Chapter 2 (cryptography)

Mathematics of cryptography

Modular Arithmetic, Congruence and Matrices

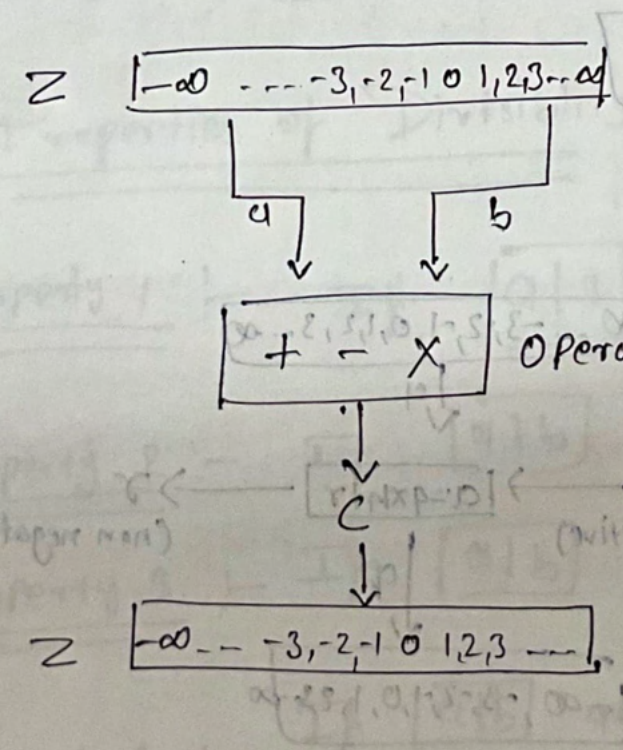
Integer Arithmetic :-

(1) Binary Operations :-

~~The~~ In cryptography there are 5 Binary operations.

they are :-

→ Addition
→ Substraction
→ Multiplication



Integer Division :—

If we devide 'a' by 'n' then we get two integer 'q' and 'r'

the relationship B/w these four integer is

$a = q \times n + r$

- a → Divident
- n → Divisor
- q → Quotient
- r → remainder

n) a (q

r

The four Number can be anything But In cryptography we impose 2 restrictions :—

① $n > 0$

② $r \geq 0$

$-\infty \ldots -3, -2, -1, 0, 1, 2, 3 \ldots \infty$

↓ q

n (Positive) → $a = q \times n + r$ → r (non negative)

↓ q

$-\infty, -3, -2, -1, 0, 1, 2, 3 \ldots \infty$

Divisibility :-

case1 :- If 'a' is Divisible By 'n' then we write it as

$n \mid a$

case2 :- If 'a' is Not Divisible By 'n' the we write it as

$a \nmid n$

Example :-

for case1 $13 \mid 78$, $7 \mid 98$, $-6 \mid 24$ $4 \mid 44$

for case2 :- ~~$13 \mid 27$~~ $13 + 27$, $7 + 50$ $-6 + 23$

Properties of Divisiblity :-

Property 1 :- If $a \mid 1$, then $a = \pm 1$

Property 2 :- If $a \mid b$, and $b \mid a$ then $a = \pm b$

Property 3 :- If $a \mid b$ and $b \mid c$ then $a \mid c$

Property 4 :- If $a \mid b$ and $a \mid c$ then

$$a \mid (mxb + nxc)$$

where m & n are arbitary integer.

Property 3 example

$3 \mid 15$ & $15 \mid 45$ then $3 \mid 45$

Property 4 example :-

$3 \mid 15$ & $3 \mid 9$ then

$3 \mid (15 \times 2 + 9 \times 4)$ which means $3 \mid 66$

All ~~Post~~ Divisor :- A positive integer can have more then one divisor.

Example :-

32 has :- 1, 2, 4, 16, 32 as Divisor

facts about Divisor of Positive integer :-

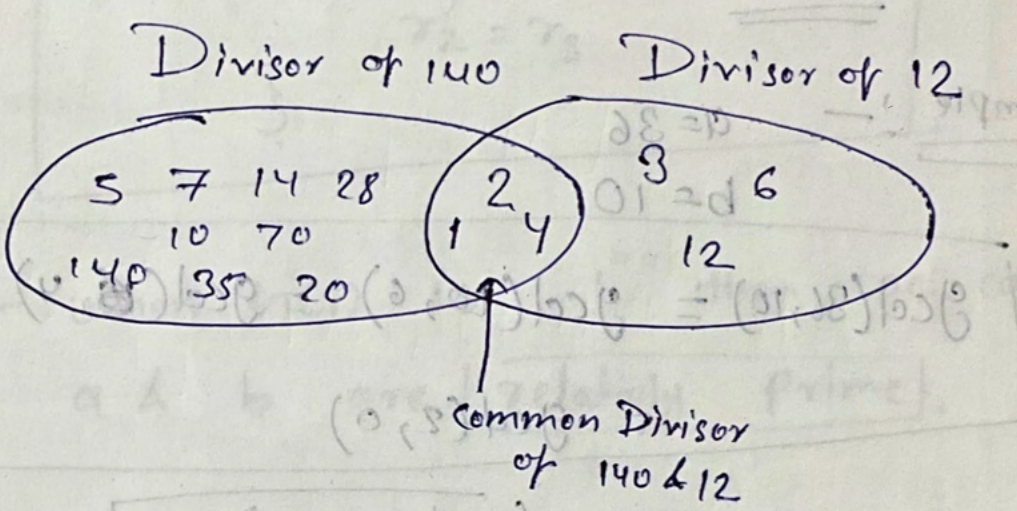
fact 1 :- The integer 1 has only one divisor Itself.

fact 2 :- Any Positive integer has atleast 2 divisor, 1 and itself.

Greatest Common Divisor :- One Integer often needed in cryptography is the "Greatest Common Divisor"

Two Positive integer may have many comman divisors, But only one Greatest common Divisor.

Example :- GCD of 140 & 12



Euclidean Algorithm :- finding the GCD of 2 Positive integer by listing all common divisor is not Practical. when two integer are too large.

The Mathematician named Euclid developed an algorithm for finding the GCD of 2 integers.

The "Euclidean Algorithm" Based on the 2 facts

fact 1 :- $\boxed{gcd(a,0) = a}$

fact 2 :- $\boxed{gcd(a,b) = gcd(b,r)}$ where r is remainder of dividing a by b.

fact1 :- If the second integer is 0, the gcd is first Number.

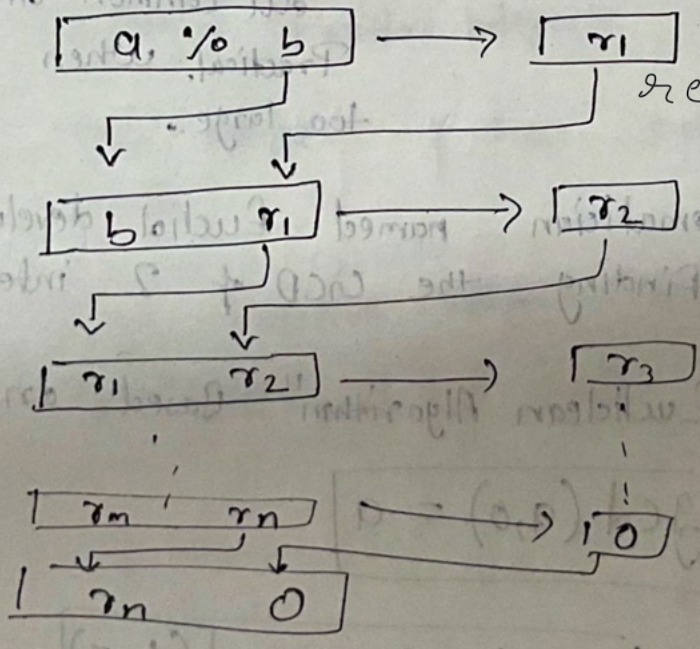
fact2 :- The second fact allow us to change the value of 'a' & 'b' until 'b' becomes '0'. then we can use the fact 1

Example :- a = 36
b = 10

$$gcd(36,10) = gcd(10,6) = gcd(6,4) = gcd(4,2) = gcd(2,0)$$

So our final $gcd(36,10) = 2$

```
int fun(a,b)
{
  if(b==0)
    return a;
  return fun(b, a%b);
}
```



r_n is our gcd.

Algorithm :-

```
r1 ← a , r2 ← b , r3
while (r2 != 0)
{
    r3 = r1 % r2;
    r1 = r2
    r2 = r3
}
```

Note :- when GCD is 1 then we can say a & b are **relativly prime**.

Example GCD of (25, 60)

→ a = 25 , b = 60 , r = 25
→ a = 60 , b = 25 , r = 10
→ a = 25 , b = 10 , r = 5
→ a = 10 , b = 5 , r = 0
⇒ **a = 5 , b = 0**

Extended Euclidean Algorithm :-

Given two integer a & b we often need to find other two integers 's' & 't' such that

$$s \times a + t \times b = \gcd(a, b)$$

This Algorithm is same as Euclidean Algorithm we are using 3 sets of variables r's s's & t's

(1) in r's set we have :-

r_1 r_2 & r

all have same value as in Euclidean Algorithm.

(2) in s's set we have :-

$s_1 = 1$ $s_2 = 0$ s

(3) in t's set we have :-

$t_1 = 0$ $t_2 = 1$ t

Algorithm for this :-

$r_1 \leftarrow a$, $r_2 \leftarrow b$

$s_1 \leftarrow 1$, $s_2 \leftarrow 0$

$t_1 \leftarrow 0$, $t_2 \leftarrow 1$

while ($r_2 \neq 0$)

{

$r = r_1 - q \times r_2$

$r_1 = r_2$

$r_2 = r$

$t = t_1 - q \times t_2$

$t_1 = t_2$

$t_2 = t$

$s = s_1 - q \times s_2$

$s_1 = s_2$

$s_2 = s$

}

$gcd(a,b) \leftarrow r_1$, $s \leftarrow s_1$, $t \leftarrow t_1$

Example :- $a = 161$, $b = 28$ find $\gcd(a,b)$ & value of s & t.

$$r = r_1 - q \times r_2 \qquad s = s_1 - q \times s_2$$

$$t = t_1 - q \times t_2$$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	

$\boxed{GCD = 7}$ $\boxed{s = -1}$ $\boxed{t = 6}$

then

$$161 \times (-1) + 28 \times 6 = 7$$

Example2 :- $a = 17$, $b = 0$, $s_1 = 1, s_2 = 0$, $t_1 = 0, t_2 = 1$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	17	0		1	0		0	1	

$\boxed{\gcd(17,0) = 17}$ $\boxed{s = 1}$, $\boxed{t = 0}$

~~17x0~~

$17 \times 1 + 0 \times 0 = 17$ Ans

Example3 $a=0, b=45, s_1=1, s_2=0, t_1=0, t_2=1$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	0	45	0	1	0	1	0	1	0
	45	0		0	1		1	0	

gcd = 45 , s = 0 , t = 1

$0 \times 0 + 45 \times 1 = 45$

Linear Diophantine Equations :-

This is the application of "Extended Euclidean algorithm".

we have to find the solution of this equation using the prevous algorithm.

the equation is of type $ax+by+c$

we need to find the value of x & y that satisfy the equation.

If $d = gcd(a,b)$

→ If $d \nmid c$ (c is Not divisible By d) then the equation have ~~infinite~~ no solution

→ If $d \mid c$ (c is divisible By d) then the equation have infinite solution.

In the infinite Number of Solution one is 'Particular' & the rest, are 'general'.

linear Diophantine equation of two variable :-

$ax+by+c$

Particular Solution :-

If $d|c$ then particular Solution can be found using these steps :-

Step1 :- Reduce the equation By deviding Both Side of equation By 'd',
This is possible because 'd' divides a, b, c By assumption.

Step2 :- Solve for '3' & 't' in relation.
$a_1 3 + b_1 t = 1$ using Extended Equlidean Algorithm.

Step3 :- Particular Solution founded By

$x_0 = \left(\frac{c}{d}\right) \times 3$ $\quad$ $y_0 = \left(\frac{c}{d}\right) t$

General Solution :-

After finding Particular Solution the general Solution can be found :-

$$x = x_0 + K\left(\frac{b}{d}\right) \qquad y = y_0 - K\left(\frac{a}{d}\right)$$

where K is an integer

Example :- Find the particular and general solutions to the equation.

$$21x + 14y = 35$$

Solution

$$GCD(21, 14) = 7 = d$$

Since $7 \mid 35$ So the equation have Infinite number of solution.

~~So Step1~~ So first we are going to find Particular Solution :-

Step1 our New equation after deviding Both side By $d = 7$

$$3x + 2y = 5$$

Step 2 :- Using Extended Euclidean Algorithm we Find s & t such as

$$3s + 2t = 1$$

Using Extended Euclidean algorithm :-

~~$a = 3 \quad b = 2$~~

$r_1 = 3,\ r_2 = 2,\ r,\quad s_1 = 1,\ s_2 = 0,\ s,\quad t_1 = 0,\ t_2 = 1,\ t$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
1	3	2	1	1	0	1	0	1	-1
2	2	1	0	0	1	-2	1	-1	3
	1	0		1	-2		-1	3	

So we got $\boxed{s_0 = 1}$ & $\boxed{t = -1}$

So our Particular solution is :-

$$x_0 = \left(\frac{c}{d}\right)s \Rightarrow \left(\frac{35}{7}\right) \times 1 = 5$$

$$y_0 = \left(\frac{c}{d}\right)t \Rightarrow \left(\frac{35}{7}\right)(-1) = -5$$

our $\boxed{x_0 = 5}$ $\boxed{y_0 = -5}$

our Particular solution is :-

$$x = x_0 + k\left(\frac{b}{d}\right) \qquad y = y_0 - k\left(\frac{a}{d}\right)$$

$$x = 5 + k(2) \qquad y = -5 - k(3)$$

where K is any integer

Let K = 0, 1, 2, 3, - - -

So our (x, y) = (5, -5) (7, -8), (9, -11) - - - -

these solusion satisfy the original equation.

Modular ARithmetic

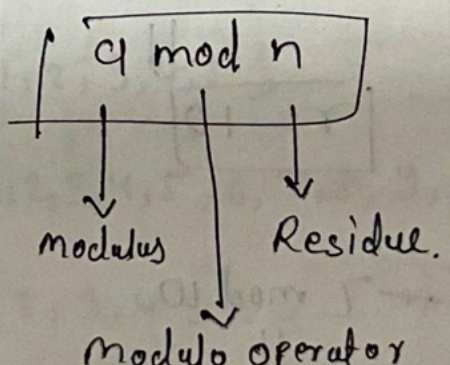
In division Relationship ($a = q \times n + r$)

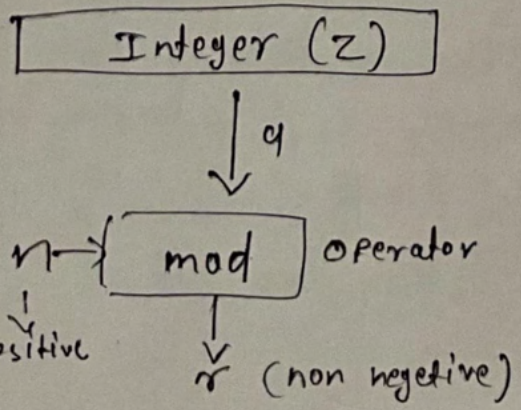
we have 2 inputs q & n

& 2 output q & r

But in modular arithmetic we are interested in only r (remainder)

Modulo Operator:-





Example :- $27 \bmod 5 = 2$

$36 \bmod 12 = 0$

If a is Negetive then we add 'n' Continously untill $a \geq 0$ $a < 0$

Example (1)

$-18 \bmod 14$

$\Downarrow$

~~$-4 \bmod 14$~~

$(-18+14) \bmod 14$

$\Downarrow$

$-4 \bmod 14$

$\Downarrow$

$(-4+14) \bmod 14$

$\Downarrow$

$10 \bmod 14$

$\Downarrow$

$r = 10$

(2) $-7 \bmod 10$

$\Downarrow$

$(-7+10) \bmod 10$

$\Downarrow$

$3 \bmod 10$

$\Downarrow$

$r = 3$

Set of Residues : Z_n

The result of the modulo operation with modulus n is always an integer between 0 and $n-1$.

Or

we can say that the modulo operation creates a set. In modulo arithmetic this set is referred to as the

> Set of least residues modulo n or Z_n

Example :-

$Z_2 = \{0, 1\}$

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

$Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$Z_n = \{0, 1, 2, 3, 4 \ldots n-1\}$

Congruence :- ($\equiv$)

Two integers a & b are congruent modulo m iff they have the same remainder when divided by m.

Denoted By

$$a \equiv b \pmod{m}$$

a is congruent to b mod m

Note :-

(1) $a \equiv b \pmod{m}$ means $a \bmod m = b \bmod m$

(2) $a \equiv b \pmod{m}$ iff m divides $a-b$

Residue classes :- $[a]$ or $[a]_n$ is a set of integers congruent modulo n.

example :-

$n = 5$

then Residue classes

$[0] = \{\ldots -15, -10, -5, 0, 5, 10, 15 \ldots\}$

$[1] = \{\ldots -14, -9, -4, 1, 6, 11, 16 \ldots\}$

$[2] = \{\ldots -13, -8, -3, 2, 7, 12, 17 \ldots\}$

$[3] = \{\ldots -12, -7, -2, 3, 8, 13, 18 \ldots\}$

$[4] = \{\ldots -11, -6, -1, 4, 9, 14, 19 \ldots\}$

Set of least residue = $Z_5 \{0,1,2,3,4\} = Z_n$

Modulo arithmetic Example in daily life is clock. (It start from 12 instead of 0)

It is mod 12

Operation on Z_n :- 3 Binary operations are defined for Z_n

1. addition
2. Substraction
3. Multiplication.

After Performing these operation Between 2 numbers, the result will be mapped to Z_n using **mod n**

$(a+b) \bmod n$

$(a-b) \bmod n$

$(a*b) \bmod n$

Properties :-

1. $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
2. $(a-b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
3. $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

These Property are helpful when number is too Big. So the addition & multiplication also become too big.

Inverse :-

In cryprography we mainly focus on 2 types of inverse :-

(1) **Additive Inverse** :- It is related to addition operation.

Two numbers 'a' & 'b' are additive inverse of each other

if $a+b \equiv 0 \bmod n$

Example, n=10

a=4

the additive inverse of 4 is 6

Multiplicative Inverse :-

In Z_n, two number a & b are the multiplicative inverse of each other if.

$$a \times b \equiv 1 \bmod n$$

* **Note** :- 'a' has multiplicative inverse in Z_n if $\gcd(a,n) = 1$, or 'a' & 'n' are relatively Prime.

Example :- The multiplicative inverse of '8' in Z_{10} (Multiply 8 by some no in Z_{10} than find mod 10 if it is 1 so than no is multiplicative inverse of 8)

There is No number in Z_{10} such that when it is multiplied to 8 ~~leave~~ ~~it~~ ~~remainder~~ '1'. & after multiply the modulo 10 become 1.

Note :- The multiplicative inverse of a number exist only when ~~the~~ 'n' & 'a' are relatively prime.

Example :-

$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

3 pairs (1,1) (3,7) (9,9) has a multiplicative inverse in Z_n

$(1*1) \bmod 10 = 1$

$(3*7) \bmod 10 = 1$

$(9*9) \bmod 10 = 1$

0, 2, 4, 5, 6, 8 do Not have multiplicative inverse.

Finding Multiplicative inverse using Extended Euclidean Algorithm:-

The Extended Euclidean Algorithm finds the multiplicative inverse of 'b' in Z_n

when 'n' & 'b' are given & $\boxed{\gcd(n, b) = 1}$

The multiplicative inverse of 'b' is 't' after it mapped to Z_n. (means after $\boxed{t \bmod n}$ ↓ multiplicative inverse.)

Example ① find multiplicative inverse of 11 in Z_6

~~r_1 r_2~~

$r_1 = n$, $r_2 = b$, r,
$t_1 = 0$, $t_2 = 1$, t

$\boxed{r = r_1 - q \times r_2}$
$\boxed{t = t_1 - q \times t_2}$

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		-7	26	

$\gcd = r_1 = 1$

$t_1 = -7 \bmod 26 = 19$

So the multiplicative inverse of 23 is 19

Example 2 :- Multiplicative inverse of 23^{-1} in Z_{100}

$b = 23 \quad n = 100$

$r_1 = 100, \quad r_2 = 23, \quad r$

$t_1 = 0, \quad t_2 = 1, \quad t$

q	r_1	r_2	r	t_1	t_2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
1	8	7	1	-4	9	-13
7	7	1	0	9	-13	100
	1	0		-13	100	

gcd = 1 means Multiplicative inverse exist

t = -13

-13 mod 100 = 87 is the multiplicative inverse of 23.

$(87 \times 23) \bmod 100 = (2001) \bmod 100 = 1$

Example 3 :- Multiplicative inverse of 12 in Z_{26}

q	r_1	r_2	r	t_1	t_2	t
2	26	12	2	0	1	-2
6	12	2	0	1	-2	13
	2	0		-2	13	

$\gcd(12,26) = 2 \neq 1$ so there is No multiplicative inverse of 12

Addition table for Z_{10}

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

In addition each no. has an inverse

Multiplication table for Z_{10}

×	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	0	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

But in case of multiplication It is Not Possible

Different set for addition and Multiplication :-

If the operation is addition the Z_n Be the set of Possible key because each element in Z_n have a inverse.

On other hand when the operation is multiplication the Z_n can Not be a set of Possible key. Because some of the elements has a inverse.

Because of this we need another set Z_n^* . This set contains all the element of Z_n such that ~~it has~~ each element of Z_n^* has a multiplicative inverse.

Note :- we need Z_n when addative inverse are needed.
we need Z_n^* when multiplicative inverse is needed.

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

$Z_7 = \{0,1,2,3,4,5,6\}$, $Z_7^* = \{1,2,3,4,5,6\}$

$Z_{10} = \{0,1,2,3,4,5,6,7,8,9\}$ $Z_{10}^* = \{1,3,7,9\}$

We have two more Set Z_p & Z_p^*.

Z_p is same as Z_n :- But p is prime number only.
↳ It contains $0 \rightarrow n-1$

Z_p^* contain $1 \rightarrow n-1$ In this set all the numers has a addative as well as Multiplicative inverse.

Example

$Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

$Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

Residue Matrix :- Matrix with all elements are in Z_n.

All operations are same as integer matrix only addition is that all operations ~~is~~ are done in modular arithmetic.

this Matrix has Multiplicative inverse only if $\boxed{\gcd(\det(A), n) = 1}$

...

Inverse of a matrix 'A'

$$A^{-1} = \frac{Adj(A)}{det(A)}$$

~~Adj~~

find inverse of a matrix

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \Rightarrow \begin{bmatrix} 4 & -3 \\ -2 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 2 \end{bmatrix} \Rightarrow \text{C} \downarrow \text{TC} \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 2 & -1 & -1 \\ 0 & 3 & 0 \\ -1 & -1 & 2 \end{bmatrix} \Rightarrow \frac{1}{|A|} \begin{bmatrix} 2 & -1 & -1 \\ 0 & 3 & 0 \\ -1 & -1 & 2 \end{bmatrix}$$

$$|A| = 3 \quad \Rightarrow \frac{1}{3} \begin{bmatrix} 2 & -1 & -1 \\ 0 & 3 & 0 \\ -1 & -1 & 2 \end{bmatrix}$$

$$A = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$$A^{-1} = \frac{Adj(A)}{Det(A)}$$

$$Det(A) = 17(18\times19 - 2\times21) - 17(21\times19 - 2\times21) + 5(21\times2 - 2\times18)$$
$$= -939 \Rightarrow -939 \bmod 26$$
$$= -3 \bmod 26 \Rightarrow 23$$

$$Adj(A) = \begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$$

$(18\times19 - 2\times21) = 300 \bmod 26 = 14$
$-(21\times19 - 2\times21) = -357 \bmod 26 = 7$
$(21\times2 - 2\times18) = 6 \bmod 26 = 6$
$-(17\times19 - 2\times5) = -313 \bmod 26 = 25$
$(17\times19 - 2\times5) = 313 \bmod 26 = 1$
$-(17\times2 - 2\times17) = 0 \bmod 26 = 0$
$(17\times21 - 18\times5) = 267 \bmod 26 = 7$
$-(17\times21 - 21\times5) = -252 \bmod 26 = 8$
$(17\times18 - 21\times17) = -51 \bmod 26 = 1$

$$\text{Co-factor of } A = \begin{bmatrix} 14 & 7 & 6 \\ 25 & 1 & 0 \\ 7 & 8 & 1 \end{bmatrix}$$

$$A^T = \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \bmod 26$$

$$A^{-1} = \frac{1}{23} \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \bmod 26$$

Multiplicative inverse of 23 is 17 by Extended Ecludian Algo

q	r_1	r_2	r	t_1	t_2	t
1	26	23	3	0	1	-1
7	23	3	2	1	-1	8
1	3	2	1	-1	8	-9
1	2	1	1	8	-9	17
1	1	1	0	-9	17	-26
	1	0		17	-26	

17 → multiplicative inverse of 23

$$A^{-1} = 17 \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$A^{-1} = \begin{pmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{pmatrix} \bmod 26$$

$$A^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

To verify it is inverse or not

$$A \times A^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$A = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \qquad A^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} = \begin{bmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$