PCS7D001 Computational Numbers Theory (HONOR SUBJECT)4-0-0

Module I

Algorithms for integer arithmetic: Divisibility, gcd, modular arithmetic, modular exponentiation, Montgomery arithmetic, congruence, Chinese remainder theorem, Hensel lifting, orders and primitive roots, quadratic residues, integer and modular square roots, prime number theorem, continued fractions and rational approximations.

Module II

Representation of finite fields: Prime and extension fields, representation of extension fields, polynomial basis, primitive elements, normal basis, optimal normal basis, irreducible polynomials.

Algorithms for polynomials: Root-finding and factorization, Lenstra-Lenstra-Lovasz algorithm, polynomials over finite fields.

Module III

Elliptic curves: The elliptic curve group, elliptic curves over finite fields, Schoof's point counting algorithm.

Primality testing algorithms: Fermat test, Miller-Rabin test, Solovay-Strassen test, AKS test.

Integer factoring algorithms: Trial division, Pollard rho method, p-1 method, CFRAC method, quadratic sieve method, elliptic curve method.

Module V

Computing discrete logarithms over finite fields: Baby-step-giant-step method, Pollard rho method, Pohlig-Hellman method, index calculus methods, linear sieve method, Coppersmith's algorithm.

Applications: Algebraic coding theory, cryptography.

References

1. V. Shoup, A computational introduction to number theory and algebra, Cambridge University Press.
2. M. Mignotte, Mathematics for computer algebra, Springer-Verlag.
3. I. Niven, H. S. Zuckerman and H. L. Montgomery, An introduction to the theory of numbers, John Wiley.
4. J. von zur Gathen and J. Gerhard, Modern computer algebra, Cambridge University Press.
5. R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press.
6. A. J. Menezes, editor, Applications of finite fields, Kluwer Academic Publishers.
7. J. H. Silverman and J. Tate, Rational points on elliptic curves, Springer International Edition.
8. D. R. Hankerson, A. J. Menezes and S. A. Vanstone, Guide to elliptic curve cryptography, Springer-Verlag.
9. A. Das and C. E. Veni Madhavan, Public-key cryptography: Theory and practice, Pearson Education Asia.
10. H. Cohen, A course in computational algebraic number theory, Springer-Verlag.