Under-Graduate Programme with MATHEMATICS; 4th Semester

MATHEMATICS **MAJOR COURSE**
MMT426J3: Theory of numbers and Polynomial Equations **Credits: 6 (4-TH + 2- TUT)**
Theory: 4 Credits (60 Hours) **Tutorial: 2 Credits (30 Hours)**

Course Objectives: To build up the basic theory of the integers, prime numbers and their primitive roots, the theory of congruence, number theoretic functions, Fermat's last theorem, to acquire knowledge in cryptography especially in RSA encryption and decryption.

Course Outcome: Upon successful completion of this course students will able to know the basic definitions and theorems in number theory, to solve congruences, linear diophantine equations, primitive roots, Euler's criterion, to understand modular arithmetic number-theoretic functions and apply them to cryptography.

Theory: 4 Credits

Unit –I

Arithmetic Properties of Integers, Fundamental theorem of arithmetic's, sequence of primes, Goldbach conjecture, Euclid's division algorithm, GCD and LCM of integers and their properties, Euclid's first theorem.

Unit –II

Linear Diophantine equations. Necessary and sufficient condition for solvability of linear Diophantine equations, Positive solutions. Linear Congruence's, solutions and applications, Euclid's Second theorem, Fermat Numbers and their properties. Fermat's Last Theorem (statements only).

Unit –III

Complete Residue System (*CRS*), Reduced Residue System (*RRS*) and their properties. Fermat and Euler's theorems with applications. Number theoretic functions, Euler's ϕ-function, $\phi(mn) = \phi(m)\phi(n)$ where $(m, n) = 1$, $\Sigma\phi(d) = n$, $\phi(m) = m\prod(1 - \frac{1}{p})$ for $m > 1$. Chinese Remainder theorem with applications. Order of an integer modulo *n.*

Unit –IV

Theory of polynomial equations; remainder and factor theorems; synthetic division; relation between roots and coefficients; complex roots and their properties; fundamental theorem of algebra; solutions of cubic and biquadratic equations; Descartes' rule of signs.

Tutorial: 2 Credits

Unit –V

Problems on divisibility, prime numbers, fundamental theorem of arithmetic, Euclid's division algorithm, GCD and LCM, and basic properties of integers.
Problems on linear Diophantine equations, conditions for solvability, positive solutions, linear congruences, and applications.

Unit –VI

Problems on complete and reduced residue systems, Euler's phi-function, Fermat's and Euler's theorems, Chinese Remainder Theorem, and order of an integer modulo n.
Problems on remainder and factor theorems, synthetic division, relations between roots and coefficients, complex roots, solutions of cubic and biquadratic equations, and Descartes' rule of signs.

Recommended Books:

1. Aziz and Nisar, Theory of Equations, Kapoor and Son's, Srinagar.
2. W. J. Leveque, Topics in Number Theory, Vol (I & II) Addition Wesley Publishing Company, INC.
3. Niven and H.S Zuckerman, An introduction of the Theory of Numbers.
4. T. M. Apostal, Analytic Number Theory, Springer Verlag.
5. G.H Hardy and Wright, An introduction to the theory of Numbers.
6. Theory of Equations, C.C. Mac Duffee, John Wiley and Sons Inc., 1954.