I. Hạ bậc lũy thừa Modulo

a = 419; m = 6217; n= 6217

II. Euclid mở rộng

Anmod m

Q = A2/B2

A1 = B1

A2 = B2

B2 = A2 mod B2

B1 = A1 – B1\* Q(mới)

Khởi tạo thì

Q = -

A1 = 0

B1 = 1

Làm đến khi B2 ra bằng 1 thì dừng nếu ra âm thì + m

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Q | A1 | A2 | B1 | B2 |
| - | 0 | n | 1 | a |

III. Hạ bậc lũy thừa theo định lý Fermat

ap mod p

* Nếu p là số nguyên tố và a là số nguyên tố không chia hết cho p, thì ap-1 đồng dư với 1 mod p => ap mod p = 1
* Nếu a là tùy ý, ta có ap đồng dư với a mod p

Ví dụ 7222 mod 11

Ta thấy 11 là số nguyên tố và 7 là số nguyên không chia hết cho a nên:

710mod 11 = 1

Lại có k = 222 phân tích theo 10 . k ta được

710 \* 22 + 2 mod 11

Mà 710mod 11 = 1 nên

(710 mod 11)22 72 mod 11 = 122 \* 49 mod 11 = 49 mod 11 = 5

IV. Định lý euler (Đây là một định lý mở rộng của Fermat)

1, Định nghĩa hàm euler

Hàm euler đối với số nguyên n được kí hiệu ϕ(n)

Là số lượng nguyên tố nhỏ hơn n và nguyên tố cùng nhau với n

Vd: ϕ(6) có các số 1,2,3,4,5,6 nhỏ hơn n và chỉ có 1, 5 là nguyên tố cùng nhau với 6 nên là ϕ(6) = 2

2, Một số định lý

Nếu n là một số nguyên tố thì **ϕ(n) = n-1**

Nếu p,q là 2 số nguyên tố cùng nhau thì: **ϕ(p\*q) = ϕ(p) \* ϕ(q)**

Nếu n là số nguyên tố và m là số nguyên dương thì ϕ(nm) = nm – nm-1

Vd : tính giá trị 23,55,180

ϕ (23) = 22 (vì 23 là số nguyên tố)

ϕ (55) = ϕ (11 \* 5) = ϕ(11) \* ϕ(5) (vì 11 và 5 đều là nguyên tố cùng nhau)

= 10 \* 4 = 40 (vì 11 là số nguyên tố nên $(11) = 10 và ϕ (5) cũng thế và bằng 4)

\*mẹo máy tính(bấm phân tích số nguyên tố bằng cách nhân số đó rồi nhấn shift fact)

Bấm máy tính 180 ra thành : 180 = 22\*32\*5

ϕ(180) = ϕ(22\*32\*5) = ϕ(22\*32)\*4 = (22 - 2)\*( 32 - 3)\*4 = 48 (áp dụng cả 2 công thức 2 và 3)

3, Sử dụng euler để tính số dư

Nếu ak mod n (nếu a với n là số nguyên tố cùng nhau thì aϕ(n) mod n = 1)

Vd: 135162 mod 64

Ta thấy 135 > 64 ta có 135 mod 64 = 7

* 7162 mod 64

Ta có 7 và 64 là nguyên tố cùng nhau GCD(7,64) = 1 nên là

ϕ(64) = 32 => 732 mod 64 = 1 (định lí euler)

B = 732\*5+2 mod 64 = 72 mod 64 = 49 mod 64 = 49

4, Phần dư trung hoa

SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo 𝒃 = 𝒂**k** 𝒎𝒐𝒅 𝒏 Input: a = 227; k = 80; n = 60421 Tìm Output: b =

VD 10159 mod 323

Đặt 10159 = A và M = 323

B1 : phân tích n ra thành thừa số nguyên tố (fact) để tìm m1,m2,…

M = 323 = 17\*19

* m1 = 17, m2 = 19

B2 : Tính theo các modulo thành phần tìm a1,a2,…

a1 = 10159 mod 17 = 16

a1 = 10159 mod 19 = 5

B3: Tính kết quả A mod M

Ta có

M1 = M/m1

M2 = M/m2

M1 = 19, M2 = 17

M1-1 mod m1=19-1 mod 17 = 9

M2-1 mod m2=17-1 mod 19 = 9

Áp vào công thức

Ci = Mi \* (Mi-1 mod mi)

C1 = 19\* 9 = 171

C2 = 17\*9 = 153

A = (a1c1+a2c2) mod M = (16\*171+5\*153) mod 323 = 3501 mod 323 = 271

5, Sử lý số dư trung hoa để giải hệ phương trình

𝒙 𝒎𝒐𝒅 𝒎𝟏 = 𝒂𝟏

𝒙 𝒎𝒐𝒅 𝒎𝟐 = 𝒂𝟐

𝒙 𝒎𝒐𝒅 𝒎𝟑 = 𝒂𝟑

Input: m1 = 17; m2 = 19; m3 = 11; a1 = 5; a2 = 16; a3 = 3; Tìm Output: x =

Cthuc tim x = (a1M1y1+a2M2y2 + … ) trong đó a đã biết

M = m1\*m2\*m3\*…

M1= M/m1 …

Y1 = M1-1 mod m1

M = m1\*m2\*m3 = 17\*19\*11 = 3553

M1 = M/m1 = 3553/17 = 209

M2 = M/m2 = 3553/19 = 186

M3 = M/m3 = 3553/11 = 323

Y1 = M1-1 mod m1 = 209-1 mod 17

Y2 = M2-1 mod m2 = 186-1 mod 19

Y3 = M3-1 mod m3 = 323-1 mod 11