PARALLEL ALGORITHMS FOR INTEGER FACTORISATION

RICHARD P. BRENT

Abstract

The problem of finding the prime factors of large composite numbers has always been of mathematical interest. With the advent of public key cryptosystems it is also of practical importance, because the security of some of these cryptosystems, such as the Rivest-Shamir-Adleman (RSA) system, depends on the difficulty of factoring the public keys.

In recent years the best known integer factorisation algorithms have improved greatly, to the point where it is now easy to factor a 60-decimal digit number, and possible to factor numbers larger than 120 decimal digits, given the availability of enough computing power.

We describe several algorithms, including the *elliptic curve method* (ECM), and the *multiple-polynomial quadratic sieve* (MPQS) algorithm, and discuss their parallel implementation. It turns out that some of the algorithms are very well suited to parallel implementation. Doubling the degree of parallelism (i.e. the amount of hardware devoted to the problem) roughly increases the size of a number which can be factored in a fixed time by 3 decimal digits.

Some recent computational results are mentioned – for example, the complete factorisation of the 617-decimal digit Fermat number $F_{11} = 2^{2^{11}} + 1$ which was accomplished using ECM [2].

Comments

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

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary Primary 11A51; Secondary 11-04, 11Y05, 11Y11, 11Y16, 14H52, 68Q22, 68Q25.

Key words and phrases. Factorization, integer factorization, cryptography, public-key cryptography, RSA system, elliptic curve method, ECM, multiple-polynomial quadratic sieve, MPQS, Fermat number, eleventh Fermat number.

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, "Factorization of the eleventh Fermat number (preliminary report)", *AMS Abstracts* 10 (1989), 89T-11-73. rpb113a.
3. 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. Also appeared as Report TR-CS-89-22, Computer Sciences Laboratory, ANU, and as Report CMA-R49-89, Centre for Mathematical Analysis, ANU, October 1989, 12 pp. rpb115.
4. 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.

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