**MODULO**

1. TÍNH LŨY THỪA MODULO ***b ≡ mod n*** BẰNG CÁCH HẠ BẬC LŨY THỪA

Input: a = 277; m = 6863; n = 6863

Tìm Output: b =

**Giải:**

Viết biểu thức nhị phân của 6863: 1101011001111

Cách 1: Sử dụng phép lặp bình phương với nhân cơ số

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| m |  |  |  |  |  |  |  |  |  |
| 6863 | ≡ | 3431 \* 2 +1 |  | 277^6863 | ≡ | (277^3431)^2 \* 277 | mod 6863 | ≡ | **277** |
| 3431 | ≡ | 1715 \* 2 +1 |  | 277^3431 | ≡ | (277^1715) ^2 \* 277 | mod 6863 | ≡ | 1 |
| 1715 | ≡ | 857 \* 2 +1 |  | 277^1715 | ≡ | (277^857) ^2 \* 277 | mod 6863 | ≡ | 596 |
| 857 | ≡ | 428 \* 2 +1 |  | 277^857 | ≡ | (277^428) ^2 \* 277 | mod 6863 | ≡ | 2518 |
| 428 | ≡ | 214 \* 2 |  | 277^428 | ≡ | (277^214) ^2 | mod 6863 | ≡ | 803 |
| 214 | ≡ | 107 \* 2 |  | 277^214 | ≡ | (277^107) ^2 | mod 6863 | ≡ | 4961 |
| 107 | ≡ | 53 \* 2 + 1 |  | 277^107 | ≡ | (277^53) ^2 \* 277 | mod 6863 | ≡ | 5575 |
| 53 | ≡ | 26 \* 2 + 1 |  | 277^53 | ≡ | (277^26) ^2 \* 277 | mod 6863 | ≡ | 2874 |
| 26 | ≡ | 13 \* 2 + 1 |  | 277^26 | ≡ | (277^13) ^2 \* 277 | mod 6863 | ≡ | 2866 |
| 13 | ≡ | 6 \* 2 + 1 |  | 277^13 | ≡ | (277^6) ^2 \* 277 | mod 6863 | ≡ | 5864 |
| 6 | ≡ | 3 \* 2 |  | 277^6 | ≡ | (277^3) ^2 | mod 6863 | ≡ | 1340 |
| 3 | ≡ | 1 \* 2 + 1 |  | 277^3 | ≡ | 277 ^2\*277 | mod 6863 | ≡ | 6085 |
| 1 | ≡ | 1 |  | 277 | ≡ | 277 | mod 6863 | ≡ | 277 |

Cách 2: Biểu diễn nhị phân của số mũ m

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6863(2) | m0 |  | 1 |  |  |  |  |  |  |  |  |  |
| 1 | m1 |  |  |  | = | 1 | .277 | = |  |  | 277 | mod 6863 |
| 1 | m2 |  |  |  | = | 76729 | .277 | = | 21253933 |  | 6085 | mod 6863 |
| 0 | m3 |  |  |  | = | 3702722 | .1 | = | 37027225 |  | 1340 | mod 6863 |
| 1 | m4 |  |  |  | = | 1795600 | .277 | = | 497381200 |  | 5864 | mod 6863 |
| 0 | m5 |  |  |  | = | 34386496 | .1 | = | 34386496 |  | 2866 | mod 6863 |
| 1 | m6 |  |  |  | = | 8213956 | .277 | = | 2275265812 |  | 2874 | mod 6863 |
| 1 | m7 |  |  |  | = | 8259876 | .277 | = | 2287985652 |  | 5575 | mod 6863 |
| 0 | m8 |  |  |  | = | 31080625 | .1 | = | 31080625 |  | 4961 | mod 6863 |
| 0 | m9 |  |  |  | = | 24611521 | .1 | = | 24611521 |  | 803 | mod 6863 |
| 1 | m10 |  |  |  | = | 644809 | .277 | = | 178612093 |  | 2518 | mod 6863 |
| 1 | m11 |  |  |  | = | 6340324 | .277 | = | 1756269748 |  | 596 | mod 6863 |
| 1 | m12 |  |  |  | = | 355216 | .277 | = | 98394832 |  | 1 | mod 6863 |
| 1 | m13 |  |  |  | = | 1 | .277 | = |  |  | **277** | **mod 6863** |

* b 277 mod 6863 277

Cách 3: Phép cộng các bình phương modulo (Cách dễ hiểu nhất)

Viết biểu thức nhị phân của (6863)2: 1101011001111 (6863 cơ số 2- số nhị phân - binary)

Ta có: (6863)10 = (6863 cơ số 10 - số thập phân – decimal)

= + + + + + + + +

= 4096 + 2048 + 512 + 128 + 64 + 8 + 4 + 2 + 1

* (. . . . . . . .277)mod6863(\*)

Từ quy tắc nhân trong số học modulo, suy ra (\*) như sau:

[( mod 6863) \* ( mod 6863) \* ( mod 6863)

\* ( mod 6863) \* ( mod 6863) \* ( mod 6863)

\* ( mod 6863) \* ( mod 6863) \* (277 mod 6863)] mod 6863 (\*\*)

Tạo bảng sau:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | = | 277 |  |  |  |  |
|  |  | mod 6863 | = | 1236 |  |  |
|  |  | mod 6863 |  | mod 6863 | = | 4110 |
|  |  | mod 6863 |  | mod 6863 | = | 2257 |
|  |  | mod 6863 |  | mod 6863 | = | 1703 |
|  |  | mod 6863 |  | mod 6863 | = | 4023 |
|  |  | mod 6863 |  | mod 6863 | = | 1575 |
|  |  | mod 6863 |  | mod 6863 | = | 3082 |
|  |  | mod 6863 |  | mod 6863 | = | 332 |
|  |  | mod 6863 |  | mod 6863 | = | 416 |
|  |  | mod 6863 |  | mod 6863 | = | 1481 |
|  |  | mod 6863 |  | mod 6863 | = | 4064 |
|  |  | mod 6863 |  | mod 6863 | = | 3718 |

Từ (\*\*)

=> (3718 \* 4064 \* 416 \* 3082 \* 1575 \* 2257 \* 4110 \* 1236 \* 277) mod 6863

= 277 mod 6863 = 277

1. TÌM NGHỊCH ĐẢO 𝒙 ≡ 𝒎𝒐𝒅 𝒏 THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞ RỘNG

Input: a ≡ 3331; n ≡ 6551

Tìm Output: x ≡

**Giải:**

( x | 3331x ≡ 1 (mod 6551) ) => Tìm biểu thức 3331x + 6551y = 1

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Thuật toán Euclidean tìm USCLN | | | |  | Mở rộng để tìm x | | | |
| 1) | 6551 | = | 1\*3331 + 3220 |  | 1) | => |  | 3220 = 1\*6551 - 1\*3331 |
| 2) | 3331 | = | 1\*3220 + 111 |  | 2) | 3331 | = | 1\*(6551 – 1\*3331) + 111 |
| 3) | 3220 | = | 29\*111 + 1 |  | => | 111 | = | 2\*3331 – 1\*6551 |
|  |  |  |  |  | 3) | => | = | 1 = 3220 – 29\*111 |
|  |  |  |  |  | => | 1 | = | -59\*3220 + 30\*3220 |

* x = -59 mod 6551 = 6492

Cách rút gọn:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 6551 | 0 | 1 | 3331 |
| 1 | 0 | 1 | 3331 | 1 | -1 | 3220 |
| 1 | 1 | -1 | 3320 | -1 | 2 | 111 |
| 29 | -1 | 2 | 111 | 30 | -59 | 1 |

A3 div B3 A1-QB1 A2-QB2 A3-QB3

(Màu xanh, xám, tím là hạ B1, B2, B3 xuống A1, A2, A3  
Màu vàng là kết quả của x (B2)  
Màu đỏ là khi kết quả (B3) bằng 1 thì phép tìm x dừng, x sẽ là kết quả B2 ngay trước điểm dừng)

1. SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO 𝒃 = 𝒎𝒐𝒅 𝒏

Input: a = 241; m = 850; n = 6737

Tìm Output: b =

**Giải:**

Vì, n (n >1) là số nguyên tố và a (a > 0) là số nguyên không chia hết cho n nên:

Ta có 1 mod 6737 (Định lý nhỏ Fermat)

= mod 6737

= \* mod 6737

= \* mod 6737

= mod 6737

Ta có:

mod 6737 = mod 6737 = **3330**

mod 6737 = \*241 mod 6737 = 4772

mod 6737 = 4185

* b = 3330

1. TÍNH GIÁ TRỊ HÀM EULER (n).

Input: n = 2856

Tìm Output: (n) =

Vì n không phải là số nguyên tố, ta áp dụng công thức sau để tính giá trị hàm Euler:

=

= ( – ) \* 2 \* 6 \* 16 ( φ(n)=m∏i=1(pi−1)pki−1i )

= 768

(Cách để biết các số nguyên tố là cứ chia hết cho 2, 3, 5, 7, ... đến khi nào phép toàn bằng 1 thì thôi)

φ(n)=nm∏i=1(1−1pi)

Ví dụ:

= 2856 \* (1−1/2) \* (1−1/3) \* (1−1/7) \* (1−1/17)

= 2856 \* (1/2) \* (2/3)\* (6/7) (16/17)

= (2856 \* 1 \* 2 \* 6 \* 16 )/(2 \* 3 \* 7 \* 17)

= 768

1. SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO 𝒃 = 𝒎𝒐𝒅 𝒏

Input: a = 26; m = 3369; n = 363

Tìm Output: b =?

= \* = 2 \* (121-11) = 220

Định lý Euler: mod n = mod n = mod n

mod 363 = mod 363

= mod 363

= mod 363

= (2)

Hạ bậc lũy thừa:

26^2 mod 363 = 313 26^8 mod 363 = 229

26^3 mod 363 = 152 26^16 mod 363 = 169

26^4 mod 363 = 322 26^32 mod 363 = 247

26^5 mod 363 = 23 26^64 mod 363 = 25

(2) ⬄ = ( mod 363)\*(mod 363) mod 363

= 23\*25 mod 363 = 212

=> b = 212

1. SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo 𝒃 = 𝒎𝒐𝒅 𝒏

Input: a = 191; k = 58; n = 79663

Tìm Output: b =?

A = , M = 79663 = 29 \* 41 \* 67, m1=29, m2=41, m3=67

Suy ra M1=79663/29=2747, M2=1943, M3=1189 (Mi=M/mi)

=> =>

Ta có (1) ⬄ x = 2747^(-1)mod29 => 2747x mod 29 = 1  
Nên ta có biểu thức tiếp theo: (2747x mod 29) + (29y mod 29)= 1 => 2747x +29y = 1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 29 | 0 | 1 | 2747 |
| 0 | 0 | 1 | 2747 | 1 | 0 | 29 |
| 94 | 1 | 0 | 29 | -94 | 1 | 21 |
| 1 | -94 | 1 | 21 | 95 | -1 | 8 |
| 2 | 95 | -1 | 8 | -284 | 3 | 5 |
| 1 | -284 | 3 | 5 | 379 | -4 | 3 |
| 1 | 379 | -4 | 3 | -663 | -7 | 2 |
| 1 | -663 | 7 | 2 | 1042 | -11 | 1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 41 | 0 | 1 | 1943 |
| 0 | 0 | 1 | 1943 | 1 | 0 | 16 |
| 47 | 1 | 0 | 41 | -47 | 1 | 21 |
| 2 | -47 | 1 | 16 | 95 | -2 | 9 |
| 1 | 95 | -2 | 9 | -142 | 3 | 7 |
| 1 | -142 | 3 | 7 | 237 | -5 | 2 |
| 2 | 237 | -5 | 2 | -616 | 13 | 3 |
| 0 | -616 | 13 | 3 | 237 | -5 | 2 |
| 1 | 237 | -5 | 2 | -853 | 18 | 1 |

Làm tương tự với phép tính còn lại

**;**

Ta có công thức tính toán theo modulo số lớn của Định lý phần dư Trung Hoa như sau:

b = () mod M ⬄ b = (2747\*(-11)\*28 + 1943\*8\*32 + 1189\*(-4)\*16) mod 79663 = 37670

1. SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ GIẢI HỆ PHƯƠNG TRÌNH MODULO.

Input: m1 = 19; m2 = 11; m3 = 13; a1 = 8; a2 = 2; a3 = 8;

Tìm Output: x =?

Ta có:

=> M = 19\*11\*13 = 2717

=>

x = (286\*8 + 2223\*2 + 209\*8) mod 2717 = 255

1. KIỂM TRA SỐ NGUYÊN A CÓ LÀ MỘT CĂN NGUYÊN THỦY CỦA SỐ NGUYÊN N?

Input: a = 3; n = 353

Tìm Output: a có là căn nguyên thủy của n không?

a là căn nguyên thủy của n ⬄ 1 (mod n) với gcd(a,n)=1

mà a = 3 và n = 353 cùng là 2 số nguyên tố cùng nhau => gcd(a,n)=1

Ta có:

3 mod 353 = 3 mod 353 = 23 mod 353 = 140

mod 353 = 9 mod 353 = 69 mod 353 = 185

mod 353 = 81 mod 353 = 207 mod 353 = 337

mod 353 = 243 mod 353 = 136 mod 353 = 256

mod 353 = mod 353 = (256\*185\*140) mod 353 = 1

mod 353 = (27\*268\*175) mod 353 = 89 ////// check lại xem có trùng 1 (mod 353) không

Φ(353) là số nguyên dương nhỏ nhất thoả mãn ≡ 1 (mod353) ⇒ 3 là căn nguyên thuỷ của 353

1. TÌM LOGARITHM RỜI RẠC CỦA SỐ b VỚI CƠ SỐ 𝒂 (𝒎𝒐𝒅 𝒏), 𝒌 **=** *(*𝒎𝒐𝒅 𝒏).

Input: a = 2; b = 7; n = 11

Tìm Output: k =

Để tìm logarithm rời rạc của số b với cơ số a (mod n), nghĩa là tìm k sao cho:

≡ 𝑏 (mod 𝑛) với 𝑎 = 2, 𝑏 = 7 và 𝑛 = 11

Chúng ta cần tìm k thỏa mãn:

≡ 7 (mod 11)

Một cách để tìm 𝑘 là thử từng giá trị của 𝑘 từ 0 trở đi và tính

mod 11 cho đến khi tìm thấy kết quả bằng 7.

Tính toán từng bước:

1. k = 0

≡ 1 (mod 11)

1. k = 1

≡ 2 (mod 11)

1. k = 2

≡ 4 (mod 11)

1. k = 3

≡ 8 (mod 11)

1. k = 4

≡ 5 (mod 11)

1. k = 5

≡ 10 (mod 11)

1. k = 6

≡ 9 (mod 11)

1. k = 7

≡ 7 (mod 11)

Như vậy,

k = 7 là giá trị chúng ta cần tìm. Kết quả là:

k = 7

1. TÍNH CÁC BIỂU THỨC MODULO CƠ BẢN

A𝟏 = (𝒂^𝒙+𝒃^𝒚) 𝒎𝒐𝒅 𝒏

A𝟐 = (𝒂^𝒙−𝒃^𝒚) 𝒎𝒐𝒅 𝒏

A𝟑 = (𝒂^𝒙∗𝒃^𝒚) 𝒎𝒐𝒅 𝒏

A𝟒 = (𝒃^𝒚)^(−𝟏) 𝒎𝒐𝒅 𝒏

A𝟓 = (𝒂^𝒙/𝒃^𝒚) 𝒎𝒐𝒅 𝒏

Input: a = 53; b = 31; x = 336; y = 585; n = 293

Tìm Output: A1 = ; A2 = ; A3 = ; A4 = ; A5 = ?

mod n = mod 293(1); mod n = mod 293(2)

Từ (1) ta áp dụng định lý Euler ⬄ mod 293 = mod 293

= mod 293

Ta có: 53 mod 293 = 53 53^16 mod 293 = 115 53^256 mod 293 = 258

53^2 mod 293 = 172 53^32 mod 293 = 40

53^4 mod 293 = 284 53^64 mod 293 = 135

53^8 mod 293 = 81 53^128 mod 293 = 59

* mod 293 = (258\*135\*115) mod 293 = 140

Từ (2) ta có: mod 293 = mod 293 = (53\*1) mod 293 = 53 (áp dụng định lý fermat nhỏ)

Tính các biểu thức:

A1 = ( + ) mod n = 140 mod 293 + 53 mod 293 = 193

A2 = ( - ) mod n = 140 – 53 = 87

A3 = ( \* ) mod n = (140\*53) mod 293 = 95

A4 = ( / ) mod n = (140/53) mod 293 = 140/53