Trường đại học Cần Thơ
Khoa Công nghệ thông tin và truyền thông
Bộ môn Khoa học máy tính

LÝ THUYẾT CHIA VÀ ĐỒNG DƯ

NỘI DUNG

1. Phép chia hết và có dư
2. Ước chung lớn nhất và bội chung nhỏ nhất
3. Số nguyên tố và hợp số
4. Phương trình nguyên
5. Quan hệ đồng dư
6. Phương trình đồng dư

PHÉP CHIA HẾT VÀ CÓ DƯ

Phép chia hết

- *Định nghĩa:*
  - Xét a,b $\in$ Z và **b$\neq$0**
  - **b chia hết a** *(b là ước của a)* hay
  - **a chia hết cho b** *(a là bội của b)* khi và chỉ khi tồn tại **q$\in$Z** sao cho: **a = bq**
- *Ký hiệu:* $b \mid a \Leftrightarrow \exists q \in \mathrm{Z}\ \text{sao cho}\ a = bq \quad \Leftrightarrow a \vdots b$
- *Ví dụ:* 3 chia hết 6 không?

a = **6** b = **3** q = **2**

$\exists$ 2$\in$Z , 6=3.2

Phép chia hết

- *Nhận xét:*
  - Với mọi $b \neq 0$ thì
    - 0 chia hết cho b vì $0 = b0$
    - Vậy 0 là bội của mọi số nguyên $b \neq 0$
  - Với mọi a thì
    - $1|a$ vì $a \in Z$, $a = 1.a$
    - Vậy 1 là ước của mọi số nguyên a

Tính chất của phép chia hết

1. $b|a \Leftrightarrow \pm b| \pm a$
2. $\forall a \neq 0 \quad a|a$
3. $\forall a \quad \pm 1|\ a$
4. $\forall a \neq 0 \quad a|0$
5. ($\forall a \neq 0$, $\forall b \neq 0$, a|b và b|a) khi và chỉ khi $a = \pm b$
6. Nếu b|a thì b|ax
7. Nếu c|a và c|b thì c|(a+b) và c|(a-b)
8. Nếu (a|b và b|c) thì a|c (tính bắc cầu)
9. Nếu c|a và c|b thì c|(ax+by)
10. Nếu a|x và b|y thì ab|xy

Phép chia có dư

- *Định lý*
  - a,b∈Z và b≠0
  - Tồn tại duy nhất cặp số nguyên q và r∈Z sao cho:

$$\begin{cases} a = bq + r \\ 0 \le r < |b| \end{cases}$$

    - q được gọi là thương, r được gọi là số dư
  - Khi r = 0 ⇨ ta có phép chia hết
- *Ví dụ: Hãy tìm q và r?*

a=7, b=2: q= 3 , r= 1 7=2*3+1

a=10, b=5: q= 2 , r= 0 10=5*2+0

UCLN VÀ BCNN

Ước chung lớn nhất (UCLN)

- $a_1,a_2,\ldots,a_n$ là các số nguyên không đồng thời bằng 0
- Số nguyên **$d \in Z$** được gọi là **ước chung** của các a_i (i=1,2,...,n) khi và chỉ khi **d là ước của mỗi a_i ($d|a_i$)**
- **Ước chung d** của các a_i (i=1,2,...,n) được gọi là **UCLN** của các a_i nếu và chỉ nếu **d là bội của mọi ước chung của các a_i**
- *Ký hiệu:* $d = (a_1,a_2,\ldots,a_n)$
- *Quy ước:* UCLN là một số dương
- *Ví dụ:*
  - (18,24,-30)= 6
  - (13,34,8)= 1

Ước chung lớn nhất (UCLN)

- *Định lý:*
  - Tồn tại UCLN của các số nguyên không đồng thời bằng 0
- *Nhận xét:*
  - (a,b) = (|a| , |b|)
  - (a,b)=(b,a): UCLN có tính giao hoán
  - (a,b,c)=((a,b),c)=(a,(b,c)): UCLN có tính kết hợp

Ước chung lớn nhất (UCLN)

- *Số nguyên tố cùng nhau:* UCLN của các a_i (i=1,2,...,n) bằng 1 thì các a_i được gọi là nguyên tố cùng nhau
- *Số nguyên tố sánh đôi:* Hai số bất kỳ trong các số $a_1,a_2,\ldots,a_n$ là nguyên tố cùng nhau, thì các số $a_1,a_2,\ldots,a_n$ được gọi là nguyên tố sánh đôi
- Nếu $a_1,a_2,\ldots,a_n$ là nguyên tố sánh đôi thì $a_1,a_2,\ldots,a_n$ là nguyên tố cùng nhau
- *Ví dụ:*
  - (2,5,12,15) = 1 ⇨ 2,5,12,15 là các số nguyên tố cùng nhau
  - (4, 21,19,11) là các số nguyên tố sánh đôi

Các tính chất của UCLN

1. Nếu $(a_1, a_2, \ldots, a_n) = d$ thì tồn tại các số nguyên $x_1, x_2, \ldots, x_n$ sao cho: $a_1x_1 + a_2x_2 + \ldots + a_nx_n = d$
2. Nếu m là số nguyên dương thì

   $(ma_1, ma_2, \ldots, ma_n) = m(a_1, a_2, \ldots, a_n)$
3. Nếu $d > 0$ là UC của $a_1, a_2, \ldots, a_n$ thì

$$\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) = \frac{(a_1, a_2, \ldots, a_n)}{d}$$

Các tính chất của UCLN

4. Nếu d>0 là UC của $a_1,a_2,\ldots,a_n$ thì d là UCLN của $a_1,a_2,\ldots,a_n$ khi và chỉ khi

$$\left(\frac{a_1}{d},\frac{a_2}{d},\ldots\ldots,\frac{a_n}{d}\right)=1$$

5. Nếu b>0 là ước của a thì (a,b) = b, đặc biệt (0,b) = b
6. Nếu c|ab và (a,c)=1 thì c | b
7. Nếu b|a và c|a và (b,c) = 1 thì bc | a
8. Nếu (a,b)=1 thì (ac,b) = (c,b)
9. Nếu (a, b) = (a, c) = 1 thì (a, bc) = 1

Ước chung lớn nhất (UCLN)

- *Định lý:*
  - Nếu a và b là hai số nguyên dương
  - Và $a = bq + r$ với $0 \leq r < b$ thì: $(a,b) = (b,r)$
- *Thuật toán Euclid tìm UCLN:*
  - Thực hiện phép chia có dư a cho b,
    - Nếu a chia hết cho b thì $(a,b) = b$
    - Nếu a không chia hết cho b, $a = bq + r$ thì $(a,b) = (b,r)$
  - ⇨ Thực hiện phép chia có dư b cho r
  - ....
  - Quá trình thực hiện sẽ dừng sau một số hữu hạn bước
- *Ví dụ:*
  - $(51,45) = (45,6) = (6,3) = 3$

Bội chung nhỏ nhất (BCNN)

- $a_1, a_2, \ldots, a_n$ là các số nguyên khác 0
- Số nguyên M được gọi là **bội chung** của các a_i (i=1,2,...,n) khi và chỉ khi M là bội của mỗi a_i
- Bội chung M của các a_i (i=1,2,...,n) được gọi là **bội chung nhỏ nhất** (BCNN) của các a_i nếu và chỉ nếu M là ước của mọi bội chung của các a_i
- *Ký hiệu:* $M = [a_1, a_2, \ldots, a_n]$
- *Quy ước:* BCNN là một số nguyên dương
- *Ví dụ:*
  - *[2,3,4] = 12*
  - *[7,3,5] = 105*

Bội chung nhỏ nhất (BCNN)

- *Nhận xét*
  - [a,b] = [|a|,|b|]
  - [a,b]=[b,a]: BCNN có tính chất giao hoán
  - [a,b,c]=[a,[b,c]]=[[a,b],c]: BCNN có tính chất kết hợp
- *Định lý về sự tồn tại BCNN:*
  - Luôn luôn tồn tại BCNN của các số nguyên khác không a_1, a_2,...,a_n cho trước

Bội chung nhỏ nhất (BCNN)

- *Định lý tìm BCNN*
  - Với hai số nguyên a và b khác 0, ta có:

$$[a, b] = \frac{|ab|}{(a, b)}$$

$$[90, -84] = [90, 84] = \frac{90.84}{(90.84)} = \frac{90.84}{6} = 1260$$

Các tính chất của BCNN

$a_1, a_2,.....,a_n$ là các số nguyên khác 0

1. Nếu $d = (a_1, a_2,.....,a_n)$ thì:

$$\left[\frac{a_1}{d}, \frac{a_2}{d}, \ldots\ldots, \frac{a_n}{d}\right] = \frac{[a_1, a_2, \ldots\ldots, a_n]}{d}$$

2. Nếu $a_1, a_2,.....,a_n$ là các số nguyên tố sánh đôi thì:

$$[a_1, a_2,.....,a_n] = a_1 a_2 \ldots\ldots a_n$$

Các tính chất của BCNN

$a_1, a_2, \ldots\ldots, a_n$ là các số nguyên khác 0

1. Nếu số nguyên M>0 là bội chung của $a_1, a_2, \ldots\ldots, a_n$ thì:

$M = [a_1, a_2, \ldots\ldots, a_n]$ khi và chỉ khi

$$\left(\frac{M}{a_1}, \frac{M}{a_2}, \ldots\ldots, \frac{M}{a_n}\right) = 1$$

2. Nếu k>0 là một số nguyên thì:

$[ka_1, ka_2, \ldots\ldots, ka_n] = k[a_1, a_2, \ldots\ldots, a_n]$

SỐ NGUYÊN TỐ VÀ HỢP SỐ

Số nguyên tố (SNT)

- Số nguyên p>1 được gọi là **số nguyên tố** nếu p không có ước số dương nào khác ngoài 1 và chính nó.
- Hay số nguyên p>1 được gọi là số nguyên tố nếu p chỉ có hai ước số dương là 1 và p
- ***Ví dụ:***
  - 2,3,5,7,........ là các số nguyên tố

Hợp số

- Số nguyên a>1 được gọi là hợp số nếu a có ước số dương khác 1 và khác chính nó.
- Hay số nguyên a>1 được gọi là hợp số nếu a không phải là số nguyên tố
- *Ví dụ:*
  - 4, 6, 8, 9,....... là các hợp số

Số nguyên tố và Hợp số

- ***Định lý:***
- Ước số dương nhỏ nhất khác 1 của số nguyên lớn hơn 1 là một số nguyên tố
- ***Ví dụ:***
  - Các ước số dương lớn hơn 1 của 20 là: 2, 4, 5, 10, 20; ⇨ 2 là nguyên tố
  - Các ước số dương lớn hơn 1 của 45 là: 3, 5, 9, 15, 45; ⇨ 3 là nguyên tố

⇨ **Mọi số nguyên lớn hơn 1 đều có ước là số nguyên tố**

Số nguyên tố và Hợp số

- *Định lý Euclid:*
    - Tập hợp các số nguyên tố là vô hạn

⇨ tập hợp số nguyên tố là không rỗng.

⇨ không thể liệt kê tất cả các số nguyên tố

Bảng số nguyên tố

- Phương pháp sàng (Erathosthene): liệt kê tất cả các số nguyên tố trên một đoạn
- *Bổ đề:* Nếu a>1 là hợp số thì a có ít nhất một ước số nguyên tố không vượt quá $\sqrt{a}$
- ⇨ lập bảng các số nguyên tố không vượt quá một số n>1 cho trước, gọi là sàng Erathosthene:
  1. Viết dãy số từ 2 đến n
  2. Tìm các số nguyên tố từ 2 đến $\sqrt{n}$
  3. Xóa đi các bội thực sự của các số nguyên tố này
  4. Các số còn lại là các số nguyên tố cần tìm

Tìm SNT không quá 100

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	16	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Bảng số nguyên tố

- *Nhận xét:*
  - a>1 là số nguyên
  - Nếu a không có ước nguyên tố trong khoảng từ 1 đến $\sqrt{a}$ thì a là số nguyên tố
  - *Ví dụ:* Xét số 257, $\sqrt{257} < 17$

    Các số nguyên tố không vượt quá 17 là ?

    2, 3, 5, 7, 11, 13 đều không là ước của 257

    ⇨ 257 là số nguyên tố

Định lý cơ bản của số học

- *Bổ đề:*
  - Nếu p là số nguyên tố, a là số nguyên ≥ 0 thì
    - Hoặc p là ước của a: p|a
    - Hoặc p và a là nguyên tố cùng nhau: (a,p) = 1
  - Nếu một tích các số nguyên chia hết cho số nguyên tố p thì phải có ít nhất một thừa số của tích đó chia hết cho p
- *Hệ quả:* Nếu tích các số nguyên tố chia hết cho số nguyên tố p thì p phải trùng với một trong các thừa số của tích đó

Định lý cơ bản của số học

- Mỗi số nguyên a>1 đều có thể phân tích thành tích của các thừa số nguyên tố và sự phân tích đó là **duy nhất** nếu không kể đến thứ tự các thừa số
  - 8 = 2.2.2
  - 18 = 2.3.3
- *Dạng phân tích tiêu chuẩn*
  - Những thừa số nguyên tố khi phân tích số nguyên a>1 có thể trùng nhau
  - Gọi p_1, p_2,...,p_n là các thừa số nguyên tố khác nhau từng đôi một và αi (i=1,2,...,n) là số lần xuất hiện của chúng thì dạng phân tích tiêu chuẩn của a:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$$

Một số vấn đề về SNT


Pierre de Fermat

- *Số nguyên tố thứ n*
  - $p_1 = 2$, $p_2 = 3$, $p_3 = 5$
  - ....
  - ⇨ Công thức tính số nguyên tố thứ n?
- *Số nguyên tố Fermat:*

$$F_n = 2^{2^n} + 1 \qquad (n = 0,1,2....)$$

⇨ $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$ là các số nguyên tố

⇨ Euler chỉ ra rằng F_5 là hợp số ☺

Một số vấn đề về SNT

- *Giả thiết Goldbach-Euler*

1)- Có phải chăng mọi số nguyên lẻ lớn hơn 5 đều được biểu diễn thành tổng của 3 số nguyên tố?

- 25 = 3+11+11 = 7+7+11

2)- Có phải chăng mọi số chẵn lớn hơn 2 đều được biểu diễn thành tổng của 2 số nguyên tố?

- 34 = 5+29 = 3+31

PHƯƠNG TRÌNH NGUYÊN

Phương trình nguyên

- *Định nghĩa:* **Phương trình(PT) có**
  - ẩn số: số nguyên
  - hệ số: số nguyên
  - tìm nghiệm nguyên

⇨ phương trình nguyên

- *Ví dụ:* Tìm x, y, z $\in$Z
  - $7x + 4y = 100$
  - $x^2 + y^2 = z^2$
  - $x^3 - 7y^2 = 1$

PT nguyên bậc nhất 2 ẩn

- *Định nghĩa:* **Phương trình có dạng**
  - **$ax + by = c$**
  - $a,b \in Z$ là các hệ số
  - $x,y \in Z$ là các ẩn số cần xác định giá trị
- *Ví dụ:*
  - Tìm $x, y \in Z : 7x + 4y = 100$

PT nguyên bậc nhất 2 ẩn

- *Định lý:* Tìm nghiệm của phương trình $ax + by = c$ (1)
- **$d = (a,b)$**.
- Khi đó:
  - Nếu d không là ước của c thì (1) không có nghiệm nguyên
  - Nếu d là ước của c thì (1) có vô số nghiệm nguyên. Khi (x_0,y_0) là một nghiệm nguyên nào đó của (1) thì mọi nghiệm nguyên (x, y) của (1) có dạng:

$$\begin{cases} x = x_0 + \dfrac{b}{d}t \\ y = y_0 - \dfrac{a}{d}t \end{cases} \quad t \in Z$$

PT nguyên bậc nhất 2 ẩn

- *Ví dụ:* Tìm nghiệm của phương trình 2x -3y = 5
  - d = (2,-3)=1|5: PT có nghiệm nguyên
  - Một nghiệm nguyên: $x_0 = 4$, $y_0 = 1$
  - Nghiệm nguyên tổng quát: $\begin{cases} x = 4 - 3t \\ y = 1 - 2t \end{cases} \quad t \in Z$
  - Với t = -1 thì x = 7 y = 3
  - Với t = 0 thì x = 4 y = 1
  - Với t = 1 thì x = 1 y = -1
  - Với t = 2 thì x = -2 y = -3
  - ....

PT nguyên bậc nhất 2 ẩn

- *Giải trực tiếp phương trình nguyên* ax +by = c (1)

1)- Nếu |a|=1 hay |b|=1 thì việc tìm nghiệm nguyên của phương trình (1) coi như được giải quyết xong

Ví dụ: Giải phương trình : x - 4y = 2

- Phương trình này tương đương với x=2+4y
- Nghiệm của phương trình có dạng:

$$\begin{cases} x = 2 + 4t \\ y = t \end{cases} \qquad t \in Z$$

PT nguyên bậc nhất 2 ẩn

- *Giải trực tiếp phương trình nguyên* $ax + by = c$ (1)

2)- Trong trường hợp $|a|$ và $|b|$ đều khác 0 và khác 1 thì chuyển việc tìm nghiệm nguyên của phương trình (1) về việc tìm nghiệm nguyên của phương trình bậc nhất hai ẩn mà ít nhất một hệ số của ẩn là ± 1

Ví dụ: Giải phương trình: $47x - 17y = 5$

PT nguyên bậc nhất 2 ẩn

- *Giải trực tiếp phương trình nguyên* ax +by = c (1)

Ví dụ: Giải phương trình : 47x - 17y = 5

Phương trình này tương đương với 17(2x-y)+13x=5

$$\Leftrightarrow \begin{cases} u = 2x - y \\ 17u + 13x = 5 \end{cases} \Leftrightarrow \begin{cases} u = 2x - y \\ 13(u + x) + 4u = 5 \end{cases}$$

$$\Leftrightarrow \begin{cases} u = 2x - y \\ \mathrm{v} = \mathrm{u} + \mathrm{x} \\ 13v + 4u = 5 \end{cases} \Leftrightarrow \begin{cases} u = 2x - y \\ \mathrm{v} = \mathrm{u} + \mathrm{x} \\ 4(3v + u) + v = 5 \end{cases} \Leftrightarrow \begin{cases} u = 2x - y \\ \mathrm{v} = \mathrm{u} + \mathrm{x} \\ \mathrm{t} = 3\mathrm{v} + \mathrm{u} \\ 4t + v = 5 \end{cases}$$

Phương trình sau cùng có hệ số của v bằng 1

⇨ v = 5 - 4t $t \in Z$

PT nguyên bậc nhất 2 ẩn

- *Giải trực tiếp phương trình nguyên* ax +by = c (1)

Ví dụ: Giải phương trình: 47x - 17y = 5

$$\Leftrightarrow \begin{cases} u = 2x - y \\ v = u + x \\ t = 3v + u \\ 4t + v = 5 \end{cases}$$

⇨ v = 5 - 4t $t \in Z$

⇨ u = t - 3v = t - 3(5 - 4t) = -15 + 13t

x = v - u = (5 - 4t) -(-15 + 13t) = 20 -17t

y = 2x - u = 2(20 -17t) - (-15 +13t) = 55 - 47t

⇨Nghiệm của phương trình: $\begin{cases} x = 20 - 17t \\ y = 55 - 47t \end{cases} \quad t \in Z$

PT nguyên bậc nhất nhiều ẩn

- *PT nguyên bậc nhất n>2 ẩn:*
  - $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ (1)
  - $a_1, x_1 \in Z$, i=1,2,…,n
- *Định lý:*
  - Một phương trình nguyên bậc nhất n ẩn có nghiệm nguyên khi và chỉ khi hệ số của các ẩn là nguyên tố cùng nhau

Giải phương trình nguyên bậc nhất n ẩn rất phức tạp.

⇨Xét ví dụ cụ thể

PT nguyên bậc nhất nhiều ẩn

- *Giải PT:* 2x - 5y - 6z = 4 (1)
- Vì (2,-5,-6)= 1 nên PT có nghiệm nguyên.
- Ta có (2,-5)=1

  (1)⇔2x - 5y = 4 + 6z ⇔ $\begin{cases} z = u \\ c = 4 + 6z = 4 + 6u \\ 2x - 5y = c \end{cases}$
- Phương trình cuối có một nghiệm là (3c,c) nên có nghiệm tổng quát là: $\begin{cases} x = 3c - 5t = 3(4 + 6u) - 5t = 12 + 18u - 5t \\ y = c - 2t = 4 + 6u - 2t \end{cases}$
- Vậy nghiệm của PT(1) $\begin{cases} x = 12 + 18u - 5t \\ y = 4 + 6u - 2t \quad u, t \in Z \\ z = u \end{cases}$

PT nguyên bậc nhất nhiều ẩn

- *Giải PT:* 6x + y + 3z = 15 (2)
- Vì (6,1,3) = 1 nên PT có nghiệm nguyên
- PT có hệ số của ẩn y bằng 1
  ⇨ x, z có giá trị nguyên bất kỳ
- Vậy nghiệm của PT (2)

$$\begin{cases} x = u \\ z = t \\ y = 15 - 6u - 3t \end{cases} \qquad u, t \in Z$$

PT nguyên bậc nhất nhiều ẩn

- *Giải PT:* 6x +15y + 10z = 3 (3)
- Vì (6,15,10) = 1 nên PT có nghiệm nguyên
- Do các hệ số của PT không có cặp các nguyên tố cùng nhau nên giải (3) ta đặt ẩn phụ để đưa về dạng pt có chứa hệ số bằng 1
- (3) ⇔6x+10(y+z)+5y=3

$$\Leftrightarrow \begin{cases} y+z=u \\ 6x+10u+5y=3 \end{cases} \Leftrightarrow \begin{cases} y+z=u \\ x+10u+5(y+x)=3 \end{cases}$$

$$\Leftrightarrow \begin{cases} y+z=u \\ x+y=v \\ x+10u+5v=3 \end{cases}$$

PT nguyên bậc nhất nhiều ẩn

- *Giải PT:* $6x + 15y + 10z = 3$ (3) $\Leftrightarrow \begin{cases} y + z = u \\ x + y = v \\ x + 10u + 5v = 3 \end{cases}$
- PT cuối có hệ số của x bằng 1 nên

$$\begin{cases} x = 3 - 10u - 5v \\ y = v - x = v - (3 - 10u - 5v) = -3 + 10u + 6v \\ z = u - y = u - (-3 + 10u + 6v) = 3 - 9u - 6v \end{cases}$$

- Vậy nghiệm của PT (3) $\begin{cases} x = 3 - 10u - 5v \\ y = -3 + 10u + 6v \quad\quad u, v \in Z \\ z = 3 - 9u - 6v \end{cases}$

Phương trình nguyên bậc cao

- 1)- Tìm nghiệm nguyên ≥ 0 của PT:

$$2x^3 + xy = 7$$

$$\Leftrightarrow x(2x^2 + y) = 7$$

Vì 7 là số nguyên tố nên:

$$\begin{cases} x = 1 \\ 2x^2 + y = 7 \end{cases} \quad \text{hoặc} \quad \begin{cases} x = 7 \\ 2x^2 + y = 1 \end{cases}$$

- Giải hệ, ta được:

$$x = 1 \quad y = 5$$

Phương trình nguyên bậc cao

- 2)- Tìm nghiệm nguyên của PT:

$$6x^2 + 5y^2 = 74$$

$$\Leftrightarrow 6(x^2 - 4) = 5(10 - y^2)$$

Vì (6,5)=1 nên

$$\begin{cases}(x^2-4)\,\vdots\,5\\(10-y^2)\,\vdots\,6\end{cases} \Leftrightarrow \begin{cases}x^2-4=5u\\10-y^2=6v\end{cases} \Leftrightarrow \begin{cases}x^2=4+5u\\y^2=10-6v\end{cases} \quad u, v \in Z$$

- Mặt khác: $6.5u = 5.\ 6v \Rightarrow u=v \Rightarrow \begin{cases}x^2 = 4+5u & (1)\\ y^2 = 10-6u & (2)\end{cases}$

Phương trình nguyên bậc cao

- 2)- Tìm nghiệm nguyên của PT:

$$6x^2 + 5y^2 = 74$$

$$\begin{cases} x^2 = 4 + 5u & (1) \\ y^2 = 10 - 6u & (2) \end{cases}$$

- Vì x^2, $y^2 \geq 0$ nên từ (1) và (2) $\Rightarrow$

$$\begin{cases} 4 + 5u \geq 0 \\ 10 - 6u \geq 0 \end{cases} \Rightarrow \begin{cases} u \geq -\dfrac{4}{5} \\ u \leq \dfrac{5}{3} \end{cases} \Rightarrow \left[\begin{array}{l} u = v = 0 \\ u = v = 1 \end{array} \right. \quad \text{vì } u, v \in Z$$

Phương trình nguyên bậc cao

- 2)- Tìm nghiệm nguyên của PT:

$$6x^2 + 5y^2 = 74$$

$$\begin{cases} 4+5u \geq 0 \\ 10-6u \geq 0 \end{cases} \Rightarrow \begin{cases} u \geq -\dfrac{4}{5} \\ u \leq \dfrac{5}{3} \end{cases} \Rightarrow \left[\begin{array}{l} u = v = 0 \\ u = v = 1 \end{array}\right. \quad \text{vì u, v} \in Z$$

- Với u=v=0:

$$\begin{cases} x^2 = 4+u = 4 \\ y^2 = 10-v = 10 \end{cases} \Leftrightarrow \begin{cases} x = \pm 2 \\ y = \pm\sqrt{10} \end{cases}$$

(loại, vì y không phải là số nguyên)

Phương trình nguyên bậc cao

- 2)- Tìm nghiệm nguyên của PT:

$$6x^2 + 5y^2 = 74$$

$$\begin{cases} 4+5u \geq 0 \\ 10-6u \geq 0 \end{cases} \Rightarrow \begin{cases} u \geq -\dfrac{4}{5} \\ u \leq \dfrac{5}{3} \end{cases} \Rightarrow \left[\begin{array}{l} u=v=0 \\ u=v=1 \end{array}\right. \quad \text{vì } u, v \in Z$$

- Với u=v=1:

$$\begin{cases} x^2 = 4+5=9 \\ y^2 = 10-6=4 \end{cases} \Leftrightarrow \begin{cases} x = \pm 3 \\ y = \pm 2 \end{cases}$$

(Nghiệm của pt)

Phương trình nguyên bậc cao

- 3)- Tìm nghiệm nguyên của PT:

$$x^2 + y^2 = 3z^2$$

- (0,0,0) là nghiệm của PT.
- CM bằng phản chứng: PT không có nghiệm nào khác
  - Giả sử (x, y, z) khác (0, 0, 0) là nghiệm của PT

    Gọi d= (x, y, z)$\neq$0 ta có:

    x= ad , y= bd , z= cd ; a, b, c là nguyên tố cùng nhau
  - Vì ad, bd, cd là nghiệm của PT nên:

    $(ad)^2 + (bd)^2 = 3(cd)^2$

  ⇨a, b, c không phải là nguyên tố cùng nhau (mâu thuẫn)
  - Vậy phương trình không có nghiệm khác (0, 0, 0)

Phương trình nguyên bậc cao

- 4)- Tìm nghiệm nguyên dương của PT:

$$x + y + z = xyz$$

- Giả sử $0 < x \le y \le z$ thì $x+y+z \le 3z$
- Vì $x+y+z = xyz$ nên $xyz \le 3z$. ⇨ $xy \le 3$. Ta có các TH:
  - $xy=3 \Rightarrow x=1$ và $y=3 \Rightarrow 4+z = 3z \Rightarrow z=2$: mâu thuẫn
  - $xy=2 \Rightarrow x=1$ và $y=2 \Rightarrow 3+z = 2z \Rightarrow z=3$
  - $xy=1 \Rightarrow x=1$ và $y=1 \Rightarrow 2+z = z$: mâu thuẫn
- Vậy (1,2,3) và các hoán vị của nó là nghiệm của PT

Phương trình nguyên bậc cao

- Định lý của PT nguyên bậc cao dạng

$$x^n + y^n = z^n \quad (1)$$

- n=2, PT Pythagor, nghiệm nguyên PT có dạng

$$\begin{cases} x = m(p^2 - q^2) \\ y = 2mpq \\ z = m(p^2 + q^2) \end{cases}$$

- *Trong đó:*
  - m,p,q là số nguyên
  - (p,q)=1
  - p và q chẵn lẻ khác nhau

Phương trình nguyên bậc cao

- Định lý của PT nguyên bậc cao dạng

  $x^2 + y^2 = z^2$ (1)

- Vài nghiệm được tìm từ công thức trên:

  3 4 5   5 12 13

  7 24 25   8 15 17 ....

Phương trình nguyên bậc cao

- Định lý của PT nguyên bậc cao

$$x^n + y^n = z^n \quad (1)$$

- Fermat: Với mọi số nguyên n > 2, PT (1) không có nghiệm nguyên khác không

QUAN HỆ ĐỒNG DƯ

Quan hệ đồng dư

- *Định nghĩa:*
  - a, b, m>0 là các số nguyên
  - a được gọi là **đồng dư** với b theo modulo m
  - nếu a có cùng số dư với b khi chia cho m
  - *Ký hiệu:*

$$a \equiv b \pmod m$$

Quan hệ đồng dư

- *Nhận xét:*
  1. $a \equiv b \pmod{m}$ khi và chỉ khi $b \equiv a \pmod{m}$
  2. a chia hết cho m khi và chỉ khi $a \equiv 0 \pmod{m}$
  3. Quan hệ đồng dư là một quan hệ tương đương
- *Ví dụ:*
  - $16 \equiv 11 \pmod{5}$ $\quad$ $16 \equiv 6 \pmod{5}$ $\quad$ $16 \equiv 1 \pmod{5}$
  - $-7 \equiv 2 \pmod{3}$ $\quad$ $-7 \equiv 5 \pmod{3}$ $\quad$ $12 \equiv 0 \pmod{2}$
  - $12 \equiv 4 \pmod{2}$

Quan hệ đồng dư

- *Định lý:*
  - a, b , m>0 là các số nguyên
  - Những mệnh đề sau đây là tương đương:

    1)- $a \equiv b \pmod{m}$

    2)- $a = b+mt$ (t là một số nguyên)

    3)- $(a - b) \equiv 0 \pmod{m}$

Tính chất của quan hệ đồng dư

- *m là số nguyên dương*

1)- Nếu $a_i \equiv b_i$ (mod m) (i=1,2,..., n) thì

$(a_1+a_2+....+a_n) \equiv (b_1+b_2+....+ b_n)$ (mod m)

$(a_1.a_2......a_n) \equiv (b_1.b_2......b_n)$ (mod m)

2)- $a \equiv b$ (mod m) $\Leftrightarrow$ $(a\pm c) \equiv (b\pm c)$ (mod m)

(c là một số nguyên)

3)- $a \equiv b$ (mod m) $\Leftrightarrow$ $a \equiv (b+km)$ (mod m)

$\Leftrightarrow$ $(a+km) \equiv b$ (mod m), (k là một số nguyên)

Tính chất của quan hệ đồng dư

- *m là số nguyên dương*

4)- Nếu $a \equiv b \pmod{m}$ thì $a^n \equiv b^n \pmod{m}$

(n là số nguyên dương)

5)- Nếu $a \equiv b \pmod{m}$ thì $ac \equiv bc \pmod{m}$

(c là một số nguyên)

Nếu $(c,m)=1$

thì $a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{m}$

6)- Nếu c là số nguyên dương

thì $a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{mc}$

Tính chất của quan hệ đồng dư

- *m là số nguyên dương*

7)- Nếu d>0 là ước chung của a, b, m thì

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

8)- Nếu d là ước chung của a, b và (d,m)=1 thì

$$a \equiv b\,(\mathrm{mod}\ m) \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d}\,(\mathrm{mod}\ \ m)$$

Tính chất của quan hệ đồng dư

- *m là số nguyên dương*

9)- Nếu $a \equiv b \pmod{m_i}$ $(i=1,2,\ldots, n)$
và $m = [m_1,m_2,\ldots,m_n]$ thì $a \equiv b \pmod{m}$

10)- Nếu $a \equiv b \pmod{m}$ và $d>0$ là ước của m
thì $a \equiv b \pmod{d}$

11)- Nếu $a \equiv b \pmod{m}$ và d là ước chung của a, m thì d là ước của b

12)- Nếu $a \equiv b \pmod{m}$ thì $(a,m) = (b,m)$

Định lý Fermat nhỏ

- *Nếu p là số nguyên tố và a là số nguyên không chia hết cho p*

  $a^{p-1} \equiv 1 \pmod{p}$

- *Nếu p là số nguyên tố và a là số nguyên không chia hết cho p*

  $a^{p} \equiv a \pmod{p}$

Định lý Euler

- *Nếu n là số nguyên dương bất kỳ và a là số nguyên tố cùng nhau với n, thì*

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

  $\varphi(n)$ là phi hàm Euler đếm số các số nguyên giữa 1 và n nguyên tố cùng nhau với n

PHƯƠNG TRÌNH ĐỒNG DƯ

PT đồng dư một ẩn

- *Định nghĩa:*
  - Phương trình đồng dư bậc n một ẩn có dạng:

$$a_0x^n + a_1x^{n-1} + \dots\dots + a_{n-1}x + a_n \equiv b \pmod{m} \qquad (1)$$

  - Trong đó:
    - n, m nguyên dương
    - $a_i \in Z$ (i= 0,1,2,...,n) là các hệ số nguyên
    - a_0 không là bội của m
    - x là ẩn số nguyên
- *Ví dụ:*
  - $x^2+x+1 \equiv 1 \pmod{5}$
  - $9x \equiv 6 \pmod{15}$

PT đồng dư tương đương

- Khái niệm:
  - Hai phương trình đồng dư gọi là tương đương khi và chỉ khi tập hợp các giá trị nghiệm đúng phương trình này là tập hợp các giá trị nghiệm đúng phương trình kia
- *Ví dụ:*
  - $x^2 \equiv 1 \pmod 5 \Leftrightarrow x^2 + 2 \equiv 3 \pmod 5$

PT đồng dư bậc nhất một ẩn

- *Định nghĩa:*
  - Phương trình đồng dư bậc nhất một ẩn có dạng:

$$ax \equiv b \pmod{m}$$

PT đồng dư bậc nhất một ẩn

- *Định lý:*
  - Xét phương trình $ax \equiv b \pmod{m}$ (2)
  - $d = (a,m)$. Khi đó:

1)- Nếu d **không** là ước của b thì (2) **vô nghiệm**

2)- Nếu d là ước của b thì (2) có đúng d nghiệm. Gọi x_0 là một giá trị thỏa phương trình thì d nghiệm đó được xác định bởi công thức

$$\left[\begin{array}{l} x \equiv x_0 + 0.\dfrac{m}{d} \pmod{m} \\ x \equiv x_0 + 1.\dfrac{m}{d} \pmod{m} \\ \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv x_0 + (d-1).\dfrac{m}{d} \pmod{m} \end{array}\right.$$

PT đồng dư bậc nhất một ẩn

- ***Ví dụ:*** Giải phương trình đồng dư **$9x \equiv 6 \pmod{15}$**
  - d = (a,m) = (9,15) = 3 là ước của b = 6: phương trình có d = 3 nghiệm
  - Dư đầy đủ không âm nhỏ nhất modulo 15 là:
    0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
  - Một giá trị thỏa phương trình là **$x_0 = 4$**
  - Phương trình có ba nghiệm là:

$$\left[\begin{array}{ll} x \equiv 4 + 0.\frac{15}{3} & \pmod{15} \\ x \equiv 4 + 1.\frac{15}{3} & \pmod{15} \\ x \equiv 4 + 2.\frac{15}{3} & \pmod{15} \end{array}\right. \Leftrightarrow \left[\begin{array}{ll} x \equiv 4 & \pmod{15} \\ x \equiv 9 & \pmod{15} \\ x \equiv 14 & \pmod{15} \end{array}\right.$$

Hệ PT đồng dư bậc nhất một ẩn

- *Định nghĩa:* Hệ phương trình đồng dư bậc nhất một ẩn đơn giản:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots\dots\dots\dots\dots \\ x \equiv a_n \pmod{m_n} \end{cases} \qquad (1)$$

- a_i là các số nguyên, m_i là các số nguyên dương (i=1,2,...,n)

Hệ PT đồng dư bậc nhất một ẩn

- *Định nghĩa:* Hệ phương trình đồng dư bậc nhất một ẩn đơn giản:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \ldots\ldots\ldots\ldots \\ x \equiv a_n \pmod{m_n} \end{cases} \quad (1)$$

- Nếu với $x_0 \in Z$, ta có đồng thời các đồng dư thức:

$$\begin{cases} x_0 \equiv a_1 \pmod{m_1} \\ x_0 \equiv a_2 \pmod{m_2} \\ \quad \ldots\ldots\ldots\ldots \\ x_0 \equiv a_n \pmod{m_n} \end{cases} \quad (1)$$

- x_0 được gọi là một giá trị nghiệm đúng (1)

Hệ PT đồng dư bậc nhất một ẩn

- *Giải hệ phương trình:* Tìm tất cả các giá trị nghiệm đúng hệ phương trình đồng dư
- *Nhận xét:*
  - Khi số nguyên x_0 là một giá trị nghiệm đúng (1) thì mọi số nguyên thuộc lớp $\overline{x_0}$ gồm các x sao cho $x \equiv x_0 \pmod{m}$
  - $m = [m_1, m_2, ..., m_n]$, cũng là các giá trị nghiệm đúng (1)
  - Lớp $\overline{x_0}$ là một nghiệm của hệ phương trình đồng dư(1)

Hệ PT đồng dư bậc nhất một ẩn

- *Định lý Trung Quốc về phần dư:*

Xét hệ phương trình

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \ldots\ldots\ldots\ldots\ldots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \ldots\ldots\ldots\ldots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

Hệ PT đồng dư bậc nhất một ẩn

- Định lý Trung Quốc về phần dư:
  - Nếu các modulo m_1, m_2,..., m_n là nguyên tố sánh đôi thì hệ có nghiệm duy nhất x được xác định
  - Tính $M = [m_1, m_2, \ldots, m_n] = m_1 m_2 \ldots m_n$
  - Tính $M_i = \dfrac{M}{m_i} \quad (i = 1,2,\ldots,n)$
  - Giải các PT đồng dư $M_i y \equiv a_i \pmod{m_i} \quad (i = 1,2,\ldots,n)$
  - ⇨ tìm được các nghiệm $y \equiv N_i \pmod{m_i} \quad (i = 1,2,\ldots,n)$
  - Nghiệm của hệ:

$$x \equiv M_1 N_1 + M_2 N_2 + \ldots + M_n N_n \pmod{M}$$

Hệ PT đồng dư bậc nhất một ẩn

- Ví dụ áp dụng Định lý Trung Quốc về phần dư:
  - Giải hệ PT:

$$\begin{cases} x \equiv 2 \pmod{3} & (1) \\ x \equiv 3 \pmod{5} & (2) \\ x \equiv 4 \pmod{7} & (3) \end{cases}$$

  - Các modulo nguyên tố sánh đôi ⇨ áp dụng định lý Trung Quốc về phần dư
  - Tính M = [3,5,7] = 3.5.7 = 105

$$\begin{cases} x \equiv 2 \pmod{3} & (1) \\ x \equiv 3 \pmod{5} & (2) \\ x \equiv 4 \pmod{7} & (3) \end{cases}$$

Hệ PT đồng dư bậc nhất một ẩn

- Ví dụ áp dụng Định lý Trung Quốc
  - M = [3,5,7] = 3.5.7 = 105
  - Tính

$$\begin{cases} M_1 = \dfrac{M}{m_1} = \dfrac{105}{3} = 35 \\ M_2 = \dfrac{M}{m_2} = \dfrac{105}{5} = 21 \\ M_3 = \dfrac{M}{m_3} = \dfrac{105}{7} = 15 \end{cases}$$

⇨ Giải các PT đồng dư

Hệ PT đồng dư bậc nhất một ẩn

$$\begin{cases} x \equiv 2 \pmod{3} & (1) \\ x \equiv 3 \pmod{5} & (2) \\ x \equiv 4 \pmod{7} & (3) \end{cases}$$

$$\begin{cases} M_1 = \dfrac{M}{m_1} = \dfrac{105}{3} = 35 \\ M_2 = \dfrac{M}{m_2} = \dfrac{105}{5} = 21 \\ M_3 = \dfrac{M}{m_3} = \dfrac{105}{7} = 15 \end{cases}$$

- Ví dụ áp dụng Định lý Trung Quốc
  - M = [3,5,7] = 3.5.7 = 105. Tính
  - ⇨ Giải các PT đồng dư

$$35y \equiv 2 \pmod{3} \Leftrightarrow y \equiv 1 \pmod{3}$$

$$21y \equiv 3 \pmod{5} \Leftrightarrow y \equiv 3 \pmod{5}$$

$$15y \equiv 4 \pmod{7} \Leftrightarrow y \equiv 4 \pmod{7}$$

  - Nghiệm của hệ:

$$x \equiv (35.1+21.3+15.4) \pmod{105}$$

$$\Leftrightarrow x \equiv 158 \pmod{105}$$

$$\Leftrightarrow x \equiv 53 \pmod{105}$$

Hệ PT đồng dư bậc nhất một ẩn

- Giải hệ PT đồng dư bậc nhất một ẩn bằng phương pháp thế: **Hệ PT có n>2 hai phương trình**
  - Bước 1: giải hệ hai phương trình nào đó của hệ
  - Bước 2: thay hai phương trình này bằng nghiệm vừa tìm được ⇨ hệ có n-1 phương trình
  - Bước 3: Tiếp tục áp dụng các bước 1, 2 để giải cho đến khi hệ còn 2 pt
  - Bước 4: Áp dụng phương pháp thế đối với hệ có 2 PT

Hệ PT đồng dư bậc nhất một ẩn

- Ví dụ: Giải hệ PT đồng dư bậc nhất một ẩn bằng phương pháp thế

$$\begin{cases} x \equiv 5 \pmod{6} \\ x \equiv 8 \pmod{15} \end{cases}$$

$$\Leftrightarrow \begin{cases} x = 8 + 15t \quad (t \in Z) \\ 8 + 15t \equiv 5 \pmod{6} \end{cases}$$

$$\Leftrightarrow \begin{cases} x = 8 + 15t \quad (t \in Z) \\ 15t \equiv -3 \pmod{6} \end{cases}$$

$$\Leftrightarrow \begin{cases} x = 8 + 15t \quad (t \in Z) \\ 3t + 12t \equiv -3 \pmod{6} \end{cases}$$

Hệ PT đồng dư bậc nhất một ẩn

- Ví dụ: Giải hệ PT đồng dư bậc nhất một ẩn bằng
- phương pháp thế

$$\Leftrightarrow \begin{cases} x = 8 + 15t & (t \in Z) \\ 3t \equiv -3 \pmod{6} \end{cases}$$

chia tất cả cho 3

$$\Leftrightarrow \begin{cases} x = 8 + 15t & (t \in Z) \\ t \equiv -1 \pmod{2} \end{cases}$$

$$\Leftrightarrow \begin{cases} x = 8 + 15t & (t \in Z) \\ t = -1 + 2k & (k \in Z) \end{cases}$$

$\Leftrightarrow$ x = 8+15(-1+2k) = -7 + 30k

$\Leftrightarrow$x $\equiv$ -7 (mod 30)

$\Leftrightarrow$x $\equiv$ 23 (mod 30)

Hệ PT đồng dư bậc nhất một ẩn

- Ví dụ: Giải hệ PT đồng dư bậc nhất một ẩn bằng phương pháp thế

$$\begin{cases} x \equiv 4 \pmod{5} & (1) \\ x \equiv 1 \pmod{12} & (2) \\ x \equiv 7 \pmod{14} & (3) \end{cases}$$

- Từ (1), ta có: x = 4+k5
- Thay vào (2): 4+k5 $\equiv$ 1 (mod 12)

$\Leftrightarrow$ 5k $\equiv$ -3 (mod 12)

$\Leftrightarrow$ 5k $\equiv$ (-3+4.12) (mod 12)

$\Leftrightarrow$ 5k $\equiv$ 45 (mod 12) (chia 2 vế cho 5, (5,12)=1)

$\Leftrightarrow$ k $\equiv$ 9 (mod 12)

$\Leftrightarrow$ k = 9+12m

Hệ PT đồng dư bậc nhất một ẩn

- Ví dụ áp dụng Giải hệ PT đồng dư bậc nhất một ẩn bằng phương pháp thế

$$\begin{cases} x \equiv 4 \pmod{5} & (1) \\ x \equiv 1 \pmod{12} & (2) \\ x \equiv 7 \pmod{14} & (3) \end{cases}$$

$\Leftrightarrow k = 9+12m$

- Thay vào (1): $x= 4+(9+12m).5=49+60m$

$\Leftrightarrow x \equiv 49 \pmod{60}$

- ⇨ Xét hệ:

$$\begin{cases} x \equiv 49 \pmod{60} & (*) \\ x \equiv 7 \pmod{14} & (**) \end{cases}$$

Hệ PT đồng dư bậc nhất một ẩn

- Ví dụ:Giải hệ PT đồng dư bậc nhất một ẩn bằng phương pháp thế

$$\begin{cases} x \equiv 49 \pmod{60} & (*) \\ x \equiv 7 \pmod{14} & (**) \end{cases}$$

- Từ (**) ta có: $x = 7+k.14$
- Thay vào (*) $7+14k \equiv 49 \pmod{60}$

$\Leftrightarrow 14k \equiv 42 \pmod{60}$ (chia 2 vế cho 7 , (7,60)=1)

$\Leftrightarrow 2k \equiv 6 \pmod{60}$ (chia tất cả cho 2)

$\Leftrightarrow k \equiv 3 \pmod{30}$

$\Leftrightarrow k = 3+ 30.m$

- Thay vào (**): $x = 7+(3+30m).14 = 49+420.m$

$\Leftrightarrow x \equiv 49 \pmod{420}$