

Approval: 8th Senate Meeting

Course Name : Number Theory

Course Number : MA552

Credit : 3-0-0-3

Students intended for: UG/PG

Semester :Even/Odd

Prerequisites :

Elective or Compulsory: Elective

Prerequisites

Course Preamble: This one semester course is designed to study the fundamentals of Number Theory and to demonstrate its applications in some real world phenomena. Upon completion of the course, students will have a working knowledge of the fundamental definitions and theorems of elementary number theory, be able to work with congruences, solve congruence equations and systems of equations with one and more variables, and be literate in the language and notation of number theory.

Course Outline:

[10 Lectures]

Introduction & Divisibility Theory: Basics, Divisibility, Euclidean Algorithm, Primes and their Distribution, Prime Number Theorem (without proof). Congruences, Linear Congruences and Congruences with prime modulus, Some Diophantine Equations, The Chinese remainder theorem.

[8 Lectures]

Number Theoretic Functions & Applications: Arithmetic functions and the Möbius inversion formula, Greatest Integer Function, Sum of integer squares and Applications.

[10 Lectures]

Fermat's Theorem & Primitive Roots: Fermat's little theorem, Euler and Wilsons Theorems, Primitive Roots, Indices, Quadratic Reciprocity, Legendre Symbol, Gauss Theorem.

[10 Lectures]

Applications to Cryptography & Special Topics: Applications to Primality Testing, RSA & cryptography, Fibonacci Numbers, Numbers of Special Form, Continued Fractions and Rational Approximations.

Text books

1. Elementary Number Theory by D. Burton, seventh edition, McGraw Hill, 2012.

Reference Books

1. Elementary Number Theory and its Applications by Kenneth Rosen, 4th Edition, Addison-Wesley, 2000.
2. An Introduction to the Theory of Numbers by I. Niven, H.S. Zuckerman and Hugh L. Montgomery, 5th Edition, Wiley, 1991.