mod 25

Ta có :

BT1.

* 215 mod 29 = 203mod 29+12mod 29 = 0 + 12 mod 29 = 12
* (-157) mod 29=29-157mod 29 = 29-12=17

BT2

1.

* 1. 101 mod 13 = 10
  2. 36 mod 13 = 10
  3. True

2.

a. (-101) mod 13 = 13 - 101 mod 13 = 13 – 10 = 3

b.(-36) mod 13 = 13 – 36 mod 13 = 13 – 10 = 3

c. True

3.

a. 165 mod 65 = 35

b. 34 mod 65=34

c.False

4.

a. (-165) mod 65 = 65 – 165 mod 65 = 30

b. 30 mod 65 = 30

c. True

BT3

* (74 - 215) mod 9=(74 mod 9 -215 mod 9 ) mod= (2- 8) mod 9 = (9-6) mod 9=3
* (244.315) mod 250 = ([244 mod 250 ].[315 mod 250]) mod 250 = ((-6).65)mod 250 = (-390) mod 250 = 250 – 140 =110
* (144.315 – 265.657 ) mod 51 =((144.315) mod 51 –( 265.657 ) mod 51) mod 51)=

(((144 mod 51 ) (315 mod 51) mod 51) -((256 mod 51 ) (657 mod ) mod 51)) =

((-2).9 mod 51 – (1.(-6) mod 51)) mod 51 = 51 – 12 = 39

BT4. Tìm các cặp nghịch đảo nhau theo modulo 11

(1 , 1 )

(2 , 6 )

(3 , 4 )

(4 , 3 )

(5 , 9 )

(6 , 2 )

(7 , 8 )

(8 , 7 )

(9 , 5 )

(10 , 10 )

5. Tìm trực tiếp bằng định nghĩa đối với modulo theo

mod 11 =?

Ta có : (6.2) mod 11=1 => = 2 mod 11= 2

mod 11 =

Ta có : (5.9) mod 11=1 => = 9 mod 11= 9

mod 13 =

Ta có : (6.11) mod 13=1 => = 11 mod 13= 11

mod 13 = 12

mod 15 = 7

mod 25 = 6

BT6. Tìm nghịch đảo theo mod 19, mod 23, mod 29

19

(1 , 1 )(2 , 10 )(3 , 13 )(4 , 5 )(5 , 4 )(6 , 16 )(7 , 11 )(8 , 12 )(9 , 17 )(10 , 2 )(11 , 7 )(12 , 8 )(13 , 3 )(14 , 15 )(15 , 14 )(16 , 6 )(17 , 9 )(18 , 18 )

23

(1 , 1 )(2 , 12 )(3 , 8 )(4 , 6 )(5 , 14 )(6 , 4 )(7 , 10 )(8 , 3 )(9 , 18 )(10 , 7 )(11 , 21 )(12 , 2 )(13 , 16 )(14 , 5 )(15 , 20 )(16 , 13 )(17 , 19 )(18 , 9 )(19 , 17 )(20 , 15 )(21 , 11 )(22 , 22 )

29

(1 , 1 )(2 , 15 )(3 , 10 )(4 , 22 )(5 , 6 )(6 , 5 )(7 , 25 )(8 , 11 )(9 , 13 )(10 , 3 )(11 , 8 )(12 , 17 )(13 , 9 )(14 , 27 )(15 , 2 )(16 , 20 )(17 , 12 )(18 , 21 )(19 , 26 )(20 , 16 )(21 , 18 )(22 , 4 )(23 , 24 )(24 , 23 )(25 , 7 )(26 , 19 )(27 , 14 )(28 , 28 )

7. Sử dụng thuật toán Euclid mở rộng để tìm các giá trị nghịch đảo

mod 2011 = ?

Extend Euclid (M,B) nghịch đảo của B theo modulo M

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 2011 | 0 | 1 | 845 |
| 2 | 0 | 1 | 845 | 1 | 0-2\*1=-2 | 2011-845\*2=321 |
| 2 | 1 | -2 | 321 | -2 | 5 | 203 |
| 1 | -2 | 5 | 203 | 3 | -7 | 118 |
| 1 | 3 | -7 | 118 | -5 | 12 | 85 |
| 1 | -5 | 12 | 85 | 8 | -19 | 33 |
| 2 | 8 | -19 | 33 | -21 | 50 | 19 |
| 1 | -21 | 50 | 19 | 29 | -69 | 14 |
| 1 | 29 | -69 | 14 | -50 | 119 | 5 |
| 2 | -50 | 119 | 5 | 129 | -307 | 4 |
| 1 | 129 | -307 | 4 | -179 | 426 | 1 |
| 845\*426=359970 | /2011=179 | \*2011 | =359969 |  | | |

mod 187;

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 187 | 0 | 1 | 47 |
| 3 | 0 | 1 | 47 | 1 | -3 | 46 |
| 1 | 1 | -3 | 46 | -1 | 4 | 1 |
|  |  |  |  |  | | |

mod 323;

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 323 | 0 | 1 | 101 |
| 3 | 0 | 1 | 101 | 1 | -3 | 20 |
| 5 | 1 | -3 | 20 | -5 | 16 | 1 |
|  |  |  |  |  | | |

d 809

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 809 | 0 | 1 | 357 |
| 2 | 0 | 1 | 357 | 1 | -2 | 95 |
| 3 | 1 | -2 | 95 | --3 | 7 | 72 |
| 1 | -3 | 7 | 72 | 4 | -9 | 23 |
| 3 | 4 | -9 | 23 | -15 | 34 | 3 |
| 7 | -15 | 34 | 3 | 109 | -247 | 2 |
| 1 | 109 | -247 | 2 | 134 | 281 | 1 |
|  |  |  |  |  | | |

Định lý Ferma