Bài 1: thuật toán euclid (tính nghịch đảo)

* A1 =0 , B1 =1

Q = A2 div B2 ( chia lấy phần nguyên)

A1 = B1 (cũ)

A2 = B2 (cũ)

B1 = A1(cũ) – Q \* B1(cũ)

B2 = A2(cũ) - Q \* B2(cũ)

84-1 mod 197 = ?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Q | A1 | A2 | B1 | B2 |
|  | 0 | 197 | 1 | 84 |
| 2 | 1 | 84 | -2 | 29 |
| 2 | -2 | 29 | 5 | 26 |
| 1 | 5 | 26 | -7 | 3 |
| 8 | -7 | 3 | 61 | 2 |
| 1 | 61 | 2 | -68 | 1 |

B1 = -68 (nhưng ko dc là số âm 0=> 197 -🡪 -68 + 197 = 129)

84-1 mod 197 = 129

Bài 2: định lí ferma

254 mod 11 =( (211-1 )5 . 24) mod 11 = ((211-1 mod 11)5 mod 11 x 24 mod 11) mod 11 = (1 x 5)mod 11 = 5

Bài 3 : định lí euler

12402 mod 25 = ?

Bài 4: Ứng dụng của định lý phần dư trung hoa – Tính toán trên modulo lớn

1745 mod 220 = ?

220 = 4 x 5 x11

A = 1745 ,

Khi đó M1 = 220/4 =55, M2 = 220/5= 44, M3 = 220/11= 20

C1 = 55 x (55-1 mod 4) = 55 x (3-1 mod 4 ) = 55 \* 3 = 165

C2 = 44 x (44-1 mod 5) = 44 x (4-1 mod 5) = 44 \* 4 = 176

C3= 20 x (20-1 mod 11) = 20 x (9-1 mod 11) = 20 \* 5 = 100

a1 = A mod m1 = 1745 mod 4 = ( 1 mod 4 )45 mod4 = 1

a2 = A mod m2 = 1745 mod 5 = 245 mod 5= (24)11 \* 2mod 5 = 2

a3 = 1745 mod 11 = 645 mod 11= (610)4 \* 65 mod 11 = 65 mod 11 = (62)2 \* 6 mod 11 = 9 \*6 mod 11 = 10

1745 mod 220 = (1 \* 165 + 2 \*176 + 10 \*100) mod 220 = 1517 mod 220 = 197

Căn nguyên thủy

a có là căn nguyên thủy của n khi

1. a(n) mod n = 1 (a mũ

am mod n != 1

VD: 10 có là CNT của 19 ko

Bài lm

1. 10 = 2.5

19 =19

* 2 số nguyên tố cùng nhau

Xét 103 mod 19 = 12

102 mod 19 = 5

101 mod 19 = 10

106 mod 19 = (102)3 mod 19 = 53 mod 19 = 11

109 mod 19 = (103)3 mod 19 = 123 mod 19 = 18

Từ (1),(2) => 10 là CNT của 19

VD2 : 13 có là CNT của 19 ko

Bài làm

1. Có GCD(13,19) = 1 =>
2. US(

m =1 131 mod 19 = 13

m =2 132 mod 19 = 17

m= 3 133 mod 19 = (132.131) mod 19 = 132 mod 19.131 mod 19 = 13.17 mod 19 = 12

m=6 136 mod 19 = (133)2 mod 19 = 122 mod 19 =11

m= 9 139 mod 19 =(133)3 mod 19 = 123 mod 19=11

* 13 là CNT của 19

Logarit rời rạc

VD : Tìm x = dlog3 12 (mod 19)

VD2; tìm x = dlog3 5 (mod 13)

* 3x mod 13 = 5

Xét 0,1,2,3,4,....,12