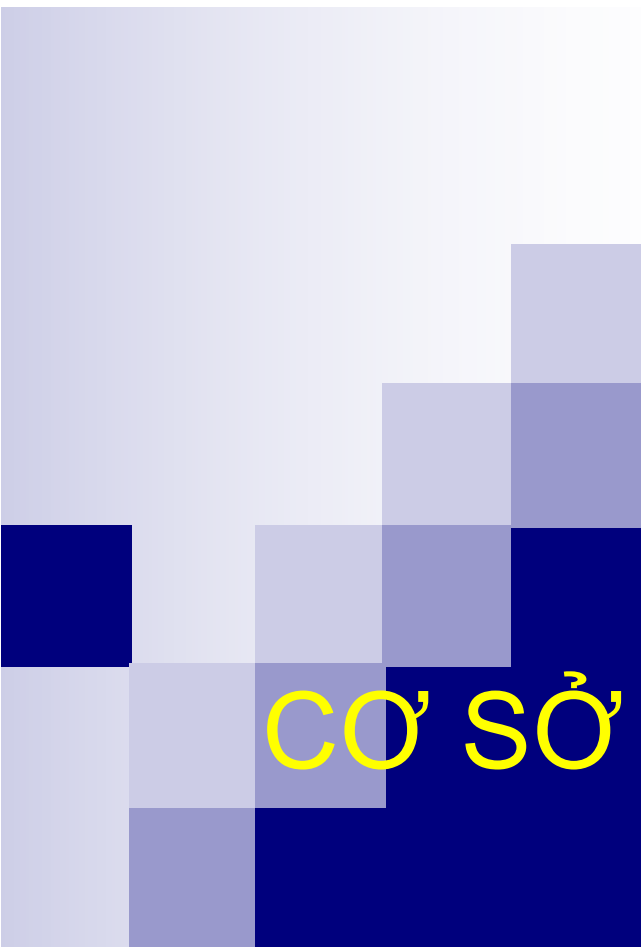




CƠ SỞ TOÁN CHO LÝ THUYẾT MẬT MÃ



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. Quan hệ đồng dư
5. Shannon entropy



PHÉP CHIA HẾT VÀ CÓ DƯ

Phép chia hết

■ Định nghĩa:

□ Xét $a, b \in \mathbb{Z}$ 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 $q \in \mathbb{Z}$ sao cho: $a = bq$

■ *Ký hiệu:* $b \mid a \Leftrightarrow \exists q \in \mathbb{Z} \text{ sao cho } a = bq \Leftrightarrow a : b$

■ *Ví dụ:* 3 chia hết 6 không?

$$a = 6 \quad b = 3 \quad q = 2$$

$$\exists 2 \in \mathbb{Z}, 6 = 3 \cdot 2$$

Phép chia hết

■ Nhận xét:

□ Với mọi $b \neq 0$ thì

■ 0 chia hết cho b vì $0 = b \cdot 0$

■ Vậy 0 là bội của mọi số nguyên $b \neq 0$

□ Với mọi a thì

■ $1 \mid a$ vì $a \in \mathbb{Z}$, $a = 1 \cdot a$

■ 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. $(\forall a \neq 0, \forall b \neq 0, a|b \text{ và } b|a)$ 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 $(a|b \text{ và } b|c)$ 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

□ $a, b \in \mathbb{Z}$ và $b \neq 0$

□ Tồn tại duy nhất cặp số nguyên q và $r \in \mathbb{Z}$ sao cho:

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

■ q được gọi là **thương**, r được gọi là **số dư**

□ Khi $r = 0 \Rightarrow$ ta có **phép chia hết**

■ Ví dụ: Hãy tìm q và r ?

$$a=7, b=2: q=3, r=1 \quad 7=2 \cdot 3 + 1$$

$$a=10, b=5: q=2, r=0 \quad 10=5 \cdot 2 + 0$$



UCLN VÀ BCNN

Ước chung lớn nhất (UCLN)

- $a_1, a_2, \dots, a_n$ là các số nguyên không đồng thời bằng 0
- Số nguyên $d \in \mathbb{Z}$ được gọi là **ước chung** của các a_i ($i=1, 2, \dots, n$) khi và chỉ khi **d là ước của mỗi a_i ($d|a_i$)**
- **Ước chung d** của các a_i ($i=1, 2, \dots, n$) 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:* $d = (a_1, a_2, \dots, a_n)$
- *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 ($i=1,2,\dots,n$) 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 $a_1, a_2, \dots, a_n$ là nguyên tố cùng nhau, thì các số $a_1, a_2, \dots, a_n$ được gọi là nguyên tố sánh đôi
- Nếu $a_1, a_2, \dots, a_n$ là nguyên tố sánh đôi thì $a_1, a_2, \dots, a_n$ là nguyên tố cùng nhau
- Ví dụ:
 - $(2, 5, 12, 15) = 1 \Rightarrow 2, 5, 12, 15$ 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 $(a_1, a_2, \dots, a_n) = d$ thì tồn tại các số nguyên $x_1, x_2, \dots, x_n$ sao cho: $a_1x_1 + a_2x_2 + \dots + a_nx_n = d$
2. Nếu m là số nguyên dương thì
 $(ma_1, ma_2, \dots, ma_n) = m(a_1, a_2, \dots, a_n)$
3. Nếu $d > 0$ là UC của $a_1, a_2, \dots, a_n$ thì

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

Các tính chất của UCLN

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

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

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)

- $a_1, a_2, \dots, a_n$ là các số nguyên khác 0
- Số nguyên M được gọi là **bội chung** của các a_i ($i=1,2,\dots,n$) khi và chỉ **khi M là bội của mỗi a_i**
- Bội chung M của các a_i ($i=1,2,\dots,n$) 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:* $M = [a_1, a_2, \dots, a_n]$
- *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 $a_1, a_2, \dots, a_n$ cho trước

Bội chung nhỏ nhất (BCNN)

■ Định lý tìm BCNN

□ Với hai số nguyên a và b khác 0, ta có:

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

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

Các tính chất của BCNN

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

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

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

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

$$[a_1, a_2, \dots, a_n] = a_1 a_2 \dots a_n$$

Các tính chất của BCNN

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

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

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

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

2. Nếu $k > 0$ là một số nguyên thì:

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



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; $\Rightarrow$ 2 là nguyên tố
- ☐ Các ước số dương lớn hơn 1 của 45 là: 3, 5, 9, 15, 45; $\Rightarrow$ 3 là nguyên tố

$\Rightarrow$ **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 $\sqrt{a}$
- $\Rightarrow$ 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	26	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 $p_1, p_2, \dots, p_n$ là các thừa số nguyên tố khác nhau từng đôi một và α_i ($i=1, 2, \dots, n$) là số lần xuất hiện của chúng thì **dạng phân tích tiêu chuẩn của a :**

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

Một số vấn đề về SNT

■ 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:

$$F_n = 2^{2^n} + 1 \quad (n = 0, 1, 2, \dots)$$

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

⇒ Euler chỉ ra rằng F_5 là hợp số ☺



Pierre de Fermat

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?

□ $34 = 5 + 29 = 3 + 31$



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:*

$$a \equiv b(\text{mod } m)$$

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:

- | | | |
|--|------------------------|------------------------|
| ☐ $16 \equiv 11 \pmod{5}$ | $16 \equiv 6 \pmod{5}$ | $16 \equiv 1 \pmod{5}$ |
| ☐ $-7 \equiv 2 \pmod{3}$ | $-7 \equiv 5 \pmod{3}$ | $12 \equiv 0 \pmod{2}$ |
| ☐ $12 \equiv 4 \pmod{2}$ | | |

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 $a_i \equiv b_i \pmod{m}$ ($i=1,2,\dots, n$) thì

$$(a_1+a_2+\dots+a_n) \equiv (b_1+b_2+\dots+b_n) \pmod{m}$$

$$(a_1.a_2.\dots.a_n) \equiv (b_1.b_2.\dots.b_n) \pmod{m}$$

2)- $a \equiv b \pmod{m} \Leftrightarrow (a \pm c) \equiv (b \pm c) \pmod{m}$

(c là một số nguyên)

3)- $a \equiv b \pmod{m} \Leftrightarrow a \equiv (b+km) \pmod{m}$

$\Leftrightarrow (a+km) \equiv b \pmod{m}$, (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

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

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

$$a \equiv b \pmod{m} \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{m}$$

Tính chất của quan hệ đồng dư

■ *m là số nguyên dương*

9)- Nếu $a \equiv b \pmod{m_i}$ ($i=1,2,\dots, n$)

và $m = [m_1, m_2, \dots, m_n]$ 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



SHANNON ENTROPY

Shannon entropy

- thông tin được đo lường bằng *bits*
 - cho 1 phân phối xác suất, thông tin cần thiết để dự đoán 1 sự kiện là *entropy* 😊
- công thức tính entropy:

$$\text{entropy}(p_1, p_2, \dots, p_n) = -p_1 \log p_1 - p_2 \log p_2 \dots - p_n \log p_n$$

"Father of information theory"



Claude Shannon

Born: 30 April 1916

Died: 23 February 2001

Shannon entropy

