

TOÁN RỜI RẠC

CHƯƠNG 1: KHÁI NIỆM CƠ BẢN

Lý thuyết số và hệ đếm

NỘI DUNG

1. Các phép toán trên số nguyên.
2. Biểu diễn các số nguyên.
3. Định lý về số dư Trung Quốc và ứng dụng.
4. Các hệ đếm.

1. Các phép toán trên số nguyên (1/5)

1.1. Phép chia nguyên.

- Cho hai số nguyên n và m ta nói n chia hết cho m nếu tồn tại số nguyên k sao cho $n = k.m$ và ký hiệu là $m \mid n$.
- **Định lý 1.** Cho n , m và k là các số nguyên. Khi đó
 - a- Nếu $k \mid n$ và $k \mid m$ thì $k \mid (n + m)$.
 - b- Nếu $k \mid n$ thì $k \mid n.m$ với mọi số nguyên m .
 - c- Nếu $k \mid n$ và $n \mid m$ thì $k \mid m$.

1. Các phép toán trên số nguyên (2/5)

1.1. Phép chia nguyên (tiếp)

- **Định lý 2:** Mọi số nguyên dương đều có thể được viết duy nhất dưới dạng tích của các số nguyên tố.
- **Định lý 3:** Cho a là một số nguyên và d là số nguyên dương. Khi đó tồn tại các số q và r duy nhất, với $0 \leq r < d$, sao cho $a = dq + r$.
- Hai số nguyên n và m gọi là nguyên tố cùng nhau nếu $USCLN(n, m) = 1$.
- Các số nguyên a_1, a_2, \dots, a_n được gọi là đôi một nguyên tố cùng nhau nếu $USCLN(a_i, a_j) = 1$ với mọi $1 \leq i, j \leq n$.

1. Các phép toán trên số nguyên (3/5)

1.1. Phép chia nguyên (tiếp)

- **Định lý 4:** Cho n, m là hai số nguyên dương. Khi đó

$$mn = USCLN(n, m) BSCNN(n, m)$$

- Hai số nguyên n và m gọi là đồng dư theo **modulo k** nếu

$$n \bmod k = m \bmod k, \text{ ta ký hiệu } n \equiv m \pmod{k}.$$

- **Định lý 5:** Nếu $n \equiv m \pmod{k}$ và $p \equiv q \pmod{k}$. Khi đó:

$$a) \quad n + p \equiv m + q \pmod{k}$$

$$b) \quad np \equiv mq \pmod{k}$$

- Phần tử b được gọi là phần tử nghịch đảo của a theo modulo m nếu $ab \equiv 1 \pmod{m}$ và ký hiệu là a^{-1} , khi đó $aa^{-1} \equiv 1 \pmod{m}$.

1. Các phép toán trên số nguyên (4/5)

1.2. Thuật toán Euclid.

- **Bổ đề:** Cho $a = b \times q + r$ trong đó a, b, q, r là các số nguyên dương. Khi đó

$$USCLN(a, b) = USCLN(b, r)$$

- **Chứng minh:** Với mọi ước số chung d của a và b khi đó

$$a - b \times q = r$$

suy ra d cũng là ước số của r , tức là d cũng là ước số chung của b và r vậy $USCLN(a, b) = USCLN(b, r)$.

- **Thuật toán Euclid:**

- Input: a, b ($a \geq b$) đặt $r_0 = a$ và $r_1 = b$.
- Bước 1: $r_0 = r_1 \times q_1 + r_2$ $0 \leq r_2 < r_1$
- Bước 2: Nếu $r_2 \neq 0$ thì $r_0 = r_1$ và $r_1 = r_2$ quay lại bước 1 ngược lại sang bước 3.
- Output: r_1 .

1. Các phép toán trên số nguyên (5/5)

1.2. Thuật toán Euclid (tiếp)

- Thuật toán Euclid được dùng để tìm ước số chung lớn nhất của hai số nguyên.
- Ví dụ tìm $USCLN(91,287)$. Trước hết lấy số lớn hơn 287 chia cho số nhỏ 91 ta được

$$287 = 91 \times 3 + 14$$

bất kỳ ước số chung nào của 287 và 91 cũng là ước số của $287 - 91 \times 3 = 14$. Và cũng như vậy, bất kỳ ước số chung nào của 91 và 14 cũng là ước số của $287 = 91 \times 3 + 14$. Do đó $USCLN$ của 91 và 14 cũng là $USCLN$ của 287 và 91. Từ đó có

$$USCLN(91,287) = USCLN(91,14)$$

Tương tự như vậy, vì $91 = 14 \times 6 + 7$ ta được

$$USCLN(91,14) = USCLN(14,7) = 7$$

2. Biểu diễn các số nguyên (1/2)

- **Định lý 6:** Cho **b** là một số nguyên dương lớn hơn 1. Khi đó nếu **n** là một số nguyên dương thì nó có thể được biểu diễn một cách duy nhất dưới dạng:

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b^1 + a_0$$

Trong đó **k** là số nguyên không âm, **$a_0, a_1, a_2, \dots, a_k$** là các số nguyên không âm nhỏ hơn **b** và **$a_k \neq 0$** .

- Biểu diễn **n** trong định lý trên được gọi là **triển khai cơ số b của n**.

2. Biểu diễn các số nguyên (2/2)

Ví dụ:

- Ví dụ: Cho $n = 165$, $b = 8$ ta được

$$165 = 2 \times 8^2 + 4 \times 8^1 + 5$$

Trong ví dụ này ta có thể biểu diễn như sau $(245)_8$ gọi là cách biểu diễn theo hệ bát phân.

- Ví dụ: Cho $n = 351$, $b = 2$ ta được

$$351 = 1 \times 2^8 + 0 \times 2^7 + 1 \times 2^6 + 0 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$$

ta nhận được dãy $\{a_k\}$ sau $(101011111)_2$ gọi là biểu diễn nhị phân của số 351.

3. Định lý về số dư Trung Quốc và ứng dụng (1/13)

Số dư Trung Quốc:

Định lý về số dư Trung Quốc:

- Giả sử m_1, m_2, \dots, m_n là các số nguyên dương, nguyên tố cùng nhau từng đôi một và a_1, a_2, \dots, a_n là các số nguyên. Khi đó hệ n phương trình đồng dư $x \equiv a_i \pmod{m_i}$ với $1 \leq i \leq n$ sẽ có một nghiệm duy nhất theo modulo $M = m_1 \times m_2 \times \dots \times m_n$ được cho theo công thức sau:

$$x = \sum_{i=1}^n a_i M_i y_i \pmod{M}$$

- Trong đó $M_i = \frac{M}{m_i}$ và $y_i = M_i^{-1} \pmod{m_i}$ với $1 \leq i \leq n$.

3. Định lý về số dư Trung Quốc và ứng dụng (2/13)

Ứng dụng

- Giả sử m_1, m_2, \dots, m_n là các số nguyên tố cùng nhau từng đôi một, hay $USCLN(m_i, m_j) = 1$ với mọi $i \neq j$.
- Giả sử rằng a_1, a_2, \dots, a_n là các số nguyên, xét hệ các phương trình đồng dư sau:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2} \tag{1}$$

...

$$x \equiv a_n \pmod{m_n}$$

- Khi đó định lý về số dư Trung Quốc khẳng định rằng hệ này có nghiệm duy nhất theo modulo $M = m_1 \times m_2 \times \dots \times m_n$.

3. Định lý về số dư Trung Quốc và ứng dụng (3/13)

Chứng minh định lý:

- Ta cần chứng minh, tồn tại nghiệm và duy nhất theo modulo M .
- Ta có: $x = \sum_{i=1}^n a_i M_i y_i \pmod{M}$ và
 $M_i \equiv 0 \pmod{m_k}$ với $i \neq k$
- Mặt khác: $M_i y_i \equiv 1 \pmod{m_i}$ với $i = 1 \div n$
- Vậy: $x \equiv a_i M_i y_i \equiv a_i \pmod{m_i}$ với $i = 1 \div n$
- Do đó, x là nghiệm của hệ đồng dư.

3. Định lý về số dư Trung Quốc và ứng dụng (4/13)

Chứng minh định lý (tiếp):

- Ta chứng minh tính duy nhất.
- Giả sử, tồn tại x và y ($x \neq y$) theo modulo M cùng là nghiệm của hệ đồng dư.
- Do m_i và m_j nguyên tố cùng nhau, nên với p^r là phân tích thừa số nguyên tố m_i hay $p^r | m_i$ thì $p^r \nmid m_j$.
- Mặt khác $x \equiv a_i \pmod{m_i}$ và $y \equiv a_i \pmod{m_i}$. Nên ta có $p^r | x - y$. Vậy $m_1 m_2 \dots m_n | x - y$ hay $M | x - y$.
- Theo giả thiết $x \neq y$, điều này vô lý (theo modulo M).
- Vậy, ta có ĐPCM.

3. Định lý về số dư Trung Quốc và ứng dụng (8/13)

Thuật toán Euclid mở rộng: Giải thuật sau chỉ thực hiện với các số nguyên $m > a > 0$, biểu diễn bằng giả mã:

Procedure Euclid_Extended (a,m)

int $y_0=0$, $y_1:=1$, $y:=1$;

While $a > 0$ **do**

{ $r := m \bmod a$

if $r=0$ then Break

$q := m \div a$

$y := y_0 - y_1 * q$

$m := a$

$a := r$

$y_0 := y_1$

$y_1 := y$ }

If $a > 1$ **Then Return** "A không khả nghịch theo modulo m"

else Return " Nghịch đảo modulo m của a là y"

3. Định lý về số dư Trung Quốc và ứng dụng (9/13)

Ví dụ về tìm nghịch đảo theo Modulo:

- Cho $a=143$, $m=7$, tìm nghịch đảo của a .
- Giải:
 - Vì $143 \bmod 7 = 3$, nên cần tìm nghịch đảo của 3 modulo 7.

Bước	m	a	r	q	y_0	y_1	y
0	7	3	1	2	0	1	-2
1	3	1	0

Kết quả tính toán trong bảng cho ta - 2. Lấy số đối của 2 theo modulo 7 được 5. Vậy: $3^{-1} \bmod 7 = 5$

3. Định lý về số dư Trung Quốc và ứng dụng (10/13)

Ví dụ về tìm nghịch đảo theo Modulo:

- Cho $a=30$, $m=101$, tìm nghịch đảo của a .
- Giải:

Bước	m	a	r	q	y_0	y_1	y
0	101	30	11	3	0	1	-3
1	30	11	8	2	1	-3	7
2	11	8	3	1	-3	7	-10
3	8	3	2	2	7	-10	27
4	3	2	1	1	-10	27	-37
5	2	1	0

Kết quả tính toán trong bảng cho ta - 37. Lấy số đối của 37 theo modulo 101 được 64. Vậy: $30^{-1} \bmod 101 = 64$

3. Định lý về số dư Trung Quốc và ứng dụng (11/13)

Ví dụ về hệ phương trình đồng dư:

- Cho hệ phương trình đồng dư:

$$x \equiv 5 \pmod{7}$$

$$x \equiv 3 \pmod{11}$$

$$x \equiv 10 \pmod{13}$$

3. Định lý về số dư Trung Quốc và ứng dụng (12/13)

Ví dụ về hệ phương trình đồng dư (tiếp):

- Tính:
 - $M = 7 \times 11 \times 13 = 1001,$
 - $M_1 = 11 \times 13 = 143,$
 - $M_2 = 7 \times 13 = 91,$
 - $M_3 = 7 \times 11 = 77,$
 - $y_1 = 143^{-1} \bmod 7 = 5$ theo Euclid mở rộng
 - $y_2 = 91^{-1} \bmod 11 = 4$ theo Euclid mở rộng
 - và $y_3 = 77^{-1} \bmod 13 = 12$ theo Euclid mở rộng

3. Định lý về số dư Trung Quốc và ứng dụng (13/13)

Ví dụ về hệ phương trình đồng dư (tiếp):

- Khi đó với $a_1 = 5$, $a_2 = 3$ và $a_3 = 10$ nghiệm của hệ phương trình là:

$$\begin{aligned} X &= (5 \times 143 \times 5 + 3 \times 91 \times 4 + 10 \times 77 \times 12) \bmod 1001 \\ &= (3\,575 + 1\,092 + 9\,240) \bmod 1001 \\ &= 13\,907 \bmod 1001 \\ &= 894 \bmod 1001 = 894 \end{aligned}$$

4. Các hệ đếm (1/5)

Xem xét một số hệ đếm:

1. Hệ đếm thập phân.
2. Hệ đếm nhị phân.
3. Hệ đếm bát phân (Octal).
4. hệ đếm thập lục phân (Hexa).

4. Các hệ đếm (2/5)

1. Hệ đếm thập phân.

- Biểu diễn số n bất kỳ trong hệ thập phân theo công thức:

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10^1 + a_0 10^0$$

trong đó $0 \leq a_i \leq 9, i = 1, 2, 3, \dots k$

4. Các hệ đếm (3/5)

2. Hệ đếm nhị phân.

- Biểu diễn số n bất kỳ trong hệ nhị phân theo công thức:

$$n = a_k 2^k + a_{k-1} 2^{k-1} + \dots + a_1 2^1 + a_0 2^0$$

trong đó $0 \leq a_i \leq 1, i = 1, 2, 3, \dots k$

4. Các hệ đếm (4/5)

3. Hệ đếm bát phân (Octal).

- Số n bất kỳ được biểu diễn trong hệ bát phân theo công thức:

$$n = a_k 8^k + a_{k-1} 8^{k-1} + \dots + a_1 8^1 + a_0 8^0$$

trong đó $0 \leq a_i \leq 7, i = 1, 2, 3, \dots k$

4. Các hệ đếm (5/5)

4. Hệ đếm thập lục phân (Octal).

- Số n bất kỳ được biểu diễn trong thập lục phân theo công thức:

$$n = a_k 16^k + a_{k-1} 16^{k-1} + \dots + a_1 16^1 + a_0 16^0$$

trong đó $0 \leq a_i \leq 15, i = 1, 2, 3, \dots, k$

tức là $a_i \in \{0, 1, 2, \dots, A, B, \dots, F\}$