CHƯƠNG 3: SỐ HỌC ĐỒNG DƯ

Trong bài này chúng ta sẽ xét các số nguyên không âm và tìm kiếm các phép toán mới trên chúng sao cho nhận được một tập hữu hạn các số, trên đó có thể thực hiện các phép toán giống như các phép số học thông thường, mà kết quả vẫn nằm trong tập hữu hạn đó. Khi đó chúng ta có thể kiểm soát được kích thước và thời gian tính toán của các kết quả nhận được. Do đó mở ra khả năng mới ứng dụng cấu trúc toán học đó trong tin học.

3.1 Quan hệ đồng dư

Trước hết chúng ta xét quan hệ có cùng phần dư khi chia hết cho một số tự nhiên cố định trên tập các số nguyên không âm.

3.1.1. Định nghĩa modulo và các phép toán trên 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 $q = \lfloor a/n \rfloor$. Ở đây ký hiệu $\lfloor x \rfloor$. là số nguyên lớn nhất nhỏ hơn hoặc bằng x.
- Khi đó ký *hiệu phần dư dương r = a mod n* và ta có thể viết dưới dạng

  $$a = \lfloor a/n \rfloor.n + a \bmod n$$

  Ví dụ 1: 25 mod 7 = 4, vì 25 = 3.7 + 4

  (-25) mod 7 = 3, vì -25 = -4.7+ 3
- Định nghĩa *quan hệ tương đương* trên tập số nguyên,

  Nếu: a mod n = b mod n, thì ta viết $a \equiv b \bmod n$

  Khi đó ta gọi là a và b có quan hệ đồng dư theo n, tức là khi chia cho n, thì a và b có phần dư như nhau.

  Ví dụ 2: $100 \equiv 34 \bmod 11$, $21 \equiv (-9) \bmod 10$

  Số b được gọi là *đại diện của a theo mod n*, nếu

  $a \equiv b \bmod n$ (tức là $a = qn + b$) và $0 \le b \le n - 1$

  hay nói cách khác: b = a mod n là đại diện của a theo mod n

  Ví dụ 3: 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

  $-12 \bmod 7 \equiv -5 \bmod 7 \equiv 2 \bmod 7 \equiv 9 \bmod 7$

  Do đó 2 là đại diện của –12, -5, 2 và 9.

  Ví dụ 4: Trong modulo 7 ta có, các số trên cùng một cột là tương đương đồng dư với nhau vì chúng có cùng phần dư dương khi chia cho 7 và hàng viết đậm là các đại diện của chúng:

  ```
  . . .
  -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 = { **0, 1, 2, 3, …, n-1** }

Các phép toán số học trên modulo

Cho trước một số n. Ta muốn thực hiện các phép toán theo modulo của n, khi đó có thể 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 hoặc cũng có thể vừa tính toán, kết hợp với rút gọn theo modulo tại bất cứ thời điểm nào:

(a+b) mod n = [a mod n + b mod n] mod n (*)

(a.b) mod n = [a mod n . b mod n] mod n (**)

Như vậy khi thực hiện các phép toán ta có thể thay các số bằng các số tương đương theo modulo n đó hoặc đơn giản hơn có thể thực hiện các phép toán trên các đại diện của nó: Z_n = { 0, 1, 2, 3, …, n-1 }.

Ví dụ 5. Áp dụng tính chất (*):

(144 + 215) mod 7 = (144 mod 7 + 215 mod 7) mod 7 = (4 + 5) mod 7 = 2

Ví dụ 6. Áp dụng tính chất (**):

(144 . 315) mod 150 = (144 mod 150 . 315 mod 150) mod 150 =

((-6) mod 150 . 15 mod 150) mod 150 = (-6 . 15) mod 150 = (-90) mod 150 = 60

Ví dụ 7. Áp dụng các tính chất của modulo, ta có thể thay các số lớn bằng các số tương đương đồng dư:

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

$((11.19)$ mod 7 + 10^{17} mod 7) mod 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) mod 7 = 4

Ví dụ 8. Bảng 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

Ví dụ 9. Bảng 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

Ước số

- Số nguyên b không âm được gọi là ước số của a, nếu có số m sao cho: $a = mb$ trong đó a, b, m đều nguyên. Khi a chia hết cho b, ta ký hiệu là $b|a$
- Ví dụ: 1, 2, 3, 4, 6, 8, 12, 24 là các ước số của 24

Ước số chung lớn nhất.

Bài toán. Cho hai số nguyên dương a và b. Bài toán tìm ước chung lớn nhất của hai số nguyên dương là bài toán chung của lý thuyết số. Ta ký hiệu GCD(a,b) là ước số chung dương lớn nhất của a và b, tức là số nguyên dương vừa là ước của a vừa là ước của b và là số nguyên dương lớn nhất có tính chất đó.

Ví dụ 10: GCD(60,24) = 12 ; GCD (6, 15) = 3; GCD(8, 21) = 1.

- **Nguyên tố cùng nhau**. Ta thấy 1 bao giờ cũng là ước số chung của hai số nguyên dương bất kỳ. Nếu GCD(a, b) = 1, thì a, b được gọi là hai số nguyên tố cùng nhau.

Ví dụ 11: GCD(8,15) = 1, do đó 8 và 15 là hai số nguyên tố cùng nhau.

- **Tìm ước chung lớn nhất**. Bây giờ chúng ta xét bài toán tìm ước số chung lớn nhất của hai số nguyên dương cho trước. Dễ dàng chứng minh được tính chất sau với a, b là hai số nguyên dương và b không lớn hơn a:

  GCD(a,b) = GCD(b, a mod b)

  Như vậy để tìm ước số chung của một cặp số cho trước, ta đưa về bài toán tìm ước chung của cặp số gồm số nhỏ hơn trong hai số đó và phần dư của số lớn khi chia cho số nhỏ hơn. Thuật toán Euclid tạo nên vòng lặp, ở mỗi bước ta áp dụng tính chất trên cho đến khi phần dư đó còn khác 0. Khi một trong hai số bằng 0, thì số kia chính là ước số chung lớn nhất cần tìm.

- **Thuật toán Euclid tìm GCD(a, b)**

  A=a, B=b

  while B>0 • R = A mod B

  A = B, B = R

  return A

Ví dụ 10: Tính GCD(1970,1066)

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

Vậy gcd(1970, 1066) = 2

3.2. Phép toán nghịch đảo

Bây giờ ta xét bài toán: nếu GCD(m, b) = 1, thì tìm nghịch đảo của b theo modulo m, tức là tìm số a nguyên dương trong khoảng từ 1 đến m – 1, sao cho

(a.b) mod m = 1

Ta mở rộng thuật toán Euclid để vừa tìm ước chung lớn nhất của m và b, vừa tính nghịch đảo trong trường hợp GCD(m, b) = 1.

Thuật toán Euclid mở rộng:

```
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
```

Thật vậy, các quan hệ sau là bất biến:

$$mA_1 + bA_2 = A_3; \quad (1)$$

$$mB_1 + bB_2 = B_3 \quad (2)$$

$$mT_1 + bT_2 = T_3; \quad (3)$$

Vì ban đầu: m.1 + b.0 = m; m.0 +b.1 = b, nên ta có (1) và (2) đúng. Và ta chứng minh trong một bước lặp từ (1) và (2) suy ra (3). Từ thuật toán ta có :

$$T_1 = A_1 – Q.B_1$$

$$T_2 = A_2 – Q.B_2$$

$$T_3 = A_3 – Q.B_3$$

Nên ta sẽ chứng minh đẳng thức (3) còn lại

$$\begin{aligned} mT_1 + bT_2 &= m(A_1 – Q.B_1) + b\,(A_2 – Q.B_2) \\ &= (mA_1 + bA_2) - Q(mB_1 + bB_2) \\ &= A_3 – Q.B_3 \\ &= T_3 \end{aligned}$$

Khi sang bước lặp tiếp theo đổi vai trò B sang A và T sang B, thì các công thức (1) và (2) đối với A, B sẽ đúng, và do đó theo chứng minh trên (3) sẽ đúng trong bước lặp tiếp theo. Vậy (1), (2), (3) là các bất biến của vòng lặp.

Cuối cùng khi $B_3 = 1$, thì từ các bất biến ta có:

$$mB_1 + bB_2 = 1$$

$$bB_2 = 1 - mB_1$$

$$bB_2 \bmod m = 1$$

Do đó theo định nghĩa số nghịch đảo ta có: $B_2 = b^{-1} \bmod m$

Ví dụ 11. Tìm nghịch đảo của 550 theo mod 1759 (nếu có).

Mỗi bước thực hiện thuật toán Euclid mở rộng sẽ được mô tả bởi một hàng trong bảng sau:

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

Sau 4 bước, ta có $B_3 = 1$, khi đó thuật toán dừng, GCD(1759, 550) = 1 và 550^{-1} mod 1759 = 355.

Dễ dàng kiểm chứng lại: (355*550) mod 1759 = 195250 mod 1759 = 1

3.3. Hàm số Euler

3.3.1. Các số nguyên tố

Như chúng ta đã biết 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 hai số khác. 1 là số nguyên tố, nhưng không quan tâm đến nó. Xét các số nhỏ hơn 10 ta có: 2, 3, 5, 7 là số nguyên tố, vì chúng không có ước số nào khác 1 và chính nó; 4, 6, 8, 9, 10 không phải là số nguyên tố. Có thể nói 2 là số chẵn duy nhất là số nguyên tố. Các số nguyên tố là trung tâm của lý thuyết số. Số các số nguyên tố là vô hạn.

Ví dụ 12. Sau đây là 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
```

3.3.2. Phân tích ra thừa số nguyên tố

Một trong những bài toán cơ bản của số học là phân tích số a ra thừa số nguyên tố, tức là viết nó dưới dạng tích của lũy thừa các số nguyên tố. Lưu ý rằng phân tích là bài toán khó hơn rất nhiều so với bài toán nhân các số để nhận được tích.

Ta có kết luận, mọi số nguyên dương đều có phân tích duy nhất thành tích các lũy thừa của các số nguyên tố:

$$a = \prod_{p \in P} p^{a_p}$$

Ví dụ 13: $91 = 7 \times 13$; $3600 = 2^4 \times 3^2 \times 5^2$

Thông thường để tìm phân tích trên, ta phải kiểm tra tính chia hết cho các số nguyên tố từ nhỏ đến lớn và thực hiện phép chia liên tiếp cho các số nguyên tố, rồi gộp thành lũy thừa của các số nguyên tố.

3.3.3. Các số nguyên tố cùng nhau và GCD

Hai số nguyên dương a và b không có ước chung nào ngoài 1, được gọi là nguyên tố cùng nhau.

Ví dụ 14: 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 của 8 và 15.

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 trong hai phân tích của hai số đó.

Ví dụ 15. Ta có phân tích: $300 = 2^1 \times 3^1 \times 5^2$ và $18 = 2^1 \times 3^2$. Vậy

$$GCD(18,300) = 2^1 \times 3^1 \times 5^0 = 6$$

3.3.4. Hàm Euler

Cho n là một số nguyên dương. Khi thực hiện phép tính đồng dư n của mọi số nguyên khác ta nhận được tập đầy đủ các phần dư có thể có là:

0, 1, 2,…, n - 1

Từ tập trên ta tìm tập rút gọn bao gồm các số nguyên tố cùng nhau với n và quan tâm đến số lượng các phần tử như vậy đối với số nguyên dương n cho trước.

Ví dụ 16. Với n = 10:

- Tập đầy đủ các phần dư là {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}
  - Số các phần tử của tập rút gọn trên là giá trị của hàm Euler Φ(n). Như vậy, Φ(10) = 4.
- Muốn tính Φ(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 có thể tính hàm Euler của một số dựa trên biểu thức phân tích ra thừa số của số đó.
  - Dễ dàng thấy, nếu p là số nguyên tố, thì Φ(p) = p-1
  - Nếu p và q là hai số nguyên tố khác nhau, thì có thể chứng minh được rằng: Φ(p.q) = (p -1).(q -1)
  - Nếu p là số nguyên tố, thì $\Phi(p^n) = p^n - p^{n-1}$
  - Nếu s và t là hai số nguyên tố cùng nhau, thì Φ(s.t) = Φ(s).Φ(t)

Ví dụ 17.

$\Phi(37) = 37 - 1 = 36$

$\Phi(21) = (3-1)\times(7-1) = 2\times 6 = 12$

$\Phi(72) = \Phi(8.9) = \Phi(8).\ \Phi(9) = \Phi(2^3).\Phi(3^2) =$

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

3.4. Một số định lý số học cơ bản

3.4.1. Định lý Ferma nhỏ

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

trong đó p là số nguyên tố và a là số nguyên bất kỳ khác bội của p, tức là GCD(a, p) = 1, hay với mọi số nguyên tố p và số nguyên a không là bội của p, ta luôn có

$$a^p = a \bmod p$$

Công thức trên luôn đúng, nếu p là số nguyên tố, còn a là số nguyên dương nhỏ hơn p.

Ví dụ 18. Vì 5 và 7 là các số nguyên tố. Và 2 và 3 không là bội tương ứng của 7 và 5, nên theo định lý Ferma ta có

$2^{7-1} \bmod 7 = 1$ (= $2^6 \bmod 7 = 64 \bmod 7 = 1$)

$3^{5-1} \bmod 5 = 1$ (= $3^4 \bmod 5 = 81 \bmod 5 = 1$)

$(-2)^{11-1} \bmod 11 = 1$ (= $2^{10} \bmod 11 = 1024 \bmod 11 = 1$)

Kết quả trên được dùng trong mã khoá công khai. Nó cũng được sử dụng để kiểm tra tính nguyên tố của một số nguyên p nào đó, bằng cách lấy ngẫu nhiên các số a và kiểm tra xem có tính chất nêu trên không, kết luận là p nguyên tố càng thuyết phục nếu phép thử trên đúng với nhiều lần chọn ngẫu nhiên các số a.

3.4.1.1. Kiểm tra tính nguyên tố

Giả sử cần phải tìm một số nguyên tố rất lớn. Lấy ngẫu nhiên một số đủ lớn, ta cần phải kiểm tra xem số đó có phải là số nguyên tố không. Phương pháp truyền thống là thử bằng phép chia như sau:

- Chia cho tất cả các số (chỉ cần nguyên tố) nhỏ hơn hoặc bằng căn bậc hai của số đó. Nếu nó không chia hết cho số nào, thì đó là số nguyên tố.
- Chỉ hiệu quả khi xét các số nhỏ.

Có phương pháp khác, mà ta sẽ xét ở đây, sử dụng các phép kiểm tra tính nguyên tố thống kê dựa trên các tính chất:

- Mà mọi số nguyên tố phải thỏa mãn;
- Nhưng có một số số không nguyên tố, gọi là giả nguyên tố cũng thoả mãn tính chất đó.

Cụ thể là phép kiểm tra dựa trên định lý Ferma như sau: nếu số n cần kiểm là số nguyên tố, thì nó sẽ thỏa mãn định lý Ferma đối với mọi số a nhỏ hơn nó $a^{n-1} \bmod n = 1$. Như vậy, lấy ngẫu nhiên số a và kiểm tra xem nó có tính chất trên không. Nếu có thì n có thể là số nguyên tố, nếu cần độ tin cậy lớn hơn, thì ta kiểm tra liên tiếp nhiều lần như vậy với các số ngẫu nhiên a được chọn. Sau mỗi lần qua được phép thử, xác suất để n là số nguyên tố lại tăng lên. Chú ý rằng

- nếu $b^i \bmod n = 1$, thì $b^{2i} \bmod n = (1)^2 \bmod n = 1$ và
- nếu $b^i \bmod n = n - 1$, thì $b^{2i} \bmod n = (n - 1)^2 \bmod n = (n^2 - 2n + 1) \bmod n = 1$

Kiểm tra số n có là số nguyên tố không, ta chỉ cần xét n là lẻ, khi đó n-1 là chẵn và biểu diễn nó dạng: $(n-1) = 2^k.q$

Khi đó để tính a^{n-1}, ta tính a^q, sau đó bình phương liên tiếp k lần. Cụ thể thuật toán thể hiện ở phần sau.

3.4.1.2. Thuật toán Miller - Rabin

Thuật toán như sau:

```
TEST (n) is:
1. Find integers k, q, k > 0, q odd, so that (n-1)= 2^k.q
2. Select a random integer a, 1<a<n-1
3. if a^q mod n = 1 then return ("maybe prime");
4. for j = 0 to k - 1 do
5. if (a^(2^j.q) mod n = n-1)
    then return(" maybe prime ")
6. return ("composite")
```

Các xem xét về mặt xác suất.

Nếu thuật toán Miller - Rabin trả về số "composite" thì số đó chắc chắn không là số nguyên tố, vì khi đó số n và số a < n không thoả mãn định lý Ferma, tức là $a^{n-1} \bmod n \neq 1$.

Ngược lại số đó có thể là số nguyên tố hoặc giả nguyên tố theo nghĩa nó thoả mãn định lý Ferma với số a < n. Người ta chứng minh được rằng xác suất để số giả nguyên tố đó không là số nguyên tố là là 1/4. Suy ra nếu lặp t phép thử với các lựa chọn ngẫu nhiên khác nhau của số a, thì khi đó xác suất để số n sau t phép thử là số nguyên tố là: $1-(1/4)^t$.

Ví dụ. Sau 10 bước, t = 10, mà số đã cho n đều có thể là nguyên tố, thì xác suất để n là số nguyên tố là $1 - (1/4)^{10} > 0{,}99999$.

3.4.2. Định lý Euler

Định lý Euler là tổng quát hoá của Định lý Ferma, khẳng định như sau:

$$a^{\Phi(n)} \bmod n = 1$$

với mọi cặp số nguyên dương nguyên tố cùng nhau a và n: gcd(a,n)=1.

Ví dụ 19: $a = 3; n = 10; \Phi(10)=4;$

Vì vậy $3^4 = 81 = 1 \bmod 10$

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

Do đó $2^{10} = 1024 = 1 \bmod 11$

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

Do đó $4^8 \bmod 15 = 1,$

Ta có thể tính trực tiếp $4^8 \bmod 15 = (4^2)^4 \bmod 15 = 1$

Như vậy, cho các số nguyên dương a, n, m bất kỳ, áp dụng tính chất của phép nhân modulo và Định lý Euler ta luôn có:

$$a^m \bmod n = (a \bmod n)^{(m \bmod \Phi(n))} \bmod n$$

Chẳng hạn: $45^{18} \bmod 20 = (45 \bmod 20)^{18 \bmod \Phi(20)} \bmod 20 = 5^2 \bmod 20 = 5$

3.4.3. Định lý phần dư Trung Hoa

Trong nhiều trường hợp ta muốn tìm cách để tăng tốc độ tính toán modulo. Các phép toán trên modulo các số nhỏ tính nhanh hơn nhiều so với các số lớn. Chính vì vậy nếu số lớn phân tích được thành tích của các số nhỏ, từng cặp nguyên tố cùng nhau, thì ta sẽ có cách tính hiệu quả nhờ vào định lý Phần dư Trung hoa.

Tính toán trên modulo của một tích các số mod M với $M= m_1m_2..m_k$, trong đó $GCD(m_i, m_j) = 1$, với mọi i khác j. Định lý phần dư Trung Hoa cho phép làm việc trên từng modulo m_i riêng biệt. Vì thời gian tính toán các phép toán trên modulo tỷ lệ với kích thước của số lấy modulo nên điều đó sẽ nhanh hơn tính toán trên toàn bộ M.

Có thể triển khai Định lý Trung Hoa theo một số cách như sau:

- **Tính toán theo modulo số lớn.** Để tính A mod M, với M khá lớn và A là biểu thức số học nào đó. Trước hết ta cần tính tất cả $a_i = A \bmod m_i$. Sau đó sử dụng công thức:

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

trong đó $M_i = M/m_i$

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

Ví dụ 20. Tính 17^8 mod 77. Áp dụng định lý phần dư Trung Hoa, ta coi $A = 17^{18}$, $m_1 = 7$, $m_2 = 11$. Khi đó $M_1 = 11$, $M_2 = 7$ và

$11^{-1} \bmod 7 = 4^{-1} \bmod 7 = 2$, suy ra $c_1 = 11.2 = 22$

$7^{-1} \bmod 11 = 8$, suy ra $c_2 = 7.8 = 56$

$a_1 = 17^8 \bmod 7 = (17 \bmod 7)^8 \bmod 7 = 3^8 \bmod 7 = (3^2)^4 \bmod 7 = 2$

$a_2 = 17^8 \bmod 11 = (17 \bmod 11)^8 \bmod 11 = 6^8 \bmod 11 =$

$= (6^2)^4 \bmod 11 = 3^4 \bmod 11 = 4$

Vậy $A = 17^8 \bmod 77 = (2.22 + 4.56) \bmod 77 = 268 \bmod 77 = 37$

- **Giải hệ phương trình modulo**. Cho $a_i = x \bmod m_i$, với $GCD(m_i, m_j) = 1$, với mọi i khác j. Khi đó ta cũng áp dụng định lý phần dư Trung Hoa để tìm x. Coi x là biểu thức cần tính theo modulo số lớn $M = m_1 m_2 .. m_k$.

Ví dụ 21. Cho $x \equiv 5 \bmod 7$ và $x \equiv 6 \bmod 11$. Tìm x.

Áp dụng định lý phần dư Trung hoa, ta tính:

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

$x = (5.2.11 + 6.8.7) \bmod (7.11) = 61 \bmod 77$.

3.5. Thuật toán bình phương và nhân liên tiếp

Trong các bài toán mã hoá công khai, chúng ta sử dụng nhiều phép toán lũy thừa với số mũ lớn. Như vậy cần có thuật toán nhanh hiệu quả đối với phép toán này. Trước hết ta phân tích số mũ theo cơ số 2, xét biểu diễn nhị phân của số mũ, sau đó sử dụng thuật toán bình phương và nhân liên tiếp. Khái niệm được dựa trên phép lặp cơ sở bình phương và nhân liên tiếp để nhận được kết quả mong muốn. Độ phức tạp của thuật toán là $O(\log_2 n)$ phép nhân đối với số mũ n.

Ví dụ 22:

$7^5 \bmod 11 = 7^4 \bmod 11.7^1 \bmod 11 = 3.7 \bmod 11 = 10$

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

$7^4 \bmod 11 = 7^2 \bmod 11 \,.7^2 \bmod 11 = (5.5) \bmod 11 = 3$

$3^{129} \bmod 11 = (3^{128} \bmod 11.3^1 \bmod 11) \bmod 11 = (5.3) \bmod 11 = 4$

Vì $3^2 \bmod 11 = 9 \bmod 11 = (-2) \bmod 11$

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

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

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

$3^{32} \bmod 11 = 5$

$3^{64} \bmod 11 = 4$

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

Khi cài đặt thuật toán tính lũy thừa ta có thể kết hợp bình phương và nhân liên tiếp dựa trên triển khai nhị phân của lũy thừa.

Phân tích số mũ theo cơ số 2

Trước hết ta chuyển số mũ 11 từ cơ số 10 sang cơ số 2: $(11)_{10} = (1011)_2$. Sau đó tính toán như sau:

$M^{11} = M^{1.2\hat{}3 + 0.2\hat{}2 + 1.2\hat{}1 + 1.2\hat{}0}$

$= (M^{1.2\hat{}2 + 0.2\hat{}1 + 1.2\hat{}0})^2 M$

$= (M^{1.2\hat{}1 + 0.2\hat{}0})^2 M)^2 M$

$= ((M^2)^2 M)^2 M$

Như vậy, giả sử ta có số mũ là số nguyên được biểu diễn dưới dạng cơ số 2.

Bước khởi tạo: ban đầu gán kết quả bằng 1, thực hiện vòng lặp:

Bước lặp: duyệt dãy bit biểu diễn lũy thừa từ trái qua phải cho đến hết:

- Bình phương kết quả
- Nếu bit là 1, thì nhân kết quả với cơ số;

Kết thúc: khi duyệt hết dãy bit, kết quả cho giá trị lũy thừa cần tìm.

Thuật toán bình phương và nhân liên tiếp

Giả sử $b_k b_{k-1} \ldots b_0$ là biểu diễn cơ số 2 của c.

Tính $a^c \bmod n$

```
C ← 0; d ← 1
for i ← k downto 0
        do c ← 2 × c
           d ← (d ×d) mod n
           if      b_i = 1
                   then    c ← c + 1
                           d ← (d × a) mod n
```

Trong thuật toán trên giá trị của c chỉ dùng để kiểm tra số mũ của lũy thừa. Còn d chính là giá trị lũy thừa cần tính và a là cơ số của luỹ thừa.

3.6. Căn nguyên thủy

Từ định lý Euler ta có $a^{\Phi(n)} \bmod n = 1$, với a và n là nguyên tố cùng nhau. Nếu không có số mũ dương nào nhỏ hơn $\Phi(n)$, mà có tính chất như vậy đối với a, thì khi đó ta gọi a là căn nguyên thủy của n. Cụ thể như sau:

- Tìm m nguyên dương nhỏ nhất, sao cho: $a^m \bmod n = 1$, trong đó GCD(a,n)=1

Theo định lý Euler ta có m = Φ(n) thỏa mãn hệ thức trên, nhưng có thể cũng có giá trị nhỏ hơn của m < Φ(n) cũng thoả mãn. Khi có được m như vậy, thì nó cũng thoả mãn với bội của m, tức là sẽ có vòng lặp.

- Nếu giá trị m = Φ(n) là số dương nhỏ nhất thoả mãn công thức trên thì a được gọi là căn nguyên thủy của n. Khi đó: a^0, a^1, …, a^{m-1} sẽ sinh ra m số nguyên dương, nguyên tố cùng nhau với n và nhỏ hơn n.
- Nếu p là số nguyên tố và a là căn nguyên thủy của p, thì các luỹ thừa của a: a^0, a^1, …, a^{p-2} sẽ sinh ra p-1 số nguyên đầu tiên.

Việc tìm các căn nguyên thủy a của n sẽ có ích trong việc xét mã công khai.

Ví dụ 23. Xét số nguyên tố p = 5 và xét xem a = 2 có phải là căn nguyên thủy của 5 không?

Ta có:

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

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

- Xét số n = 6 và xét xem a = 3 có phải là căn nguyên thủy của 3 không?

Ta có

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

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

Logarit rời rạc

Bài toán ngược của bài toán lũy thừa là tìm logarit rời rạc của một số modulo p, tức là tìm số nguyên x sao cho

$$a^x = b \bmod p$$

Hay còn được viết là $x = \log_a b \bmod p$ hoặc $x = \text{ind}_{a,p}(b)$

Nếu a là căn nguyên thủy của p và p là số nguyên tố, thì luôn luôn tồn tại logarit rời rạc. Hoặc tổng quat hơn, nếu a là căn nguyên thủy của n và hai số b, n số nguyên tố cùng nhau, thì luôn luôn tồn tại logarit rời rạc cơ số a của b.

Ví dụ 24.

Tìm $x = \log_2 3 \bmod 13$. Bằng cách thử lần lượt:

$2^0 \bmod 13 = 1$; $2^1 \bmod 13 = 2$, $2^2 \bmod 13 = 4$, $2^3 \bmod 13 = 8$, $2^4 \bmod 13 = 3$.

Vậy $\log_2 3 \bmod 13 = 4$.

Tìm $x = \log_3 4 \bmod 13$ (tìm x: $3^x = 4 \bmod 13$). Trong trường hợp này không có lời giải, vì:

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

Do đó, lũy thừa của 3 theo modulo 13 chỉ nhận các giá trị 1, 3, 9 và không có lũy thừa nào đạt giá trị bằng 4. Ở đây 3 không là căn nguyên thủy của 13, vì 3 < Φ(13) = 12.

Ta nhận thấy, trong khi bài toán lũy thừa là dễ dàng, thì bài toán logarit rời rạc là rất khó. Đây cũng là một cơ sở để thiết lập mã công khai.

3.7. Các bài tập

3.7.1. Số học đồng dư

- Giả sử n là số nguyên dương, a là số nguyên, ta biểu diễn dưới dạng:

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

- Viết công thức (*) cho các cặp số (n, a) sau:
  - (15, 51): 51 = ?
  - (15, -51): -51 = ?
- Tìm đại diện của các số 215 và -157 theo mod 29
  - 215 mod 29 =
  - (-157) mod 29 =
- Theo modulo 13: chia tập các số từ -26 đến 25 thành các lớp tương đương, nêu các đại diện của chúng?
- Biểu thức nào đúng:
  - 101 ≡ 36 mod 13?
  - (-101) ≡ (-36) mod 13?
  - 165 ≡ 34 mod 65?
  - (-165) ≡ 30 mod 65?
- Viết công thức (*) cho các cặp số (n, a) sau:
  - (15, 51): 51 = 3.15 + 6; Do đó theo định nghĩa: 51 mod 15 = 6
  - (15, -51): -51 =-4.15 + 9; Vậy: (-51) mod 15 = 9
- Tìm đại diện của các số 215 và -157 theo mod 29
  - 215 mod 29 = 12; Do đó theo định nghĩa: 12 là đại diện của 215 theo modulo 29
  - -158 mod 29 = 29 – 158 mod 29 = 29 – 13 = 16
- Các lớp tương đương và đại diện modulo 13:

-26	-25	-24	-23	-22	-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

Hàng viết đậm từ 0 đến 12 gồm các đại diện của modulo 13.

- Quan hệ tương đương đồng dư: hai số có quan hệ đồng dư theo modulo n, nếu chúng có cùng số dư khi chia cho n:
  - 101 ≡ 36 mod 13? – Đúng
  - -101 ≡ -36 mod 13? – Sai
  - 165 ≡ 34 mod 65? - Sai
  - -165 ≡ 30 mod 65? - Đúng

Các công thức cộng, trừ, nhân theo modulo:

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

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

- Lập bảng nhân theo modulo 11, nêu các cặp nghịch đảo nhau trong bảng.
- Bạn có thể thay các số bằng các số tương đương theo mod n bất cứ lúc nào?
  - (74 - 215) mod 9 = ?
  - (244.315) mod 250 = ?
  - (144.315 – 265.657) mod 51 = ?

Bảng nhân modulo 11

X	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	8	2	6	10	3	4
5	0	5	10	4	8	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	11	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Các cặp sau nghịch đảo nhau theo modulo 11, vì chúng có tích theo modulo bằng 1:
(1, 1), (2, 6), (3, 4), (4, 3), (5, 9), (6, 2), (7, 8), (8, 7), (9, 5), (10, 10)
Cộng, nhân modulo

- Áp dụng tính chất (**):
  (74 -215) mod 9 = -141 mod 9 = 9 -141 mod 9 = 9-6=3
  hay (74 mod 9 - 215 mod 9) mod 9 =
  (2 - 8) mod 9 = -6 mod 9 = 3
- Áp dụng tính chất (***):
  (244 . 315) mod 250 = (244 mod 250 . 315 mod 250) mod 250
  = ((-6) mod 250 . 65 mod 250) mod 250 = (-6 .65) mod 250 = (-390) mod 250
  = 250 - 390 mod 250 = 250 -140 =110
- (144.315 – 265.657) mod 51
  = (144.315 mod 51 – 265.657 mod 51) mod 51
  = (-9.9 mod 51– (10.(-6)) mod 51) mod 51
  = (-81 + 60) mod 51 = -21 mod 51 = 51 – 21 mod 51 = 30

3.7.2. Thuật toán Euclid

Áp dụng thuật toán Euclid:

2110 = 1 x 1945 + 165 gcd(1945, 165)
1945 = 11 x 165 + 130 gcd(165, 130)

165 = 1 x 130 + 35 gcd(130, 35)
130 = 3 x 35 + 25 gcd(35, 25)
35 = 1 x 25 + 10 gcd(25, 10)
25 = 2 x 10 + 5 gcd(10, 5)
10 = 2 x 5 + 0 gcd(5, 0)

Vậy ta có ước chung cần tìm là 5:

GCD(2110, 1945) = GCD(5, 0) = 5

Thuật toán Euclid mở rộng

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

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

  Nếu gcd(b, m) = 1, tức là hai số nguyên tố cùng nhau, thì tồn tại $b^{-1} \bmod m$
- Tìm trực tiếp bằng định nghĩa:
  - $6^{-1} \bmod 11 = ?$
  - $5^{-1} \bmod 11 = ?$
  - $6^{-1} \bmod 13 = ?$
  - $12^{-1} \bmod 13 = ?$; $(n-1)^{-1} \bmod n = ?$
  - $13^{-1} \bmod 15 = ?$
  - $21^{-1} \bmod 25 = ?$

Giải:

- $6^{-1} \bmod 11 = 2$, vì $6.2 \bmod 11 = 1$
- $5^{-1} \bmod 11 = 9$, vì $9.5 \bmod 11 = 1$
- $6^{-1} \bmod 13 = 11$, vì $(-2).6 \bmod 13 = 1$
- $12^{-1} \bmod 13 = (-1)^{-1} \bmod 13 = -1 \bmod 13 = 12$
- $(n-1)^{-1} \bmod n = n-1$
- $13^{-1} \bmod 15 = (-2)^{-1} \bmod 15 = -8 \bmod 15 = 7$
- $21^{-1} \bmod 25 = (-4)^{-1} \bmod 15 = 6$
- Với các số lớn thì ta dùng thuật toán nào để tìm nghịch đảo của số b theo modulo n?
  - $845^{-1} \bmod 2011 = ?$ Ta sử dụng thuật toán Euclid mở rộng để tìm nghịch đảo.

Q	A1	A2	A3	B1	B2	B3
—	1	0	2011	0	1	845
2	0	1	845	1	–2	321
2	1	–2	321	–2	5	203
1	–2	5	203	3	–7	118
1	3	-7	118	-5	12	85

1	-5	12	85	8	-19	33
2	8	-19	33	-21	50	19
1	-21	50	19	29	-69	14
1	29	-69	14	-50	119	5
2	-50	119	5	129	-307	4
1	129	-307	4		426	1

- Vậy $845^{-1} \bmod 2011 = 426 \bmod 2011 = 426$

3.7.3. Các định lý số học cơ bản

- **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 $$a^p \pmod p = a \pmod p$$

- Tính các giá trị sau:
  - $5^{12} \pmod{13} = 1$
  - $8^{13} \pmod{13} = 8$
  - $10^{100} \pmod{17} = (10^{16})^6 . 10^4 \pmod{17} = 9^2 \bmod 17 = 13$
  - $15^{125} \pmod{19} = (15^{18})^7 . 15^{-1} \pmod{19} = 14$
- **Hàm Euler**. Hàm Euler của một số n là số các số nguyên tố cùng nhau với n và nhỏ hơn n.

N	Φ(n)	Điều kiện
P	P - 1	p nguyên tố
p^n	$p^n - p^{n-1}$	p nguyên tố
s.t	Φ(s).Φ(t)	s, t nguyên tố cùng nhau
p.q	(p-1)(q-1)	p, q hai nguyên tố khác nhau

- Tính giá trị hàm Euler:
  - $\Phi(23) = 22$
  - $\Phi(55) = \Phi(5.11) = \Phi(5).\Phi(11) = 4.10 = 40$
  - $\Phi(180) = \Phi(4.5.9) = \Phi(4).\Phi(5).\Phi(9) = \Phi(2^2).\Phi(5).\Phi(3^2) = (2^2 - 2).4.(3^2 - 3) = 48$
  - $\Phi(200) = \Phi(8.25) = \Phi(2^3).\Phi(5^2) = (2^3 - 2^2).(5^2 - 5) = 80$
  - $\Phi(900) = \Phi(4.9.25) = \Phi(4).\Phi(9).\Phi(25) = \Phi(2^2).\Phi(3^2).\Phi(5^2)$ $= (2^2 - 2).(3^2 - 3).(5^2 - 5) = 2.6.20 = 240$
  - $\Phi(6300) = \Phi(7.900) = \Phi(7).\Phi(900) = 6.240 = 1440$

Định lý Euler

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

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

- Tính:
  - $4^8 \bmod 15 = 1$, vì $\Phi(15) = 8$, $\gcd(4, 15) = 1$.
  - $11^9 \bmod 20 = 10$, vì $\Phi(20) = 8$, $\gcd(11, 20) = 1$
  - $12^{402} \bmod 25 = 19$, vì $\Phi(25) = 20$, $\gcd(12, 25) = 1$, $402 = 20.20 + 2$,
  - $12^{402} \bmod 25 = 12^{400}.12^2 \bmod 25 = 144 \bmod 25 = 19$
  - $135^{162} \bmod 64 = (135 \bmod 64)^{32.5+2} \bmod 64 = 7^2 \bmod 64 = 49$, vì $\Phi(64) = \Phi(2^6) = 64 - 32 = 32$
  - $335^{453} \bmod 23 = (335 \bmod 23)^{22.20+13} \bmod 23 = 5^{13} \bmod 23 = 5^8.5^4.5 \bmod 23 = 16.4.5 \bmod 23 = 21$, vì $\Phi(23) = 22$
  - $(3/7)^8 \bmod 10 = (3.7^{-1})^8 \bmod 10 = (3.3)^8 \bmod 10 = (-1)^8 \bmod 10 = 1$

3.7.4. Lũy thừa theo modulo

- Dựa vào định lý Euler đơn giản bài toán
- Theo thuật toán lũy thừa dựa trên biểu diễn nhị phân của số mũ n
  - $11^{23} \bmod 187$

    $23 = 16 + 4 + 2 + 1$; $23_2 = 10111$

    $11^{23} \bmod 187 = (((1^2.11)^2)^2.11)^2.11)^2.11) \bmod 187$
- Trên thực tế tính toán bằng tay được dựa trên phép lặp bình phương và nhân với cơ số
  - $11^{23} \bmod 187 = 11^{16}.11^4.11^2.11 \bmod 187$
  - $11^2 \bmod 187 = 121$
  - $11^4 \bmod 187 = 121^2 \bmod 187 = 55$
  - $11^8 \bmod 187 = 55^2 \bmod 187 = 3025 \bmod 187 = 33$
  - $11^{16} \bmod 187 = 33^2 \bmod 187 = 1089 \bmod 187 = 154$
  - $11^{23} \bmod 187 = 11^{16}.11^4.11^2.11 \bmod 187 = (154.55.121.11) \bmod 187$
    $= (-33.(-66).5.11.11) \bmod 187 = 3.6.5.11^4 \bmod 187 = 3.6.5.55 \bmod 187$
    $= 265 \bmod 187 = 88$

Căn nguyên thủy

- Xét m để $a^m \bmod n = 1$.

  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.
- a = 2 có phải là căn nguyên thủy của 7 không? $\Phi(7) = 6$

  $2 \bmod 7 = 2$; $2^2 \bmod 7 = 4$; $2^3 \bmod 7 = 1$;

  $3 < 6 = \Phi(7)$, vậy 2 không là căn nguyên thủy của 7.
- a = 2 có phải là căn nguyên thủy của 11 không? $\Phi(11) = 10$

  $2 \bmod 11 = 2$; $2^2 \bmod 11 = 4$; $2^3 \bmod 11 = 8$;

$2^4 \bmod 11 = 5$; $2^5 \bmod 11 = 10$; $2^6 \bmod 11 = 9$,

$2^7 \bmod 11 = 7$; $2^8 \bmod 11 = 3$; $2^9 \bmod 11 = 6$, $2^{10} \bmod 11 = 1$

Vậy 2 là căn nguyên thủy của 11.

- a = 3 có phải là căn nguyên thủy của 11 không? $\Phi(11)= 10$

  $3 \bmod 11 = 3$; $3^2 \bmod 11 = 9$; $3^3 \bmod 11 = 5$;

  $3^4 \bmod 11 = 4$; $3^5 \bmod 11 = 1$;

  $5 < 10 = \Phi(11)$, vậy 3 không là căn nguyên thủy của 11.

- Ta lấy ví dụ một số cặp (số nguyên tố, căn nguyên thủy) sau:

  (3, 2); (5, 2); (7, 3), (11, 2); (13, 6); (17, 10); (19, 10); (23, 10)

Logarit rời rạc

- Cho a, b, p là các số tự nhiên, với gcd(a,p)=1 = gcd(b,p)
- Tìm x sao cho $a^x = b \bmod p$ Hay $x = \log_a b \bmod p$
- Dễ dàng thấy, nếu a là căn nguyên thủy của p thì luôn luôn tồn tại:
  - $x = \log_2 5 \bmod 11 = 4$

    $2^0 \bmod 11 = 1$; $2^1 \bmod 11 = 2$; $2^2 \bmod 11 = 4$;
    $2^3 \bmod 11 = 8$; $2^4 \bmod 11 = 5$;
  - $x = \log_2 5 \bmod 13 = 9$

    $2^0 \bmod 13 = 1$; $2^1 \bmod 13 = 2$; $2^2 \bmod 13 = 4$;

    $2^3 \bmod 13 = 8$; $24 \bmod 13 = 3$; $2^5 \bmod 13 = 6$;

    $2^6 \bmod 13 = 12$; $2^7 \bmod 13 = 11$; $2^8 \bmod 13 = 9$;

    $2^9 \bmod 13 = 5$;
  - $x = \log_3 7 \bmod 13 = ?$

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

Vô nghiệm (3 không phải là căn nguyên thủy của 13).

- Trong khi lũy thừa là bài toán dễ dàng, thì bài toán logarit rời rạc là bài toán khó.

TÓM LƯỢC CUỐI BÀI

- Các phép toán modulo với các số nguyên
- Các số nguyên tố
- Thuật toán Euclid và Euclid mở rộng
- Hàm Euler
- Định lý Ferma nhỏ và Euler
- Thuật toán bình phương và nhân liên tiếp
- Căn nguyên thủy và logarit rời rạc

CÂU HỎI TRẮC NGHIỆM CUỐI BÀI

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 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 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) mod 39 = (411 mod 39 . 800 mod 39)mod 39 = (21 . 20) mod 39 = 420 mod 39 = 1
B. 411^{-1} mod 39 = 800 mod 39 = 20
C. 13^{33} mod 8 = $(13 \bmod 8)^{33} \bmod 8 = 5^{33} \bmod 8 = (5^2 \bmod 8)^{16}$. 5 mod 8 = 5 mod 8 = 5
D. (3/7) mod 17 = 3.7^{-1}mod 17 = (3.(7^{-1}mod 17)) mod 17 = 3. 4 mod 17 = 12

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 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 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 13: a là căn nguyên thủy 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. $\{a^0 \bmod n, a^1 \bmod n, \ldots, a^{ø(n)-1} \bmod n\}$ 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 thủy của n
B. b nguyên tố cùng nhau với n
C. a là căn nguyên thủy 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 CUỐI BÀI

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, $7^{-1} \bmod 17 = 5$ chứ không phải 4
Câu 7: D, không thể lấy modulo cho số mũ
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 thủy thì lũy thừa của a sẽ tạo nên tập các số nguyên tố với n

THUẬT NGỮ TRONG BÀI

- 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 thủy 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.

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.
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 thủy 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 THƯỜNG GẶP

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
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 nhỏ 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.
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 thủy 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 thủy của n và số lấy logarit cũng là nguyên tố cùng nhau với n

CÂU HỎI TỰ LUẬN

Câu 1. Trên tập các số nào trong số các tập sau: N - tập số tự nhiên, **Z** - tập số nguyên, **P** - tập số hữu tỷ và **R** tập số thực; bạn có thể cộng, trừ, nhân, chia cho một số khác không, mà vẫn nhận được kết quả là các số trong tập đó?

Câu 2. Bạn hãy nói rõ thuật toán Euclid dùng để làm gì và được thực hiện như thế nào?

Câu 3. Số n có tính chất gì để trên tập các đại diện Z_n ta có thể thực hiện các phép toán: cộng, trừ, nhân và chia cho số khác 0? Tại sao?

Câu 4. Thế nào là số nguyên tố? Nêu cách phân tích một số ra tích lũy thừa của các thừa số nguyên tố.

Câu 5. Thế nào là hai số nguyên tố cùng nhau? Dùng thuật toán nào để kiểm tra hai số có nguyên tố cùng nhau không.

Câu 6. Bạn hãy nói rõ thuật toán Euclid mở rộng dùng để làm gì và được thực hiện như thế nào?

Câu 7. Nêu định nghĩa hàm số Euler.

Câu 8. Nêu cách tính hàm số Euler của một số nguyên dương? Nó tương đương với bài toán nào và có là bài toán khó không?

Câu 9. Phát biểu định lý Ferma nhỏ?

Câu 10. Phát biểu định lý Euler. Tại sao định lý Euler là mở rộng của định lý Ferma nhỏ

Câu 11. Bạn hãy nói rõ thuật toán tính lũy thừa hiệu quả dựa trên biểu diễn theo cơ số 2 của số mũ được thực hiện như thế nào?

Câu 12. Phát biểu định lý Phần dư Trung Hoa.

Câu 13. Nêu các ứng dụng của định lý phần dư Trung Hoa.

Câu 14. Phát biểu định nghĩa căn nguyên thủy của một số nguyên dương n. Nêu cách kiểm tra số nguyên dương a có là căn nguyên thủy của n hay không?.

Câu 15. Phát biểu định nghĩa logarit rời rạc cơ số a của b theo modulo n. Nêu cách tính nó.

Câu 16. Bài toán tính logarit rời rạc là bài toán ngược của bài toán nào? Nó có là bài toán khó không, vì sao?

BÀI TẬP TRẮC NGHIỆM

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.
2. Tập các số hữu tỷ không đóng với phép toán nào
   a) phép cộng, trừ;
   b) phép nhân;
   c) phép chia;
   d) phép khai căn bậc hai.
3. Hỏi có bao nhiêu phần dư dương khác nhau khi chia các số nguyên cho số nguyên dương n
   a) n +1 và đó là tập {0, 1, 2, ..., n-1, n}
   b) n - 1 và đó là tập {0, 1, 2, ..., n-2}
   c) n và đó là tập {1, 2, ..., n-1, n}
   d) n và đó là tập {0, 1, 2, ..., n-2, n-1}
4. Hai số có quan hệ đồng dư với nhau theo modulo n là hai số không có tính chất nào
   a) Có cùng phần dư dương khi chia cho n;
   b) Hiệu của chúng chia hết cho n;
   c) Tổng của chúng chia hết cho n;
   d) Có cùng đại diện theo modulo n.
5. Khi thực hiện các phép toán cộng và nhân 2 số theo modulo n, ta không thể thay mỗi số bằng
   a) số bất kỳ có quan hệ đồng dư với nó
   b) đại diện của nó theo modulo n
   c) số bất kỳ thuộc cùng lớp tương đương theo modulo n
   d) số có cùng trị tuyệt đối nhưng trái dấu với số đó
6. Số nguyên tố là số nguyên dương và
   a) Chỉ chia hết cho chính nó;
   b) Chỉ chia hết cho chính nó và 1;
   c) Chỉ chia hết cho 1.
   d) Có ước số khác 1 và chính nó.
7. Phép chia cho một số là phép nhân với số nghịch đảo. Nghịch đảo của một số a theo modulo n là số b có tích với số đã cho a theo modulo n bằng

a) 1 và luôn tồn tại;
b) 1 và tồn tại khi n là số nguyên tố;
c) 1 và tồn tại khi a và n nguyên tố cùng nhau;
d) 1 và tồn tại khi a là số nguyên tố.

8. 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
9. 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) $39 \equiv 25 \bmod 15$
10. Khẳng định nào sau đây không đúng:
   a) (411.800) mod 39 = (411 mod 39 . 800 mod 39)mod 39 = (21 . 20) mod 39 = 420 mod 39 = 1
   b) $410^{-1} \bmod 39 = 20^{-1} \bmod 39 = 2$
   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) $(3/7) \bmod 17 = 3.7^{-1} \bmod 17 = (3.(7^{-1} \bmod 17)) \bmod 17 = 3.5 \bmod 17 = 15$
11. Khẳng định nào sau đây không đúng:
   a) $3^{10} \bmod 16 = 9$
   b) $15^{-1} \bmod 52 = 7$
   c) $25^{-1} \bmod 274 = 10$
   d) (51.53) mod 45 = 3
12. Tìm ra kết luận đúng trong các khẳng định sau về hàm Euler
   a) $\Phi(9) = 7, \quad \Phi(33) = 21$
   b) $\Phi(9) = 6, \quad \Phi(33) = 22$
   c) $\Phi(9) = 7, \quad \Phi(33) = 19$
   d) $\Phi(9) = 6, \quad \Phi(33) = 20$
13. Áp dụng định lý Ferma và định lý Euler xem khẳng định nào sai:
   a) $6^{16} \bmod 17 = 1$
   b) $7^{13} \bmod 13 = 7$
   c) $4^{11} \bmod 15 = 4$
   d) $6^{10} \bmod 15 = 1$
14. Áp dụng định lý phần dư Trung Hoa: cho $X \bmod 15 = 1$ và $X \bmod 11 = 3$, khi đó đáp án đúng là
   a) $X = 89 \bmod 55$
   b) $X = 90 \bmod 55$

c) X = 91 mod 55
d) X = 92 mod 55

15. Áp dụng định lý phần dư Trung Hoa xem khẳng định nào đúng:
a) 67^2 mod 11.13 = 55 mod 143
b) 67^2 mod 11.13 = 56 mod 143
c) 67^2 mod 11.13 = 57 mod 143
d) 67^2 mod 11.13 = 58 mod 143
16. Tìm ra kết luận đúng trong các khẳng định sau
a) 2 là căn nguyên thủy của 6
b) 2 là căn nguyên thủy của 4
c) 2 là căn nguyên thủy của 5
d) 3 là căn nguyên thủy của 6
17. Tìm kết luận đúng trong các khẳng định sau
a) Log_2 5 mod 9 = 2
b) Log_2 6 mod 9 = 3
c) Log_2 7 mod 9 = 4
d) Log_2 4 mod 9 = 5

BÀI TẬP ÔN TẬP

1. Tìm phần dư dương khi chia:
   a. 51 cho 15
   b. -51 cho 15
2. Tìm đại diện của các số 215 và -157 theo mod 29
3. Chia tập các số từ -26 đến 25 thành các lớp tương đương theo mod 13, nêu các đại diện của chúng?
4. Biểu thức nào đúng:
   a. 101 ≡ 36 mod 13?
   b. (-101) ≡ (-36) mod 13?
   c. 165 ≡ 34 mod 65?
   d. (-165) ≡ 30 mod 65?
5. Lập bảng nhân theo modulo 11, nêu cặp các số nghịch đảo nhau trong bảng.
6. Thay các số bằng các số tương đương đồng dư để tính các biểu thức sau
   a. (74 -215) mod 9
   b. (244 . 315) mod 250
   c. (144.315 – 265.657) mod 51
7. Tìm các số nghịch đảo sau trực tiếp bằng định nghĩa:
   a. 6^{-1} mod 11 = ?
   b. 5^{-1} mod 11 = ?
   c. 6^{-1} mod 13 = ?

d. $12^{-1} \bmod 13 = ?$; $(n-1)^{-1} \bmod n = ?$

e. $13^{-1} \bmod 15 = ?$

f. $21^{-1} \bmod 25 = ?$

8. Tìm ước chung GCD(2110, 1945) theo thuật toán Euclide.

9. Dùng thuật toán Euclide mở rộng để tìm nghịch đảo $845^{-1} \bmod 2011 = ?$

10. Giải hệ phương trình Modulo sau: cho $X \bmod 25 = 5$ và $X \bmod 23 = 15$. Tìm X

11. Dùng Định lý Ferma tính

a. $5^{12} (\text{mod } 13) = ?$

b. $8^{13} (\text{mod } 13) = ?$

c. $10^{100} (\text{mod } 17) = ?$

d. $15^{125} (\text{mod } 19) = ?$

12. Tính giá trị hàm Euler:

a. $\Phi(23) = ?$

b. $\Phi(55) = ?$

c. $\Phi(180) = ?$

d. $\Phi(200) = ?$

e. $\Phi(900) = ?$

f. $\Phi(6300) = ?$

13. Dùng Định lý Euler tính giá trị các biểu thức sau:

a. $4^8 \bmod 15 = ?$

b. $11^9 \bmod 20 = ?$

c. $12^{402} \bmod 25 = ?$

d. $135^{162} \bmod 64 = ?$

e. $335^{453} \bmod 23 = ?$

f. $(3/7)^8 \bmod 10 = ?$

14. Sử dụng thuật toán lũy thừa dựa trên biểu diễn nhị phân của số mũ n, tính $11^{23} \bmod 187$.

15. Tính toán các lũy thừa sau dựa trên phép lặp bình phương và nhân với cơ số $11^{23} \bmod 187$

16. Kiểm tra các khẳng định sau:

a. a = 2 có phải là căn nguyên thủy của 7 không? .

b. a = 2 có phải là căn nguyên thủy của 11 không?

c. a = 3 có phải là căn nguyên thủy của 11 không?

d. Trong các cặp số sau số sau có là căn nguyên thủy của số trước không:

(3, 2); (5, 2); (7, 3), (11, 2); (13, 6); (17, 10); (19, 10); (23, 10)

17. Tính logarit rời rạc sau:

a. $\log_2 5 \bmod 11 = ?$

b. $\log_2 5 \bmod 13 = ?$

c. $\log_3 7 \bmod 13 = ?$

d. $\log_2 5 \bmod 9 = ?$

e. $\log_2 6 \bmod 9 = ?$

f. $\log_2 7 \bmod 9 = ?$

g. $\log_2 4 \bmod 9 = ?$