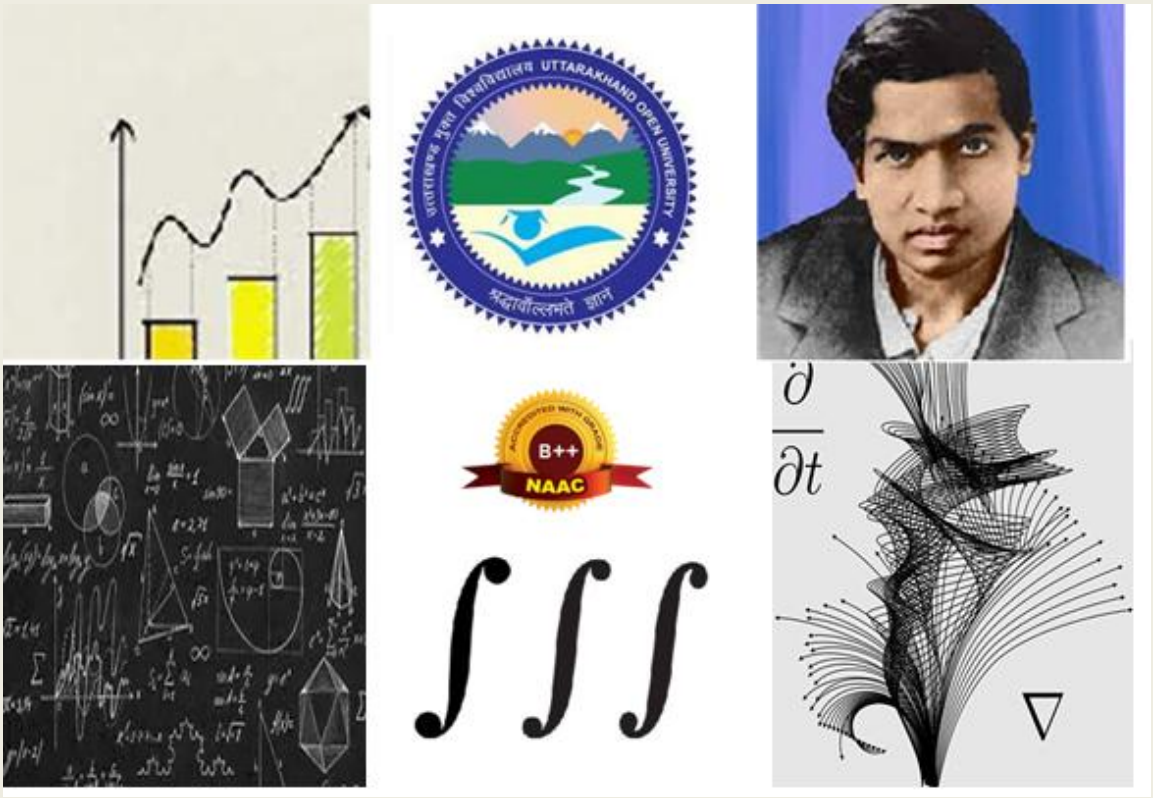
# Master of Science

## Mathematics

## Fourth Semester

# MAT 606
# NUMBER THEORY




**DEPARTMENT OF MATHEMATICS**
**SCHOOL OF SCIENCES**
**UTTARAKHAND OPEN UNIVERSITY**
**HALDWANI, UTTARAKHAND**
**263139**

# COURSE NAME: NUMBER THEORY

# COURSE CODE: MAT 606

**Department of Mathematics**
**School of Science**
**Uttarakhand Open University**
**Haldwani, Uttarakhand, India,**
**263139**

# NUMBER THEORTY MAT 606

**BOARD OF STUDIES - 2023**



**Editor**


**Dr. Deepak Kumar Sharma**
Assistant Professor (AC)
Department of Mathematics
**Uttarakhand Open University**
Haldwani, Uttarakhand


| Unit Writer | Blocks | Units |
|---|---|---|
| **Dr. Deepak Kumar Sharma**<br>Assistant Professor (AC)<br>Department of Mathematics<br>Uttarakhand Open University<br>Haldwani, Uttarakhand | I, II & IV | 1, 2, 5, 12, 13, 14 and 15 |
| **Prof. Arvind Bhatt**<br>Department of Mathematics<br>**Uttarakhand Open University**<br>Haldwani, Uttarakhand | I | 3 and 4 |
| **Dr. Kamlesh Bisht**<br>Assistant Professor (AC)<br>Department of Mathematics<br>**Uttarakhand Open University**<br>Haldwani, Uttarakhand | II & III | 6, 7, 8, 9, 10 and 11 |

# CONTENTS
# MAT - 606

# COURSE INFORMATION

The present self-learning material **"Number Theory"** has been designed for **M.Sc. (IV Semester)** learners of Uttarakhand Open University, Haldwani. This course is divided into 15 units of study. This Self Learning Material is a mixture of Four Block.

First block is **Distribution of Primes and Theory of Congruencies,** in this block Divisibility theory, Linear Diophantine equation, Twin-prime conjecture, Odd perfect numbers conjecture, Fermat and Congruence relation and its properties, Linear congruence and Chinese remainder theorem, Fermat's little theorem, Wilson's theorem.

Second block is **The Number theoretic Function,** in this block Number theoretic functions for sum and number of divisors, Multiplicative function, The Möbius inversion formula, Greatest integer function, Euler's phi-function and properties, Euler's theorem. defined clearly.

Third block is **Primitives roots,** in this block Order of an integer modulo n, Primitive roots for primes, Composite numbers having primitive roots, Perfect Number, Mersenne prime. Definition of quadratic residue of an odd prime, Euler's criterion are defined.

Fourth block is **Quadratic Reciprocity Law,** in this block The Legendre symbol and its properties, Quadratic reciprocity Law, Quadratic congruencies with composite moduli. Public key encryption, RSA encryption and decryption with applications in security systems.

Adequate number of illustrative examples and exercises have also been included to enable the leaners to grasp the subject easily.

# COURSE NAME: NUMBER THEORY

## COURSE CODE: MAT-606

# BLOCK - I: DISTRIBUTION OF PRIMES AND THEORY OF CONGRUENCIES

# UNIT-1: DIVISIBILITY THEORY AND LINEAR DIOPHANTINE EQUATION

## CONTENTS:



## 1.1 *INTRODUCTION*

Divisibility theory is one of the fundamental topics in Number Theory. It studies the divisibility properties of integers and forms the basis for concepts such as prime numbers, greatest common divisors, congruences, and Diophantine equations. In mathematics, a Diophantine equation is a polynomial equation with integer coefficients, for which only integer solutions are of interest. A linear Diophantine equation equates the sum of two or more unknowns, with coefficients, to a constant. An exponential Diophantine equation is one in which unknowns can appear in exponents. Diophantine problems have fewer equations than unknowns and involve finding integers that solve all equations simultaneously. Because such systems of equations define algebraic curves, algebraic surfaces, or, more generally, algebraic sets, their study is a part of algebraic geometry that is called Diophantine geometry.

In mathematics, the prime number theorem (PNT) describes the asymptotic distribution of prime numbers among the positive integers. It formalizes the intuitive idea that primes become less common as they become larger by precisely quantifying the rate at which this occurs. The theorem was proved independently by Jacques Hadamard and Charles Jean de la Vallée Poussin in 1896 using ideas introduced by Bernhard Riemann (in particular, the Riemann zeta function).

## 1.2 *OBJECTIVE*

After reading this unit you will be able to:

- Divisibility theory
- Division Algorithm
- Greatest Common Divisor
- Least Common Multiple
- Linear Diophantine equation

## 1.3 *DIVISIBILITY THEORY*

**Definition:** Let $a$ and $b$ be integers with $a \neq 0$. We say that **a divides b**, written as

$$a \mid b$$

if there exists an integer $k$such that

$$b = ak.$$

If no such integer exists, we write

$$a \nmid b.$$

**Examples:**

- $3 \mid 12$because $12 = 3 \times 4$.
- $5 \nmid 12$.

**Basic Properties of Divisibility**

For integers $a, b,$and $c$:

1. If $a \mid b$and $a \mid c$, then $a \mid (b + c)$.
2. If $a \mid b$, then $a \mid bc$.
3. If $a \mid b$and $b \mid c$, then $a \mid c$.
4. If $a \mid b$and $a \mid c$, then $a \mid (mb + nc)$for all integers $m, n$.

**Theorem 1.1:** If $c = ax + by$ and $d \mid a$ but $d \nmid c$ then $d \nmid b$.

**Proof:** we have $d \mid a \Longrightarrow \exists$ an integer $q_1$ such that

$$a = dq_1$$

Therefore, $$a = ax + by = dq_1 + by$$

Suppose $d \mid b \Longrightarrow \exists$ an integer $q_2$ such that $b = dq_2$

Therefore, $c = dq_1x + dq_2y = d(q_1x + q_2y)$

$\Rightarrow d|c$

Contrapositively $d \nmid c \Rightarrow d \nmid b$.

**Theorem 1.2:** If integer $b$ divides a positive integer $a$ then $b$ is not numerically greater than $a$.

**Proof:** we have

$d \mid b \Rightarrow \exists$ an integer $q$ (with $|q| \geq 1$)

Such that $a = bq$

Hence, $a = |a| = |bq| = |b||q| \geq |b|$.

## 1.4 *DIVISON ALGORITHM*

For any integers $a$and $b > 0$, there exist unique integers $q$and $r$such that

$$a = bq + r,$$

Where,

$$0 \leq r < b.$$

**Proof**

Let

$$S = \{a - bk \mid a - bk \geq 0, k \in \mathbb{Z}\}.$$

Since $S$is a non-empty set of non-negative integers, by the Well-Ordering Principle it contains a least element $r$.

Then

$$r = a - bq$$

for some integer $q$.

Thus,

$$a = bq + r.$$

If $r \geq b$, then

$$r - b = a - b(q + 1) \geq 0,$$

which contradicts the minimality of $r$.

Hence

$$0 \leq r < b.$$

Uniqueness follows by assuming

$$a = bq_1 + r_1 = bq_2 + r_2$$

and showing $q_1 = q_2$and $r_1 = r_2$.

Hence proved.

**Theorem 1.3:** The square of an odd integer is of the form $8q + 1$.

**Proof:** Let $n$ be an odd integer.

Then there exists an integer $k$ such that

$$n = 2k + 1.$$

Squaring both sides, we get

$$n^2 = (2k + 1)^2.$$

Expanding,

$$n^2 = 4k^2 + 4k + 1.$$

Factor out 4 from the first two terms:

$$n^2 = 4k(k + 1) + 1.$$

Since $k$ and $k + 1$are consecutive integers, one of them must be even. Therefore,

$$k(k + 1) = 2q$$

for some integer $q$.
Substituting this into the expression for $n^2$,

$$n^2 = 4(2q) + 1.$$

Hence,

$$n^2 = 8q + 1.$$

Therefore, the square of every odd integer is of the form

$$\boxed{8q + 1}$$

for some integer $q$.
**Example:** Take the odd integer 7.

$$7^2 = 49 = 8(6) + 1.$$

Take the odd integer 11.

$$11^2 = 121 = 8(15) + 1.$$

Thus, the theorem is verified.

**Theorem 1.4:** One of every three consecutive integers is divisible by 3.
**Proof:** Let the three consecutive integers be

$$n, n + 1, n + 2.$$

By the Division Algorithm, when an integer $n$ is divided by 3, the remainder is either 0, 1, or 2.
We consider the following cases:
**Case 1: $n = 3q$**
Then $n$is divisible by 3.
**Case 2: $n = 3q + 1$**
Then

$$n + 2 = 3q + 3 = 3(q + 1),$$

which is divisible by 3.

**Case 3: $n = 3q + 2$**
Then

$$n + 1 = 3q + 3 = 3(q + 1),$$

which is divisible by 3.
Thus, in every possible case, one of the integers among

$$n,\ n + 1,\ n + 2$$

is divisible by 3.
Therefore, One of every three consecutive integers is divisible by 3.
**Example:** Consider the consecutive integers:

- $7, 8, 9 \rightarrow$ 9 is divisible by 3.
- $14, 15, 16 \rightarrow$ 15 is divisible by 3.
- $25, 26, 27 \rightarrow$ 27 is divisible by 3.

Hence the result is verified.

**Theorem 1.5:** The product of any three consecutive integers is divisible by 3 !.
**Proof:** Let the three consecutive integers be

$$n, n + 1, n + 2.$$

Their product is

$$P = n(n + 1)(n + 2).$$

To show that $P$is divisible by 6, we must show that it is divisible by both 2and 3.
**Divisibility by 2**
Among any two consecutive integers, one is even. Therefore, among the three consecutive integers $n$, $n + 1$, and $n + 2$, at least one is even.
Hence,

$$2 \mid P.$$

Divisibility by 3
From the theorem that one of every three consecutive integers is divisible by 3, one of $n$, $n + 1$, or $n + 2$is divisible by 3.
Hence,

$$3 \mid P.$$

Since 2and 3are relatively prime, and $P$is divisible by both 2and 3, it follows that

$$6 = 2 \times 3 \mid P.$$

Therefore,

$$6 \mid n(n + 1)(n + 2).$$

Since $3! = 6$,

$$3! \mid n(n + 1)(n + 2)$$

Hence, the product of any three consecutive integers is divisible by 3 !.

**Example:** Take the consecutive integers $4, 5, 6$.

$$4 \times 5 \times 6 = 120.$$

Since

$$120 = 6 \times 20,$$

the product is divisible by $3! = 6$. Thus, the theorem is verified.

**Remark: Applications of Divisibility Theory**

- Prime number testing
- Cryptography and information security
- RSA encryption
- Congruence equations
- Diophantine equations
- Computer algorithms
- Coding theory

## 1.5 *GREATEST COMMON DIVISOR*

The **Greatest Common Divisor (GCD)** of two integers $a$ and $b$, not both zero, is the largest positive integer that divides both $a$ and $b$.
It is denoted by

$$\gcd(a, b) \text{ or simply } (a, b).$$

**Important Properties of GCD**

1. $\gcd(a, b) = \gcd(b, a)$
2. $\gcd(a, 0) = |a|$
3. $\gcd(a, b) = \gcd(a - b, b)$
4. $\gcd(a, b) = \gcd(a + kb, b)$ for any integer $k$
5. If $\gcd(a, b) = 1$, then $a$ and $b$ are called **relatively prime**.

**Example:** The divisors of 24 are

$$1, 2, 3, 4, 6, 8, 12, 24$$

and the divisors of 36 are

$$1, 2, 3, 4, 6, 9, 12, 18, 36.$$

The common divisors are

$$1, 2, 3, 4, 6, 12.$$

Therefore,

$$\gcd(24, 36) = 12.$$

**Theorem 1.6:** If $d = \gcd(a, b)$, then $d \mid a$ and $d \mid b$.

Moreover, if $c \mid a$ and $c \mid b$, then $c \mid d$.

**Proof**

Since $d = \gcd(a, b)$, by definition $d$ is a common divisor of $a$ and $b$. Thus,

$$d \mid a, \qquad d \mid b.$$

Also, every common divisor of a and b must divide the greatest common divisor d. Hence proved.

**Theorem 1.7: Euclid's Algorithm:**

Let $a$ and $b$ be positive integers with $a > b$. If

$$a = bq + r, 0 \leq r < b,$$

Then $$\gcd(a, b) = \gcd(b, r).$$

**Proof:**

Let $d = \gcd(a, b)$.

Then $d$ divides both $a$ and $b$. Therefore,

$$d \mid a \text{and} d \mid b.$$

Since $a = bq + r,$

we have $r = a - bq.$

Because $d$ divides both $a$and $b$, it must divide any linear combination of $a$ and $b$.

Hence,

$$d \mid (a - bq).$$

Therefore, $\mathrm{d} \mid \mathrm{r}.$

Thus, d is a common divisor of band r.

Hence, $\mathrm{d} \leq \gcd(\mathrm{b}, \mathrm{r}).$

Now let $\mathrm{d}' = \gcd(\mathrm{b}, \mathrm{r}).$

Then $\mathrm{d}' \mid \mathrm{b} \text{and} \mathrm{d}' \mid \mathrm{r}.$

Since $\mathrm{a} = \mathrm{bq} + \mathrm{r},$

and $\mathrm{d}'$divides both band r, it follows that

Therefore,

$$d' \mid a.$$

Thus, $d'$is a common divisor of $a$and $b$, which implies

$$d' \leq \gcd(a, b).$$

Hence,

$$\gcd(b, r) \leq \gcd(a, b).$$

Combining both inequalities,

$$\gcd(a, b) \leq \gcd(b, r)$$

and

$$\gcd(b, r) \leq \gcd(a, b),$$

we obtain

$$\boxed{\gcd(a, b) = \gcd(b, r)}.$$

Therefore, the theorem is proved.

**Example:** Find $\gcd(252, 105)$.

**Solution:** $252 = 105(2) + 42$
Therefore, $\gcd(252,105) = \gcd(105,42)$.
Next, $105 = 42(2) + 21$
so, $\gcd(105,42) = \gcd(42,21)$.
Finally, $42 = 21(2) + 0$.
Hence, $\boxed{\gcd(252,105) = 21}$.

## 1.6 *LEAST COMMON MULTIPLE*

The **Least Common Multiple (LCM)** of two non-zero integers $a$and $b$is the smallest positive integer that is divisible by both $a$and $b$.
It is denoted by $\text{lcm}(a, b)$.
**Example:** Find the LCM of 12 and 18.
Multiples of 12:

$$12, 24, 36, 48, 60, \ldots$$

Multiples of 18: $18, 36, 54, 72, \ldots$

The smallest common multiple is 36.

Therefore, $\text{lcm}(12,18) = 36$.
**Example:** Find the LCM of 24 and 36.
Prime factorizations: $24 = 2^3 \times 3$
$36 = 2^2 \times 3^2$
Take the highest power of each prime:

$$\text{lcm}(24,36) = 2^3 \times 3^2$$
$$= 8 \times 9$$
$$= 72.$$

Hence, $\text{lcm}(24,36) = 72$.
**Relation Between GCD and LCM**
**Theorem:** For any two positive integers $a$and $b$,

$$\gcd(a, b) \times \text{lcm}(a, b) = ab.$$

**Proof:** Let

$$d = \gcd(a, b).$$

Then there exist relatively prime integers $m$and $n$such that

$$a = dm, b = dn.$$

Since $m$ and $n$ are relatively prime,

$$\text{lcm}(a, b) = dmn.$$

Therefore,

$$\gcd(a, b) \times \text{lcm}(a, b) = d \times (dmn) = d^2mn.$$

But

$$ab = (dm)(dn) = d^2mn.$$

Hence, $\gcd(a,b) \times \text{lcm}(a,b) = ab$
Thus proved.

**Example:** Find the LCM of 84 and 126.
For gcd

$$84 = 2^2 \times 3 \times 7$$
$$126 = 2 \times 3^2 \times 7$$

Therefore,

$$\gcd(84,126) = 42.$$

Using

$$\text{lcm}(a,b) = \frac{ab}{\gcd(a,b)},$$

we get

$$\text{lcm}(84,126) = \frac{84 \times 126}{42} = 252.$$

Hence, $\text{lcm}(84,126) = 252.$

**Properties of LCM**

1. $\text{lcm}(a,b) = \text{lcm}(b,a)$
2. $\text{lcm}(a,a) = a$
3. If $a \mid b$, then $\text{lcm}(a,b) = b$.
4. For relatively prime integers $a$and $b$, $\text{lcm}(a,b) = ab$.
5. $\gcd(a,b) \times \text{lcm}(a,b) = ab$.

## 1.7 *LINEAR DIOPHANTINE EQUATION*

A Diophantine equation is an indeterminate polynomial equation that allows the variables to be integers only. Diophantine problems have fewer equations that unknowns variable and involve finding integers that work correctly for all equations. They are named after the Hellenistic Mathematician Diophantine of Alexandria. The mathematical study of Diophantine problems is called Diophantine Analysis. The formulation of general theories of Diophantine equations was an achievement of the twentieth century. There are Diophantine equations which possess no solutions, finite number of solution or infinite number of solutions. The motivation to study more equations in one or more unknowns having only integral solutions lead to the origin of Diophantine equation as a polynomial equation with Integral co-efficient which is solvable in integers.

**Definition:** A **Linear Diophantine Equation** is an equation of the form $ax + by = c$ where $a$, $b$, and $c$are given integers, and the solutions $x$and $y$are required to be integers. The name "Diophantine" comes from the Greek mathematician Diophantus, who studied equations whose solutions are restricted to integers.

**Theorem: (Existence of Solutions)** The linear Diophantine equation $ax + by = c$ has an integer solution if and only if $\gcd(a, b) \mid c$.

**Proof:** Let $d = \gcd(a, b)$.
Suppose $ax + by = c$ has an integer solution.

Since $d \mid a$and $d \mid b$, $d$ divides every linear combination of $a$ and $b$. Therefore,

$$d \mid (ax + by).$$

Hence, $d \mid c$. Thus, $\gcd(a, b) \mid c$.
Conversely, suppose $d = \gcd(a, b)$
and $d \mid c$.
Then $c = dk$ for some integer $k$. By Bézout's Identity, there exist integers $m$and $n$such that $am + bn = d$.

Multiplying by $k$, $a(mk) + b(nk) = dk = c$.

Hence, $x = mk, y = nk$ is an integer solution.

Therefore, $\gcd(a, b) \mid c$ is the necessary and sufficient condition for solvability.

Hence proved.

**Remark: Method of Solution**
To solve $ax + by = c$, follow these steps:
**1.** Find $d = \gcd(a, b)$.
**2.** Check whether $d \mid c$.
**3.** Use the Euclidean Algorithm to find one solution.
**4.** Obtain all solutions using the general formula.
**Example 1** Solve $15x + 21y = 12$.
**Solution: Step 1:** $\gcd(15,21) = 3$.
Since $3 \mid 12$, solutions exist.
**Step 2: Find a Particular Solution**

Using Euclid's Algorithm: $15 = 6(2) + 3$
$6 = 3(2) + 0.$

Thus, $3 = 15 - 2(6)$
$= 15 - 2(21 - 15)$
$= 3(15) - 2(21)$

Multiplying by 4: $12 = 12(15) - 8(21).$

Hence, $x_0 = 12, y_0 = -8.$

**General Solution** If $d = \gcd(a, b)$,

and $(x_0, y_0)$ is one solution, then all integer solutions are

$$x = x_0 + \frac{b}{d}t,$$
$$y = y_0 - \frac{a}{d}t, \quad \text{where } t \in \mathbb{Z}.$$

Therefore $x = 12 + 7t,$
$y = -8 - 5t.$ Is a general solution.

**Example 2** Solve $18x + 30y = 6.$

**Solution:** Since $\gcd(18,30) = 6,$
and $6 \mid 6$, then solutions exist.

Dividing by 6: $3x + 5y = 1.$

One solution is $x = 2, y = -1.$

General solution: $x = 2 + 5t,$
$y = -1 - 3t,$ where $t \in \mathbb{Z}.$

**Corollary.** If gcd (a, b) = 1 and if $x_0$, $y_0$ is a particular solution of the linear Diophantine equation ax + by = c, then all solutions are given by

$x = x_0 + bt$ $y = y_0 - at$ for integral values of t.

**Applications**

Linear Diophantine equations are used in:

1. Number Theory
2. Cryptography
3. Congruences
4. Computer Science
5. Coding Theory
6. Optimization Problems

## CHECK YOUR PROGRESS

**MCQ Questions**

**Problem 1.** The equation $ax + by = c$ has an integer solution if:

(A) $a \mid c$

(B) $b \mid c$
(C) $\gcd(a, b) \mid c$
(D) $a + b = c$

**Problem 2.** The equation $6x + 9y = 4$ has:
(A) One solution
(B) No integer solution
(C) Two solutions
(D) Infinite prime solutions

**Problem 3.** A linear Diophantine equation is an equation whose solutions are:
(A) Real numbers
(B) Rational numbers
(C) Complex numbers
(D) Integers

**Problem 4.** If $\gcd(a, b) = 1$, then $a$and $b$are:
(A) Composite
(B) Equal
(C) Relatively Prime
(D) Odd

**Problem 5.** $\gcd(24, 36)$ equals:
(A) 6
(B) 8
(C) 12
(D) 18

## 1.8 *SUMMARY*

**(i)** Diophantine equations are a central topic in number theory that study integer solutions of algebraic equations. Their close relationship with divisibility, GCD, and the Euclidean Algorithm makes them an essential tool in both pure mathematics and modern applications such as cryptography and information security.

**(ii) Divisibility Theory** is a fundamental branch of Number Theory that studies the divisibility properties of integers. It provides the foundation for understanding prime numbers, factorization, greatest common divisors, least common multiples, congruences, and Diophantine equations.

**(iii)** A central concept in divisibility theory is that of **prime numbers**. A prime number is an integer greater than 1 that has exactly two positive divisors, namely 1 and itself. Every integer greater than 1 can be expressed uniquely as a product of prime numbers, a result known as the **Fundamental Theorem of Arithmetic**.

**(iv)** The concepts of **Greatest Common Divisor (GCD)** and **Least Common Multiple (LCM)** are also important. The GCD of two integers is the largest integer that divides both numbers, while the LCM is the smallest positive integer divisible by both. These quantities are related by the formula

$$\gcd(a,b) \times \operatorname{lcm}(a,b) = ab.$$

## 1.9 *GLOSSARY*

- Integer
- Divisibility
- Divisor (Factor)
- Remainder

## 1.10 *REFERENCES*


- **Burton, D. M.** (2007). Elementary number theory (6th ed.). McGraw-Hill.
- **T. M. Apostol**, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford.
- **Tom M. Apostol**, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York.
- **G. A. Jones and J. M. Jones**, *Elementary Number Theory*, Springer-Verlag, Berlin, 1998.
- **T. Nagell**, *Introduction to Number Theory*, Wiley, New York.


## 1.11 *SUGGESTED READING*


- **Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery**, *An Introduction to the Theory of Numbers*, John Wiley & Sons.
- **Hugh L. Montgomery and Robert C. Vaughan**, *Multiplicative Number Theory I: Classical Theory*, Cambridge University Press.
- **H. Iwaniec and E. Kowalski**, *Analytic Number Theory*, American

Mathematical Society, 2004.

- **T. Koshy**, *Elementary Number Theory with Applications*, Academic Press.
- **Eric W. Weisstein**, "Möbius Inversion Formula," *MathWorld – Wolfram Resource*.

## 1.12 *TERMINAL QUESTIONS*

**Long answer type questions**

**1:** Solve $14x + 35y = 7$.

**2.** Solve $24x + 30y = 18$.

**3.** Find all integer solutions of $18x + 30y = 6$.

**4.** Show that if $a \mid b$, then lcm $(a, b) = b$.

**Short answer type questions**

**1.** Define a Linear Diophantine Equation.

**2.** State the solvability condition for $ax + by = c$.

**3.** Find gcd (24,36).

**4.** Determine whether $12x + 18y = 5$ has an integer solution.

**5.** What is the LCM of two relatively prime numbers?

## 1.13 *ANSWERS*

**Answer of objective questions**

**1:** C **2:** B **3:** D **4:** C

**5:** C

# UNIT-2: PRIMES AND THEIR DISTRIBUTIONS

## CONTENTS:



## 2.1 *INTRODUCTION*

Prime numbers have fascinated mathematicians for more than 2,000 years. A **prime number** is a natural number greater than 1 that has exactly two distinct positive divisors: 1 and itself.

- **Ancient Period**: The study of prime numbers began with the ancient Greeks. Around 300 BCE, Euclid gave the first known proof that there are infinitely many prime numbers in his famous work Elements. Eratosthenes developed the Sieve of Eratosthenes, an efficient method for finding prime numbers.
- **17th Century:** Interest in prime numbers increased significantly. Pierre de Fermat studied special primes now known as Fermat numbers and proposed several important theorems. Marin Mersenne investigated numbers of the form $2^p - 1$, known today as Mersenne primes.

- **18th Century:** Leonhard Euler made major contributions to prime number theory. Euler proved important results connecting prime numbers with infinite series and established the divergence of the sum of reciprocals of primes.
- **19th Century**

Carl Friedrich Gauss and Adrien-Marie Legendre studied the distribution of primes. Their work led to the development of the Prime Number Theorem, which describes how primes are distributed among the integers. Bernhard Riemann introduced the Riemann Hypothesis in 1859, one of the most important unsolved problems in mathematics.

- **20th Century:** In 1896, the Prime Number Theorem was independently proved by Jacques Hadamard and Charles Jean de la Vallée-Poussin. New techniques in analytic number theory greatly advanced the study of primes. Computers enabled the discovery of increasingly large prime numbers.
- **Modern Era:** Prime numbers play a crucial role in cryptography, especially in systems such as RSA Cryptosystem. Research continues on problems such as the Goldbach Conjecture, the Twin Prime Conjecture, and the Riemann Hypothesis.

Large prime numbers are regularly discovered using advanced computational methods.

## 2.2 *OBJECTIVE*

After reading this unit you will be able to:
$(i)$ Prime numbers
$(ii)$ Twin primes
$(iii)$ Odd perfect number

## 2.3 *PRIME NUMBER*

A **prime number** is a natural number greater than 1 that has exactly two positive divisors: 1 and itself.
**Examples:** 2, 3, 5, 7, 11, 13, 17, 19, ...
A positive integer greater than 1 that is not prime is called a **composite number**.
**Examples:** 4, 6, 8, 9, 10, 12, 14, 15, ...

## 2.4 *DISTRIBUTION OF PRIME NUMBERS*

The **distribution of prime numbers** is one of the central topics in number theory. It studies how prime numbers are spread among the positive integers. Although primes appear irregularly, deep mathematical results show that their overall distribution follows certain predictable patterns.

**Prime Counting Function**

The distribution of primes is described by the **prime counting function**:

$$\pi(x) = \#\{p \leq x : p \text{ is prime}\}$$

where $\pi(x)$denotes the number of prime numbers less than or equal to $x$.

**Examples:**

| $x$ | $\pi(x)$ |
|---|---|
| 10 | 4 |
| 20 | 8 |
| 50 | 15 |
| 100 | 25 |

**Remark: Density of Prime Numbers**

As numbers become larger, primes become less frequent.

For a large integer $n$, the probability that $n$ is prime is approximately $\frac{1}{\log n}$

This shows that the density of primes decreases slowly as $n$ increases.

**Remark: Prime Number Theorem (PNT)**

The most important theorem concerning the distribution of primes is the Prime Number Theorem.

**Statement**

As $x \to \infty$,

$$\pi(x) \sim \frac{x}{\log x}$$

This means

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log\, x} = 1.$$

**Interpretation**

The theorem implies that the number of primes less than $x$is approximately $x/\log\, x$.

For example,

$$\pi(1000) = 168$$

while

$$\frac{1000}{\log\,(1000)} \approx 145.$$

The approximation improves as $x$ becomes larger.

**Theorem 2.1:** The smallest divisor (other than 1) of a composite number is a prime.

**Proof:** Let $a$ be any given composite number. Then $a$ has at least one divisor other than 1 and $a$. This implies that $a$ has a smallest divisor d which is less than $a$. If d is

a composite number, then it has at least one divisor $d_1$ other than 1 and d. Thus, $d_1$ is less than d and divides $a$. This contradicts our assumption that d is the smallest divisor of $a$. Therefore, d cannot be a composite number. Hence, d is a prime.

**Theorem 2.2:** If p is a prime and $a$ is any integer. Then either $(a, p) = 1$ or $a$ is a multiple of p.

**Proof:** Since p is a prime, it has two divisors 1 and p. Therefore, $(a, p) = 1$ or $(a, p) = p$

If $(a, p) = 1$ then theorem is proved. If $(a, p) = p$ then obviously $a$ is a multiple of p.

## 2.5 *FUNDAMENTAL THEOREM OF ARITHMETIC*

**Statement**

Every integer $n > 1$can be expressed as a product of prime numbers, and this representation is unique except for the order of the prime factors.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1, p_2, \ldots, p_k$are distinct prime numbers and $\alpha_1, \alpha_2, \ldots, \alpha_k$are positive integers.

**Proof:** The proof consists of two parts:

**Part I: Existence**

We show that every integer $n > 1$can be expressed as a product of primes.

Suppose there exists a positive integer greater than 1 which cannot be expressed as a product of primes. Let $n$be the smallest such integer.

Since $n$ is not prime, it is composite. Therefore, $n = ab$

Where $1 < a < n, 1 < b < n$. Since $a$and $b$are smaller than $n$, by the minimality of $n$, both can be expressed as products of primes.

Hence $n = ab$ is also a product of primes, contradicting our assumption.

Therefore, every integer greater than 1 can be expressed as a product of primes.

**Part II: Uniqueness**

Suppose $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ are two prime factorizations of $n$.

Since $p_1$divides $q_1 q_2 \cdots q_s$,

by **Euclid's Lemma**, $p_1$must divide one of the primes $q_i$.

Since $q_i$ is prime, $p_1 = q_i$.

Cancelling equal factors from both sides and repeating the argument, we obtain

$$r = s$$

and after rearrangement,

$$p_i = q_i \text{ for all } i.$$

Hence the factorization is unique.

**For Example:** $12 = 2^2 \times 3,\ 60 = 2^2 \times 3 \times 5,\ 360 = 2^3 \times 3^2 \times 5$

Each factorization is unique apart from the order of the factors.

**Theorem 2.3:** If $n$ is not divisible by any prime $\leq \sqrt{n}$ then $n$ is a prime.

**Proof:** Suppose if possible $n$ is not a prime. Then it is composite number. So it can be written as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \geq p_1 p_2$$

But $p_1, p_1 > \sqrt{n}$. ($\because n$ is not divisible by any prime $\leq \sqrt{n}$).

Therefore, $n > \sqrt{n}\sqrt{n}$.

Which is impossible. Hence, $n$ is a prime.

**Corollary:** if $n$ is a composite number then the smallest prime divisor of $n$ is $\leq \sqrt{n}$.

**Question 1:** Show that $\sqrt{2}$ is not a rational number.

**Solution:** Assume, contrary to the claim, that $\sqrt{2}$ is rational.

Then there exist integers $a$ and $b$ with $\gcd(a, b) = 1$such that

$$\sqrt{2} = \frac{a}{b}, \text{ where } b \neq 0.$$

Squaring both sides, we obtain

$$2 = \frac{a^2}{b^2}.$$

Multiplying by $b^2$,

$$a^2 = 2b^2.$$

Thus $a^2$ is even. Since the square of an odd number is odd, $a$ must be even.

Hence,

$$a = 2k$$

for some integer $k$.

Substituting into $a^2 = 2b^2$,

$$(2k)^2 = 2b^2,$$
$$4k^2 = 2b^2,$$
$$b^2 = 2k^2.$$

Therefore $b^2$ is even, which implies that $b$ is even.

Thus both $a$ and $b$ are even, so they are divisible by 2.

This contradicts the assumption that

$$\gcd(a, b) = 1.$$

Hence our assumption that $\sqrt{2}$ is rational is false.

Therefore, $\sqrt{2}$ is not a rational number.

**Question 2:** Show that $503$ is a prime number.

**Solution:** We have that $2, 3, 5, 7, 11, 13, 17$ and $19$ are only primes $\leq \sqrt{503}$. Also, none of the primes divides $503$. Therefore, $503$ is a prime number.

**Theorem 2.4:** There are infinitely many prime numbers. (Euclids theorem)

**Proof:** Suppose there are only finitely many primes p1, p2, ..., pr in ascending order.

Let $p = p_1 . p_2 \ldots p_r + 1$

Then obviously $p > p_r$.

If $p$ is a prime, then there exists a prime greater than $p_r$.

If p is a composite number, then it is not divisible by any of the primes $p_1, p_2, ..., p_r$ since division by any of these primes leaves remainder 1. Therefore, $p$ must be divisible by a prime greater than $p_r$.
Thus, in either case, there exists a prime greater than $p_r$. This contradicts our assumption that there are only finitely many prime numbers.
Hence, there are infinitely many prime numbers.

**Remark 1:** if $p_r$ is the $rth$ prime number then $p_r \leq 2^{2^r-1}$.

**Remark 2:** For $n > 1$ there are at least $(n+1)$ primes less that $2^{2^n}$.

**Remark 3:** There are infinitely many primes of the form $4q + 3$.

## 2.6 *THE GOLDBACH CONJECTURE*

The **Goldbach Conjecture** is one of the oldest and most famous unsolved problems in number theory. It concerns that every even integer can be written as sum of two numbers that are either primes or 1.

**For Example: $2 = 1 + 1$ , $3 = 2 + 1$ , $4 = 3 + 1 = 2 + 2$ , $8 = 7 + 1 = 3 + 5$ etc.**

The conjecture was proposed in 1742 by Christian Goldbach in a letter to Leonhard Euler.

**Property P:** If an integer n possesses the property that numbers less than n and relatively prime to $n$ are only unity and the primes less than n, then it is said that n possesses the property P.

No integer greater than 30 possesses property P.

**Theorem 2.5:** If $n \geq 9$ then $p_n > 2n + 3$.

**Solution:** We will prove this result by mathematical induction.

For $n = 9$ we have

$$p_9 = 23 > 2 \times 9 + 3$$

This shows that the result holds good for $n = 9$.

Let the result hold for $n = m$, i.e.,

$$p_m > 2m + 3$$

Now,
$$p_m \geq 2m + 2$$
$$> 2m + 3 + 2 = 2[m + 1] + 3$$

This shows that the result is true for $n = m + 1$.

Hence, by mathematical induction, the result is true for all values of $n \geq 9$.

## 2.7 *TWIN PRIMES*

A pair of prime numbers $(p, p + 2)$is called a **twin prime pair** if both $p$and $p + 2$ are prime.

**Examples**

$$(3,5), (5,7), (11,13), (17,19), (29,31)$$

are twin prime pairs.

**Remark: Twin Prime Conjecture**:
The Twin Prime Conjecture is one of the most famous unsolved problems in number theory. It concerns pairs of prime numbers that differ by 2.

**Question 3:** If $p$ and $q$ are twin primes then show that $(pq + 1)$ is a perfect square.
**Solution: let** $p$ and $q$ are twin primes such that $q = p + 2$. Then

$$\begin{aligned} pq + 1 &= p[p + 2] + 1 \\ &= p^2 + 2p + 1 \\ &= (p + 1)^2 \end{aligned}$$

Thus, $pq + 1$ is a perfect square.
**Question 4: If** $p$ and $q$ are twin primes then show that $12|(p + q)$ whenever $p > 3$.
**Solution:** let $p$ and $q$ are twin primes such that $q = p + 2$. Then

$$\begin{aligned} p + q &= p + p + 2 \\ &= 2p + 2 \\ &= 2(p + 1) \\ &= 2[3k + 2 + 1] \quad (\text{taking } p = 3k + 1) \\ &= 2[3k + 3] \\ &= 6[k + 1] \\ &= 6.2m \qquad (\because k \text{ cannot be even}) \\ &= 12m \end{aligned}$$

This gives that $12|(p + q)$.

## 2.8 *ODD PERFECT NUMBERS CONJECTURE*

A **perfect number** is a positive integer that is equal to the sum of its proper divisors (all positive divisors excluding the number itself).
**Examples**

$$6 = 1 + 2 + 3$$
$$28 = 1 + 2 + 4 + 7 + 14$$

Thus, 6 and 28 are perfect numbers.
Equivalently, a number $n$ is perfect if

$$\sigma(n) = 2n,$$

where $\sigma(n)$denotes the sum of all positive divisors of $n$.

$$\sigma(n) = 2n$$

**The Odd Perfect Numbers Conjecture**
**Statement: There are no odd perfect numbers.**
In other words, no odd integer $N$satisfies

$$\sigma(N) = 2N.$$

Although many even perfect numbers are known, no odd perfect number has ever been found.

The **Odd Perfect Numbers Conjecture** posits that no odd perfect numbers exist. A perfect number is a positive integer equal to the sum of its proper divisors (e.g., 6 and 28 are even perfect numbers). Despite over two millennia of study, mathematicians still do not know if odd perfect numbers exist, making it one of the oldest unsolved problems in mathematics.

## CHECK YOUR PROGRESS

**MCQ Questions**

**Problem 1. The function $\pi(x)$counts:**
A. Composite numbers
B. Divisors
C. Prime numbers less than or equal to $x$
D. Twin primes
**Problem 2. The Prime Number Theorem was proved in:**
A. 1792
B. 1859
C. 1896
D. 1910
**Problem 3.** The Fundamental Theorem of Arithmetic states that every integer greater than 1 can be written as:
A. Sum of primes
B. Product of primes
C. Difference of primes
D. Multiple of primes
**Problem 4.** Which theorem is used to prove uniqueness of fundamental theorem of arithmetic?
A. Wilson's Theorem
B. Fermat's Theorem
C. Euclid's Lemma
D. Chinese Remainder Theorem
**Problem 5.** Prime factorization of 72 is:
A. $2^3 \times 3^2$
B. $2^2 \times 3^3$
C. $2^3 \times 3$
D. $2 \times 3^2$
**Problem 6. The Goldbach Conjecture states that every even integer greater than 2 is the sum of:**

A. Two odd numbers
B. Two primes
C. Three primes
D. Two composite numbers

**Problem 7. Goldbach proposed the conjecture in:**
A. 1642
B. 1707
C. 1742
D. 1859

**Problem 8. The Goldbach Conjecture is currently:**
A. Proved
B. Disproved
C. Open
D. Trivial

**Problem 9. The difference between twin primes is:**
A. 1
B. 2
C. 3
D. 4

**Problem 10. Who proved the convergence of the reciprocal sum of twin primes?**
A. Euler
B. Gauss
C. Brun
D. Hardy

**Problem 11. The Twin Prime Conjecture states that:**
A. There are finitely many twin primes.
B. Every prime is part of a twin pair.
C. There are infinitely many twin prime pairs.
D. Every even number is a sum of twin primes.

**Problem 12 A perfect number satisfies**
A. $\sigma(n) = n$
B. $\sigma(n) = 2n$
C. $\sigma(n) = n^2$
D. $\sigma(n) = 0$

**Problem 13. The smallest perfect number is**
A. 4
B. 5
C. 6
D. 8

**Problem 14. Every known perfect number is**
A. Odd
B. Prime

C. Composite and even
D. Square-free

**Problem 15. The Odd Perfect Numbers Conjecture states**

A. Odd perfect numbers exist.
B. There are infinitely many odd perfect numbers.
C. No odd perfect number exists.
D. Every odd number is perfect.

## 2.9 *SUMMARY*

**(i)** The study of perfect numbers dates back to ancient Greek mathematicians, particularly Euclid. More than 2,000 years of research have failed to produce a single example of an odd perfect number.

**(ii)** The **Odd Perfect Numbers Conjecture** remains one of the deepest unsolved problems in number theory. Despite centuries of effort and many powerful restrictions on their possible form, no odd perfect number has ever been discovered, and mathematicians still do not know whether one exists.

**(iii)** Prime numbers form the foundation of number theory and continue to be a major area of mathematical research due to their rich structure, deep theoretical significance, and practical applications.

**(iv)** Prime numbers have numerous applications in modern science and technology, particularly in cryptography, computer security, coding theory, and digital communication. Their unique properties make them one of the most important and widely studied objects in mathematics.

**(v)** Twin primes are among the most fascinating objects in number theory. Despite their simple definition, the question of whether infinitely many twin prime pairs exist remains unsolved, making the Twin Prime Conjecture one of the most celebrated open problems in mathematics.

## *2.10 GLOSSARY*

**1.** Arithmetic Function
**2.** Number Theoretic
**3.** Divisor
**4.** Prime Number
**5.** Composite Number
**6.** Greatest Common Divisor (GCD)
**7.** Relatively Prime (Coprime)

## 6.8 *REFERENCES*


- **Burton, D. M.** (2007). Elementary number theory (6th ed.). McGraw-Hill.
- **T. M. Apostol**, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford.
- **Tom M. Apostol**, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York.
- **G. A. Jones and J. M. Jones**, *Elementary Number Theory*, Springer-Verlag, Berlin, 1998.
- **T. Nagell**, *Introduction to Number Theory*, Wiley, New York.


## 6.9 *SUGGESTED READING*


- **Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery**, *An Introduction to the Theory of Numbers*, John Wiley & Sons.
- **Hugh L. Montgomery and Robert C. Vaughan**, *Multiplicative Number Theory I: Classical Theory*, Cambridge University Press.
- **H. Iwaniec and E. Kowalski**, *Analytic Number Theory*, American Mathematical Society, 2004.
- **T. Koshy**, *Elementary Number Theory with Applications*, Academic Press.


## 2.13 *TERMINAL QUESTIONS*

**Long answer type questions**

**1.** Define twin prime number with examples.
**2.** Prove that there are infinitely many primes number.
**3.** Show that $\sqrt{5}$ is irrational using prime factorization.
**4.** Discuss the distribution of prime numbers and explain the asymptotic formula for $\pi(x)$.
**5.** State and prove the Fundamental Theorem of Arithmetic.

## 2.14 *ANSWERS*

**Answer of objective questions**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | C | **2:** | C | **3:** | B | **4:** | C |
| **5:** | A | **6:** | B | **7:** | C | **8:** | C |
| **9:** | B | **10:** | C | **11:** | C | **12:** | B |
| **13:** | C | **14:** | C | **15:** | C | | |

# UNIT-3: THEORY OF CONGRUENCES AND FERMAT'S THEOREM

**CONTENTS:**



## 3.1. INTRODUCTION:

This unit introduces the foundational tools of modern modular arithmetic. The unit focuses on solving divisibility problems, manipulating remainders, and utilizing Fermat's Little Theorem to test for primality. A central concept in number theory is congruence**,** introduced systematically by the German mathematician Carl Friedrich Gauss. Building upon congruences,

one of the most important results in elementary number theory is Fermat's Little Theorem, given by the French mathematician Pierre de Fermat.

| | |
|---|---|
| **Pierre de Fermat** (17 August 1601 – 12 January 1665) was a French magistrate, polymath ,and above all, a mathematician wh o is given credit for early developments that led to infinitesimal calculus, including his technique of adequality. |  ***Fig 3.1.*** https://en.wikipedia.org/wiki/Pierre_de_Fermat#/media/File:Pierre_de_Fermat.jpg |

## 3.2. OBJECTIVES:

After studying this unit learner will be able to:

**i.** Explained the definition and properties of congruences

**ii.** Learn how to perform arithmetic operations under modulo

**iii.** Study linear congruences and their solutions

**iv.** Explore Fermat's Little Theorem and its applications

## 3.3. CONGRUENCE:

A mathematical **congruence** asserts that two integers leave the identical remainder when divided by a positive integer called the modulus.

Formally written as a $\equiv b(modn)$, this concept means that the modulus a $n$ perfectly divides the difference $a-b$. Popularized by Carl Friedrich Gauss, congruences mimic "clock arithmetic" where numbers wrap around, such as $17 \equiv 5(mod6)$. This system preserves basic arithmetic operations like addition and multiplication. Leonhard Euler heavily utilized congruences to prove Euler's Theorem $a^{\varphi(n)} \equiv a(modn)$ creating the foundational mathematical framework that securely powers modern internet RSA encryption today. Gauss introduces the concept of congruence and the notation that makes it such a powerful technique he was induced to adopt the symbol $\equiv$.

## *3.3.1. DEFINITION:*

Let $n$ be a fixed positive integer. Two integers $a$ and $b$ are said to be congruent modulo $n$, symbolized by a $\equiv b(modn)$.If $n$ divides the difference $a-b$; that is, provided that $a-b=kn$ for some integer $k$. Consider $n=7$. Now we check that $3\equiv 24(mod7). 3-24=(-3)7$. When $n \nmid (a-b)$, we say that $a$ and is incongruent $b$ modulo $n$, now we can write a $\not\equiv b(modn)$.We can see that $25 \not\equiv 12(mod7)$. Because a $\not\equiv 7$ fails to divide $25-12=13$. Two integers $a$ and $b$ are said to be congruent modulo $n$. If and only if they have same remainder when divided by $n$.

**Note:** Any two integers are congruent modulo 1, whrereas two integers are congruent modulo 2 when they are both even or both odd.

- Given an integer $a$ let $q$ and $r$ be its quotient and remainder upon division by $n$, so that $a=qn+r, 0 \leq r <$n. Then by definition of congruence, a $\equiv r(modn)$. Because there are $n$ choices for a $r$ we see that every integer is congruent modulo $n$ to exactly one of the values a $0,1,2,\ldots\ldots\ldots n-1$; in particular a $\equiv 0(modn)$ if and only if $n|a$. The set of integers$0,1,2,\ldots\ldots\ldots n-1$ is called the set of least nonnegative residue modulo $n$.

- A collection of n integers $a_1, a_2, \ldots\ldots\ldots\ldots a_n$ is said to form a complete set of residues(or a complete system of residues) modulo $n$ if every integer is congruent modulo $n$ to one and only one of the $a_k$.

## *3.3.2 THEORM :*

**Theorem 1:** For arbitrary integer $a$ and $b$, a $\equiv b(modn)$ if and only if $a$ and $b$ leave the same nonnegative remainder when divided by $n$.

**Proof**. We are taking a $\equiv b(modn)$, so that $a = b + kn$, for some integer $k$.
Upon division by n, $b$ leaves a certain remainder $r$;
that is,
$b = qn + r$, where $0 \leq r <$n.
Therefore,
$a = b + kn = (qn + r) + kn = (q + k)n + r$.
Which indicates that a has the same remainder as $b$.
Now we can write $a = q_1 n + r$ and $b = q_2 n + r$, with the same reminder r ( $0 \leq$ r <n).
Then $a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$.
Whence $n|a - b$. In the terms of congruences, we have , a $\equiv b(modn)$.

**Theorem 2:-** Let $n > 1$ be fixed a, b, c, d be arbitrary integers. Then the following properties hold:

- **i.** a $\equiv a(modn)$.
- **ii.** If a $\equiv b(modn)$, then $b \equiv a(modn)$.
- **iii.** If a $\equiv b(modn)$, and $b \equiv c(modn)$, then a$\equiv c(modn)$.
- **iv.** If a $\equiv b(modn)$, and $c \equiv d(modn)$, then a$+c \equiv b + d(modn)$ and a$c \equiv bd(modn)$.
- **v.** If a $\equiv b(modn)$, then a$+c \equiv b + c(modn)$ and a$c \equiv bc(modn)$.
- **vi.** If a $\equiv b(modn)$, then $a^k \equiv b^k(modn)$ for any positive integer $k$.

**Proof.** For any integer a,

we have $a - a = 0.n$,

Therefore, $a \equiv a(modn)$. Hence first property proved.

Now if a $\equiv b(modn)$,

Then a $a - b = kn$ for some integer $k$.

Hence $b - a = -(kn) = (-k)n$.

Because $-k$ is an integer, this yields property second.

Suppose that a $\equiv b(modn)$ and also a $b \equiv c(modn)$.

Then there exists integers $h$ and $k$ satisfying $a - b = hn$ and $b - c = kn$.

It follows that $a - c = (a - b) + (b - c) = hn + kn = (h + k)n$.

Which is $a \equiv c(modn)$ in congruence notation.

By the same method,

if a $\equiv b(modn)$, and $c \equiv d(modn)$,

then we are assured that $a - b = k_1 n$ ……..(A)

and

$c - d = k_2 n$ ……..(B)

for some choice of $k_1$ and $k_2$.

Adding these equations,

we obtain,

$$(a + c) - (b + d) = (a - b) + (c - d) = k_1 n + k_2 n = (k_1 + k_2)n.$$

Or as a congruence statement $a + c = b + d(mod)n$.

As regards the second assertion of property iv, note that,

$$ac = (b + k_1 n)(d + k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2 n)n$$

Because, $bk_2 + dk_1 + k_1 k_2 n$ is an integer, this says that $ac - ad$ is divisible by $n$ whence

a$c \equiv bc(modn)$. The proof of property fifth is covered by fourth and the fact that $c \equiv c(modn)$. Finally we obtain property fifth by making an induction argument. The statement certainly holds for $k = 1$, we will assume it is true for some fixed $k$. From fourth we know that a $\equiv b(modn)$, and $a^k = b^k(modn)$ together imply that $aa^k = bb^k(modn)$ equivalently $a^{k+1} = b^{k+1}(modn)$. This is the form the statement should take for $k + 1$ and so the induction step is complete.

**Theorem 3:-** ca≡ $cb(modn)$ then a ≡ $b(mod\, n/d)$, where $d = gcd(c,n)$.

**Proof.** Since $c(a-b) = ca - cb = kn$ for some integer $k$…….(1)

We know that $gcd(c,n) = d$, there exist relatively prime integers $r$ and $s$ satisfying $c = dr, n = ds$. Putting these values in equation (1), $dr(a-b) = dra - drb = kds$.It implies that

$$r(a-b) = ks.$$

Therefore, $s|r(a-b)$ and $gcd(r,s) = 1$. Euclid's lemma yields $s|a-b$, which may be recast as a $a \equiv b(mods)$; in other words, a $a \equiv b(mod\, n/d)$.

- If $ca \equiv cb(modn)$ and ≡ $\gcd(c,n) = 1$, then $a = b(modn)$.
- If $ca \equiv cb(modp)$ and $p \nmid c$, where $p$ is a prime number, then $a \equiv b(modp)$.

## *3.3.3. SOLVED PROBLEMS:*

**Problem 1:** Show that for any integer $a$,

$$a^3 \equiv 0,1\ or\ 8(mod\ 9).$$

**Solution:** Let $a = 3k + r, 0 \le r < 3$.

If $r = 0, then\ a = 3k$.

This implies that $\mathbf{a^3 = 27k^3 \equiv 0(mod\ 9)}$.

If $r = 1, then\ a = 3k + 1$.

Therefore, $a^3 = 27(3k+1)^3 \equiv 27k^3 + 1 + 9k^2 + 9k$.

This implies that $a^3 \equiv 1(mod\ 9)$.

If $a = 3k + 2$.

Then $a^3 = 27(3k+2)^3 \equiv 27k^3 + 8 + 27k^2 + 36k^2$.

This implies that $a^3 \equiv 8(mod\ 9)$.

So $a^3 \equiv 0,1\ or\ 8(mod\ 9)$.

**Problem 2:** Find the remainder obtained by dividing, $1! + 2! + 3! + \cdots 100!$ by $12$.

**Solution:** Each number 4! Onwards is a multiple of $12$.

Therefore,

$1! + 2! + 3! + \cdots 100! \equiv 1! + 2! + 3! + 0 + \cdots 0(mod 12)$

This implies,

$$1! + 2! + 3! + \cdots 100! \equiv 9(mod 12)$$

Therefore 9 is the required remainder.

**Problem 3:** Find the remainder when $2^{50}$ is divided by 7.

**Solution:** Now, $2^3 \equiv 1\ (mod 7)$.

This implies that $2^3 \equiv 1(mod\ 7)$.

$$(2^3)^{16} \equiv 1(mod 7)$$

Therefore $2^{48} \equiv 1(mod 7)$

This implies that $2^{48} - 2^2 \equiv 2^2(mod 7)$.

So $2^{50} \equiv 4(mod 7)$.

Therefore 4 is the remainder.

**Problem 4:** What is the remainder when the sum $1^5 + 2^5 + 3^5 + \cdots 99^5 + 100^5$ is divided by 4.

**Solution:** We can write $1 \equiv 1(mod 4) \Longrightarrow 1^5 \equiv 1(mod\ 4)$.

$$2^2 \equiv 0(mod\ 4) \Longrightarrow 2^5 \equiv 0(mod\ 4).$$

$$3^2 \equiv 1(mod\ 4) \Longrightarrow 3^5 \equiv 3(mod\ 4).$$

This implies $3^5 \equiv -1(mod\ 4)$.

$$4^2 \equiv 0(mod\ 4) \Longrightarrow 4^5 \equiv 0(mod\ 4).$$

Therefore, $1^5 + 2^5 + 3^5 + 4^5 = 1 + 0 - 1 + 0 \equiv 0(mod\ 4)$.

Any number after these will be of the form $2k + 1, 2k + 2, 2k + 3, 2k + 4, \ldots\ldots k > 1$.

Now, $(2k + 1)^2 \equiv 1(mod\ 4) \Longrightarrow (2k + 1)^5 \equiv 2k + 1 \equiv 1(mod\ 4)$.

$$(2k + 2)^2 \equiv 0(mod\ 4) \Longrightarrow (2k + 2)^5 \equiv 0(mod\ 4).$$

$$(2k + 3)^2 \equiv 1(mod\ 4) \Longrightarrow (2k + 3)^5 \equiv 2k + 3 \equiv -1(mod\ 4).$$

$$(2k + 4)^2 \equiv 0(mod\ 4) \Longrightarrow (2k + 4)^5 \equiv 2k + 3 \equiv 0(mod\ 4).$$

$$1^5 + 2^5 + 3^5 + \cdots 99^5 + 100^5 \equiv 0(mod\ 4).$$

So, remainder is 0 when above number is divided by 4.

**CHECK YOUR PROGRESS**

**Fill in the Blanks**

**CYP 1:** For any value $n \in \mathbb{N}$, remainder obtained when $6^n - 5^n$ is divided by……

**CYP 2:** The product of the last two digits of $(1919)^{1919}$ is……..

**CYP3:** If $147 \equiv 3(modk)$, what is the largest possible value of $k$ … … … … ..

**CYP4:** Two integers $a$ and $b$ are said to be congruent modulo $n$, symbolized by …….

**CYP5:** For arbitrary integer $a$ and $b$, a $\equiv b(modn)$ if and only if $a$ and $b$ leave the ……. nonnegative remainder when divided by $n$.

## *3.4.* EULER'S $\varphi$ FUNCTION*:*

Leonhard Euler introduced the totient function $\varphi(n)$ in 1763 to generalize Fermat's Little Theorem and solve problems involving modular congruences. It counts the positive integers up to n that are relatively prime (coprime) to n .It is now fundamentally important in areas like abstract algebra and modern internet cryptography. For a positive integer $n, \varphi(n)$ is the number of integers k in the range $1 \leq k \leq n$ such that $\gcd(n, k) = 1$. Now with the help of following formula we can find the $\varphi(n)$.

i. **Prime Numbers:** If $p$ is prime, $\varphi(p) = p - 1$.

ii. **Prime Power:** If $p$ is prime and $k \geq 1$, $\varphi(p^k) = p^k - p^{k-1}$

iii. If $p_1, p_2, \ldots . p_n$ are distinct prime factors of $n(> 1)$, then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots .\left(1 - \frac{1}{p_k}\right)$$

iv. If $m, n$ are coprime then $\varphi(mn) = \varphi(m)\varphi(n), (m, n \geq 1)$.

The function is central to RSA encryption, where the security relies on the difficulty of factoring, which is related to calculating $\varphi(n)$ for large

numbers. It is used to compute the private decryption exponent $d$ from the public encryption exponent $e$, securing digital communications, web browsing, and electronic signatures worldwide

## 3.5. FERMAT'S THEOREM:

Around 1637, Pierre de Fermat wrote a theorem in the margin of Diophantus's *Arithmetica*, famously claiming he had a "marvelous proof" that the margin was too small to contain. He stated that the equation $a^n + b^n = c^n$ has no integer solutions for n > 2. For over 300 years, this became math's greatest mystery. Fermat only left a proof for n = 4. Later, Leonhard Euler (n=3), Sophie Germain, and Ernst Kummer proved it for various categories of numbers, but a general proof remained elusive. The breakthrough came in the 1980s when mathematicians linked the theorem to the Taniyama-Shimura-Weil conjecture, which concerned elliptical curves. British mathematician Andrew Wiles worked in secret for seven years to bridge this gap. In 1993, he announced his proof, but a flaw was soon discovered. After a year of intense revision with Richard Taylor, Wiles had a sudden "revelation" that fixed the error. He published the final proof in 1995, ending the 358-year quest.

**Theorem 4: (Statement)** Let $p$ be a prime and suppose that $p \nmid a$ *or* $g.c.d\ (a,p) = 1$. Then $a^{\mathrm{p}-1} \equiv 1(mod p)$.

**Proof:** We begin by considering the first $\mathrm{p} - 1$ positive multiples of $a$;
that is, the integers
$a, 2a, 3a, \ldots\ldots\ldots\ldots\ldots\ldots (p-1)a$.
None of these numbers is congruent modulo $p$ to any other, nor is any congruent to zero.
Indeed, if it happened that

$$ra \equiv sa\ (mod\ p) \quad 1 \leq r < s \leq p-1.$$

Then $a$ could be canceled to give $r \equiv s\ (mod\ p)$.
Which is impossible.

Therefore, the previous set of integers must be congruent modulo $p$ to 1,2,3 ……

$p-1$, taken in same order.

Multiplying all these congruences together,

we find that

$a.2a.3a\ldots\ldots\ldots\ldots(p-1)a \equiv 1,2,3\ldots\ldots(p-1)(mod\ p)$.

Whence

$$a^{p-1}(p-1)! \equiv (p-1)!\,(modp).$$

Once $(p-1)!$ is canceled from both sides of the preceding congruence (this is possible because since $p \nmid (p-1)!$ .

Now we can say that $a^{p-1} \equiv 1(modp)$, which is Fermat's theorem.

**Corollary 1:** If $p$ is a prime, then $a^p \equiv a(modp)$ for any integer $a$.

**Proof:** Since from Euler's Theorem if $g.c.d\ (a,p)=1, then\ a^{\varphi(p)} \equiv 1(modp)$. Where $a, (n \geq 1)$ be any integer and prime $p$. It implies $a^{p-1} \equiv 1(modp)$as $\varphi(p) = p-1$. This implies that $a^p \equiv a(modp)$. If $(a,p)=1$, then $p|a \Rightarrow p|a^p$. Therefore $p|a^p - a$. This implies $a^p \equiv a(modp)$. [Note $(a,p)=1$ or $p$ as 1 and $p$ are only divisors of $p$]

**Lemma 1:** If $p$ and $q$ are distinct primes $a^p \equiv a(modq)$ and

$a^q \equiv a(modp), then\ a^{pq} \equiv a(mod\ pq)$.

**Proof:**

**Step 1:** Prove $a^{pq} \equiv a(mod\ pq)$.

$$a^{pq} = (a^q)^p.$$

Using the given condition $a^q \equiv a(modp)$ substitute $a$ for $a^q$ .

$(a^q)^p \equiv a(mod\ p)$.

By Fermat's Little Theorem, we know that $a^p \equiv a(modp)$ for any integer $a$.

Therefore, $a^{pq} \equiv a(mod\ p)$ this implies that $p|(a^{pq} - a)$.

**Step 2:** Prove $a^{pq} \equiv a(mod\ pq)$.

$$a^{pq} = (a^p)^q.$$

Using the given condition $a^p \equiv a(modq)$ substitute $a$ for $a^p$ .

$(a^p)^q \equiv a(mod\ q)$.

By Fermat's Little Theorem, we know that $a^q \equiv a(modq)$ for any integer $a$.

Therefore, $a^{pq} \equiv a(mod\ q)$ this implies that $q|(a^{pq} - a)$.

**Step 3:** Combine Using Coprimality: We have established that $(a^{pq} - a)$ is simultaneously divisible by $p$ and by $q$. Because $p$ and $q$ are distinct prime numbers, their least common multiple $lcm$ is exactly $pq. p|x\ and\ q|x$ where $(p, q) = 1$. Then $pq|x$. Thus $pq|(a^{pq} - a)$ which directly translates to the final result: $a^{pq} \equiv a(mod\ pq)$.

Fermat's Little Theorem is a cornerstone of modern digital security and computational mathematics. Its primary application lies in public-key cryptography, specifically serving as the mathematical foundation for the RSA encryption algorithm that secures global internet communications. Additionally, the theorem enables fast probabilistic primality testing, allowing computers to efficiently screen and generate massive prime numbers required for cryptographic keys by quickly filtering out composite numbers. It also simplifies complex modular arithmetic, enabling computer systems to compute massive exponents instantly. Ultimately, this simple formula acts as a vital mechanism protecting online banking, data privacy, and secure digital infrastructure.

## *3.5.1. PSEUDOPRIME*:

**Pseudoprime:** A pseudoprime is a composite number that masquerades as a prime number because it successfully passes specific probabilistic primality tests. Historically, these numbers arose from attempts to find an efficient, converse shortcut to Pierre de Fermat's Little Theorem.

Fermat's little theorem states that if $p$ is prime and $a$ is coprime to $p$, then $a^{p-1} - 1$ is divisible by $p$. For an integer $a > 1$, if a composite integer $x$ divides $a^{x-1} - 1$, then $x$ is called a Fermat pseudoprime to base $a$. It

follows that if $x$ is a Fermat pseudoprime to base $a$, then $x$ is coprime to $a$. The primary application of pseudoprimes is in probabilistic primality testing (such as the Miller-Rabin or Fermat tests). These algorithms generate large candidate prime numbers for public-key cryptography (like RSA), where pseudoprimes are used to rapidly filter out non-primes, vastly accelerating cryptographic key generation.

**Theorem 5:** If $n$ is an odd pseudoprime then $M_n = 2^n - 1$ is a larger one.

**Proof.** To prove $M_n$ is a pseudoprime, it must satisfy two conditions: it must be composite and it must satisfy the congruence relation $2^{M_n-1} \equiv 1(mod\ M_n)$.

$i.\ M_n$ is composite: Since $n$ is a pseudoprime, it is composite by definition. If we let $n = rs\ (where\ r, s > 1)$, then $2^n - 1 = 2^{rs} - 1$ is divisible by $2^r - 1$. Since $1 < 2^r - 1 < 2^n - 1$, the number $M_n$ is also composite.

$ii.$ The Congruence Condition: By the definition of a pseudoprime to base 2, $n$ must divide $2^{n-1} - 1$ which means $2^{n-1} - 1 = kn$ for some integer $k$.

- Multiply by 2 to get $2^n - 2 = 2kn$.
- Since $M_n = 2^n - 1$, we can rewrite this as $M_n - 1 = 2kn$.
- Now consider the term $2^{M_n-1} - 1 = 2^{2kn-1} - 1 = (2^n)^{2k} - 1$.
- Using the algebraic identity $(x - 1)|(x^m - 1)$, we see that $(2^n - 1)$ divides $(2^n)^{2k} - 1$.

Therefore, $M_n|2^{M_n-1} - 1$, which is equivalent to $2^{M_n-1} \equiv 1(mod\ M_n)$.

**Theorem 5:** Let $n$ be a composite square free integer say $n = p_1\ p_2 \ldots\ldots p_r,\ where$ the $p_i$ are distinct primes. If $p_i - 1|n - 1\ for\ i = 1,2 \ldots \ldots \ldots \ldots, r$,then $n$ is an absolute pseudoprime.

**Proof.** Suppose that $a$ is an integer satisfying $\gcd(a, n) = 1$, so that $\gcd(a, p_i) = 1$ for each $i$. Then Fermat's theorem yields $p_i|\ a^{p_i-1} - 1$. From the divisibility hypothesis $p_{i-1}|\ n - 1$, we have$p_i|\ a^{p_i-1} - 1$, and therefore $p_i|$

$a^n - a$ for all $a$ and $i = 1,2, \ldots \ldots r$. We end up with $n|a^n - a,$ which makes $n$ an absolute pseudoprime.

## *3.5.2. SOLVED PROBLEMS:*

**Problem 5:** Find the remainder when $7^{100}$ is divided by 13.

**Solution:** Since 13 is a prime number, we can apply Fermat's theorem, which states:

$$7^{12} \equiv 1(mod\ 13).$$

Now, $100 = 12 \times 8 + 4,$
So:

$$7^{100} = (7^{12})^8 . 7^4 \equiv 1^8 . 7^4 \equiv 7^4(mod\ 13).$$

Calculate $7^4 mod\ 13$:

- $7^2 = 49 \Rightarrow 49\ mod\ 13 = 10.$
- $7^4 = (7^2)^2 = 10^2 = 100 \Rightarrow 100\ mod\ 13 = 9.$

Therefore, the remainder when $7^{100}$ is divided by 13 is 9.

**Problem 5:** Find the remainder when $3^{100,000}$ when divided by 53.

**Solution:** Since 53 is a prime number, we can apply Fermat's theorem, which states:

$$3^{52} \equiv 1(mod\ 53).$$

Now:
$100000 = 52 \times 1923 + 4 \Rightarrow 3^{10000} = (3^{52})^{1923} . 3^4 \equiv 1^{1923} . 3^4 = 3^4(mod\ 53).$

- $3^4 = 81 \Rightarrow 81\ mod\ 53 = 28.$

Therefore, the remainder when $3^{100,000}$ is divided by 53 is 28.

In words the application of above mention terms is as given below:

Every time you tap a credit card, send a secure chat, or stream a video, hidden digital systems protect your privacy using mathematical principles. The most vital use is protecting personal identity on the internet. Shopping sites rely on two separate keys: one unlocks your connection to the site, while the other translates your financial data into scrambled text. Because calculating these keys requires immense processing power, hackers cannot break into your bank accounts. This strategy shields global banking networks, government communications, and digital medical history records from modern network vulnerability exploits. Beyond online protection, these formulas help tech

companies sort massive files efficiently. Computers process vast spreadsheets by sorting labels into numbered boxes using a standard cycle. This process assigns every file an exclusive bucket, letting software pull up your search queries instantly. Additionally, barcode scanners use cyclical calculations to check for human typing mistakes. If a cashier enters a digit wrong, the final check value fails, and the terminal blocks the transaction. This simple safety mechanism prevents shipping errors and inventory accidents globally. Finally, scheduling applications use similar repeating cycles to coordinate calendar notifications across different time zones automatically.

## 3.6. SUMMARY:

This unit provides a foundational overview of modern modular arithmetic, centred on the concepts and notations introduced by Carl Friedrich Gauss. The core of the unit is the congruence relation, where two integers a and b are congruent modulo n if n divides their difference. This relationship is essentially an equivalence that identifies integers by their remainders upon division.

Key mathematical properties explored include:

- Arithmetic Laws: Congruences behave like equations; they are reflexive, symmetric, and transitive, and allow for addition, multiplication, and exponentiation.
- Cancellation.
- Fermat's Little Theorem.
- Euler's Totient Function.

Through solved problems, the unit demonstrates practical applications like finding remainders of massive factorials or powers, providing learners with the tools to solve complex divisibility challenges.

## 3.7 GLOSSARY:

i. **Euclid's Algorithm:** Let $k > 0$ be an integer and $j$ be any integer. Then $\exists$ unique integers $q$ and $r$ such that $j = kq + r$, where $0 \leq r < k$.

ii. **Greatest Common Divisor:** An integer $d > 0$ is called greatest common integer (g.c.d.) of two integers $a, b$ (non zero) if
   **a.** $d|a, d|b$
   **b.** If $c|a, c|b$ then $c|d$.
   **c.** We write $d = g.c.d.(a, b)$ or simply $d = (a, b)$.

iii. **Cyclic group:** A group $G$ is called a cyclic group if $\exists$ an element $a \in G$, such that every element of $G$ can be expressed as a power of $a$. In that case $a$ is called generator of $G$.

iv. **Euler's Theorem:** *Let* $a, \mathrm{n}\ (\mathrm{n} \geq 1)$ *be any integers such that* $g.c.d\ (a, n) = 1, then\ a^{\varphi(\mathrm{n})} \equiv 1 (mod n)$.

## 3.8. REFERENCES:


1. Burton, David M. *Elementary Number Theory*. 7th ed., McGraw-Hill Education, 2011.
2. Niven, Ivan, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers.* 5th ed., Wiley, 1991.
3. Pundir, Sudhir K., and Rajiv Pundir. *Algebra and Number Theory.* Pragati Prakashan, 2010.
4. Titu Andreescu, and Dorin Andrica. *Number Theory: Structures, Examples, and Problems*. Birkhäuser, 2009.


## 3.9. SUGGESTED READINGS:


1. Lipschutz, Seymour. *Schaum's Outline of Theory and Problems of Number Theory*. McGraw-Hill, 1968.
2. https://nptel.ac.in/courses/111101137


## 3.10. TERMINAL QUESTIONS:

**TQ1.** Find the remainder when $5^{123}$ is divided by 13.

**TQ2**. Compute the remainder when $11^{50}$ is divided by 17.

**TQ3.** What is the remainder when $7^{300}$ is divided by 19.

**TQ4.** Calculate the remainder of $2^{200} modulo\ 31$.

**TQ5.** Find the remainder when $8^{75}$ is divided by 29.

## 3.11. ANSWERS:

### Answer of Terminal Questions:

**TQ1.** B

**TQ2**. 2

**TQ3.** 1

**TQ4.** 1

**TQ5.** 2

### Answer of Check your progress Questions:

**CYP1:** 1.

**CYP2:** 63.

**CYP3:** 144.

**CYP4:** a $\equiv b(modn)$.

**CYP5:** Same.

# UNIT 4: CHINESE REMAINDER THEOREM AND WILSON THEOREM

**CONTENTS:**



## 4.1. INTRODUCTION:

The study of divisibility, prime numbers, and congruences has led to the development of several important concepts and theorems that have both theoretical significance and practical applications in modern fields such as cryptography, coding theory, computer science, and information security.

In this unit, we explore some fundamental topics related to prime numbers and congruences. We begin with Mersenne Primes, a special class of prime numbers which have attracted mathematicians for centuries due to their

unique properties and connection with perfect numbers. The unit then introduces Linear Congruences, which are equations involving congruence relations and play a central role in solving problems related to modular arithmetic.

The discussion continues with the Chinese Remainder Theorem, one of the most important results in number theory. This theorem provides a method for finding solutions to systems of simultaneous congruences and has numerous applications in computational mathematics and cryptography. Next, we study Wilson's Theorem, a remarkable characterization of prime numbers that establishes a necessary and sufficient condition for determining whether a number is prime.

## 4.2. OBJECTIVES:

After studying this unit, learners will be able to:

**i.** Understand the concept of Mersenne Primes and identify prime numbers of the form $M_p = 2^p - 1$

**ii.** Define and solve linear congruences of the form $ax \equiv b(mod n)$.

**iii.** Determine the conditions under which a linear congruence has a solution and find all incongruent solutions.

**iv.** Understand the statement and significance of the Chinese Remainder Theorem.

**v.** State and prove Wilson's Theorem and use it to test the primality of integers.

## 4.3. MERSENE PRIME:

Marin Mersenne was a French mathematician, philosopher, and theologian. In his book *Cogitata Physico-Mathematica* (1644), he studied numbers of the form $M_p = 2^p -$ and proposed a list of exponents that he believed produced prime numbers.

These special primes were later named **Mersenne primes** in his honor A Mersenne prime is a prime number that is one less than a power of two, written in the form $M_p = 2^p - 1$. For $M_p$ to be prime, the exponent $p$ must also be a prime number. They are highly sought after because they represent the largest known prime numbers.

**Top Five Smallest Mersenne Primes:**

The first few Mersenne primes are:

- $3(2^2 - 1)$
- $7(2^3 - 1)$
- $31(2^5 - 1)$
- $127(2^7 - 1)$
- $(2^{13} - 1)$

**Properties:**

- Connection to perfect numbers: Every Mersenne prime corresponds exactly to one even perfect number (a positive integer equal to the sum of it's proper divisors, like $6\ or\ 28$). The formula for these even perfect numbers is $2^{p-1}(2^p - 1)$.
- Fast Primality Testing: Because of their structure, it is much easier to prove whether a Mersenne number is prime using the specialized Lucas – Lehmer test compared to standard numbers of smaller size.

The Lucas – Lehmer test (LLT) is a highly efficient deterministic primality test used exclusively to determine if a Mersenne number $M_p = 2^p - 1$ is a prime number. Because of its mathematical design, it is vastly faster than general primality tests, making it the foundational tool used by the great internet Mersenne Prime Search (GIMPS). If a Mersenne number is composite, its factor must follow a very rigid structure, which helps computer programs rule out candidates quickly.

**CHECK YOUR PROGRESS**

Solve the following multiple-choice questions:

**CYP1:** A Mersenne number is of the form:

a. $2^p + 1$

b. $2^p - 1$

c. $p^2 - 1$

d. $p! - 1$

**CYP2:** Which of the following is a Mersenne prime?

a. 15

b. 21

c. 31

d. 63

## 4.4. LINEAR CONGRUENCE:

Dear learners, previous unit we have explained about congruence now in this unit we are explaining the linear congruence. The main difference is that a congruence is a statement of relationship between two fixed numbers, while a linear congruence is an algebraic equation containing an unknown variable $x$ that you need to solve. The concept of linear congruence has its roots in ancient Chinese and Indian mathematics. Early mathematicians studied problems involving remainders and divisibility, leading to methods for solving equations equivalent to congruences. The Chinese mathematician Sunzi developed problems that inspired the Chinese Remainder Theorem, while Aryabhata introduced the Kuttaka method for solving indeterminate equations. The modern theory of congruences was established by Carl Friedrich Gauss in 1801 through his book Disquisitiones Arithmeticae. Since then, linear congruences have become a fundamental topic in number theory, with important applications in cryptography, coding theory, and computer science.

An equation of the form $ax \equiv b(modn)$ is called a linear congruence, and by a solution of such an equation we mean an integer $x_0$ for which $ax_0 \equiv b(modn)$. An algebraic equation where the variable $x$ is raised only to the first power. $3x \equiv 2(mod5)$. You must find the value of $x$ that makes this true. Linear Congruence can have one unique solution, multiple solutions, or no solution at all depending on the Greatest Common Divisor (GCD) of $a$ and $n$.

**CHECK YOUR PROGRESS**

Check that the following statement is **True/False:**

**CYP 3:** A linear congruence has the form $ax \equiv b(modn)$ True/False.

**CYP 4:** The congruence $4x \equiv 3(mod8)$ has a solution. True/False

## 4.5. CHINESE REMAINDER THEOREM:

The Chinese Remainder Theorem is one of the oldest results in number theory. Its origin is traced to the Chinese mathematician Sunzi, who presented a remainder problem in his work *Sunzi Suanjing* around the 3rd to 5th century CE. The theorem provides a method for finding an integer that satisfies several congruence conditions simultaneously. Later, Chinese mathematicians expanded and refined these ideas. In the eighteenth century, the theorem was studied systematically by Leonhard Euler and Carl Friedrich Gauss, who incorporated it into modern number theory. Today, it has important applications in cryptography, computer science, and coding theory.

**Statement:** Let $n_1, n_2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots n_r$ be positive integers such that $gcd(n_i, n_j) = 1 \; for \; i \neq j$.

Then the system of linear congruences

$$x \equiv a_1(mod\, n_1)$$

$$x \equiv a_2(mod\, n_2)$$

…

…..

$$x \equiv a_r (mod\ n_r)$$

has a simultaneous solution, which is unique modulo the integer $n_1, n_2$ … … … … … … … … $n_r$.

**Proof:** We start by forming the product $n = n_1\ n_2 \ldots n_r$..

For each $k = 1,2, \ldots \ldots \ldots r$.

Let $N_k = \frac{n}{n_k} = n_1, n_2 \ldots \ldots \ldots \ldots \ldots n_{k-1} n_{k+1} \ldots . n_r$.

In words, $N_k$ is the product of all the integers $n_i$ with the factor $n_k$ omitted.

By hypothesis, the $n_i$ are relatively prime in pairs, so that

$$\gcd(N_k, n_k) = 1$$

according to the theory of a single linear congruence, it is therefore possible to solve the congruence $N_k x \equiv 1 (mod\ n_r)$; call the unique solution $x_k$.

Our aim is to prove that the integer

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots a_r N_r x_r \equiv a_k N_k x_k\ (mod\ n_k).$$

But the integer $x_k$ was chosen to satisfy the congruence $N_k x \equiv 1 (mod\ n_r)$, which forces:

$$\bar{x} \equiv a_k . 1 \equiv a_k (mod\ n_k).$$

This shows that a solution to the given system of congruences exists.

As for the uniqueness assertion, suppose that $x'$ is any other integer that satisfies these congruences.

Then: $\bar{x} \equiv a_k . 1 \equiv x'\ (mod\ n_k)\ \ k = 1,2, \ldots \ldots \ldots . . r$ so $n_k | \bar{x} - x'$ for each value of $k$. Because $gcd(n_i, n_j) = 1\ for\ i \neq j$.

Since we know that; If $a|c$ and $b|c$, with $\gcd(a, b) = 1$, then $ab|c$.

Therefore $n_1 n_{2.}$ … … … … … … … $n_r\ | \bar{x} - x'$;

hence: $\bar{x} \equiv x'\ (mod\ n)$.

With this, the Chinese Remainder Theorem is proven.

## CHECK YOUR PROGRESS

Solve the following multiple-choice questions:

**CYP 5:** The Chinese Remainder Theorem is applicable when the moduli are:

**a.** Equal numbers

**b.** Prime numbers only

**c.** Pairwise relatively prime integers

**d.** Even integers only

**CYP 6:** The Chinese Remainder Theorem is applicable when the moduli are:

**a.** Equal numbers

**b.** Prime numbers only

**c.** Pairwise relatively prime integers

**d.** Even integers only

## 4.6. WILSON THEOREM:

Wilson's Theorem is an important result in number theory that provides a necessary and sufficient condition for a number to be prime. The theorem is named after the English mathematician John Wilson, who discovered the statement in the eighteenth century. However, he did not publish a proof. The theorem was publicized by Edward Waring in 1770, and the first rigorous proof was given by Joseph-Louis Lagrange in 1771. Later, it became a significant tool in the study of prime numbers and modular arithmetic. Today, Wilson's Theorem is widely taught in elementary and advanced courses on number theory.

**Statement:** If $p$ is a prime, then $(p-1)! \equiv -1(mod\ p)$.

**Proof.** Dismissing the cases $p = 2$ and $p = 3$ as being evident,

let us take $p > 3$.

Suppose that $a$ is any one of the $p-1$ positive integers

$$1,2,3,\ldots\ldots\ldots\ldots\ldots p-1$$

and consider the linear congruence

$$ax \equiv 1(mod\ p)$$

Then,

$$\gcd(a, p) = 1.$$

Since, we know the result the linear congruence $ax \equiv b(mod n)$ has a solution if and only if $d|b$,

where $d = \gcd(a, n)$.

If $d|b$, then it has $d$ mutually incongruent solutions modulo $n$.

Therefore, this congruence admits a unique solution modulo $p$;

hence, there is a unique integer $a'$,

with $1 \leq a' \leq p - 1$, satisfying $aa' \equiv 1(mod\ p)$.

Because $p$ is prime, $a = a'$ if and only if $a = 1\ or\ a = p - 1$.

Indeed, the congruence $a^2 \equiv 1(mod\ p)$ is equivalent to

$$(a - 1).(a + 1) \equiv 0(mod p).$$

Therefore, either $a - 1 \equiv 0(mod p)$, in which case $a = 1\ or\ a + 1 = 0(mod p)$, in which case $a = p - 1$.

If we omit the numbers 1 and $p - 1$, the effect is to group the remaining integers $2,3, \ldots \ldots p - 2$ into pairs $a, a'$ where $a \neq a'$, such that their product

$$aa' \equiv 1(mod p).$$

When these $(p - 3)/2$ congruences are multiplied together and the factors rearranged,

we get $2, 3, \ldots \ldots \ldots \ldots \ldots \ldots (p - 2) \equiv 1(mod\ p)$

$$(p - 2)! \equiv 1(mod\ p).$$

Now multiply by $(p - 1)$ to obtain the congruence

$$(p - 1)! \equiv p - 1 \equiv -1(mod\ p).$$

As was to be proved.

## CHECK YOUR PROGRESS

Solve the following multiple-choice questions:

**CYP 7.** Wilson's theorem states that a positive integer $p > 1$ is prime if and only if $(p - 1)! \equiv -1(mod\ p)$.

**a.** $(p - 1)! \equiv 0(mod\ p)$

**b.** $(p-1)! \equiv 1(mod\ p)$

**c.** $(p-1)! \equiv -1(mod\ p)$

**d.** $(p-1)! \equiv p(mod\ p)$

**CYP 8.** Using Wilson's theorem, the value of $4!\ (mod 5)$ is:

**a.** 0

**b.** 1

**c.** 2

**d.** 4

## 4.7. IMPORTANT RESULTS:

**Theorem 1.** If $p$ is an odd prime, any prime factor $q$ of $M_p = 2^p - 1$ must satisfy two conditions:

**i.** $q \equiv 1(mod 2p)$

**ii.** $q \equiv \pm 1(mod 8)$

**Proof:**

**i.** Condition $q \equiv 1(mod 2p)$

This condition states that any prime divisor $q$ of $2^p - 1$ must be one more than a multiple of $2p$.

- Order of 2: Since $q$ divides $2^p - 1$, we have $2^p \equiv 1(mod q)$. This implies that the multiplicative order of $2(mod q)$ is $p$ (it cannot be 1 because $2^1 - 1 = 1$, and $q$ must be prime).
- Fermat's Little Theorem: By this theorem, $2^{q-1} \equiv 1(mod q)$. Therefore, the order $p$ must divide $q - 1 = kp, or\ q = kp + 1$.
- Parity: Since $p$ is an odd prime and $q$ is an odd prime, $q - 1$ is even. For $kp$ to be even when $p$ is odd, $k$ must be even. Thus, $q$ is of the form $2mp + 1$, which is equivalent to $q \equiv 1(mod 2p)$.

**ii.** Condition $q \equiv \pm 1(mod 8)$

This condition relates to whether 2 is a quadratic residue modulo $q$.

- Quadratic Residue: If $q$ divides $2^p - 1$, then $2^p \equiv 1(mod q)$. Multiplying both sides by 2 gives $2^{p+1} \equiv 2(mod q)$.
- Square Root of 2: Since $p$ is odd, $p + 1$ is even. This allows us to write $2^{p+1}$ as $\left(2^{(p+1)/2}\right)^2 \equiv 2\ (mod q)$. This shows that 2 is a "square"(quadratic residue) modulo $q$.

**iii.** Law of Quadratic Reciprocity: According to the Second Supplement to the law of Quadratic Reciprocity, the number 2 is a quadratic residue modulo a prime $q$ if and only if $q$ $1 or\ 7\ (mod 8)$, which is written as $q \equiv \pm 1(mod 8)$.

**Example:** $M_{11} = 2^{11} - 1 = 2047$.

For $p = 11$, any prime factor $q$ must satisfy:

**a.** $q \equiv 1(mod 22)$(Potential $q$: $23, 67, 89, 199, \ldots.$)

**b.** $q \equiv \pm 1(mod 8)$(Potential $q$: $7, 17, 23, 31, 41, 47, 71, 73, 79, 89 \ldots..$)

The actual factors of $M_{11}$ are 23 and 89, both of which satisfy both conditions:

- $23 = (1 \times 22) + 1\ and\ 23 \equiv 7 \equiv -1(mod 8)$ .
- $89 = (4 \times 22) + 1\ and\ 89 \equiv 1(mod 8)$ .

**Theorem 2:** The linear congruence $ax \equiv b(mod n)$ has a solution if and only if $d|b$, where $d = \gcd(a, n)$. If $d|b$, then it has $d$ mutually incongruent solutions modulo $n$.

**Proof:** Since we know that the given congruence is equivalent to the linear Diophantine equation $ax - ny = b$. We know the result:

The linear Diophantine equation $ax + by = c$ has a solution if and only if $d|c$, where $d = \gcd(a, b)$. If $x_0, y_0$ is any particular solution of this equation, then all other solutions are given by:

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

where $t$ is an arbitrary integer.

Therefore, it is known that the latter equation can be solved if and only if $d|b$; moreover, if it is solvable and $x_0, y_0$ is one specific solution, then any other solution has the form:

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

for some choice of $t$.

Among the various integers satisfying the first of these formulas, consider those that occur when $t$ takes on the succesive values $t = 0,1,2 \ldots \ldots . d - 1$:

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d} \ldots \ldots x_0 + \frac{(d-1)n}{d}$$

We claim that these integers are incongruent modulo $n$, and all other such integers $x$ are congruent to some one of them. If it happened that

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 (mod\ n)$$

Where $0 \leq t_1 < t_2 \leq d - 1$, then we would have:

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 (mod\ n)$$

Now $\gcd(n/d, n) = \frac{n}{d}$, we know that $ca \equiv cb (mod n)$ then $a \equiv b (mod\ n/d)$, where $d = gcd(c, n)$. Therefore, the factor $\frac{n}{d}$ could be canceled to arrive at the congruence

$$t_1 \equiv t_2 (mod\ d)$$

which is to say that $d/t_2 - t_1$. But this is impossible in view of the inequality $0 < t_2 - t_1 < d$.

It remains to argue that any other solution $x_0 + (n/d)t$ is congruent modulo $n$ to one of the $d$ integers listed above. The Division Algorithm permits us to write $t$ as $t = qd + r$, where $0 \leq r \leq d - 1$.

Hence,

$$x_0 + (n/d)t = x_0 + (n/d)[qd + r] = x_0 + nq + \frac{n}{d}r = x_0 + \frac{n}{d}r(modn)$$

With $x_0 + (n/d)r$ being one of our $d$ selected solutions.

This ends the proof.

The statement of the above theorem stating explicitly:

If $x_0$ is any solution of $ax \equiv b(modn)$, then the $d = \gcd(a, n)$ incongruent solutions are given by: $x_0, x_0 + (n/d), x_0 + 2(n/d) + \cdots x_0 + (d-1)(n/d)$.

**Corollary:** If $gcd(a, n) = 1$ then the linear congruence $ax \equiv b(modn)$, has a unique solution modulo $n$.

- In two variable that is congruences of the form

$$ax + by \equiv c(mod\ n)$$

**Theorem 3:** The linear congruence $ax \equiv b(mod\ n)$ has a solution if and only if $d|b, where\ d = \gcd(a, n)$. If $d|b$ then it has $d$ mutually incongruent solutions modulo $n$.

In analogy of above with theorem such a congruence has a solution if and only if $\gcd(a, b, n)$ divides c.

The condition for solvability holds if either $\gcd(a, n) = 1$ or $\gcd(b, n) = 1$.

Say $\gcd(a, n) = 1$.

When the congruence is expressed as $ax \equiv c - by(mod\ n)$ the corollary to above theorem guarantees a unique solution $x$ for each of the $n$ incongruent values of $y$.

Take as a simple illustration $7x + 4y \equiv 5(mod\ 12)$, that would be treated as $7x \equiv 5 - 4y\ (mod\ 12)$.

Substitution of $y \equiv 5(mod12)$ gives $7x \equiv -15(mod12)$;

but this is equivalent to $-5x \equiv -15(mod12)$ so that $x \equiv 3(mod12)$.

It follows that $x \equiv 3(mod12), y \equiv 5(mod12)$ is one of the 12 incongruent solutions of $7x + 5y \equiv 5(mod12)$.

Another solution having the same value of $x$ is $x \equiv 3(mod\ 12), y \equiv 8(mod\ 12)$.

**Theorem 4:** The system of linear congruences

$$ax + by \equiv r(mod\ n)$$
$$cx + dy \equiv s(mod\ n)$$

has a unique solution $n$ whenever $\gcd(ad - bc, n) = 1$.

**Proof:** Let us multiply the first congruence of the system by $d$, the second congruence by $b$, and subtract the lower result from the upper. These calculations yield:

$(ad - bc)x \equiv dr - bs(modn)$……..(i)

The assumption $\gcd(ad - bc, n) = 1$ ensures that the congruence

$$(ad - bc)z \equiv 1(modn)$$

possesses a unique solution: denote the solution by $t$, when congruence (i) is multiplied by $t$,

we obtain,

$x \equiv t(dr - bs)(modn)$.

A value for $y$ is found by a similar elimination process. That is, multiply the first congruence of the system by $c$, the second one by $a$, and subtract to end up with

$(ad - bc)y \equiv as - cr(modn)$…….(ii)

Multiplication of this congruence by $t$ leads to

$$y \equiv t(as - cr)(modn)$$

**Theorem 5:** The quadratic congruence $x^2 + 1 \equiv 0(modp)$, where $p$ is an odd prime, has solution if and only if $p \equiv 1(mod\ 4)$.

**Proof.** Let $a$ be any solution of $x^2 + 1 \equiv 0(modp)$, so that $a^2 \equiv -1(modp)$. Because $p \nmid a$, the outcome of applying Fermat's theorem is

$1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2}(mod\ p)$.

The possibility that $p = 4k + 3$ for some $k$ does not arise. If it did, we would have:

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1$$

hence, $1 \equiv -1(modp)$. The net result of this is that $p/2$, which is patently false. Therefore, $p$

must be of the form $4k + 1$.

Now for the opposite direction. In the product,

$(p-1)! = 1.2 \ldots \ldots \ldots \ldots \ldots \frac{p-1}{2}. \frac{p+1}{2} \ldots \ldots \ldots \ldots . (p-2)(p-1)$

We have the congruences:

$$p - 1 \equiv -1(modp)$$

$$p - 2 \equiv -1(modp)$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$\frac{p+1}{2} \equiv -\frac{p-1}{2}(modp)$$

$$(p-1)! = 1.(-1).2.(-2) \ldots \ldots \ldots \ldots \ldots \frac{p-1}{2}. \left(-\frac{p-1}{2}\right)(modp)$$

$$\equiv (-1)^{(p-1)/2}\left(1.2 \ldots \frac{p-1}{2}\right)^2 (modp)$$

Because there are $\frac{p-1}{2}$ minus signs involved. It is at this point that Wilson's theorem can brought to bear; for $-1 \equiv (-1)^{(p-1)/2}\left[\left(\frac{p-1}{2}\right)!\right]^2 (mod\ p)$.

If we assume that $p$ is of the form $4k + 1$, then $(-1)^{(p-1)/2} = 1$, leaving us with the congruence: $-1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 (mod\ p)$.

The conclusion is that the integer $\left[\left(\frac{p-1}{2}\right)\right]!$ Satisfies the quadratic congruence $x^2 + 1 \equiv 0(modp)$.

## 4.8. EXAMPLES:

**Example 1:** Consider the linear congruence $18x \equiv 30(mod42)$. Because $gcd(18, 42) = 6$ and 6 surely divides 30. Now the above theorem gurantees the existence of exactly six solutions which are incongruent modulo 42. The six solutions are as follows:

$$x \equiv 4 + \left(\frac{42}{6}\right)t \equiv 4 + 7t(mod42) \qquad t = 0,1,2 \ldots \ldots .5$$

Or, plainly enumerated,

$$x \equiv 4, 11, 18, 25, 32, 39 (mod\ 42)$$

**Example 2:** In modern modular arithmetic notation, Sun Tzu's specific problem is written as a system of simultaneous linear congruences:

$$x \equiv 2 (mod\ 3)$$
$$x \equiv 3 (mod\ 5)$$
$$x \equiv 2 (mod\ 7)$$

From Chinese Remainder Theorem we have $n = 3.5.7 = 105\ and$

$$N_1 = \frac{n}{3} = 35, N_2 = \frac{n}{5} = 21, N_3 = \frac{n}{7} = 15,$$

Now the linear congruences

$$35x \equiv 1 (mod\ 3)$$
$$21x \equiv 1 (mod\ 5)$$
$$15x \equiv 1 (mod\ 7)$$

are satisfied by $x_1 = 2, x_2 = 1, x_3 = 1,$ respectively. Thus, a solution of the system is given by:

$$x = 2.35.2 + 3.21.1 + 2.15.1 = 233$$

Modulo 105, we get the unique solution $x = 233 \equiv 23 (mod\ 105)$.

**Example 3 :** Solve the linear congruence:

$$17x \equiv 9 (mod\ 276)$$

Since $276 = 3.4.23$, this is equivalent to finding a solution for the system of congruences:

$$17x \equiv 9 (mod\ 3) \text{ or } x \equiv 0 (mod\ 3)$$
$$17x \equiv 9 (mod\ 4) \text{ or } x \equiv 1 (mod\ 4)$$
$$17x \equiv 9 (mod\ 23) \text{ or } x \equiv 9 (mod\ 23)$$

Note that if $x \equiv 0 (mod\ 3)$, then $x = 3k$ for any integer $k$. We substitute into the second congruence of the system and obtain

$$3k \equiv 1 (mod\ 4)$$

Multiplication of both sides of this congruence by 3 gives us:

$$k \equiv 9k \equiv 3 (mod 4)$$

So that $k = 3 + 4j$, where $j$ is an integer. Then

$x = 3(3 + 4j) = 9 + 12j.$

For $x$ to satisfy the last congruence, we must have:

$$17(9 + 12j) = 9(mod\ 23)$$

Or

$$204j = -144(mod 23),$$

Which reduces to

$$3j \equiv 6(mod\ 23):$$

In consequence

$$j \equiv 2(mod\ 23)$$

This yields

$j = 2 + 23t$, with $t$ an integer, whence:

$x = 9 + 12(2 + 23t) = 33 + 276t.$

All in all $x \equiv 33(mod\ 276)$

Provides a solution to the system of congruence and in turn, a solution to

$$17x \equiv 9(mod\ 276)$$

**Example 4:** Consider the system of linear congruences

$$7x + 3y \equiv 10(mod\ 16)$$

$$2x + 5y \equiv 9(mod\ 16)$$

Because $\gcd(7.5 - 2.3.16) = \gcd(29, 16) = 1$ a solution exists.

$7x + 3y \equiv 10(mod\ 16)$ ….(iii)

$2x + 5y \equiv 9(mod\ 16)$……(iv)

multiplying the first congruence eq(iii) of the system by 5, the second congruence eq(iv) by 3, and subtracting, we arrive at $29x \equiv 5.10 - 3.9 \equiv 23(mod\ 16)$.

Or what is the same thing $13x \equiv 7(mod\ 16)$. Multiplication of this congruence by 5 (nothing that $(5.13 \equiv 1(mod\ 16))$ produces $x \equiv 35 \equiv 3(mod\ 16)$. When the variable $x$ is eliminated from the system of congruences in a like manner, it is found that, $29y \equiv 7.9 - 2.10 \equiv 43(mod\ 16)$.

But then $13y \equiv 11(mod\ 16)$, which upon multiplication by 5, results in $y \equiv 55 \equiv 7(mod\ 16)$.

The unique solution of our system turns out to be

$x \equiv 3(mod\ 16)$ and $y \equiv 7(mod\ 16)$.

**Example 5:** Find the remainder when 10! is divided by 11.

**Solution:** Wilson Theorem states that for any prime $p$;

If $p$ is a prime, then $(p-1)! \equiv -1(mod\ p)$.

Here, $p = 11$, which is a prime number.

Therefore, $(11-1) = 10$.

$$10! \equiv -1(mod\ 11).$$

A remainder of $-1$ modulo 11 is equivalent to: $-1 + 11 = 10$.

**Example 6:** Find the remainder when $16! + 2$ is divided by 17.

**Solution:** Wilson Theorem states that for any prime $p$;

If $p$ is a prime, then $(p-1)! \equiv -1(mod\ p)$

$$(17-1)! \equiv -1(mod\ 17)$$

Substitute the value of 16! Into the original expression:

$$16! + 2 \equiv -1 + 2(mod\ 17)$$

$$-1 + 2 = 1$$

The remainder when when $16! + 2$ is divided by 17.

**Example 7:** What is the remainder when 18! is divided by 23.

**Solution:** The nearest prime greater than 18 is 23.

Using Wilson theorem:

$$22! \equiv -1(mod\ 23).$$

Break apart 22! Until isolate the target term (18!):

$$22 \times 21 \times 20 \times 19 \times 18! \equiv -1(mod 23)$$

Convert each of the large multiplying factors into their smaller, negative equivalents modulo 23;

$$22! \equiv -1(mod\ 23)$$
$$21! \equiv -2(mod\ 23)$$
$$20! \equiv -3(mod\ 23)$$
$$19! \equiv -4(mod\ 23)$$

substitute these back into the equation:

$$(-1) \times (-2) \times (-3) \times (-4) \times 18! \equiv -1(mod23)$$
$$24 \times 18! \equiv -1(mod23)$$

Since $24 \equiv -1(mod23)$, the equation simplifies directly to:

$$18! \equiv 22(mod23)$$

The remainder when when $18!$ is divided by $23$ is $22$.

## 4.9 SUMMARY:

This unit introduced some important topics in number theory related to prime numbers and congruences. It began with Mersenne primes, a special class of prime numbers that have fascinated mathematicians for centuries because of their unique properties and their connection with perfect numbers. The unit highlighted their historical development and importance in modern computational mathematics.

The concept of linear congruence was then discussed. Linear congruences are mathematical statements involving an unknown quantity and are widely used in solving problems related to divisibility and remainders. The conditions for the existence of solutions and methods for finding such solutions were studied.

The Chinese Remainder Theorem was presented as a powerful tool for solving several congruence conditions simultaneously. This theorem, originating from ancient Chinese mathematics, provides a systematic way to determine a number satisfying multiple remainder conditions and has significant applications in computer science, cryptography, and coding theory.

The unit also examined Wilson's Theorem, an important result that provides a criterion for identifying prime numbers. Various examples illustrated its use in determining remainders and testing primality.

Finally, several important theorems and worked examples were included to strengthen understanding of the concepts. Overall, the unit demonstrated how prime numbers and congruences form a fundamental part of number theory and contribute to many modern technological applications.

## 4.10 GLOSSARY:

i. **Euclid's Algorithm:** Let $k > 0$ be an integer and $j$ be any integer. Then $\exists$ unique integers $q$ and $r$ such that $j = kq + r$, where $0 \leq r < k$.

ii. **Greatest Common Divisor:** An integer $d > 0$ is called greatest common integer (g.c.d.) of two integers $a, b$ (non zero) if

**A.** $d|a, d|b$

**B.** If $c|a, c|b$ then $c|d$.

**C.** We write $d = g.c.d.(a, b)$ or simply $d = (a, b)$.

iii. **Cyclic group:** A group $G$ is called a cyclic group if $\exists$ an element $a \in G$, such that every element of $G$ can be expressed as a power of $a$. In that case $a$ is called generator of $G$.

iv. **Euler's Theorem:** *Let* $a, \mathrm{n}\ (\mathrm{n} \geq 1)$ *be any integers such that* $g.c.d\ (a, n) = 1, then\ a^{\varphi(\mathrm{n})} \equiv 1 (mod n)$.

v. **Diophantine equation:** A Diophantine equation is a polynomial equation, usually containing two or more unknowns, where the only valid solutions sought are integers. Named after the ancient Greek mathematician Diophantus of Alexandria, these equations are a fundamental pillar of number theory. While they look like standard algebraic equations, restricting the domain to whole numbers makes them uniquely challenging and algebraically complex.

vi. **Congruence**: A mathematical **congruence** asserts that two integers leave the identical remainder when divided by a positive integer called

the modulus. Formally written as a $\equiv b(modn)$, this concept means that the modulus a $n$ perfectly divides the difference $a - b$.

vii. **Prime and Composite Number:** A prime number is a whole number greater than 1 that cannot be formed by multiplying two smaller natural numbers. In other words, it has exactly two distinct positive divisors: 1 and itself. Numbers greater than 1 that are not prime are called composite numbers. The number 1 is unique; it is classified as neither prime nor composite.

## 4.11. REFERENCES:


1. Burton, David M. *Elementary Number Theory*. 7th ed., McGraw-Hill Education, 2011.
2. Niven, Ivan, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. 5th ed., Wiley, 1991.
3. Pundir, Sudhir K., and Rajiv Pundir. *Algebra and Number Theory*. Pragati Prakashan, 2010.
4. Titu Andreescu, and Dorin Andrica. *Number Theory: Structures, Examples, and Problems*. Birkhäuser, 2009.


## 4.12. SUGGESTED READINGS:-


1. Lipschutz, Seymour. *Schaum's Outline of Theory and Problems of Number Theory*. McGraw-Hill, 1968.
2. https://nptel.ac.in/courses/111101137


## 4.13. TERMINAL QUESTIONS:

**TQ1:** Define a Mersenne prime. Show that $2^7 - 1$ is a Mersenne prime.

**TQ2:** Explain the relationship between Mersenne primes and perfect numbers.

**TQ3:** Define a linear congruence and describe the conditions for its

solvability.

**TQ4:** Solve the linear congruence $7x \equiv 5(mod12)$

**TQ5:** State and prove the theorem for the existence of solutions of the congruence $ax \equiv b(modn)$

**TQ6:** State and prove the Chinese Remainder Theorem.

**TQ7:** Solve the system of congruences:

$$x \equiv 2(mod3), x \equiv 3(mod5), x \equiv 2(mod7),$$

**TQ8:** Discuss the applications of the Chinese Remainder Theorem in number theory and cryptography.

**TQ9:** State and prove Wilson's Theorem. Hence test whether 13 is a prime number.

**TQ10:** Using Wilson's Theorem, verify that 7 is prime and explain the limitations of Wilson's Theorem as a primality test.

## 4.14. ANSWERS:

**Answer of Terminal Questions:**

**TQ4:** $x \equiv 11(mod12), x = 11 + 12k, \forall k \in Z.$

**TQ7:** $23 \equiv 2(mod3), 23 \equiv 3(mod5), 23 \equiv 2(mod7)$, x = 23 satisfies all three congruences.

**Answer of Check your progress Questions:**

**CYP1**. $b. 2^p - 1$

**CYP2.** 31.

**CYP3.** True.

**CYP4.** False.

**CYP5.** c, pairwise relatively prime integers.

**CYP6.** b, A number satisfying several congruences simultaneously.

**CYP7.** c, $(p-1)! \equiv -1(mod\ p)$.

**CYP8.** d, 4.

# COURSE NAME: NUMBER THEORY

# COURSE CODE: MAT-606

# BLOCK - II: NUMBER THEORETIC FUNCTIONS

# UNIT-5: *NUMBER THEORETIC FUNCTIONS FOR SUM AND NUMBER OF DIVISORS*

## CONTENTS:



## 5.1 *INTRODUCTION*

The study of number theoretic functions can be traced back to ancient Greek mathematics. Around 300 BCE, Euclid investigated prime numbers and divisibility in his work *Elements*. His results laid the foundation for later developments in arithmetic functions. Certain functions are found to be of special importance in connection with the study of the divisors of an integer. Any function whose domain of definition is the set of positive integers is said to be a number-theoretic (or arithmetic) function. Although the value of a number-theoretic function is not required to be a positive integer or, for that matter, even an integer, most of the number-theoretic functions that we shall encounter are integer-valued. Number-theoretic functions are functions defined on the set of positive integers and play a fundamental role in number theory. Their development spans more than two millennia, from ancient studies of divisibility to modern analytic number theory and cryptography.

## 5.2 *OBJECTIVE*

Number theoretic functions (also called arithmetic functions) are functions defined on the set of positive integers and play a fundamental role in number theory. They

help describe properties of integers such as divisibility, primality, and factorization. After reading this unit you will be able to:

$(i)$ The function of $\tau$ *and* $\sigma$

$(ii)$ multiplicative functions

## 5.3 *THE FUNCTION OF* $\tau$ *AND* $\sigma$

Given a positive integer n, let $\boldsymbol{\tau}$**(n)** denote the number of positive divisors of n and $\boldsymbol{\sigma}$**(n)** denote the sum of these divisors.

For an example of these notions, consider n = 12. Because 12 has the positive divisors 1, 2, 3, 4, 6, 12, we find that

$\tau(12) = 6$ and $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$

**Remark:** For the first few integers

$\tau(1) = 1$, $\tau(2) = 2$, $\tau(3) = 3$, $\tau(4) = 3$, $\tau(5) = 2$, $\tau(6) = 4$ and so on

And $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 4$, $\sigma(4) = 7$, $\sigma(5) = 6$, $\sigma(6) = 12$ and so on

**Question 1:** Find $\tau(18)$ and $\sigma(18)$ .

**Solution:** The divisors of 18 are 1, 2, 3, 6, 9, 18

therefore, $\tau(18) = 6$ and $\sigma(18) = 1 + 2 + 3 + 6 + 9 + 18 = 39$.

**Question 2:** If $p$ is a prime number then find $\tau(p)$ and $\sigma(\mathrm{p})$.

**Solution:** prime $p$ has only two factors 1 and $p$ itself. Therefore, $\tau(p) = 2$ and $\sigma(\mathrm{p}) = p + 1$.

**Remark:** Before studying the functions $\tau$ and $\sigma$ in more detail, we wish to introduce notation that will clarify a number of situations later. It is customary to interpret the symbol $\sum_{d/n} f(d)$

to mean, "Sum the values $f(d)$ as $d$ runs over all the positive divisors of the positive integer n." For instance, we have

$$\sum_{d\,|\,20} f(d) = f(1) + f(2) + f(4) + f(5) + f(10) + f(20)$$

With this understanding, $\sigma$ and $\tau$ may be expressed in the form

$$\tau(n) = \sum_{d\,|\,n} 1 \qquad \sigma(n) = \sum_{d\,|\,n} d$$

The notation $\sum_{d/n} 1$, in particular, says that we are to add together as many 1 's as there are positive divisors of n.

The integer 10 has the four positive divisors 1, 2, 5, 10, whence

$$\tau(10) = \sum_{d\,|\,10} 1 = 1 + 1 + 1 + 1 = 4$$

And

$$\sigma(10) = \sum_{d\,|\,10} d = 1 + 2 + 5 + 10 = 18$$

Our first theorem makes it easy to obtain the positive divisors of a positive integer n once its prime factorization is known.

**Theorem 5.1:** If $n = p_1^{k_1}p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of $n$ are precisely those integers $d$ of the form $d = p_1^{a_1}p_2^{a_2} \dots p_r^{a_r}$ Where $0 \le a_i \le k_i$ $(i = 1, 2, \dots, r)$.

**Proof:** Note that the divisor d = 1 is obtained when $a_1 = a_2 = \cdots = a_r = 0$, and $n$ itself occurs when $a_1 = k_1, a_2 = k_2, \dots, a_r = k_r$. Suppose that d divides, $n$ nontrivially; say, $n = dd'$, where d > 1, d' > 1. Express both d and d' as products of (not necessarily distinct) primes:

$$d = q_1q_2 \dots q_s = p_1^{a_1}p_2^{a_2} \dots p_r^{a_r}$$

With $t_j, q_i$ prime then

$$p_1^{k_1}p_2^{k_2} \dots p_r^{k_r} = q_1q_2 \dots q_st_1t_2 \dots t_u$$

are two prime factorizations of the positive integer n. By the uniqueness of the prime factorization, each prime $q_i$; must be one of the $p_j$. Collecting the equal primes into a single integral power, we get

$$d = q_1q_2 \dots q_s = p_1^{a_1}p_2^{a_2} \dots p_r^{a_r}$$

where the possibility that $a_i$ = 0 is allowed.

**Conversely**, every number $d = p_1^{a_1}p_2^{a_2} \dots p_r^{a_r}$ $(0 \le a_i \le k_i)$ turns out to be a divisor of n. For we can write

$$n = p_1^{k_1}p_2^{k_2} \dots p_r^{k_r}$$
$$n = (p_1^{a_1}p_2^{a_2} \dots p_r^{a_r})(p_1^{k_1-a_1}p_2^{k_2-a_2} \dots p_r^{k_r-a_r})$$
$$n = dd'$$

With $d' = p_1^{k_1-a_1}p_2^{k_2-a_2} \dots p_r^{k_r-a_r}$ and $k_i - a_i \ge 0$ for each $i$. Then $d' > 0$ and $d/n$.

**Theorem 5.2:** If $n = p_1^{k_1}p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of n > 1, then

(a) $\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$, and

(b) $\sigma(n) = \dfrac{p_1^{k_1+1} - 1}{p_1 - 1} \dfrac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}$.

**Proof:** According to Theorem 5.1, the positive divisors of n are precisely those integers

$$d = p_1^{a_1}p_2^{a_2} \dots p_r^{a_r}$$

where $(0 \le a_i \le k_i)$. There are $k_1 + 1$ choices for the exponent $a_1$; $k_2 + 1$ choices for $a_2$, ... and $k_r + 1$ choices for $a_r$. Hence, there are

$$(k_1 + 1)(k_2 + 1) \dots (k_r + 1)$$ possible divisors of n.

To evaluate $\sigma(p)$, consider the product

$$(1 + p_1 + p_1^2 + \cdots + p_1^{k_1})(1 + p_2 + p_2^2 + \cdots + p_2^{k_2}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r})$$

Each positive divisor of n appears once and only once as a term in the expansion of this product, so that

$$\sigma(n) = (1 + p_1 + p_1^2 + \cdots + p_1^{k_1}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r})$$

Applying the formula for the sum of a finite geometric series to the $ith$ factor on the right-hand side, we get

$$1 + p_i + p_i^2 + \cdots + p_i^{k_i} = \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

It follows that

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

Corresponding to the Σ notation for sums, the notation for products may be defined using Π, the Greek capital letter pi. The restriction delimiting the numbers over which the product is to be made is usually put under the Π sign. Examples are

$$\prod_{1 \le d \le 5} f(d) = f(1)f(2)f(3)f(4)f(5)$$

$$\prod_{d \mid 9} f(d) = f(1)f(3)f(9)$$

$$\prod_{\substack{p \mid 30 \\ p \text{ prime}}} f(p) = f(2)f(3)f(5)$$

With this convention, the conclusion to Theorem 5.2 takes the compact form: If $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ is the prime factorization of n > 1, then

$$\tau(n) = \prod_{1 \le i \le r} (k_i + 1)$$

And

$$\sigma(n) = \prod_{1 \le i \le r} \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

**Question 3:** Find $\tau(180)$ and $\sigma(180)$.

**Solution:** The number $180 = 2^2.3^2.5$ has

$$\tau(180) = (2 + 1)(2 + 1)(1 + 1) = 18$$

positive divisors. These are integers of the form $2^{a_1}.3^{a_2}.5^{a_3}$

where $a_1$ = 0, 1, 2; $a_2$ = 0, 1, 2; and $a_3$ = 0, 1. Specifically, we obtain

1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180

The sum of these integers is

$$\sigma(180) = \frac{2^3 - 1}{2 - 1} \frac{3^3 - 1}{3 - 1} \frac{5^2 - 1}{5 - 1} = \frac{7}{1} \frac{26}{2} \frac{24}{4} = 7 \cdot 13 \cdot 6 = 546$$

**Theorem 5.3:** For any integer $n > 1$, $\tau(n)$ is odd iff $n$ is a perfect square.

**Proof:** let $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ be square of an integer.

Then $a_1, a_2, \ldots, a_k$ are all even.

Therefore, $(a_1 + 1), (a_2 + 1), \ldots (a_k + 1)$ are all odd

Now $\tau(n) = (a_1 + 1)(a_2 + 1) \ldots \ldots (a_k + 1)$

= an odd integer (product of odd integers is an odd integer)

**Conversely:** let $\tau(n) = (a_1 + 1)(a_2 + 1) \ldots \ldots (a_k + 1)$ is an odd integer. Then each $a_i + 1, i = 1, 2, \ldots, k$ is an odd integer. This implies each $a_i$ is even i.e.

$$a_i = 2m_i$$

Therefore $n = p_1^{2m_1} p_2^{2m_2} \dots p_k^{2m_k}$

$n = \left(p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}\right)^2$

This shows that $n$ is a perfect square.

**Remark: Applications of $\sigma(n)$ functions**

- Classification of **perfect numbers**, **abundant numbers**, and **deficient numbers**.
- Study of divisor-related problems.
- Analysis of arithmetic functions and multiplicative functions.
- Cryptography and computational number theory.

**Applications of $\tau(n)$ function**

- Finding the number of factors of an integer.
- Studying highly composite numbers.
- Analyzing divisor-related problems in number theory.
- Computational mathematics and cryptography.

## 5.4 *MULTIPLICATIVE FUNCTION*

A number-theoretic function f is said to be multiplicative if f(mn) = f(m)f(n) whenever gcd (m, n) = 1.

**Theorem 5.4:** The functions $\tau$ and $\sigma$ are both multiplicative functions.

**Proof.** Let m and n be relatively prime integers. Because the result is trivially true if either morn is equal to 1, we may assume that m > 1 and n > 1. If

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \quad \text{and} \quad n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

are the prime factorizations of m and n, then because gcd (m, n) = 1, no $p_i$ can occur among the $q_j$. It follows that the prime factorization of the product mn is given by

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}$$

Appealing to Theorem 5.2, we obtain

$$\begin{aligned}\tau(mn) &= [(k_1 + 1) \cdots (k_r + 1)][(j_1 + 1) \cdots (j_s + 1)] \\ &= \tau(m)\tau(n)\end{aligned}$$

In a similar fashion, Theorem 5.2 gives

$$\begin{aligned}\sigma(mn) &= \left[\frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}\right]\left[\frac{q_1^{j_1+1} - 1}{q_1 - 1} \cdots \frac{q_s^{j_s+1} - 1}{q_s - 1}\right] \\ &= \sigma(m)\sigma(n)\end{aligned}$$

Thus, $\tau$ and $\sigma$ are both multiplicative functions.

**Theorem 5.5:** If $f$ is a multiplicative function and $S(n) = \sum_{d/n} f(d)$ then $S(n)$ is also multiplicative.

**Proof.** Let m and n be relatively prime integers. Then

$$\begin{aligned}S(mn) &= \sum_{d/mn} f(d) \\ &= \sum_{\substack{d_1/m \\ d_2/n}} f(d_1 d_2)\end{aligned}$$

$$= \sum_{\substack{d_1/m \\ d_2/n}} f(d_1)f(d_2)$$
$$= \sum_{d_1/m} f(d_1) \sum_{d_2/n} f(d_2)$$
$$= S(m)S(n)$$

**Question 4:** Evaluate $\tau$ and $\sigma$ for $n = 3655$.

**Solution:** we have $3655 = 5^1.17^1.43^1$

Therefore $\tau(3655) = (1+1)(1+1)(1+1) = 8$ .

And $\sigma(3655) = \left(\frac{5^2-1}{5-1}\right)\left(\frac{17^2-1}{17-1}\right)\left(\frac{43^2-1}{43-1}\right)$

$= \frac{(25-1)(289-1)(1849-1)}{4.16.42}$

$= \frac{24\times288\times1848}{4\times16\times42} = 18 \times 264 = 4752$ .

**Question 5:** Evaluate $\tau$ and $\sigma$ for $n = 3000$.

**Solution:** we have $3000 = 2^3.3^1.5^3$

Therefore $\tau(3000) = (3+1)(1+1)(3+1) = 32$ .

And $\sigma(3000) = \left(\frac{2^4-1}{2-1}\right)\left(\frac{3^2-1}{3-1}\right)\left(\frac{5^4-1}{5-1}\right)$

$= \frac{(16-1)(9-1)(625-1)}{1\times2\times4}$

$= 15 \times 4 \times 156 = 9360.$

**Question 6:** If $f(n) = n^2 + 2$ and $n = 6$ then show that $\sum_{d/6} f(d) = \sum_{d/6} f\left(\frac{6}{d}\right)$.

Solution: here divisors of 6 are given by

d = 1, 2, 3, 6

therefore, $\frac{6}{d} = 6, 3, 2, 1$

Now $\sum_{d/6} f(d) = (1^2+2) + (2^2+2) + (3^2+2) + (6^2+2)$

$= 58.$

And $\sum_{d/6} f\left(\frac{6}{d}\right) = (6^2+2) + (3^2+2) + (2^2+2) + (1^2+2)$

$= 58.$

Thus, $\sum_{d/6} f(d) = \sum_{d/6} f\left(\frac{6}{d}\right)$.

**Question 7:** Verify that $\tau(n) = \tau(n+1) = \tau(n+2)$ holds for $n = 4503$.

**Solution:** we have $n = 4503 = 3.19.79$

$\tau(n) = \tau(4503) = (1+1).(1+1).(1+1) = 8$

Further $n + 1 = 4504 = 2^3.563$

$\therefore$ $\tau(n+1) = (3+1).(1+1) = 8$

Finally, $n + 2 = 4505 = 5.17.53$

$\therefore$ $\tau(n+2) = (1+1).(1+1).(1+1) = 8.$

Thus, $\tau(n) = \tau(n+1) = \tau(n+2).$

**Question 8:** Show that $\tau(n)$ is equal to the lattice points on the hyperbola $xy = n$ lying in the first quadrant.

**Solution:** Suppose $d_1, d_2, \dots, d_r$ be the divisors of $n$. Then the lattice points $\left(d_1, \frac{n}{d_1}\right)$, $\left(d_2, \frac{n}{d_2}\right), \dots, \left(d_r, \frac{n}{d_r}\right)$ lies on the hyperbola $xy = n$ in the first quadrant. Also, if

$\left(d, \frac{n}{d}\right)$ be any lattice point on the hyperbola $xy = n$ then it belongs to above lattice points as $\frac{n}{d}$ is an integer. Therefore, $\tau(n)$ is equal to the number of lattice points on the hyperbola $xy = n$.

## 5.5 *BEHAVIOUR OF $\tau(n)$ AS $n \to \infty$*

For every prime p we have $\tau(p) = 2$. For any integer $n$ there are at least two divisors 1 and $n$. Therefore, $\tau(n) \geq 2$ for all $n$. For any integer of the form $n = p^a, p$ is a prime, we have
$\tau(n) = a + 1$. This depends on $a$. For large $a$, $\tau(n)$ is sufficiently large.
Therefore, $\lim_{n\to\infty} \tau(n) = \infty$. The behavior of $\tau(n)$ is irregular.

## 5.6 *BEHAVIOUR OF $\sigma(n)$ AS $n \to \infty$*

We know that $\sigma(n) > n$. Therefore, $\sigma(n)$ takes values large than any given sufficiently large number $n$. Hence, $\lim_{n\to\infty} \sigma(n) = \infty$. But it is not an increasing function as shown below:
Let $p = 2^r + 1, r > 1$ be a prime $> 3$ then

$$\sigma(p-1) = \sigma(2^r) = 2^r + 2^{r-1} + \cdots + 2 + 1 > 2^r + 2 = p + 1 = \sigma(p)$$

If $p - 1 = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ then

$$\begin{aligned}\sigma(p-1) &= \sigma\left(p_1^{r_1}\right)\sigma\left(p_2^{r_2}\right)\ldots\sigma\left(p_k^{r_k}\right)\\ &= \left(p_1^{r_1}+1\right)\left(p_2^{r_2}+1\right)\ldots\left(p_k^{r_k}+1\right)\\ &\geq p_1^{r_1}p_2^{r_2}\ldots p_k^{r_k} + \left(p_1^{r_1} + p_2^{r_2} + \cdots + p_k^{r_k}\right)\\ &= p - 1 + k + 1 \qquad [\because k > 1]\\ &> p + 1 = \sigma(p)\end{aligned}$$

$\sigma(n)$ is also irregular function.

## CHECK YOUR PROGRESS

**MCQ Questions**

**Problem 1.** The sigma function $\sigma(n)$represents:
A. Number of prime factors of $n$
B. Number of divisors of $n$
C. Sum of positive divisors of $n$
D. Sum of prime divisors of $n$

**Problem 2.** What is $\sigma(6)$?
A. 6
B. 10

C. 12
D. 14

**Problem 3.** The value of $\sigma(8)$is:
A. 12
B. 15
C. 18
D. 20

**Problem 4.** If pis a prime number, then σ(p)equals:
A. p
B. $p + 1$
C. $2p$
D. 1

**Problem 5.** The positive divisors of 10 are $1,2,5,10$. Hence $\sigma(10)$is:
A. 16
B. 18
C. 20
D. 22

**Problem 6.** Which of the following is the formula for $\sigma(p^k)$?
A. $k + 1$
B. $p^k + 1$
C. $\frac{p^{k+1}-1}{p-1}$
D. $p^{k+1} - 1$

**Problem 7.** Which of the following is a multiplicative arithmetic function?
A. $\sigma(n)$
B. $n^2$
C. $\log n$
D. $n + 1$

**Problem 8.** If $n = 2^2 \times 3$, then $\sigma(n)$is:
A. 24
B. 28
C. 18
D. 20

**Problem 9.** A perfect number $n$ satisfies:
A. $\sigma(n) = n$
B. $\sigma(n) = 2n$
C. $\sigma(n) = n + 1$
D. $\sigma(n) = 3n$

**Problem 10.** The value of $\sigma(1)$is:
A. 0
B. 1

C. 2
D. Undefined

**Problem 11.** If gcd $(m,n) = 1$, then:
A. $\sigma(mn) = \sigma(m) + \sigma(n)$
B. $\sigma(mn) = \sigma(m)\sigma(n)$
C. $\sigma(mn) = mn$
D. $\sigma(mn) = 1$

**Problem 12**. If $n = p^2$ where $p$ is prime, then:
A. $\sigma(n) = 1 + p$
B. $\sigma(n) = 1 + p + p^2$
C. $\sigma(n) = p^2$
D. $\sigma(n) = 2p$

**Problem 13.** The tau function $\tau(n)$represents:
A. Sum of divisors of $n$
B. Number of positive divisors of $n$
C. Number of prime divisors of $n$
D. Sum of prime divisors of $n$

**Problem 14.** Which formula gives $\tau(n)$when

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}?$$

A. $a_1 + a_2 + \cdots + a_r$
B. $(a_1 + 1)(a_2 + 1) \cdots (a_r + 1)$
C. $p_1 + p_2 + \cdots + p_r$
D. $a_1 a_2 \cdots a_r$

**Problem 15.** What is $\tau(24)$?
A. 6
B. 7
C. 8
D. 10

**Problem 16.** The tau function is:
A. Additive
B. Completely additive
C. Multiplicative
D. Constant

**Problem 17.** Find $\tau(100)$.
A. 7
B. 8
C. 9
D. 10

**Problem 18.** The smallest positive integer having exactly 6 divisors is:
A. 10
B. 12

C. 18
D. 20

## 5.7 *SUMMARY*

**(i)** The sigma function $\sigma(n)$gives the sum of all positive divisors of $n$, possesses strong multiplicative properties, and is a fundamental tool in the study of number theory. the sigma function $\sigma(n)$ provides valuable information about the divisor structure of integers and plays a central role in analytic and algebraic number theory. It is closely related to perfect numbers, divisor sums, and the distribution of integers with special arithmetic properties.
**(ii)** The tau function $\tau(n)$is a fundamental arithmetic function that counts the number of positive divisors of an integer. Its simple formula based on prime factorization makes it a powerful tool for studying the structure and properties of integers in number theory.
**(iii)** A number has an odd number of divisors if and only if it is a perfect square.
**(iv)** The history of number theoretic functions spans more than two thousand years, beginning with Euclid's study of divisibility and continuing through the contributions of Euler, Gauss, Dirichlet Today, arithmetic functions form a cornerstone of modern number theory and have important applications in mathematics, computer science, and information security.

## 5.8 *GLOSSARY*

1. Arithmetic Function
2. Number Theoretic
3. Divisor
4. Prime Number
5. Composite Number
6. Greatest Common Divisor (GCD)
7. Relatively Prime (Coprime)

## 6.8 *REFERENCES*


- **Burton, D. M.** (2007). Elementary number theory (6th ed.). McGraw-Hill.
- **T. M. Apostol**, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

- **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford.
- **Tom M. Apostol**, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York.
- **G. A. Jones and J. M. Jones**, *Elementary Number Theory*, Springer-Verlag, Berlin, 1998.
- **T. Nagell**, *Introduction to Number Theory*, Wiley, New York.


## 5.11 *TERMINAL QUESTIONS*

**Long answer type questions**

**1.** Find $\tau(n)$ and $\sigma(n)$ for $n = 7056$.

**2.** For $n = 957$ show that $\sigma(n) = \sigma(n+1)$.

**3.** Prove that $\sigma(2^{k-1}) = 2^k - 1$.

**4.** Define $\sigma$ function with examples.

**5.** Define $\tau(n)$ function with examples.

## 5.12 *ANSWERS*

**Answer of objective questions**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | C | **2:** | C | **3:** | B | **4:** | B |
| **5:** | B | **6:** | C | **7:** | A | **8:** | B |
| **9:** | B | **10:** | B | **11:** | B | **12:** | B |
| **13:** | B | **14:** | B | **15:** | B | **16:** | C |
| **17:** | C | **18:** | B | | | | |

# UNIT-6: THE MÖBIUS INVERSION FORMULA, GREATEST INTEGER FUNCTION

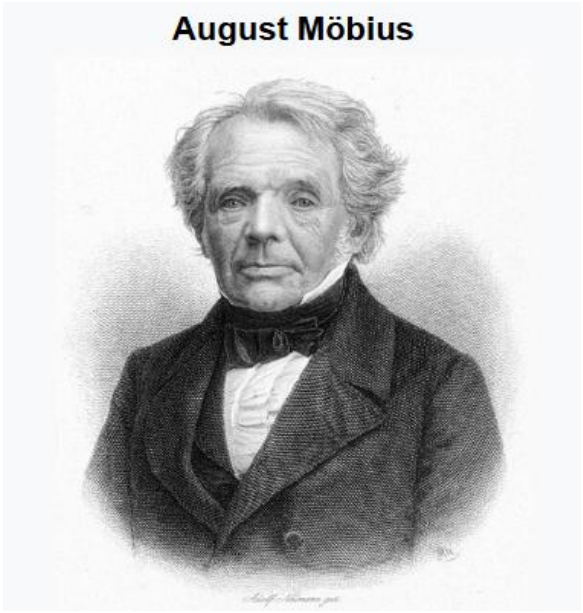
## CONTENTS:



## 6.1 *INTRODUCTION*

In number theory, two foundational ideas that grew out of attempts to understand arithmetic structure are the **Möbius inversion formula** and the **greatest integer function**. The Möbius inversion formula has its roots in the nineteenth century, emerging from the study of

multiplicative functions and divisor sums; it was introduced by the German mathematician **August Ferdinand Möbius** while investigating relationships between arithmetic functions defined on the divisors of integers. The formula provides a systematic way to invert summatory relations of the form $F(n) = \sum_{d|n} f(d)$, making it a powerful tool in analytic and algebraic number theory. In parallel, the greatest integer function, commonly denoted by $[x]$, arose naturally from the need to connect discrete arithmetic properties with continuous variables; it captures the integer part of a real number and appears prominently in counting arguments, estimates, and the study of distribution of integers. Together, these concepts illustrate a central theme of number theory: translating between discrete divisor-based structures and analytic expressions, a theme that has shaped the development of the subject from classical to modern times.




17 November 1790- 26 September 1868

https://en.wikipedia.org/wiki/August_Ferdinand_M%C3%B6bius

*Möbius was born in Schulpforta, Electorate of Saxony, and was descended on his mother's side from religious reformer Martin Luther. He was home-schooled until he was 13, when he attended the college in Schulpforta in 1803, and studied there, graduating in 1809. He then enrolled at the University of Leipzig, where he studied astronomy under the mathematician and astronomer Karl Mollweide. In 1813, he began to study astronomy under mathematician Carl Friedrich Gauss at the University of Göttingen, while Gauss was the director of the Göttingen Observatory. From there, he went to study with Carl Gauss's instructor, Johann Pfaff, at the University of Halle, where he completed his doctoral thesis The occultation of fixed stars in 1815. In 1816, he was appointed as Extraordinary Professor to the "chair of astronomy and higher mechanics" at the University of Leipzig. Möbius died in Leipzig in 1868 at the age of 77.*

## 6.2 *OBJECTIVE*

After reading this unit learners will be able,

- To introduce the Möbius function and develop the Möbius inversion formula as a fundamental tool for reversing divisor-sum relations between arithmetic functions.
- To understand the concept and properties of the greatest integer (floor) function and its role in connecting real numbers with integer values.
- To apply the Möbius inversion formula in solving problems involving arithmetic functions, divisor sums, and multiplicative functions.
- To use the greatest integer function in counting arguments, inequalities, and evaluations of number-theoretic sums.
- To illustrate how discrete and continuous methods interact in number theory through practical examples and standard identities.
- To build problem-solving skills by applying these concepts to classical results and exercises in elementary and analytic number theory.

## 6.3 *THE MÖBIUS $\mu$ – FUNCTION*

The Möbius $\mu$ – function, denoted by $\mu(n)$, is an important arithmetic function in number theory introduced by August Ferdinand Möbius. It is defined for every positive integer *n* as follows:

**Definition 1:** For a positive integer n, define $\mu$ by the rules,

$$\mu(n) = \begin{cases} 1; & \text{if } n = 1 \\ 0; & \text{if } p^2 \mid n \text{ for some prime } p \\ (-1)^r; & \text{if } n = p_1 p_2 p_3 \ldots p_r, \text{ where } p_i \text{ are distinct primes} \end{cases}$$

The Möbius $\mu$ – function plays a central role in the **Möbius inversion formula**, where it is used to invert divisor-sum relations between arithmetic functions, and it is fundamental in the study of multiplicative functions and many classical results in number theory.

**Example 1:** Find the value of first six natural numbers and also find the value of $\mu(30)$.

**Solution:** From the definition 1 of Möbius $\mu$ – function,

$\mu(1) = 1;\ \mu(2) = (-1)^1 = -1;\ \mu(3) = (-1)^1 = -1;\ \mu(4) = \mu(2^2) = 0$

$\mu(5) = (-1)^1 = -1;\ \mu(6) = \mu(2.3) = (-1)^2 = 1$ and $\mu(30) = \mu(2.3.5) = (-1)^3 = -1$

**Theorem 1:** The $\mu$ – function is a multiplicative function.

**Proof:** As we know that the number theoretic function *f* is said to be murltiplicative if,

$f(mn) = f(m)f(n)$, whenever $\gcd(m,n) = 1$.

So, if we want to show that $\mu -$ function is multiplicative, we have only to show that $\mu(mn) = \mu(m)\mu(n)$, whenever $\gcd(m,n) = 1$.

Now, let *m* and *n* be co-prime positive integers.

**Case I:** Either *m* or *n* is divisible by the square of a prime. Then *mn* is also divisible by the square of that prime. Hence,

$\mu(m) = 0 \ or \ \mu(n) = 0 \Rightarrow \mu(m)\mu(n) = 0$

So, we can say that $\mu(mn) = 0 = \mu(m)\mu(n)$

**Case II:** Both *m* and *n* are square –free. Since $\gcd(m,n) = 1$, their prime factorizations involve distinct primes. Suppose

$m = p_1 p_2 ... p_r ; \ n = q_1 q_2 ... q_s$

Where all $p_i$ and $q_j$ are distinct primes. Then,

$mn = p_1 p_2 ... p_r . q_1 q_2 ... q_s$ is also square free with $(r+s)$ distinct prime factors. Therefore,

$\mu(mn) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(m)\mu(n).$

Which complete the proof.

## 6.4 *THE MÖBIUS INVERSION FORMULA*

Let us see what happens if $\mu(d)$ is evaluated for all the positive divisors *d* of an integer *n* and the results are added. In the case where $n = 1$, the answer is easy;

Here, $\sum_{d|1} \mu(d) = \mu(1) = 1$

If $n > 1$, then put $F(n) = \sum_{d|n} \mu(d)$

To prepakkre the ground, we first calculate $F(n)$ for the power of a prime, say, $n = p^k$. So, the positive divisors of $p^k$ are $1, p, p^{2,}, ..., p^k$, so that

$$F(p^k) = \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + ... + \mu(p^k) = 1 + (-1) + 0 + 0 + ... + 0 = 0$$

Because $\mu$ is known to be a multiplicative function, an appeal to theorem that "if f is a multiplicative function and F is defined by $F(n) = \sum_{d|n} f(d)$ then F is multiplicative" is legitimate; this result guarantees that F is also multiplicative. Thus, if the canonical factorization of n is $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$, then $F(n)$ is the product of the values assigned to F for the prime powers in this representation.

$$F(n) = F(p_1^{k_1}) F(p_2^{k_2}) ... F(p_r^{k_r}) = 0$$

**Theorem 2:** For each positive integer $n \geq 1$,

$$\sum_{d|n} \mu(d) = \begin{cases} 1; \text{if } n = 1 \\ 0; \text{if } n > 1 \end{cases}$$

Where $d$ runs through the positive divisor of $n$

**Example 2:** For an illustration of this theorem, consider $n = 10$. The positive divisors of 10 are 1, 2, 5, 10 and the desired sum is,

$$\sum_{d|n} \mu(d) = \mu(1) + \mu(2) + \mu(5) + \mu(10) = 1 + (-1) + (-1) + 1 = 0$$

**Theorem 3: (Mobius inversion formula)** Let $F$ and $f$ be two number-theoretic functions related by the formula $F(n) = \sum_{d|n} f(d)$

Then, $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$

**Proof:** The two sum mentioned in the conclusion of the theorem are seen to be the same upon replacing the dummy index $d$ by $d' = n/d$; as $d$ ranges over all positive divisors of $n$, so does $d'$.

Carrying out the required computation, we get

$$\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d|n}\left(\mu(d)\sum_{c|(n/d)}f(c)\right)$$

$$=\sum_{d|n}\left(\sum_{c|(n/d)}\mu(d)f(c)\right) \qquad (1)$$

It is easily verified that $d\mid n$ and $c\mid(n/d)$ if and only if $c\mid n$ and $d\mid(n/c)$. Because of this, the last repression in Eq. (1) becomes

$$\sum_{d|n}\left(\sum_{c|(n/d)}\mu(d)f(c)\right)=\sum_{c|n}\left(\sum_{d|(n/c)}f(c)\mu(d)\right)=\sum_{c|n}\left(f(c)\sum_{d|(n/c)}\mu(d)\right) \qquad (2)$$

In compliance with theorem 2, the sum $\sum_{d|(n/c)}\mu(d)$ must vanish except when $n/c=1$ (that is, when $n=c$), in which case it is equal to 1, the upshot is that the right-hand side of Eq. (2) simplifies to

$$\sum_{c|n}\left(f(c)\sum_{d|(n/c)}\mu(d)\right)=\sum_{c=n}f(c).1=f(n)$$

**Example 3:** If $n=10$, then illustrate how the double sum in equation (2) is turned around.

$$\sum_{d|10}\left(\sum_{c|(10/d)}\mu(d)f(c)\right)=\mu(1)[f(1)+f(2)+f(5)+f(10)]+\mu(2)[f(1)+f(5)]+\mu(5)[f(1)+f(2)]$$

$$+\mu(10)f(1)$$

$$=f(1)[\mu(1)+\mu(2)+\mu(5)+\mu(10)]+f(2)[\mu(1)+\mu(5)]+f(5)[\mu(1)+\mu(2)]+f(10)\mu(1)$$

$$=\sum_{c|10}\left(\sum_{d|(10/c)}f(c)\mu(d)\right)$$

**Example 4:** To see how the Mobius inversion formula works in a particular case, we remind the reader that the functions $\tau$ and $\sigma$ may both be described as "sum functions".

$$\tau(n) = \sum_{d|n} 1 \text{ and } \sigma(n) = \sum_{d|n} d$$

**Theorem 4:** If $F$ is a multiplicative function and $F(n) = \sum_{d|n} f(d)$, then $f$ is also multiplicative.

**Proof:** Let $m, n$ are relatively prime positive integers. Then any divisor d of mn can be uniquely written as $d = d_1 d_2$, where $d_1 \mid m, d_2 \mid n$, and $\gcd(d_1, d_2) = 1$. Thus, using the inversion formula,

$$f(mn) = \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right) = \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right)$$

$$= \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right)$$

$$= f(m) f(n)$$

This completes the theorem.

**Note:** For $n \geq 1$, we define the sum

$$M(n) = \sum_{k=1}^{n} \mu(k)$$

Then $M(n)$ is the difference between the number of square-free positive integers $k \leq n$ with an even number of prime factors and those with an odd number of prime factors. For example, $M(n) = 2 - 4 = -2$. In 1897, Franz Mertens (1840-1927) published a paper with a 50-page table of values of $M(n)$ for $n$ = 1, 2,..., 10000. On the basis of the tabular evidence, Mertens concluded that the inequality

$|M(n)| < \sqrt{n}, n > 1$

is "very probable." (In the previous example, $|M(9)| = 2 < \sqrt{9}$.) This conclusion later became known as the Mertens conjecture. A computer search carried out in 1963 verified the conjecture for all n upto 10 billion. But is 1984, Andrew Odlyzko and Herman te Riele showed that the Mertens conjecture is flase. Their proof, which is involved the use of a computer, was indirect and produced no specific value of $n$ for which $|M(9)| \geq \sqrt{n}$; all it demonstrated was that such a number $n$ must exist somewhere. Subsequently, it has been shown that there is a counterexample to the mertens conjecture for at least one $n \leq (3.21)10^{64}$.

**Theorem 5:** If $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$, then $\sum_{d|n} |\mu(d)| = 2^k$.

**Proof:** As we know that, for every divisor $d$ for which $\mu(d) \neq 0$, we have $|\mu(d)| = 1$. Using definition of Mobius function, the number of divisor given by

$1 + {}^kC_1 + {}^kC_2 + ... + {}^kC_k = (1+1)^k = 2^k$

Hence, $\sum_{d|n} |\mu(d)| = 2^k.1 = 2^k$

**Theorem 6:** If $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$, then $\sum_{d|n} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right)$.

**Proof:** Write, $f(n) = \frac{1}{n}$

Then, $\sum_{d|n} \mu(d) f(d) = \sum_{d|n} \frac{\mu(d)}{d}$

Since, $f(n) = \frac{1}{n}$ is a multiplicative function. [Since, $f(mn) = \frac{1}{mn} = \frac{1}{m}.\frac{1}{n} = f(m)f(n)$]

Therefore, $\sum_{d|n} \mu(d) f(d) = [1 - f(p_1)][1 - f(p_2)]...[1 - f(p_k)]$

$$= \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right)$$

$$\Rightarrow \sum_{d|n} \mu(d).\frac{1}{d} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right)$$

Hence, $\sum_{d|n} \mu(d).\frac{1}{d} = \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right)$

## 6.5 *THE GREATEST INTEGER FUNCTION*

The greatest integer function $[x]$ has roots in classical number theory, appearing implicitly in the works of Carl Friedrich Gauss and later formalized in summation methods by Peter Gustav Lejeune Dirichlet, especially in the study of arithmetic functions and divisor problems. It is widely used in counting integers with given properties, divisor and summatory functions, distribution of primes, Diophantine problems, and in converting real-variable expressions into discrete number-theoretic results.

The greatest integer function 'or' bracket function [] is especially suitable for treating divisibility problems. Although not strictly a number-theoretic function, its study has a natural place in this unit.

**Definition:** For an arbitrary real number $x$, we denote it by $[x]$ the largest integer less than or equal to $x$; that is, $[x]$ is the unique number satisfying $x-1<[x]\le x$.

By way of illustration, $[x]$ assumes the particular values

$[-3/2]=-2$; $[\sqrt{2}]=1$; $[1/3]=0$; $[\pi]=3$; $[-\pi]=-4$; $[e]=2$.

The important observation to be made here is that the quality $[x]=x$ holds if and only if $x$ is an integer. Definition 2 also makes plain that any real number $x$ can be written as,

$$x=[x]+\theta$$

For a suitable choice of $\theta$, with $0\le\theta<1$.

We now plan to investigate the question of how many times a particular prime $p$ appears in $n!$. For instance, if $p = 3$ and $n = 9$, then

$$9! = 1.2.3.4.5.6.7.8.9 = 2^7.3^4.5.7$$

So that the exact power of 3 that divides $9!$ is 4. It is desirable to have formulas that will this count, without the necessity of always writing $n!$ in canonical form.

**Theorem 7:** If $n$ is a positive integer and $p$ a prime, then the exponent of the highest power of $p$ that divides $n!$ is $\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$

Where the series is finite, because $\left[n/p^k\right] = 0$ for $p^k > n$.

**Proof:** As we know among the first $n$ positive integers, those divisible by $p$ are multiple of $p$ i.e., they are $p, 2p, 3p, ..., tp$, where $t$ is the largest integer such that $tp \le n$; in other words, $t$ is the largest integer less than or equal to $n/p$ (which is to say $t = [n/p]$). Thus there are exactly $[n/p]$ multiples of $p$ occurring in the product that defines $n!$, namely

$$p, 2p, 3p, ..., \left[\frac{n}{p}\right]p \qquad \ldots (1)$$

The exponent of $p$ in the prime factorization of $n!$ is obtained by adding to the number of integers in Eq. (1), the number of integers among 1, 2, …, $n$ divisible by $p^2$, and then the number divisible by $p^3$, and so on. The reason behind this that the integers between 1 and $n$ which are divisible by $p^2$ are

$$p^2, 2p^2, 3p^2, ..., \left[\frac{n}{p^2}\right]p^2$$

Which are $\left[\frac{n}{p^2}\right]$ in total number. Of these, $\left[\frac{n}{p^3}\right]$ are again divisible by $p$ :

$$p^3, 2p^3, 3p^3, ..., \left[\frac{n}{p^2}\right]p^3$$

So, after a finite number of repetitions of this process, we are led to conclude that the total number of times $p$ divides $n!$ is,

$$\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$$

This result can be cast as the following equation, which usually appears under the name of the Legendre formula:

$$n! = \prod_{p \le n} p^{\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]}$$

**Example 5:** Find the number of zeroes in $50!$.

**Solution:** The number of zeroes in $50!$ count on the basis of number of times 10 enters into the product of $50!$. Also, the number to times 10 appear in the product of $50!$ count on the basis of 5 and 2 appears in the product of $50!$. So, it is enough to find out the exponents of 2 and 5 in the prime factorization of $50!$ and then we count the smaller number in the count of exponent of 2 and 5. Now we have to find the least value of $k$ such that $2^k \mid 50!$ but $2^{k+1} \nmid 50!$.

So, $\left[\frac{50}{2^1}\right]+\left[\frac{50}{2^2}\right]+\left[\frac{50}{2^3}\right]+\left[\frac{50}{2^4}\right]+\left[\frac{50}{2^5}\right]+0+...+0 = 25+12+6+3+1 = 47$

Here, $2^{47} \mid 50!$ but $2^{48} \nmid 50!$.

Similarly, we will find the least value of $k$ such that $5^k \mid 50!$ but $5^{k+1} \nmid 50!$.

So, $\left[\frac{50}{5^1}\right]+\left[\frac{50}{5^2}\right]+0+...+0=10+2=12$

Here, $5^{12} \mid 50!$ but $5^{13} \nmid 50!$

The minimum value between (12, 47) is 12. This means that $50!$ ends with 12 zeroes.

**Theorem 8:** If $n$ and $r$ are positive integers with $1 \le r < n$, then the binomial coefficient $\binom{n}{r} = {}^nC_r = \frac{n!}{r!(n-r)!}$ is also an integer.

**Proof:** As we know that if $a$ and $b$ are arbitrary real number, then $[a+b] \ge [a]+[b]$. In particular, for each prime factor $p$ of $r!(n-r)!$,

$$\left[\frac{n}{p^k}\right] \ge \left[\frac{r}{p^k}\right]+\left[\frac{(n-r)}{p^k}\right]; \qquad k=1,2,...$$

Adding these inequalities, we obtain

$$\sum_{k\ge1}\left[\frac{n}{p^k}\right] \ge \sum_{k\ge1}\left[\frac{r}{p^k}\right]+\sum_{k\ge1}\left[\frac{(n-r)}{p^k}\right] \qquad (1)$$

The left-hand side of Eq. (1) gives the exponent of the highest power of the prime $p$ that divides $n!$, whereas the right-hand side equals the highest power of this prime contained in $r!(n-r)!$. Hence, $p$ appears in the numerator of $n!/r!(n-r)!$ at least as many times as it occurs in the denominator. Because this holds true for every prime divisor of the denominator, $r!(n-r)!$ must divide $n!$, making $n!/r!(n-r)!$ an integer.

**Corollary 1:** For a positive integer $r$, the product of any $r$ consecutive positive integers is divisible by $r!$

**Proof:** The product of *r* consecutive positive integers, the largest of which is *n*, is

$$n(n-1)(n-2)...(n-r+1)$$

Now we have,

$$n(n-1)(n-2)...(n-r+1)=\left(\frac{n!}{r!(n-r)!}\right)r!$$

Because $\frac{n!}{r!(n-r)!}$ is an integer by theorem, it follows that $r!$ must divide the product $n(n-1)(n-2)...(n-r+1)$, as asserted.

**Theorem 9:** Let $f$ and $F$ be number-theoretic functions such that, $F(n)=\sum_{d|n} f(d)$

Then, for any positive integer *N*, $\sum_{n=1}^{N} F(n)=\sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$

**Proof:** We begin by noting that,

$$\sum_{n=1}^{N} F(n)=\sum_{n=1}^{N}\sum_{d|n} f(d)$$

The strategy is to collect terms with equal values of $f(d)$ in this double sum. For a fixed positive integer $k \le N$, the term $f(k)$ appears in $\sum_{d|n} f(d)$ if and only if *k* is a divisor of *n*. (Because each integer has itself as a divisor, the right hand-side of Eq. (1) includes $f(k)$, at least once). Now, to calculate the number of sums $\sum_{d|n} f(d)$ in which $f(k)$ occurs as a term, it is sufficient

to find the number of integers among 1, 2, … , *N*, which are divisible by $k$ . There are $[N/K]$ of them:

$$k, 2k, 3k, ..., \left[\frac{N}{k}\right]k$$

Thus, for each $k$ such that, $1 \le k \le N$, $f(k)$ is a term of the sum $\sum_{d|n} f(d)$ for $[N/k]$ different positive integers less than or equal to $N$ . Knowing this, we may rewrite the double sum in Eq. (1) as, $\sum_{n=1}^{N}\sum_{d|n} f(d) = \sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$, and our task is complete.

**Corollary 2:** If *N* is a positive integer, then $\sum_{k=1}^{N}\tau(n) = \sum_{n=1}^{N}\left[\frac{N}{n}\right]$

**Proof:** Nothing that $\tau(n) = \sum_{d|n} 1$, we may write $\tau$ for $F$ and take $f$ to be constant function $f(n) = 1$ for all $n$ .

**Corollary 3:** If *N* is a positive integer, then $\sum_{k=1}^{N}\sigma(n) = \sum_{n=1}^{N} n\left[\frac{N}{n}\right]$

**Example 6:** Consider the case $N = 6$ . The definition of $\tau$ tells us that, $\sum_{k=1}^{6}\tau(n) = 14$

From corollary 1, $\sum_{n=1}^{6}\left[\frac{6}{n}\right] = [6] + [3] + [2] + [3/2] + [6/5] + [1]$

$$= 6 + 3 + 2 + 1 + 1 + 1 = 14$$

As it should. In the present case, we also have, $\sum_{n=1}^{6}\sigma(n) = 33$

And a simple calculation leads to,

$$\sum_{n=1}^{6} n\left[\frac{6}{n}\right] = 1[6] + 2[3] + 3[2] + 4[3/2] + 5[6/5] + 6[1]$$

$$= 1.6 + 2.3 + 3.2 + 4.1 + 5.1 + 6.1 = 33$$

**Example 7:** Find the highest power of 18 contained in $500!$.

**Answer:** The composite number 18 can be decomposed into a product of primes as, $18 = 2.3^2$

Thus, the primes contained in 18 are 2 and 3.

Further, the highest powers of 2 in $500!$ is given by

$$H_1 = \left[\frac{500}{2}\right] + \left[\frac{500}{2^2}\right] + \left[\frac{500}{2^3}\right] + \left[\frac{500}{2^4}\right] + \left[\frac{500}{2^5}\right] + \left[\frac{500}{2^6}\right] + \left[\frac{500}{2^7}\right] + \left[\frac{500}{2^8}\right] + 0 + 0 + ... + 0$$

$$\Rightarrow H_1 = 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 494$$

Also, the highest power of 3, contained in $500!$ is given by

$$H_2 = \left[\frac{500}{3}\right] + \left[\frac{500}{3^2}\right] + \left[\frac{500}{3^3}\right] + \left[\frac{500}{3^4}\right] + \left[\frac{500}{3^5}\right] = 166 + 55 + 18 + 6 + 2 = 247$$

Hence, $500! = 2^{494}.3^{247}.p_i$, for some $p_i$ such that $\gcd(p_i, 18) = 1$.

So, $500! = (2^2.3)^{247}.p_i$.

Hence, the highest power of 18 in $500!$ is 247.

## Check your progress

**Problem 1:** Find the highest power of 13 contained in $20000!$

**Answer:** 1665

**Problem 2:** Find the value of $\mu(500)$ and $\mu(243)$

**Answer:** $\mu(500) = 0$ and $\mu(243) = 0$

## 6.6 *SUMMARY*

This chapter on the Möbius inversion formula and the greatest integer function highlights two powerful tools that connect divisor theory with analytic and counting techniques in number theory. The Möbius function and the Möbius inversion formula, introduced by August Ferdinand Möbius, provide a systematic method for inverting divisor-sum relations and studying multiplicative arithmetic functions, forming a foundation for deeper results in elementary and analytic number theory. Alongside this, the greatest integer (floor) function serves as an essential bridge between real variables and discrete integers, playing a key role in counting arguments, summation formulas, and estimates. Together, these concepts illustrate how algebraic structure and analytic reasoning combine to solve problems involving divisibility, prime factorization, and integer distribution, thereby strengthening both theoretical understanding and problem-solving skills in number theory.

## 6.7 *GLOSSARY*

- The *Möbius* $\mu-$ *function*
- The Möbius inversion formula
- The greatest integer function

## 6.8 *REFERENCES*


- **Burton, D. M.** (2007). *Elementary number theory* (6th ed.). McGraw-Hill.

- **T. M. Apostol**, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford.
- **Tom M. Apostol**, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York.
- **G. A. Jones and J. M. Jones**, *Elementary Number Theory*, Springer-Verlag, Berlin, 1998.
- **T. Nagell**, *Introduction to Number Theory*, Wiley, New York.


## 6.9 *SUGGESTED READING*


- **Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery**, *An Introduction to the Theory of Numbers*, John Wiley & Sons.
- **Hugh L. Montgomery and Robert C. Vaughan**, *Multiplicative Number Theory I: Classical Theory*, Cambridge University Press.
- **H. Iwaniec and E. Kowalski**, *Analytic Number Theory*, American Mathematical Society, 2004.
- **T. Koshy**, *Elementary Number Theory with Applications*, Academic Press.
- **Eric W. Weisstein**, "Möbius Inversion Formula," *MathWorld – Wolfram Resource*.


## 6.10 *TERMINAL QUESTION*

**Long Answer Type Question:**

**1.** Let $F$ and $f$ be two number-theoretic functions related by the formula $F(n) = \sum_{d|n} f(d)$

Then prove that, $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$

**2.** Let $f$ and $F$ be number-theoretic functions such that, $F(n) = \sum_{d|n} f(d)$

Then, prove that for any positive integer $N$, $\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$

**Short answer type question:**

**1:** What is the Möbius function?

**2:** Who introduced the Möbius function?

**3:** Define the Möbius inversion formula.

**4:** Prove that $\mu$ is multiplicative function.

**5:** What is the greatest integer function?

**6:** What is the value of $\mu(pq) = 1$ where $p$ and $q$ are distinct primes?

**Objective type questions:**

**1:** The Möbius function $\mu(n)$ was introduced by

**(A)** Leonhard Euler

**(B)** Carl Friedrich Gauss

**(C)** August Ferdinand Möbius

**(D)** Pierre de Fermat

**2:** The value of $\mu(1)$ is

**(A)** 0

**(B)** 1

**(C)** $-1$

**(D)** 2

**3:** If $n$ is divisible by the square of a prime, then $\mu(n)$ equals

**(A)** 1

**(B)** $-1$

**(C)** 0

**(D)** $n$

**4:** If $n$ is the product of $k$ distinct primes, then $\mu(n)$ equals

**(A)** $k$

**(B)** 1

**(C)** $(-1)k$

**(D)** 0

**Answer:** (C)

**5:** The function that gives the greatest integer less than or equal to $x$ is called the

**(A)** Ceiling function

**(B)** Greatest integer (floor) function

**(C)** Logarithmic function

**(D)** Absolute value function

**6:** The value of $\mu(p)$, where $p$ is a prime number, is

**(A)** 0

**(B)** 1

**(C)** $-1$

**(D)** p

**7:** If $n = p^2$ where $p$ is prime, then $\mu(n)$ equals

**(A)** 1

**(B)** $-1$

**(C)** 0

**(D)** 2

**8:** If $n = pq$ , where $p$ and $q$ are distinct primes, then $\mu(n)$ equals

**(A)** 1

**(B)** $-1$

**(C)** 0

**(D)** 2

**9:** The Möbius function is an example of a

**(A)** Additive function

**(B)** Multiplicative function

**(C)** Continuous function

**(D)** Periodic function

**10:** If, $F(n) = \sum_{d|n} f(d)$, then the Möbius inversion formula gives

**(A)** $f(n) = \sum_{d|n} F(d)$

**(B)** $f(n) = \sum_{d|n} \mu(d) F(n/d)$

**(C)** $f(n) = F(n)$

**(D)** $f(n) = \mu(n) F(n)$

**11:** The value of $[5.2]$ is

**(A)** 6

**(B)** 5

**(C)** 4

**(D)** 5.2

**12:** The value of $[-2.3]$ is

**(A)** $-2$

**(B)** $-3$

**(C)** 2

**(D)** 3

**13:** The greatest integer function gives

**(A)** The nearest integer

**(B)** The smallest integer greater than $x$

**(C)** The greatest integer less than or equal to $x$

**(D)** The absolute value of $x$

**14:** The greatest integer function is also known as the

**(A)** Ceiling function

**(B)** Floor function

**(C)** Modulus function

**(D)** Identity function

**15:** The value of $[7]$ is

**(A)** 6

**(B)** 7

**(C)** 8

**(D)** 0

**True and False question:**

**1:** The Möbius function is a multiplicative arithmetic function.

**2:** If $n$ contains a squared prime factor, then $\mu(n)=0$.

**3:** The greatest integer function is denoted by $[x]$

**4:** The value of $[3.9]$ is 4.

**5:** The Möbius inversion formula is used to invert divisor-sum relations.

**Fill in the blanks question:**

**1:** The Möbius function is denoted by _____.

**2:** If $n=1$, then $\mu(n)=$_____.

**3:** If $n$ is divisible by the square of a prime, then $\mu(n)=$ _____.

**4:** The greatest integer function is also called the _____ function.

**5:** The greatest integer less than or equal to $x$ is written as _____.

## 6.11 *ANSWERS*

**Answer of short answer type question:**

**Answer 6:** $\mu(pq) = 1$

**Answer of the objective questions:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | C | **2:** | B | **3:** | C | **4:** | C |
| **5:** | B | **6:** | C | **7:** | C | **8:** | A |
| **9:** | B | **10:** | B | **11:** | B | **12:** | B |
| **13:** | C | **14:** | B | **15:** | B | | |

**Answer of true and false questions:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | True | **2:** | True | **3:** | True | **4:** | False |
| **5:** | True | | | | | | |

**Answer of fill in the blanks questions:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | $\mu(n)$ | **2:** | 1 | **3:** | 0 | **4:** | Floor |
| **5:** | $[x]$ | | | | | | |

# UNIT-7: EULER'S PHI-FUNCTION AND PROPERTIES, EULER'S THEOREM

## CONTENTS:



## 7.1 *INTRODUCTION*

This unit "Euler's Phi-Function and Properties, Euler's Theorem" in number theory studies an important arithmetic function that counts the number of positive integers less than or equal to $n$ that are relatively prime to $n$. This function, known as Euler's Totient Function (or

Euler's phi-function $\phi(n)$, was introduced and systematically studied by the Swiss mathematician Leonhard Euler in the 18th century while extending earlier ideas related to Pierre de Fermat and his famous Fermat's Little Theorem. Euler generalized Fermat's result to obtain Euler's Theorem, which states that if $a$ and $n$ are relatively prime, then $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$. The historical development of the phi-function played a significant role in the advancement of Number Theory, particularly in the study of divisibility, modular arithmetic, and arithmetic functions. Today, Euler's phi-function and Euler's theorem are fundamental tools with important applications in modern mathematics and areas such as Cryptography, especially in public-key systems like RSA.


15 April 1707- 18 September 1783

https://en.wikipedia.org/wiki/Leonhard_Euler

*Leonhard Euler (*15 *April* 1707 – 18 *September* 1783*) was a Swiss polymath who was active as a mathematician, physicist, astronomer, logician, geographer, music theorist and engineer. He founded the studies of graph theory and topology and made influential discoveries in many other branches of mathematics, such as analytic number theory, complex analysis, and infinitesimal calculus. He also introduced much of modern mathematical terminology and notation, including the notion of a mathematical function. He is known for his work in mechanics, fluid dynamics, optics, astronomy, and music theory. Euler has been called a "universal genius" who "was fully equipped with almost unlimited powers of imagination, intellectual gifts and extraordinary memory". He spent most of his adult life in Saint Petersburg, Russia, and in Berlin, then the capital of Prussia*.

## 7.2 *OBJECTIVE*

After reading this unit learners will be able,

- To introduce the concept of the Euler's Totient Function $\phi(n)$ and understand its definition as the number of positive integers less than or equal to $n$ that are relatively prime to $n$.
- To study the basic properties of the phi-function, including its values for prime numbers, prime powers, and composite numbers.
- To derive formulas for calculating $\phi(n)$ using the prime factorization of an integer.
- To understand the multiplicative property of the phi-function and its importance in arithmetic functions.
- To introduce and prove Euler's Theorem, which states that if $a$ and $n$ are relatively prime, then $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$.
- To understand the relationship between Euler's theorem and Fermat's Little Theorem, originally given by Pierre de Fermat and later generalized by Leonhard Euler.
- To apply Euler's theorem and the phi-function in solving problems involving congruences, modular arithmetic, and other results in number theory.

## 7.3 *EULER'S PHI-FUNCTION*

The Euler's Totient Function, also called Euler's phi-function and denoted by $\phi(n)$, is an important arithmetic function in Number Theory. It is defined as the number of positive integers less than or equal to $n$ that are relatively prime to $n$; that is, integers whose greatest common divisor with $n$ is 1. The function was introduced by the Swiss mathematician Leonhard Euler while studying properties of integers and congruences.

**Definition:** For $n \geq 1$, number of positive integers which are less than $n$ and relatively prime with $n$ $(i.e.\ \gcd(a,n) = 1; a < n)$ are denoted by $\phi(n)$.

Mathematically, we represent it as

$\phi(n) = \text{Cardinality of the set } U(n) \text{ where, } U(n) = \{n \in N : \gcd(a,n) = 1 \text{ and } a < n\}$

**Note 1:** The term "cardinality" is referred as the number of elements in the set.

**2:** Sometime we refereed $\phi(n) = |U(n)| = |\{n \in N : \gcd(a,n) = 1 \text{ and } a < n\}|$, where $|U(n)|$ denotes the number of elements in the set $U(n)$.

**Example 1:** Here, we are writing some Euler $\phi$ – function of some numbers as:

$\phi(1)=1;\ \phi(2)=1;\ \phi(3)=|U(3)|=|\{1,2\}|=2;$

$\phi(4)=|U(4)|=|\{1,4\}|=2$

$\phi(5)=|U(5)|=|\{1,2,3,4\}|=4$

$\phi(6)=|U(6)|=|\{1,5\}|=2$

$\phi(8)=|U(8)|=|\{1,3,5,7\}|=4$

$\phi(9)=|U(9)|=|\{1,2,4,5,7,8\}|=6$

$\phi(10)=|U(10)|=|\{1,3,7,9\}|=4$

**Theorem 1:** If $p$ is prime then $\phi(p)$ is $p-1$.

**Answer:** As we know that if $p$ is prime then $\{1,2,3,...,p-1\}$ are the natural numbers which are less than $p$ and relatively prime with $p$. Because, if it is not then $\exists a \in N$ and $a < p$ such that $\gcd(a,p)=d\neq 1$.

$\Rightarrow d \mid p$, which is a contradiction that $p$ is prime (since prime has only two positive divisors 1 and $p$ itself).

Hence, $U(p)=\{1,2,3,...,p-1\}$

Then, $\phi(p)=|U(p)|=|\{1,2,3,...,p-1\}|=p-1$.

**Theorem 2:** If $p$ is prime and $k \in N$ then $\phi(p^k)=p^k-p^{k-1}=p^k\left(1-\frac{1}{p}\right)$.

**Proof:** To find the $\phi(p^k)$, we have only to find the number of natural numbers (positive integers) which are less than $p^k$ and relatively prime to $p^k$.

As, we know that $\gcd(n,p^k)=1 \Leftrightarrow p \nmid n$.

$\Rightarrow$There are $p^{k-1}$ integers between 1 and $p^k$ divisible by $p$, which are $p, 2p, 3p, ..., (p^{k-1})p$.

Thus, the set $\{1,2,3,...,p^k\}$ contains exactly $p^k-p^{k-1}$ positive integers that are relatively prime to $p^k$. Hence by definition, $\phi(p^k)=p^k-p^{k-1}$.

In a similar way, $\phi(p^k)=p^k-p^{k-1}=p^k\left(1-p^{-1}\right)=p^k\left(1-\frac{1}{p}\right)$

**Example 2:** Find the value of $\phi(9)$ and $\phi(16)$.

**Answer:** As we know $\phi(9) = \phi(3^2)$. Since 3 is prime then using the Theorem 2, we get

$\phi(9) = \phi(3^2) = 3^2 - 3^{2-1} = 9 - 3 = 6$.

Hence number of positive integers which are less than 9 and relatively prime with 9 are 6. For shake of knowledge these integers are 1, 2, 4, 5, 7, 8.

Similarly, $\phi(16) = \phi(2^4) = 2^4 - 2^{4-1} = 16 - 8 = 8$ and these are 1, 3, 5, 7, 9, 11, 13, 15.

**Lemma 1:** For given integers $a, b, c$, $\gcd(a, bc) = 1 \Leftrightarrow \gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

**Proof:** Initially, we assume that $\gcd(a, bc) = 1$, and put $d = \gcd(a, b)$.

$\Rightarrow d \mid a$ and $d \mid b$

$\Rightarrow d \mid a$ and $d \mid bc$

$\Rightarrow \gcd(a, bc) \geq d$ but we have already given that $\gcd(a, bc) = 1$

$\Rightarrow d = 1$ *i.e.*, $\gcd(a, b) = 1$

With the similar reasoning we can prove that $\gcd(a, c) = 1$

Now to prove in reverse direction, let we assume that $\gcd(a, b) = 1 = \gcd(a, c)$ and also assume that $\gcd(a, bc) = d > 1$.

$\Rightarrow d \mid a$ and $d \mid bc$. Since $d > 1$ then, there exist a prime divisor of $d$ let say it $p$. As $d \mid bc \Rightarrow p \mid bc$. In a consequence $p \mid b$ or $p \mid c$.

Since $p \mid b$ and $p \mid a \Rightarrow \gcd(a, b) \geq p$ (which is a contradiction that $\gcd(a, b) = 1 = \gcd(a, c)$).

So, our assumption is wrong that $d > 1$, while it is $d = 1$.

**Theorem 3:** The function $\phi$ is multiplicative function.

'OR'

If $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$

**Proof:** To find the positive integers less than *mn* and relatively prime to *mn*, we arrange the integers 1, 2, 3, …, *mn* in a rectangular array having *n*-rows and *m*-column in the following manner.

| | | | | | |
|---|---|---|---|---|---|
| 1 | 2 | … | $k$ | … | $m$ |
| $m+1$ | $m+2$ | … | $m+k$ | … | $2m$ |

| | | | | | |
|---|---|---|---|---|---|
| $2m+1$ | $2m+2$ | … | $2m+k$ | … | $3m$ |
| … | … | … | … | … | … |
| … | … | … | … | … | … |
| $(n-1)m+1$ | $(n-1)m+2$ | … | $(n-1)m+k$ | … | $nm$ |

In the above arrangement of integers, we have to find the integers $a$ such that $1 \le a < mn$ and $\gcd(a, mn) = 1$.

But we know that if $a \in Z$, then $(a, mn) = 1$ if and only if $(a, m) = 1$ and $(a, n) = 1$.

Thus, in the above arrangement of integers, we have to find the integers *a* such that $1 \le a < mn$ and $(a, m) = 1$ as well as $(a, n) = 1$.

For this, we first consider the *m*-columns that begin with $1, 2, ..., k, m$. If *b* is any integer, then we have $(m, k) = 1$ iff $(m, bm + k) = 1$

Thus, if the first term of a column is relatively prime to *m*, then, every other term of that column is also relatively prime to *m*. But the number of integers 1, 2, …, *m* that are relatively prime to *m* is $\phi(m)$. Therefore, they are $\phi(m)$ columns in each of which every integers is relatively prime to *m*.

Now, we have to find the number of integers in these $\phi(m)$ columns that are relatively prime to *n*.

Out of these $\phi(m)$ columns, let us consider the columns that begin with *k*. The terms in this column are, $k, m + k, 2m + k, ..., (n-1)m + k$

which are $m$ in number. These *n* integers when divided by *n* yield remainders 0, 1, 2, …, *n*-1, though not necessarily in this order.

If $r$ is the remainder when $bm + k$ is divided by $n$, then

$bm + k = nq + r$, where $q \in Z$ and $0 \le r < n$

Now, $(bm + k, n) = (nq + r, n) = (r, n)$

$\therefore (bm + k, n) = 1$ if and only if $(r, n) = 1$.

But the number of positive integers among the *n* remainders 0, 1, 2, …, *n*-1 that are relatively prime to *n* is $\phi(m)$. Therefore, the number of integers in the $k^{th}$ column that are relatively prime to *n* is $\phi(n)$. This is true for each of the $\phi(m)$ columns. Thus, each of the $\phi(m)$ columns in

which every term is relatively prime to *m* contains $\phi(n)$ integers which are relatively prime to *n*. Hence, in the whole arrangement, there are $\phi(m)$ integers that are relatively prime to *m* as well as to *n* and consequently relatively prime to *mn.*

Hence, $\phi(mn) = \phi(m)\phi(n)$

**Theorem 4:** If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$, then

$$\phi(n) = \phi(p_1^{k_1} p_2^{k_2} ... p_r^{k_r}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})...(p_r^{k_r} - p_2^{k_r-1})$$

**Proof:** Since we that for any prime *p* and $k \in N$, we have $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$. As we know that $\phi -$ function is multiplicative function *i.e.*, $\phi(mn) = \phi(m)\phi(n)$.

Here, the prime factorization of $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$

such that $\gcd(p_i^{k_i}, p_j^{k_j}) = 1 \forall\, i \neq j$ and $i, j = 1 to r$.

So, we get by using the Theorem 2 and 3,

$$\phi(n) = \phi(p_1^{k_1} p_2^{k_2} ... p_r^{k_r}) = \phi(p_1^{k_1})\phi(p_2^{k_2})...\phi(p_r^{k_r}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})...(p_r^{k_r} - p_2^{k_r-1})$$

**Example 3:** Evaluate the $\phi(360)$.

**Answer:** First we write down the prime factorization of the number 360 *i.e.*, $360 = 2^3.3^2.5$

Now, $\phi(360) = \phi(2^3).\phi(3^2).\phi(5) = (2^3 - 2^{3-1})(3^2 - 3^{2-1})(5-1)$

$\Rightarrow \phi(360) = 4.6.4 = 96$

**Theorem 5:** For $n > 2, \phi(n)$ is an integer.

**Proof:** For any $n > 2$, the prime factorization of *n* is either even odd. So, here there are two subcases are arise:

**Case I:** If *n* is a power of 2, let us say that $n = 2^k$, with $k \geq 2$.

Then, $\phi(n) = \phi(2^k) = (2^k - 2^{k-1}) = 2^k\left(1 - \frac{1}{2}\right) = 2^{k-1}$, which is an even integer.

**Case II:** If *n* does not happen to be power of 2, then it is divisible by an odd prime *p*; we therefore may write *n* as $n = p^k m$, where $k \geq 1$ and $\gcd(p^k, m) = 1$.

Then, $\phi(n) = \phi(p^k m) = \phi(p^k)\phi(m) = (p^k - p^{k-1})\phi(m) = p^{k-1}(p-1)\phi(m)$

As we know that if $p$ is an odd prime then, $(p-1)$ is an even integer i.e., $2 \mid (p-1)$.

$\Rightarrow \phi(n)$ is an even integer.

**Note:** If we have given any positive integer *n* and someone asked about which positive integer (*k*) such that its $\phi-$function gives the value *n*. Then our answer will be cannot be find. In other word we can say that the $\phi-$function is not invertible. Since it is not one-one because, $\phi(3)=2$ and $\phi(4)=2$ but $3 \neq 4$.

## 7.4 *EULER'S THEOREM*

As remarked earlier, the first published proof of Fermat's theorem (namely that $a^{p-1} \equiv 1 (\text{mod } p)$ if $p \nmid a$) was given by Euler in 1736. Somewhat later, in 1760, he succeeded in generalizing Fermat's theorem from the case of a prime $p$ to an arbitrary positive integer *n*. This landmark result states: If $\gcd(a,n)=1$, then $a^{\phi(n)} \equiv 1 (\text{mod } n)$.

**Lemma 2:** Let $n>1$ and $\gcd(a,n)=1$. If $a_1, a_2, ..., a_{\phi(n)}$ are the positive integers less than *n* and relatively prime to $n$, then $aa_1, aa_2, ..., aa_{\phi(n)}$ are congruent modulo $n$ to $a_1, a_2, ..., a_{\phi(n)}$ is some order.

**Proof:** Here, it is to observe that no two of these integers $aa_1, aa_2, ..., aa_{\phi(n)}$ are congruent modulo *n*. If it is that, $aa_i \equiv aa_j (\text{mod } n)$, with $1 \leq i < j \leq \phi(n)$, then the cancellation law yields $a_i \equiv a_j (\text{mod } n)$, and thus $a_i = a_j$, which is a contradiction.

Furthermore, because $\gcd(a_i, n)=1 \forall i$ and $\gcd(a,n)=1$, the lemma preceding Theorem 3 guarantees that each of the $aa_i$ is relatively prime to $n$.

Fixing on a particular $aa_i$, there exist a unique integer $b$, where $0 \leq b < n$, for which $aa_i \equiv b (\text{mod } n)$. Because,

$\gcd(b,n) = 1 = \gcd(aa_i, n) = 1$

$b$ must be one of the integers $a_1, a_2, ..., a_{\phi(n)}$. All told, this proves that the members $aa_1, aa_2, ..., aa_{\phi(n)}$ and the numbers $a_1, a_2, ..., a_{\phi(n)}$ are identical (modulo *n*) in a certain order.

**Example 4:** If we take, $n = 30$ and $a = 11$ then we have

$11^{\phi(30)} \equiv 11^8 \equiv (11^2)^4 \equiv 121^4 \equiv 1^4 \equiv 1 (\text{mod}\, 30)$.

*i.e.*, $11^{\phi(30)} \equiv 1 (\text{mod}\, 30)$ as $\gcd(11,30) = 1$

**Theorem 6:** If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 (\text{mod}\, n)$.

**Proof:** There is no harm in taking $n > 1$. Let $a_1, a_2, ..., a_{\phi(n)}$ be the positive integers less than $n$.

Because $\gcd(a, n) = 1$, it follows from the lemma that $aa_1, aa_2, ..., aa_{\phi(n)}$ are congruent, not necessarily in order of appearance, to $a_1, a_2, ..., a_{\phi(n)}$. Then,

$$aa_1 \equiv a_1' (\text{mod}\, n)$$
$$aa_2 \equiv a_2' (\text{mod}\, n)$$
$$\vdots$$
$$a_{\phi(n)} \equiv a'_{\phi(n)} (\text{mod}\, n)$$

Where, $a_1', a_2', ..., a'_{\phi(n)}$ are the integers $a_1, a_2, ..., a_{\phi(n)}$ in some order. On taking the product of these $\phi(n)$ congruences, we get

$$(aa_1)(aa_2)...(aa_{\phi(n)}) \equiv a'_1 a'_2 ... a'_{\phi(n)} (\text{mod}\, n)$$
$$\equiv a_1 a_2 ... a_{\phi(n)} (\text{mod}\, n)$$

And so,

$$a^{\phi(n)} (a_1 a_2 ... a_{\phi(n)}) \equiv a_1 a_2 ... a_{\phi(n)} (\text{mod}\, n)$$

Because $\gcd(a_i, n) = 1$ for each *i*, the lemma preceding Theorem 3 implies that $\gcd(a_1 a_2 ... a_{\phi(n)}, n) = 1$. Therefore, we may divide both sides of the foregoing congruence by the common factor $a_1 a_2 ... a_{\phi(n)}$, leaving us with, $a^{\phi(n)} \equiv 1 (\text{mod}\, n)$.

**Example 5:** The above proof is illustrated by some specific numbers. Let $n = 9$, for shake of interest. The positive integers less than and relatively prime to 9 are 1, 2, 4, 5, 7 and 8. These numbers are same like $a_1, a_2, ..., a_{\phi(n)}$.

If $a = -4$, then the integers $aa_i$ are

$-4.1, -4.2, -4.4, -4.5, -4.7, -4.8$ i.e., $-4, -8, -16, -20, -28, -32$

Also modulo 9 are, $-4 \equiv 5, -8 \equiv 1, -16 \equiv 2, -20 \equiv 7, -28 \equiv 8, -32 \equiv 4$

When the above congruence are multiplied together, we obtain

Which becomes, $1.2.4.5.7.8(-4)^6 \equiv (5.1.2.7.8.4)(\text{mod}\,9)$

$\Rightarrow (-4)^6 \equiv 1(\text{mod}\,9)$

Also, verify by the congruence that, $(-4)^6 \equiv 4^6 \equiv (64)^2 \equiv 1^2 \equiv 1(\text{mod}\,9)$

**Corollary:** If $p$ is a prime and $p \nmid a$, then $a^{p-1} \equiv 1\,(\text{mod}\,p)$

**Example 6:** Find the last two digits in the decimal representation of $3^{256}$.

**Solution:** To evaluate the last two digits in the decimal representation of $3^{256}$, we have to find the smallest nonnegative integer to which $3^{256}$ is congruent modulo 100.

Since, $\gcd(3,100) = 1$ and

$$\phi(100) = \phi(2^2.5^2) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40$$

Now, by the Euler's theorem (Theorem 6), $3^{40} \equiv 1(\text{mod}\,100)$

By the division algorithm, $256 = 6.40 + 16$ ; whence

$3^{256} \equiv 3^{6.40+16} \equiv (3^{40})^6.3^{16} \equiv 3^{16}\,(\text{mod}\,100)$

Since, $3^2 \equiv 9\,(\text{mod}\,100); 3^4 \equiv 81\,(\text{mod}\,100)$; $3^8 \equiv 61\,(\text{mod}\,100)$; $3^{16} \equiv 21\,(\text{mod}\,100)$

Hence, $3^{256} \equiv 21(\text{mod}\,100)$

## 7.5 *PROPERTIES OF PHI-FUNCTION*

The following theorem highlights an interesting property of the Euler's Totient Function. It states that if $d$ runs through all the positive divisors of a number $n$, then the sum of the values $\phi(d)$ is equal to $n$ itself. This remarkable observation was first noted by Carl Friedrich Gauss.

**Theorem 7: (Gauss Theorem)** For each positive integer $n \geq 1$, $n = \sum_{d|n} \phi(d)$

The sum being extended over all positive divisor of $n$.

**Proof:** The integer between 1 and $n$ can be separated into classes as follows: If $d$ is a positive divisor of $n$, we put the integer $m$ is the class $S_d$ provided that $\gcd(m,n) = d$. Stated in symbols,

$S_d = \{m \mid \gcd(m,n) = d; 1 \leq m \leq n\}$

Since, $\gcd(m,n) = d$ *iff* $\gcd(m/d, n/d) = 1$. Thus, the number of integers in the class $S_d$ is equal to the number of positive integers not exceeding $n/d$ that are relatively prime to $n/d$; in other words, equal to $\phi(n/d)$. Because each of the $n$ integers in the set $\{1,2,3,...,n\}$ lies in exactly one class $S_d$, we obtain the formula $n = \sum_{d|n} \phi\left(\frac{n}{d}\right)$

But as *d* runs through all positive divisors of *n*, so does $n/d$; hence,

$$n = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$$

Which proves the theorem.

**Example 7:** For $n = 10$,

$S_d = \{m \mid \gcd(m,n) = d; 1 \le m \le n\}$

Then, $S_1 = \{1,3,7,9\}$; similarly, $S_2 = \{2\,4,6,8\}$; $S_5 = \{5\}$; $S_{10} = \{10\}$

So, these contain, $\phi(10) = 4$, $\phi(5) = 4$, $\phi(2) = 1$,and $\phi(1) = 1$ integers, respectively. Therefore,

$$\sum_{d|10} \phi(d) = \phi(10) + \phi(5) + \phi(2) + \phi(1) = 4 + 4 + 1 + 1 = 10$$

**Theorem 8:** For $n > 1$, the sum of the positive integers less than *n* and relatively prime to *n* is $\frac{1}{2} n\phi(n)$.

**Proof:** Let $a_1, a_2, ..., a_{\phi(n)}$ be the positive integers less than *n* and relatively prime to *n*. Now because $\gcd(a,n) = 1$ if and only if $\gcd(n-a,n) = 1$, the numbers $n - a_1, n - a_2, ..., n - a_{\phi(n)}$ are equal in some order to $a_1, a_2, ..., a_{\phi(n)}$. Thus,

$$a_1 + a_2 + ... + a_{\phi(n)} = (n - a_1) + (n - a_2) + ... + (n - a_{\phi(n)}$$

$$a_1 + a_2 + ... + a_{\phi(n)} = (n - a_1) + (n - a_2) + ... + (n - a_{\phi(n)}) = n\phi(n) - (a_1 + a_2 + ... + a_{\phi(n)})$$

Thus, $n\phi(n) = 2(a_1 + a_2 + ... + a_{\phi(n)})$

Hence, the sum of the positive integers less than *n* and relatively prime to *n* is $\frac{1}{2} n\phi(n)$.

**Example 8:** If $n = 30$, then $\phi(30) = 8$. So, the integers less than *n* and relatively prime to 30 are 1, 7, 11, 13, 17, 19, 23, 29

In this setting, we find that the desired sum is,

$$1+7+11+13+17+19+23+29=120=\frac{1}{2}.30.8$$

Also, note the pairings

$1+29=30\ ;\ 7+23=30\ ;\ 11+19=30\ ;\ 13+17=30$

This is a good point at which to give an application of the Mobius inversion formula.

**Theorem 9:** For any positive integer $n$, $\phi(n)=n\sum_{d|n}\frac{\mu(d)}{d}$.

**Proof:** By the inversion formula we have,

$$F(n)=n\sum_{d|n}\frac{\mu(d)}{d}$$

The result is, $\phi(n)=\sum_{d|n}\mu(d)\frac{n}{d}$

**Example 9:** For $n=10$,

$$10\sum_{d|10}\frac{\mu(d)}{d}=10\left[\mu(1)+\frac{\mu(2)}{2}+\frac{\mu(5)}{5}+\frac{\mu(10)}{10}\right]=10\left[1+\frac{(-1)}{2}+\frac{(-1)}{5}+\frac{(-1)^2}{10}\right]$$

$$=10\left[1-\frac{1}{2}-\frac{1}{5}+\frac{1}{10}\right]=4=\phi(10)$$

**Example 10:** Show that $\phi(n)=\phi(n+1)=\phi(n+2)$ for $n=5186$.

**Solution:** As we know that, $\phi(n)=\phi(5186)=2592$

Further, $\phi(n+1)=\phi(5187)=\phi(3.7.13.19)=\phi(3)\phi(7)\phi(13)\phi(19)$

$=(3-1)(7-1)(13-1)(19-1)=2592$.

Again, $\phi(n+2)=\phi(5188)=\phi(2^2.1297)=\phi(2^2)\phi(1297)=(2^2-2)(1297-1)=2\times1296=2592$.

Hence the result.

**Example 11:** If $n\,\&\,n+2$ both are primes, then show that $\phi(n+2)=\phi(n)+2$.

**Solution:** Consider, $\phi(n+2)=n+2-1=n+1$, where $n+2$ is prime

Again, $\phi(n)=n-1$, where $n$ is prime

Then, $\phi(n+2)=n+2-1=n+1=(n-1)+2=\phi(n)+2$

Thus, $\phi(n+2)=\phi(n)+2$.

## Check your progress

**Problem 1:** Find the highest power of 13 contained in $20000!$

**Answer:** 1665

**Problem 2:** Find the value of $\mu(500)$ and $\mu(243)$

**Answer:** $\mu(500) = 0$ and $\mu(243) = 0$

## 7.6 *SUMMARY*

The unit on Euler's Phi-Function and Properties, Euler's Theorem introduces the arithmetic function $\phi(n)$, defined as the number of positive integers less than or equal to $n$ that are relatively prime to $n$. It develops key properties of the phi-function, including its value for prime numbers $\phi(p) = p - 1$, for prime powers $\phi(p^k) = p^k - p^{k-1}$, and its multiplicative nature when two integers are coprime, i.e., $\phi(mn) = \phi(m)\phi(n)$ if gcd($m$, $n$)=1. The chapter also explains methods to compute $\phi(n)$ using the prime factorization of $n$. A central result discussed is Euler's theorem, which states that for any integer $a$ co-prime to $n$, $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$, generalizing Fermat's Little Theorem. The unit highlights applications of these results in number theory, particularly in modular arithmetic, congruences, and cryptographic systems, emphasizing their fundamental role in understanding the structure of integers.

## 7.7 *GLOSSARY*

- Euler $\phi$ – function
- Gauss Theorem

## 7.8 *REFERENCES*

- **Burton, D. M.** (2007). *Elementary number theory* (6th ed.). McGraw-Hill.
- **T. M. Apostol**, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford.
- **Tom M. Apostol**, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York.
- **G. A. Jones and J. M. Jones**, *Elementary Number Theory*, Springer-Verlag, Berlin, 1998.
- **T. Nagell**, *Introduction to Number Theory*, Wiley, New York.


## 7.9 *SUGGESTED READING*


- **Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery**, *An Introduction to the Theory of Numbers*, John Wiley & Sons.
- **Hugh L. Montgomery and Robert C. Vaughan**, *Multiplicative Number Theory I: Classical Theory*, Cambridge University Press.
- **H. Iwaniec and E. Kowalski**, *Analytic Number Theory*, American Mathematical Society, 2004.
- **T. Koshy**, *Elementary Number Theory with Applications*, Academic Press.
- **Eric W. Weisstein**, "Möbius Inversion Formula," *MathWorld – Wolfram Resource*.


## 7.10 *TE1RMINAL QUESTION*

**Long Answer Type Question:**

**1.** Prove that the Euler $\phi-$function is multiplicative function.

**2.** If $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$, derive the following inequalities.

($a$) $\sigma(n)\phi(n) \geq n^2\left(1-1/p_1^2\right)\left(1-1/p_2^2\right)..\left(1-1/p_r^2\right)$

($b$) $\tau(n)\phi(n) \geq n$

**Hint:** For easier way to prove this we first prove, $\tau(n)\phi(n) \geq 2^r . n(1/2)^r$

**Short answer type question:**

**1:** What is the Euler $\phi -$ function?

**2:** Calculate $\phi(1001)$ and $\phi(5040)$?

**3:** Show that the equation $\phi(n) = \phi(n+2)$ is satisfied by $n = 2(2p-1)$, where $p$ and $2p-1$ are odd primes.

**Objective type questions:**

**1:** Euler's phi-function $\phi(n)$ counts:

**(A)** Number of primes less than $n$

**(B)** Number of divisors of $n$

**(C)** Positive integers $\leq n$ that are coprime to $n$

**(D)** Multiples of $n$

**2:** If $p$ is a prime, then $\phi(p) =$

**(A)** $p$

**(B)** $p-1$

**(C)** 1

**(D)** 0

**3:** If $p$ is a prime and $k \geq 1$, then $\phi(p^k) =$

**(A)** $p^k - 1$

**(B)** $p^k$

**(C)** $p^k - p^{k-1}$

**(D)** $p^{k-1}$

**4:** Euler's theorem states that $\gcd(a, n) = 1$, then:

**(A)** $a^n \equiv 1 (\mathrm{mod}\, n)$

**(B)** $a^{\phi(n)} \equiv 1 \pmod{n}$

**(C)** $a^{n-1} \equiv 0 \pmod{n}$

**(D)** $a^{\phi(n)} \equiv 0 \pmod{n}$

**5:** If $\gcd(m,n) = 1$, then

**(A)** $\phi(mn) = \phi(m) + \phi(n)$

**(B)** $\phi(mn) = \phi(m)\phi(n)$

**(C)** $\phi(mn) = mn$

**(D)** None

**6:** The value of $\phi(10)$ is:

**(A)** 2

**(B)** 4

**(C)** 5

**(D)** 8

**7:** If $p$ and $q$ are distinct primes, then $\phi(pq) =$

**(A)** $pq$

**(B)** $(p\text{-}1)(q-1)$

**(C)** $p+q$

**(D)** $p-q$

**8:** Fermat's Little theorem is special case of:

**(A)** Wilson's theorem

**(B)** Euler theorem

**(C)** Lagrange's theorem

**(D)** Gauss lemma

**True and False question:**

**1:** $\phi(n)$ is always even for $n > 2$

**2:** $\phi(1) = 1$

**3:** If $p$ is prime, then $\phi(p) = p$

**4:** Euler's theorem requires $a$ and $n$ to be coprime.

**5:** $\phi(n)$ is multiplicative for all integer $m, n$.

**Fill in the blanks question:**

**1:** $\phi(n)$ counts integers that are _____ to $n$.

**2:** If $p$ is prime, then $\phi(p) =$ _____.

**3:** Eulers theorem: $a^{\phi(p)} \equiv$ .....(mod $n$)

**4:** $\phi(p^k) \equiv p^k -$ .....

**5:** If $\gcd(m, n) = 1$, then $\phi(mn) =$ ……

**Match the following:**

| **Column A** | **Column B** |
|---|---|
| $\phi(p)$ | $(p-1)(q-1)$ |
| $\phi(pq)$ | $(p-1)$ |
| Euler's theorem | $a^{\phi(n)} \equiv 1 (\text{mod}\, n)$ |
| $\phi(p^k)$ | $p^k - p^{k-1}$ |

## 7.11 *ANSWERS*

**Answer of the objective questions:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | C | **2:** | B | **3:** | C | **4:** | B |
| **5:** | B | **6:** | B | **7:** | B | **8:** | B |

**Answer of true and false questions:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | True | **2:** | True | **3:** | False | **4:** | True |
| **5:** | False | | | | | | |

**Answer of fill in the blanks questions:**

**1:** Co-prime **2:** $p-1$ **3:** 1 **4:** $p^{k-1}$

**5:** $\phi(m)\phi(n)$

**Match the following**

**1-(b), 2-(a), 3-(c), 4-(d)**

# COURSE NAME: NUMBER THEORY

## COURSE CODE: MAT-606

# BLOCK - III: PRIMITIVE ROOTS

# UNIT 8: ORDER OF AN INTEGER MODULO *n* AND PRIMITIVE ROOTS FOR PRIMES

## CONTENTS:



## 8.1 *INTRODUCTION*

The unit on *Order of an Integer Modulo n and Primitive Roots for Primes* introduces fundamental concepts in multiplicative number theory that describe the behavior of integers under modular arithmetic. The *order* of an integer $a$ modulo $n$ is defined as the smallest positive integer $k$ such that $a^k \equiv 1 (\mathrm{mod}\, n)$, provided that $a$ and $n$ are coprime; this concept helps in understanding periodicity within modular systems and is closely linked to Euler's Theorem.

Building on this idea, the chapter explores *primitive roots*, which are integers whose powers generate all the units modulo a prime $p$, thereby forming a cyclic multiplicative group. The existence of primitive roots for prime moduli and their properties play a crucial role in simplifying computations and have important applications in modern areas such as cryptography. Overall, the chapter provides a bridge between abstract theory and practical applications by examining how multiplicative structures behave in modular arithmetic.

## 8.2 *OBJECTIVE*

After reading this unit learners will be able,

- To introduce the concept of the *order* of an integer modulo $n$, i.e., the smallest positive integer $k$ such that $a^k \equiv 1 (\mathrm{mod}\, n)$, and to study its fundamental properties.
- To explain the connection between order and Euler's Theorem, including how the order of an integer divides $\phi(n)$.
- To develop methods for computing the order of an integer modulo $n$ through examples and theorems.
- To define *primitive roots* modulo a prime $p$ and explain their significance in generating all nonzero residues modulo $p$.
- To prove the existence of primitive roots for prime moduli and study their properties.
- To determine how many primitive roots exist modulo a prime and how to find them.
- To explore the cyclic nature of the multiplicative group modulo a prime using primitive roots.

## 8.3 *THE ORDER OF AN INTEGER MODULO n*

In number theory, the order of an integer modulo $n$ describes how powers of an integer behave under modular arithmetic.

**Definitions:** Let $a$ and $n$ be integers with $\gcd(a, n)=1$ . The The order of a modulo n is the smallest positive integer $k$ such that:

$$a^k \equiv 1 (\mathrm{mod}\, n)$$

This value is denoted by; $ord_n(a) = k$

**Note 1:** The order exists only if *a* is relatively prime to *n*.

**2:** The order tells us the period of repetition of powers of *a* modulo *n*.

**3:** By, Euler's theorem, $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$

**Example 1:** Find the order of 2 modulo 7.

**Answer:** As we know that, $2^1 \equiv 2 (\mathrm{mod}\, 7)$

Similarly, $2^2 \equiv 4 (\mathrm{mod}\, 7)$; $2^3 \equiv 8 \equiv 1 (\mathrm{mod}\, 7)$

So, the smallest positive *k*, such that $2^k \equiv 1 (\mathrm{mod}\, 7)$ is $k = 3$.

Hence, $ord_7(2) = 3$.

**Theorem 1:** Let the integer *a* have order *k* modulo *n*, then $a^m \equiv 1 (\mathrm{mod}\, n)$ iff $k \mid m$; in particular, $k \mid \phi(n)$.

**Proof:** Suppose, $a^m \equiv 1 (\mathrm{mod}\, n)$. Then by division algorithm, $m = qk + r; 0 \le r < k$

Then, $a^m = a^{qk+r} = (a^k)^q . a^r; 0 \le r < k$

Taking modulo *n*: $a^m = (a^k)^q . a^r \equiv a^r (\mathrm{mod}\, n)$.

We have given, $a^m \equiv 1 (\mathrm{mod}\, n)$, So;

$a^r \equiv 1 (\mathrm{mod}\, n)$.

Since, *k* is the smallest positive integer satisfying this, we must have; $r = 0$

Hence, $m = qk \Rightarrow k \mid m$

**Conversely**, let us suppose that, $k \mid m$.

$\Rightarrow m = qk$ for some integer $q$. So,

$a^m = a^{qk} = (a^k)^q$

Taking modulo $n$; $a^m \equiv (a^k)^q \equiv 1^q \equiv 1 (\mathrm{mod}\, n)$.

Conclusion, $a^m \equiv 1 (\mathrm{mod}\, n) \Leftrightarrow k \mid m$

**In particular**, $k \mid \phi(n)$

By Euler's theorem, $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$

Using the result just proved, this implies: $k \mid \phi(n)$.

**Example 2:** As we know, $\gcd(2,13) = 1$.

Now, $2^1 \equiv 2 (\mathrm{mod} 13)$, $2^2 \equiv 4 (\mathrm{mod} 13)$; $2^3 \equiv 8 (\mathrm{mod} 13)$; $2^4 \equiv 3 (\mathrm{mod} 13)$; $2^5 \equiv 6 (\mathrm{mod} 13)$;

$2^6 \equiv 12 \equiv -1 (\mathrm{mod} 13)$

Then, $(2^6)^2 \equiv 2^{12} \equiv (-1)^2 \equiv 1 (\mathrm{mod} 13)$.

Hence, $2^{\phi(13)} \equiv 1 (\mathrm{mod} 13)$.

**Theorem 2:** If the integer $a$ has order $k$ modulo $n$, then $a^i \equiv a^j (\mathrm{mod}\, n)$ if and only if $i \equiv j (\mathrm{mod}\, k)$.

**Proof:** Let us suppose that, $a^i \equiv a^j (\mathrm{mod}\, n)$.

Then,

$\Rightarrow a^{i-j} \equiv 1 (\mathrm{mod}\, n)$. Now since the, $a^k \equiv 1 (\mathrm{mod}\, n)$, where $k$ is the least such integer.

Then by using the earlier theorem 1, we can say that $k \mid i-j$

Hence, $i \equiv j \pmod{k}$

Conversely, let us suppose that, $i \equiv j \pmod{k}$

Then, $k \mid (i-j) \Rightarrow i-j = kq$ for some integer $q$.

So, $a^{i-j} = a^{kq} = (a^k)^q$

Taking modulo $n$: $a^{i-j} = a^{kq} = (a^k)^q \equiv 1 \pmod{n}$

Thus, $a^i \equiv a^j \pmod{n}$

Hence, $a^i \equiv a^j \pmod{n} \Leftrightarrow i \equiv j \pmod{k}$.

**Corollary 1:** If a has order $k$ modulo $n$, then the integers $a, a^2, a^3, ..., a^k$ are incongruent modulo $n$.

**Theorem 3:** If the integer $a$ has order $k$ modulo $n$ and $h > 0$, then $a^h$ has order $k / \gcd(h,k)$ modulo $n$.

**Proof:** Let the order of $a$ modulo $n$ be $k$. Then, $a^k \equiv 1 \pmod{n}$ and $k$ is the least positive integer with this property. We want to find the order of $a^h$ modulo $n$.

By definition, $(a^h)^m \equiv 1 \pmod{n}$

i.e, $(a^h)^m \equiv 1 \pmod{n}$

that is, $a^{hm} \equiv 1 \pmod{n}$

Since $a$ has order $k$, we know that

$$a^r \equiv 1 (\text{mod}\, n) \Leftrightarrow k \mid r$$

Hence, $k \mid hm$

So, $m$ must be the smallest positive integer such that $k \mid hm$.

Let $d = \gcd(h,k)$ then $h = dh_1, k = dk_1$

Where, $\gcd(h_1, k_1) = 1$

Now the condition $k \mid hm$ becomes

$dk_1 \mid dh_1 m$ or $k_1 \mid h_1 m$ [ Since $\gcd(h_1, k_1) = 1$, it follows that $k_1 \mid m$ ]

Thus the smallest positive such $m$ is, $m = k_1 = \frac{k}{d}$

Therefore, $m = \frac{k}{\gcd(h,k)}$.

Hence the order of $a^h$ modulo $n$ is $\frac{k}{\gcd(h,k)}$

Or we can write, $ord_n(a^h) = \frac{ord_n(a)}{\gcd(h, ord_n(a))}$

**Example 3:** If $a$ has order 12 modulo $n$, then $a^8$ has order $\frac{12}{\gcd(8,12)} = \frac{12}{4} = 3$

So, $ord_n(a^8) = 3$

**Definition:** If $\gcd(a,n) = 1$ and $a$ is of order $\phi(n)$ modulo $n$, then $a$ is a primitive root of the integer $n$.

**Example 4:** 3 is a primitive root of 7, for

$3^1 \equiv 3; 3^2 \equiv 2; 3^3 \equiv 6; 3^4 \equiv 4; 3^5 \equiv 5; 3^6 \equiv 1 \pmod 7$

Thus, we will observed here, $3^{\phi(7)} \equiv 1 \pmod 7$ i.e., $3^6 \equiv 1 \pmod 7$.

**Theorem 4:** Let $\gcd(a, n) = 1$ and let $a_1, a_2, a_3, ..., a_{\phi(n)}$ be the positive integers less than $n$ and relatively prime to $n$. If $a$ is a primitive root of $n$, then $a, a^2, a^3, ..., a^{\phi(n)}$ are congruent modulo $n$ to $a_1, a_2, a_3, ..., a_{\phi(n)}$, in some order.

**Proof:** Since $a$ is a primitive root modulo $n$, its order is $ord_n(a) = \phi(n)$.

This means the least positive integer $k$ for which, $a^k \equiv 1 \pmod n$ is $k = \phi(n)$.

Because $\gcd(a, n) = 1$, every power of $a$ is also relatively prime to $n$. Thus $a, a^2, a^3, ..., a^{\phi(n)}$ are all integers relatively prime to $n$.

Hence each of these powers must be congruent modulo $n$ to one of numbers

$$a_1, a_2, a_3, ..., a_{\phi(n)}.$$

Suppose, $a^i \equiv a^j \pmod n \Leftrightarrow i \equiv j \pmod{\phi(n)}$.

Since the order of $a$ is $\phi(n)$. But i and j both lie between 1 and $\phi(n)$, so the only possibility is $i = j$.

Therefore, $a, a^2, a^3, ..., a^{\phi(n)}$ are pairwise incongruent modulo $n$.

There are exactly $\phi(n)$ integers less than n and relatively prime to $n$, namely

$$a_1, a_2, a_3, ..., a_{\phi(n)}.$$

We have obtained $\phi(n)$ distinct residues

$a, a^2, a^3, ..., a^{\phi(n)}$

All relatively prime to *n*.

Hence they must be exactly the same set as, $a_1, a_2, a_3, ..., a_{\phi(n)}$ possibly in a different order.

**Corollary 2:** If *n* has a primitive root, then it has exactly $\phi(\phi(n))$ of them.

**Proof:** Assume *n* has a primitive root and let a be one such primitive root. Then the order of *a* modulo *n* is $Ord_n(a) = \phi(n)$,

So the powers, $a, a^2, a^3, ..., a^{\phi(n)}$

Given all integers less than *n* that are relatively prime to *n*.

Thus every primitive root modulo *n* must be of the form $a^r$ for some integer *r* with $1 \le r \le \phi(n)$

As we know that, $ord_n(a^r) = \dfrac{\phi(n)}{\gcd(r, \phi(n))}$.

For $a^r$ to be a primitive root, its order must be $\phi(n)$. Hence,

$$\phi(n) = \frac{\phi(n)}{\gcd(r, \phi(n))} \Rightarrow \gcd(r, \phi(n)) = 1$$

Therefore, $a^r$ is a primitive root modulo $n \Leftrightarrow \gcd(r, \phi(n)) = 1$.

The number of integer *r* satisfying, $1 \le r \le \phi(n)$ and $\gcd(r, \phi(n)) = 1$, are by definition $\phi(\phi(n))$.

Hence there are exactly $\phi(\phi(n))$ primitive roots modulo *n*.

## 8.4 *PRIMITIVE ROOTS FOR PRIMES*

In number theory, primitive roots for primes are very important in the study of modular arithmetic and abstract algebra.

**Theorem 5:** If $p$ is a prime and $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0; a_n \not\equiv 0 \pmod{p}$ is a polynomial of degree $n \geq 1$ with integral coefficients, then the congruence $f(x) \equiv 0 \pmod{p}$ that has at most *n* incongruent solutions modulo *p*.

**Proof:** We prove the theorem by induction on the degree *n*.

**Base case (*n* = 1):** If $f(x) = a_1 x + a_0$ with $a_1 \neq 0$ (mod p), then the congruence $a_1 x + a_0 \equiv 0 \pmod{p}$ has exactly one solution modulo *p*, because $a_1$ has a multiplicative inverse modulo *p*.

**Inductive step:** Assume that every polynomial congruence of degree $n-1$ modulo *p* has at most $n-1$ incongruent solutions. Now let $f(x)$ be a polynomial of degree *n* and suppose *a* is a solution of $f(x) \equiv 0 \pmod{p}$. By the factor theorem over the field $Z_p$, we can write $f(x) \equiv (x-a)\, g(x) \pmod{p}$, where $g(x)$ is a polynomial of degree $n-1$ modulo *p*.

If *b* is any other solution of $f(x) \equiv 0 \pmod{p}$ with $b \neq a$ (mod p), then

$0 \equiv f(b) \equiv (b-a)g(b) \pmod{p}$.

Since *p* is prime and $b-a \not\equiv 0 \pmod{p}$, it follows that $g(b) \equiv 0 \pmod{p}$.

Thus every solution other than *a* is a solution of $g(x) \equiv 0 \pmod{p}$.

By the induction hypothesis, $g(x) \equiv 0 \pmod{p}$ has at most $n-1$ incongruent solutions.

Including the root *a*, the total number of incongruent solutions of $f(x) \equiv 0 \pmod{p}$ is at most $1+(n-1) = n$.

Hence the congruence $f(x) \equiv 0 \pmod{p}$ has at most *n* incongruent solutions modulo *p*.

**Corollary 3:** If *p* is a prime number and $d \mid p-1$, then the congruence $x^d - 1 \equiv 0 \pmod{p}$ has exactly *d* solutions.

**Proof:** Let $p$ be prime and let $d$ be a positive divisor of $p-1$. Write $p-1=d\cdot k$ for some integer $k\geq 1$.

**Step 1: Fermat's Little Theorem gives a factorization.**

By Fermat's Little Theorem, for any integer $x$ not divisible by $p$, we have

$$x^{p}-1\equiv 0\,(\mathrm{mod}\ p)$$

Thus every nonzero residue modulo $p$ satisfies

$$x^{p-1}-1\equiv 0\,(\mathrm{mod}\ p)$$

But $x^{p-1}-1=x^{dk}-1=(x^{d})^{k}-1$.
Using the algebraic identity

$$a^{k}-1=(a-1)(a^{k-1}+a^{k-2}+\cdots+a+1),$$

with $a=x^{d}$, we obtain

$$x^{p-1}-1=(x^{d}-1)\cdot Q(x),$$

where, $Q(x)=x^{d(k-1)}+x^{d(k-2)}+\cdots+x^{d}+1$.

Hence for every $x$ with $p\nmid x$,

$$(x^{d}-1)\cdot Q(x)\equiv 0\ (\mathrm{mod}\ p).$$

**Step 2: Degree argument and number of roots.**

The polynomial $x^{p-1}-1$ modulo $p$ has exactly $p-1$ distinct roots modulo $p$ (namely, all nonzero residues), by Fermat's theorem and the fact that a nonzero polynomial of degree $n$ over a field has at most $n$ roots.

Let $N$ be the number of solutions modulo $p$ to $x^{d}\equiv 1(\mathrm{mod}\ p)$.
Note: $x\equiv 0$ is not a solution, since $0^{d}=0\neq 1$.

We know:

- Every solution of $x^d \equiv 1$ is a solution of $x^{p-1} \equiv 1$.
- Conversely, if $x^{p-1} \equiv 1$ and $x$ is not a solution of $x^d \equiv 1$, then $Q(x) \equiv 0 (\text{mod } p)$.

Thus the $p-1$ nonzero residues are partitioned into:

- $N$ roots of $x^d - 1$, and
- Roots of $Q(x)$ among the remaining.

**Step 3: Show *N=d.***

The degree of $Q(x)$ is $d(k-1)=(p-1)-d$.
If $Q(x)$ had all $p-1-N$ remaining residues as roots, that would be too many roots unless $p-1-N \leq \deg Q = p-1-d$.

Thus, $p-1-N \leq p-1-d \Rightarrow -N \leq -d \Rightarrow N \geq d$.

On the other hand, $x^d - 1$ is a degree-$d$ polynomial over the field $Zp$, so it can have at most $d$ roots. Hence $N \leq d$.

Combining, $N = d$.

**Step 4: Conclusion.**

Therefore, the congruence $x^d - 1 \equiv 0 \pmod{p}$ has exactly $d$ solutions modulo $p$.

**Theorem 6:** If $p$ is a prime number and $d \mid p-1$, then there are exactly $\phi(d)$ incongruent integers having order $d$ modulo $p$.

**Proof:** Since $p$ is prime, there exists a primitive root modulo $p$.
Let $g$ be a primitive root modulo $p$. Then $Ord_p(g) = p-1$

This means every integer relatively prime to $p$ is congruent modulo $p$ to one of

$g, g^2, g^3, \ldots, g^{p-1}$.

**Consider powers of the primitive root**

Every nonzero residue modulo $p$ can be written in the form $g^r$ for some integer $r$, where $1 \le r \le p-1$.

We want to determine when $g^r$ has order $d$.

From the theorem on the order of a power,

$$ord_p(g^r) = \frac{p-1}{\gcd(r, p-1)}.$$

For the order to be $d$, we must have $\frac{p-1}{\gcd(r, p-1)} = d$.

Hence, $\gcd(r, p-1) = \frac{p-1}{d}$

Let, $m = \frac{p-1}{d}$.

Then the condition becomes, $\gcd(r, p-1) = m$

Now, write $r = mt$

Since, $\gcd(r, p-1) = m$, we can write

$r = mt$

Also, $p-1 = dm$

Substituting, $\gcd(mt, dm) = m$

Dividing by $m$, $\gcd(t, d) = 1$.

Thus $g^r$ has order $d$ if and only if $r = mt$ where $\gcd(t, d) = 1$.

Now, $t$ can take values, $1, 2, 3, ..., d$

Such that, $\gcd(t, d) = 1$. So, the number of such integers are exactly, $\phi(d)$. Therefore, there are exactly, $\phi(d)$ incongruent integers of order $d$ modulo $p$.

**Note:** The following table shows the least positive primitive root corresponding to each prime number less than 200.

**Table:** The least positive primitive root corresponding to each prime number less than 200.

| Prime | Least | Prime | Least | Prime | Least |
|---|---|---|---|---|---|

| | positive primitive root | | positive primitive root | | positive primitive root |
|---|---|---|---|---|---|
| 2 | 1 | 59 | 2 | 137 | 3 |
| 3 | 2 | 61 | 2 | 139 | 2 |
| 5 | 2 | 67 | 2 | 149 | 2 |
| 7 | 3 | 71 | 7 | 151 | 6 |
| 11 | 2 | 73 | 5 | 157 | 5 |
| 13 | 2 | 79 | 3 | 163 | 2 |
| 17 | 3 | 83 | 2 | 167 | 5 |
| 19 | 2 | 89 | 3 | 173 | 2 |
| 23 | 5 | 97 | 5 | 179 | 2 |
| 29 | 2 | 101 | 2 | 181 | 2 |
| 31 | 3 | 103 | 5 | 191 | 19 |
| 37 | 2 | 107 | 2 | 193 | 5 |
| 41 | 6 | 109 | 6 | 197 | 2 |
| 43 | 3 | 113 | 3 | 199 | 3 |
| 47 | 5 | 127 | 3 | | |
| 53 | 2 | 131 | 2 | | |

## Check your progress

**Problem 1:** Find the highest power of 13 contained in $20000!$

**Answer:** 1665

**Problem 2:** Find the value of $\mu(500)$ and $\mu(243)$

**Answer:** $\mu(500) = 0$ and $\mu(243) = 0$

## 8.5 *SUMMARY*

The unit "Order of an Integer Modulo $n$, primitive roots for primes" introduces two fundamental concepts in number theory: the order of an integer modulo $n$ and primitive roots. It explains that the order of an integer $a$ relatively prime to $n$ is the smallest positive integer $k$ such that $a^k \equiv 1 (\text{mod } n)$, and establishes important properties such as $k|\varphi(n)$ and the periodicity of powers modulo $n$. The chapter then develops the theory of **primitive roots**, especially for prime moduli, showing that a primitive root modulo a prime $p$ is an integer whose order is $p-1$, so its powers generate all nonzero residues modulo $p$. It further proves key results, including the existence of primitive roots for primes, the fact that the number of primitive roots modulo $p$ is $\varphi(p-1)$, and that for every divisor $d$ of $p-1$, exactly $\varphi(d)$ integers have order $d$ modulo $p$. Overall, the chapter highlights the cyclic structure of nonzero residues modulo a prime and its significance in solving congruences and understanding modular arithmetic.

## 8.6 *GLOSSARY*

- Order of an integer modulo $n$
- Primitive roots

## 8.7 *REFERENCES*


- **Burton, D. M.** (2007). *Elementary number theory* (6th ed.). McGraw-Hill.
- **T. M. Apostol**, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford.
- **Tom M. Apostol**, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York.
- **G. A. Jones and J. M. Jones**, *Elementary Number Theory*, Springer-Verlag, Berlin, 1998.

- **T. Nagell**, *Introduction to Number Theory*, Wiley, New York.


## 8.8 *SUGGESTED READING*


- **Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery**, *An Introduction to the Theory of Numbers*, John Wiley & Sons.
- **Hugh L. Montgomery and Robert C. Vaughan**, *Multiplicative Number Theory I: Classical Theory*, Cambridge University Press.
- **H. Iwaniec and E. Kowalski**, *Analytic Number Theory*, American Mathematical Society, 2004.
- **T. Koshy**, *Elementary Number Theory with Applications*, Academic Press.
- **Eric W. Weisstein**, "Möbius Inversion Formula," *MathWorld – Wolfram Resource*.


## 8.9 *TE1RMINAL QUESTION*

**Long Answer Type Question:**

**1.** Determine all the primitive roots of the primes $P = 11,19$ and 23, expressing each as a power of some one of the roots.

**2.** Given that 3 is primitive root of 43, find the following:

**(a)** All positive integers less than 43 having order 6 modulo 43.

**(b)** All positive integers less than 43 having order 21 modulo 43.

**3.** Find all positive integers less than 61 having order 4 modulo 61.

**Hint:** For easier way to prove this we first prove, $\tau(n)\phi(n) \geq 2^r . n(1/2)^r$

**Short answer type question:**

**1:** Find the order of the integers 2, 3 and 5 corresponds to respective one.

***a)*** Modulo 7

***b)*** Modulo 19

***c)*** Modulo 23.

**2 (a):** Find two primitive roots of 10.

**(b):** Using the fact that 3 is a primitive root modulo 17, determine all eight primitive roots of 17.

**3(a)**: Verify that 2 is a primitive root of 19, but not of 17.

**(b)**: Show that 15 has no primitive root by calculating the orders of 2, 4, 7, 8, 11, 13 and 14 modulo 15.

**Objective type questions:**

**1. The order of an integer *a* modulo *n* is the least positive integer *k* such that**

A) $a^k = n$
B) $a^k \equiv 1 (\mathrm{mod}\, n)$
C) $a + k \equiv 0 (\mathrm{mod}\, n)$
D) $a^k \equiv 0 (\mathrm{mod}\, n)$

**2. The order of 2 modulo 7 is**

A) 2
B) 3
C) 6
D) 1

**3. If *a* has order *k* modulo *n*, then *k* divides**

A) $a$
B) $n$
C) $\varphi(n)$
D) $a + n$

**4. A primitive root modulo a prime *p* has order**

A) $p$
B) $p-1$
C) $\varphi(p-1)$
D) 1

**5. The number of primitive roots modulo a prime $p$ is**

A) $p$
B) $p-1$
C) $\varphi(p)$
D) $\varphi(p-1)$

**6. Which of the following is a primitive root modulo 7?**

A) 1
B) 2
C) 3
D) 6

**7. If the order of a modulo $n$ is $k$, then the least positive integer satisfying, $a^m \equiv 1 \pmod{n}$ is**

A) $m = n$

B) $m = \phi(n)$

C) $m = k$

D) $m = 1$

**8. The order of 3 modulo 7 is**

A) 2

B) 3

C) 6

D) 1

**9. Which of the following is a primitive root modulo 5?**

**A)** 1

**B)** 2

**C)** 4

**D)** 0

**10: The order of $a^h$ modulo *n* is**

**A)** $hk$

**B)** $h+k$

**C)** $\dfrac{k}{\gcd(h,k)}$

**D)** $\gcd(h,k)$

**11: If a is a primitive root modulo prime *p*, then its power generate**

**A)** Only quadratic residues

**B)** All residues modulo $p$

**C)** All non-zero residues modulo $p$

**D)** Only prime residues

**12: The number of integers of order d modulo prime *p*, where $d \mid (p-1)$ is**

A) $d$

B) $(p-1)$

C) $\phi(d)$

D) $\phi(p)$

**True and False:**

**1:** Every prime number has at least one primitive root.

**2:** The order of an integer modulo $n$ always exists even if $\gcd(a,n) \neq 1$.

**3:** If $a$ has order $k$ modulo $n$, then $a^m \equiv 1 (\mathrm{mod}\, n)$ iff $k \mid m$.

**4:** Every integer relatively prime to $n$ is a primitive root modulo $n$.

**5:** If $a$ is a primitive root modulo $p$, then $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$

**Fill in the blanks question:**

**1:** If $p$ is prime, then the order of any primitive root modulo $p$ is ……

**2:** The number of primitive roots modulo $p$ is ... ...

**3:** If $a$ has order $k$, $a^i \equiv a^j (\mathrm{mod}\, n)$ *iff* $i \equiv j (\mathrm{mod} .....)$

**4:** The order of 2 modulo 7 is ……

**5:** The number of primitive roots modulo 11 is ……

## 8.10 *ANSWERS*

**Answer of long answer type questions:**

**1:** 2, $6 \equiv 2^9, 7 \equiv 2^7, 8 \equiv 2^3$

2, $3 \equiv 2^{13}, 10 \equiv 2^{17}, 13 \equiv 2^5, 14 \equiv 2^7, 15 \equiv 2^{11}$

5, $7 \equiv 5^{19}, 10 \equiv 5^3, 11 \equiv 5^9, 14 \equiv 5^{21}, 15 \equiv 5^{17}, 17 \equiv 5^7, 19 \equiv 5^{15}, 20 \equiv 5^5, 21 \equiv 5^{13}$

**4(a):** 7, 37 **4(b):** 9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38, 40

**5** 11, 50

**Answer of short questions:**

**1 (a):** 8, 16, 16 **(b):** 18, 18, 9 **(c):** 11, 11, 22

**2 (a):** 3, 7 **(b):** 3, 5, 6, 7, 10, 11, 12, 14

**Answer of the objective questions:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | B | **2:** | B | **3:** | C | **4:** | B |
| **5:** | D | **6:** | C | **7:** | C | **8:** | 6 |
| **9:** | B | **10:** | **C** | **11:** | C | **12:** | C |

**Answer of true and false questions:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | T | **2:** | F | **3:** | T | **4:** | F |
| **5:** | T | | | | | | |

**Answer of fill in the blanks questions:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | $p-1$ | **2:** | $\phi(p-1)$ | **3:** | $k$ | **4:** | 3 |
| **5:** | 4 | | | | | | |

# UNIT 9: THE THEORY OF INDICES

## CONTENTS:



## 9.1 *INTRODUCTION*

The unit **"**Theory of Indices**"** is an important part of elementary number theory that extends the study of primitive roots from prime numbers to certain composite numbers. It explains the conditions under which a composite number possesses primitive roots and examines the structure of the multiplicative system modulo $n$. The chapter also introduces the theory of indices**,** which is closely related to logarithms in modular arithmetic and provides a powerful method for simplifying complicated congruences and exponential calculations. Through concepts such as orders of integers, primitive roots of powers of primes, and indices modulo $n$, this

chapter develops important techniques that are widely used in solving congruences, studying cyclic groups, and understanding deeper properties of integers in modular arithmetic.

## 9.2 *OBJECTIVE*

After reading this unit learners will be able,

- To understand the concept of primitive roots for composite numbers.
- To identify which composite numbers possess primitive roots.
- To study the order of integers modulo $n$ and its properties.
- To examine primitive roots of powers of primes and their applications.
- To introduce the theory of indices and its relation to modular arithmetic.
- To learn methods for solving congruences using indices.
- To simplify exponential congruences through the use of primitive roots and indices.
- To develop computational techniques in number theory involving modular powers.
- To understand the cyclic nature of reduced residue systems when primitive roots exist.
- To provide a foundation for advanced topics in algebra, cryptography, and higher number theory.

## 9.3 *COMPOSITE NUMBERS HAVING PRIMITIVE ROOTS*

The topic *"Composite Numbers Having Primitive Roots"* is an important part of elementary number theory that studies those composite integers for which primitive roots exist. A primitive root of a number $n$ is an integer whose powers generate all integers relatively prime to $n$ under modular arithmetic. While primitive roots always exist for prime numbers, not every composite number possesses them. This topic focuses on identifying and characterizing the special composite numbers that admit primitive roots, namely numbers of the forms 2,4, $p^k$ and $2p^k$, where $p$ is an odd prime and $k\geq 1$. The study of primitive roots helps in understanding cyclic structures in modular systems and has important applications in cryptography, coding theory, and computational number theory.

**Theorem 1:** For $k \geq 3$, the integers $2^k$ has no primitive roots.

**Proof:** Assume that $k \geq 3$. We shall prove that there does not exist any integer whose order modulo $2^k$ is equal to

$\phi(2^k) = 2^{k-1}$

Now, every odd integer relatively prime to $2^k$ can be written in the form, $a = 2m+1$.

Consider the square of $a$: $a^2 = (2m+1)^2 = 4m^2 + 4m + 1$

Hence, $a^2 - 1 = 4m(m+1$

Since two consecutive integers $m$ and $m$+1 are such that one of them is even, the product $m(m$+1) is divisible by 2. Therefore, $4m(m+1$ is divisible by 8. Thus, $a^2 \equiv 1 (\mathrm{mod}\, 8)$

Because $k \geq 3$, we have $8 | 2^k$. Hence, $a^2 \equiv 1 (\mathrm{mod}\, 2^k)$

cannot hold for order greater than $2^{k-2}$. In fact, the order of every odd integer modulo $2^k$ divides $2^{k-2}$.

But, $\phi(2^k) = 2^{k-1}$

Therefore, no integer modulo $2^k$ can have order $2^{k-1}$

Hence, there is no primitive root modulo $2^k$.

Therefore, for $k \geq 3$, the integers $2^k$ has no primitive roots**.**

**Theorem 2:** For the integers $m, n > 2$ such that $\gcd(m,n) = 1$, then the integers $mn$ has no primitive roots.

**Proof:** Assume that $a$ is any integer relatively prime to $mn$.

Since $\gcd(m,n) = 1$, by Euler's theorem we have,

$a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)$ and $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$

Now consider the exponent, $\frac{\phi(mn)}{2}$.

Because, $\phi(mn) = \phi(m)\phi(n)$,

Since $m, n > 2$, both $\phi(m)$ and $\phi(n)$.

Therefore, $a^{\phi(mn)/2} \equiv 1 (\text{mod}\, m)$

And $a^{\phi(mn)/2} \equiv 1 (\text{mod}\, n)$.

Since, *m* and *n* are relatively prime, the congruence together imply, $a^{\phi(mn)/2} \equiv 1 (\text{mod}\, mn)$.

Thus every integers *a* relatively prime to *mn* satisfies, $a^{\phi(mn)/2} \equiv 1 (\text{mod}\, mn)$

Thus every integers *a* relatively prime to *mn* satisfies, $a^{\phi(mn)/2} \equiv 1 (\text{mod}\, mn)$.

So, no element can have order $\phi(mn)$.

Therefore, *mn* has no primitive roots.

**Corollary 1:** The integer $n$ fails to have a primitive root if either

**(*a*)** $n$ is divisible by two odd primes, or

**(*b*)** $n$ is of the form $n = 2^m p^k$, where $p$ is an odd prime and $m \geq 2$ .2

**Lemma 1:** For $a$ odd prime number $p$, there exists a primitive root $r$ of $p$ such that $r^{p-1} \not\equiv 1 (\text{mod}\, p^2)$.

**Proof:** Let *g* be a primitive root modulo *p*. Since *g* is a primitive root modulo *p*, its order is, $ord_p(g) = p - 1$.

Now consider the numbers,

$g, g + p, g + 2p, ..., g + (p-1)p$.

These are *p* distnict integers congruent to *g* (mod *p*).

We shall show that at least one of them satisfies,

$r^{p-1} \not\equiv 1 (\text{mod}\, p^2)$.

Assume, to the contrary, that for every integer, $k = 0, 1, 2, ..., p-1$

$(g + kp)^{p-1} \equiv 1 (\text{mod}\, p^2)$.

Using the binomial theorem,

$(g + kp)^{p-1} = g^{p-1} + (p-1)g^{p-2}(kp) + \text{terms containing } p^2$.

Hence modulo $p^2$,

$(g+kp)^{p-1} \equiv g^{p-1} + (p-1)kg^{p-2}p \pmod{p^2}$

By assumption this is congruent to $1 \pmod{p^2}$, so

$g^{p-1} + (p-1)kg^{p-2}p \equiv 1 \pmod{p^2}$

Take two different values $k_1 \neq k_2$. Substracting the corresponding congruence gives,

$(p-1)(k_1 - k_2)g^{p-2}p \equiv 0 \pmod{p^2}$

Dividing by $p$, $(p-1)(k_1 - k_2)g^{p-2} \equiv 0 \pmod{p}$

Since $p \nmid (p-1), p \nmid g$ and $k_1 - k_2 \not\equiv 0 \pmod{p}$, the above congruence is impossible.

Thus our assumption is false. Therefore, at least one integer among

$g, g+p, g+2p, ..., g+(p-1)p$

Satisfies, $r^{p-1} \not\equiv 1 \pmod{p^2}$.

Since each of these integers is congruent to $g \pmod{p}$, each is also a primitive root modulo $p$.

Hence there exists a primitive root r of p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$

**Lemma 2:** If $r$ be a primitive root of an odd prime $p$ with the property that $r^{p-1} \not\equiv 1 \pmod{p^2}$.

Then for each positive integer $k \geq 2$, $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$.

**Proof:** As we know that if $r$ be a primitive root of an odd prime $p$ such then by lemma 1, $r^{p-1} \not\equiv 1 \pmod{p^2}$.

We must show that for every integer $k \geq 2$,

$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$

Now, we proceed by induction on $k$.

For, $k = 2$, $p^{k-2}(p-1) = p^0(p-1) = p-1$

Hence the statement becomes, $r^{p-1} \not\equiv 1 \pmod{p^2}$

Which is true by the given hypothesis.

Assuming for some $k \geq 2$,

$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$

So, we have only to prove that, $r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$

Suppose, contrary to what we want to prove, that

$r^{p^{k-1}(p-1)} \equiv 1 (\text{mod } p^{k+1})$

Then there exist an integer *m* such that,

$r^{p^{k-1}(p-1)} = 1 + mp^{k+1}$

Now observe that,

$r^{p^{k-1}(p-1)} = \left(r^{p^{k-2}(p-1)}\right)^p$.

Let, $r^{p^{k-2}(p-1)} = 1 + ap^k$,

Where $a$ is an integer and $P \nmid a$.

(The condition $P \nmid a$ follows from the inductive hypothesis, since otherwise the expression would be congruent to $1 \pmod{p^{k+1}}$.

Then, $(1 + ap^k)^p = 1 + \binom{p}{1} ap^k + \binom{p}{2} a^2 p^{2k} + \ldots$

Since, $\binom{p}{1} = p$, $(1 + ap^k)^p = 1 + ap^k + (\text{terms divisible by } p^{k+2})$.

Therefore, $r^{p^{k-1}(p-1)} \equiv 1 + ap^{k+1} (\text{mod } p^{k+2})$.

Because $p \nmid a$, $1 + ap^{k+1} \not\equiv 1 (\text{mod } p^{k+2})$.

Hence, $r^{p^{k-1}(p-1)} \equiv 1 (\text{mod } p^{k+1})$, which contradicts our assumption. Thus the result holds for k+1.

Thus, for $k \geq 2$, $r^{p^{k-2}(p-1)} \not\equiv 1 (\text{mod } p^k)$.

**Theorem 3:** If $p$ is an odd prime number and $k \geq 1$, then there exist a primitive root for $p^k$.

**Proof:** We will prove the theorem in two cases.

**Case I:** For, $k = 1$, we know that every odd prime possesses a primitive root modulo *p*. Hence the theorem is true for $k = 1$.

**Case II:** For $k \geq 2$

Let *r* be a primitive root modulo *p*. Then the order of *r* modulo *p* is *p*-1.

Now consider the two integers $r$ and $r + p$.

Since both are congruent modulo *p*, $r + p \equiv r (\text{mod } p)$, the number $r + p$ is also a primitive root

modulo $p$. We show that at least one of $r$ or $r+p$ satisfies, $a^{p-1} \not\equiv 1 (\text{mod } p^2)$.

Indeed, suppose both satisfy, $r^{p-1} \equiv 1 (\text{mod } p^2)$

And $(r+p)^{p-1} \equiv 1 (\text{mod } p^2)$.

Using the binomial theorem, $(r+p)^{p-1} = r^{p-1} + (p-1)pr^{p-2} + \text{terms divisible by } p^2$.

Since $r^{p-1} \equiv 1 (\text{mod } p^2)$, $(r+p)^{p-1} \equiv 1 + (p-1)pr^{p-2} (\text{mod } p^2)$.

If this is congruent to 1 $(\text{mod } p^2)$, then $(p-1)pr^{p-2} \equiv 0 (\text{mod } p^2)$

Dividing by $p$, $(p-1)r^{p-2} \equiv 0 (\text{mod } p)$.

But $p \nmid (p-1)$ and $p \nmid r$, giving a contradiction.

Hence at least one of $r$ or $r+p$ satisfies, $a^{p-1} \not\equiv 1 (\text{mod } p^2)$.

Let this integer be denoted by $a$. Now, by lemma 2, for $k \geq 2$, $a^{p^{k-2}(p-1)} \not\equiv 1 (\text{mod } p^k)$.

Since for every $k \geq 2$, the Euler's phi-function gives, $\phi(p^k) = p^{k-1}(p-1)$.

Since the order of $a$ modulo $p^k$ gives $\phi(p^k)$, and no smaller exponent of the form $p^{k-2}(p-1)$ gives 1, the order of $a$ modulo $p^k$ must be exactly, $\phi(p^k) = p^{k-1}(p-1)$.

Since the order of $a$ modulo $p^k$ divides $\phi(p^k)$, and no smaller exponent of the form $p^{k-2}(p-1)$ gives 1, the order of $a$ modulo $p^k$ must be exactly, $\phi(p^k) = p^{k-1}(p-1)$.

Therefore $a$ is a primitive root modulo $p^k$.

For every odd prime $p$ and every integer $k \geq 1$, there exists a primitive root modulo $p^k$.

**Corollary:** There are primitive roots for $2p^k$, where $p$ is an odd prime and $k \geq 1$.

**Theorem 4:** An integer $n > 1$ has a primitive root if and only if $n = 2, 4, p^k \text{ or } p^k$, where $p$ is an odd prime.

**Proof:** It is already known that 2 and 4 possess primitive roots, and from the preceding theorem every power $p^k$ of an odd prime has a primitive root. Further, if $r$ is a primitive root modulo $p^k$, then $r$ is odd and its order modulo $2p^k$ is also $\phi(2p^k) = \phi(p^k)$; hence $2p^k$ also has a primitive root. Conversely, suppose that $n$ has a primitive root. If $n$ contains two distinct odd prime divisors, say $p$ and $q$, then the order of any integer modulo $n$ must divide both $\phi(p^a)$ and $\phi(q^b)$,

and therefore cannot equal $\phi(n)$; hence no primitive root exists in this case. Also, for $k \geq 3$, every odd integer satisfies $a^2 \equiv 1 (\text{mod}\, 8)$, which implies that the order of every integer modulo $2^k$ is strictly less than $\phi(2^k)$; thus $2^k$ has no primitive root for $k \geq 3$. Therefore the only integers greater than 1 that can possess primitive roots are $2, 4, p^k$ , and $2p^k$, where $p$ is an odd prime. Hence proved.

## 9.4 *THE THEORY OF INDICES*

The Theory of Indices is a powerful tool in number theory that simplifies the study of congruences by expressing integers as powers of a primitive root, thereby transforming multiplicative problems into additive ones.

Let $n$ be any integer that admits a primitive root $r$. As we know, the first $\phi(n)$ powers of $r$, $r, r^2, ..., r^{\phi(n)}$ are congruent modulo $n$, in some order, to those integers less than $n$ and relatively prime to it. Hence, if $a$ is an arbitrary integer relatively prime to $n$, then $a$ can be expressed in the form $a \equiv r^k (\text{mod}\, n)$

For a suitable choice of $k$, where $1 \leq k \leq \phi(n)$. This allow us to frame the following definition:

**Definition 1:** Let $r$ be a primitive root of $n$. If $\gcd(a, n) = 1$, then the smallest positive integer $k$, such that $a \equiv r^k (\text{mod}\, n)$ is called the index of $a$ relative to $r$.

Customarily, we denote the index of $a$ relatively to $r$ by $ind_r a$ or, if no confusion is likely to occur, by $ind\, a$. Clearly, $1 \leq ind_r a \leq \phi(n)$ and $r^{ind_r a} \equiv a (\text{mod}\, n)$

The notation $ind_r a$ is meaningless unless $\gcd(a, n) = 1$; in the future, this will be tactically assumed.

**Example 1:** As we know 2 is primitive root of 5 and

$2^1 \equiv 2 (\text{mod}\, 5), 2^2 \equiv 4 (\text{mod}\, 5), 2^3 \equiv 3 (\text{mod}\, 5), 2^4 \equiv 1 (\text{mod}\, 5)$

So, it followed that, $ind_2 1 = 4; ind_2 2 = 1, ind_2 3 = 3, ind_2 4 = 2$

**Theorem 5:** If $n$ has a primitive root $r$ and $ind\, a$ denotes the index of a relative to $r$, then the following property holds:

**(a)** $ind\ (ab) \equiv ind\ a + ind\ b \pmod{\phi(n)}$.

**(b)** $ind\ a^k \equiv k ind\ a \pmod{\phi(n)}$ for $k > 0$

**(c)** $ind\ 1 \equiv 0 \pmod{\phi(n)}$, $ind\ r \equiv 1 \pmod{\phi(n)}$

**Poof:** Since $r$ is a primitive root modulo $n$, every integer relatively prime to $n$ can be expressed as a power of $r$. Let

$r^{ind_r a} \equiv a \pmod{n}$, $r^{ind_r b} \equiv b \pmod{n}$

Multiplying these congruences, we obtain

$ab \equiv r^{ind_r a + ind_r b} \pmod{n}$

By the uniqueness of indices modulo $\phi(n)$,

$ind(ab) \equiv ind\ a + ind\ b \pmod{\phi(n)}$,

Which proves (a), raising $a \equiv r^{ind_r a}$ to the $k$-th power gives

$a^k \equiv r^{k ind_r a} \pmod{n}$

And therefore, $ind(a^k) \equiv k\ ind\ a \pmod{\phi(n)}$,

Proving (b). Finally, since

$1 \equiv r^0 \pmod{n}$ and $r \equiv r^1 \pmod{n}$

It follows directly that, $ind\ 1 \equiv 0 \pmod{\phi(n)}$

And $ind\ r \equiv 1 \pmod{\phi(n)}$.

Hence all the stated properties if indices are established.

**Example 2:** Solve the congruence, $4x^9 \equiv 7 \pmod{13}$

**Solution:** Since 2 is a primitive root modulo 13, we use indices relative to 2. The index table modulo 13 is:

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $ind\ a$ | 0 | 1 | 4 | 2 | 9 | 5 | 11 | 3 | 8 | 10 | 7 | 6 |

Given $4x^9 \equiv 7 \pmod{13}$,

Taking indices of both sides yields, $ind(4x^9) \equiv ind\ 7 \pmod{12}$

Using the properties of indices, $ind\ 4 + ind(x^9) \equiv 11 \pmod{12}$

Since, $ind\ 4 = 2$,

And $ind\,4 + ind(x^9) \equiv 11 \pmod{12}$

Since, $ind\,4 = 2$

And, $ind(x^9) \equiv 9\,ind\,x \pmod{12}$

We obtain, $2 + 9\,ind\,x \equiv 11 \pmod{12}$

Or, $9\,ind\,x \equiv 9 \pmod{12}$

Dividing by 3,

$3\,ind\,x \equiv 3 \pmod{4}$

Since, $3^{-1} \equiv 3 \pmod{4}$, $ind\,x \equiv 1 \pmod{4}$.

Therefore, $ind\,x \equiv 1, 5, 9 \pmod{12}$

From the index table: $ind\,2 = 1, ind\,6 = 5, ind\,5 = 9 \pmod{12}$

Hence, $x \equiv 2, 5, 6 \pmod{13}$.

Thus the solution of $4x^9 \equiv 7 \pmod{13}$ are

$x = 2, 5, 6 \pmod{13}$

**Theorem 5:** Let $n$ be an integer possessing a primitive root and let $\gcd(a, n) = 1$. Then the congruence $x^k \equiv a \pmod{n}$ has a solution if and only if $a^{\phi(n)/d} \equiv 1 \pmod{n}$

Where, $d = \gcd(k, \phi(n))$; if the solution are exist then there are exactly $d$ solution modulo $n$.

**Proof:** Suppose $g$ is a primitive root modulo $n$. Then every invertible residue can be written as

$a \equiv g^m, x \equiv g^t$

Substitute into $x^k \equiv a \pmod{n}$ gives, $g^{kt} \equiv g^m \pmod{n}$,

Which is equivalent to the linear congruence, $kt \equiv m \pmod{\phi(n)}$.

A linear congruence $kt \equiv m \pmod{\phi(n)}$ has solution iff $\gcd(k, \phi(n)) = d$ divides $m$.

Now, $d \mid m$ is equivalent to, $g^{m\phi(n)/d} \equiv 1$,

And since $a = g^m$, $a^{\phi(n)/d} \equiv 1 \pmod{n}$.

This proves the solvability criterion. Furthermore, a linear congruence modulo $\phi(n)$ has exactly $d$ solutions when solvable, yielding exactly $d$ solution for $x$.

**Example 3:** Solve $x^2 \equiv 4 \pmod 7$

**Answer:** Since, $\phi(7) = 6$, and $d = \gcd(2,6) = 2$.

Check the criterion, $4^{6/2} = 4^3 = 64 \equiv 1 \pmod 7$.

So, solution exist. Since $d = 2$, then there must be exactly two solutions modulo 7:

$x \equiv 2, 5 \pmod 7$. Indeed, $2^2 \equiv 4 \pmod 7, 5^2 \equiv 4 \pmod 7$

## Check your progress

---

**Problem 1:** Find the solution of the congruence, $x^3 \equiv 4 \pmod{13}$

**Answer:** $x \equiv 7, 8, \text{ and } 11 \pmod{13}$

**Problem 2:** Find the index of 5 relative to each of the primitive roots of 13

**Answer:** $ind_2 5 = 9$; $ind_6 5 = 9$; $ind_7 5 = 3$; $ind_{11} 5 = 3$

---

## 9.5 *SUMMARY*

---

The chapter "Composite Numbers Having Primitive Roots and Theory of Indices" deals with composite integers that possess primitive roots, namely numbers of the form 2, 4, $p^k$, and $2p^k$, where $p$ is an odd prime. A primitive root modulo $n$ generates all integers relatively prime to $n$ through its powers, and the concept of the **order** of an element is used to determine whether a number is a primitive root. The chapter introduces the **theory of indices (discrete logarithms)**, where every residue relatively prime to $n$ can be expressed as a power of a primitive root, and the corresponding exponent is called its index. Indices satisfy properties similar to ordinary logarithms, converting multiplication into addition and powers into multiplication, which greatly simplifies computations in modular arithmetic. Using indices, higher-degree congruences such as $x^k \equiv a \pmod n$ can be reduced to linear congruences, leading to important solvability conditions

and methods for finding all solutions. Overall, the chapter provides powerful tools for studying modular arithmetic, primitive roots, orders of elements, and exponential congruences.

## 9.6 *GLOSSARY*

- Theory of indices
- Primitive roots

## 9.7 *REFERENCES*


- **Burton, D. M.** (2007). *Elementary number theory* (6th ed.). McGraw-Hill.
- **T. M. Apostol**, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford.
- **Tom M. Apostol**, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York.
- **G. A. Jones and J. M. Jones**, *Elementary Number Theory*, Springer-Verlag, Berlin, 1998.
- **T. Nagell**, *Introduction to Number Theory*, Wiley, New York.


## 9.8 *SUGGESTED READING*


- **Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery**, *An Introduction to the Theory of Numbers*, John Wiley & Sons.
- **Hugh L. Montgomery and Robert C. Vaughan**, *Multiplicative Number Theory I: Classical Theory*, Cambridge University Press.
- **H. Iwaniec and E. Kowalski**, *Analytic Number Theory*, American Mathematical Society, 2004.
- **T. Koshy**, *Elementary Number Theory with Applications*, Academic Press.
- **Eric W. Weisstein**, "Möbius Inversion Formula," *MathWorld – Wolfram Resource*.

## 9.9 *TE1RMINAL QUESTION*

**Long Answer Type Question:**

**1.** Show that if $n \neq 2, 4, p^k, 2p^k$, where $p$ is an odd prime, then $n$ has no primitive root.

**2.** Solve the congruences $13x \equiv 2 \pmod{40}$ and $3x \equiv 13 \pmod{77}$.

**3.** Find the index of 5 relative to each of the primitive roots of 13.

**4.** Using a table of indices for a primitive root of 11, solve the following congruences:

**(a)** $7x^3 \equiv 3 \pmod{11}$

**(b)** $3x^4 \equiv 5 \pmod{11}$

**(c)** $x^8 \equiv 10 \pmod{11}$

**Answer of long question:**

**2.** $x \equiv 34 \pmod{40}$; $x \equiv 30 \pmod{77}$

**3.** $ind_2 5 = 9; ind_6 5 = 9; ind_7 5 = 3; ind_{11} 5 = 3$

**4.** **(a)** $x \equiv 7 \pmod{11}$

**(b)** $x \equiv 5, 6 \pmod{11}$

**(c)** No solution

**Short answer type question:**

**1:** Find the four primitive root of 26 and the eight primitive roots of 25.

**2:** Determine all the primitive root of $3^2, 3^3$ and $3^4$.

**3:** Find the remainder when $3^{24}.5^{13}$ is divisible by 17.

**4:** Show that the congruence $x^3 \equiv 3 \pmod{19}$ has no solutions, whereas $x^3 \equiv 11 \pmod{19}$ has three incongruent solutions.

**5:** Determine whether the two congruence $x^5 \equiv 13 \pmod{23}$ and $x^7 \equiv 15 \pmod{29}$ are solvable.

**Answer of short questions:**

**1:** $7, 11, 15, 19;\ 2, 3, 8, 12, 13, 17, 22, 23$

**2:** $2, 5;$

$2, 5, 11, 14, 20, 23;$

$2, 5, 11, 14, 20, 23, 29, 32, 38, 41, 47, 50, 56, 59, 65, 68, 74, 77;$

**3:** 14

**4:** Only the first congruence has a solution.

**Objective type questions:**

**1.** A primitive root modulo *n* is an integer whose powers generate:

(A) All integers modulo *n*

(B) All integers relatively prime to *n*

(C) Only prime numbers

(D) Only quadratic residues

**2.** Primitive roots exist modulo:

(A) Every positive integer

(B) Only prime numbers

(C) 2, 4, $p^k$, and $2p^k$, where $p$ is an odd prime

(D) All composite numbers

**3.** The order of an element $a$ modulo n is:

(A) The largest power of $a$

(B) The smallest positive integer $m$ such that $a^k \equiv 1 (\mathrm{mod}\, n)$

(C) $\phi(n)$

(D) The index of $a$

**4.** If $g$ is a primitive root modulo $n$, then the order of $g$ is:

(A) $n$

(B) $n-1$

(C) $\varphi(n)$

(D) 1

**5.** The index of a number is defined with respect to:

(A) Euler's function

(B) A primitive root

(C) A prime number

(D) A divisor of $n$

**6.** If $ind(a) = r$, then:

(A) $a = r$

(B) $a \equiv g^r \,(\mathrm{mod}\, n)$

(C) $a^r \equiv 1$

(D) $g \equiv a^r$

**7.** Which of the following is true?

(A) $ind\,(ab) = ind(a)\,ind(b)$

(B) $ind\,(ab) = ind(a) + ind(b)$

(C) $ind\,(ab) = 0$

(D) None of these

**8.** The congruence $x^k \equiv a \pmod{n}$ can be reduced to:

(A) A quadratic equation

(B) A differential equation

(C) A linear congruence in indices

(D) A matrix equation

**9.** The number of incongruent solutions of $x^k \equiv a \pmod{n}$, when solutions exist, is:

(A) $k$

(B) $\phi(n)$

(C) $d = \gcd(k, \phi(n))$

(D) 1

**10.** Euler's theorem states that if $\gcd(a, n) = 1$, then:

(A) $a^n \equiv 1 \pmod{n}$

(B) $a^{\phi(n)} \equiv 1 \pmod{n}$

(C) $a^{n-1} \equiv 1 \pmod{n}$

(D) $a^2 \equiv 1 \pmod{n}$

**True (T) and False (F):**

**1:** Every composite number has a primitive root.

**2:** The order of an element always divides φ(n).

**3:** Indices are analogous to ordinary logarithms.

**4:** If g is a primitive root modulo n, every reduced residue modulo n can be expressed as a power of g.

**5:** Primitive roots exist modulo 15.

**6:** The index method converts multiplication into addition.

**7:** The congruence $x^k \equiv a \pmod{n}$ may have more than one solution

**8:** The order of a primitive root is always 1.

**Fill in the blanks question:**

**1:** A primitive root modulo *n* has order equal to _____.

**2:** The Euler totient function is denoted by _____.

**3:** The index of a number is defined relative to a _____ root.

**4:** If $d = \gcd(k, \phi(n))$, then $x^k \equiv a \pmod{n}$ has exactly _____ solutions whenever it is solvable.

**5:** The theory of indices is also known as the theory of _____ logarithms.

**6:** Every reduced residue modulo n can be expressed as a power of a primitive root when a primitive root _____.

**7:** The order of an element *a* modulo *n* is the least positive integer *m* such that $a^m \equiv$ _____ (mod n).

**8:** The composite numbers possessing primitive roots are 2, 4, $p^k$, and _____.

## 9.10 *ANSWERS*

**Answer of long answer type questions:**

**Answer of the objective questions:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | B | **2:** | C | **3:** | B | **4:** | C |
| **5:** | B | **6:** | B | **7:** | B | **8:** | C |
| **9:** | C | **10:** | B | | | | |

**Answer of the true and false:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | F | **2:** | T | **3:** | T | **4:** | T |
| **5:** | F | **6:** | T | **7:** | T | **8:** | F |

**Answer of fill in the blanks:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | $\phi(n)$ | **2:** | $\phi(n)$ | **3:** | primitive | **4:** | d |
| **5:** | discrete | **6:** | exists | **7:** | 1 | **8:** | $2p^k$ |

# UNIT-10: QUADRATIC CONGRUENCE

## CONTENTS:



## 10.1 *INTRODUCTION*

Quadratic congruences form a fundamental topic in number theory and extend the study of linear congruences to polynomial congruences of degree two. A quadratic congruence is generally of the form $ax^2 + bx + c \equiv 0 \pmod{n}$, where $a$, $b$, $c$, and $n$ are integers and $a \neq 0$. The primary objective is to determine the existence and nature of solutions modulo a given integer $n$. The investigation of quadratic congruences naturally leads to the concepts of quadratic residues and quadratic non-residues, which describe whether an integer is congruent to a perfect square modulo $n$. These ideas play a central role in understanding the arithmetic properties of integers and have deep connections with Euler's criterion, Legendre symbols, Jacobi symbols, and the

law of quadratic reciprocity, one of the most celebrated results in number theory. The methods developed for solving quadratic congruences provide powerful tools for analyzing higher-degree congruences and contribute significantly to modern applications such as cryptography, coding theory, computer security, and computational number theory. Thus, the study of quadratic congruences not only enriches the theory of modular arithmetic but also serves as a gateway to many advanced topics in mathematics.

## 10.2 *OBJECTIVE*

After studying this chapter, the learner will be able to:

- Understand the concept of a quadratic congruence and distinguish it from linear congruences.
- Solve quadratic congruences of the form $ax^2 + bx + c \equiv 0 \pmod{n}$.
- Define and identify quadratic residues and quadratic non-residues modulo an integer.
- Determine whether a given integer is a quadratic residue modulo a prime.
- Understand and use the Legendre symbol and its properties in solving congruences.
- Apply the Law of Quadratic Reciprocity and its supplementary laws.
- Find square roots modulo prime and composite moduli when they exist.
- Analyze the number and nature of solutions of quadratic congruences modulo $n$.
- Develop proficiency in modular arithmetic techniques related to higher-degree congruences.
- Appreciate the importance of quadratic congruences in advanced number theory, cryptography, coding theory, and computational mathematics.

These objectives provide a systematic understanding of the theory, properties, and applications of quadratic congruences in elementary and advanced number theory.

## 10.3 *QUADRATIC CONGRUENCE*

The quadratic congruence in one variable is given by, $ax^2 + bx + c \equiv 0 \pmod{p}$ , where $a, b, c$ are

integers, $p$ is an odd prime and $p \nmid a$.

**Theorem 1:** The quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ can be reduced to the form $y^2 \equiv d \pmod{p}$, where $y = 2ax + b$ and $d = b^2 - 4ac$.

**Proof:** Multiplying the given quadratic congruence by $4a$, we get

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$$

Which can be written as $(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}$.

Putting $2ax + b = y$ and $b^2 - 4ac = d$, we get

$$y^2 \equiv d \pmod{p}.$$

**Theorem 2:** If the congruence $x^2 \equiv a \pmod{p}$ is solvable then it has exactly two solutions.

**Proof:** Let $x_0$ be a solution of the given congruence. Then

$${x_0}^2 \equiv a \pmod{p} \qquad \textbf{..... (1)}$$

Obviously $(p - x_0)$ is also satisfies the given congruence

$$(p - x_0)^2 \equiv a \pmod{p} \qquad [\because (p - x_0)^2 \equiv (-x_0)^2 \pmod{p}] \textbf{ ..... (2)}$$

Thus, $x_0$ and $(p - x_0)$ are two solutions of given congruence.

Suppose if possible $x_1$ be a third solution of the given congruence. Then

$${x_1}^2 \equiv a \pmod{p} \qquad \textbf{..... (3)}$$

From equation **(1)** and **(3)** we get

$${x_1}^2 \equiv {x_0}^2 \pmod{p}$$

This gives that $p$ divides $(x_1 - x_0)(x_1 + x_0)$. This implies that either p divides $x_1 - x_0$ or $p$ divides $(x_1 + x_0)$. In first case we have $x_1 \equiv x_0 \pmod{p}$ and in second case we have $x_1 \equiv p - x_0 \pmod{p}$. This shows that $x_1$ is not a distinct solution. Thus, the congruence $x^2 \equiv a \pmod{p}$ has exactly two solutions.

**Theorem 3:** The congruence $x^{(p-1)/2} \equiv 1 \pmod{p}$ has exactly $\frac{(p-1)}{2}$ solutions given by $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$.

**Solution:** Let $A = \left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$

Now if, $r^2 \in A$ then $(r, p) = 1$. By Fermat's theorem we have

$$x^{p-1} \equiv 1 \pmod{p}$$

Then

$$(r^2)^{\left(\frac{p-1}{2}\right)} \equiv 1 \pmod{p}.$$

This shows that every number of $A$ is a solution of the given congruence.

Further if $r_1{}^2 \equiv r_2{}^2 \pmod{p}$ such that $1 \le r_1 \le r_2 \le \frac{p-1}{2}$, then $(r_1 - r_2)(r_1 + r_2)$, will be divisible by $p$. But this is not possible because $r_1 - r_2$ and $r_1 + r_2$ both are numerically less than $p$. Also $\frac{p-1}{2}$ divides $p-1$. Therefore, the given congruence has exactly $\left(\frac{p-1}{2}\right)$ solutions given by $A$.

**Question 1:** Solve $x^2 \equiv 1 \pmod 8$

**Solution:** Checking the residues modulo 8:

$$1^2 = 1 \pmod 8$$
$$3^2 = 9 \equiv 1 \pmod 8$$
$$5^2 = 25 \equiv 1 \pmod 8$$
$$7^2 = 49 \equiv 1 \pmod 8$$

Hence the solutions are $x \equiv 1, 3, 5, 7 \pmod 8$.

**Question 2:** Solve $x^2 \equiv 4 \pmod 7$

**Solution:** Since $2^2 = 4,\ 5^2 = 25 \equiv 4 \pmod 7$, the solutions are $x \equiv 2, 5 \pmod 7$.

**Question 3:** Solve $x^{11} \equiv 1 \pmod{23}$.

**Solution:** Here, 23 is a prime and $\frac{23-1}{2} = 11$. Therefore $x^{11} \equiv 1 \pmod{23}$ has exactly 11 solutions given by,

$$x \equiv 1^2, 2^2, 3^2, \ldots, 11^2 \pmod{23}$$
$$\equiv 1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6 \pmod{23}.$$

**Question 4:** Solve the congruence $x^2 + 3x + 11 \equiv 0 \pmod{13}$.

**Solution:** We have $x^2 + 3x + 11 \equiv 0 \pmod{13}$

$\Longrightarrow \quad 4x^2 + 12x + 44 \equiv 0 \pmod{13}$

$\Longrightarrow \quad (2x+3)^2 \equiv 4 \pmod{13}$

Or $\quad y^2 \equiv 4 \pmod{13}$, where $y = 2x + 3$

$y \equiv 2 \pmod{13}$

$y \equiv 11 \pmod{13}$.

Thus, $2x + 3 \equiv 2 \pmod{13}$ and $2x + 3 \equiv 11 \pmod{13}$

Or $2x \equiv 12 \pmod{13}$ and $2x \equiv 8 \pmod{13}$

Or $x \equiv 6 \pmod{13}$ and $x \equiv 4 \pmod{13}$.

**Question 5:** Solve the congruence $x^2 \equiv 5 \pmod{29}$.

**Solution:** We have $x^2 \equiv 5 \pmod{29}$

$\Rightarrow \quad x^2 \equiv 5 \pmod{29}$

$\Rightarrow \quad x^2 \equiv (5 + 29) \pmod{29}$

$\Rightarrow \quad y^2 \equiv (34 + 29) \pmod{29}$

$\Rightarrow \quad y^2 \equiv (63 + 29) \pmod{29}$

$\Rightarrow \quad y^2 \equiv (92 + 29) \pmod{29}$

$\Rightarrow \quad y^2 \equiv 121 \pmod{29}$

$\Rightarrow \quad y^2 \equiv 11^2 \pmod{29}$

Therefore the required solution are

$$x \equiv 11, (29 - 11) \pmod{29}$$

$$\equiv 11, 18 \pmod{29}.$$

Thus, $2x + 3 \equiv 2 \pmod{13}$ and $2x + 3 \equiv 11 \pmod{13}$

Or $2x \equiv 12 \pmod{13}$ and $2x \equiv 8 \pmod{13}$

Or $x \equiv 6 \pmod{13}$ and $x \equiv 4 \pmod{13}$.

**Question 6:** Solve the congruence $3x^2 + 5x + 9 \equiv 0 \pmod{11}$.

**Solution:** We have, $3x^2 + 5x + 9 \equiv 0 \pmod{11}$. … (1)

Multiplying (1) by $3 \times 4 = 12$, we get

$36x^2 + 60x + 108 \equiv 0 \pmod{11}$.

This can be written as, $(6x + 5)^2 \equiv 5 \pmod{11}$. … (2)

Putting, $y \equiv (6x + 5)$ in (2), we get

$y^2 \equiv 5 \pmod{11}$

$\equiv (5 + 11) \pmod{11}$

$\equiv 4^2 \pmod{11}$

This gives, $y \equiv \pm 4 \pmod{11}$

Or $6x + 5 \equiv \pm 4 \pmod{11}$

Or $6x \equiv (2, 10) \pmod{11}$

Or $x = 4, 9 \pmod{11}$

## Check your progress

**Problem 1:** Solve the congruence $x^2 + 9x + 20 \equiv 0 \pmod{41}$

**Answer:** $x \equiv 36, 37 \pmod{41}$

**Problem 2:** Determine all the solution of $4x^2 - 3x - 5 \equiv 0 \pmod{53}$

**Answer:** $x \equiv 21, 46 \pmod{53}$

## 10.4 *SUMMARY*

The chapter on Quadratic Congruence deals with congruences of the form $ax^2 + bx + c \equiv 0 \pmod{n}$, where the objective is to determine integer solutions modulo $n$. It introduces the fundamental concepts of quadratic residues and non-residues, which help identify whether a congruence of the form $x^2 \equiv a \pmod{n}$ has a solution. The chapter explores various methods for solving quadratic congruences modulo primes and composite moduli. It also examines the application of quadratic congruences and primitive roots, as well as techniques for finding all incongruent solutions. Through these concepts, the chapter highlights the importance of quadratic congruences in understanding the structure of integers modulo $n$ and their applications in advanced number theory, cryptography, and algebraic investigations.

## 10.5 *GLOSSARY*

- Quadratic congruence

- Solvable
- Quadratic incongruence

## 10.6 *REFERENCES*


- **Burton, D. M.** (2007). *Elementary number theory* (6th ed.). McGraw-Hill.
- **T. M. Apostol**, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford.
- **Tom M. Apostol**, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York.
- **G. A. Jones and J. M. Jones**, *Elementary Number Theory*, Springer-Verlag, Berlin, 1998.
- **T. Nagell**, *Introduction to Number Theory*, Wiley, New York.


## 10.7 *SUGGESTED READING*


- **Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery**, *An Introduction to the Theory of Numbers*, John Wiley & Sons.
- **Hugh L. Montgomery and Robert C. Vaughan**, *Multiplicative Number Theory I: Classical Theory*, Cambridge University Press.
- **H. Iwaniec and E. Kowalski**, *Analytic Number Theory*, American Mathematical Society, 2004.
- **T. Koshy**, *Elementary Number Theory with Applications*, Academic Press.
- **Eric W. Weisstein**, "Möbius Inversion Formula," *MathWorld – Wolfram Resource*.


## 10.8 *TE1RMINAL QUESTION*

**Long Answer Type Question:**

**1.** Solve the quadratic congruence, $x^2 \equiv 23 \pmod{41}$.

**2.** Find all incongruent solution of the congruence $x^2 \equiv 45 \pmod{77}$.

**3.** Solve the quadratic congruence $3x^2 + 5x + 2 \equiv 0 \pmod{17}$.

**4.** Determine all solution of $5x^2 - 7x + 6 \equiv 0 \pmod{19}$.

**5.** Solve the congruence $x^2 \equiv 64 \pmod{105}$.

**6.** Show that the congruence $x^2 \equiv 7 \pmod{29}$ has no solution.

**7.** Find all integers satisfying $x^2 + 4x + 1 \equiv 0 \pmod{23}$

**8.** Solve the quadratic congruence $2x^2 + 7x + 3 \equiv 0 \pmod{31}$

**9.** Determine all incongruent solution of $x^2 \equiv 16 \pmod{65}$

**10.** Solve the congruence $x^2 \equiv 121 \pmod{143}$

**Short answer type question:**

**1:** Using the Chinese Remainder theorem, solve $x^2 \equiv 9 \pmod{91}$.

**2:** Find all solution of $x^2 + 6x + 8 \equiv 0 \pmod{29}$.

**3:** Determine whether the congruence, $x^2 \equiv 11 \pmod{43}$ is solvable. If it is, find all solutions.

**4:** Solve, $7x^2 + 4x + 9 \equiv 0 \pmod{37}$.

**5:** Find all incongruent solution of $x^2 \equiv 36 \pmod{119}$.

**Objective type questions:**

**1.** A congruence of the form $ax^2 + bx + c \equiv 0 \pmod{n}$ is called:

A) Linear congruence
B) Quadratic Congruence

C) Cubic Congruence
D) Exponential congruence

**2.** The congruence $x^2 \equiv a \pmod{p}$ is solvable if and only if *a* is a:

A) Primitive root
B) Quadratic residue
C) Composite number
D) Prime number

**3.** The solution of $x^2 \equiv 1 \pmod{p}$, where *p* is an odd prime, are:

A) $x \equiv 0$

B) $x \equiv \pm 1$

C) $x \equiv 2$

D) None of these

**4.** The congruence $x^2 \equiv -1 \pmod{p}$ is solvable when:

A) $p \equiv 1 \pmod{4}$

B) $p \equiv 3 \pmod{4}$

C) $p = 2$

D) Never

**5.** A quadratic congruence is *a* of congruence of the form:

A) $ax + b \equiv 0 \pmod{n}$

B) $ax^2 + bx + c \equiv 0 \pmod{n}$

C) $ax^3 + bx + c \equiv 0 \pmod{n}$

D) $a^x \equiv b \pmod{n}$

**6.** The congruence $x^2 \equiv 1 \pmod{7}$ has

A) One solution

B) Two solution

C) Three solution

D) No solution

**7.** The congruence $x^2 \equiv 0 \pmod{p}$, where $p$ is prime, has the solution.

A) $x \equiv 1$

B) $x \equiv -1$

C) $x \equiv 0$

D) No solution

**8.** Which of the following congruence's has no solution 7?

A) $x^2 \equiv 1$

B) $x^2 \equiv 2$

C) $x^2 \equiv 3$

D) $x^2 \equiv 4$

**9.** If $a$ is quadratic non-residue modulo $p$, then the congruence $x^2 \equiv a \pmod{p}$

A) Has one solution

B) Has two solutions

C) Has no solution

D) Has infinitely many solutions

**10.** The congruence $x^2 \equiv -1 \pmod{5}$ has:

A) No solution

B) One solution

C) Two solutions

D) Four solutions

**True and False:**

**1.** Every quadratic congruence is a polynomial congruence of degree two.

**2.** Every integer is a quadratic residue modulo a prime.

**3.** The congruence $x^2 \equiv 1 \pmod{p}$ has the solutions $x \equiv \pm \pmod{p}$, where $p$ is an odd prime.

**4.** If $a$ is a quadratic residue modulo $p$, then $-a$ must also be a quadratic residue modulo $p$.

**5.** A quadratic congruence modulo a prime may have zero or two incongruent solutions.

**6.** The congruence $x^2 \equiv 2 \pmod{7}$ has a solution.

**Fill in the blanks question:**

**1:** The congruence $x^2 \equiv a \pmod{n}$ is called a ⋯⋯⋯⋯congruence.

**2:** The solution of $x^2 \equiv 1 \pmod{7}$ are ……. and ⋯⋯⋯

**3:** If $a$ is a quadratic non-residue modulo $p$, then the congruence $x^2 \equiv a \pmod{p}$ has so ……. solution (s).

## 10.9 *ANSWERS*

**Answer of long questions:**

**1:** $x \equiv 8, 33 \pmod{41}$ **2:** No solution **3:** $x \equiv 5, 16 \pmod{17}$

**4:** $x \equiv 13, 15 \pmod{19}$ **5:** $x \equiv 8, 13, 22\ 43, 62, 83, 92, 97 \pmod{105}$

**6:** $x \equiv 6, 23 \pmod{29}$ **7:** $x \equiv 5, 14 \pmod{105}$ **8:** $x \equiv 15, 28 \pmod{31}$

**9:** $x \equiv 4, 9, 56, 61 \pmod{65}$ **10:** $x \equiv 11, 132 \pmod{143}$

**Answer of short questions**

**1:** $x \equiv 3, 10, 81, 88 \pmod{91}$ **2:** $x \equiv 25, 27 \pmod{29}$

**3:** $x \equiv 21, 22 \pmod{43}$ **4:** No solution

**5:** $x \equiv 6, 57, 62, 113 \pmod{119}$

**Answer of the objective questions:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | B | **2:** | B | **3:** | B | **4:** | A |
| **5:** | B | **6:** | B | **7:** | C | **8:** | C |
| **9:** | C | **10:** | **C** | | | | |

**Answer of true and false:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1.** | True | **2.** | False | **3.** | True | **4.** | False |
| **5.** | True | **6.** | True | | | | |

**Answer of fill in the blanks:**

| | | | | | |
|---|---|---|---|---|---|
| **1:** | Quadratic | **2:** | 1, 6 | **3.** | No |

# UNIT 11: EULER'S CRITERION AND PERFECT NUMBER

## CONTENTS:



## 11.1 *INTRODUCTION*

The unit "Euler's Criterion" introduces important concepts in elementary number theory that highlight the deep relationships between divisibility, quadratic residues, and special classes

of integers. Euler's Criterion provides an efficient method for determining whether an integer is a quadratic residue modulo an odd prime by using modular exponentiation, thereby connecting the ideas of powers and congruences. It serves as a fundamental tool in the study of quadratic congruences and forms the basis for more advanced results such as the Legendre symbol and the Law of Quadratic Reciprocity. This unit also explores Perfect Numbers**,** which are positive integers equal to the sum of their proper divisors. Beginning with the ancient examples 6 and 28, the discussion extends to Euclid's theorem and Euler's characterization of even perfect numbers, revealing a remarkable connection between perfect numbers and Mersenne primes. Together, these topics demonstrate the elegance and richness of number theory, combining algebraic techniques with fascinating numerical patterns and historical discoveries.

## 11.2 *OBJECTIVE*

After studying this chapter, students will be able to:

**1.** Understand Euler's Criterion and explain its significance in determining quadratic residues modulo an odd prime.

**2.** Apply Euler's Criterion to test whether a given integer is a quadratic residue or a quadratic non-residue modulo a prime number.

**3.** Solve numerical problems involving quadratic residues using modular exponentiation.

**4.** Understand the concept of perfect numbers and identify their fundamental properties.

**5.** Determine whether a given positive integer is a perfect number by evaluating the sum of its proper divisors.

**6.** State and prove Euclid's theorem on the construction of even perfect numbers.

**7.** Explain Euler's characterization of even perfect numbers and its importance in number theory.

**8.** Define Mersenne primes and distinguish them from ordinary prime numbers.

**9.** Explore the relationship between Mersenne primes and even perfect numbers, recognizing that every even perfect number is generated by a Mersenne prime.

**10.** Solve problems involving Mersenne primes and perfect numbers using theorems and computational techniques.

**11.** Develop logical reasoning and proof-writing skills through the study of classical theorems in number theory.

**12.** Appreciate the historical development and modern significance of Euler's Criterion, Perfect Numbers, and Mersenne Primes in mathematics and cryptography.

These objectives provide a comprehensive understanding of the theoretical foundations and practical applications of Euler's Criterion, Perfect Numbers, and Mersenne Primes within elementary number theory.

## 11.3 *QUADRATIC RESIDUE*

If $p$ is a prime and $a$ is an integer coprime to $p$ then $a$ is called a quadratic residue (mod $p$) iff $x^2 \equiv a \pmod{p}$ has a solution otherwise $a$ is called quadratic non-residue (mod $p$).

For example $x^2 = 4 \pmod{5}$ has solutions $2, 3 \pmod{5}$. Therefore 4 is a quadratic residue (mod 5).

## 11.4 *EULER's CRITERION*

**Theorem 1:** If $p$ is an odd prime and $a$ is any integer such that $(a, p) = 1$ then $a$ is a quadratic residue (mod $p$) *iff* $a^{\left(\frac{p-1}{2}\right)} \equiv 1 \pmod{p}$.

**Proof:** We prove both directions.

($\Rightarrow$) If $a$is a quadratic residue modulo $p$, then

$$a^{(p-1)/2} \equiv 1 (\mathrm{mod} p).$$

Since $a$is a quadratic residue modulo $p$, there exists an integer $x$such that

$$x^2 \equiv a (\mathrm{mod} p).$$

Raise both sides to the power $(p-1)/2$:

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} = x^{p-1} (\mathrm{mod} p).$$

Since $\gcd(x,p)=1$, by Fermat's Little Theorem

$$x^{p-1} \equiv 1(\mathrm{mod} p).$$

Therefore,

$$a^{(p-1)/2} \equiv 1(\mathrm{mod} p).$$

Hence proved.

($\Leftarrow$) If

$$a^{(p-1)/2} \equiv 1(\mathrm{mod} p),$$

then $a$is a quadratic residue modulo $p$.

Let $G=(\mathbb{Z}/p\mathbb{Z})^{\times}$, be the multiplicative group modulo $p$. Since $p$is prime, $G$is cyclic of order $p-1$. Let $g$be a primitive root modulo $p$. Every non-zero residue modulo $p$can be written as

$$a \equiv g^{k} (\mathrm{mod} p)$$

for some integer $k$.

Now

$$a^{(p-1)/2} \equiv (g^{k})^{(p-1)/2} = g^{k(p-1)/2} (\mathrm{mod} p).$$

Given

$$a^{(p-1)/2} \equiv 1(\mathrm{mod} p),$$

we obtain

$$g^{k(p-1)/2} \equiv 1(\mathrm{mod} p).$$

Since $g$has order $p-1$,

$$p-1 \mid k\frac{(p-1)}{2}.$$

Dividing by $(p-1)/2$,

$$2 \mid k.$$

Hence

$$k = 2m$$

for some integer $m$.

Therefore

$$a \equiv g^{2m} = (g^m)^2 (\mathrm{mod} p).$$

Thus $a$is the square of $g^m$modulo $p$.

Hence $a$is a quadratic residue modulo $p$.

This proves the converse.

Combining both directions,

$$a \text{ is a quadratic residue mod p } \Leftrightarrow \text{ a}^{(\mathrm{p}-1)/2} \equiv 1(\mathrm{mod p}).$$

Therefore, Euler's Criterion is proved.

**Example 1:** Take $p = 11$and $a = 3$.

$$3^{(11-1)/2} = 3^5 = 243 \equiv 1(\mathrm{mod} 11).$$

Therefore 3 is a quadratic residue modulo 11.

Indeed,

$$5^2 = 25 \equiv 3(\mathrm{mod} 11).$$

Hence the theorem is verified.

**Corollary 1:** If $r$ is a primitive root (mod $p$) then $r^k$ is a quadratic residue (mod $p$) iff $k$ is even.

**Proof:** Since $r$is a primitive root modulo $p$, every non-zero residue modulo $p$can be expressed as a power of $r$. By Euler's Criterion, $a$ is a quadratic residue mod $p \Leftrightarrow a^{(p-1)/2} \equiv 1(\mathrm{mod} p)$. Take, $a = r^k$, then,

$$\left(r^k\right)^{(p-1)/2} = r^{k(p-1)/2}.$$

Since $r$is a primitive root modulo $p$, its order is $p-1$. Therefore,

$$r^{(p-1)/2} \equiv -1(\mathrm{mod}p).$$

Hence

$$r^{k(p-1)/2} = \left(r^{(p-1)/2}\right)^k \equiv (-1)^k(\mathrm{mod}p).$$

**Case 1:** $k$is even, say $k = 2m$.

Then

$$(-1)^k = (-1)^{2m} = 1.$$

Therefore,

$$(r^k)^{(p-1)/2} \equiv 1(\mathrm{mod}p).$$

By Euler's Criterion, $r^k$ is a quadratic residue modulo $p$.

**Case 2:** $k$is odd, say $k = 2m+1$.

Then, $(-1)^k = (-1)^{2m+1} = -1$.

Therefore, $(r^k)^{(p-1)/2} \equiv -1(\mathrm{mod}p)$.

Again, by Euler's Criterion, $r^k$, is not a quadratic residue modulo $p$.

**Theorem 2:** Let $p$be an odd prime and let $a$be an integer such that $\gcd(a,p) = 1$. Then $a^{(p-1)/2} \equiv 1(\mathrm{mod}p)$

or

$$a^{(p-1)/2} \equiv -1(\mathrm{mod}p).$$

**Proof:** Since $\gcd(a,p) = 1$, by Fermat's Little Theorem

$$a^{p-1} \equiv 1(\mathrm{mod}p).$$

Observe that

$$a^{p-1} = \left(a^{(p-1)/2}\right)^2.$$

Hence

$$\left(a^{(p-1)/2}\right)^2 \equiv 1(\mathrm{mod}p).$$

Therefore,

$$\left(a^{(p-1)/2}\right)^2 - 1 \equiv 0(\mathrm{mod}p).$$

Factorizing,

$$\left(a^{(p-1)/2}-1\right)\left(a^{(p-1)/2}+1\right) \equiv 0(\mathrm{mod}p).$$

Since $p$is prime, by Euclid's Lemma,

$$p \mid \left(a^{(p-1)/2}-1\right)\left(a^{(p-1)/2}+1\right)$$

implies that either

$$p \mid a^{(p-1)/2} - 1$$

or

$$p \mid a^{(p-1)/2} + 1.$$

Consequently,

$$a^{(p-1)/2} \equiv 1(\mathrm{mod}p)$$

or

$$a^{(p-1)/2} \equiv -1(\mathrm{mod}p).$$

This proves the theorem.

$$\boxed{a^{(p-1)/2} \equiv \pm 1(\mathrm{mod}p)}$$

**Example 2:** Find the quadratic residue and non-quadratic of 13.

**Answer: Step 1:** Compute $x^2(\mathrm{mod}13)$

$$\begin{aligned} 1^2 &\equiv 1(\text{mod}13) \\ 2^2 &\equiv 4(\text{mod}13) \\ 3^2 &\equiv 9(\text{mod}13) \\ 4^2 &\equiv 16 \equiv 3(\text{mod}13) \\ 5^2 &\equiv 25 \equiv 12(\text{mod}13) \\ 6^2 &\equiv 36 \equiv 10(\text{mod}13) \end{aligned}$$

The remaining squares repeat:

$$7^2 \equiv 6^2, 8^2 \equiv 5^2, 9^2 \equiv 4^2, 10^2 \equiv 3^2, 11^2 \equiv 2^2, 12^2 \equiv 1^2.$$

**Step 2:** Collect the distinct quadratic residues

$$\boxed{\{1, 3, 4, 9, 10, 12\}}$$

These are the quadratic residues modulo 13.

**Step 3:** Find the quadratic non-residues

The non-zero residues modulo 13 are

$$\{1,2,3,4,5,6,7,8,9,10,11,12\}.$$

Removing the quadratic residues gives

$$\boxed{\{2, 5, 6, 7, 8, 11\}}$$

These are the quadratic non-residues modulo 13.

**Example 3:** Show that 3 is a quadratic residue of 23, but a non-residue of 31.

**Answer:** We will use Euler's Criterion:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(\text{mod}p).$$

For an odd prime $p$:

$$a^{(p-1)/2} \equiv \begin{cases} 1(\text{mod}p), & \text{if } a \text{ is a quadratic residue,} \\ -1(\text{mod}p), & \text{if } a \text{ is a quadratic non-residue.} \end{cases}$$

**Part I:** Show that 3 is a Quadratic Residue of 23

Here $a = 3$and $p = 23$.

Compute

$$3^{(23-1)/2} = 3^{11}(\text{mod}23).$$

Using repeated squaring:

$$3^2 = 93^4 = 9^2 = 81 \equiv 12(\text{mod}23)3^8 = 12^2 = 144 \equiv 6(\text{mod}23)$$

Therefore, $3^{11} = 3^8 \cdot 3^2 \cdot 3 \equiv 6 \cdot 9 \cdot 3 = 162162 \equiv 1(\text{mod}23)$ (since $162 = 23 \times 7 + 1$).

Thus

$$3^{11} \equiv 1(\text{mod}23).$$

By Euler's Criterion,

$$\boxed{\text{3 is a quadratic residue modulo 23.}}$$

Verification

Indeed,

$$7^2 = 49 \equiv 3(\text{mod}23).$$

Hence $x = 7$is a solution of

$$x^2 \equiv 3(\text{mod}23).$$

**Part II:** Show that 3 is a Quadratic Non-Residue of 31

Now $a = 3$and $p = 31$.

Compute

$$3^{(31-1)/2} = 3^{15}(\text{mod}31).$$

Using repeated squaring:

$$3^2 = 93^4 = 81 \equiv 19(\text{mod}31)3^8 = 19^2 = 361 \equiv 20(\text{mod}31)$$

Hence

$$3^{15} = 3^8 \cdot 3^4 \cdot 3^2 \cdot 3 \equiv 20 \cdot 19 \cdot 9 \cdot 3(\text{mod}31).$$

Compute step by step:

$$20 \cdot 19 = 380 \equiv 8(\text{mod}31)8 \cdot 9 = 72 \equiv 10(\text{mod}31)10 \cdot 3 = 30 \equiv -1(\text{mod}31).$$

Therefore,

$$3^{15} \equiv -1(\text{mod}31).$$

By Euler's Criterion,

$$\boxed{3 \text{ is a quadratic non-residue modulo } 31.}$$

**Final Conclusion**

$$3^{11} \equiv 1(\text{mod}23)$$

therefore

$$\boxed{3 \text{ is a quadratic residue modulo } 23.}$$

and

$$3^{15} \equiv -1(\text{mod}31)$$

therefore

$$\boxed{3 \text{ is a quadratic non-residue modulo } 31.}$$

Hence proved.

**Example 4:** Find all the quadratic residue of 23.

**Answer:** To find all quadratic residues modulo 23, compute $x^2(\text{mod}23)$ for $x = 1,2, \ldots, \frac{23-1}{2} = 11$.

(After 11, the squares repeat because $(23 - \text{x})^2 \equiv \text{x}^2(\text{mod}23)$.)

Now compute the computation table

| x | $x^2$ | $x^2 (\mathrm{mod} 23)$ |
|---|---|---|
| 1 | 1 | 1 |
| 2 | 4 | 4 |
| 3 | 9 | 9 |
| 4 | 16 | 16 |
| 5 | 25 | 2 |
| 6 | 36 | 13 |
| 7 | 49 | 3 |
| 8 | 64 | 18 |
| 9 | 81 | 12 |
| 10 | 100 | 8 |
| 11 | 121 | 6 |

Collecting the distinct residues:

$$\boxed{\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}}$$

Therefore

The quadratic residues modulo 23 are

$$\boxed{1,2,3,4,6,8,9,12,13,16,18}.$$

Since there are $(23-1)/2 = 11$ quadratic residues, the remaining non-zero residues are the quadratic non-residues:

$$\boxed{5,7,10,11,14,15,17,19,20,21,22}.$$

Verification

Since

$$7^2 = 49 \equiv 3 (\mathrm{mod} 23),$$

we see that 3belongs to the list of quadratic residues modulo 23, confirming the previous result.

| $QR(23) = \{1,2,3,4,6,8,9,12,13,16,18\}$ | $QNR(23) = \{5,7,10,11,14,15,17,19,20,21,22\}$ |
|---|---|

## 11.5 *PERFECT NUMBER*

A perfect number is a positive integer that is equal to the sum of all its proper positive divisors (excluding the number itself). Perfect numbers have fascinated mathematicians since ancient Greek times and are closely related to Mersenne primes through Euclid's and Euler's theorems.

**Definition (Perfect Number):** A positive integer $n$is called a perfect number if the sum of all its proper positive divisors is equal to the number itself. Equivalently, $\sigma(n) = 2n$, where $\sigma(n)$ denotes the sum of all positive divisors of $n$.

**Example 5:** We will prove that 6, 28 are perfect number.

- Proper divisors of 6 are: 1,2,3
- Sum of divisors of 6 are:

$$1 + 2 + 3 = 6.$$

Hence, 6is a perfect number.

Similarly, Proper divisors of 28: 1,2,4,7,14

$$1 + 2 + 4 + 7 + 14 = 28.$$

Thus, 28 is also a perfect number.

**Note:** The first few perfect numbers are

$$6,\ 28,\ 496,\ 8128,\ 33550336, \ldots$$

**Theorem 3 (Euclid's Theorem on Perfect Numbers):** If $2^p - 1$, is prime, then $N = 2^{p-1}(2^p - 1)$ is a perfect number.

**Proof:** Since, $2^p - 1$, is prime, it is relatively prime to $2^{p-1}$. Using the multiplicative property of the divisor-sum function, $\sigma(ab) = \sigma(a)\sigma(b)$, when $\gcd(a, b) = 1$,

we obtain,

$$\sigma(N) = \sigma(2^{p-1})\sigma(2^p - 1).$$

Now,

$$\sigma(2^{p-1}) = 1 + 2 + 2^2 + \cdots + 2^{p-1} = \frac{2^p - 1}{2 - 1} = 2^p - 1.$$

Since, $2^p - 1$ is prime, $\sigma(2^p - 1) = 1 + (2^p - 1) = 2^p$.

Therefore, $\sigma(N) = (2^p - 1)(2^p)$.

Since, $N = 2^{p-1}(2^p - 1)$,

we have

$$2N = 2^p(2^p - 1).$$

Hence, $\sigma(N) = 2N$.

Therefore, $N$ is a perfect number.

Hence proved.

**Theorem 4(Euler's Converse Theorem):** Every even perfect number is of the form $2^{p-1}(2^p - 1)$, where $2^p - 1$ is a prime number.

**Proof:** Let $N$ be an even perfect number.

Since $N$is even (as given) then, $N = 2^{k-1}m$,

Where $m$is odd and $\gcd(2, m) = 1$.

Since $N$is perfect so, $\sigma(N) = 2N$.

Using multiplicativity,

$$\sigma(2^{k-1})\sigma(m) = 2^k m.$$

But

$$\sigma(2^{k-1}) = 2^k - 1.$$

Hence,

$$(2^k - 1)\sigma(m) = 2^k m.$$

Since

$$\gcd(2^k, 2^k - 1) = 1,$$

it follows that $2^k - 1$ divides $m$.

Write

$$m = (2^k - 1)t.$$

Substituting,

$$\sigma(m) = 2^k t.$$

Since

$$\sigma(m) \geq m + t,$$

we obtain

$$2^k t \geq (2^k - 1)t + t = 2^k t.$$

Equality holds only when $m$ has exactly two positive divisors.

Thus, $m = 2^k - 1$ must be prime.

Hence, $N = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is prime.

Therefore, every even perfect number has the required form. Hence proved.

**Theorem 5 (Euclid–Euler Theorem):** A positive even integer is perfect if and only if

$N = 2^{p-1}(2^p - 1)$,where $2^p - 1$ is prime.

**Proof:** The forward implication follows from Euler's theorem, and the reverse implication follows from Euclid's theorem. Hence, $N$ is an even perfect number if and only if $N = 2^{p-1}(2^p - 1)$, with $2^p - 1$ prime. Hence proved.

**Corollary 1:** If $2^p - 1$ is a Mersenne prime, then $2^{p-1}(2^p - 1)$is an even perfect number.

**Note:** Table of the First Few Perfect Numbers

| $p$ | $2^p - 1$ | **Perfect Number** |
|---|---|---|
| 2 | 3 | 6 |
| 3 | 7 | 28 |
| 5 | 31 | 496 |
| 7 | 127 | 8128 |
| 13 | 8191 | 33,550,336 |
| 17 | 131071 | 8,589,869,056 |

**Note:** Important Properties of Perfect Numbers

**1.** Every known perfect number is even.

**2.** Every even perfect number is generated by a Mersenne prime.

**3.** No odd perfect number has ever been discovered.

**4.** It is still an open problem whether an odd perfect number exists.

**5.** If $N$is perfect, then $\sigma(N) = 2N$.

**6.** Every even perfect number ends alternately in the digits **6** and **28** (for numbers greater than 28, the last digit alternates between 6 and 8 in a predictable pattern).

**Note:** Some important properties

**1.** A perfect number equals the sum of its proper divisors.

**2.** The divisor-sum characterization is $\sigma(n) = 2n$.

**3.** Euclid's theorem constructs perfect numbers from Mersenne primes.

**4.** Euler's theorem proves that every even perfect number arises in this way.

**5.** Together, these results form the Euclid–Euler theorem, which completely characterizes all even perfect numbers.

## 11.6 *MERSENNE PRIME NUMBERS*

One of the most fascinating classes of prime numbers in number theory is the Mersenne prime. These primes were studied extensively by the French mathematician Marin Mersenne, who investigated numbers of the form $2^p - 1$. Today these numbers are fundamental in Number Theory, Cryptography, Computer Science, Perfect Numbers, Random Number Generation

The search for large Mersenne primes continues today through the Great Internet Mersenne Prime Search (GIMPS).

**Definition:** A Mersenne Number is a number of the form $M_n = 2^n - 1$, where $n \geq 1$.

**Examples 6:** List of some Mersenne number.

| $n$ | $M_n = 2^n - 1$ |
|---|---|
| 1 | 1 |

| $n$ | $M_n = 2^n - 1$ |
|---|---|
| 2 | 3 |
| 3 | 7 |
| 4 | 15 |
| 5 | 31 |
| 6 | 63 |
| 7 | 127 |

Not every Mersenne number is prime.

**Definition (Mersenne Prime):** A Mersenne Prime is a Mersenne number that is itself prime. Thus, $M_p = 2^p - 1$ is called a Mersenne prime if

**1.** $p$is prime, and

**2.** $2^p - 1$is prime.

**Examples 7:** Prove that these are $3, 7, 31, 127, 8191, \ldots$ Mersenne prime.

**Solution 1:** $2^2 - 1 = 3$, which is a prime number. Hence 3 is a Mersenne prime.

**2:** $2^3 - 1 = 7$, which is a prime number. Hence 7 is a Mersenne prime.

**3:** $2^5 - 1 = 31$, which is a prime number. Hence 31 is a Mersenne prime.

**4:** $2^7 - 1 = 127$, which is a prime number. Hence 127 is a Mersenne prime.

**5:** $2^{11} - 1 = 2047$. Now $2047 = 23 \times 89$. Therefore, 2047 is **not** prime. Hence it is **not** a Mersenne prime.

**Basic Properties of Mersenne prime:**

**Property 1:** Every Mersenne prime has the form $2^p - 1$.

**Property 2:** The exponent must be prime.

**Property 3:** Not every prime exponent gives a Mersenne prime.

For example, $2^{11} - 1 = 2047$ is composite.

**Property 4:** Every even perfect number is generated by a Mersenne prime.

**Theorem 6 (Necessary Condition):** If $2^n - 1$ is prime, then $n$ must be prime.

**Proof:** Suppose $n$ is composite. Then $n = ab$, where $a > 1, b > 1$.

Hence, $2^n - 1 = 2^{ab} - 1$.

Using the algebraic identity, $x^{ab} - 1 = (x^a - 1)\left(x^{a(b-1)} + \cdots + x^a + 1\right)$,
put $x = 2$.
Then, $2^{ab} - 1 = (2^a - 1)\left(2^{a(b-1)} + \cdots + 2^a + 1\right)$. Both factors exceed 1.

Therefore, $2^n - 1$ is composite.

This contradicts the assumption that $2^n - 1$ is prime.

Hence, $n$ must be prime.

Therefore proved.

$$\boxed{\text{If } 2^n - 1 \text{ is prime, then } n \text{ is prime.}}$$

**Example 8:** The converse of the previous theorem (Theorem 6) is not true.

**Proof:** Take, $p = 11$. Then 11 is prime. But

$$2^{11} - 1 = 2047 = 23 \times 89.$$

Hence, $2^{11} - 1$ is not prime.

Therefore, prime exponent does not always produce a Mersenne prime.

**Theorem 7 (Euclid's Theorem):** If, $2^p - 1$ is a Mersenne prime, then $2^{p-1}(2^p - 1)$ is a perfect number.

**Proof:** Let $N = 2^{p-1}(2^p - 1)$. Since $2^{p-1}$ and $2^p - 1$ are relatively prime,

$$\sigma(N) = \sigma(2^{p-1})\sigma(2^p - 1).$$

Now,

$$\sigma(2^{p-1}) = 1 + 2 + \cdots + 2^{p-1} = 2^p - 1.$$

Since $2^p - 1$ is prime, $\sigma(2^p - 1) = 2^p$.

Hence, $\sigma(N) = (2^p - 1)2^p = 2N$.

Thus, $N$ is perfect.

**Note:** First Few Mersenne Primes

| **Prime Exponent** $p$ | **Mersenne Prime** $2^p - 1$ |
|---|---|
| 2 | 3 |
| 3 | 7 |
| 5 | 31 |
| 7 | 127 |
| 13 | 8191 |
| 17 | 131071 |
| 19 | 524287 |
| 31 | 2147483647 |

**Some Applications of Mersenne Primes**

**1.** Generation of even perfect numbers.

**2.** Cryptography and public-key systems.

**3.** Random number generators (e.g., Mersenne Twister algorithm).

**4.** Testing algorithms for primality.

**5.** Computational number theory and distributed computing projects.

**Some important results**

**1.** Every Mersenne prime has the form $2^p - 1$.

**2.** If $2^n - 1$ is prime, then $n$must be prime. The converse is false.

**3.** Every Mersenne prime produces an even perfect number.

**4.** Every even perfect number comes from a Mersenne prime.

## Check your progress

**Problem 1:** Determine whether **5** is a quadratic residue modulo **19**

**Answer:** 5 is a quadratic residue modulo 19

**Problem 2:** Determine whether $x^2 \equiv 6 \pmod{29}$ is solvable.

**Answer:** $x \equiv 8, 21 \pmod{29}$

## 11.7 *SUMMARY*

This unit "Euler's Criterion and Perfect Numbers" introduces important concepts in elementary number theory that connect quadratic residues with special classes of integers. Euler's Criterion provides a simple and powerful method for determining whether an integer is a quadratic residue modulo an odd prime. It states that for an odd prime ($p$) and an integer ($a$) with (gcd(a, p)=1), (a) is a quadratic residue modulo (p) if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$; otherwise, $a^{(p-1)/2} \equiv -1 \pmod{p}$). This criterion simplifies the testing of quadratic residues and forms the basis for many results in modular arithmetic and the theory of quadratic reciprocity.

The unit also discusses perfect numbers, which are positive integers equal to the sum of their proper divisors. The study of perfect numbers dates back to ancient mathematics and remains an active area of research. A fundamental result, known as the Euclid–Euler Theorem, establishes

that every even perfect number is of the form $2^{(p-1)}(2^p-1)$ where $(2^p-1)$ is a prime number. Such primes are called Mersenne primes, named after the French mathematician Marin Mersenne. This unit also explains the close relationship between Mersenne primes and even perfect numbers, showing that every even perfect number arises from a Mersenne prime and, conversely, every Mersenne prime generates an even perfect number. Learners learn how to identify Mersenne primes, construct perfect numbers, verify whether a given number is perfect, and apply Euler's Criterion to determine quadratic residues. Overall, the chapter highlights the elegance and interconnectedness of these classical concepts, illustrating their significance in number theory and their applications in modern mathematics and cryptography

## 11.8 *GLOSSARY*

- Quadratic residue
- Euler's criterion
- Perfect number
- Mersenne prime number

## 11.9 *REFERENCES*


- **Burton, D. M.** (2007). *Elementary number theory* (6th ed.). McGraw-Hill.
- **T. M. Apostol**, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford.
- **Tom M. Apostol**, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York.
- **G. A. Jones and J. M. Jones**, *Elementary Number Theory*, Springer-Verlag, Berlin, 1998.
- **T. Nagell**, *Introduction to Number Theory*, Wiley, New York.

## 11.10 *SUGGESTED READING*


- **Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery**, *An Introduction to the Theory of Numbers*, John Wiley & Sons.
- **Hugh L. Montgomery and Robert C. Vaughan**, *Multiplicative Number Theory I: Classical Theory*, Cambridge University Press.
- **H. Iwaniec and E. Kowalski**, *Analytic Number Theory*, American Mathematical Society, 2004.
- **T. Koshy**, *Elementary Number Theory with Applications*, Academic Press.
- **Eric W. Weisstein**, "Möbius Inversion Formula," *MathWorld – Wolfram Resource*.


## 11.11 *TE1RMINAL QUESTION*

**1.** Explain and derive the Euler's criterion?

**2.** Explain the perfect number.

**3.** Explain the Mersenne prime.

**4.** Prove that if $p$ is an odd prime and $a$ is any integer such that $(a, p) = 1$ then $a$ is a quadratic residue $(\text{mod } p)$ *iff* $a^{\left(\frac{p-1}{2}\right)} \equiv 1 (\text{mod } p)$.

**Objective type questions:**

**1. Euler's criterion states that for an odd prime *p* and an integer *a* with** $\gcd(a, p) = 1$

**A)** $a^{p-1} \equiv 0 (\text{mod } p)$

**B)** $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) (\text{mod } p)$

**C)** $a^{p} \equiv a + 1 (\text{mod } p)$

**D)** $a^{\frac{p+1}{2}} \equiv 1 (\text{mod } p)$

**2. Euler's Criterion is applicable only when**

**A)** $p$ is any positive integer

**B)** $p$ is an even prime

**C)** $p$ is an odd prime

**D)** $p$ is a composite number

**3. If *a* is quadratic residue modulo an odd prime *p*, then**

**A)** $a^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$

**B)** $a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$

**C)** $a^{p-1} \equiv -1 (\text{mod } p)$

**D)** None of these

**4. If *a* is a quadratic non-residue modulo an odd prime *p*, then**

**A)** $a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$

**B)** $a^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$

**C)** $a^{p-1} \equiv 0 (\text{mod } p)$

**D)** $a \equiv 1 (\text{mod } p)$

**5. Euler's criterion is mainly used to determine**

**A)** Primitive roots

**B)** Quadratic residues modulo a prime

**C)** Prime factorization

**D)** Greatest common divisor

**6. For** $p = 7, 2^3 \equiv$

**A)** 1 (mod 7)

**B)** 2 (mod 7)

**C)** -1 (mod 7)

**D)** 0 (mod 7)

**7. According to Euler's criterion, if $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, then *a* is**

**A)** A primitive root

**B)** A quadratic residue

**C)** A quadratic non-residue

**D)** A multiple of $p$

**8. For an odd prime *p*, Euler's criterion requires**

**A)** $a \equiv 0 \pmod{p}$

**B)** $\gcd(a, p) = 1$

**C)** $a > p$

**D)** $a$ must be even

**9: Which theorem is closely related to Euler's Criterion?**

**A)** Wilson's Theorem

**B)** Fermat's Little Theorem

**C)** Chinese Remainder Theorem

**D)** Euclidean Algorithm

**10: If *p*=11, then the exponent used in Euler's Criterion is**

**A)** 4

**B)** 5

**C)** 6

**D)** 10

**11:** **If** $3^5 \equiv 1 (\mathrm{mod}\, 11)$**, then 3 is**

**A)** a quadratic residue modulo 11

**B)** a quadratic non-residue modulo 11

**C)** a primitive root

**D)** divisible by 11

**12:** **If** $2^5 \equiv -1 (\mathrm{mod}\, 11)$**, then 2 is**

**A)** a quadratic residue modulo 11

**B)** a quadratic non-residue modulo 11

**C)** a multiple of 11

**D)** a prime number

**True (T) and False (F) question:**

**1:** Euler's Criterion applies to every composite modulus.

**2:** If $a$ is a quadratic residue modulo an odd prime $p$, then $a^{(p-1)/2} \equiv 1 (\mathrm{mod}\, p)$

**3:** A perfect number is equal to the sum of its proper positive divisors.

**4:** The smallest perfect number is 6.

**5:** Every perfect number is odd.

**6:** The number 28 is a perfect number.

**7:** The proper divisors of 28 are 1, 2, 4, 7, and 14.

**8:** The sum of the proper divisors of 496 is 496.

**9:** Every prime number is a perfect number.

**10:** The number 12 is a perfect number.

**11:** All known perfect numbers are even.

**12:** It is known that at least one odd perfect number exists.

**13:** Every even perfect number has the form $2^{(p-1)}(2^p - 1)$, where $(2^p - 1)$ is prime.

**14:** The number 8128 is a perfect number.

**15:** Every multiple of a perfect number is also perfect.

**16:** The sum of all positive divisors of a perfect number equals twice the number.

**17:** Every even perfect number ends with the digit 6 or 8.

**18:** Every Mersenne number is prime.

**19:** $2^3 - 1 = 7$ is a Mersenne prime.

**20:** $2^{11} - 1 = 2047$ is a Mersenne prime.

**21:** The smallest Mersenne prime is 3.

**Fill in the blanks question:**

**1:** Euler's Criterion is valid for an _____ prime number.

**2:** Euler's Criterion is mainly used to determine _____ residues modulo an odd prime.

**3:** The condition required for Euler's Criterion is $\gcd(a, p) =$ _____.

**4:** Euler's Criterion is closely related to _____ Little Theorem.

**5:** For an odd prime $p = 13$, the exponent in Euler's Criterion is _____.

**6:** A perfect number is equal to the sum of its _____ divisors.

**7:** The smallest perfect number is _____.

**8:** The second perfect number is _____.

**9:** The third perfect number is _____.

**10:** The fourth perfect number is _____.

**11:** Euler proved that every _____ perfect number is of Euclid's form.

**12:** No _____ perfect number has yet been discovered.

**13:** Euler's Criterion connects powers modulo an odd prime with the _____ symbol.

**14:** The perfect number generated by the Mersenne prime 7 is _____.

**15:** The perfect number generated by the Mersenne prime 31 is _____.

**16:** The Euclid–Euler theorem establishes a relationship between _____ primes and even perfect numbers.

## 11.12 *ANSWERS*

**Answer of the objective questions:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | B | **2:** | C | **3:** | B | **4:** | B |
| **5:** | B | **6:** | A | **7:** | C | **8:** | B |
| **9:** | B | **10:** | B | **11:** | A | **12:** | B |

**Answer of True (T) and False (F):**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | F | **2:** | T | **3:** | T | **4:** | T |
| **5:** | F | **6:** | T | **7:** | T | **8:** | T |
| **9:** | F | **10:** | F | **11:** | T | **12:** | F |
| **13:** | T | **14:** | T | **15:** | F | **16:** | T |
| **17:** | T | **18:** | F | **19:** | T | **20:** | F |
| **21:** | T | | | | | | |

**Answer of fill in the blanks questions:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | odd | **2:** | quadratic | **3:** | 1 | **4:** | Fermat's |
| **5:** | 6 | **6:** | proper | **7:** | 6 | **8:** | 28 |
| **9:** | 496 | **10:** | 8128 | **11:** | even | **12:** | odd |
| **13:** | Legendre | **14:** | 28 | **15:** | 496 | **16:** | Mersenne |

# COURSE NAME: NUMBER THEORY

# COURSE CODE: MAT-606

# BLOCK - IV: QUADRATIC RECIPROCITY LAW AND APPLICATIONS

# UNIT-12: THE LEGENDRE SYMBOL AND ITS PROPERTIES

## CONTENTS:



## 12.1 *INTRODUCTION*

The **Legendre symbol** is one of the most important concepts in elementary number theory. It was introduced by the French mathematician **Adrien-Marie Legendre** in the late 18th century during his investigations of quadratic congruences and quadratic residues. Thus, the Legendre symbol serves as a fundamental tool for determining the solvability of quadratic equations modulo prime numbers and forms the foundation of many advanced topics in number theory.

The **Legendre symbol** is a fundamental concept in number theory that provides a convenient way to determine whether an integer is a quadratic residue modulo an odd prime number. Introduced by the French mathematician **Adrien-Marie Legendre** in the eighteenth century, it is denoted by $\left(\frac{a}{p}\right)$, where $a$is an integer and $p$is an odd prime. The symbol takes the value $1$ if $a$ is a quadratic residue modulo $p$, $-1$ if $a$is a quadratic non-residue modulo $p$, and $0$if $p$divides $a$. The Legendre symbol simplifies the study of quadratic congruences and is closely connected with important results such as Euler's Criterion and the Law of Quadratic Reciprocity. Because of its efficiency in determining the solvability of quadratic equations modulo primes, it has become an essential tool in elementary and advanced number theory, finite field theory, and modern cryptography. Its introduction marked a significant step in the systematic development of number theory and continues to influence contemporary mathematical research.

## 12.2 *OBJECTIVE*

After reading this unit you will be able to:
(i) Legendre symbol
(ii) Gauss's Lemma

## 12.3 *LEGENDRE SYMBOL AND ITS PROPERTIES*

**Definition:** Let $p$ be an odd prime and let $a$ be an integer. The Legendre symbol is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a, \\ 1, & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1, & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Thus, the Legendre symbol indicates whether the congruence $x^2 \equiv a(\mathrm{mod}\, p)$ has a solution.

**Theorem 12.1:** If $p$ is an odd prime and $a$ and $b$ are any integers coprime to $p$ then the Legendre symbol has the following properties:

**(i)** $a \equiv b(\mathrm{mod} p) \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

**(ii)** $\left(\frac{a^2}{p}\right) = \left(\frac{b}{p}\right)$.

**(iii)** $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

**(iv)** $\left(\frac{1}{p}\right) = 1$ and $\left(-\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

**(v)** $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.

**Proof: (i)** Suppose $a \equiv b(\mathrm{mod}\, p)$

Then $a$ and $b$ belong to the same residue class modulo $p$.

If $x^2 \equiv a(\mathrm{mod}\, p)$, then $x^2 \equiv b(\mathrm{mod}\, p)$.

Hence $a$ is a quadratic residue modulo $p$ if and only if $b$ is a quadratic residue modulo $p$.

Therefore $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

**(ii)** Since $a^2 \equiv (a)^2(\mathrm{mod}\, p)$,

the congruence $x^2 \equiv a^2(\mathrm{mod}\, p)$ has the solution $x \equiv a(\mathrm{mod}\, p)$.

Thus $a^2$ is always a quadratic residue modulo $p$.

Hence $\left(\frac{a^2}{p}\right) = 1$.

**(iii)** Using Euler's Criterion,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} (\mathrm{mod} p),$$

And $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} (\mathrm{mod}\, p)$.

Multiplying, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} (\mathrm{mod}\, p)$.

Therefore $= (ab)^{(p-1)/2} (\mathrm{mod} p)$.

Applying Euler's Criterion again,

$$(ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right) (\mathrm{mod} p).$$

Hence $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

**(iv) first part**

Since $1 \equiv 1^2 (\mathrm{mod} p)$, 1 is a quadratic residue modulo $p$.

Thus $\left(\frac{1}{p}\right) = 1$.

**Second part**

By Euler's Criterion, $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} (\mathrm{mod} p)$.

Since the Legendre symbol can take only the values $\pm 1$,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Equivalently,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 (\mathrm{mod} 4), \\ -1, & p \equiv 3 (\mathrm{mod} 4). \end{cases}$$

$(v)$ Using property (iii),

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right).$$

By property (ii),

$$\left(\frac{b^2}{p}\right) = 1.$$

Therefore $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right) \cdot 1.$

Hence

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right).$$

This completes the proof of all the properties of the Legendre symbol.

**Importance of the Legendre Symbol**

- The Legendre symbol provides a compact and efficient way to study quadratic residues. It is widely used in:
- Quadratic congruences
- Euler's Criterion
- The Law of Quadratic Reciprocity
- Algebraic number theory
- Finite field theory
- Cryptography and information security

**Theorem 12.2:** There are infinitely many primes of the form $4k+1$ where $k$ is an integer.

**Proof:** Assume, for contradiction, that there are only finitely many primes of the form $4k+1$. Let them be $p_1, p_2, \dots, p_n$.

Consider the number $N = (2p_1p_2 \cdots p_n)^2 + 1$.

That is, $N = 4(p_1p_2 \cdots p_n)^2 + 1$.

Clearly, $N \equiv 1(\mathrm{mod}4)$.

Since $N > 1$, it has at least one prime divisor. Let $q$ be a prime divisor of $N$. Then $q \mid N$ and hence $(2p_1p_2 \cdots p_n)^2 \equiv -1(\mathrm{mod}q)$.

Thus $-1$is a quadratic residue modulo $q$.

By a standard result in number theory,

$-1$ is a quadratic residue mod $q \iff q \equiv 1(\mathrm{mod}4)$.

Therefore, $q = 4m + 1$

for some integer $m$. Hence $q$is a prime of the form $4k+1$.

Now, $q$cannot be any of the primes $p_1, p_2, \dots, p_n$. Indeed, if $q = p_i$for some $i$, then $p_i$divides $(2p_1p_2 \cdots p_n)^2$, and since $p_i \mid N$,

$p_i \mid (N - (2p_1p_2 \cdots p_n)^2) = 1$, which is impossible.

Thus $q$ is a prime of the form $4k+1$ not contained in our original list $p_1, p_2, \dots, p_n$.

This contradicts the assumption that $p_1, p_2, \dots, p_n$were all the primes of the form $4k+1$.

Therefore, our assumption is false.

Hence there are infinitely many primes of the form $4k+1$.

**Theorem 12.3: (Gauss Lemma):** If $p$ is an odd integer, $a$ is an integer such that $(a,p) = 1$ and $n$ is number of integers in the set

$$\left\{a, 2a, \dots, \left(\frac{p-1}{2}\right)a\right\} \qquad \dots\dots..(1)$$

Then $\left(\frac{a}{p}\right) = (-1)^n$. where $\left(\frac{a}{p}\right)$ is the Legendre symbol.

**Proof:** Let

$$\mathrm{r}_1, \mathrm{r}_2, \dots, \mathrm{r}_{\frac{\mathrm{p}-1}{2}}$$

be the least absolute residues of

$$\mathrm{a}, 2\mathrm{a}, \dots, \frac{\mathrm{p}-1}{2}\mathrm{a}(\mathrm{mod p}).$$

Thus each $\mathrm{r_i}$ satisfies

$$-\frac{\mathrm{p}}{2} < \mathrm{r_i} < \frac{\mathrm{p}}{2},$$

and $r_i \equiv ia(\mathrm{mod}p)$.

Suppose exactly $n$of the residues are negative. Then

$$r_1 r_2 \cdots r_{\frac{p-1}{2}} = (-1)^n \mid r_1 r_2 \cdots r_{\frac{p-1}{2}} \mid.$$

The absolute values $\mid r_1 \mid, \mid r_2 \mid, \dots, \mid r_{\frac{p-1}{2}} \mid$

are precisely the integers $1, 2, \dots, \frac{p-1}{2}$ in some order. Therefore,

$$\mid r_1 r_2 \cdots r_{\frac{p-1}{2}} \mid = \left(\frac{p-1}{2}\right)!.$$

Hence $$r_1 r_2 \cdots r_{\frac{p-1}{2}} = (-1)^n \left(\frac{p-1}{2}\right)!. \qquad \dots\dots(1)$$

On the other hand, since $r_i \equiv ia(\mathrm{mod}\, p)$,

$$r_1 r_2 \cdots r_{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! (\mathrm{mod}p). \qquad \dots\dots(2)$$

Comparing (1) and (2),

$$(-1)^n \left(\frac{p-1}{2}\right)! \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! (\mathrm{mod}p).$$

Since $p \nmid \left(\frac{p-1}{2}\right)!$, we may cancel the factorial to obtain

$$(-1)^n \equiv a^{\frac{p-1}{2}} (\mathrm{mod}p).$$

By Euler's Criterion,

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\mathrm{mod} p).$$

Since both sides are equal to $\pm 1$, it follows that

$$\boxed{\left(\frac{a}{p}\right) = (-1)^n}.$$

Thus, Gauss's Lemma is proved.

**Theorem 12.4:** If $p$ is an odd prime then

$$\left(\frac{a}{p}\right) = \begin{cases} 1, if\ p = 1(mod\ 8)\ or\ \ p \equiv 7(mod\ 8) \\ -1, if\ p = 3(mod\ \ 8)\ or\ \ p \equiv 5(mod\ 8) \end{cases}$$

Hence $\frac{a}{p} = (-1)^{\frac{p^2-1}{8}}$.

**Solution:** Consider the numbers

$$2,4,6, \dots, (p-1).$$

Let $n$ be the number of these integers whose least positive residues modulo $p$ are greater than $p/2$.

By **Gauss's Lemma**,

$$\left(\frac{2}{p}\right) = (-1)^n.$$

Now count such residues.

For $2k(1 \leq k \leq \frac{p-1}{2})$, we have $2k > \frac{p}{2}$ precisely when

$$k > \frac{p}{4}.$$

Hence

$$n = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor.$$

We evaluate $n$according to the residue class of $p$modulo 8.

**Case 1: $p = 8m + 1$**

$$n = 4m - \lfloor 2m + \frac{1}{4} \rfloor = 4m - 2m = 2m,$$

which is even. Therefore

$$\left(\frac{2}{p}\right) = 1.$$

**Case 2: $p = 8m + 3$**

$$n = (4m + 1) - \lfloor 2m + \frac{3}{4} \rfloor = 4m + 1 - 2m = 2m + 1,$$

which is odd. Hence

$$\left(\frac{2}{p}\right) = -1.$$

**Case 3: $p = 8m + 5$**

$$n = (4m + 2) - \lfloor 2m + 1 + \frac{1}{4} \rfloor = 4m + 2 - (2m + 1) = 2m + 1,$$

which is odd. Thus

$$\left(\frac{2}{p}\right) = -1.$$

**Case 4: $p = 8m + 7$**

$$n = (4m + 3) - \lfloor 2m + 1 + \frac{3}{4} \rfloor = 4m + 3 - (2m + 1) = 2m + 2,$$

which is even. Therefore

$$\left(\frac{2}{p}\right) = 1.$$

Combining all four cases,

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv 1, 7 (\text{mod } 8), \\ -1, & p \equiv 3, 5 (\text{mod } 8). \end{cases}$$

Since

$$\frac{p^2 - 1}{8}$$

is even when $p \equiv 1, 7 (\text{mod } 8)$and odd when $p \equiv 3, 5 (\text{mod } 8)$, we obtain

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Hence proved.

**Theorem 12.4:** If $p$ and $2p+1$ both are odd primes then $(-1)^{\frac{p-1}{2}}.2$ is primitive root of $2p+1$.

**Proof:** Let

$$q = 2p + 1.$$

Since $q$ is prime, the multiplicative group $\left(\frac{\mathbb{Z}}{q\mathbb{Z}}, \times\right)$ has order

$$q - 1 = 2p.$$

To prove that $g = (-1)^{\frac{p-1}{2}}2$ is a primitive root modulo $q$, it suffices to show that the order of $g$ modulo $q$ is $2p$.

Since the order of an element modulo a prime divides $2p$, the only possible orders are

$$1,\ 2,\ p,\ 2p.$$

Clearly $g \not\equiv 1(\mathrm{mod}q)$and $g \not\equiv -1(\mathrm{mod}q)$, so its order is neither 1 nor 2.

It remains to show that

$$g^p \equiv -1(\mathrm{mod}q).$$

Using Euler's Criterion,

$$g^p \equiv \left(\frac{g}{q}\right)(\mathrm{mod}q).$$

Now

$$\left(\frac{g}{q}\right) = \left(\frac{(-1)^{(p-1)/2}}{q}\right)\left(\frac{2}{q}\right).$$

Since $q = 2p + 1$,

$$q \equiv \begin{cases} 3\ (\mathrm{mod}\ 8), & p \equiv 1(\mathrm{mod}\ 4), \\ 7\ (\mathrm{mod}\ 8), & p \equiv 3(\mathrm{mod}\ 4). \end{cases}$$

By the supplementary laws,

$$\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2} = (-1)^p = -1,$$

and

$$\left(\frac{2}{q}\right) = \begin{cases} -1, & q \equiv 3(\mathrm{mod}8), \\ 1, & q \equiv 7(\mathrm{mod}8). \end{cases}$$

Hence, in either case,

$$\left(\frac{g}{q}\right) = -1.$$

Therefore,

$$g^p \equiv -1(\mathrm{mod} q).$$

Consequently,

$$g^{2p} \equiv 1(\mathrm{mod} q),$$

but

$$g^p \not\equiv 1(\mathrm{mod} q).$$

Thus, the order of $g$ does not divide $p$. Since the only remaining divisor of $2p$ is $2p$, we obtain

$$\mathrm{ord}_q(g) = 2p.$$

Therefore, $g$is a primitive root modulo $q = 2p + 1$.

$(-1)^{\frac{p-1}{2}} 2$ is a primitive root modulo $2p + 1$.

Hence proved.

**Theorem 12.5:** There are infinitely many primes of the form $8k - 1$.

**Proof:** Suppose, on the contrary, that there are only finitely many primes of the form $8\mathrm{k} - 1$. Let them be

$$\mathrm{p}_1, \mathrm{p}_2, \dots, \mathrm{p}_\mathrm{n}.$$

Consider the integer

$$\mathrm{N} = (2\mathrm{p}_1\mathrm{p}_2 \cdots \mathrm{p}_\mathrm{n})^2 + 1.$$

Clearly,

$$\mathrm{N} > 1.$$

Let q be any prime divisor of N. Then

$$(2\mathrm{p}_1\mathrm{p}_2 \cdots \mathrm{p}_\mathrm{n})^2 \equiv -1(\mathrm{modq}).$$

Hence $-1$ is a quadratic residue modulo q. Therefore,

$$\left(\frac{-1}{\mathrm{q}}\right) = 1.$$

By Euler's criterion,

$$\left(\frac{-1}{\mathrm{q}}\right) = (-1)^{\frac{\mathrm{q}-1}{2}},$$

so

$$(-1)^{\frac{\mathrm{q}-1}{2}} = 1.$$

Thus

$$q \equiv 1(\mathrm{mod}4).$$

Since $q$ is an odd prime and $q \equiv 1(\mathrm{mod}4)$, it follows that

$$q \equiv 1(\mathrm{mod}8) \text{or } q \equiv 7(\mathrm{mod}8).$$

Now $q$ cannot be any of $p_1, p_2, \ldots, p_n$, because if $p_i \mid N$, then

$$N \equiv 1(\mathrm{mod}p_i),$$

which is impossible.

Therefore, every prime divisor $q$ of Nis different from the listed primes.

Also,

$$N = (2p_1p_2 \cdots p_n)^2 + 1 \equiv 1(\mathrm{mod}8).$$

If all prime divisors of $N$ were congruent to $1(\mathrm{mod}8)$, then their product would also be congruent to $1(\mathrm{mod}8)$. Since $N \equiv 1(\mathrm{mod}8)$, at least one prime divisor $q$must satisfy

$$q \equiv 7(\mathrm{mod}8).$$

That is,

$$q = 8m - 1$$

for some integer $m$.

Hence, we have found a prime of the form $8k - 1$that is not among

$$p_1, p_2, \ldots, p_n,$$

contradicting the assumption that these were all such primes.

Therefore, the assumption is false.

There are infinitely many primes of the form $8k - 1$.

Hence proved.

**Question12.1:** Evaluate $\left(\frac{504}{23}\right)$.

**Solution**: We have $\left(\frac{504}{23}\right) = \left(\frac{6^2 \times 14}{23}\right) = \left(\frac{6^2}{23}\right).\left(\frac{14}{23}\right) = \left(\frac{14}{23}\right)$ $[\because (6, 23) = 1]$

$= -1.$ $[\because 14 \text{ is a quadratic non} - \text{residue of } 23]$

**Question12.2:** Evaluate $\left(\frac{168}{11}\right)$.

**Solution**: We have $168 = 2^3.3.7$

$$\left(\frac{168}{11}\right) = \left(\frac{2^3.\ 3.\ 7}{11}\right) = \left(\frac{2}{11}\right)^3.\left(\frac{3}{11}\right).\left(\frac{7}{11}\right)$$

$$= -(1)^3.(1).(-1)$$

[∵ 2 and 7 are quadratic non −
residues of 11 and 3 is a quadratic residue of 11 is a quadratic non −
residue of 23]

$= 1.$

**Question12.3:** Evaluate $\left(\frac{1372}{29}\right)$.

**Solution**: We have $1372 = 7 \times 14^2$

$$\left(\frac{1372}{29}\right) = \left(\frac{4 \times 14^2}{29}\right) = \left(\frac{7}{29}\right)\left(\frac{14}{29}\right)^3$$

$$= \left(\frac{7}{29}\right) \qquad [\because (14, 29) = 1]$$

$$= 1 \qquad [\because 7 \text{ is a quadratic residue of } 29]$$

**Question12.4:** Evaluate $\left(\frac{-23}{59}\right)$.

**Solution**: We have $\left(\frac{-23}{59}\right) = \left(\frac{-1 \times 23}{59}\right) = \left(\frac{-1}{59}\right)\left(\frac{23}{59}\right)$

$$= -1.\left(\frac{23}{59}\right)$$

$$= -\left(\frac{23}{59}\right)$$

$$= -1 \qquad [\because 23 \text{ is a quadratic residue of } 59].$$

**Question12.5:** Evaluate $n$ of gauss Lemma for $\left(\frac{5}{19}\right)$.

**Solution**: Here using **Gauss's Lemma**, let

$$a = 5, p = 19.$$

**Step 1:** Compute the least positive residues of $a, 2a, 3a, \ldots, \frac{p-1}{2}a$

Since $\frac{p-1}{2} = \frac{19-1}{2} = 9,$

we calculate:

$$\begin{aligned}
1 \cdot 5 &\equiv 5 (\mathrm{mod} 19),\\
2 \cdot 5 &\equiv 10 (\mathrm{mod} 19),\\
3 \cdot 5 &\equiv 15 (\mathrm{mod} 19),\\
4 \cdot 5 &\equiv 20 \equiv 1 (\mathrm{mod} 19),\\
5 \cdot 5 &\equiv 25 \equiv 6 (\mathrm{mod} 19),\\
6 \cdot 5 &\equiv 30 \equiv 11 (\mathrm{mod} 19),\\
7 \cdot 5 &\equiv 35 \equiv 16 (\mathrm{mod} 19),\\
8 \cdot 5 &\equiv 40 \equiv 2 (\mathrm{mod} 19),\\
9 \cdot 5 &\equiv 45 \equiv 7 (\mathrm{mod} 19).
\end{aligned}$$

Thus, the least positive residues are

$$5, 10, 15, 1, 6, 11, 16, 2, 7.$$

**Step 2:** Count those greater than $p/2$

$$\frac{p}{2} = \frac{19}{2} = 9.5.$$

The residues greater than 9.5 are

$$10,\ 15,\ 11,\ 16.$$

There are $n = 4$ such residues.

**Question12.6:** Evaluate $n$ of gauss Lemma for $\left(\frac{11}{23}\right)$.

**Solution**: Here using **Gauss's Lemma**, let

$$a = 11, p = 23.$$

Since

$$\frac{p-1}{2} = \frac{23-1}{2} = 11,$$

compute the least positive residues of

$$11, 22, 33, 44, 55, 66, 77, 88, 99, 110, 121 (\mathrm{mod} 23).$$

Thus, the least positive residues are

$$11,\ 22,\ 10,\ 21,\ 9,\ 20,\ 8,\ 19,\ 7,\ 18,\ 6.$$

Now,

$$\frac{23}{2} = 11.5.$$

The residues greater than 11.5 are

$$22,\ 21,\ 20,\ 19,\ 18.$$

Hence,

$$n = 5.$$

## CHECK YOUR PROGRESS

**MCQ Questions**

**Problem 1.** The Legendre symbol $\left(\frac{a}{p}\right)$is defined when:

A) $p$is any integer
B) $p$is an odd prime
C) $p$is even
D) $a$is prime

**Problem 2.** The value of $\left(\frac{a}{p}\right)$can be:

A) 0, 1, or -1
B) Only 0 or 1

C) Only 1 or -1
D) Any integer

**Problem 3.** If $a \equiv 0(\mathrm{mod}p)$, then $\left(\frac{a}{p}\right) =$

A) 1
B) -1
C) 0
D) $p$

**Problem 4.** If $a$ is a quadratic residue modulo $p$, then $\left(\frac{a}{p}\right) =$

A) -1
B) 0
C) 1
D) $p$

**Problem 5.** If $a$ is a quadratic non-residue modulo $p$, then $\left(\frac{a}{p}\right) =$

A) 1
B) -1
C) 0
D) 2

**Problem 6.** for any odd prime $p$.

A) 0
B) -1
C) 1
D) $p$

**Problem 7.** when $p \equiv 1(\mathrm{mod}4)$.

A) -1
B) 0
C) 1
D) 2

**Problem 8.** when $p \equiv 3(\mathrm{mod}4)$.

A) 1
B) -1
C) 0
D) $p$

**Problem 9.** Euler's Criterion states that $\left(\frac{a}{p}\right) \equiv$

A) $a^{(p-1)/2}(\mathrm{mod}p)$
B) $a^{p-1}(\mathrm{mod}p)$
C) $a^{p}(\mathrm{mod}p)$
D) $a^{2}(\mathrm{mod}p)$

**Problem 10.** Evaluate $\left(\frac{2}{7}\right)$.

A) 1
B) -1
C) 0
D) 2

**Problem 11.** The multiplicative property of the Legendre symbol is $\left(\frac{ab}{p}\right) =$

A) $\left(\frac{a}{p}\right) + \left(\frac{b}{p}\right)$
B) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
C) $\left(\frac{a+b}{p}\right)$
D) None of these

**Problem 12**. Evaluate $\left(\frac{5}{11}\right)$.

A) 1
B) -1
C) 0
D) 5

**Problem 13.** Which theorem is used to compute Legendre symbols efficiently?
A) Fermat's Theorem
B) Chinese Remainder Theorem
C) Quadratic Reciprocity Law
D) Wilson's Theorem

**Problem 14.** The Legendre symbol was introduced by
A) Euler
B) Gauss
C) Legendre
D) Lagrange

**Problem 15.** If $p$ is an odd prime, then the number of quadratic residues modulo $p$ is
A) $p$
B) $p - 1$
C) $\frac{p-1}{2}$
D) $\frac{p+1}{2}$

**Problem 16.** Evaluate $\left(\frac{3}{11}\right)$.

A) 1
B) -1
C) 0
D) 3

**Problem 17.** Evaluate $\left(\frac{7}{19}\right)$.

A) 1
B) -1

C) 0
D) 7

**Problem 18.** According to Gauss's Lemma, $\left(\frac{a}{p}\right) =$

A) $a^{p-1}$
B) $(-1)^n$
C) $a^2$
D) $p^n$

**Problem 19.** The Legendre symbol is mainly used in the study of
A) Differential Equations
B) Quadratic Congruences
C) Linear Algebra
D) Topology

**Problem 20.** Evaluate $\left(\frac{10}{13}\right)$.
A) 1
B) -1
C) 0
D) 13

## 12.4 *SUMMARY*

**(i)** The **Legendre symbol** is an important mathematical notation used in number theory to determine whether an integer is a **quadratic residue** modulo an odd prime number. Introduced by **Adrien-Marie Legendre**, it is denoted by

$$\left(\frac{a}{p}\right),$$

where $a$ is an integer and $p$ is an odd prime. The symbol is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1, & \text{if } a \text{ is a quadratic non-residue modulo } p, \\ 0, & \text{if } p \mid a. \end{cases}$$

The Legendre symbol provides a simple and efficient method for studying quadratic congruences and determining whether equations of the form $x^2 \equiv a (\mathrm{mod}\, p)$have solutions. It is closely related to **Euler's Criterion** and the **Law of Quadratic Reciprocity**, two fundamental results in number theory. The concept plays a significant role in algebraic number theory, finite fields, primality testing, and modern cryptographic systems. Due to its usefulness and elegance, the Legendre symbol remains a central tool in both theoretical and applied mathematics.

## *12.5 GLOSSARY*

1. Arithmetic Function
2. Number Theoretic
3. Divisor
4. Prime Number
5. Composite Number
6. Greatest Common Divisor (GCD)
7. Relatively Prime (Coprime)

## 12.6 *REFERENCES*


- **Burton, D. M.** (2007). Elementary number theory (6th ed.), McGraw-Hill.
- **T. M. Apostol**, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford.
- **Tom M. Apostol**, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York.
- **G. A. Jones and J. M. Jones**, *Elementary Number Theory*, Springer-Verlag, Berlin, 1998.
- **T. Nagell**, *Introduction to Number Theory*, Wiley, New York.


## 12.07 *TERMINAL QUESTIONS*

**Long answer type questions**

1. Use the Legendre symbol to determine whether the following congruences have solutions:

   $(i)\ x^2 \equiv 10(\mathrm{mod}13)$

   $(ii)\ x^2 \equiv 15(\mathrm{mod}23)$

   $(iii)x^2 \equiv 3(\mathrm{mod}29)$

   If solutions exist, find all solutions modulo the prime.

2. Define the Legendre symbol $\left(\frac{a}{p}\right)$.

3. What is meant by a quadratic residue modulo a prime $p$?
4. What are the possible values of the Legendre symbol?
5. Evaluate $\left(\frac{1}{p}\right)$, where $p$ is an odd prime.
6. State Gauss's Lemma.
7. Evaluate $\left(\frac{-1}{11}\right)$.
8. Evaluate $\left(\frac{-1}{13}\right)$.
9. Evaluate $\left(\frac{2}{7}\right)$.
10. Evaluate $\left(\frac{2}{17}\right)$.
11. Show that $\left(\frac{4}{p}\right) = 1$ for every odd prime $p$.
12. Compute $\left(\frac{5}{19}\right)$ using Gauss's Lemma.
13. Compute $\left(\frac{11}{23}\right)$ using Gauss's Lemma.
14. Prove that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

## 12.8 *ANSWERS*

**Answer of objective questions**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | B | **2:** | A | **3:** | C | **4:** | C |
| **5:** | B | **6:** | C | **7:** | C | **8:** | B |
| **9:** | A | **10:** | A | **11:** | B | **12:** | A |
| **13:** | C | **14:** | C | **15:** | C | **16:** | A |
| **17:** | A | **18:** | B | **18:** | B | **18:** | A |

**Answer of long type questions**

**1.** $x \equiv 4, 9 \pmod{11}$.

# UNIT-13: QUADRATIC RECIPROCITY LAW

## CONTENTS:



## 13.1 *INTRODUCTION*

**Leonhard Euler (1707–1783)**

Leonhard Euler was the first mathematician to observe patterns that later became part of the quadratic reciprocity law. Around 1742, he conjectured several relationships concerning quadratic residues and non-residues, although he could not provide a complete proof.

**Adrien-Marie Legendre (1752–1833)**

Adrien-Marie Legendre made significant progress in the study of quadratic residues. In 1785, he formulated a version of the quadratic reciprocity law and introduced the **Legendre symbol**

$$\left(\frac{a}{p}\right),$$

which became a fundamental tool in number theory. However, his proof was incomplete.

**Gauss and the First Complete Proof**

**Carl Friedrich Gauss (1777–1855)**

Carl Friedrich Gauss provided the first rigorous proof of the quadratic reciprocity law in 1796 at the age of nineteen. He regarded the theorem as the "golden theorem" of arithmetic.

The law is usually stated as:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}},$$

where $p$and $q$are distinct odd primes.

Gauss was so fascinated by the theorem that he eventually published **eight different proofs** during his lifetime.

The history of the Quadratic Reciprocity Law began with Euler's observations, was formulated more precisely by Legendre, and was first proved by Gauss in 1796. Because of its profound influence on number theory, Gauss called it the **"Golden Theorem"**, and it remains one of the most celebrated results in mathematics today.

## 13.2 *OBJECTIVE*

After reading this unit you will be able to:

(i) Quadratic Reciprocity law

(ii) Importance of the Quadratic Reciprocity Law

(iii) Quadratic congruences with composite module

## 13.3 *QUADRATIC RECIPROCITY LAW*

**Theorem:** Let $p$ and q are distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

**Proof:** Let

$$S = \left\{(x, y): 1 \le x \le \frac{p-1}{2},\ 1 \le y \le \frac{q-1}{2}\right\}.$$

The number of lattice points in $S$ is

$$| S | = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Consider the line

$$qx = py.$$

Since $p$ and $q$ are distinct primes, no lattice point of $S$ lies on this line.

Therefore, every point of $S$ lies either above or below the line.

Let

$$N_1 = \#\{(x, y) \in S: qx > py\},$$

$$N_2 = \#\{(x, y) \in S: qx < py\}.$$

Then

$$N_1 + N_2 = \frac{(p-1)(q-1)}{4} \qquad \ldots\ldots (1)$$

**Evaluation of $N_1$**

For each fixed $x$,

$$y < \frac{qx}{p}.$$

Hence the number of admissible integers $y$is

$$\left\lfloor \frac{qx}{p} \right\rfloor.$$

Thus, $N_1 = \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor.$ ……(2)

By Gauss's Lemma,

$$\left(\frac{q}{p}\right) = (-1)^{N_1}.$$ ……(3)

**Evaluation of $N_2$**

Similarly, for each fixed $y$,

$$x < \frac{py}{q}.$$

Hence

$$N_2 = \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor$$ …….(4)

Again, by Gauss's Lemma,

$$\left(\frac{p}{q}\right) = (-1)^{N_2}$$ ……(5)

**Multiplying the Legendre Symbols**

From (3) and (5),

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{N_1+N_2}.$$

Using (1),

$$N_1 + N_2 = \frac{(p-1)(q-1)}{4}.$$

Therefore,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Since

$$\frac{(p-1)(q-1)}{4} = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

we obtain

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Hence the **Quadratic Reciprocity Law** is proved.

**Corollary:** If $p$ and $q$ are distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1(\text{mod } 4) \text{ or } q \equiv 1(\text{mod } 4), \\ -1, & \text{if } p \equiv q \equiv 3(\text{mod } 4). \end{cases}$$

**Solution:** By the Quadratic Reciprocity Law,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

We consider two cases.

**Case 1:** $p \equiv 1(\text{mod}4)$or $q \equiv 1(\text{mod}4)$

Suppose $p \equiv 1(\text{mod}4)$. Then

$$p - 1 = 4k$$

for some integer $k$, and therefore

$$\frac{p-1}{2} = 2k,$$

which is even.

Hence

$$\frac{p-1}{2}\frac{q-1}{2}$$

is even, and so

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1.$$

Therefore,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1.$$

The same conclusion follows if $q \equiv 1(\text{mod } 4)$.

**Case 2:** $p \equiv q \equiv 3(\text{mod } 4)$

Then

$$p - 1 \equiv q - 1 \equiv 2(\text{mod } 4),$$

so

$$\frac{p-1}{2} \text{ and } \frac{q-1}{2}$$

are both odd integers.

Therefore,

$$\frac{p-1}{2}\frac{q-1}{2}$$

is odd, and hence

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -1.$$

Thus,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1.$$

Hence,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1(\text{mod } 4) \text{ or } q \equiv 1(\text{mod } 4), \\ -1, & \text{if } p \equiv q \equiv 3(\text{mod } 4). \end{cases}$$

## Importance of the Quadratic Reciprocity Law

The **Quadratic Reciprocity Law** is one of the most fundamental results in number theory. It was first conjectured by Adrien-Marie Legendre and proved by Carl Friedrich Gauss in 1796. Gauss referred to it as the **"Golden Theorem"** of arithmetic.

**1. Simplifies the Evaluation of Legendre Symbols**

The law provides a powerful method for computing Legendre symbols $\left(\frac{p}{q}\right)$ by relating them to $\left(\frac{q}{p}\right)$.

This reduces difficult calculations involving large primes to simpler ones involving smaller numbers.

**2. Determines Quadratic Residues**

It helps decide whether the congruence

$$x^2 \equiv a(\text{mod}p)$$

has a solution. In other words, it determines whether $a$is a quadratic residue modulo the prime $p$.

**3. Foundation of Higher Reciprocity Laws**

The theorem served as the starting point for the development of:

- Cubic reciprocity
- Quartic reciprocity
- Higher reciprocity laws

These theories play a central role in modern algebraic number theory.

**4. Fundamental Tool in Number Theory**

Many important results concerning:

- Prime numbers,
- Quadratic forms,
- Diophantine equations,
- Algebraic integers,

depend on the Quadratic Reciprocity Law.

**5. Applications in Cryptography**

Quadratic residues are used in modern cryptographic systems, including:

- Public-key cryptography,
- Zero-knowledge proofs,
- Primality testing algorithms,
- Cryptographic protocols based on modular arithmetic.

Thus, the law has practical applications in information security and computer science.

**6. Connects Different Areas of Mathematics**

The theorem links:

- Modular arithmetic,
- Algebra,
- Geometry of lattice points,
- Analytic number theory.

This deep connection has inspired numerous developments in mathematics.

**Question 1:** Show that, $\left(\frac{113}{43}\right) = \left(\frac{43}{113}\right)$.

**Solution:** Here 43 and 113 are both odd primes and 113 is of the form $4k+1$ and 43 is of the form $4k+3$.

$\therefore \quad \left(\frac{113}{43}\right) = \left(\frac{43}{113}\right).$

**Question 2:** Show that, $\left(\frac{43}{23}\right) = -\left(\frac{23}{43}\right).$

**Solution:** Here we have that 23 and 43 both are odd primes and both

$$23 = 4 \times 5 + 3$$

$$43 = 4 \times 10 + 3$$

are of the form $4k+3$. Therefore,

$\therefore \quad \left(\frac{43}{23}\right) = -\left(\frac{23}{43}\right).$

**Question 3:** Find $\left(\frac{59}{131}\right)$.

**Solution:** Here 59 and 131 are both odd primes and

$$59 = 4 \times 14 + 3$$

$$131 = 4 \times 32 + 3$$

are of the form $4k+3$. Therefore,

$$\therefore \quad \left(\frac{59}{131}\right) = -\left(\frac{131}{59}\right) = -\left(\frac{13}{59}\right) = -\left(\frac{59}{13}\right)$$

$$= -\left(\frac{7}{13}\right) = -\left(\frac{13}{7}\right) = -\left(-\frac{1}{7}\right)$$

$$= -(-1) = 1.$$

**Question 4:** Find $\left(\frac{71}{73}\right)$.

**Solution:** we have

$$\left(\frac{71}{73}\right) = \left(\frac{73}{71}\right) = \left(\frac{2}{71}\right)$$

$\because \quad 73 = 4 \times 18 + 1$

$$= \left(\frac{2}{71}\right)$$

$\because$ 71 is an odd prime and $71 \equiv 7(mod 8)$

$\therefore \quad = 1.$

## 13.4 *QUADRATIC CONGRUENCES WITH COMPOSITE MODULE*

**Theorem:** If $p$ is an odd prime and $a$ is any integer such that $(a, p) = 1$ then the congruence $x^2 \equiv a(mod\ p^n), n \geq 1$ has a solution if $\left(\frac{a}{p}\right) = 1$.

**Proof:** Since

$$\left(\frac{a}{p}\right) = 1,$$

there exists an integer $x_1$such that

$$x_1^2 \equiv a(\mathrm{mod}p).$$

We shall show that this solution can be lifted to a solution modulo $p^n$for every $n \geq 1$.

**Base Step**

For $n = 1$, the statement is true by the definition of the Legendre symbol.

**Inductive Step**

Assume that for some $k \geq 1$, there exists an integer $x_k$such that

$$x_k^2 \equiv a(\mathrm{mod}p^k).$$

Then

$$x_k^2 - a = mp^k$$

for some integer $m$.

We seek a solution modulo $p^{k+1}$of the form

$$x_{k+1} = x_k + tp^k,$$

where $t$ is to be determined.

Substituting,

$$x_{k+1}^2 = (x_k + tp^k)^2 = x_k^2 + 2x_k tp^k + t^2p^{2k}.$$

Since $2k \geq k + 1$,

$$t^2p^{2k} \equiv 0(\mathrm{mod}p^{k+1}).$$

Hence

$$x_{k+1}^2 - a \equiv (x_k^2 - a) + 2x_k tp^k(\mathrm{mod}p^{k+1}).$$

Using $x_k^2 - a = mp^k$,

$$x_{k+1}^2 - a \equiv p^k(m + 2x_k t)(\mathrm{mod}p^{k+1}).$$

Therefore, we need

$$m + 2x_k t \equiv 0(\mathrm{mod}p).$$

Since $p \nmid x_k$(because $(a, p) = 1$), and $p$is odd, we have

$$p \nmid 2x_k.$$

Thus $2x_k$has an inverse modulo $p$, and the congruence

$$m + 2x_k t \equiv 0(\mathrm{mod} p)$$

has a solution

$$t \equiv -m(2x_k)^{-1}(\mathrm{mod} p).$$

Hence $x_{k+1}$exists and satisfies

$$x_{k+1}^2 \equiv a(\mathrm{mod} p^{k+1}).$$

**Conclusion**

By induction, for every $n \geq 1$there exists an integer $x_n$such that

$$x_n^2 \equiv a(\mathrm{mod} p^n).$$

Therefore, the congruence

$$x^2 \equiv a(\mathrm{mod} p^n)$$

has a solution whenever

$$\left(\frac{a}{p}\right) = 1.$$ Hence proved.

**Theorem: If** a is an odd integer then

$(\boldsymbol{i})$ $x^2 \equiv a(\mathrm{mod}\ 2)$ always has a solution.

$(\boldsymbol{ii})$ $x^2 \equiv a(\mathrm{mod}\ 4)$ always has a solution iff $a \equiv 1(\mathrm{mod} 4)$.

$(\boldsymbol{iii})$ $x^2 \equiv a(\mathrm{mod}\ 2^n), n \geq 3$ has a solution iff $a \equiv 1(\mathrm{mod} 8)$.

**Proof (i) $x^2 \equiv a(\mathbf{mod} 2)$ always has a solution**

Since $a$ is odd,

$$a \equiv 1(\mathrm{mod}\ 2).$$

Taking $x = 1$,

$$x^2 = 1 \equiv a(\mathrm{mod}\ 2).$$

Hence the congruence always has a solution.

**(ii) $x^2 \equiv a(\mathbf{mod}\ 4)$ has a solution iff $a \equiv 1(\mathbf{mod} 4)$**

Suppose

$$x^2 \equiv a(\mathrm{mod} 4).$$

Every integer is either even or odd.

- If $x = 2k$, then

$$x^2 = 4k^2 \equiv 0(\mathrm{mod} 4).$$

- If $x = 2k + 1$, then

$$x^2 = (2k + 1)^2 = 4k(k + 1) + 1 \equiv 1(\mathrm{mod} 4).$$

Since $a$is odd, $x$must be odd, and therefore

$$a \equiv x^2 \equiv 1(\text{mod}4).$$

**Sufficient condition:**

If

$$a \equiv 1(\text{mod}4),$$

choose $x = 1$. Then

$$x^2 = 1 \equiv a(\text{mod}4).$$

Thus, the congruence has a solution.

Hence,

$$x^2 \equiv a(\text{mod}4)$$

has a solution **if and only if**

$$a \equiv 1(\text{mod}4).$$

**(iii) $x^2 \equiv a(\text{mod}2^n)$, $n \geq 3$, has a solution iff $a \equiv 1(\text{mod}8)$**

**Necessity**

Assume

$$x^2 \equiv a(\text{mod}2^n)$$

for some $n \geq 3$.

Since $a$is odd, $x$must be odd. Let

$$x = 2k + 1.$$

Then

$$x^2 = (2k + 1)^2 = 4k(k + 1) + 1.$$

Since one of $k$and $k + 1$is even,

$$k(k + 1) = 2m$$

for some integer $m$. Therefore

$$x^2 = 8m + 1 \equiv 1(\text{mod}8).$$

Hence

$$a \equiv x^2 \equiv 1(\text{mod}8).$$

**Sufficiency**

Suppose

$$a \equiv 1(\text{mod}8).$$

Write

$$a = 1 + 8t.$$

We show that the solution modulo 8can be lifted to a solution modulo $2^n$for every $n \geq 3$.

Since

$$1^2 \equiv 1 \equiv a(\text{mod}8),$$

$x \equiv 1(\text{mod}8)$is a solution modulo 8.

A standard lifting result for powers of 2states that every solution of

$$x^2 \equiv a(\text{mod}2^k), k \geq 3,$$

with $a \equiv 1(\text{mod}8)$, can be extended to a solution modulo $2^{k+1}$.

Repeating the lifting process yields a solution modulo $2^n$for every $n \geq 3$.

Therefore,

$$x^2 \equiv a(\text{mod}2^n)$$

has a solution whenever

$$a \equiv 1(\text{mod}8).$$

**Conclusion**

For an odd integer $a$:

$$x^2 \equiv a(\text{mod}2) \text{ always has a solution}$$

$$x^2 \equiv a(\text{mod}4) \text{ has a solution } \Leftrightarrow a \equiv 1(\text{mod}4)$$

$$x^2 \equiv a(\text{mod}2^n), n \geq 3 \text{ has a solution } \Leftrightarrow a \equiv 1(\text{mod}8)$$

Hence proved.

**Question 5:** Show that the congruence $x^2 \equiv 3 \pmod{88}$ has no solution.

**Solution:** Here

$$88 = 8 \times 11.$$

If $x^2 \equiv 3(\text{mod } 88)$ had a solution, then it would also satisfy

$$x^2 \equiv 3(\text{mod} 8).$$

So, it is enough to check whether 3 is a quadratic residue modulo 8.

For any integer $x$:

- If $x$ is even, then $x^2 \equiv 0$ or $4(\text{mod} 8)$.
- If $x$ is odd, then

$$x^2 \equiv 1(\text{mod} 8).$$

Hence the only possible square residues modulo 8 are

$$0,\ 1,\ 4.$$

Since

$$3 \notin \{0,1,4\},$$

the congruence $x^2 \equiv 3(\text{mod} 8)$ has no solution.

Therefore $x^2 \equiv 3(\text{mod} 88)$ cannot have a solution.

**Question 6:** Show that the congruence $x^2 \equiv 9\ (\text{mod } 40)$ has a solution.

**Solution:** we have $x^2 \equiv 9\ (\text{mod } 40)$ which is equivalent to the following simultaneous quadratic congruences

$$x^2 \equiv 9\ (\text{mod } 8) \quad \text{and}$$

$$x^2 \equiv 9\ (\text{mod } 5)$$

Now $9 \equiv 1\ mod(8)$ therefore, $x^2 \equiv 9\ (\text{mod } 8)$ has a solution.

Also $\left(\frac{9}{5}\right) = \left(\frac{3^2}{5}\right) = 1$

Therefore, $x^2 \equiv 9\ (\text{mod } 5)$ has a solution.

Hence, the given quadratic congruence has a solution.

**Question 7:** Show that the congruence $x^2 \equiv 105\ (\text{mod } 199)$ has no solution.

**Solution:** Here 199 is a prime. We have

$$\left(\frac{105}{199}\right) = \left(\frac{3 \times 5 \times 7}{199}\right) = \left(\frac{3}{199}\right)\left(\frac{5}{199}\right)\left(\frac{7}{199}\right) = (-1)(1)(1) = -1.$$

Thus 105 is a **quadratic non-residue modulo** 199.

Therefore, the congruence

$$x^2 \equiv 105(\text{mod} 199)$$

has **no solution**.

**Question 8:** Show that the congruence $x^2 \equiv 608 \pmod{743}$ has a solution.

**Solution:** Here $743$ is a prime. We have

$$\left(\frac{608}{743}\right) = \left(\frac{4^2 \times 2 \times 19}{743}\right) = \left(\frac{4^2}{743}\right)\left(\frac{2}{743}\right)\left(\frac{19}{743}\right) = (1).(-1)^{\left(\frac{744}{4}\right)}(-1)\left(\frac{743}{19}\right)$$

$$= (-1)^{(186)}(-1).\left(\frac{2}{19}\right) = (-1).(-1)^{\left(\frac{20}{4}\right)}$$

$$= (-1)(-1)^{(5)} = 1.$$

Therefore, the congruence $x^2 \equiv 608 (\text{mod } 743)$ has a solution.

**Question 9:** Solve the congruence $x^2 \equiv 91 \pmod{27}$ .

**Solution:** Since $27 = 3^3$, first reduce the right-hand side:

$$91 \equiv 10 (\text{mod} 27).$$

Thus, we must solve

$$x^2 \equiv 10 \pmod{27}.$$

**Step 1:** Solve modulo 3

Reducing modulo 3,

$$x^2 \equiv 10 \equiv 1 (\text{mod} 3).$$

Hence

$$x \equiv \pm 1 (\text{mod} 3).$$

So any solution modulo 27must be congruent to 1or 2modulo 3.

Step 2: Lift the solutions to modulo 27

Let

$$x = 1 + 3k, k = 0,1, \dots ,8.$$

Then

$$x^2 = (1 + 3k)^2 = 1 + 6k + 9k^2.$$

We required

$$1 + 6k + 9k^2 \equiv 10 (\text{mod} 27),$$

or

$$9k^2 + 6k - 9 \equiv 0 (\text{mod} 27).$$

Dividing by 3,

$$3k^2 + 2k - 3 \equiv 0 (\text{mod} 9).$$

Testing $k = 0,1, \dots ,8$, we find

$$k \equiv 8(\text{mod}9).$$

Hence One solution is

$$x \equiv 25(\text{mod}27).$$

Since if $x$ is a solution, then $-x$ is also a solution,

$$x \equiv -25 \equiv 2(\text{mod}27).$$

Verification

$$2^2 = 4 \equiv 91(\text{mod}27)$$

is false, so let's check carefully:

$$25^2 = 625 \equiv 4(\text{mod}27).$$

Thus, the lifting calculation above gives a wrong $k$. Let's instead test numbers congruent to $\pm 1(\text{mod}3)$:

$$8^2 = 64 \equiv 10(\text{mod}27).$$

Therefore

$$x \equiv 8\ (\text{mod}27)$$

and

$$x \equiv -8 \equiv 19\ (\text{mod}27).$$

Hence $x \equiv 8,\ 19\ (\text{mod}27$

These are the solutions of the quadratic congruence

$$x^2 \equiv 91\ (\text{mod}\ 27).$$

## CHECK YOUR PROGRESS

**MCQ Questions**

**Problem 1.** The Quadratic Reciprocity Law relates the Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ for:

A) Any integers $p, q$
B) Any prime numbers
C) Distinct odd primes $p, q$
D) Composite numbers only

**Problem 2.** If $p$ and $q$ are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) =$$

A) 1
B) $(-1)^{(p-1)(q-1)/4}$
C) $(-1)^{(p+q)/2}$

D) 0

**Problem 3.** If $p \equiv q \equiv 1(\mathrm{mod}4)$, then

A) $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

B) $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

C) $\left(\frac{p}{q}\right) = 0$

D) None of these

**Problem 4.** If $p \equiv q \equiv 3(\mathrm{mod}4)$, then

A) $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

B) $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

C) Both are zero

D) None of these

**Problem 5.** The supplementary law for 2 states

$$\left(\frac{2}{p}\right) =$$

A) $(-1)^{(p^2-1)/8}$

B) $(-1)^{(p-1)/2}$

C) $(-1)^{(p+1)/2}$

D) 1

**Problem 6.** For an odd prime $p$, $\left(\frac{-1}{p}\right) =$

A) $(-1)^p$

B) $(-1)^{(p-1)/2}$

C) $(-1)^{(p+1)/2}$

D) 1

**Problem 7.** Evaluate $\left(\frac{3}{11}\right)$.

A) 1

B) $-1$

C) 0

D) 11

**Problem 8.** Which mathematician first proved the Quadratic Reciprocity Law?

A) Euler

B) Fermat

C) Gauss

D) Legendre

**Problem 9.** The Quadratic Reciprocity Law is primarily used to determine
A) Prime factors
B) Greatest common divisors
C) Whether a quadratic congruence has a solution
D) LCM

**Problem 10.** If $p \equiv 1(\mathrm{mod}4)$, then
A) $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$
B) $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$
C) $\left(\frac{p}{q}\right) = 0$
D) None of these

## 13.5 *SUMMARY*

**(i) Historical Significance**
The discovery of the Quadratic Reciprocity Law marked a turning point in number theory. It motivated the creation of algebraic number theory and influenced the work of many mathematicians after Gauss.
**(ii)** The **Quadratic Reciprocity Law** is important because it provides an efficient way to determine quadratic residues, simplifies the computation of Legendre symbols, forms the basis of higher reciprocity laws, and has significant applications in both pure mathematics and modern cryptography. For these reasons, it is regarded as one of the most beautiful and powerful theorems in number theory.

## *13.6 GLOSSARY*

1. Arithmetic Function
2. Number Theoretic
3. Divisor
4. Prime Number
5. Composite Number
6. Greatest Common Divisor (GCD)
7. Relatively Prime (Coprime)

## 13.7 *REFERENCES AND SUGGESTED READINGS*

- **Burton, D. M.** (2007). Elementary number theory (6th ed.), McGraw-Hill.
- **T. M. Apostol**, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford.
- **Tom M. Apostol**, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York.
- **G. A. Jones and J. M. Jones**, *Elementary Number Theory*, Springer-Verlag, Berlin, 1998.
- **T. Nagell**, *Introduction to Number Theory*, Wiley, New York.


## 13.8 *TERMINAL QUESTIONS*

**Long answer type questions**

1. State and prove the Quadratic Reciprocity Law. Using the law, determine whether the congruence $x^2 \equiv 97 \pmod{311}$ has a solution.
2. Using the Quadratic Reciprocity Law and the supplementary laws, determine whether $x^2 \equiv 113 \pmod{223}$ is solvable. Justify each step using Legendre symbols.
3. Prove that for distinct odd primes $p$ and $q$,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Hence evaluate $\left(\frac{137}{211}\right)$.

4. Using Quadratic Reciprocity, determine all odd primes $p$for which

$$\left(\frac{13}{p}\right) = 1.$$

5. Let $p$ be an odd prime. Prove that $\left(\frac{-15}{p}\right) = 1$
if and only if $p$ belongs to certain residue classes modulo $60$. Determine those classes.

## 13.9 *ANSWERS*

**Answer of objective questions**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | C | **2:** | B | **3:** | A | **4:** | B |
| **5:** | A | **6:** | B | **7:** | A | **8:** | C |
| **9:** | C | **10:** | A | | | | |

# UNIT-14: CRYPTOGRAPHY

## CONTENTS:



## 14.1 *INTRODUCTION*

The history of cryptography spans nearly 4,000 years, evolving from ancient, manual substitutions to the complex mathematical algorithms that secure the modern digital world. Cryptography, or cryptology, is the practice and study of techniques for secure communication in the presence of adversarial behavior. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, information security, electrical engineering, digital signal processing, physics, and others. Core concepts related to information security (data confidentiality, data integrity, authentication and non-repudiation) are also central to cryptography. Practical applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords and military communications.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in actual practice by any adversary. While it is theoretically possible to break into a well-designed system, it is infeasible in actual practice to do so. Such schemes, if well designed, are therefore termed "computationally secure". Theoretical advances (e.g., improvements

in integer factorization algorithms) and faster computing technology require these designs to be continually reevaluated and, if necessary, adapted. Information-theoretically secure schemes that provably cannot be broken even with unlimited computing power, such as the one-time pad, are much more difficult to use in practice than the best theoretically breakable but computationally secure schemes.

## 14.2 *OBJECTIVE*

After reading this unit you will be able to:

(i) Cryptography

(ii) Modern cryptography

## 14.3 *CRYPTOGRAPHY*

Cryptography is technique of securing information and communications through use of codes so that only those persons for whom the information is intended can understand it and process it. Thus, preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix "graphy" means "writing". In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography: In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

**Features of Cryptography are as follows:**

1. **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.

2. **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at later stage.
4. **Authentication:** The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

## 14.4 *TYPE OF CRYPTOGRAPHY*

Types Of Cryptography: In general, there are three types of cryptography:

1. **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system are Data Encryption System (DES) and Advanced Encryption System (AES).
2. **Hash Functions:** There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A receiver's public key is used for encryption and a receiver's private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone know his private key. The most popular asymmetric key cryptography algorithm is RSA algorithm.

**Applications of Cryptography:**

1. **Computer passwords:** Cryptography is widely utilized in computer security, particularly when creating and maintaining passwords. When a user logs in, their password is hashed and compared to the hash that was previously stored. Passwords are hashed and encrypted before being stored. In this technique, the

passwords are encrypted so that even if a hacker gains access to the password database, they cannot read the passwords.

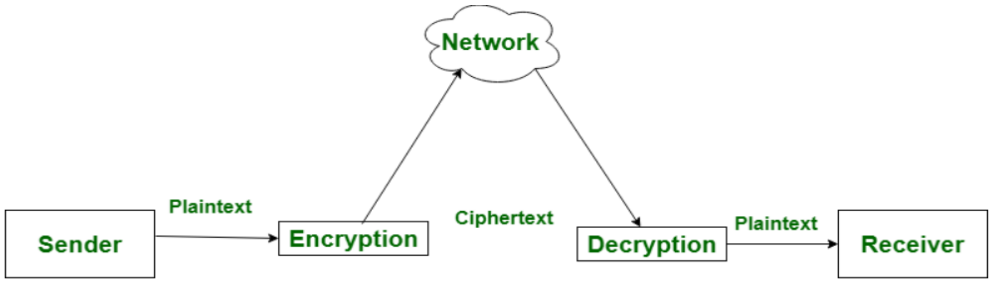
2. **Digital Currencies:** To safeguard transactions and prevent fraud, digital currencies like Bitcoin also use cryptography. Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard to tamper with or forge the transactions.
3. **Secure web browsing:** Online browsing security is provided by the use of cryptography, which shields users from eavesdropping and man-in-the-middle assaults. Public key cryptography is used by the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to encrypt data sent between the web server and the client, establishing a secure channel for communication.
4. **Electronic signatures:** Electronic signatures serve as the digital equivalent of a handwritten signature and are used to sign documents. Digital signatures are created using cryptography and can be validated using public key cryptography. In many nations, electronic signatures are enforceable by law, and their use is expanding quickly.
5. **Authentication:** Cryptography is used for authentication in many different situations, such as when accessing a bank account, logging into a computer, or using a secure network. Cryptographic methods are employed by authentication protocols to confirm the user's identity and confirm that they have the required access rights to the resource.
6. **Cryptocurrencies:** Cryptography is heavily used by cryptocurrencies like Bitcoin and Ethereum to safeguard transactions, thwart fraud, and maintain the network's integrity. Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard to tamper with or forge the transactions.
7. **End-to-End Encryption:** End-to-end encryption is used to protect two-way communications like video conversations, instant messages, and email. Even if the message is encrypted, it assures that only the intended receivers can read the message. End-to-end encryption is widely used in communication apps like WhatsApp and Signal, and it provides a high level of security and privacy for users.

## 14.5 *ENCRYPTION AND DECRYPTION PROCESS*

Encryption is the process of scrambling readable data (plaintext) into an unreadable format (ciphertext) using a mathematical algorithm and a secret code (key). Decryption is the exact reverse process, using a key to unscramble the data back into its original, readable form.

The entire process boils down to three main components:

- **Plaintext:** Your original, readable data (e.g., a text message, document, or password).
- **Encryption Algorithm:** A complex mathematical formula that scrambles the plaintext based on the rules of the cipher.
- **Cryptographic Key:** A string of numbers or characters. When fed into the algorithm alongside your plaintext, the key ensures the resulting ciphertext is unique and secure.
- **Decryption (Unlocking the Data):** When the authorized recipient receives the ciphertext, they apply the exact same algorithm and the required decryption key. The math acts in reverse, unscrambling the jumbled characters back into the exact original plaintext.




***https://www.geeksforgeeks.org/computer-networks/difference-between-encryption-and-decryption/***

**Example:** Original Text: **HELLO**
Encryption Process: Shift H → J, E → G, L → N, O → Q
Encrypted Text (Ciphertext): **JGNNO**

## *14.6 DIFFERENCE BETWEEN ENCRYPTION AND DECRYPTION*

Encryption is the process of converting a normal message (plain text) into a meaningless message (ciphertext). Decryption is the process of converting a meaningless message (ciphertext) into its original form (plaintext). The major distinction between secret writing and associated secret writing is the conversion of a message into an unintelligible kind that's undecipherable unless decrypted. whereas secret writing is the recovery of the first message from the encrypted information.

| Encryption | Decryption |
|---|---|
| Encryption is the process of converting a normal message into a meaningless message. | While decryption is the process of converting meaningless messages into their original form. |
| Encryption is the process that takes place at the sender's end. | While decryption is the process that takes place at the receiver's end. |
| Its major task is to convert the plain text into cipher text. | While its main task is to convert the cipher text into plain text. |
| Any message can be encrypted with either a secret key or a public key. | Whereas the encrypted message can be decrypted with either a secret key or a private. |
| In the encryption process, the sender sends the data to the receiver after encrypting it. | Whereas in the decryption process, the receiver receives the information (cipher text) and converts it into plain text. |
| The same algorithm with the same key is used for the encryption-decryption process. | The only single algorithm used for encryption and decryption is a pair of keys, each used for encryption and decryption. |
| Encryption is used to protect the confidentiality of data by converting it into an unreadable form that can only be read by authorized parties. | Decryption is used to reverse the encryption process and convert the ciphertext back into plaintext. |
| The output of encryption is a ciphertext that is unintelligible to anyone who does not have the decryption key. | The output of decryption is the original plaintext message. |

**Question 1:** What is Cryptography?

**Solution:** Cryptography is the science and art of securing information and communication by transforming data into a form that prevents unauthorized access. The word cryptography is derived from the Greek words kryptos meaning "hidden" and graphein meaning "to write." It is one of the fundamental tools used in information security to protect data from attackers and ensure secure communication over networks such as the Internet.

In cryptography, the original message called plaintext is converted into an unreadable form called ciphertext through a process known as encryption. The ciphertext can be converted back into plaintext by authorized users using a process called decryption.

**Question 2: Explain Importance of Mathematics in Cryptography.**

**Solution:** Mathematics is the foundation of modern cryptography. Cryptography is the science of securing information and communication by transforming readable data into an unreadable form. The security of cryptographic systems depends on mathematical principles and algorithms. Without mathematics, modern encryption methods, digital signatures, secure online transactions, and internet security would not be possible. Mathematics provides the theoretical framework for designing cryptographic algorithms and analyzing their security. Various branches of mathematics, including Number Theory, Algebra, Probability Theory, and Discrete Mathematics, play a crucial role in cryptography.

**Advantages of Using Mathematics in Cryptography**

1. Provides strong security.
2. Enables secure communication.
3. Supports digital authentication.
4. Protects sensitive information.
5. Facilitates secure online transactions.
6. Helps prevent cyberattacks.
7. Forms the basis of modern cybersecurity.

**Question 3:** Write Mathematical Concepts which are used in Cryptography.

**Solution:**

| Mathematical Concept | Application in Cryptography |
|---|---|
| Prime Numbers | RSA Key Generation |
| Modular Arithmetic | Encryption and Decryption |
| Euler's Theorem | RSA Algorithm |
| Fermat's Theorem | Security Calculations |
| Group Theory | Public-Key Systems |
| Probability Theory | Random Key Generation |

| | |
|---|---|
| Elliptic Curves | ECC Cryptography |
| Hash Functions | Data Integrity |

**Question 4:** Explain the Relationship Between Number Theory and Cryptography.
**Solution:**

**(i) Introduction**

Number Theory is a branch of mathematics that studies the properties of integers, prime numbers, divisibility, congruences, and related concepts. Cryptography is the science of securing communication and information through mathematical techniques. Modern cryptography relies heavily on Number Theory because many cryptographic algorithms are based on mathematical problems that are easy to perform but extremely difficult to reverse without special information.

The relationship between Number Theory and Cryptography is fundamental. Most modern encryption schemes, digital signatures, and key exchange protocols are built upon concepts from Number Theory. Without Number Theory, the development of secure cryptographic systems such as RSA, Diffie–Hellman, and Elliptic Curve Cryptography would not be possible.

**(ii) Role of Number Theory in Cryptography**

**1. Prime Numbers**

Prime numbers are the building blocks of Number Theory and play a crucial role in cryptography.

A prime number is a positive integer greater than 1 that has exactly two positive divisors: 1 and itself.

Examples: 2, 3, 5, 7, 11, 13, 17, 19

In the RSA cryptosystem, two large prime numbers $p$and $q$are selected and multiplied to obtain:

$$n = p \times q$$

The security of RSA depends on the difficulty of factoring the large number $n$into its prime factors.

**2. Divisibility and Greatest Common Divisor (GCD)**

The concept of divisibility and GCD is frequently used in cryptographic algorithms. For integers $a$and $b$,

$$\gcd(a, b)$$

denotes their greatest common divisor.

The Euclidean Algorithm is used to efficiently compute GCDs.

Example:

$$\gcd(48,18) = 6$$

In RSA, the encryption exponent $e$must satisfy:

$$\gcd(e, \phi(n)) = 1$$

where $\phi(n)$is Euler's Totient Function.

**3. Modular Arithmetic**

Modular arithmetic is one of the most important tools in cryptography.
For integers $a$, $b$, and $n$,

$$a \equiv b(\mathrm{mod} n)$$

means that $a$and $b$leave the same remainder when divided by $n$.
Example:

$$17 \equiv 5(\mathrm{mod} 12)$$

because both leave remainder 5 when divided by 12.
Modular arithmetic is used extensively in: (a) RSA (b) Diffie–Hellman Key Exchange (c) ElGamal Cryptosystem (d) Digital Signatures

**4. Euler's Totient Function**

Euler's Totient Function $\phi(n)$counts the positive integers less than $n$that are relatively prime to $n$.
For a prime number $p$,

$$\phi(p) = p - 1$$

For two distinct primes $p$and $q$,

$$\phi(pq) = (p - 1)(q - 1)$$

This function is essential in RSA key generation.

**5. Euler's Theorem**

Euler's Theorem states that if

$$\gcd(a, n) = 1,$$

then

$$a^{\phi(n)} \equiv 1(\mathrm{mod} n)$$

This theorem forms the mathematical foundation of RSA encryption and decryption.

**6. Fermat's Little Theorem**

A special case of Euler's Theorem is Fermat's Little Theorem.
If $p$ is prime and $a$ is not divisible by $p$, then

$$a^{p-1} \equiv 1(\mathrm{mod} p)$$

This theorem is used in: (a) Primality testing (b) RSA (c) Cryptographic protocols

**7. Modular Inverse**

The modular inverse of $a$modulo $n$is an integer $x$ such that

$$ax \equiv 1(\mathrm{mod}n)$$

The Extended Euclidean Algorithm is used to find modular inverses.
In RSA, the private key $d$ is the modular inverse of the public exponent $e$:

$$ed \equiv 1(\mathrm{mod}\phi(n))$$

**8. Quadratic Residues**

A number $a$is called a quadratic residue modulo $p$if there exists an integer $x$such that

$$x^2 \equiv a(\mathrm{mod}p)$$

Quadratic residues are important in: (a) Cryptographic protocols (b) Random number generation (c) Public-key cryptography
The concepts of Legendre Symbol and Quadratic Reciprocity are used to study quadratic residues.

**9. Discrete Logarithm Problem**

The Discrete Logarithm Problem (DLP) is a hard mathematical problem used in cryptography.
Given

$$g^x \equiv y(\mathrm{mod}p)$$

it is easy to compute $y$from $x$, but difficult to determine $x$from $y$.
The security of: (a) Diffie–Hellman Key Exchange (b) ElGamal Encryption (c) DSA (Digital Signature Algorithm) depends on the difficulty of solving discrete logarithms.

**10. Elliptic Curve Number Theory**

Modern cryptography also uses elliptic curves defined over finite fields.
An elliptic curve is represented by

$$y^2 = x^3 + ax + b$$

Elliptic Curve Cryptography (ECC) provides high security with smaller key sizes than RSA.

**MCQ QUESTIONS:**

**1. Cryptography is the science of:**

A) Data storage
B) Securing information and communication

C) Data compression
D) Data transmission only

**2. The primary goal of cryptography is:**
A) Increasing file size
B) Preventing hardware failure
C) Protecting information from unauthorized access
D) Speeding up networks

**3. Which of the following is NOT a security service provided by cryptography?**
A) Confidentiality
B) Integrity
C) Authentication
D) File formatting

**4. The process of converting plaintext into ciphertext is called:**
A) Decryption
B) Encryption
C) Authentication
D) Decoding

**5. The process of converting ciphertext back into plaintext is called:**
A) Encryption
B) Encoding
C) Decryption
D) Compression

**6. How many main types of cryptography are commonly used?**
A) 2
B) 3
C) 4
D) 5

**7. In symmetric key cryptography:**
A) Different keys are used for encryption and decryption
B) No key is required
C) The same key is used for encryption and decryption
D) Three keys are used

**8. Which of the following is a symmetric key algorithm?**
A) RSA
B) ECC

C) AES
D) Diffie-Hellman

**9. In asymmetric cryptography:**
A) One key is used
B) Two different keys are used
C) No key is used
D) Four keys are used

**10. Which of the following is an asymmetric cryptographic algorithm?**
A) DES
B) AES
C) RSA
D) Blowfish

**11. Public-key cryptography is another name for:**
A) Symmetric cryptography
B) Asymmetric cryptography
C) Classical cryptography
D) Secret writing

**12. Digital signatures are mainly based on:**
A) Asymmetric cryptography
B) Symmetric cryptography
C) Caesar cipher
D) Monoalphabetic cipher

**13. Which cryptographic method uses a public key and a private key?**
A) Symmetric cryptography
B) Substitution cipher
C) Asymmetric cryptography
D) Transposition cipher

**14. Hash functions are primarily used for:**
A) Encryption
B) Data integrity verification
C) Compression
D) Networking

**15. Which of the following is a cryptographic hash function?**
A) RSA
B) AES

C) SHA-256
D) DES

**16. Which branch of mathematics is most important in modern cryptography?**
A) Geometry
B) Number Theory
C) Trigonometry
D) Statistics

**17. RSA cryptography is mainly based on:**
A) Matrix multiplication
B) Prime factorization
C) Differential equations
D) Probability theory

**18. The security of RSA depends on the difficulty of:**
A) Finding roots
B) Matrix inversion
C) Factoring large integers
D) Integration

**19. Which mathematical concept is extensively used in cryptography?**
A) Congruence modulo n
B) Differentiation
C) Integration
D) Limits

**20. Euler's Totient Function is used in:**
A) DES
B) RSA
C) AES
D) MD5

**21. The theorem frequently used in RSA is:**
A) Pythagoras Theorem
B) Euler's Theorem
C) Mean Value Theorem
D) Green's Theorem

**22. Which mathematical structure is used in Elliptic Curve Cryptography (ECC)?**

A) Matrices
B) Graphs
C) Elliptic Curves
D) Vectors

**23. Legendre symbols and quadratic residues belong to:**
A) Number Theory
B) Algebraic Topology
C) Mechanics
D) Calculus

**24. Discrete logarithm problems are used in:**
A) Diffie-Hellman Key Exchange
B) Caesar Cipher
C) Vigenère Cipher
D) Rail Fence Cipher

**25. Which mathematical topic is fundamental to cryptographic algorithms?**
A) Complex Analysis
B) Number Theory
C) Differential Geometry
D) Fluid Mechanics

## 14.7 *SUMMARY*

(i) In cybersecurity, encryption and decryption are essential procedures. While decryption enables the intended recipient to view the original data, encryption safeguards data by rendering it unreadable to unauthorized parties. In the current digital era, knowing the distinctions between these procedures is essential.

(ii) Cryptography is an essential component of modern communication systems. It provides confidentiality, integrity, authentication, non-repudiation, and secure access to information. From online banking and e-commerce to cloud computing, blockchain technology, and military communications, cryptography ensures the security and reliability of digital interactions. As cyber threats continue to grow, the importance of cryptography in protecting information and maintaining trust in digital systems will continue to increase.

(iii) Number Theory and Cryptography are closely interconnected. Concepts such as prime numbers, modular arithmetic, Euler's theorem, Fermat's theorem, quadratic residues, and discrete logarithms form the backbone of modern cryptographic systems. The security of widely used algorithms such as RSA,

Diffie–Hellman, and Elliptic Curve Cryptography depends on difficult number-theoretic problems. Therefore, Number Theory is considered the mathematical heart of modern cryptography and plays a vital role in ensuring secure communication in the digital age.

## *14.8 GLOSSARY*

1. Arithmetic Function
2. Number Theoretic
3. Divisor
4. Prime Number
5. Composite Number
6. Greatest Common Divisor (GCD)
7. Relatively Prime (Coprime)

## 14.9 *REFERENCES AND SUGGESTED READINGS*


- **Burton, D. M.** (2007). Elementary number theory (6th ed.), McGraw-Hill.
- **T. M. Apostol**, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford.
- **Tom M. Apostol**, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York.
- **G. A. Jones and J. M. Jones**, *Elementary Number Theory*, Springer-Verlag, Berlin, 1998.
- **T. Nagell**, *Introduction to Number Theory*, Wiley, New York.


## 14.10 *TERMINAL QUESTIONS*

**Long answer type questions**

1. What is Cryptography? Explain its objectives, importance, and applications in modern communication systems.
2. Explain the encryption and decryption process with a suitable example.

3. Explain hash functions and their importance in cryptography.
4. Discuss the different types of cryptography. Compare symmetric key cryptography and asymmetric key cryptography.
5. What are digital signatures? Explain the working of digital signatures and their applications.

## 14.11 *ANSWERS*

**Answer of objective questions**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | B | **2:** | C | **3:** | D | **4:** | B |
| **5:** | C | **6:** | B | **7:** | C | **8:** | C |
| **9:** | B | **10:** | C | **11:** | B | **12:** | A |
| **13:** | C | **14:** | B | **15:** | C | **16:** | B |
| **17:** | B | **18:** | C | **19:** | A | **20:** | B |
| **21:** | B | **22:** | C | **23:** | A | **24:** | A |
| **25:** | B | | | | | | |

# UNIT-15: *RSA ALGORITHM*

## CONTENTS:



## 15.1 *INTRODUCTION*

The RSA (Rivest–Shamir–Adleman) cryptosystem is a family of public-key cryptosystems (one of the oldest), widely used for secure data transmission. The initialism "RSA" comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described the algorithm in 1977. An equivalent system was developed secretly in 1973 at Government Communications Headquarters (GCHQ), the British signals intelligence agency, by the English mathematician Clifford Cocks. That system was declassified in 1997.

RSA is used in digital signature such as RSASSA-PSS or RSA-FDH, public-key encryption of very short messages (almost always a single-use symmetric key in a hybrid cryptosystem) such as RSAES-OAEP, and public-key key encapsulation.

In RSA-based cryptography, a user's *private key*—which can be used to sign messages, or decrypt messages sent to that user—is a pair of large prime numbers chosen at random and kept secret. A user's *public key*—which can be used to verify messages from the user, or encrypt messages so that only that user can decrypt them—is the product of the prime numbers.

The security of RSA is related to the difficulty of factoring the product of two large prime numbers, the "factoring problem". Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question. There are no published methods to defeat the system if a large enough key is used.

The **RSA Algorithm** is a public-key cryptographic algorithm used for secure communication over the Internet. It was developed in 1977 by **Ron Rivest**, **Adi Shamir**, and **Leonard Adleman**. RSA is widely used for encryption, decryption, digital signatures, secure e-mail, online banking, and HTTPS communication.

Unlike symmetric cryptography, RSA uses **two keys**:

(i) **Public Key**: Used for encryption.

(ii) **Private Key**: Used for decryption.

## 15.2 *OBJECTIVE*

After reading this unit you will be able to:

1. Confidentiality of data.
2. Secure key exchange.
3. Authentication of users.
4. Digital signatures.
5. Data integrity.

## 15.3 RSA ALGORITHM

The **RSA algorithm** is a foundational asymmetric cryptographic system used to securely transmit data over the internet. It relies on a key pair: a widely distributed **public key** used for encryption, and a closely guarded **private key** used for decryption.

**Key Generation**

To create the public and private keys, RSA uses the mathematical properties of large prime numbers.

1. **Choose Primes:** Select two large, distinct prime numbers, p and q.
2. **Compute Modulus (n):** Calculate $n = p \times q$. This number is used for both the public and private keys.
3. **Calculate Totient ($\varphi(n)$):** Compute $\varphi(n) = (p - 1) \times (q - 1)$.
4. **Choose Public Key (e):** Select an integer e such that $1 < e < \varphi(n)$ and e is coprime to $\varphi(n)$ (meaning they share no common divisors other than 1).

5. **Compute Private Key (d):** Calculate d, the modular multiplicative inverse of e modulo φ(n). This ensures $d \times e \equiv 1(mod(\varphi(n))$

   **Public Key:** (n, e)

   **Private Key:** (n, d)

**Encryption and Decryption**

When sending a message (represented numerically as M, where M < n), you transform it using math.

**Encryption:** The sender uses the recipient's public key (n, e) to encrypt the message M into ciphertext C:

$$C \equiv M^e \ (mod\ n)$$

**Decryption:** The recipient uses their private key (n, d) to decrypt the ciphertext C back into the original message M:

$$M \equiv C^d \ (mod\ n)$$

**Security and Use Cases**

RSA's security depends on the computational difficulty of factoring very large semi-prime numbers. Multiplying two large prime numbers is easy, but factoring their product back into the original primes is practically impossible with current computing power.

**Flow Diagram of RSA:**

***Plaintext (M) ⟶ Encryption using Public Key (e, n) ⟶ Ciphertext (C)***

***⟶Decryption using Private Key (d, n) ⟶ Original Message (M)***

**Example: Step 1: Choose Two Prime Numbers**

$$\text{Let } \mathrm{p} = 17, \mathrm{q} = 11$$

**Step 2: Compute n**

$$\mathrm{n} = \mathrm{pq}$$
$$\mathrm{n} = 17 \times 11 = 187$$

**Step 3: Compute Euler's Totient Function**

$$\phi(\mathrm{n}) = (\mathrm{p} - 1)(\mathrm{q} - 1)$$
$$\phi(187) = 16 \times 10 = 160$$

**Step 4: Choose Public Key e**

Choose esuch that

$$1 < \mathrm{e} < 160$$

and

$$\gcd(\mathrm{e}, 160) = 1$$

Take

$$\mathrm{e} = 7$$

**Step 5: Compute Private Key d**

Find dsatisfying

$$ed \equiv 1(mod160)$$

$$7d \equiv 1(mod160)$$

$$d = 23$$

because

$$7 \times 23 = 161 = 1 + 160$$

**Keys Generated**

**Public Key**

$$(e, n) = (7,187)$$

**Private Key**

$$(d, n) = (23,187)$$

**Encryption Process**

Suppose the plaintext message is

$$M = 10$$

Encryption formula:

$$C = M^e(modn)$$

$$C = 10^7(mod187)$$

$$C = 175$$

Thus,

$$\boxed{C = 175}$$

**Decryption Process**

Use the private key:

$$M = C^d(modn)$$

$$M = 175^{23}(mod187)$$

$$M = 10$$

Hence the original message is recovered.

**Question:** Given $p = 17$, $q = 11$, and $e = 7$, generate the RSA public and private keys. Then encrypt and decrypt the message "HELLO" and verify the result.

**Solution:**

**Step 1: Generate RSA Keys**

Choose two prime numbers:

$$p = 17, q = 11$$

Calculate:

$$n = p \times q = 17 \times 11 = 187$$

Compute Euler's Totient Function:

$$\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$$

Choose public exponent:

$$e = 7$$

Find private exponent dsuch that

$$ed \equiv 1(\mathrm{mod}160)$$
$$7 \times 23 = 161 = 1 + 160$$

Therefore,

$$d = 23$$

**Keys**

Public Key = (7, 187)

Private Key = (23, 187)

**Step 2: Convert HELLO into Numbers**

Using the alphabet numbering:

| **Letter** | **Number** |
|---|---|
| H | 8 |
| E | 5 |
| L | 12 |
| L | 12 |
| O | 15 |

Message: $\mathrm{HELLO} = (8,5,12,12,15)$

**Step 3: Encrypt Each Letter**

RSA Encryption Formula:

$$C = M^e(\mathrm{mod}n)$$

where $e = 7$and $n = 187$.

**Encrypt H = 8**

$$C = 8^7(\mathrm{mod}187)$$
$$8^7 = 2097152$$
$$2097152(\mathrm{mod}187) = 134$$

**Encrypt E = 5**

$$5^7 (\text{mod} 187) = 146$$

**Encrypt L = 12**

$$12^7 (\text{mod} 187) = 177$$

**Encrypt O = 15**

$$15^7 (\text{mod} 187) = 93$$

**Ciphertext**

$$(134,\ 146,\ 177,\ 177,\ 93)$$

So, the encrypted form of **HELLO** is:

$$134\ 146\ 177\ 177\ 93$$

**Step 4: Decryption**

Use RSA Decryption Formula:

$$M = C^d (\text{mod} n)$$

Where,

$$d = 23, n = 187$$

Decrypting:

$$134^{23} (\text{mod} 187) = 8$$
$$146^{23} (\text{mod} 187) = 5$$
$$177^{23} (\text{mod} 187) = 12$$
$$177^{23} (\text{mod} 187) = 12$$
$$93^{23} (\text{mod} 187) = 15$$

Recovered numbers:

$$(8,\ 5,\ 12,\ 12,\ 15)$$

Converting back to letters:

| **Number** | **Letter** |
|---|---|
| 8 | H |
| 5 | E |
| 12 | L |
| 12 | L |
| 15 | O |

Therefore, HELLO is successfully recovered.

**Summary**

- Original Message: **HELLO**
- Numerical Form: **(8,5,12,12,15)**
- Public Key: **(7,187)**
- Private Key: **(23,187)**
- Ciphertext: **(134,146,177,177,93)**
- Decrypted Message: **HELLO**

This example demonstrates how RSA encrypts and decrypts each character of a message using public and private keys.

## 15.4 ELGAMAL CRYPTOSYSTEM

ElGamal Cryptosystem

ElGamal encryption is based on Number Theory and the difficulty of solving the Discrete Logarithm Problem.

Key Generation

1. Choose a large prime $p$.
2. Select a primitive root $g$ modulo $p$.
3. Choose a private key $x$.
4. Compute:

$$y = g^x \pmod{p}$$

- Public Key: $(p, g, y)$
- Private Key: $x$

Encryption

For message $M$:

1. Choose a random integer $k$.
2. Compute:

$$C_1 = g^k \pmod{p}$$

3. Compute:

$$C_2 = M \cdot y^k \pmod{p}$$

Ciphertext:

$$(C_1, C_2)$$

Decryption

Compute:

$$M = C_2 (C_1^x)^{-1} \pmod{p}$$

Example

Let:

- $p = 23$
- $g = 5$
- $x = 6$

Public key:

$$y = 5^6 \pmod{23} = 8$$

Message:

$$M = 10$$

Choose:

$$k = 3$$

Encryption:

$$C_1 = 5^3 (\text{mod} 23) = 10$$
$$C_2 = 10 \times 8^3 (\text{mod} 23) = 10 \times 6 (\text{mod} 23) = 14$$

Ciphertext:

$$(10, 14)$$

Decryption:

$$M = 14(10^6)^{-1} (\text{mod} 23) = 10$$

Original message is recovered.

---

Comparison of RSA and ElGamal

| Feature | RSA | ElGamal |
|---|---|---|
| Mathematical Basis | Integer Factorization | Discrete Logarithm |
| Key Type | Public Key | Public Key |
| Encryption Formula | $C = M^e (\text{mod} n)$ | $(C_1, C_2)$ |
| Decryption Formula | $M = C^d (\text{mod} n)$ | $M = C_2 (C_1^x)^{-1} (\text{mod} p)$ |
| Security Based On | Factoring Large Integers | Discrete Logarithm Problem |
| Ciphertext Size | Smaller | Larger |

Conclusion

RSA and ElGamal are two important cryptographic algorithms based on Number Theory. RSA relies on the difficulty of factoring large integers, while ElGamal relies on the discrete logarithm problem. Both provide secure encryption and decryption mechanisms and form the foundation of modern secure communication systems.

## 15.5 *DIFFIE–HELLMAN KEY EXCHANGE*

The Diffie–Hellman Key Exchange (DHKE) is a cryptographic protocol introduced by Whitfield Diffie and Martin Hellman in 1976. It allows two parties to establish a shared secret key over an insecure communication channel without previously sharing any secret information.

The security of the Diffie–Hellman Key Exchange is based on the Discrete Logarithm Problem.

**Mathematical Background**

Let $p$ be a large prime number and $g$ be a primitive root modulo $p$.

These values are public and known to everyone.

Suppose two users:

- Alice
- Bob

wish to communicate securely.

**Diffie–Hellman Algorithm**

**Step 1:** Public Parameters

Choose

$$p = \text{large prime}$$
$$g = \text{primitive root modulo } p$$

Both $p$ and $g$ are public.

**Step 2:** Alice Chooses a Secret Key

Alice selects a private integer

$$a$$

and computes

$$A = g^a \pmod{p}$$

She sends $A$ to Bob.

**Step 3:** Bob Chooses a Secret Key

Bob selects a private integer

$$b$$

and computes

$$B = g^b \pmod{p}$$

He sends $B$ to Alice.

**Step 4:** Alice Computes the Shared Key
Using Bob's public value $B$,

$$K_A = B^a (\mathrm{mod} p)$$

Substituting $B = g^b$,

$$K_A = (g^b)^a (\mathrm{mod} p)$$
$$K_A = g^{ab} (\mathrm{mod} p)$$

**Step 5:** Bob Computes the Shared Key
Using Alice's public value $A$,

$$K_B = A^b (\mathrm{mod} p)$$

Substituting $A = g^a$,

$$K_B = (g^a)^b (\mathrm{mod} p)$$
$$K_B = g^{ab} (\mathrm{mod} p)$$

**Proof of Correctness:**
We must prove that Alice and Bob obtain the same secret key.
Alice computes:

$$K_A = (g^b)^a (\mathrm{mod} p)$$

Using exponent laws,

$$K_A = g^{ba} (\mathrm{mod} p)$$

Since multiplication is commutative,

$$ab = ba$$

Therefore,

$$K_A = g^{ab} (\mathrm{mod} p)$$

Bob computes:

$$K_B = (g^a)^b (\mathrm{mod} p)$$

Again,

$$K_B = g^{ab} (\mathrm{mod} p)$$

Hence,

$$K_A = K_B$$

Thus, both users obtain the same shared secret key.
Therefore, the Diffie–Hellman Key Exchange is correct.
Numerical Example
Let

$$p = 23$$
$$g = 5$$

These values are public.
Alice's Computation
Choose private key

$$a = 6$$

Compute

$$A = 5^6 (\mathrm{mod} 23)$$
$$5^2 = 25 \equiv 2(\mathrm{mod} 23)$$
$$5^4 = 2^2 = 4$$
$$5^6 = 5^4 \times 5^2$$
$$= 4 \times 2 = 8$$

Thus

$$A = 8$$

Alice sends 8 to Bob.
Bob's Computation
Choose private key

$$b = 15$$

Compute

$$B = 5^{15} (\mathrm{mod} 23)$$

Using repeated squaring:

$$5^1 \equiv 5$$
$$5^2 \equiv 2$$
$$5^4 \equiv 4$$
$$5^8 \equiv 16$$
$$5^{15} = 5^8 \cdot 5^4 \cdot 5^2 \cdot 5$$
$$= 16 \times 4 \times 2 \times 5$$
$$= 640$$
$$640 \equiv 19(\mathrm{mod} 23)$$

Thus

$$B = 19$$

Bob sends 19 to Alice.

Alice Computes Shared Key
Received $B = 19$.

$$K_A = 19^6 (\text{mod} 23)$$
$$19^2 = 361 \equiv 16$$
$$19^4 = 16^2 = 256 \equiv 3$$
$$19^6 = 19^4 \times 19^2$$
$$= 3 \times 16$$
$$= 48$$
$$48 \equiv 2(\text{mod} 23)$$

Hence

$$K_A = 2$$

Bob Computes Shared Key
Received $A = 8$.

$$K_B = 8^{15} (\text{mod} 23)$$

Using repeated squaring:

$$8^2 = 64 \equiv 18$$
$$8^4 = 18^2 = 324 \equiv 2$$
$$8^8 = 2^2 = 4$$
$$8^{15} = 8^8 \cdot 8^4 \cdot 8^2 \cdot 8$$
$$= 4 \times 2 \times 18 \times 8$$
$$= 1152$$
$$1152 \equiv 2(\text{mod} 23)$$

Therefore

$$K_B = 2$$

Verification
Alice obtained:

$$K_A = 2$$

Bob obtained:

$$K_B = 2$$

Thus

$$K_A = K_B = 2$$

The common secret key is 2 .

Why an Attacker Cannot Find the Key
An eavesdropper knows:

$$p = 23, \quad g = 5, \quad A = 8, \quad B = 19$$

but does not know:

$$a = 6, b = 15$$

To compute the shared key, the attacker must determine either $a$or $b$from

$$A = g^a \pmod{p}$$

or

$$B = g^b \pmod{p}$$

This requires solving the Discrete Logarithm Problem, which is computationally difficult for very large prime numbers.

**MCQ QUESTIONS:**

**1.** RSA is an example of which type of cryptographic algorithm?
A) Symmetric Key Cryptography
B) Public Key Cryptography
C) Hash Function
D) Stream Cipher

**2.** RSA stands for:

A) Rivest-Shamir-Adleman
B) Rivest-Secure-Algorithm
C) Random-Security-Algorithm
D) Rivest-Shannon-Adleman

**3.** RSA was introduced in:
A) 1975
B) 1976
C) 1977
D) 1980

**4.** RSA is primarily based on the difficulty of:
A) Solving linear equations
B) Factoring large integers
C) Finding square roots
D) Matrix multiplication

**5.** In RSA, the public key consists of:
A) (d, n)
B) (p, q)
C) (e, n)
D) (e, d)

**6.** In RSA, the private key consists of:
A) (e, n)
B) (d, n)
C) (p, q)
D) (e, d)

**7.** The value of $n$ in RSA is:
A) $p + q$
B) $p - q$
C) $p \times q$
D) $p^q$

**8.** Euler's Totient Function for RSA is:
A) $p + q$
B) $(p - 1)(q - 1)$
C) $pq$
D) $p^2 + q^2$

**9.** The encryption formula in RSA is:

A) $C = M + d$
B) $C = M^e (\mathrm{mod} n)$
C) $C = M^d (\mathrm{mod} n)$
D) $C = e^M$

**10.** The decryption formula in RSA is:
A) $M = C^e (\mathrm{mod} n)$
B) $M = C + d$
C) $M = C^d (\mathrm{mod} n)$
D) $M = e^C$

**11.** Which mathematical theorem is fundamental to RSA?
A) Binomial Theorem
B) Euler's Theorem
C) Mean Value Theorem
D) Green's Theorem

**12.** In RSA, the public exponent $e$must satisfy:
A) $e > n$
B) $gcd(e, \phi(n)) = 1$
C) $e = \phi(n)$
D) $e = n$

**13.** The private exponent $d$satisfies:
A) $ed = 0$
B) $ed = n$
C) $ed \equiv 1 (\mathrm{mod} \phi(n))$
D) $d = e$

**14.** Which of the following is NOT an application of RSA?
A) Digital Signatures
B) Secure E-mail
C) HTTPS
D) Data Compression

**15.** RSA is generally slower than:
A) Hashing Algorithms
B) Symmetric Key Algorithms
C) Block Ciphers Only
D) Stream Ciphers Only

**16.** Which pair of numbers is used to generate RSA keys?

A) Two composite numbers
B) Two prime numbers
C) Two even numbers
D) Two odd numbers

**17.** If $p = 11$and $q = 13$, then $n$equals:
A) 24
B) 121
C) 143
D) 169

**18.** If $p = 11$and $q = 13$, then $\phi(n)$equals:
A) 120
B) 143
C) 110
D) 132

19. RSA provides:
A) Confidentiality only
B) Authentication only
C) Confidentiality and Digital Signatures
D) Compression and Authentication

20. Which of the following attacks threatens RSA if small keys are used?
A) Brute-force factorization attack
B) SQL Injection
C) Phishing Attack
D) Trojan Attack

21. RSA belongs to:
A) Secret Key Cryptography
B) Asymmetric Key Cryptography
C) Classical Cryptography
D) Transposition Cipher

22. Which key is used for encryption in RSA?
A) Private Key
B) Secret Key
C) Public Key
D) Session Key

23. Which key is used for decryption in RSA?

A) Public Key
B) Session Key
C) Secret Key
D) Private Key

24. The security of RSA increases when:
A) Smaller primes are used
B) Larger prime numbers are used
C) $e = 1$is chosen
D) $p = q$

25. RSA is widely used in:
A) Secure Internet Communication
B) Operating System Scheduling
C) Database Indexing
D) Image Compression

26. Assertion–Reason
Assertion (A): RSA is an asymmetric cryptographic algorithm.
Reason (R): RSA uses different keys for encryption and decryption.
A) Both A and R are true and R is the correct explanation of A.
B) Both A and R are true but R is not the correct explanation of A.
C) A is true but R is false.
D) A is false but R is true.

## 15.7 *SUMMARY*

(i) RSA is a secure public-key cryptographic algorithm that uses mathematical principles of number theory and prime factorization to provide secure communication, authentication, and digital signatures in modern computer networks.

(ii) The RSA Algorithm is one of the most widely used public-key (asymmetric) cryptographic algorithms for securing digital communication. It was developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, whose initials form the name RSA. RSA uses a pair of keys: A Public Key for encryption, A Private Key for decryption. The algorithm is based on the mathematical difficulty of factoring large composite numbers into their prime factors. RSA key generation involves selecting two large prime numbers, computing their product $n$, determining Euler's Totient Function $\phi(n)$, choosing a public exponent $e$, and calculating the private exponent $d$.

## *15.8 GLOSSARY*

1. Arithmetic Function
2. Number Theoretic
3. Divisor
4. Prime Number
5. Composite Number
6. Greatest Common Divisor (GCD)
7. Relatively Prime (Coprime)

## 15.9 *REFERENCES AND SUGGESTED READINGS*


- **Burton, D. M.** (2007). Elementary number theory (6th ed.), McGraw-Hill.
- **T. M. Apostol**, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford.
- **Tom M. Apostol**, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York.
- **G. A. Jones and J. M. Jones**, *Elementary Number Theory*, Springer-Verlag, Berlin, 1998.
- **T. Nagell**, *Introduction to Number Theory*, Wiley, New York.


## 15.10 *TERMINAL QUESTIONS*

**Long answer type questions**

1. Explain RSA Algorithm with a numerical example.
2. Describe the key generation process in RSA.
3. Prove the correctness of RSA using Euler's theorem.
4. Explain RSA encryption and decryption with an example.
5. Discuss applications, advantages, and limitations of RSA.
6. Compare RSA with symmetric key cryptography.
7. Explain the role of prime numbers in RSA security.

8. Describe the mathematical foundations of RSA cryptosystem.
9. Write short notes on public key and private key in RSA.
10. Why is factorization important in RSA security? Explain.

## 15.10 *ANSWERS*

**Answer of objective questions**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1:** | B | **2:** | A | **3:** | C | **4:** | B |
| **5:** | C | **6:** | B | **7:** | C | **8:** | B |
| **9:** | B | **10:** | C | **11:** | B | **12:** | B |
| **13:** | C | **14:** | D | **15:** | B | **16:** | B |
| **17:** | C | **18:** | A | **19:** | C | **20:** | A |
| **21:** | B | **22:** | C | **23:** | D | **24:** | B |
| **25:** | A | **26:** | A | | | | |


**Teen Pani Bypass Road, Transport Nagar**
**Uttarakhand Open University,**
**Haldwani, Nainital-263139**
**Phone No. 05946-261122, 261123**
**Toll free No. 18001804025**
**Fax No. 05946-264232,**

**E-mail:info@uou.ac.in**
**Website: https://www.uou.ac.in/**