PRIMALITY TESTING AND 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-Adelman (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 recent algorithms for primality testing and factorisation, give examples of their use, and outline some applications.

Comments

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

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*, Proceedings of a Symposium held at the Australian Academy of Science (Canberra, 20 April 1990), Australian Academy of Science, 1991, 14–26. ISBN 0-85847-170-1. Also appeared as Report TR-CS-90-03, Computer Sciences Laboratory, ANU, May 1990, 15 pp. 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. rpb122.

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

1991 *Mathematics Subject Classification.* 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, number field sieve, NFS, Fermat number, eleventh Fermat number.

rpb120a typeset using $\mathcal{AMS}$-LaTeX.