Lenstra, H. W. jun.

Elliptic curves and number-theoretic algorithms. (English) Zbl 0686.14039

Proc. Int. Congr. Math., Berkeley/Calif. 1986, Vol. 1, 99-120 (1987).

[For the entire collection see Zbl 0657.00005.]

The problem under consideration is the prime factor decomposition problem and the use of elliptic curve to find solutions to it. One considers two stages: firstly one decides whether a given large integer is a prime or not; secondly, if it is composite, one searches for a nontrivial divisor.

Applications are found in cryptography. This is based on the fact that primality testing is relatively easy, whereas factorization is hard. After surveying the older algorithms, the author explains the necessary tools from elliptic curve theory, especially point counting theorems and algorithms. He then applies the theory to primality testing on the one hand and to factorization on the other, providing solutions that lead (e.g. method of Atkins) to algorithms that can be used in practical implementations.

Together with the algorithms, the author discusses running time or probable running time. Not only primality test are discussed. A number is called pseudo-prime if it passes a test which every prime number passed and most of the composites don't. A variety of pseudo-prime test are considered in the article.

Reviewer: G.Molenbergh

MSC:

14H45	Special algebraic curves and curves of low genus
68W30	Symbolic computation and algebraic computation
14-04	Software, source code, etc. for problems pertaining to algebraic geometry
11A41	Primes
14H52	Elliptic curves
94A60	Cryptography

Keywords:

prime factor decomposition problem; elliptic curve; cryptography; algorithms; point counting theorems; pseudo-prime test