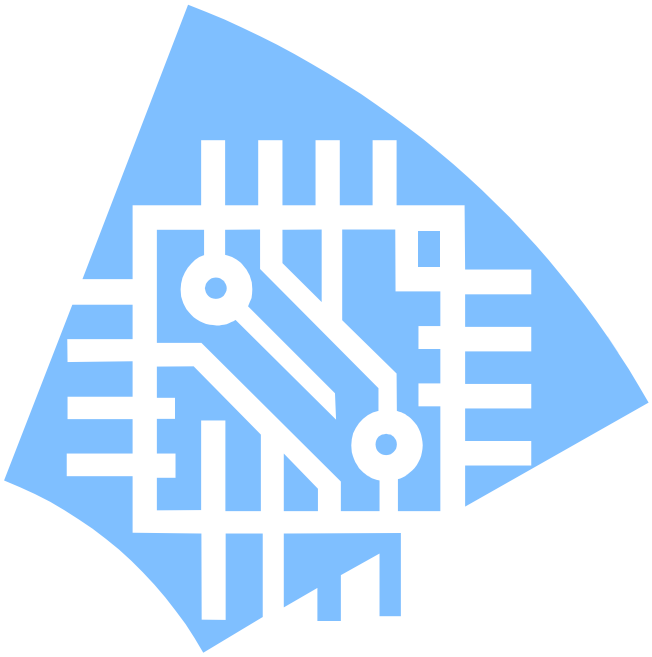
TRƯỜNG THPT CHUYÊN NGUYỄN BỈNH KHIÊM
NHÓM CHUYÊN ĐỀ 11T1

☆ ☆ ☆

MỘT SỐ VẤN ĐỀ SỐ HỌC

MỘT SỐ VẤN ĐỀ SỐ HỌC



Tháng 10/2007

CHƯƠNG 1: LÍ THUYẾT CHIA HẾT

I.Tính chia hết.

Các định lý:

1. Giả sử a,b,c∈ $\mathbb{Z}$. Nếu b⋮a và c⋮b thì c⋮a.
2. Giả sử a,b,c,m,n∈ $\mathbb{Z}$. Nếu a⋮c và b⋮c thì (ma+nb)⋮c.
3. (Thuật toán chia) Giả sử a,b,∈ $\mathbb{Z}$ và b>0. Khi đó ,c,m,n∈ $\mathbb{Z}$. Nếu a⋮c và b⋮c thì (ma+nb)⋮c.

(Thuật toán chia) Giả sử a,b,∈ $\mathbb{Z}$ và b>0. Khi đó tồn tại duy nhất các số nguyên q và r sao cho

$$a = bq + r, \quad 0 \le r < b.$$

Ta gọi q là thương và r là phần dư. Như vậy, a chia hết cho b khi và chỉ khi phần dư trong phép chia bằng không.

Ví dụ. Chứng minh rằng:

a) $\left(n^3 - n\right) \vdots 3$,

b) $n(n-1)(2n-1) \vdots 6$.

II. Số nguyên tố:

Khái niệm: Số nguyên tố là số nguyên lớn hơn 1 chỉ chia hết chó và chính nó.

Các định lý:

1. Mỗi số nguyên lớn hơn 1 đều có ước nguyên tố.
2. Tồn tại vô hạn số nguyên tố.
3. Nếu n là hợp số, thì n có ước nguyên tố không vượt quá $\sqrt{n}$.

III. Ước chung lớn nhất:

Khái niệm: Ước chung lớn nhất của hai số a và b không đồng thời bằng 0 là số nguyên lớn nhất chia hết cả a và b.

Kí hiệu: (a,b)

Định nghĩa: Các số nguyên a và b được gọi là nguyên tố cùng nhau nếu (a,b) =1.

Các định lý:

1. Giả sử a, b, c là các số nguyên, (a,b)=d. Khi đó ta có:

i) $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$,

ii) $(a + cb, b) = (a, b)$.

2. Ước chung lớn nhất của các số nguyên a và b không đồng thời bằng 0 là số nguyên dương nhỏ nhất biểu diễn được bởi một tổ hợp tuyến tính của a và b.

Trong đó tổ hợp tuyến tính của a và b là một tổng có dạng ma + nb (m,n∈ $\mathbb{Z}$).

Hệ quả: $(a,b)=1 \Leftrightarrow \exists m,n : ma+nb=1$ (m,n$\in \mathbf{Z}$).

3. (Thuật toán Ơ-clít) giả sử r_0=a, r_1=b là các số nguyên không âm, b$\neq 0$. Ta áp dụng liên tiếp các phép chia

$$r_j = r_{j+1}q_{j+1} + r_{j+2},$$

với $0<r_{j+2}<r_{j+1}$, j=0,1,2,…,n-2, r_n=0. Khi đó (a,b)=r_{n-1} (phần dư khác không cuối cùng của phép chia).

Ví dụ. (IMO 1959) Chứng minh rằng với mọi số nguyên dương n, phân số sau đây tối giản:

$$\frac{21n+4}{14n+3}.$$

Giải. Đặt $d=(21n+4,14n+3)$. Suy ra $2(21n+4)-3(14n+3)\vdots d \Leftrightarrow 1\vdots d \Leftrightarrow d=1$

❁❁❁

CHƯƠNG 2 : LÍ THUYẾT ĐỒNG DƯ

I. Các khái niệm cơ bản:

Khái niệm: giả sử a, b là các số nguyên. Ta nói a đồng dư b modul m nếu (a−b)⋮m. Khi a đồng dư b môđul m. Ta viết a≡b (mod m).

Các định lý:

1. Giả sử a, b là các số nguyên thì a≡b (mod m) $\Leftrightarrow \exists k$:a=b+km($k\in \mathbf{Z}$).

2. (Tính chất phản xạ). Nếu a là một số nguyên, thì

$$a \equiv a(\mathrm{mod}\, m)$$

3. (Tính chất đối xứng). Giả sử a, b là các số nguyên. Khi đó, nếu $a \equiv b(\mathrm{mod}\, m)$ thì $b \equiv a(\mathrm{mod}\, m)$.

4. (Tính chất bắc cầu). Giả sử a, b, c là các số nguyên. Khi đó nếu $a \equiv b(\mathrm{mod}\, m)$, $b \equiv c(\mathrm{mod}\, m)$ thì $a \equiv c(\mathrm{mod}\, m)$.

5. Già sử a, b, c và m là các số nguyên, m>0 và $a \equiv b(\mathrm{mod}\, m)$. Khi đó:

i) $a+c \equiv b+c(\mathrm{mod} m)$,

ii) $a-c \equiv b-c(\mathrm{mod} m)$,

iii) $ac \equiv bc(\mathrm{mod} m)$.

6. Giả sử a, b, c và m là các số nguyên, m>0, $ac \equiv bc(\mathrm{mod} m)$ và $d=(c,m)$. Khi đó ta có

$$a \equiv b\left(\mathrm{mod}\frac{m}{d}\right).$$

Hệ quả. Nếu a,b,c,m là các số nguyên sao cho m>0, $(c,m)=1$ và $ac \equiv bc(\bmod m)$.

Khi đó $a \equiv b(\bmod m)$.

7. Giả sử a, b, c, d, m là các số nguyên, m>0, $a \equiv b(\bmod m)$, $c \equiv d(\bmod m)$. Khi đó:

i) $a+c \equiv b+d(\bmod m)$,

ii) $a-c \equiv b-d(\bmod m)$,

iii) $ac \equiv bd(\bmod m)$.

8. Giả sử a, b, k, m là các số nguyên, đồng thời k>0, m>0, $a \equiv b(\bmod m)$. Khi đó

$$a^k \equiv b^k(\bmod m).$$

9. Giả sử $a \equiv b(\bmod m_1)$, $a \equiv b(\bmod m_2)$, … , $a \equiv b(\bmod m_k)$, trong đó a, b, m_1, m_2, … , m_k là các số nguyên, m_1, m_2, … , m_k>0. Khi đó

$$a \equiv b(\bmod[m_1,...,m_k]),$$

Trong đó $[m_1,...,m_k]$ là bội chung nhỏ nhất của m_1, m_2, … , m_k.

Hệ quả. Giả sử $a \equiv b(\bmod m_1)$, $a \equiv b(\bmod m_2)$, … , $a \equiv b(\bmod m_k)$, trong đó a, b nguyên, m_1, m_2, … , m_k là các số nguyên dương và nguyên tố cùng nhau từng cặp.

Khi đó

$$a \equiv b(\bmod m_1...m_k).$$

II. Định lí Trung Quốc về phần dư:

Định lý: Giả sử m_1, m_2, … , m_r là các số nguyên tố cùng nhau từng cặp. Khi đó hệ các đồng dư tuyến tính

$$\begin{cases} x \equiv a_1(\bmod m_1), \\ x \equiv a_2(\bmod m_2), \\ \quad\quad M \\ x \equiv a_r(\bmod m_r). \end{cases}$$

có nghiệm duy nhất môđulô M= $m_1m_2…m_r$.

Chứng minh. Trước tiên ta xây dựng một nghiệm của hệ đồng dư tuyến tính trên. Đặt

$$M_k = \frac{M}{m_k} = m_1m_2...m_{k-1}m_{k+1}...m_r.$$

Vì $(m_k,m_j)=1$ với $j \neq k$ nên $(M_k,m_k)=1$. Do đó tồn tại y_k sao cho

$$M_k y_k \equiv 1(\bmod m_k).$$

Lập tổng

$$x = a_1M_1y_1 + a_2M_2y_2 + ... + a_rM_ry_r.$$

Khi đó, x sẽ là nghiệm của hệ đồng dư $x \equiv a_j \pmod{m}$, $j = 1,2,...,r$. Thật vậy, ta có $M_k \vdots m_j$ khi $j \neq k$ nên $M_k \equiv 0 \pmod{m_j}$, $j \neq k$. Từ đó suy ra

$$x \equiv a_k M_k y_k \pmod{m_k}.$$

Do $M_k y_k \equiv 1 \pmod{m_k}$ nên $x \equiv a_k \pmod{m_k}$

Bây giờ ta chỉ ra rằng, hainghiệm tùy ý sẽ đồng dư nhau môđulô M. Giả sử x_0, x_1 là hainghiệm của hệ r đồng dư đang xét. Khi đó, với mỗi k, $x_0 \equiv x_1 \equiv a_k \pmod{m_k}$. Do đó $(x_0 - x_1) \vdots m_k$. Từ đó suy ra $x_0 \equiv x_1 \pmod{M}$. Vậy hệ đồng dư đang xét có nghiệm duy nhất môđulô M.

III. Định lí Phecma, định lí Wilson và định lý Ơ-le:

Định lý Wilson. Với mọi số nguyên tố p, ta có

$$(p-1)! \equiv -1 \pmod{p}.$$

Định lý. Giả sử n là số nguyên dương sao cho $(n-1)! \equiv -1 \pmod{n}$. Khi đó n là số nguyên tố.

Định lý Phecma bé. Giả sử p là số nguyên tố và a là số nguyên dương với $(a,p) = 1$. Khi đó $a^{p-1} \equiv 1 \pmod{p}$.

Hệ quả. Giả sử p là số nguyên tố và a là số nguyên dương. Khi đó $a^p \equiv a \pmod{p}$.

Định lý Ơ-le. Giả sử m là số nguyên dương và a là số nguyên với $(a,m) = 1$. Khi đó

$$a^{\rho(m)} \equiv 1 \pmod{m}.$$

Trong đó, $\rho(m)$ là số các số nguyên dương không vượt quá m và nguyên tố cùng nhau với m. Được tính theo công thức

$$\rho(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right) \text{ với } m = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}.$$

❁❁❁

Chương 3: PHƯƠNG TRÌNH NGHIỆM NGUYÊN

Để mở đầu cho Phần phương trình nghiệm nguyên, chúng ta hãy nhắc lại một số kiến thức và định lý cơ bản sau:

Định nghĩa 1: Với hai số nguyên a và b, ta nói a chia hết cho b (a là bội của b, b là ước của a) nếu tồn tại số nguyên k sao cho a = kb, ký hiệu a b.

Định nghĩa 2: số nguyên dương p > 1 gọi là số nguyên tố nếu nó chỉ có hai ước là 1 và chính nó.

Định lý Euclid: tồn tại vô hạn số nguyên tố.

Định lý cơ bản của số học: Cho n số nguyên > 1. Khi đó luôn có thể biểu diễn được một cách duy nhất dưới dạng:

$$n = p_1^{\alpha 1} p_2^{\alpha 2} ... p_n^{\alpha n}.$$

trong đó k, a_1 là các số tự nhiên, p_i là các số nguyên tố thỏa:

$$1 < p_1 < p_2 < \ldots < p_n.$$

Tính chất cơ bản của tính chia hết:

1) a, b nguyên mà a b thì a ≥ b
2) nếu a_i b với mọi i= 1, …, n; thì ($a_1 + a_2 + \ldots + a_n$) b
3) với hai số nguyên không âm a và b, luôn tồn tại duy nhất một cặp số nguyên q và r sao cho a = bq + r, trong đó 0 ≤ r ≤ b.
4) a, b là 2 số nguyên dương, p là số nguyên tố sao cho ab p, khí đó phải có a p hoặc b p

Định nghĩa 3 : Ước số chung lớn nhất của a và b, ký hiệu ƯCLN(a,b), hay (a,b) là số nguyên dương lớn nhất mà a và b đều chia hết cho nó.

Tính chất cơ bản:

3.1 (a, b)=(a, a + b)

3.2 (ma, mb) = m(a, b)

3.3 (a, b) d thì :($\frac{a}{d}, \frac{b}{d}$) = $\frac{1}{d}$ (a, b).

3.4 Hai số nguyên a và b được gọi là nguyên tố cùng nhau nếu (a,b) = 1. Cho a, b, c là 3 số nguyên dương sau cho ab c. nếu (a,c)=1 thì b c

3.5 Hai số nguyên liên tiếp thì nguyên tố cùng nhau.

3.6 Với mọi số nguyên dương a,b luôn tồn tại các số nguyên x, y sao cho ax + by = (a,b)

3.7 Hai số nguyên dương nguyên tố cùng nhau khi và chỉ khi tồn tại các số nguyên x, y sao cho ax + by =1.

Định nghĩa 4: Bội số chung nhỏ nhất của a và b, ký hiệu BSCNN (a,b), hay [a,b] la số nguyên nhỏ nhất chia hết cho cả a lẫn b.

[ma, mb] = m[a,b].

Định nghĩa 6: a ≡ b (mod m) ⇔ (a – b) ⋮ m.

Tính chất :

6.1 a ≡ b (mod m) và c ≡ d (mod m) thì a + c ≡ b + d (modm).

6.2 p nguyên tố và ab ≡ 0 (mod p) thì a ≡ 0 (mod p) hoặc b ≡ 0 (mod p).

Định lý Fermat:

Nếu p là số nguyên tố và a nguyên dương tùy ý: (a^p – a) ⋮ p.

(a,p)=1 thì a^{p-1} ≡ 1 (mod p).

Định lý Euler: Nếu m nguyên dương và (a,m) = 1 thì

$$a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)$$

Định lý Fermat – Euler : Nếu p = 4k + 1 thì tồn tại các số nguyên dương a, b sao cho $p=a^2 + b^2$.

Phần 2 : Phương trình nghiệm nguyên – phương trình vô định bậc nhất:

Định lý 2.1 Phương trình Đi ô Phăng tuyến tính: là phương trình có dạng:

ax + by = c, (*)

a, b, c , x, y nguyên.

Định lý 2.2: Giả sử a, b nguyên dương, d =(a,b). Khi đó (*) không có nghiệm nguyên nếu d ⋮ c, nếu d ⋮ c thì phương trình có vô số nghiệm. Hơn nữa, nếu $x = x_0$; $y = y_0$ là một nghiệm nào đó của phương trình thì mọi nghiệm của phương trình có dạng:

$$x = \frac{b}{d} n \,, \quad y = \frac{a}{d} n$$

Phương trình bậc hai hai ẩn :

$ax^2 + 2bxy + cy^2 + 2d + 2ey + f = 0$.

Tùy theo các hệ số mà phương trình có độ phức tạp khác nhau, nói chung việc giải khá phức tạp.

Xét các dạng đặc biệt:

Phương trình Pell loại 1: $x^2 – dy^2 = 1$, d nguyên.

Khi nhắc đến phương trình Pell, ta luôn hiểu đó là nghiệm nguyên dương. Tính chất cơ bản:

i) nếu d chính phương thì (1) vô nghiệm nguyên dương.

ii) nếu d nguyên âm, (1) không có nghiệm nguyên dương.

iii) điều kiện phương trình Pell loại I có nghiệm : d là số nguyên dương không chính phương.

iiii) Công thức nghiệm phương trình Pell loại I: Xét dãy $\{x_n\}$ và $\{y_n\}$ xác định bởi:

$$x_0 = 1,\ x_1 = a,\ x_{n+2} = 2x_{n+1} - x_n,\ n = 0,1,2\ldots.$$
$$y_0 = 1,\ y_1 = b,\ y_{n+2} = 2y_{n+1} - y_n,\ n = 0,1,2\ldots.$$

Các bạn có thể tự chứng minh.

Phương trình Pell loại II: $x^2 - dy^2 = -1$.

Tính chất cơ bản:

i) phương trình vô nghiệm nguyên dương khi :

d chính phương

d có ước nguyên tố $p = 4k + 3$.

ii) nếu d nguyên tố, phương trình có nghiệm nguyên dương khi và chỉ khi d không có dạng $4k + 3$.

iii) công thức nghiệm của pt:

$$x_0 = u,\ x_1 = u^3 + 3duv^2,\ x_{n+2} = 2x_{n+1} - x_n,\ n = 0,1,2\ldots$$
$$y_0 = v,\ y_1 = v^3 + 3u^2v;\quad y_{n+2} = 2y_{n+1} - y_n,\quad n = 0,1,2\ldots$$

PHƯƠNG TRÌNH NGHIỆM NGUYÊN TRONG CÁC LỚP ĐA THỨC.

Ngoài các phương trình đặc biệt như phương trình Pell, chúng ta sẽ dùng nhiều phương pháp khác nhau để giải các bài toán tìm nghiệm nguyên như: quy về hệ bậc nhất, đánh giá hai vế, lựa chọn đồng du môdul, sử dụng định lý số học, cực hạn (xuống thang), thử chọn….

Phương pháp quy về hệ bậc nhất:

Xét ví dụ sau:

$$x^2 + x + 6 = y^2. \qquad (1)$$

$$(1) \Leftrightarrow 4x^2 + 4x + 24 = 4y^2 .$$
$$\Leftrightarrow (2y)^2 - (2x + 1)^2 = 23.$$
$$\Leftrightarrow (|2y| + |2x+1|)(|2y| - |2x+1|) = 23. \qquad (2)$$

Vì $x, y \in \mathbf{Z}$ nên $|2y| + |2x+1| > 0$, từ (2) suy ra $|2y| - |2x+1| > 0$.

Hiển nhiên $|2y| + |2x+1| > |2y| - |2x+1|$.

Do đó :

$$(2) \Leftrightarrow \begin{cases} |2y| + |2x+1| = 23 \\ |2y| - |2x+1| = 1. \end{cases}$$

Giải phương trình ra các nghiệm nguyên:

$$(5,6);\ (-5,-6);\ (-6,-6);\ (5,-6).$$

Các ví bài tập tương tự (yêu cầu bạn đọc tự giải):

Tìm nghiệm nguyên của các phương trình sau:

3.1 3 $x^2 + 2y^2 + z^2 + 4xy + 2yz = 26 - 2xz.$

Đưa về : $x^2 + (x + y)^2 + (x + y + z)^2 = 26.$

3.2 $x^2 - 4xy + 5y^2 = 169$.

3.3 Giải hệ phương trình sau:

3.4 $x^3 + y^3 = 3xy + 1$.

Ad hằng đẳng thức: $a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca)$.

Phương pháp đánh giá:

Ví dụ: $x^4 + x^2 + 1 = y^2$.

Do $x^2 \geq 0, \forall x$; nên:

$$(x^2)^2 < x^4 + x^2 + 1 \leq (x^2+1)^2 .$$

hay $$(x^2)^2 < y^2 \leq (x^2+1)^2 .$$

Do x^2 và $x^2 + 1$ là 2 số tự nhiên liên tiếp nên: $y^2 = (x^2+1)^2$

Dễ dàng suy ra nghiệm nguyên của phương trình là (0,1) ; (0, -1).

Các bài tập tương tự: tìm nghiệm nguyên của các phương trình sau:

4.1 $y^3 - x^3 = 2x + 1$.

4.2 $x^4 - y^4 + z^4 + 2x^2z^2 + 3x^2 + 4z^2 + 1 = 0$.

4.3 $x^4 + x^2 + 4 = y^2 - y$.

4.4 $x + 2y + 2z = xyz$.

Sử dụng tính chất chia hết – đồng dư thức môdul.

Xét ví dụ: giải phương trình nghiệm nguyên sau:

$19x^2 + 28y^2 = 729$.

Cách 1:

(*) $(18x^2 + 27y^2) + (x^2 + y^2) = 729$.

Suy ra $(x^2 + y^2)$ chia hết cho 3, do đó x và y đều chia hết cho 3 (điều này dễ chứng minh).

Đặt : $x = 3u, y = 3v$ $(u,v \in \mathbf{Z})$.

Thay vào phương trình đã cho, được $19u^2 + 28v^2 = 81$.

Tương tự, ta được $u=4s, v=3t$, $(s, t \in \mathbf{Z})$.

Và : $19s^2 + 28t^2 = 9$.

Rõ ràng s, t không đồng thời bằng không nên : $19s^2 + 28t^2 \geq 19 > 9$. Phương trình vô nghiêm nguyên.

Cách 2:

Từ phương trình đã cho ta được: $x^2 \equiv -1 (\text{mod } 4)$, không xảy ra với mọi số nguyên x.

Các bài tương tự: giải các phương trình sau trên tập số nguyên:

5.1 $2x^6 + y^2 - 2x^3y = 320$.

5.2 $X^{15} + y^{15} + z^{15} = 19^{2003} + 7^{2003} + 9$.

Gợi ý: xét đồng dư theo mod 9 (phương trình vô nghiệm).

5.3 $1! + 2! + 3! + \ldots + (x+1)! = y^{x+1}$.

5.4 $x_1^4 + x_2^4 + \ldots + x_{14}^4 = 1599$.

5.5 $z^2 = (x^2 - 1)(y^2 - 1) + n$. Khi :

5.5.1 n=1981

5.5.2 n=1984
5.5.3 n=1985

MỘT SỐ PHƯƠNG PHÁP GIẢI PHƯƠNG TRÌNH NGHIỆM NGUYÊN

Phương pháp 1 Phân tích
Ví dụ : Tìm nghiệm nguyên của phương trình

$$x^2 - y^2 = 25 + 6y$$
$$\Leftrightarrow x^2-25 = y^2+6y+9-9$$
$$\Leftrightarrow x^2 = (y+3)^2+16$$
$$\Leftrightarrow x^2-(y+3)^2$$
$$\Leftrightarrow (x-y-3)(x+y+3) = 16$$

...
*Phân tích thành tổng các bình phương, lập phương :
Ví dụ Tìm nghiệm nguyên của phương trình

$$\frac{3}{2}x^2+6y^2 = x+332$$
$$\Leftrightarrow 9x^2+36y^2 = 6x+1992$$
$$(3x-1)^2+(6y)^2 = 1993$$

....

Phương pháp 2 Nhận xét về ẩn số
1,Nếu các ẩn x,y,z,t... có vai trò như nhau thì ta có thể giả sử $x \le y \le z \le t...$ hoặc ngược lại.
2, Nếu các ẩn có cấu trúc giống nhau như lũy thừa cùng bậc, các số nguyên liên tiếp thì ta sẽ khử ẩn để đưa về dạng quen thuộc hoặc PT ít ẩn hơn
Ví dụ: Tìm nghiệm nguyên các phương trình :
a,x+y+z=xyz
b, 5(xy+yz+xz)=4xyz

Phương pháp 3 "Kẹp" giữa 2 số bình phương, lập phương, các tích các số nguyên liên tiếp
Ví dụ : Tìm nghiệm nguyên phương trình sau:
$x^4+x^2+1 = y^2$
Ta thấy $(x^2)^2<y^2<(x^2+2)^2 \forall x \in Z$ ...

Phương pháp 4 Sử dụng phép chia hết và phép chia có dư
(còn nữa)

Bài tập (Phương pháp 4) : Tìm x,y $\in$ Z
a, $x^3+y^3+z^3$ =304197519751995
b, $19x^2+5y^2+1995z^{3^{3^3}}+3$ =
c, $x_1^4+x_2^4+...+x_{14}^4$=1995

d, $x^2+(x+y)^2=(x+9)^2$ (x,y ∈Z+)
e, $x^2+3=4y(y+1)$(x,y ∈Z+)
g, $(x^2+1)^y-(x^1-1)^y=(2x)^y$ (x,y ∈Z+)

❁❁❁

CHƯƠNG 4 : MỘT SỐ VẤN ĐỀ VỀ ƯỚC VÀ BỘI

Ước và bội là hai trong số những khái niệm cơ bản nhất của số học. Tuy nhiên sự cơ bản luôn luôn có sự thú vị riêng của nó. Những người học số học luôn cần phải nắm vững vấn đề này, không chỉ vì sự ứng dụng rộng rãi của nó mà nó còn là cả nền tảng xây dựng nên những vấn đề phức tạp và đa dạng hơn.
Trước hết chúng ta hãy điểm qua một số khái niệm cơ bản.

A. Một số khái niệm cơ bản:

I/ Ước số:

Một số nguyên d được gọi là một ước số của số nguyên a khi và chỉ khi tồn tại một số nguyên b sao cho $a=bd$.

II/ Ước số chung:

Một số nguyên dương d được gọi là một ước số chung của hai số nguyên dương a và b khi và chỉ khi d là ước số của a và d cũng là ước số của b.
Tương tự ta cũng có định nghĩa ước số chung của n số nguyên dương $a_1,a_2,...,a_n$.

III/ Ước chung lớn nhất:

Một tính chất cơ bản của ước mà các bạn cũng có thể nhận ra là: nếu d là ước của a thì $|d|\leq|a|$, do đó tập hợp các ước của một số là hữu hạn. Trong một tập hợp hữu hạn thì luôn tồn tại phần tử bé nhất, lớn nhất. Do đó khái niệm về ước chung lớn nhất được hình thành.
Số nguyên dương d được gọi là ước chung lớn nhất của 2 số nguyên dương a và b nếu d đồng thời thoả mãn 2 điều kiện sau:
- d là ước số chung của a và b
- Với mọi số nguyên dương d' là ước số chung của a và b thì $d'\leq d$

Kí hiệu: $(a,b)=d$
Tương tự ta cũng có định nghĩa ước số chung lớn nhất của n số nguyên dương $a_1,a_2,...,a_n$

IV/ Nguyên tố cùng nhau:

Hai số nguyên dương a,b được gọi là nguyên tố cùng nhau khi và chỉ khi $(a,b)=1$
Tương tự ta định nghĩa các số $a_1,a_2,...,a_n$ nguyên tố cùng nhau khi và chỉ khi $(a_1,a_2,...,a_n)=1$

V/ Bội số:

Một số nguyên k được gọi là bội số của số nguyên a khi và chỉ khi tồn tại một số nguyên b sao cho $k=ab$

VI/ Bội số chung:

Một số nguyên dương k được gọi là bội chung của hai số nguyên dương a và b nếu

k là bội số của a và k cũng là bội số của b.
Tương tự ta cũng có định nghĩa về bội chung của n số. $a_1,a_2,...,a_n$

VII/ Bội chung nhỏ nhất:

Số nguyên dương k được gọi là bội chung lớn nhất của 2 số nguyên dương a,b nếu k thoả mãn đồng thời 2 điều kiện sau:
- k là bội số chung của a và b.
- Với mọi số nguyên dương k' là bội số chung của a và b thì $k \le k'$

Kí hiệu $k=[a,b]$
Tương tự cũng có định nghĩa bội số chung nhỏ nhất của n số nguyên dương $a_1,a_2,...,a_n$

B. Một số tính chất của ước và bội:

Với a,b,c,d là số nguyên dương ta có:
- $(ac,bc)=c(a,b)$
- Nếu c là ước chung dương của a và b thì $\left(\frac{a}{c},\frac{b}{c}\right)=\frac{(a,b)}{c}$

Từ đây suy ra $d=(a,b) \Leftrightarrow \left(\frac{a}{d},\frac{b}{d}\right)=1$
- Tồn tại các số nguyên x,y sao cho $(a,b)=ax+by$
- Nếu $(a,b)=1$ và $ac \vdots b$ thì $c \vdots b$
- Nếu $(a,b)=1$ và $(a,c)=1$ thì $(a,b,c)=1$
- $(a,b,c)=((a,b),c)=(a,(b,c))=((a,c),b)$
- $[a,b]=\frac{ab}{(a,b)}$
- Nếu k là bội chung của a và b. Khi đó $k \in [a,b] \Leftrightarrow \left(\frac{k}{a},\frac{k}{b}\right)=1$
- $[ca,cb]=c[a,b]$
- $[a,b,c]=[[a,b],c]$

C. Phép chia Euclid:

Trong các phần trên chúng ta đã thông qua các khái niệm và một số tính chất về ước số. Thế nhưng chúng ta vẫn chưa biết cách làm để tìm ước số chung lớn nhất của 2 số. Qua phần này chúng ta sẽ trả lời câu hỏi đó thông qua phép chia Euclid. Trước hết chúng ta hãy xem xét ý tưởng của phương pháp này. Euclid đã bắt đầu với nhận xét sau: $(a,b)=(b,a-b)=(b-a,b)=d$, $a \ne b(*)$. Chứng minh nhận xét này không khó. Bây giờ ta tiếp tục, giả sử $a \ge b$, khi đó từ đẳng thức $(a,b)=(a-b,b)$ ta đi về bài toán tìm ước chung lớn nhất của 2 số nguyên dương nhỏ hơn là $a-b$ và b. Tiếp tục là bài toán đó với 2 số nguyên dương nhỏ hơn nữa là $a-2b,b$ (trong trường hợp $a-b>b$) hoặc $a-b,2b-a$ (trong trường hợp $a-b<b$). Nếu ta cứ tiếp tục làm như vậy thì các số nguyên dương cần tìm ước chung lớn nhất sẽ nhỏ đi dần dần, điều này sẽ kéo dài vô tận và các số nguyên dương sẽ nhỏ dần vô hạn chăng? Câu trả lời là không vì ít ra các số nguyên dương đều bị chặn bởi 1. Như vậy tại

sao quá trình này lại không thể kéo dài vô hạn được, chỉ có thể là do (*) không đúng nữa, tức là đến một lúc nào đó ta sẽ thu được 2 số nguyên dương bằng nhau. Nghĩa là ta sẽ có: $(a,b)=(c,c)=d$. Như vậy $c=d$. Từ đây ta có thuật toán sau để tìm ước chung lớn nhất của 2 số nguyên dương a và b.

Cho $a>b>0$. Nếu $a=bq$ thì $(a,b)=b$

Nếu $a=bq+r$ thì $(a,b)=(b,r)$. Phép chia Euclid trong trường hợp này được thực hiện như sau:

$a=bq+r_1 \Rightarrow (a,b)=(b,r_1)$

$b=r_1q_1+r_2 \Rightarrow (b,r_1)=(r_1,r_2)$

$r_1=r_2q_2+r_3 \Rightarrow (r_1,r_2)=(r_2,r_3)$

$r_2=r_3q_3+r_4 \Rightarrow (r_2,r_3)=(r_3,r_4)$

.....

$r_{n-2}=r_{n-1}q_{n-1}+r_n \Rightarrow (r_{n-2},r_{n-1})=(r_{n-1},r_n)$

$r_{n-1}=r_nq_n \Rightarrow (r_{n-1},r_n)=r_n$

Từ đây suy ra $(a,b)=(b,r_1)=(r_1,r_2)=...=(r_{n-2},r_{n-1})=(r_{n-1},r_n)=r_n$

Hay nói cách khác (a,b)chính là số dư cuối cùng khác không của phép chia Euclid.

Từ phép chia Euclid, ta suy ra được tính chất: tồn tại các số nguyên x,y sao cho $(a,b)=ax+by$, một tính chất đẹp và quan trọng của lí thuyết số.

Ta có thể dễ dàng chứng minh tính chất này bằng phương pháp quy nạp lùi theo n trong phép chia Euclid.

Thật vậy nếu $a=bq$thì tính chất trên hiển nhiên đúng. Nếu $a\not\vdots b$ thì ta có đẳng thức sau:

$$r_n=0.r_{n-1}+1.r_n$$

Giả sử ta có: $r_n=(r_k,r_{k+1})=x.r_k+y.r_{k+1}$. Khi đó:

$$r_{k-1}=r_kq_k+r_{k+1} \Rightarrow y.r_{k-1}=(y.q_k-x)r_k+x.r_k+y.r_{k+1}$$
$$\Rightarrow y.r_{k-1}-(y.q_k-x).r_k=r_n=(r_{k-1},r_k)$$

như vậy theo nguyên lí quy nạp lùi, đối với các số (a,b)cũng tồn tại các số nguyên x,y sao cho $xa+yb=r_n=(a,b)$

Ta hãy xét qua một số ví dụ nhé!

Bài toán:

a/ Hãy tìm ƯCLN và BCNN của 34 và 56

b/ Hãy tìm các ƯCLN có thể có của của $2k-1$và $9k+4(k\in\mathbb{N})$

Câu a chỉ là câu áp dụng của phép chia Euclid:

Ta có: $(34,56)=(22,34)=(12,22)=(10,12)=(2,10)=2$

Suy ra $[a,b]=952$

Câu b cũng áp dụng phép chia Euclid tuy nhiên hơi phức tạp một chút vì có chứa ẩn số k. Ta cũng thực hiện phép chia bình thường, giống như chia đa thức.

$$(2k-1,9k+4)=(k+8,2k-1)=(k+8,-17)=(k+8,17)$$

Vậy $(2k-1,9k+4)=17$ khi $k=17m-8$ hoặc $(2k-1,9k+4)=1$khi $k\neq 17m-8$(với $m\in\mathbb{N}$)

Bài toán này chúng ta còn có thể giải theo cách khác:
Đặt $d=(2k-1,9k+4)$. Ta có $17\vdots d\Rightarrow d=1$ hoặc $d=17$
Lời giải trên thật ngắn gọn, tuy nhiên làm như vậy chúng ta phải xác định các trường hợp của k khi $d=1$ hoặc $d=17$. Trong trường hợp này, chúng ta phải giải phương trình nghiệm nguyên sau: Tìm k sao cho: $2k-1=17m,k,m\in\mathbb{N}$ và cũng đi đến kết quả tương tự cách 1.
Ta rút ra bài toán tổng quát: Cho $ad-bc=p$ là một số nguyên tố. Tìm tất cả các giá trị có thể có của: $(ak+c,bk+d)$.
Bằng một ý tưởng của cách 2. Tạ đặt $m=(ak+c,bk+d)$. Ta có:
$a(bk+d)-b(ak+c)=ad-bc=p\vdots m\Rightarrow m=1$ hoặc $m=p$. Cả 2 trường hợp đều có thể xảy ra bởi phương trình $ak+c\equiv 0(mod p)$ cho ta nghiệm duy nhất theo $mod p$.
Trong trường hợp này $(ak+c,bk+d)=p$, trong các trường hợp còn lại ta đều thu được: $(ak+c,bk+d)=1$.
Sau đây sẽ là phần bài tập áp dụng của phần này: Tìm tất cả các giá trị có thể có của $(6k+5,8k+3)$ với $k\in\mathbb{N}$

E. Bài tập tổng hợp:

Bài 1. Chứng minh rằng: $(\frac{a^m-1}{a-1},a-1)=(m,a-1)$ trong đó $a,m>1$
Bài 2. Chứng minh rằng nếu a,b là các số nguyên dương và $a>b$ thì:
$(\frac{a^n-b^n}{a-b},a-b)=(n(a,b)^{n-1},a-b)$
Bài 3. Chứng minh rằng: $[1,2,...,2n]=[n+1,n+2,...,2n]$
Bài 4. Cho p là số nguyên tố. Tính $[2^{2^n}-2,2^n-1]$
Bài 5. Chứng minh rằng dãy số:
a/ $A_n=\frac{n(n+1)}{2}$ với n là số tự nhiên chứa dãy vô hạn số nguyên tố cùng nhau.
b/ $B_n=2^n-1$ chứa dãy vô hạn những số nguyên tố cùng nhau.

❄ MỘT ĐỊNH LÝ VÀ ỨNG DỤNG (Dựa theo bài viết của tác giả Đoàn Quang Mạnh và bài giảng của thầy Đ.H.Thắng):

Định lý:
Giả sử $p=2^t.k+1$ là số nguyên tố lẻ với t, k là các số tự nhiên, k là số tự nhiên lẻ.
Khi đó, nếu các số tự nhiên x,y sao cho $x^{2^t}+y^{2^t}\vdots p$
thì x và y đồng thời chia hết cho p.

Chứng minh bổ đề: Ta sử dụng phép chứng minh bằng phản chứng. Giả sử x không chia hết cho p, từ giả thiết suy ra y cũng không chia hết cho p. Theo định lý nhỏ Fec-ma ta có:
$x^{p-1}\equiv 1(\bmod p),y^{p-1}\equiv 1(\bmod p)$

Hay:
$x^{2^t.k}\equiv 1(\bmod p),y^{2^t.k}\equiv 1(\bmod p)$

Suy ra:
$x^{2^t.k}+y^{2^t.k}\equiv 2(\mathrm{mod}\, p)$
Mà theo giả thiết
$x^{2^t}+y^{2^t}\equiv 0(\mathrm{mod}\, p)$
nên
$x^{2^t.k}+y^{2^t.k}\equiv 0(\mathrm{mod}\, p)$(Do k lẻ)
Vậy điều giả sử trên của ta là sai. Tóm lại ta có đpcm.

Chú ý rằng $t\geq 1$vì p là số nguyên tố lẻ. Khi t=1 và t=2 ta có các hệ quả sau.

Bài tập1: Cho số nguyên tố dạng p=4k+3 .
CMR: Nếu các số tự nhiên x,y thỏa mãn $x^2+y^2\vdots p$ thì x và y đều chia hết cho p.

Bài tập2: Cho số nguyên tố dạng p=4k+1, k là số tự nhiên lẻ.
CMR: Nếu các số tự nhiên x,y thỏa mãn $x^4+y^4\vdots p$thì x và y đều chi hết cho p.

Bài tập 3: Giả sử a,b là hai số tự nhiên khác 0 nguyên tố cùng nhau. Khi đó các ước số nguyên tố lẻ của a^2+b^2chỉ có dạng 4m+1 với m là số tự nhiên.

Các bài tập nâng cao (Sử dụng định lý và các hệ quả trên để giải quyết):

Bài 1*: Giải phương trình nghiệm nguyên: $x^2-y^3=7$

Bài 2*: Tìm tất cả các cặp số nguyên dương (x,y) sao cho
$\frac{x^2+y^2}{x-y}$
là số nguyên và là ước của 1995 (Thi HSG Bungary 1995)

Bài 3*: Giả sử a,b là các số nguyên dương sao cho 15a+16b và 16a-15b đều là các số chính phương. Tìm giá trị nhỏ nhất của số nhỏ nhất trong hai số chính phương ấy.
(IMO lần thứ 37)

Bài 4*: Tìm các nghiệm nguyên dương của các phương trình:
a) $4xy-x-y=z^2$
b) $19x^2+28y^2=729$
c) $x^2+y^2=3z^2$

Bài 5*: Tìm nghiệm nguyên dương của hệ phương trình:
$x^2+13y^2=z^2,13x^2+y^2=t^2$

Bài 6*: Cho x và y là các số nguyên khác 0 sao cho

$\frac{x^2+y^2}{x+y}$ là số nguyên và là ước của 1978. Chứng minh rằng x=y. (Chọn đội tuyển QG CHLB Đức 1979)