M.A/M.Sc Mathematics Semester 3rd

Effective from academic session 2011 ⟹ **Repetition for 2012 with minor change**

THEORY OF NUMBERS-I

Course No. MM-OP-305

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, ϕ (mn) = ϕ (m) ϕ (n) where (m, n) =1, $\sum_{d/m}\phi(d) = n$ and $\phi(m) = m\prod_{p}\left(1-\frac{1}{p}\right)$ for m>1. Wilson's theorem and its application to the solution the congruence of $x^2 \equiv -1 \pmod p$, Solutions of linear Congruence's. The necessary and sufficient condition for the solution of $a_1x_1+a_2x_2+\ldots+a_nx_n \equiv c \pmod m$. Chinese Remainder Theorm.Congruences of higher degree $F(x) \equiv 0 \pmod m$, where F(x) is a Polynomials. Congruence's with prime power, Congruences with prime modulus and related results. Lagrange's theorem, viz , the polynomial congruence $F(x) \equiv 0 \pmod p$ of degree n has at most n roots.

Unit IV

Factor theorem and its generalization. Polynomial congruences $F(x_1,x_2\ldots x_n) \equiv 0 \pmod p$ in several variables. Equivalence of polynomials. Theorem on the number of solutions of congruences: Chevalley's theorem, Warning's theorem. Quadratic forms over a field of characteristic $\neq 2$ Equivalence of Quadratic forms. Witt's theorem .Representation of Field Elements. Hermite's theorem on the minima of a positive definite quadratic form and its application to the sum of two squares.

Recommended Books:

1. Topics in number theory by W. J . Leveque, Vol. I and II Addition Wesley Publishing Company, INC.
2. An introduction of the Theory of numbers by I. Niven and H.S Zuckerman.
3. Number Theory by Boevich and Shaferivich, I.R, Academic Press.

Suggested Readings:

1. Analytic Number Theory by T.M Apostal, Springer Verlag.
2. An introduction to the theory of Numbers by G.H Hardy and Wright.
3. A course in Arithmetic, by J.P. Serre, GTM Vol. springer Verlag 1973.
4. An elementary Number theory of E. Landau.