\* R: pow(x, n) = y

- x = sqrt(y)

- m = logxy

\* p nguyên tố: Zp trường hữu hạn

Lũy thừa: pow(x, n) mod p

- hạ bậc

- tính nhanh

- fermat

- Euler

- Định lý số dư trung hoa

Căn nguyên thủy logalit rời rạc

X = b-2 mod n ⬄ x\*b mod n = x

Tính 2-1 mod 7 = x ⬄ (x\*2)/4 mod 7 = 1

x = […,-3,4,11,18,…]

x thuộc [4] mod 7

56-1 mod 283 = ?

283 = 56 \* 5 + 3

56 = 3 \* 18 + 2

3 = 2 \* 1 + 1

2 = 2 \* 1 + 0

Gcd(56, 283) = 1

=>

3 = 283 – 56 \* 5

2 = 56 – 3 \* 18

1 = 3 – 2 \* 1

=> 1 = 3 – (56 – 3 \* 18) \* 1

= 3 \* 19 – 56

= (283 – 56 \* 5) \* 19 – 56

= 283\*19 – 56 \* 96

56-1 mod 283 = -96 mod 283 = (-96 + 283) = 187

R = 56x + 283\*y

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| I | R | q | X | Y |
| -1  0 | 283  56 |  | 0  1 | 1  0 |
| 1 | 3 | 5 | -5 | 1 |
| 2 | 2 | 18 | 91 | -18 |
| 3 | 1 | 1 | -96 | -9 |
| 4 | 0 |  |  |  |

1 = (56 \* (-96) + 283\*19) mod 283

1 = 56 \* (-96) mod 283

=> 56-1 mod 283 = -96 mod 283= 187

Bài tập

2) – 3 / 7 mod 283

1) 3 / 7 mod 283 = ?

⬄ 3 \* 7 -1 mod 283

R = 7 \* x + 283 \* y

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| I | R | q | X | Y |
| -1  0 | 283  7 |  | 0  1 | 1  0 |
| 1 | 3 | 40 | -40 | 40 |
| 2 | 1 | 2 | 61 | -60 |
| 3 | 0 | 3 |  |  |

1 = 7 \* (61) + 283\*(-60) mod 283

1 = 7 \* 61 mod 283

=> 7 -1 mod 283 = 61 mod 283 = 61

=> 3 \* 7-1 mod 283 = 183

3) 328 mod 17

328 mod 17 = (314)2 mod 17 = 4

314 mod 17 = (37)2 mod 17 = 2

37 mod 17 = ((33)2 \* 3) mod 17 = 11

33 mod 17 = ((3)2 \* 3) mod 17 = 10