Mathematical Background

* Define basic Terminology:

A Group: Group is follow this all the property.

- Closure: $a, b \in G \Rightarrow (a * b) \in G$
- Associative: $a * (b * c) = (a * b) * c$
- Identity element: $(a * e) = (e * a)$
- Inverse element: $(a * a') = (a' * a)$

B Abelion Group: Abelian Group follow all the Group property with extra commutative property.

Commutative: $(a * b) = (b * a)$

C Rings: A Ring R denoted by $(R, +, *)$ is a set of element with two binary operation called addition and multiplication.

Ring is follow this Property

- Group, Abelian Group
- Closure under Multiplication:
  if $a, b \in R \Rightarrow ab \in R$

Brain Spot

- Associativity of multiplication:
  $a(bc) = (ab)c$
- Distributive laws:
  $a(b+c) = ab + ac$
  $(a+b)c = ac + bc$

d Commutative Rings: A Ring is said to be commutative, if it is follow this extra condition

- Commutativity of multiplication:
  $ab = ba \quad \forall a, b \in R$

e Integral Domain: An Integral domain is a commutative ring that Follow this extra condition.

- Multiplicative Identity:
  $a1 = 1a = a \quad \forall a, 1 \in R$

- No zero divisors:
  IF $a, b \in R \Rightarrow ab = 0$ then either
  $a = 0$ or $b = 0$

f Fields: A Fields is a Integral Domain that Follow this extra condition.

- Multiplicative Inverse:
  $aa^{-1} = a^{-1}a = 1$

Brain Spot

* Explain Modular Arithmetic Property.

=> This are the basic property of Modular Arithmetic.

1 We can divide a by n, we get the quotient q and remainder r.

$$a = qn + r, \quad 0 \leq r < n; \quad q = [a/n]$$

2 Congruence: $a = b \pmod{m}$

3 $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$

$[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$

$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

4 Commutative laws:

$(a * b) \bmod n = (b * a) \bmod n$

5 Associative laws:

$[(a * b) * c] \bmod n = [a * (b * c)] \bmod n$

Brain Spot

6 Distributive laws:

$[a * (b + c)] \bmod n = [(a * b) + (a * c)] \bmod n$

7 Identities: $(0 + a) \bmod n = a \bmod n$
$(1 + a) \bmod n = a \bmod n$

8 Additive Inverse: $a + (-a) = 0 \bmod n$

* Explain Enclidean Algorithm with example.

=> Enclidean Algorithm is also known as Enclid's Algorithm.

This algorithm is used to Find Greatest Comman Divisor (GCD) or Highest Comman Factor (HCF).

Method 1

=> Algorithm: Assumes $a > b > 0$

EUCLID(a, b)

1 A ← a; B ← b
2 IF B = 0 return A = gcd(a, b)
3 R = A mod B
4 A ← B
5 B ← R
6 goto 2

Brain Spot

Ex Find GCD(12, 33)

⇒ Here, we have to take Larger Number as A and smaller number as B.

So, A = 33, B = 12

1

Q	A	B	R
2	33	12	9

2 ← Q

12 | 33
-24
9 ← R

2

Q	A	B	R
2	33	12	9
1	12	9	3

1 ← Q

9 | 12
9
3 ← R

3

Q	A	B	R
2	33	12	9
1	12	9	3
3	9	3	0
X	3	0	X

3 ← Q

3 | 9
9
0 ← R

Here, we get zero. So, we have to stop.

At the last we get 3.

So, gcd(12, 33) = 3.

Brain Spot

=> Method 2 : Algorithm

Prerequisite : a > b

```
Euclid_GCD(a, b):
        if b = 0 then
            return a;
        else
            return Euclid_GCD
                (b, a mod b);
```

Ex. Find GCD(72, 33)

Here, a = 33, b = 72

GCD(a, b) = GCD(b, a mod b)

GCD(33, 72) = GCD(72, 33 mod 72)
= GCD(72, 9)

GCD(72, 9) = GCD(9, 72 mod 9)
= GCD(9, 3)

GCD(9, 3) = GCD(9, 9 mod 3)
= GCD(3, 0)

GCD(72, 33) = 3

Brain Spot

* Explain Extended Euclidean Algorithm with its example.

=> Extended Euclidean Algorithm is used to find the Multiplicative Inverse.

Multiplicative Inverse :

$$A \times A^{-1} = 1$$

=> Algorithm:

To find multiplicative inversce, if gcd(m, b) = 1 then b has multiplicative inverse modulo m.

Extended_E(m, b)

1 (A1, A2, A3) ← (1, 0, m);
(B1, B2, B3) ← (0, 1, b);

2 IF B3 = 0 => Return A3 = gcd(m, b);
no inverse.

3 IF B3 = 1 => Return B3 = gcd(m, b);
$B2 = b^{-1} \bmod m$

4 Q = [A3 / B3]

5 (T1, T2, T3) ← (A1 - QB1, A2 - QB2, A3 - QB3)

6 (A1, A2, A3) ← (B1, B2, B3)

Brain Spot

7 (B1, B2, B3) ← (T1, T2, T3)

8 goto step 2

Ex. Multiplicative Inverse of 11 mod 13

=> Here, We have to take A = 13 and B = 11 (A > B),
For First step, $T_1 = 0$ and $T_2 = 1$

Step 1:

Q	A	B	R	T_1	T_2	T
1	13	11	2	0	1	-1

$1 \leftarrow Q$

11 | 13
11

$2 \leftarrow R$

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

Step 2:

Q	A	B	R	T_1	T_2	T
1	13	11	2	0	1	-1
5	11	2	1	1	-1	6

$5 \leftarrow Q$

2 | 11
10

$1 \leftarrow R$

$T = T_1 - T_2 Q = 1 - (-1)5 = 6$

Brain Spot

Teacher's Signature

Step 3:

Q	A	B	R	T_1	T_2	T
1	13	11	2	0	1	-1
5	11	2	1	1	-1	6
2	2	1	0	-1	6	-13

$T = T_1 - T_2 Q = -1 - 6(2) = -13$

1	2 ← Q
	2
	0 ← R

Step 4:

Q	A	B	R	T_1	T_2	T
1	13	11	2	0	1	-1
5	11	2	1	1	-1	6
2	2	1	0	-1	6	-13
X	1	0	X	6	-13	X

0	1	=> stop.

Here, T_1 will be answer.
So, 6 is the Multiplicative Inverse of 11 and 13.

* Explain Fermat's Theorem.

=> Fermat's Little Theorem:

If p is a Prime number and a is a Integer not divisible by p then $a^{p-1} \equiv 1 \pmod{p}$

Brain Spot

Ex. Does Fermat's Theorem Hold true for $P=5$ and $a=2$?

=) For Fermat's Theorem, we have to check to two condition,
P is always prime number and
a is not divisible by P.

Here, $P=5$ is Prime and $a=2$ is not divisible by P.

According to Theorem,

$$a^{P-1} = 1 \pmod{p}$$

$$\therefore 2^{(5-1)} = 1 \pmod{5}$$

$$\therefore 2^4 = 1 \pmod{5}$$

$$\therefore 16 = 1 \pmod{5}$$ is true,

$$\begin{array}{r|l} & 3 \\ \hline 5 & 16 \\ & 15 \\ \hline & 1 \end{array}$$

So, Fermat's Theorem holds true for $P=5$ and $a=2$.

Brain Spot

* Explain Euler's Theorem.

=> Euler's Theorem:

For every positive integer 'a' & 'n', which are said to be relatively prime than $a^{\phi(n)} = 1 \bmod n$

For Prove this theorem, we have to find $\phi(n)$ which is called Euler's Totient Function.

There are Three condition to find $\phi(n)$, according to n's value.

1 If n is prime number then
$\phi(n) = n - 1$

2 If $n = p \times q$, p and q are Prime then $\phi(n) = (p-1) \times (q-1)$

3 Either, $\phi(n) = n \times \left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right) \cdots$

where, $P_1, P_2 \cdots$ are distinct primes.

Where, $n = a \times b$,
a and b are composite.

Brain Spot