**Suggested Readings**


- Brualdi, Richard A. (2009). Introductory Combinatorics (5th ed.). Pearson Education Inc.
- Cameron, Peter J. (1994). Combinatorics: Topics, Techniques, Algorithms. Cambridge University Press.


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

## DISCIPLINE SPECIFIC ELECTIVE COURSE-1(ii): ELEMENTS OF 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 | | |
| Elements of Number Theory | 4 | 3 | 1 | 0 | Class XII pass with Mathematics | Nil |

### Learning Objectives

The primary objective of this course is to introduce:

- The Euclidean algorithm and linear Diophantine equations, the Fundamental theorem of arithmetic and some of the open problems of number theory viz. the Goldbach conjecture.
- The modular arithmetic, linear congruence equations, system of linear congruence equations, arithmetic functions and multiplicative functions, e.g., Euler's Phi-function.
- Introduction of the simple encryption and decryption techniques, and the numbers of specific forms viz. Mersenne numbers, Fermat numbers etc.

### Learning Outcomes

This course will enable the students to:

- Get familiar with the basic number-theoretic techniques.
- Comprehend some of the open problems in number theory.
- Learn the properties and use of number-theoretic functions and special types of numbers.
- Acquire knowledge about public-key cryptosystems, particularly RSA.

### SYLLABUS OF DSE-1(ii)

**Unit – 1** **(12 hours)**

**Divisibility and Prime Numbers**

Revisiting: The division algorithm, divisibility and the greatest common divisor. Euclid's lemma; The Euclidean algorithm, Linear Diophantine equations; The Fundamental theorem of Arithmetic, The sieve of Eratosthenes, Euclid theorem and the Goldbach conjecture; The Fibonacci sequence and its nature.

**Unit – 2** **(21 hours)**

**Theory of Congruences and Number-Theoretic Functions**

Congruence relation and its basic properties, Linear congruences and the Chinese remainder theorem, System of linear congruences in two variables; Fermat's little theorem and its generalization, Wilson's theorem and its converse; Number-theoretic functions for sum and the number of divisors of a positive integer, Multiplicative functions, The greatest integer function; Euler's Phi-function and its properties.

**Unit – 3** **(12 hours)**

**Public Key Encryption and Numbers of Special Form**

Basics of cryptography, Hill's cipher, Public-key cryptosystems and RSA encryption and decryption technique; Introduction to perfect numbers, Mersenne numbers and Fermat numbers.

**Essential Reading**

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

**Suggestive Readings**


- Jones, G. A., & Jones, J. Mary. (2005). Elementary Number Theory. Springer Undergraduate Mathematics Series (SUMS). Indian Reprint.
- 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.**

## DISCIPLINE SPECIFIC ELECTIVE COURSE - DSE-1(iii): THEORY OF EQUATIONS AND SYMMETRIES

**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 | | |
| Theory of Equations and Symmetries | 4 | 3 | 1 | 0 | Class X pass with Mathematics | Nil |

**Learning Objectives**

The goal of this paper is to acquaint students with certain ideas about:

- Integral roots, rational roots, an upper bound on number of positive or negative roots of a polynomial.
- Finding roots of cubic and quartic equations in special cases using elementary symmetric functions.
- Using Cardon's and Descartes' methods, respectively.