|  |  |
| --- | --- |
| i | 3^(2^i) |
| 0 | 3^1 =3 |
| 1 | 3^2 = 9 |
|  | 3^4 = 81 |
|  | 3^8 = 561 |
|  | 3^16 = 721 |
|  | 3^32 =(721^2)= 841 |
|  | 3^64 = 281 |
|  | 3^128 = 961 |
|  |  |
|  |  |
|  |  |

3 mũ 218 mod 1000

3^218 = 721\* 3^2 = 489

a^b mod n :

f(a,b, n) {

if b == 0 then return 1

if b == 1 return a

r = f(a, b/2, n)

if b %2 != 0 return r\*r\*a

else return r\*r

}

3 mũ 218 mod 1000

|  |  |
| --- | --- |
| b | Res |
| 218 | 683^2 = 489 |
| 109 | 169^2\*3 = 683 |
| 54 | 987^2 = 169 |
| 27 | 323^2 \*3 = 987 |
| 13 | 729^2 \* 3 = 323 |
| 6 | 27^2 = 729 |
| 3 | 3\*3\*3=27 |
| 1 | 3 |
| 0 | 1 |

977^280001 mod 11413

Lưu ý: với mọi a thuộc Z\*(N) thì a^Phi(N) = 1 mod N

11413 = 101\*113 (đều là snt)

Phi(N) = |Z\*(N)| = 100\*112 = 11200

280001 = 11200\*… + 1

977^280001 = 977^(11200\*…) \* 977^1 mod N = 977

N = q^2

Phi(N) = q(q-1)

Ví dụ N = 169

Phi (169) = 13\*12 156

N = p \* q^2

Phi(N) = (p-1)(q-1)q

N = a\*b\*c\*…\*z

Phi(N) = N\*(1-1/a)\*(1-1/b)\*…(1-1/z)

Ảnh có chứa văn bản, Phông chữ, hàng, màu trắng

Mô tả được tạo tự động

X^4 + x^3 + x +1 = x(x^3 + x + 1) + x^3 - x^2 + 1

= x^3 + x^2 +1

= 1(x^3+x+1) + x^2 - x

= x^2 + x

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình, số

Mô tả được tạo tự động



Lần 1:

m # 0 -> (r, a, b)

Lần 2

M = 0 -> (r, b, b)

Ảnh có chứa văn bản, Phông chữ, màu trắng

Mô tả được tạo tự động

1. Cần tìm x sao cho 2^x = 13 mod 23

Z\*23 = {1…22}

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| I | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 2^i | 2 | 4 | 8 | 16 | 9 | 18 | 13 | 3 | 6 | 12 |
| i | 11 |  |  |  |  |  |  |  |  | 20 |
| 2^i | 1 | 2 | 4 | 8 |  |  |  |  |  |  |
| i |  |  |  |  |  |  |  |  |  |  |
| 2^i |  |  |  |  |  |  |  |  |  |  |