DISCIPLINE SPECIFIC ELECTIVE COURSE-1(iii): NUMBER THEORY

CREDIT DISTRIBUTION, ELIGIBILITY AND PRE-REQUISITES OF THE COURSE

Course title & Code	Credits	Credit distribution of the course			Eligibility criteria	Pre-requisite of the course (if any)
		Lecture	Tutorial	Practical/ Practice		
Number Theory	4	3	1	0	Class XII pass with Mathematics	Algebra

Learning Objectives

The primary objective of this course is to introduce:

- The number theoretic techniques of computations with the flavour of abstraction.
- The Euclidean algorithm, linear Diophantine equations, congruence equations, arithmetic functions and their applications, Fermat's little, Euler's and Wilson's theorems.
- Primitive roots, quadratic residues and nonresidues, the Legendre symbol and the law of Quadratic Reciprocity.
- Introduction to cryptography, public-key cryptosystems and applications.

Learning Outcomes

This course will enable the students to:

- Use modular arithmetic in solving linear and system of linear congruence equations.
- Work with the number theoretic functions, their properties and their use.
- Learn the forms of positive integers that possess primitive roots and the Quadratic Reciprocity Law which deals with the solvability of quadratic congruences.
- Understand the public-key cryptosystems, in particular, RSA.

SYLLABUS OF DSE - 1(iii)

Unit – 1 **(12 hours)**

Linear Diophantine equation and Theory of Congruences

The Euclidean Algorithm and linear Diophantine equation; Least non-negative residues and complete set of residues modulo n; Linear congruences, The Chinese remainder theorem and system of linear congruences in two variables; Fermat's little theorem, Wilson's theorem and its converse, Application to solve quadratic congruence equation modulo odd prime p.

Unit – 2 **(21 hours)**

Number-Theoretic Functions and Primitive Roots

Number-theoretic functions for the sum and number of divisors, Multiplicative function, Möbius inversion formula and its properties; Greatest integer function with an application to the calendar; Euler's Phi-function, Euler's theorem and some properties of the Phi-function; The order of an integer modulo n and primitive roots for primes, Primitive roots of composite numbers n: when n is of the form 2^k, and when n is a product of two coprime numbers.

Unit – 3 **(12 hours)**

Quadratic Reciprocity Law and Public Key Cryptosystems

The quadratic residue and nonresidue of an odd prime and Euler's criterion, The Legendre symbol and its properties, Quadratic Reciprocity law and its application; Introduction to cryptography, Hill's cipher, Public-key cryptography and RSA.

Essential Reading

1. Burton, David M. (2011). Elementary Number Theory (7th ed.). McGraw-Hill Education Pvt. Ltd. Indian Reprint 2017.

Suggestive Readings

- Andrews, George E. (1994). Number Theory. Dover publications, Inc. New York.
- Robbins, Neville (2007). Beginning Number Theory (2nd ed.). Narosa Publishing House Pvt. Ltd. Delhi.
- Rosen, Kenneth H. (2011). Elementary Number Theory and its Applications (6th ed.). Pearson Education. Indian Reprint 2015.

Note: Examination scheme and mode shall be as prescribed by the Examination Branch, University of Delhi, from time to time.