THEORY OF NUMBERS-I

Course No: **MM24106DCE** Total Credits: **04**

Semester: **M.A/M.Sc 1st Semester** Total Marks: **100**

Continuous Assessment: **Marks 20**, **Theory Marks: 80** Time Duration: **2½ Hrs Course**

Course objectives: To equip the student with the properties of numbers and the relationship between different sorts of numbers in order to tackle different problems arising in discrete systems.

Course Outcomes: By the end of this course, students should be able to analyze modular arithmetic and congruence relations, solving linear congruence's and applying them to various problems. It will give an introductory understanding of number theory's role in cryptography, including the encryption schemes.

UNIT-I

Divisibility, the division algorithm and its uniqueness, Greatest common divisor and its properties. The Euclidean algorithm, Prime numbers. Euclid's first theorem, Fundamental Theorem of Arithmetic, Divisor of n, Radix-representation. Linear Diophantine equations. Necessary and sufficient condition for solvability of linear Diophantine equations, Positive solutions.

UNIT-II

Sequence of primes, Euclid's Second theorem, Infinitude of primes of the form 4n+3 and of the form 6n+5. No polynomial f(x) with integral coefficients can represent primes for all integral values of x or for all sufficiently large x. Fermat Numbers and their properties. Fermat Numbers are relatively prime. There are arbitrary large gaps in the sequence of primes. Congruences, Complete Residue System (CRS), Reduced Residue System (RRS) and their properties. Fermat and Euler's theorems with applications.

UNIT-III

Euler's φ −function, $\varphi(mn) = \varphi(m)\varphi(n)$, where *gcd(m, n)* = 1, $\sum\varphi(d) = n$ and $\phi(m) = m\prod_{p}\left(1 - \frac{1}{p}\right)$ for $m > 1$**.** Wilson's theorem and its applications to the solution of the congruence $x^2 \equiv -1(modp)$. Solutions of linear congruences. The necessary and sufficient conditions for the solution of $a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv c(modm)$, Chinese remained theorem. Congruences of higher degree $F(x) \equiv 0(modm)$, where $F(x)$ is a polynomial. Congruences with prime power and related results. Lagranges theorem, viz, the polynomial congruence of degree n has at most *n* roots.

UNIT-IV

Factor theorem and its generalization. Polynomial congruences $F(x_1, x_2, \dots, x_n) \equiv 0(modp)$ in several variables. Equivalence of polynomials. Equivalence theorem on the number of solutions of congruences. Chavalley's theorem, Warning's theorem. Quadratic arms over a field of characteristic not equal to 2. Equivalence of quadratic forms, Witt's theorem. Representation of filled elements. Hermite's theorem on the minima of positive definite quadratic form and its applications to the sum of two, tree and four squares.

Recommended Books:

1. W. J. Leveque, Topics in Number Theory, Vol. I-, Dover Publications, 2002.
2. I Niven and H.S Zuckerman, An introduction of the Theory of Numbers, Wiley, 5th Edition 2008.
3. David M. Burton, Elementary Number Theory, McGraw Hill Higher Education, 6th Edition 2005.
4. G.H Hardy and Wright, An introduction to the theory of Numbers, Oxford University Press, 6th Edition 2008.