Subject :

Date :
Time :

$a \equiv r \pmod{n}$

$\Rightarrow a = qn + r$

integer

$n) a (q$

$\square$

r

positive $n > 0$

non-negative $r \geq 0$

27 mod 5

$(n)5) \overset{(a)}{27} (5 (q)$

25

$2 (r)$

$27 = 5 \times 5 + 2$

$\Rightarrow a = qn + r$

$\Rightarrow a \equiv r \pmod{n}$

$\Rightarrow 27 \equiv 2 \pmod{5}$

-18 mod 14

$\Leftrightarrow$

$14) -18 (-1$

-14

$(+)$

-4

$-18 = -1 \times 14 + (-4)$

$\Rightarrow -18 \equiv (-4) \pmod{14}$

Sum

$\Downarrow$

10

So output = 10

Subject :

Date :

Time :

⊞ $-18 \bmod 14$

$$14 \overline{)\ -18\ (\ -2}$$

$$\underline{-28}$$

$$10$$

must be less than or equal to -18

⊞ $-7 \bmod 10$

$$10 \overline{)\ -7\ (\ \square}$$

→ ?

Setu Library

Subject :

Date :
Time :

$-7 \mod 10$

$$10) \; -7 \; (-1$$
$$\underline{(+)\;-10}$$
$$3$$

$Z_n \Rightarrow$ set of integers from 0 to $n-1$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

$Z = \{\ldots -6, -5, -4, -3, \ldots, 0, 1, 2, 3, 4, \ldots\}$

$Z_{10} = ?$

$10) -6 \; (-1$ | $10) -5 \; (-2$ | $10) -4 \; (-1$ | $\ldots$

$\underline{(+)\;-10}$ | $\underline{(+)\;-10}$ | $\underline{(+)\;-10}$ |

4 | 0 | 6 |

$10) 0 \; (0$ | $10) 1 \; (0$ | $10) 4 \; (0$ | $10) 9 \; (0$ | $10) 11 \; (1$

$\underline{0}$ | $\underline{0}$ | $\underline{0}$ | $\underline{0}$ | $\underline{10}$

0 | 1 | 4 | 9 | 1

for Z_{10} ⇒

we have to find mod 10 of all elements of set Z. And by doing that, we always get value from 0 to n−1 or 0 to 9.

Modular Exponentiation

- used to efficiently calculate large power of a number modulo some integer.

$$a^b \bmod m$$

- By Squaring
  - ↳ complexity $O(\log_2 n)$

Subject :

Date :
Time :

Q1 $29^5 \bmod 100$

$\Rightarrow$

binary of $5 = 101_2$

2^2	2^1	2^0
4	2	1
1	0	1

* Now we will find $29^1 \bmod 100$.
* Then we will find $29^2 \bmod 100$ using previous value
* Then we will find $29^4 \bmod 100$ using prev value. After that we will stop (as $8 > 5$)
* Finally we will find $29^5 \bmod 100$ using prev values

$\Rightarrow$

$29^1 \bmod 100 = 29$

$29^2 \bmod 100 = (29^1 \times 29^1) \bmod 100$

$= 841 \bmod 100 = 41$

$29^4 \bmod 100 = 29^{2+2} \bmod 100$

$= (29^2 \times 29^2) \bmod 100$

$= [(29^2 \bmod 100) \times (29^2 \bmod 100)] \bmod 100$

$= (41 \times 41) \bmod 100$

$= 81$

Subject :

Date :

Time :

Finally,

$$29^{5} \bmod 100$$

$$= 29^{(4+1)} \bmod 100$$

$$= (29^{4} \times 29^{1}) \bmod 100$$

$$= \left[(29^{4} \bmod 100) \times (29^{1} \bmod 100)\right] \bmod 100$$

$$= 81 \times 29 \bmod 100$$

$$= 2349 \bmod 100$$

$$= 49$$

Ans

Subject :

Date :
Time :

$311^{127} \mod 211$

Binary of 127 =

01111111_2

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
	1	1	1	1	1	1	1

$311^1 \mod 211 = 100$

$311^2 \mod 211 = 100 \times 100 \mod 211 = 83$

$311^4 \mod 211 = 83 \times 83 \mod 211 = 137$

$311^8 \mod 211 = 137 \times 137 \mod 211 = 201$

$311^{16} \mod 211 = 201 \times 201 \mod 211 = 100$

$311^{32} \mod 211 = 100 \times 100 \mod 211 = 83$

$311^{64} \mod 211 = 83 \times 83 \mod 211 = 137$

$311^{128} =$ No as $128 > 127$

Subject :

Date :
Time :

$311^{127} \mod 211$

$= 311^{(1+2+4+8+16+32+64)} \mod 211$

$= [(311^1 \mod 211) * (311^2 \mod 211) * (311^4 \mod 211) * \ldots * (311^{64} \mod 211)] \mod 211$

$= (100 \times 83 \times 137 \times 201 \times 100 \times 83 \times 137) \mod 211$

$= [(100 \times 83 \times 137) \mod 211 \times (201 \times 100) \mod 211 \times (83 \times 137) \mod 211] \mod 211$

$= (21 \times 55 \times 188) \mod 211$

$= 21$

Ans

Subject :

Date :
Time :

- if GCD $(a, b) = 1$, then a and b is relatively prime or co-prime

⇒ **Multiplicative inverse:**

multiplicative inverse of a given number is a number that, when multiplied by the given number, results in 1.

for example:

multiplicative inverse of a $(a \neq 0)$ is $1/a$

Subject :

Date :
Time :

M.I in M.A

The multiplicative inverse of a number 'a' mod m is a number x such that

$$a * x \equiv 1 \mod m$$

$$\Rightarrow (a * x) \bmod m = 1$$

Multiplicative Inverse of a mod m exists iff a and m are co-prime

Multiplicative Inverse of 3 modulo 7 :

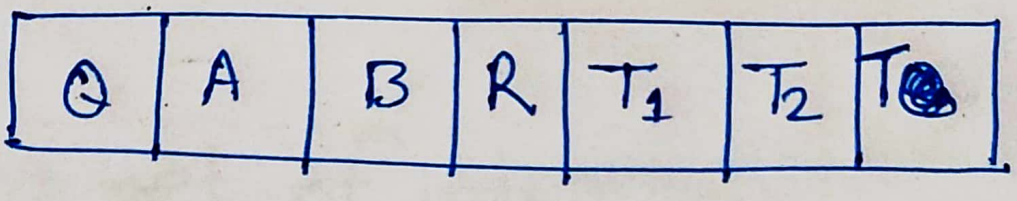
$$3 * x \equiv 1 \mod 7$$

$$\Rightarrow 3 * x \bmod 7 = 1$$

so if $x = 5$

$$3 * 5 \bmod 7 = 1$$

EEA



* $A > B$

* $T_1 = 0$ and $T_2 = 1$ initially

Subject :

Date :
Time :

What is the multiplicative inverse of 3 mod 5 ?

Q	A	B	R	T_1	T_2	T
1	5	3	2	0	1	−1
1	3	2	1	1	−1	2
2	2	1	0	−1	2	−5
	1	0		2	−5	

Ans.

3) 5 (1
   3

   2

$T = T_1 - Q \times T_2$
$= 0 - 1 \times 1$
$= -1$

2) 3 (1
   2

   1

$T = 1 - (-1) \times (1)$
$= 2$