

Chapter 2 (cryptography)

Mathematics of Cryptography

Modular Arithmetic, Congruence and
Matrices

Integer Arithmetic :-

(1) Binary Operations :-

In cryptography there are 8 binary operations.

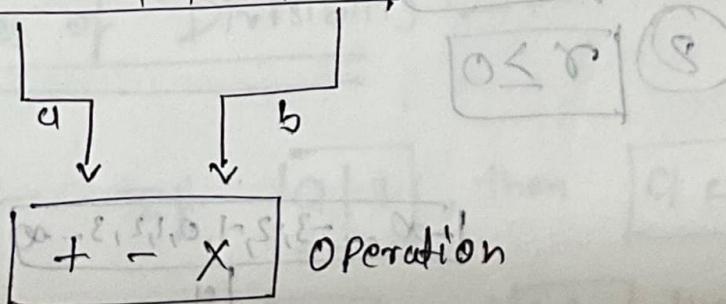
they are !

→ Addition

→ Subtraction

→ Multiplication

$$\mathbb{Z} \quad [-\infty, \dots, -3, -2, -1, 0, 1, 2, 3, \dots]$$



+ - x Operation

$$\mathbb{Z} \quad [-\infty, \dots, -3, -2, -1, 0, 1, 2, 3, \dots]$$

Integer Division :-

If we divide ' a ' by ' n ', then we get two integers ' q ' and ' r '.
The relationship b/w these four integers is

$$a = q \times n + r$$

↓ ↓ ↓ ↓
 Dividend Divisor Quotient remainder

The four numbers can be anything. But in Cryptography we impose 2 restrictions :-

$$\begin{array}{l} ① \\ ② \end{array} \quad \boxed{n > 0}$$

$$\boxed{-\infty, -3, -2, -1, 0, 1, 2, 3, \dots, \infty}$$

$\downarrow q$

$$n \xrightarrow{\text{(positive)}} \boxed{a = q \times n + r} \xrightarrow{\text{non negative}} r$$

$\downarrow q$

$$\boxed{-\infty, -3, -2, -1, 0, 1, 2, 3, \dots, \infty}$$

Divisibility :-

case 1 :- If a is Divisible By 'n' then we write it as

$$\boxed{\cancel{a}} \quad \boxed{n | a}$$

case 2 :- If a is Not Divisible By 'n' then we write it as

$$\boxed{a \cancel{|} n}$$

Example :-

for case 1 $\boxed{13178}, \boxed{7198}, \boxed{-6124}, \boxed{14744}$

for case 2 $\boxed{13+27}, \boxed{13+27}, \boxed{7+50}, \boxed{-6+23}$

Properties of Divisibility :-

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

Property 2 :- If $|a| b$, and $|b| c$ then $|a| c$

Property 3 :- If $|a| b$ and $|b| c$ then $|a| c$

Property 4 :- If $|a| b$ and $|a| c$ then

$$\boxed{|a| (mb + nc)}$$

where m & n are arbitrary integer.

Property 3 example

\rightarrow if $a \mid c$ & $b \mid c$ then $a \mid b$

$3 \mid 15$ & $3 \mid 45$ 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 than one divisor.

Example

32 has $\{1, 2, 4, 8, 16, 32\}$ as Divisors

facts about Divisors of Positive integers

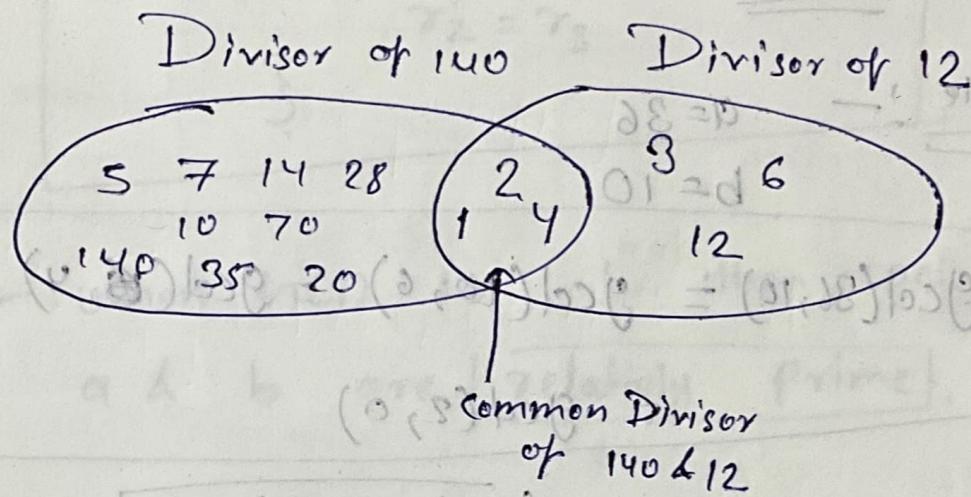
Fact 1! — The integer 1 has only one divisor Itself.

Fact 2! — Any Positive integer has at least 2 divisors, 1 and itself.

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

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

Example! :- GCD of 140 & 12



Euclidean Algorithm :- finding the GCD of 2 positive integers by listing all common divisor is not practical, when two integers 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

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

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

fact 1 :- If the second integer is 0, the gcd is first number.

fact 2 :- The second fact allow us to change the value of 'a & b' until 'b' becomes '0'. then we can use the fact 1

Example :-

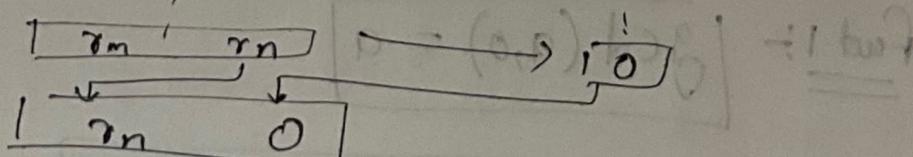
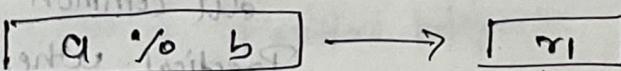
$$a = 36$$

$$b = 10$$

$$\text{gcd}(36, 10) = \text{gcd}(10, 6) = \text{gcd}(6, 4) = \text{gcd}(4, 2)$$

$$\text{gcd}(2, 0)$$

So our final $\boxed{\text{gcd}(36, 10) = 2}$



r_n is our gcd.

Algorithm :-

$$r_1 \leftarrow a, r_2 \leftarrow b, r_3$$

while ($r_2 \neq 0$)

$$\quad r_3 = r_1 \% r_2;$$

$$(d, r) \leftarrow \begin{cases} r_1 = r_2 \\ r_2 = r_3 \end{cases}$$

Note :- when HCD is 1 then we can say
a & b are relatively prime.

Example

HCD of (25, 60)

$$\rightarrow a = 25, b = 60, r = 25$$

$$\rightarrow a = 60, b = 25, r = 10$$

$$\rightarrow a = 25, b = 10, r = 5$$

$$\rightarrow a = 10, b = 5, r = 0$$

$$\Rightarrow \boxed{a = 5, b = 0}$$

Extended Euclidean Algorithm

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

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

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:-

$$r_1, r_2, \dots, r$$

all have same value as in Euclidean Algorithm.

② in s 's set we have:-

$$s_1 = 1 \quad s_2 = 0 \quad s$$

③ in t 's set we have:-

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

Algorithm for this! → $\text{gcd}(a, b) = \frac{a_1}{\text{lcm}(a_1, b_1)}$

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

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

$$d_1 \leftarrow 0, d_2 \leftarrow 1$$

[step $\rightarrow t = b$]

while ($r_2 \neq 0$)

$$r = \cancel{r_1} - q \times r_2 \quad r_1 \leftarrow r_2$$

$$r_1 \leftarrow r_2$$

$$r_2 \leftarrow r$$

$$t = \cancel{d_1} - q \times d_2 \quad d_1 \leftarrow d_2$$

$$d_1 \leftarrow d_2$$

$$d_2 \leftarrow t$$

$$s = \cancel{s_1} + s_2 \quad s_1 \leftarrow s_2$$

$$s_1 \leftarrow s_2$$

$$s_2 \leftarrow s$$

}

$$\text{gcd}(a, b) \leftarrow r_1, s \leftarrow s_1, t \leftarrow d_1$$

0.2.12.0

1.3E-002, b

t	s	16	32	128	512	2048	8192	32768	131072	524288	2100000
1	0	0	1	0	1	0	1	0	1	0	1

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

$$r = r_1 - q \times r_2$$

$$s = s_1 - q \times s_2$$

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

q	r_1	r_2	r	s_1	s_2	s	d_1	d_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	

$$\gcd = 7$$

$$s = -1$$

$$t = 6$$

then

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

Example :- $a = 17, b = 0, s_1 = 1, s_2 = 0, d_1 = 0, d_2 = 1$

a	r_1	r_2	r	s_1	s_2	s	d_1	d_2	t
17	0		17	1	0	1	0	1	

$$\gcd(17, 0) = 17$$

$$s = 1$$

$$t = 0$$

~~7x0~~

$$17x1 + 0x0 = 17$$

Examples

$$a=0, b=45, S_1=1, S_2=0, t_1=0, t_2=1$$

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	

$$\gcd = 45, S_1 = 0, S_2 = t = 1$$

$$(0x0 + 45 \times 1 = 45)$$

Linear Diophantine Equations :-

This is the application of ~~by~~ Extended Euclidean algorithm.

We have to find the solution of this equation using the previous 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:-

$$ax + by + c = 0$$

Particular Solution :-

If $a \mid c$ then Particular Solution can be found using these steps :-

Step 1 :- Reduce the equation By dividing Both Sides of equation By ' d ' ,
This is possible because ' d ' divides a, b, c By assumption.

Step 2 :- Solve for ' s ' & ' t ' in relation

$$a_1 s + b_1 t = 1 \text{ using Extended Euclidean Algorithm}$$

Step 3 :- Particular Solution founded By

$$x_0 = \left(\frac{c}{d}\right) \times s$$

$$y_0 = \left(\frac{c}{d}\right) t$$

General Solution

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

$$\boxed{n = n_0 + K\left(\frac{b}{d}\right)}$$

$$\boxed{y = y_0 - K\left(\frac{a}{d}\right)}$$

where K is an integer

Example !— find the particular and general solutions to the equation.

$$\boxed{21n + 14y = 35}$$

Solution

$$\boxed{\text{GCD}(21, 14) = 7 = d}$$

Since $7 \mid 35$ So the equation have

Infinite number of solution.

Step 1 So first we are going to find Particular Solution :-

Step 1 our new equation after dividing Both side By $d \Leftrightarrow$

$$\boxed{3n + 2y = 5}$$

Step 2 ← Using Extended Euclidean Algorithm
we find s & t such as

$$3s + 2t = 1$$

Using Extended Euclidean algorithm! —

$$\cancel{d} = 3 \quad \cancel{b} = 2$$

$$x_1 = 3, x_2 = 2, r, s_1 = 1, s_2 = 0, t, d_1 = 0, d_2 = 1, f$$

q	x_1	x_2	r	s_1	s_2	s	d_1	d_2	f
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

$$\boxed{s_0 = 1} \quad \& \quad \boxed{f = -1}$$

So our Particular Solution is! —

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

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

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

our Particular Solution is! —

$$x = x_0 + k\left(\frac{b}{d}\right)$$

$$y = y_0 - k\left(\frac{a}{d}\right)$$

$$x = 5 + k(2)$$

$$y = -5 - k(3)$$

where k is any integer

Let $k = 0, 1, 2, 3, \dots$

So our $(x, y) = (5, -5), (7, -8), (9, -1), \dots$

these solutions satisfy the original equation.

Modular Arithmetic

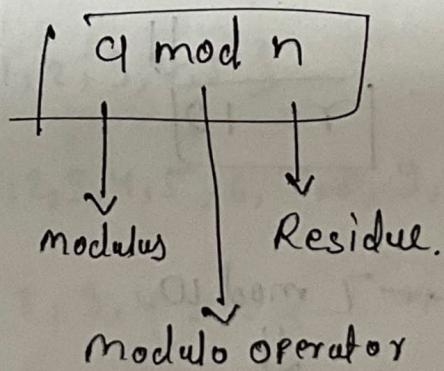
In division relationship ($a = q \times n + r$)

we have 2 inputs a & n

& 2 output q & r

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

Modulo Operator!



Integer (z)

$\downarrow q$

$n \rightarrow \{ \text{mod} \}$ operator

positive

$\downarrow r$ (non negative)

Example $\rightarrow 27 \bmod 5 = 2$

$$36 \bmod 12 = 0$$

If a is Negative then we add ' n '
Continuously until $a \geq 0$ $a < 0$

Example ①

$$-18 \bmod 14$$

↓

$$\cancel{-4 \bmod 1} \\ (-18+14) \bmod 14$$

↓

$$-4 \bmod 14$$

$$\cancel{(-4+14) \bmod 14}$$

$$(10 \bmod 14)$$

$$10 \bmod 14$$

$$\boxed{r=10}$$

②

$$-7 \bmod 10$$

$$\cancel{(-7+10) \bmod 10}$$

↓

$$3 \bmod 10$$

↓

$$\boxed{r=3}$$

(5) divisible

↓

colorless | brown ↓

(critically non)

↓

Set of Residues : \mathbb{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

\mathbb{Z}_n

Example :

$$\mathbb{Z}_2 = \{0, 1\}$$

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

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

$$\mathbb{Z}_n = \{0, 1, 2, 3, 4, \dots, n-1\}$$

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

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

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

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

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

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

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

Set of least residue $\equiv \mathbb{Z}_5 \{0, 1, 2, 3, 4\} = \mathbb{Z}_5$

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

It is $\underline{\text{mod } 12}$

Operation on \mathbb{Z}_n !

Binary operations are defined for \mathbb{Z}_n

- ① Addition
- ② Subtraction
- ③ Multiplication.

After performing these operation between 2 numbers, the result will be mapped to \mathbb{Z}_n using $\boxed{\text{mod } n}$

$$(a+b) \text{ mod } n$$

$$(a-b) \text{ mod } n$$

$$(a \times b) \text{ mod } n$$

Properties !

$$\textcircled{1} (a+b) \text{ mod } n = [(a \text{ mod } n) + (b \text{ mod } n)] \text{ mod } n$$

$$\textcircled{2} (a-b) \text{ mod } n = [(a \text{ mod } n) - (b \text{ mod } n)] \text{ mod } n$$

$$\textcircled{3} (a \times b) \text{ mod } n = [(a \text{ mod } n) \times (b \text{ mod } n)] \text{ mod } n$$

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

Inverse

In cryptography 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

$$\text{If } a+b \equiv 0 \pmod{n}$$

Example, ~~n=10~~ n=10

$$a=4$$

the additive inverse is 6

Multiplicative Inverse

In \mathbb{Z}_n , two number a & b are the multiplicative inverse of each other if.

$$a \times b \equiv 1 \pmod{n}$$

Note :- If 'a' has multiplicative inverse in \mathbb{Z}_n if $\gcd(a,n)=1$, or ' a ' & ' n ' are relatively prime.

Example 1 :- The multiplicative inverse of '8' in \mathbb{Z}_{10} (multiply 8 by some no in \mathbb{Z}_{10} than find mod 10 if it is 1 so than no is multiplicative inverse of 8 number in \mathbb{Z}_{10} such that there is No number in \mathbb{Z}_{10} multiplied to 8 leaves it when it is multiplied the remainder $\neq 1$. & after multiply the modulo 10 become 1.

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

Example 2

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

3 pairs $(1,1)$ $(3,7)$ $(9,9)$ has a multiplicative inverse in \mathbb{Z}_n

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

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

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

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

finding Multiplicative inverse using Extended Euclidean Algorithm

The Extended Euclidean Algorithm finds the multiplicative inverse of 'b' in \mathbb{Z}_n

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

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

\downarrow
multiplicative inverse.

Example ① find multiplicative inverse of 11 in \mathbb{Z}_6

$$\cancel{x_1} \cancel{x_2}$$

$$x_1 = n, x_2 = b, r, t$$

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

$$\begin{aligned} r &= r_1 - q_1 x_1 \\ t &= t_1 - q_1 x_1 \end{aligned}$$

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 11
is 19

Example 2 :- Multiplicative inverse of 23 in \mathbb{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	0	-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	

$$\boxed{\gcd = 1}$$

means Multiplicative inverse exist

$$\boxed{t = -13}$$

$-13 \bmod 100 = 87$ is the multiplicative inverse of 23.

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

Example 3 ↗ Multiplicative inverse of 12 in \mathbb{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 ≠ 1 so

there is No multiplicative inverse of 12

Addition table for \mathbb{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 \mathbb{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 additive 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 \mathbb{Z}_p & \mathbb{Z}_p^* .

\mathbb{Z}_p is same as \mathbb{Z}_n :- But p is prime number only.
It contains $0 \rightarrow n-1$

\mathbb{Z}_p^* contain $1 \rightarrow n-1$ In this set all the numbers has additive as well as Multiplicative inverse.

Example

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

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

Residue Matrix :- Matrix with all elements are in \mathbb{Z}_n .

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

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

Inverse of a matrix 'A'

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

~~Adj~~

Find inverse of a matrix

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

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

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

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

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

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

$$\begin{aligned} \text{Det}(A) &= 17(18 \times 19 - 2 \times 21) - 17(21 \times 19 - 2 \times 21) + 5(21 \times 2 - 2 \times 18) \\ &= -939 \Rightarrow -939 \bmod 26 \\ &= -3 \bmod 26 \Rightarrow 23 \end{aligned}$$

$$\text{Adj}(A) = \begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix} \quad \begin{aligned} (18 \times 19 - 2 \times 21) &= 300 \bmod 26 = 14 \\ -(21 \times 19 - 2 \times 21) &= -357 \bmod 26 = 7 \\ (21 \times 2 - 2 \times 18) &= 6 \bmod 26 = 6 \\ -(17 \times 19 - 2 \times 5) &= -313 \bmod 26 = 25 \\ (17 \times 19 - 2 \times 5) &= 313 \bmod 26 = 1 \\ -(17 \times 2 - 2 \times 17) &= 0 \bmod 26 = 0 \\ (17 \times 21 - 18 \times 5) &= 267 \bmod 26 = 7 \\ -(17 \times 21 - 21 \times 5) &= -252 \bmod 26 = 8 \\ (17 \times 18 - 21 \times 17) &= -51 \bmod 26 = 1 \end{aligned}$$

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

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

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

Multiplicative inverse of 23 is 17 by Extended Euclidean Algo

$$\begin{array}{cccc|ccc}
 2 & 21 & 22 & 2 & t_1 & t_2 & t \\
 1 & 26 & 23 & 3 & 0 & 1 & -1 \\
 7 & 23 & 3 & 2 & 1 & -1 & 8 \\
 1 & 3 & 2 & 1 & -1 & 8 & -9 \\
 1 & 2 & 1 & 1 & 8 & -9 & 17 \\
 1 & 1 & 1 & 0 & -9 & 17 & -26 \\
 1 & 0 & & & 17 & -26 &
 \end{array}$$

→ multiplicative inverse of 23

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

$$A^{-1} = \begin{pmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 162 & 0 & 17 \end{pmatrix} \text{ mod } 26$$

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

To verify it is inverse or not

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

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

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

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

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