Abstract

This exposition is the result of a year's study of the Primality and Factoring. It has two parts. In the first part of the thesis, we discuss the most popular methods of primality testing. After providing a brief survey of primality testing algorithms (i.e. the Chinese primality test, Fermat test, Lucas test, the Miller-Rabin primality test etc.), we present a thorough analysis of the unconditional deterministic polynomial time algorithm for determining that a given integer is prime or composite proposed by Agrawal, Kayal and Saxena in their paper "Primes is in P" [6]. In the second part of the report, we discuss the well known algorithms for integer factorization (such as Pollard rho method, Pollard p-1 method, Fermat factor base method, Continued fraction method etc.) along with intermediate steps of their formulation. At the end of this part, we present quadratic Sieve method for factoring integers in exponential time (in the input size) and number field Sieve algorithm briefly. At the end, we discuss Lenstra-Lenstra-Lovasz (LLL) - algorithm for getting reduced basis of a lattice and factoring any arbitrary non-constant polynomial in Z[X] in polynomial time (as in input size).