Bài 3.
Trường hữu hạn
&
Số học modulo

Thời lượng 8 tiết
Lương Thái Lê

Tình huống dẫn nhập

- Cần xây dựng một "tập hữu hạn các số" và các phép toán trên tập đó sao cho đảm bảo tính đóng
- Khi đó có thể kiểm soát được các kết quả do chúng không trở nên quá lớn và có định dạng có thể khai báo trước được

=> Ứng dụng cấu trúc toán học đó trên máy tính và đem lại hiệu quả lớn

Field

Ring

Group

(A1) If a and b belong to S, then $a + b$ is also in S

(A2) $a + (b + c) = (a + b) + c$ for all a, b, c in S

(A3) There is an element 0 in R such that
$a + 0 = 0 + a = a$ for all a in S

(A4) For each a in S there is an element $-a$ in S
such that $a + (-a) = (-a) + a = 0$

(A5) $a + b = b + a$ for all a, b in S

(M1) If a and b belong to S, then ab is also in S

(M2) $a(bc) = (ab)c$ for all a, b, c in S

(M3) $a(b + c) = ab + ac$ for all a, b, c in S
$(a + b)c = ac + bc$ for all a, b, c in S

(M4) $ab = ba$ for all a, b in S

(M5) There is an element 1 in S such that
$a1 = 1a = a$ for all a in S

(M6) If a, b in S and $ab = 0$, then either
$a = 0$ or $b = 0$

(M7) If a belongs to S and a 0, there is an
element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Nội dung

1. Quan hệ đồng dư
2. Số học Modulo
3. Phép toán nghịch đảo và Trường hữu hạn
4. Hàm Euler
5. Một số định lý số học cơ bản
6. Thuật toán bình phương, nhân liên tiếp và phép toán lũy thừa

1.1 Phép toán modulo

- Giả sử n là số nguyên dương, a là số nguyên, nếu:

$$a = q.n + r$$

trong đó r là phần dư dương $0 \le r < n$ và q là thương nguyên lớn nhất nhỏ hơn hoặc bằng a/n

- Khi đó ký hiệu phần dư dương r = a mod n và $q = \lfloor a/n \rfloor$, vậy

$$a = \lfloor a/n \rfloor .n + a \bmod n \qquad (*)$$

Ví dụ: 11 mod 7 = 4, vì 11 = 1.7 + 4

(-11) mod 7 = 3, vì -11= -2.7+ 3

100 mod 13 = 9, vì 100 = 7.13 + 9

(-100) mod 13 = 4, vì -100 = -8.13+ 4

Câu hỏi: Biểu diễn (*) có duy nhất không?

Trả lời: Duy nhất, do số hạng thứ 2 qui ước là số nguyên dương giữa 0 và n-1

1.2. Quan hệ đồng dư

- Nếu: a mod n = b mod n, thì ta viết $a \equiv b \bmod n$
  gọi là a và b có quan hệ đồng dư theo n
  ví dụ: $100 \equiv 34 \bmod 11$ vì 100 mod 11 = 1 = 34 mod 11
  $22 \equiv (-8) \bmod 10$ vì 22 mod 10 = 2 = -8 mod 10
- **<u>Định nghĩa</u>: Số b được gọi là đại diện của a theo mod n, nếu $a \equiv b \bmod n$ và $0 <= b <= n - 1$.**
  (Hay nếu b = a mod n, thì b là đại diện của a theo mod n)
  ví dụ:
  10 là đại diện của 100 theo mod 15, vì 100 mod 15 = 10
  5 là đại diện của -10 theo mod 15, vì (-10) mod 15 = 5

1.3. Quan hệ đồng dư theo 7 (Module 7)

- Các phần tử cùng cột có quan hệ đồng dư với nhau
  -12 mod 7 ≡ -5 mod 7 ≡ 2 mod 7 ≡ 9 mod 7
- Tập các đại diện theo modulo 7 là **0, 1, 2, 3, 4, 5, 6**
  Ký hiệu [2]= { …, –12, -5, 2, 9, …}
  vì -12 mod 7 = -5 mod 7 = 2 mod 7 = 9 mod 7 = 2

…

-21	-20	-19	-18	-17	-16	-15
-14	-13	-12	-11	-10	-9	-8
-7	-6	-5	-4	-3	-2	-1
0	**1**	**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

- Tập các đại diện của các số nguyên theo modulo n gồm n phần tử ký hiệu như sau

$$Z_n = \{ \mathbf{0, 1, 2, 3, \ldots, n\text{-}1} \}$$

Nội dung

1. Quan hệ đồng dư
2. Số học Modulo
3. Phép toán nghịch đảo và Trường hữu hạn
4. Hàm Euler
5. Một số định lý số học cơ bản
6. Thuật toán bình phương, nhân liên tiếp và phép toán lũy thừa

2.1. Các phép toán số học trên modulo

- Cho trước một số nguyên dương n
- Thực hiện phép toán số học trên modulo:
  - Cách 1: Thực hiện các phép toán trên các số nguyên như các phép cộng, nhân các số nguyên thông thường sau đó rút gọn lại bằng phép lấy modulo
  - Cách 2: Vừa tính toán vừa kết hợp với rút gọn theo modulo tại bất cứ thời điểm nào

$$(a \pm b) \bmod n = [a \bmod n \pm b \bmod n] \bmod n \quad (*)$$

$$(a.b) \bmod n = [a \bmod n \,.\, b \bmod n] \bmod n \quad (**)$$

- <u>Định lý</u>: Cho m, n là hai số nguyên dương, khi đó

$$(-m) \bmod n = n - m \bmod n$$

Ví dụ: $-153 \bmod 15 = 15 - 153 \bmod 15 = 15 - 3 = 12$

Câu hỏi: Bạn áp dụng công thức trên như thế nào?
Trả lời: thay các số bằng các đại diện của chúng hoặc các số đồng dư của chúng

2.2. Số học đồng dư

=>Có thể thực hiện các phép toán chỉ trên các đại diện theo modulo n:

$$Z_n = \{ 0, 1, 2, 3, ..., n -1 \}$$

- Ví dụ 1:
  - (144 + 215) mod 7 = (144 mod 7 + 215 mod 7) mod 7 = (4 + 5) mod 7 = 2
- Ví dụ 2:

(144 * 315) mod 150 =

(144 mod 150 * 315 mod 150) mod 150 =

((-6) mod 150 * 15 mod 150) mod 150 =

(-90) mod 150 = 60 mod 150 = 60

2.3. modulo 8 với phép cộng

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

2.4. modulo 8 với phép nhân

X	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

2.5. Ví dụ các phép toán trên modulo

Áp dụng các tính chất của modulo:

$(11.19 + 10^{17}) \bmod 7 =$

$((11.19) \bmod 7 + 10^{17} \bmod 7) \bmod 7 =$

$((11 \bmod 7.19 \bmod 7) \bmod 7$

$+ (10 \bmod 7)^{17} \bmod 7) \bmod 7 =$

$((4.(-2)) \bmod 7+(((3^2)^2)^2)^2 . 3 \bmod 7) \bmod 7=$

$((-1) \bmod 7 + ((2^2)^2)^2 . 3 \bmod 7) \bmod 7 =$

$(-1 + 5) \bmod 7 = 4$

Câu hỏi: Tại sao có thể thay $((3^2)^2)^2)^2$ mod 7 bằng $((2^2)^2)^2$ mod 7

Trả lời: Vì 3^2 mod 7 = 2

Nội dung

1. Quan hệ đồng dư
2. Số học Modulo
3. Phép toán nghịch đảo và Trường hữu hạn GF(p)
4. Hàm Euler
5. Một số định lý số học cơ bản
6. Thuật toán bình phương, nhân liên tiếp và phép toán lũy thừa

3.1. Ước số của số tự nhiên

- Số b không âm được gọi là ước số của a, nếu có số m sao cho

  a = m.b   với a, b, m đều nguyên.

- Tức là a chia hết cho b, ký hiệu

  b|a   hay   a⋮b

- Ước số chung lớn nhất (great common divisor) của a và b
- GCD(a,b) là ước số chung dương lớn nhất của a và b.
  - Ví dụ: GCD(60,24) = 12
- Nếu hai số a, b nguyên tố cùng nhau thì GCD(a, b) = 1,
  - Ví dụ GCD(8,15) = 1,

3.2. Thuật toán Euclid tìm ước chung lớn nhất

- Tính chất GCD(a,b) = GCD(b, a mod b)

  với a, b là hai số tự nhiên và b ≤ a
- Thuật toán Euclid tìm GCD(a, b):

```
EUCLID(a,b)
1. A = a; B = b
2. if B = 0 return  A = gcd(a, b)
3. R = A mod B
4. A = B
5. B = R
6. goto 2
```

3.3. Ví dụ: GCD(1970,1066) = GCD(2, 0) = 2

1970 = 1 x 1066 + 904	gcd(1066, 904)
1066 = 1 x 904 + 162	gcd(904, 162)
904 = 5 x 162 + 94	gcd(162, 94)
162 = 1 x 94 + 68	gcd(94, 68)
94 = 1 x 68 + 26	gcd(68, 26)
68 = 2 x 26 + 16	gcd(26, 16)
26 = 1 x 16 + 10	gcd(16, 10)
16 = 1 x 10 + 6	gcd(10, 6)
10 = 1 x 6 + 4	gcd(6, 4)
6 = 1 x 4 + 2	gcd(4, 2)
4 = 2 x 2 + 0	gcd(2, 0)

3.4. Thuật toán Euclide mở rộng và phép toán nghịch đảo

- Số a được gọi là nghịch đảo của b theo mod m, ký hiệu $a = b^{-1} \bmod m$, nếu

$$(a.b) \bmod m = 1$$

Ví dụ: $7 = 8^{-1} \bmod 11$, vì $(7.8) \bmod 11 = 1$

- **Xét tập $Z_p = \{0,1, \dots , p-1\}$, với p là số nguyên tố**
  - **Với các phép toán cộng và nhân module**
  - **Trên Z_p mọi phần tử a khác 0 đều có phần tử nghịch đảo a^{-1}: $a \cdot a^{-1} = 1$**
- Như vậy trên Z_p ta có thể thực hiện các phép toán cộng, trừ, nhân, chia (chia cho phần tử khác 0).
- Ví dụ phép chia:

$2/8 (\bmod 11) = 2 * 8^{-1} (\bmod 11) = 2*7 (\bmod 11) = 3$

3.5. Ví dụ phép nhân theo modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tìm các cặp số là nghịch đảo của nhau theo modulo 7?
(1,1), (2,4), (4,2), (3,5), (5,3),(6,6)

3.6 Trường hữu hạn GF(p)

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x + w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

Nếu n là số nguyên tố thì:

$$\forall \mathrm{w} \in Z_n, \mathrm{w} \neq 0 => \exists \mathrm{w}^{-1} \in Z_n : \mathrm{w} \times \mathrm{w}^{-1} \equiv 1 \bmod n$$

$\Rightarrow$ Vậy Z_n là một trường hữu hạn nếu n là số nguyên tố
$\Rightarrow$ **Ký hiệu GF(p) là trường hữu hạn theo modulo p**

3.7. Thuật toán Euclid mở rộng tìm số nghịch đảo

. Tìm số nghịch đảo của b theo modul m

```
EXTENDED EUCLID(m, b)
   1. (A1, A2, A3)=(1, 0, m);
      (B1, B2, B3)=(0, 1, b)
   2. if B3 = 0
      return A3 = gcd(m, b); no inverse
   3. if B3 = 1
      return B3 = gcd(m, b); B2 = b^-1 mod m
   4. Q = A3 div B3
   5. (T1, T2, T3)=(A1 - Q B1, A2 - Q B2, A3 - Q B3)
   6. (A1, A2, A3)=(B1, B2, B3)
   7. (B1, B2, B3)=(T1, T2, T3)
   8. goto 2
```

3.8. Giải thích thuật toán

- Các quan hệ sau là bất biến:

  $mT_1 + bT_2 = T_3$; $mA_1 + bA_2 = A_3$; $mB_1+bB_2=B_3$

- Vì ban đầu: m.1 + b.0 = m; m.0 +b.1 = b và

  (T1,T2,T3)=(A1−Q.B1, A2−Q.B2,A3 − Q.B3)

  Do đó:

$$mT_1 + bT_2 = m(A1 - Q.B1) + b\,(A2 - Q.B2)$$

$$= (mA1 + bA2) - Q(mB1 + bB2)$$

$$= A3 - Q.B3 = T3$$

- Khi $B_3 = 1$:

  $mB_1+bB_2=1$ suy ra $bB_2 = 1- mB_1$ hay

  $bB_2 = 1 \bmod m$,   Do đó: $B_2 = b^{-1} \bmod m$

3.9. Ví dụ: Tìm nghịch đảo của 550 theo modulo 1759.
Thuật toán dừng khi B_3=1 và
$550^{-1} \bmod 1759 = 355$

Q	A1	A2	A3	B1	B2	B3
—	1	0	1759	0	1	550
3	0	1	550	1	–3	109
5	1	–3	109	–5	16	5
21	–5	16	5	106	–339	4
1	106	–339	4	–111	355	1

Nội dung

1. Quan hệ đồng dư
2. Số học Modulo
3. Phép toán nghịch đảo và Trường hữu hạn GF(p)
4. Hàm Euler
5. Một số định lý số học cơ bản
6. Thuật toán bình phương, nhân liên tiếp và phép toán lũy thừa

4.1. Các số nguyên tố

- **Là các số nguyên dương chỉ có ước số là 1 và chính nó.**
- Chúng không thể được viết dưới dạng tích của các số khác
- 1 là số nguyên tố, nhưng không quan tâm đến nó
- Danh sách các số nguyên tố nhỏ hơn 200

  2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

4.2. Các số nguyên tố cùng nhau

- **Hai số a và b không có ước chung nào ngoài 1, được gọi là nguyên tố cùng nhau**
  - Ví dụ: 8 và 15 là nguyên tố cùng nhau, vì ước của 8 là 1, 2, 4, 8, còn ước của 15 là 1, 3, 5, 15. Chỉ có 1 là ước chung
- Ngược lại có thể xác định ước chung lớn nhất bằng cách trong các phân tích ra thừa số của chúng, tìm các thừa số nguyên tố chung và lấy bậc lũy thừa nhỏ nhất.
  - Mọi số tự nhiên bất kỳ đều có phân tích duy nhất ra lũy thừa các thừa số nguyên tố:

    Ví dụ $91=7\text{x}13$; $3600=2^4\text{x}3^2\text{x}5^2$
  - Vì $300=2^2\text{x}3^1\text{x}5^2$ $18=2^1\text{x}3^2$ nên $GCD(18,300)=2^1\text{x}3^1\text{x}5^0=6$

4.3. Hàm Euler ø(n)

- Khi thực hiện phép tính đồng dư n =>Tập đầy đủ các phần dư: 0, 1, 2, …, n-1
- Xét tập rút gọn của tập phần dư trên bao gồm các số nguyên tố cùng nhau với n
- Ví dụ với n = 10
  - Tập đầy đủ các phần dư là Z_{10} = {0,1,2,3,4,5,6,7,8,9}
  - Tập rút gọn các phần dư nguyên tố với 10 là {1,3,7,9}: có 4 phần tử
- **<u>Định nghĩa</u>: Số các phần tử của tập rút gọn gồm các số nguyên tố cùng nhau với n trên tập Z_n là giá trị của hàm Euler ø(n)**

=> ø(10) = 4

Câu hỏi: ø(20) = ?

Trả lời: ø(20) = 8: **t**ập các số nguyên tố cùng nhau với 20: {1, 3, 7, 9, 11, 13, 17, 19}

4.4. Tính giá trị hàm Euler $\varnothing(n)$

- Muốn tính **ø(n)** việc đếm số các số nguyên tố cùng nhau với n và nhỏ hơn n được loại bỏ vì đây là bài toán tốn nhiều công sức
- **Nói chung cần phân tích *n* thành tích các thừa số nguyên tố**
  - **Nếu p là số nguyên tố ø(p) = p-1**
  - **Nếu p và q là hai số nguyên tố khác nhau**

    ø(p.q) = (p-1)(q-1)
- Ví dụ

ø(37) = 36

ø(21) = ø(3.7) = (3–1)×(7–1) = 2×6 = 12

ø(143) = ø(11.13) = (11–1)×(13–1) = 10×12 = 120

Câu hỏi: ø(43) = ?; ø(55) =?

Trả lời: ø(43) = 42 ; ø(55) = 40

4.5. Tính giá trị hàm Euler ø(n) (tiếp)

n	$\phi(n) =$	Conditions
p	$p-1$	p prime
p^n	$p^n - p^{n-1}$	p prime
$s \cdot t$	$\phi(s) \cdot \phi(t)$	$\gcd(s,t) = 1$
$p \cdot q$	$(p-1) \cdot (q-1)$	p, q prime

ø(72) = ø(8.9) = ø(8). ø(9) = ø(2^3).ø(3^2) =

= (2^3-2^2)(3^2-3^1) = 4.6 = 24

ø(300) = ø(2^2.3^1.5^2) = ø(2^2). ø(3). ø(5^2) =

= (2^2-2).2.(5^2-5^1) = 2.2.20 = 80

Câu hỏi: ø(108) = ?

Trả lời: *ø(108) = ø(4.27) = ø(2^2.3^3) =*

(2^2-2)(3^3-3^2) = 2.18=36

Nội dung

1. Quan hệ đồng dư
2. Số học Modulo
3. Phép toán nghịch đảo và Trường hữu hạn GF(p)
4. Hàm Euler
5. Một số định lý số học cơ bản
6. Thuật toán bình phương, nhân liên tiếp và phép toán lũy thừa

5.1. Định lý Ferma nhỏ

- ***Cho p là số nguyên tố và a là số nguyên dương không là bội của p, tức là GCD(a, p) = 1. Khi đó***

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

Hay $$a^{p} \pmod{p} = a \pmod{p}$$

- Được dùng trong khoá công khai và kiểm tra tính nguyên tố của một số
- Ví dụ:

2^{7-1} mod 7 = 1 (2^{6} mod 7 = 64 mod 7 = 1)

3^{5-1} mod 5 = 1 (3^{4} mod 5 = 81 mod 5 = 1)

2^{11-1} mod 11 = 1 (2^{10} mod 11 = 1024 mod 11 = 1)

Câu hỏi: 4^{13} mod 13 = ?

*Trả lời: 4^{13} mod 13 = 4 mod 13 = 1*4 = 4*

5.2. Định lý Euler

- Tổng quát hoá của Định lý Ferma

Cho a,n là hai số tự nhiên nguyên tố cùng nhau, tức là gcd(a,n)=1. Khi đó

$$a^{\varnothing(n)} \pmod{n} = 1$$

- Ví dụ:

  $a=3; n=10;\ \varnothing(10)= \varnothing(2).\ \varnothing(5)=4;$

  Do đó $3^4 \bmod 10 = 81 \bmod 10 = 1$

  $a=2; n=11;\ \varnothing(11)=10;$

  Do đó $2^{10} \bmod 11 = 1$

  $a=4; n=15;\ \varnothing(15)=8;$

  Do đó $4^8 \bmod 15 = (4^2)^4 \bmod 15 = 1$

  Câu hỏi: $9^8 \bmod 20 = ?$; $3^9 \bmod 20 = ?$; $12^{402} \bmod 25=?$

  trả lời: $9^8 \bmod 20 = 1$; $3^9 \bmod 20 = 3$, vì $\varnothing(20)=8$

Định lý phần dư Trung Hoa

- Sử dụng để tăng tốc độ tính toán modulo
- Tính toán trên modulo của M với $M= m_1m_2...m_k$ (các cặp m_i nguyên tố cùng nhau từng đôi một)
- Định lý phần dư Trung Hoa cho phép làm việc trên từng modulo m_i riêng biệt. Sau đó sẽ kết hợp lại để tính theo mod M

=> Đưa việc tính toán theo modul số lớn về tính toán theo modul số nhỏ

- Vì thời gian tính toán tỷ lệ với kích thước nên điều đó sẽ nhanh hơn tính toán trên toàn bộ M

Định lý phần dư Trung Hoa - tiếp

- Cho $M = m_1 m_2 \ldots m_k$, trong đó các cặp m_i nguyên tố với nhau từng đôi một.
- Để tính A mod M
  - Trước hết ta cần tính tất cả $a_i = A \bmod m_i$
  - Tính c_i theo công thức sau, với $M_i = M/m_i$
  - Cuối cùng sử dụng công thức

$$A \equiv \left(\sum_{i=1}^{k} a_i c_i \right) (\mathrm{mod}\ M)$$

$$c_i = M_i \times (M_i^{-1} \bmod m_i) \quad \text{for } 1 \le i \le k$$

Ứng dụng của định lý phần dư trung hoa – Tính toán trên Modulo lớn

- **Ví dụ.** Tính 17^8 mod 77. Áp dụng định lý phần dư Trung hoa, ta coi A = 17^8, m1 = 7, m2 = 11.

  Khi đó, M1 = 11, M2 = 7 và

  11^{-1} mod 7 = 4^{-1} mod 7 = 2, suy ra c_1 = 11*2 = 22

  7^{-1} mod 11 = 8, suy ra c_2 = 7*8 = 56

  a_1 = 17^8 mod 7 = (17 mod 7)^8 mod 7 = 3^8 mod 7

  = $(3^2)^4$ mod 7 = 2

  a_2 = 17^8 mod 11 = (17 mod 11)^8 mod 11 = 6^8 mod 11 =

  = $(6^2)^4$ mod 11 = 3^4 mod 11 = 4

- Vậy A mod 77 = 17^8 mod 77 = (2*22 + 4*56) mod 77 = 268 mod 77 = 37

Ví dụ tiếp về tính toán trên Modulo lớn

- Giả sử ta phải tính: $A = 17^{130} \bmod 35$

  Ta thấy $35 = 5.7$

- Ta tính $17^{130} \bmod 5$ và $17^{130} \bmod 7$

  $17^{130} \bmod 5 = 2^{130} \bmod 5 = 2^{128}\ 2^2 \bmod 5 = (2^4)^{.32}\ 2^2 \bmod 5 = 2^2 \bmod 5 = 4$ (Ferma: $2^4 \bmod 5 = 1$)

  $17^{130} \bmod 7 = 3^{130} \bmod 7 = (3^6)^{21}.3^4 \bmod 7 =$ (Ferma)

  $1.\ 3^4 \bmod 7 = 81 \bmod 7 = 4$

- $7^{-1} \bmod 5 = 3$; $5^{-1} \bmod 7 = 3$

- $A = (4.7.3 + 4.5.3) \bmod 35 = (84 + 60) \bmod 35 = (14 + 25) \bmod 35 = 4$

Ứng dụng định lý phần dư trung hoa - Giải hệ phương trình modulo

- **Ví dụ.** Cho $x \equiv 5 \bmod 7$ và $x \equiv 6 \bmod 11$. Tìm x.
- Ta có x mod 7 = 5 và x mod 11 = 6
- Áp dụng định lý phần dư Trung hoa với

$m_1=7$, $m_2=11$, $a_1 = 5$, $a_2 =6$ ta tính:

$7^{-1} \bmod 11 = 8$ và $11^{-1} \bmod 7 = 2$.

Như vậy

$x = A = (a_1*c_1 + a_2*c_2) \bmod (7*11) = (5*2*11 + 6*8*7) \bmod (77) = 446 \bmod 77 = 61$

Nội dung

1. Quan hệ đồng dư
2. Số học Modulo
3. Phép toán nghịch đảo và Trường hữu hạn GF(p)
4. Hàm Euler
5. Một số định lý số học cơ bản
6. Thuật toán bình phương, nhân liên tiếp và phép toán lũy thừa

Thuật toán bình phương và nhân liên tiếp - Tính lũy thừa

- Thuật toán nhanh, hiệu quả cho phép tính lũy thừa nói chung và theo modulo nói riêng.
- Tính toán được dựa trên phép lặp trên cơ sở bình phương và nhân để nhận được kết quả
- **Ví dụ 1:**

  $$7^5 \bmod 11 = 7^4 \bmod 11 . 7^1 \bmod 11 = 3.7 \bmod 11 = 10 \bmod 11$$

  vì $7^2 \bmod 11 = 49 \bmod 11 = 5 \bmod 11$

  $7^4 \bmod 11 = 7^2.7^2 \bmod 11 = 5.5 \bmod 11 = 3 \bmod 11$

- **Ví dụ 2:**

  $$3^{129} \bmod 11 = 3^{128}.3 \bmod 11 = 5.3 \bmod 11 = 4,$$

  Vì $3^2 \bmod 11 = (-2) \bmod 11$, $3^4 \bmod 11 = (-2)^2 \bmod 11=4$

  $3^8 \bmod 11 = 4^2 \bmod 11 =5$, $3^{16} \bmod 11 = 5^2 \bmod 11=3$

  $3^{32} \bmod 11 = 3^2 \bmod 11=-2$, $3^{64} \bmod 11 = (-2)^2 \bmod 11=4$

  $3^{128} \bmod 11 = 4^2 \bmod 11=5$

Ví dụ về phân tích lũy thừa theo cơ số 2

First write $(11)_{10} = (1011)_2$. Then calculate

$$
\begin{aligned}
M^{11} &= M^{1\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0} \\
&= (M^{1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0})^2 M \\
&= ((M^{1\cdot 2^1 + 0\cdot 2^0})^2 M)^2 M \\
&= ((M^2)^2 M)^2 M
\end{aligned}
$$

Căn nguyên thủy (căn nguyên tố)

- ***Xét m để a^m mod n = 1. Nếu giá trị m = $\Phi(n)$ là số dương nhỏ nhất thoả mãn công thức trên thì a được gọi là căn nguyên thủy của n.***

- Từ Định lý Euler: $a^{\phi(n)}$ mod n=1, với GCD(a,n)=1
- ***Tức là a là căn nguyên thủy của n, nếu a nguyên tố cùng nhau với n và a^m mod n $\neq$ 1, nếu 0<m < $\phi(n)$***

- Ví dụ một số cặp (n,a)

(3, 2); (5, 2); (7, 3), (11, 2); (13,2);(13, 6); (17, 10)

Ví dụ căn nguyên thủy

- Xét số n = 5 và xét xem a = 2 có phải là căn nguyên thủy của 5 không?

  $2 \bmod 5 = 2$; $2^2 \bmod 5 = 4$; $2^3 \bmod 5 = 3$; $2^4 \bmod 5 = 1$

  Rõ ràng m= 4= ø(5) là số mũ nhỏ nhất có tính chất $2^m \bmod 5 = 1$, nên **2 là căn nguyên thủy của 5.**

- Xét số n = 8 và xét xem a = 3 có phải là căn nguyên thủy của 8 không?

  $3 \bmod 8 = 3$; $3^2 \bmod 8 = 1$; $3^3 \bmod 8 = 3$; $3^4 \bmod 8 = 1$

  Rõ ràng m= 2 < 4 = ø(8) là số mũ nhỏ nhất có tính chất $3^m \bmod 8 = 1$, nên 3 không là căn nguyên thủy của 8.

Các căn nguyên thủy của 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1

Căn nguyên thủy của 19 là :2,3,10,13,14…

Các số nguyên có căn nguyên thủy có dạng: 2, 4, p^k, và $2p^k$, với p là số nguyên tố lẻ và k là số nguyên dương.

Ví dụ căn nguyên thủy của 3^2

Here is an example using a nonprime modulus, $n = 9$. Here $\phi(n) = 6$ and $a = 2$ is a primitive root. We compute the various powers of a and find

$$
\begin{array}{ll}
2^0 = 1 & 2^4 \equiv 7 \pmod 9 \\
2^1 = 2 & 2^5 \equiv 5 \pmod 9 \\
2^2 = 4 & 2^6 \equiv 1 \pmod 9 \\
2^3 = 8 &
\end{array}
$$

This gives us the following table of the numbers with given discrete logarithms (mod 9) for the root $a = 2$:

Logarithm	0	1	2	3	4	5
Number	1	2	4	8	7	5

Logarit rời rạc

- *Dễ thấy, với số nguyên b bất kỳ, nếu a là căn nguyên thủy của số nguyên tố n, thì luôn tồn tại duy nhất 1 số m ($0 \leq$ m $\leq$n-1) sao cho b$\equiv$a^m (mod n)*
- ***ĐN: Với số nguyên b bất kỳ, Số m thỏa mãn*** $\boldsymbol{b \equiv a^m (mod\, n)}$ ***với*** $\boldsymbol{0 \leq m \leq (n-1)}$ ***được gọi là logarit rời rạc của b với cơ số a theo modulo n***
- Kí hiệu $\mathbf{m} = \boldsymbol{dlog_{a,n}(b)} = \boldsymbol{dlog_a}$ ***b(mod n)***

Ví dụ về Logarit rời rạc

- **Khi a là căn nguyên thủy của số nguyên tố n**

=> luôn tồn tại $dlog_a$ b (mod n), với b là số nguyên bất kỳ

- x = $dlog_2$ 8 (mod 19) = 3 bằng cách thử lần lượt (hoặc tra bảng)
- x = $dlog_3$ 6 (mod 19) = 8
- Khi a là căn nguyên thủy của n bất kỳ:
- Tìm x= $dlog_2$ 7 (mod 9) ; Tìm x= $dlog_2$ 6 (mod 9)
- Khi a không là căn nguyên thủy của n:
- x = $dlog_3$ 4 (mod 13) (tìm x: $3^x = 4 \bmod 13$) không có lời giải, vì

  $3^0 \bmod 13 = 1$; $3^1 \bmod 13 = 3$; $3^2 \bmod 13 = 9$;

  $3^3 \bmod 13 = 1 = 3^0 \bmod 13$
- Tìm x = $dlog_7$ 12 (mod 19) = ?
- Tìm x= $dlog_7$ 11 (mod 19) = ?

Tóm tắt

- Chúng ta đã xét đến:
  - Các phép toán modulo với các số nguyên
  - Các số nguyên tố
  - Thuật toán Euclid và Euclid mở rộng
  - Trường hữu hạn chuẩn GF(p)
  - Hàm Euler
  - Định lý Ferma nhỏ và Euler
  - Thuật toán bình phương và nhân liên tiếp
  - Căn nguyên tố và logarit rời rạc

Câu hỏi trắc nghiệm 1

- Câu 1: Tập các số nguyên không đóng với phép toán nào (một tập X được gọi là đóng đối với một phép toán, nếu việc thực hiện phép toán trên X cũng cho kết quả là phần tử thuộc X)

A. phép cộng

B. phép trừ

C. phép nhân

D. phép chia

- Câu 2: Tập các số hữu tỷ không đóng với phép toán nào

A. phép cộng, trừ

B. phép nhân

C. phép chia

D. phép khi căn bậc hai

Câu hỏi trắc nghiệm 2

- Câu 3: Hỏi có bao nhiêu phần dư dương khác nhau khi chia các số nguyên cho một số 11?

A. 12 và đó là tập {0, 1, 2, ..., 10, 11}

B. 10 và đó là tập {0, 1, 2, ..., 9}

C. 11 và đó là tập {1, 2, ..., 10, 11}

D. 11 và đó là tập {0, 1, 2, ..., 9, 10}

- Câu 4: Khẳng định nào sau đây không đúng:

A. 38 mod 17 = 4

B. -7 mod 25 = 18 (= 25 – 7 mod 25)

C. -37 mod 25 = 25 – 37 mod 25 = 25 – 12 = 13

D. -57 mod 25 = -7

Câu hỏi trắc nghiệm 3

- Câu 5: Khẳng định nào sau đây không đúng:
  A. $21 \equiv 36 \bmod 15$
  B. $12 \equiv -3 \bmod 15$
  C. $-7 \equiv 23 \bmod 15$
  D. $39 \equiv 25 \bmod 15$
- Câu 6: Khẳng định nào sau đây không đúng:
  A. (411.800) mod39 = (411 mod39 . 800 mod39)mod39 = (21 . 20) mod 39 = 420 mod39 = 30
  B. $49^{-1} \bmod 39 = 10^{-1} \bmod 39 = 4$
  C. $13^{33} \bmod 8 = (13 \bmod 8)^{33} \bmod 8 = 5^{33} \bmod 8 = (5^2 \bmod 8)^{16} . 5 \bmod 8 = 5 \bmod 8 = 5$
  D. $(3/7) \bmod 17 = 3.7^{-1} \bmod 17 = (3.(7^{-1} \bmod 17)) \bmod 17 = 3.\mathbf{4} \bmod 17 = 12$

Câu hỏi trắc nghiệm 4

- Câu 7: Trong quá trình tính toán theo modulo ta không thể sử dụng tính chất nào?

A. Thay các số bằng các đại diện của nó
B. Thay các số bằng các số tương đương đồng dư với nó
C. Có thể lấy modulo bất cứ lúc nào khi cộng và nhân
D. Có thể lấy modulo số mũ khi lũy thừa

- Câu 8: Nếu p là số nguyên tố, thì khẳng định nào sau đây không đúng: số a bất kỳ trong {1, 2, ..., p-1}

A. nguyên tố cùng nhau với p
B. có số nghịch đảo
C. có thể không có số nghịch đảo
D. Có số nghịch đảo là a^{p-2} mod p

Câu hỏi trắc nghiệm 5

- Câu 9: Khi tìm nghịch đảo của một số theo modulo, ta sử dụng

A. Thuật toán Euclid

B. Thuật toán Euclid mở rộng

C. Thuật toán bình phương và nhân liên tiếp

D. Thuật toán kiểm tra số nguyên tố

- Câu 10: Số b nào có nghịch đảo theo modulo m:

A. m là số nguyên tố

B. b và m là hai số nguyên tố khác nhau

C. b và m nguyên tố cùng nhau

D. B không phải là ước số của m

Câu hỏi trắc nghiệm 6

- Câu 11: Giá trị hàm Euler của một số tự nhiên n là
  A. Số các số nguyên tố nhỏ hơn n
  B. Số các ước số của n
  C. Số các số nguyên tố cùng nhau với n
  D. Tập các số nguyên tố cùng nhau với n
- Câu 12: Cặp nào không phải 2 bài toán ngược nhau, bài toán xuôi dễ - bài toán ngược khó
  A. Nhân 2 số và phân tích 1 số ra tích lũy thừa các thừa số nguyên tố
  B. Tính giá trị hàm Euler của 1 số khi biết và khi không biết phân tích của nó ra lũy thừa thừa số nguyên tố
  C. Lũy thừa và logarit rời rạc
  D. Cộng 2 số và trừ 2 số

Câu hỏi trắc nghiệm 7

- Câu 13: a là căn nguyên tố của một số n, điều khẳng định gì sau đây là không đúng
  - A. Có ø(n)-1 giá trị khác nhau của lũy thừa của a theo mod n
  - B. ø(n) là số mũ dương nhỏ nhất để a mũ đó lên bằng 1
  - C. $\{a^0$ mod n, a^1 mod n, …, $a^{ø(n)-1}$mod n$\}$ là tập các số nguyên tố cùng nhau với n.
  - D. ø(n) là số mũ dương lớn nhất để a mũ đó lên bằng 1
- Câu 14: Một số b có logarit cơ số a theo mod n (a, b nguyên dương nhỏ hơn n), nếu
  - A. a là căn nguyên tố của n
  - B. b nguyên tố cùng nhau với n
  - C. a là căn nguyên tố của n và b nguyên tố cùng nhau với n
  - D. a, b, n nguyên tố cùng nhau từng đôi một

Đáp án câu hỏi trắc nghiệm

- Câu 1
  - D, thương của hai số nguyên 3, 5 không là số nguyên
- Câu 2
  - D, căn bậc 2 của 2 không là số số hữu tỉ
- Câu 3
  - D, chỉ có 11 số dư và nhỏ hơn 12
- Câu 4
  - D, -57 mod 25 = 25 – 57 mod 25 = 18
- Câu 5
  - D, $39 \equiv 9 \bmod 15$, $25 \equiv 10 \bmod 15$
- Câu 6
  - D, 7^{-1}mod 17 = 5 chứ không phải 4
- Câu 7
  - D, không thể lấy modulo cho số mũ

Đáp án câu hỏi trắc nghiệm 2

- Câu 8
  - C, mọi số đều có nghịch đảo
- Câu 9
  - B, thuật toán Euclid mở rộng để tìm nghịch đảo
- Câu 10
  - C, chỉ cần 2 số nguyên tố cùng nhau
- Câu 11
  - C, Giá trị hàm Euler là số các số nguyên tố cùng nhau vơi số đó
- Câu 12
  - D, Cộng và trừ đều là hai bài toán dễ
- Câu 13
  - D, ø(n) là số mũ dương nhỏ nhất để a mũ đó lên bằng 1
- Câu 14
  - C, nếu a là căn nguyên tố thì lũy thừa của a sẽ tạo nên tập các số nguyên tố với n

Glossary - Từ điển thuật ngữ

- Quan hệ đồng dư theo modulo n: là quan hệ giữa hai số nguyên có cùng phần dư dương khi chia cho n.
- Số học đồng dư theo modulo n là việc thực hiện các phép toán số học theo modulo n.
- Số nguyên tố là số chỉ có ước là 1 và chính nó
- Hai số được gọi là nguyên tố cùng nhau nếu chúng chỉ có ước số chung là 1.
- Giá trị hàm Euler của 1 số nguyên dương là số các số nguyên dương nhỏ hơn số đó và nguyên tố cùng nhau với nó.
- Căn nguyên tố của một số n là một số nguyên tố cùng nhau với n và lũy thừa của nó theo modulo n có giá trị là các số nguyên tố cùng nhau với n
- Bài toán logarit rời rạc theo modulo là bài toán ngược của bài toán lũy thừa theo modulo, nhưng khó hơn bài toán thuận rất nhiều.

FAQ – Câu hỏi thường gặp

1. Hai số như thế nào được gọi là có quan hệ đồng dư theo modulo n
2. Thế nào là đại diện của một số theo modulo n
3. Quan hê đồng dư có tính phản xạ, đối xứng và bắc cầu không? (có là quan hệ tương đương?)
4. Khi thực hiện các phép toán theo modulo ta có thể áp dụng các tính chất gì để tính toán nhanh?
5. Muốn thực hiện được phép chia theo modulo n, thì n cần có tính chất gì? Lợi ích sử dụng số học modulo
6. Nêu định nghĩa ước số chung, nguyên tố cùng nhau của 2 số nguyên dương?
7. Nêu định nghĩa số nguyên tố và nêu thuật toán kiểm tra số nguyên tố.

FAQ – Câu hỏi thường gặp (tiếp)

8. Nêu định nghĩa hàm Euler của 1 số tự nhiên và nêu cách tính
9. Thuật toán Euclid dùng để làm gì? Mô tả các bước thực hiện nó?
10. Thuật toán Euclid mở rộng dùng để làm gì? Mô tả các bước thực hiện nó?
11. Thuật toán Bình phương và nhân liên tiếp dùng để làm gì? Mô tả các bước thực hiện nó?
12. Phát biểu và cho ví dụ minh hoạ Định lý Ferma nhỏ?
13. Phát biểu và cho ví dụ minh hoạ Định lý Euler? Tại sao nó là mở rộng của Định lý Ferma
14. Định lý phần dư Trung hoa dùng để làm gì?
15. Nêu định nghĩa căn nguyên tố của 1 số, cho ví dụ
16. Nêu định nghĩa Logarit rời rạc của số b theo cơ sở a và modulo n

Trả lời câu hỏi:

1. Hai số có quan hệ đồng dư theo mod n, nếu chúng có cùng phần dư dương khi chia cho n.
2. Đại diện của 1 số theo mod n là số có quan hệ đồng dư với số đã cho theo mod n và có giá trị nằm giữa 0 và n -1.
3. Có, vì có thể nói hai số có quan hệ đồng dư khi hiệu của nó chia hết n, nên
   - mọi số đồng dư với chính nó
   - số a đồng dư với b, thì b cũng đồng dư với a
   - số a đồng dư với b và b đồng dư với c, thì a đồng dư với c
4. Khi thực hiện các phép toán theo modulo ta có thể áp dụng các tính chất sau để tính toán nhanh:
   - Thay mỗi số bằng đại diện của nó
   - Thay mỗi số bằng số có quan hệ đồng dư với nó
   - Luôn lấy modulo cho mỗi kết quả trung gian nhận được
   - Có thể áp dụng Định lý phần dư Trung hoa để tính trên modulo số nhỏ

Trả lời câu hỏi – (tiếp 2)

5. Số đó phải có nghịch đảo theo modulo n, chia là nhân với số nghịch đảo. Sử dụng số học modulo, ta sẽ đảm bảo các kết quả trong quá trình tính toán không vượt quá giới hạn cho trước
6. Xem bài giảng
7. Muốn kiểm tra 1 số có phải là số nguyên tố hay không, ta kiểm tra nó có chia hết cho mọi số nguyên tố nhỏ hơn hoặc bằng căn bậc hai của nó hay không? Tuy nhiên nếu số đó lớn thì việc kiểm tra trên lâu, nên có thuật toán Milner Rabin kiểm tra số đó có tinh chất như trong Định lý Ferma với số a tùy ý không, thỏa với càng nhiều số a, xác suất là nguyên tố càng lớn.
8. Giá trị hàm Euler của 1 số là số các số nguyên tố cùng nhau với số đó mà nhổ hơn nó. Tính giá trị hàm Euler tương đương với việc tìm phân tích của số đó ra thừa số là lũy thừa của các số nguyên tố.
9. Thuật toán Euclid để tính ước chung lớn nhất của 2 số. Nó lặp việc thay số bằng cặp số nhỏ và phần dư của số lớn theo số nhỏ, cho đến khi 1 số bằng 0, thì số kia là Ước chung lớn nhất.
10. Thuật toán Euclid mở rộng tính ước chung lớn nhất và tính nghịch đảo trong trường hợp 2 số nguyên tố cùng nhau. Nó giống như tiến hành đồng thời nhiều thuật toán Euclid cùng một lúc.

Trả lời câu hỏi – (tiếp)

11. Thuật toán bình phương và nhân liên tiếp dùng để tính nhanh lũy thừa của 1 số. Ở một bước nó luôn bình phương kết quả trước, có nhân với cơ số hay không tùy thuộc số mũ cho trước. Xem bài giảng
12. Xem bài giảng.
13. Định lý Euler là mở rộng của Ferma, vì nếu một số p là nguyên tố, thì nó sẽ nguyên tố cùng nhau với mọi số nhỏ hơn nó và giá trị hàm Euler của p bằng p-1.
14. Định lý phần dư Trung hoa dùng để đưa việc tính toán số học Modulo theo số lớn về việc tính toán số học modulo theo số nhỏ, nếu có thể phân tích số lớn thành tích các số nhỏ nguyên tố cùng nhau. Định lý này cũng giúp giải hệ phương trình modulo.
15. Xem bài giảng: căn nguyên tố là số nguyên tố cùng nhau với số đã cho mà lũy thừa của nó tạo nên tập các số nguyên tố cùng nhau với số đó.
16. Xem bài giảng: Logarit rời rạc theo modulo n là bài toán ngược của bài toán lũy thừa, nhưng khó hơn nhiều, thường đòi hỏi cơ số là căn nguyên tố của n và số lấy logarit cũng là nguyên tố cùng nhau với n