bài 1:</u>Cho p là số nguyên tố có dạng 4k+3. Cho các số nguyên x và y. Biết $x^2+y^2 \vdots p$ Chứng minh rằng: x và y chia hết cho p.

Giả sử (x,p)=1 thì ta thấy (y,p)=1

Ta có $x^2 \equiv -y^2 (\mathrm{mod}\, p)$

$\Leftrightarrow x^{4k+2} \equiv -y^{4k+2} (\mathrm{mod}\, p)$

$\Leftrightarrow 1 \equiv -1 (\mathrm{mod}\, p)$

(Theo định lý Fermat)

Do đó $(x,p) \neq 1$ nên x chia hết cho p và dễ thấy y cũng chia hết cho p

<u>Bài 2:</u>Chứng minh rằng: với $n>1$ thì $2^{3^n}+1 \vdots 3^{n+1}$

Theo nhị thức Newton:

$2^{3^n}+1=(3-1)^{3^n}+1=3^{n+1}.A$

Từ đây ta suy ra đpcm

Bài tập luyện tập

<u>Bài 1:</u>

Cho $(a,b)=1$. Chứng minh rằng mọi ước lẻ $A=a^{2^n}+b^{2^n}$ của đều có dạng $2^{n+1}k+1$

<u>Bài 2:</u>

Chứng minh rằng $\forall n \in N, n \geq 5$ thì $\left[\frac{(n-1)!}{n(n+1)}\right]$ là số chẵn.

<u>Bài 3:</u>

Cho $x \in N^*: 2^x+1 \vdots x^2$

Chứng minh rằng: $x = 3$
Gợi ý: có thể dùng ví dụ 2.

Bài 4:

Cho p, q là 2 số nguyên tố cùng nhau. Hãy tính tổng:

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

Bài 5:

Chứng minh rằng:

$$\begin{cases} x^2 + 6y^2 = z^2 \\ 6x^2 + y^2 = t^2 \end{cases}$$

không có nghiệm nguyên.

Bài 6:

Chứng minh rằng $1! + 2! + ... + n!$ là số chính phương khi và chỉ khi $n = 3.$