Number theory

- Number theory forms a crucial foundation for modern cryptography and plays a vital role in cybersecurity.
- It provides the mathematical tools and principles necessary for secure communication and data protection.
- Most of the encryption is based heavily on number theory and abstract algebra concept.
- Here's how key concepts from number theory are applied:
  1. Prime Numbers
     - ✓ **Public key cryptography**, like RSA, relies heavily on large prime numbers.
  2. Modular Arithmetic
     - ✓ Operations like `a mod n` are central in encryption algorithms.
     - ✓ **Diffie-Hellman key exchange**, RSA, and elliptic curve cryptography all use modular arithmetic.
  3. Greatest Common Divisor (GCD)
     - ✓ Used to ensure keys are **co-prime** in RSA, meaning they share no common factors with the modulus.
     - ✓ **Euclidean algorithm** helps find GCD efficiently.
  4. Euler's Totient Function ($\varphi(n)$)
     - ✓ **Critical in RSA for computing the private key.**

Prime Number

- A **prime number** is a natural number greater than 1 that has **exactly two distinct factors**: 1 and itself.
- A **factor** of a number is another number that divides it **exactly**—that is, with **no remainder**.
  The factors of 6 are: 1, 2, 3, 6
  Because:
  $1 \times 6 = 6$
  $2 \times 3 = 6$
- Prime number plays very important role in cryptography.

- Examples of prime number: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...
- **Note**: 1 is **not** a prime number because it has only one factor.
- In **RSA encryption**, two large prime numbers are multiplied to create a modulus. The difficulty of factoring this large number (product of primes) ensures security.
- Facts about prime number
  - ✓ Only even prime: 2
  - ✓ Smallest prime number: 2
  - ✓ Except for 2 and 5, all prime number ends in the digit 1,3,7 or 9

Why prime numbers in cryptography?

- ✓ Many encryption algorithms are based on prime numbers.
- ✓ Very fast to multiply two large prime numbers.
- ✓ Extremely computer-intensive to do the reverse.
- ✓ Factoring very large prime numbers is very hard i.e., take computers a long time.

Composite Number

- ✓ Numbers that have more than 2 factors are called as Composite numbers
- ✓ Positive Integers that have more than 2 factors
- ✓ Numbers that are divisible by more than two numbers.
- ✓ 4, 6, 8, 9, 10, 12, 14, 15, 16, ...

Greatest Common Divisor (GCD)

- ✓ GCD of two or more integers which are not zero is the greatest positive integer that divides each of the integers.
- ✓ GCD of two numbers is the greatest number that divides both the number
- ✓ GCD of 12 and 8 is 4

  Here divisor of 12 and 8 is 2 and 4.

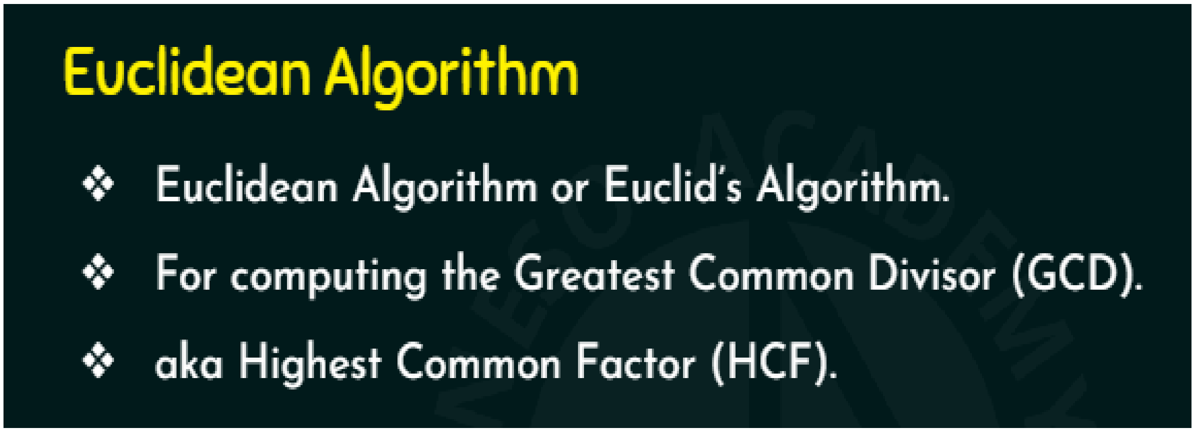
  We can divide 12 by 2 ,4, and 6.

  We can divide 8 by 2 and 4. Here **Greatest Common Divisor is 4.**

How to find GCD

- ✓ GCD by Division Method
- ✓ First take two of the given numbers, divide the greater by the smaller number and then divide the divisor by the reminder.
- ✓ The divisor which does not leave a reminder is the GCD of the two numbers.

  1. Find the **GCD** of 30 and 45.
  2. Find the **GCD** of 442 and 546.
  3. Find the **GCD** of 442, 546 and 424.



Understanding GCD – Example 1

	12	33
Divisors	1, 2, 3, 4, 6, 12	1, 3, 11, 33
Common Divisors	1, 3	
Greatest Common Divisor (GCD)	3	

∴ GCD(12, 33) = 3

Understanding GCD – Example 2

	25	150
Divisors	1, 5, 25	1, 2, 3, 5, 6, 10, 15, 25, 30, 50, 75, 150
Common Divisors	1, 5, 25	
Greatest Common Divisor (GCD)	25	

∴ GCD(25, 150) = 25

Understanding GCD – Example 3

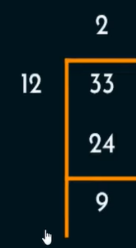
	13	31
Divisors	1, 13	1, 31
Common Divisors	1	
Greatest Common Divisor (GCD)	1	

∴ GCD(13, 31) = 1

Euclid's Algorithm for finding GCD

Find the GCD(12, 33).

Q	A	B	R
2	33	12	9



Q	A	B	R
2	33	12	9
	12	9	

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

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

$$\begin{array}{r|l} & 3 \\ \hline 3 & 9 \\ & 9 \\ \hline & 0 \end{array}$$

Euclid's Algorithm for finding GCD

GCD(12, 33) = 3.

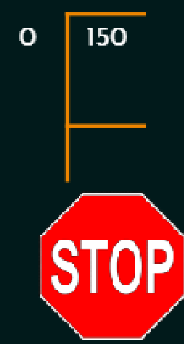
Q	A	B	R
2	33	12	9
1	12	9	3
3	9	3	0
X	3	0	X

$$\begin{array}{r|l} 0 & 3 \\ \hline & \end{array}$$

Euclid's Algorithm for finding GCD

GCD(750, 900) = 150.

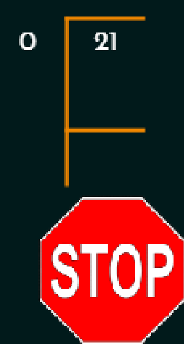
Q	A	B	R
1	900	750	150
5	750	150	0
X	$\boxed{150}$	0	X



Euclid's Algorithm for finding GCD

GCD(252, 105) = 21.

Q	A	B	R
2	252	105	42
2	105	42	21
2	42	21	0
X	$\boxed{21}$	0	X



Find the GCD(1005, 105).

Euclid's Algorithm for finding GCD

Prerequisite: a > b

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

Euclid's Algorithm – Example 1

Example 1: Find the GCD (50, 12).

Solution:

Here a=50, b=12

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

GCD (50, 12) = GCD (12, 50 mod 12) = GCD(12, 2)
GCD (12, 2) = GCD (2, 12 mod 2) = GCD(2, 0) = 2
GCD (50, 12) = 2

Euclid's Algorithm – Example 2

Example 2: Find the GCD (83, 19).

Solution:

Here a=83, b=19

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

GCD (83, 19) = GCD (19, 83 mod 19) = GCD(19, 7)
GCD (19, 7) = GCD (7, 19 mod 7) = GCD(7, 5)
GCD (7, 5) = GCD (5, 7 mod 5) = GCD(5, 2)
GCD (5, 2) = GCD (2, 5 mod 2) = GCD(2, 1)
GCD (2, 1) = GCD (1, 2 mod 1) = GCD(1, 0) = 1
GCD (83, 19) = 1

Find the GCD (529, 123).

Co-Prime Number or relatively prime

- Set of numbers that have GCD as 1 are called as Co-Prime Numbers.
- For instance, 7 and 8 are co-prime numbers.

  Here factor of 7 is 1 and 7

  And factor of 8 is 1,2,4 and 8 and in both there is only one common factor that is 1 so these two numbers 7 and 8 are co-prime number.

Two numbers are said to be relatively prime, if they have no prime factors in common, and their only common factor is 1.

❖ If GCD(a, b) = 1 then 'a' and 'b' are relatively prime numbers.

❖ Co-prime.

Question 1: Are 4 and 13 relatively prime?

Solution:

	4	13
Divisors	1, 2, 4	1, 13
Common Divisors	1	
Greatest Common Divisor (GCD)	1	

GCD(4, 13) = 1

Yes, 4 and 13 are relatively prime numbers.

Question 2: Are 15 and 21 relatively prime?

Solution:

	15	21
Divisors	1, 3, 5, 15	1, 3, 7, 21
Common Divisors	1, 3	
Greatest Common Divisor (GCD)	3	

GCD(15, 21) = 3

No, 15 and 21 are not relatively prime numbers.

Relatively Prime Numbers

a	b	GCD(a, b)	Relatively Prime?	Remarks
11	17	1	Yes	'a' and 'b' are prime
11	21	1	Yes	'a' is prime and 'b' is composite
12	77	1	Yes	'a' and 'b' are composite

Find the GCD(790, 121) using Euclid's algorithm and determine whether they are relatively prime or not.

Properties of Co-Prime Numbers

- 1 is coprime with every other number
- Prime numbers are co-prime to each other .example 3,5
- Any two successive numbers are always co-prime. example 18,19
- The sum of any two co-prime numbers is always co-prime with their product. example 2 and 3.

  2+3=5

  2*3=6, 5 and 6 are co-prime.

Euler's Totient Function (Phi Function)

Euler's Totient Function

- Denoted as $\Phi(n)$.
- $\Phi(n)$ = Number of positive integers less than 'n' that are relatively prime to n.

Solution:

Here n=5.

Numbers less than 5 are 1, 2, 3 and 4.

GCD	Relatively Prime?
GCD (1, 5) = 1	✓
GCD (2, 5) = 1	✓
GCD (3, 5) = 1	✓
GCD (4, 5) = 1	✓

$\therefore \Phi(5) = 4$.

Example 2: Find $\Phi(11)$.

Solution:

Here n=11.

Numbers less than 11 are 1, 2, 3, 4, 5, 6, 7, 8, 9 and 10.

GCD	Relatively Prime?
GCD (1, 11) = 1	✓
GCD (2, 11) = 1	✓
GCD (3, 11) = 1	✓
GCD (4, 11) = 1	✓
GCD (5, 11) = 1	✓

GCD	Relatively Prime?
GCD (6, 11) = 1	✓
GCD (7, 11) = 1	✓
GCD (8, 11) = 1	✓
GCD (9, 11) = 1	✓
GCD (10, 11) = 1	✓

$\therefore \Phi(11) = 10$.

Example 3: Find $\Phi(8)$.

Solution:

Here n=8.

Numbers less than 8 are 1, 2, 3, 4, 5, 6, and 7.

GCD	Relatively Prime?
GCD (1, 8) = 1	✓
GCD (2, 8) = 2	✗
GCD (3, 8) = 1	✓
GCD (4, 8) = 4	✗

GCD	Relatively Prime?
GCD (5, 8) = 1	✓
GCD (6, 8) = 2	✗
GCD (7, 8) = 1	✓

$\therefore \Phi(8) = 4.$

Euler's Totient Function

	Criteria of 'n'	Formula
$\Phi(n)$	'n' is prime.	$\Phi(n) = (n-1)$
	n = p x q. 'p' and 'q' are primes.	$\Phi(n) = (p-1) \times (q-1)$
	n = a x b. Either 'a' or 'b' is composite. Both 'a' and 'b' are composite.	$\Phi(n) = n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots$ where $p_1, p_2, \ldots$ are distinct primes.

Euler's Totient Function

Example 1: Find $\Phi(5)$.

Solution:

Here n=5.

'n' is a prime number.

$\Phi(n) = (n-1)$

$\Phi(5) = (5-1)$

$\Phi(5) = 4$

So, there are 4 numbers that are lesser than 5 and relatively prime to 5.

Euler's Totient Function

Example 2: Find $\Phi(31)$.

Solution:

Here n=31.

'n' is a prime number.

$\Phi(n) = (n-1)$

$\Phi(31) = (31-1)$

$\Phi(31) = 30$

So, there are 30 numbers that are lesser than 31 and relatively prime to 31.

Euler's Totient Function

Example 3: Find Φ(35).

Solution:

Here n=35.

'n' is a product of two prime numbers 5 and 7.

Let us assign p=5 and q=7.

$\Phi(n) = (p\text{-}1) \times (q\text{-}1)$

$\Phi(35) = (5\text{-}1) \times (7\text{-}1)$

$\Phi(35) = 4 \times 6$

$\Phi(35) = 24$

So, there are 24 numbers that are lesser than 35 and relatively prime to 35.

Euler's Totient Function

GCD	RP?
GCD(1,35)	✓
GCD(2,35)	✓
GCD(3,35)	✓
GCD(4,35)	✓
GCD(5,35)	✗
GCD(6,35)	✓
GCD(7,35)	✗
GCD(8,35)	✓
GCD(9,35)	✓

GCD	RP?
GCD(10,35)	✗
GCD(11,35)	✓
GCD(12,35)	✓
GCD(13,35)	✓
GCD(14,35)	✗
GCD(15,35)	✗
GCD(16,35)	✓
GCD(17,35)	✓
GCD(18,35)	✓

GCD	RP?
GCD(19,35)	✓
GCD(20,35)	✗
GCD(21,35)	✗
GCD(22,35)	✓
GCD(23,35)	✓
GCD(24,35)	✓
GCD(25,35)	✗
GCD(26,35)	✓
GCD(27,35)	✓

GCD	RP?
GCD(28,35)	✗
GCD(29,35)	✓
GCD(30,35)	✗
GCD(31,35)	✓
GCD(32,35)	✓
GCD(33,35)	✓
GCD(34,35)	✓

24

Euler's Totient Function

Example 4: Find $\Phi(1000)$.

Solution:

Here $n = 1000 = 2^3 \times 5^3$.

Distinct prime factors are 2 and 5.

$$\Phi(n) = n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots$$

$$\Phi(1000) = 1000 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$

$$\Phi(1000) = 1000 \times \left(\frac{1}{2}\right)\left(\frac{4}{5}\right)$$

$$\Phi(1000) = 400$$

Euler's Totient Function

Example 5: Find $\Phi(7000)$.

Solution:

Here $n = 7000 = 2^3 \times 5^3 \times 7^1$

Distinct prime factors are 2, 5 and 7.

$$\Phi(n) = n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right) \dots$$

$$\Phi(7000) = 7000 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)$$

$$\Phi(7000) = 7000 \times \left(\frac{1}{2}\right)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right)$$

$$\Phi(7000) = 2400$$

1. Find $\Phi(369)$.
2. Find $\Phi(372)$.