PG MA S4-02 (DSC)

TWO YEAR MASTER'S DEGREE COURSE

(CBCS in Accordance with NEP 2020)

SEMESTER - IV

NUMBER THEORY

MATHEMATICS

Hiranya Chandra Bhuyan School of Science and Technology

KRISHNA KANTA HANDIQUI STATE OPEN UNIVERSITY

Subject Expert

Prof. Bipan Hazarika, Gauhati University

Prof. Nazibuddin Ahmed, Gauhati University

Prof. Dipak Sarma, Cotton University

Dr. Dilip Kumar Sarma, Cotton University

Course Co-ordinator : Dr. Harekrishna Deka, KKHSOU

SLM Preparation Team

UNITS	CONTRIBUTORS
1, 2,3,4,5,6,7,8	Dr. Shahidul Islam Khan, PDUAM, Amjonga
9,10,11	Dr. Harekrishna Deka, KKHSOU
12,13,14	Mr Dipankar Basak,Behali Degree College,Behali

Editorial Team

Content : **Dr. Dilip Kumar Sarma,** Cotton University

Structure, Format & Graphics:**Dr. Harekrishna Deka,** KKHSOU

May, 2026 ***ISBN:***

This Self Learning Material (SLM) of the Krishna Kanta Handiqui State Open University is made available under a Creative Commons Attribution-NonCommercial-ShareAlike4.0 License (international): http://creativecommons.org/licenses/by-nc-sa/4.0/

Printed and published by Registrar on behalf of the Krishna Kanta Handiqui State Open University.

The University acknowledges with thanks the financial support provided by the **Distance Education Council**, New Delhi, for the preparation of this study material.

Head Office : Patgaon, Rani Gate, Guwahati-781017
City Office : Resham Nagar, Khanapara, Guwahati-781 022; Web: www.kkhsou.in

CONTENTS

		PAGES
UNIT 1 :	**BASIC CONCEPTS**	**7-24**
	Division algorithm, Greatest common divisor, Euclidean algorithm, least common multiple, Kronecker's theorem	
UNIT 2 :	**DIVISIBILITY THEORY**	**25-44**
	Divisibility, Tests of divisibility	
UNIT 3 :	**PRIMES AND THEIR DISTRIBUTION**	**45-62**
	Prime numbers, Fundamental theorem of arithmetic	
UNIT 4 :	**THEORY OF CONGRUENCE-I**	**63-80**
	Congruence, Basic properties of congruence, Residue system, Linear congruence	
UNIT 5 :	**THEORY OF CONGRUENCE-II**	**81-98**
	Solvability condition of a system of linear congruence, The linear Diophantine theorem, The Chinese Remainder Theorem	
UNIT 6 :	**FERMAT'S THEOREM**	**99-121**
	Fermat's factorization method, Fermat's little theorem, Wilson's theorem, Euler's factorization method	
UNIT 7 :	**NUMBER THEORETIC FUNCTIONS-I**	**122-159**
	The function τ and σ,The mobius function, The greatest integer function, Euler's function, Some properties of Euler's function	
UNIT 8 :	**NUMBER THEORETIC FUNCTIONS-II**	**160-184**
	Function $T(n), S(n), \zeta(n), \phi(n)$	
UNIT 9:	**PRIMITIVE ROOTS AND INDICES**	**185-211**
	The order of an integer modulo n,Primitive roots, Primitive roots for primes, Composite numbers having primitive roots, The theory of indices	

UNIT 10: QUADRATIC CONGRUENCE AND QUADRATIC RECIPROCITY LAW **212-254**

Quadratic congruence, Quadratic residue, Euler's residue, Legendre symbol and its properties, Quadratic reciprocity, Quadratic congruences with composite module, Jacobi symbol

UNIT 11: PERFECT NUMBERS **255-274**

Perfect numbers, Mersenne primes, Fermat number, Pythagorean triples, Other Diophantine equation, Fermat's last theorem

UNIT 12: SUM OF SQUARE OF INTEGERS **275-292**

Sum of two square, Sum of more than two squares

UNIT 13: PARTITIONS **293-311**

Introduction, Graphical Representation, Euler's Partition Theorem, Searching for Partition Identities

UNIT 14: FAREY SEQUENCES AND CONTINUED FRACTIONS **312-350**

Farey Sequence, Continued Fractions, Finite Continued Fractions, Infinite Continued Fractions, Application to Equations, Pell's Equation, Fibonacci Numbers, Fibonacci Sequence, Certain Identities involving Fibonacci Numbers

COURSE INTRODUCTION

"**Number Theory**" is a Discipline-Specific Core (DSC) course offered in the fourth semester of the M.Sc. Mathematics programme.

Number Theory is one of the oldest and most fascinating branches of mathematics that studies the properties and relationships of integers. It deals with concepts such as divisibility, prime numbers, congruences, Diophantine equations, partitions, and continued fractions. The subject has deep theoretical importance as well as modern applications in cryptography, coding theory, computer science, information security, and computational mathematics.""This course is designed to provide learners with a comprehensive understanding of classical and modern topics in number theory. It introduces fundamental arithmetic concepts, explores the properties of prime numbers and congruences, and discusses advanced topics such as quadratic reciprocity, partitions, continued fractions, and Fibonacci sequences. The course also develops logical reasoning, proof techniques, and problem-solving skills in abstract mathematics.

The course is divided into the following units:

Unit 1: Basic Concepts

This unit introduces the foundational concepts of number theory, including the division algorithm, greatest common divisor (GCD), Euclidean algorithm, least common multiple (LCM), and Kronecker's theorem. These concepts form the basis for the study of divisibility and arithmetic properties of integers.

Unit 2: Divisibility Theory

This unit discusses the theory of divisibility and various tests of divisibility. Learners will study how integers divide one another and understand important divisibility properties that are essential in elementary and advanced number theory.

Unit 3: Primes and Their Distribution

This unit focuses on prime numbers and their significance in mathematics. It includes the Fundamental Theorem of Arithmetic, which states that every positive integer can be uniquely expressed as a product of prime numbers. The unit also discusses the distribution and properties of primes.

Unit 4: Theory of Congruence-I

This unit introduces congruence relations and their basic properties. Learners will study residue systems and linear congruences, which are fundamental tools in modular arithmetic and cryptographic applications.

Unit 5: Theory of Congruence-II

This unit extends the study of congruences to systems of linear congruences and Diophantine equations. Important results such as the Chinese Remainder Theorem and solvability conditions for congruences are discussed, highlighting their applications in computational mathematics.

Unit 6: Fermat's Theorem

This unit introduces important results related to Fermat's theorem, including Fermat's factorization method, Fermat's little theorem, Wilson's theorem, and Euler's factorization method. These theorems play a central role in divisibility theory and modular arithmetic.

Unit 7: Number Theoretic Functions-I

This unit discusses important number theoretic functions such as the Möbius function, Euler's phi function, and the greatest integer function. Learners will also study various properties and applications of Euler's function in number theory.

Unit 8: Number Theoretic Functions-II

This unit continues the study of arithmetic functions and introduces additional number theoretic functions and their properties. These functions are useful in understanding the structure and behavior of integers.

Unit 9: Primitive Roots and Indices

This unit introduces the concepts of order modulo an integer, primitive roots, and the theory of indices. Learners will study primitive roots for prime and composite numbers and their importance in modular arithmetic and cryptographic systems.

Unit 10: Quadratic Congruence and Quadratic Reciprocity Law

This unit focuses on quadratic congruences, quadratic residues, Legendre symbols, Jacobi symbols, and the law of quadratic reciprocity. These topics are among the most significant results in classical number theory and have deep mathematical importance.

Unit 11: Perfect Numbers

This unit discusses perfect numbers, Mersenne primes, Fermat numbers, and Pythagorean triples. It also introduces Diophantine equations and Fermat's Last Theorem, one of the most famous problems in mathematics.

Unit 12: Sum of Squares of Integers

This unit studies representations of integers as sums of squares. Topics include the sum of two squares and sums of more than two squares, which are important in algebraic and analytic number theory.

Unit 13: Partitions

This unit introduces the theory of partitions and their graphical representations. Learners will study Euler's Partition Theorem and techniques for discovering partition identities, which are important topics in combinatorial number theory.

Unit 14: Farey Sequences and Continued Fractions

This unit discusses Farey sequences and continued fractions, including finite and infinite continued fractions. Applications to equations such as Pell's equation and the study of Fibonacci numbers and identities are also included. These topics demonstrate important connections between number theory and mathematical analysis.

Each unit includes some along-side boxes to help you know some of the difficult, unseen terms. Some "EXERCISES" have been included to help you apply your own thoughts. You may find some boxes marked with: "LET US KNOW". These boxes will provide you with some additional interesting and relevant information. Again, you will get "CHECK YOUR PROGRESS" questions. These have been designed to self-check your progress of study. It will be helpful for you if you solve the problems put in these boxes immediately after you go through the sections of the units and then match your answers with "ANSWERS TO CHECK YOUR PROGRESS" given at the end of each unit.