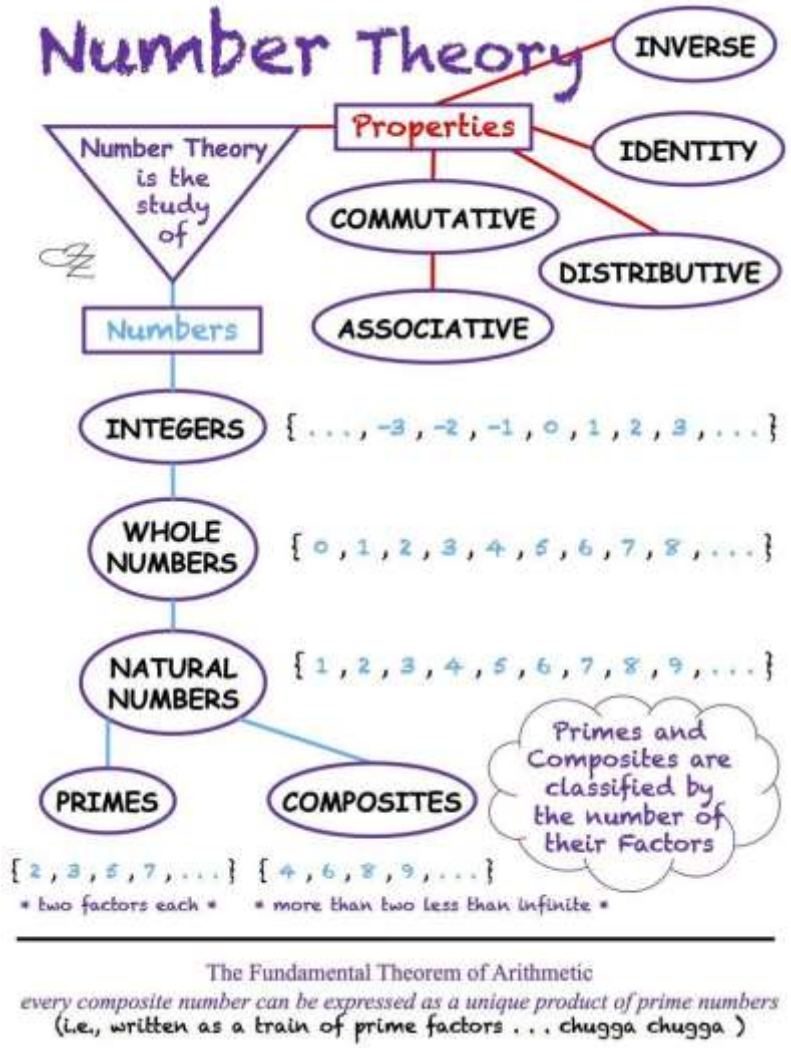
23MA301: MATHEMATICAL STATISTICAL FOUNDATION

Topic: BASICS OF NUMBER THEORY

Mrs. K.Srividya

Assistant Professor, Freshman engineering
Narsimha Reddy Engineering College (Autonomous)
Secunderabad, Telangana, India- 500100.

Basics of Number Theory :

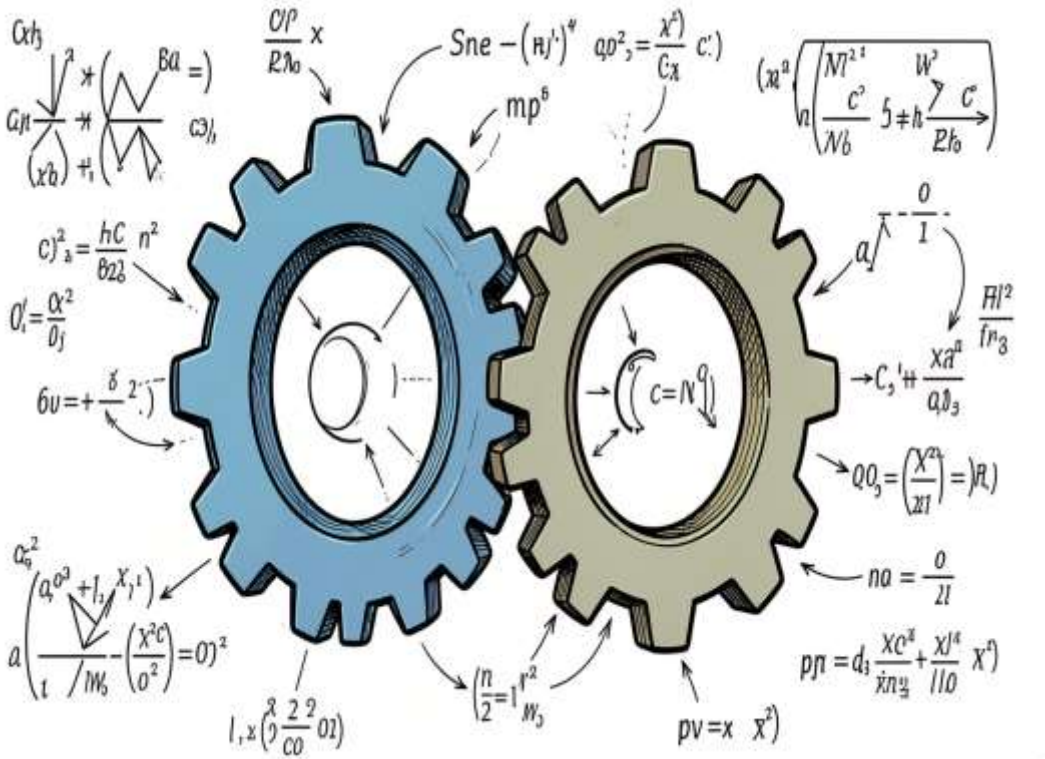


Number Theory is the branch of mathematics that studies **integers (whole numbers)** and their properties, such as divisibility, prime numbers, factors, and remainders. It forms the basis of modern cryptography and many mathematical algorithms.

Prime and Composite Numbers

- **Prime number:** Has exactly **two factors** (1 and itself).
  - Examples: **2, 3, 5, 7, 11, 13**
- **Composite number:** Has more than two factors.
  - Examples: **4, 6, 8, 9, 10**
- **1** is neither prime nor composite.
- **2** is the only even prime number

Greatest Common Divisors :



The **greatest common divisor** of two integers *a* and *b*, not both zero, is the largest positive integer dividing both. Notation: *gcd(a,b)*.

Example: *gcd(48,18) = 6*, since 6 is the largest integer dividing both 48 and 18.

Two integers are **relatively prime** when *gcd(a,b) = 1*.

The Euclidean Algorithm :

- fast, systematic method for computing *gcd(a,b)* using repeated division. At each step, replace the pair *(a,b)* with *(b, a \ bmod b)* until the remainder is zero.

Compute remainder r

Calculate r = a mod b.

Replace pair

Set a := b and b := r.

Start with a & b

a > b; prepare initial pair.

Terminate at r=0

When r=0, gcd is last nonzero remainder.

```
Example:
48 = 18×2 +12
18 = 12×1 +6
12 = 6×2 +0

GCD = 6
```

The algorithm terminates in at most *log_2 b* steps, making it highly efficient even for large integers.

The Fundamental Theorem of Arithmetic

Every integer greater than 1 is either a prime number or can be expressed as a unique product of prime numbers (except for the order of the factors).

Existence

Every $n > 1$ has at least one prime factorization.

Uniqueness

No integer has two distinct prime factorizations.

Formula

$$n = p_1^{a_1} \times p_2^{a_2} \times p_3^{a_3} \times \cdots \times p_k^{a_k}$$

Where:

$n > 1$ is a positive integer.

$p_1, p_2, \ldots, p_k$ are **distinct prime numbers.**

$a_1, a_2, \ldots, a_k$ are **positive integers (exponents).**

Fermat Number :

A **Fermat number** is a positive integer of the form

$$F_n = 2^{2^n} + 1, n = 0,1,2,3, \ldots$$

where: F_n= the n^{th}Fermat number

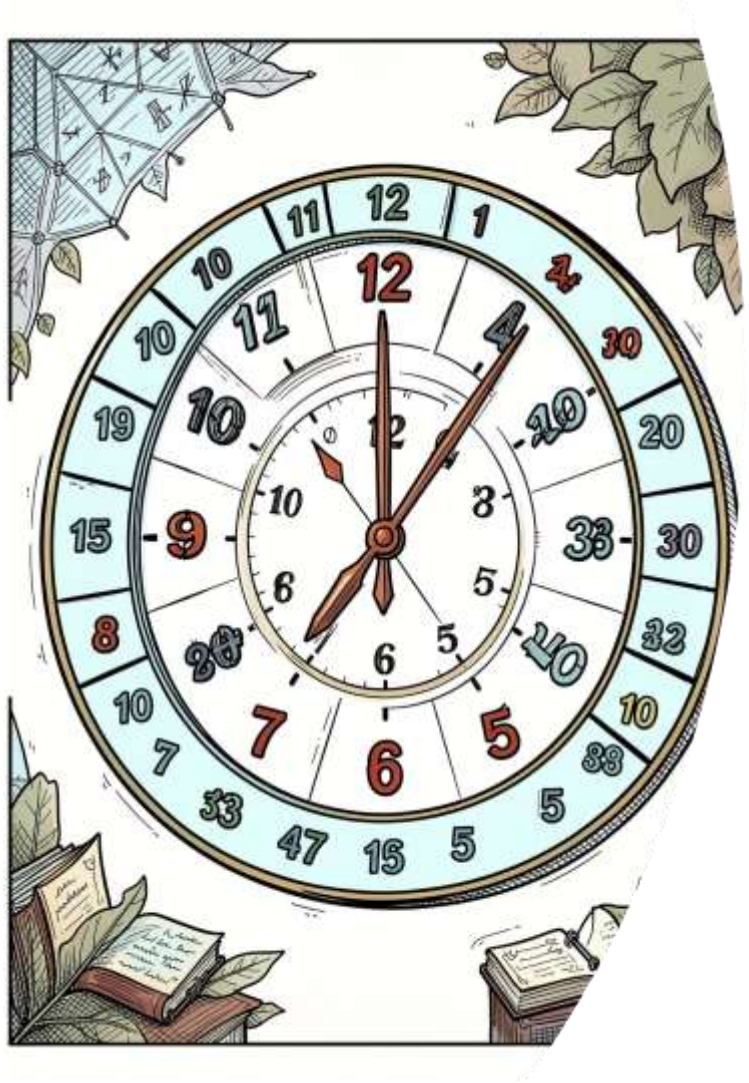
n= a non-negative integer $(0,1,2, \ldots)$

The First Five Fermat Numbers are :

n	Formula	Value
0	$2^1 + 1$	**3**
1	$2^2 + 1$	**5**
2	$2^4 + 1$	**17**
3	$2^8 + 1$	**257**
4	$2^{16} + 1$	**65537**
5	$2^{32} + 1$	**429496729**

Introduction to Congruences

:



Two integers a and b are **congruent modulo** m if m divides their difference:

$$a \equiv b \pmod{m} \quad \text{if} \quad m \mid (a - b)$$

Intuition: a and b leave the **same remainder** when divided by m

Arithmetic : Congruences respect addition, subtraction, and multiplication

Example

- $17 \equiv 5 \pmod{12}$
- Since $17 - 5 = 12$, which is divisible by 12.

Definition of Linear Congruence

A **linear congruence** is a congruence equation of the form

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

where

- a, b, and m are integers,
- $m > 1$ is called the **modulus**,
- x is the unknown integer to be determined.

A solution is an integer x that satisfies the congruence.

General Form

$$\boxed{ax \equiv b \pmod{m}}$$

where

- a= coefficient of x, b= constant , m= modulus , x= unknown variable

Condition for Existence

Let $d = \gcd(a, m)$

A solution exists **iff** $d \mid b$

Number of Solutions

If $d = \gcd(a, m)$

then the congruence has exactly d distinct solutions modulo m.

Exmample: Solve $3x \equiv 5 \pmod 7$

Since the inverse of 3 modulo 7 is 5,

$$3^{-1} \equiv 5 \pmod 7$$

Multiply both sides by 5:

$$x \equiv 5 \times 5 \equiv 25 \equiv 4 \pmod 7$$

Answer:

$$\boxed{x \equiv 4 \pmod 7}$$

Verification:

$$3(4) = 12, \qquad 12 \equiv 5 \pmod 7$$

Hence,

$x = 4$is the correct solution.

L-I-N-E-A-R

- **L** – Linear form: $ax \equiv b \pmod{m}$
- **I** – Inverse is needed when $\gcd(a, m) = 1$
- **N** – Number of solutions = $\gcd(a, m)$
- **E** – Existence only if $\gcd(a, m) \mid b$
- **A** – Arithmetic is performed modulo m
- **R** – Reduce the final answer modulo m

Key Takeaways

GCD & Euclidean Algorithm

Efficiently compute *gcd(a,b)* via repeated division — the last nonzero remainder is the answer.

Fundamental Theorem

Every integer *n > 1* has a **unique** prime factorization — the cornerstone of arithmetic.

Congruences

a ≡ b (mod m) means *a* and *b* share the same remainder modulo *m*.

Linear Congruences

`ax≡b(modm)` is solvable iff *gcd(a,m)\ mid b*, yielding *\gcd(a,m)* solutions.

Thank You..