VECTOR AND PARALLEL ALGORITHMS FOR INTEGER FACTORISATION

RICHARD P. BRENT

Abstract

The problem of finding the prime factors of large composite numbers is of practical importance since the advent of public key cryptosystems whose security depends on the presumed difficulty of this problem. In recent years the best known integer factorisation algorithms have improved greatly. It is now routine to factor 60-decimal digit numbers, and possible to factor numbers of more than 110 decimal digits.

We describe several integer factorisation algorithms, and consider their suitability for implementation on vector processors and parallel machines.

Comments

Only the Abstract is given here. The full paper appeared as [4]. For related work, see [1, 2, 3].

References

[1] R. P. Brent, "Some integer factorization algorithms using elliptic curves", *Australian Computer Science Communications* 8 (1986), 149–163. rpb097.

[2] R. P. Brent, "Parallel algorithms for integer factorisation", *Number Theory and Cryptography* (edited by J. H. Loxton), London Mathematical Society Lecture Note Series 154, Cambridge University Press, 1990, 26–37. ISBN 0-521-39877-0. MR 91h:11148. rpb115.

[3] R. P. Brent, "Primality testing and integer factorisation", in *The Role of Mathematics in Science*, Australian Academy of Science, 1991, 14–26. ISBN 0-85847-170-1. rpb120.

[4] R. P. Brent, "Vector and parallel algorithms for integer factorisation", *Proceedings Third Australian Supercomputer Conference* (Melbourne, December 1990), Strategic Research Foundation, University of Melbourne, December 1990, 12 pp. Also appeared as Report TR-CS-90-05, Computer Sciences Laboratory, ANU, October 1990, 13 pp. rpb122.

Computer Sciences Laboratory, Australian National University, Canberra
E-mail address: rpb@cslab.anu.edu.au

1991 *Mathematics Subject Classification.* Primary 11Y05; Secondary 11-04, 11Y05, 11Y16, 14H52, 68Q22, 68Q25.

Key words and phrases. Factorization, integer factorization, elliptic curve method, ECM, multiple-polynomial quadratic sieve, MPQS, number-field sieve, NFS, vector processor, parallel algorithm.

rpb122a typeset using $\mathcal{AMS}$-LaTeX.