SOME INTEGER FACTORIZATION ALGORITHMS USING ELLIPTIC CURVES

RICHARD P. BRENT

Abstract

Lenstra's integer factorization algorithm is asymptotically one of the fastest known algorithms, and is ideally suited for parallel computation. We suggest a way in which the algorithm can be speeded up by the addition of a second phase. Under some plausible assumptions, the speedup is of order $\ln(p)$, where p is the factor which is found. In practice the speedup is significant. We mention some refinements which give greater speedup, an alternative way of implementing a second phase, and the connection with Pollard's "$p - 1$" factorization algorithm.

Comments

Only the Abstract is given here. The full paper appeared as [2]. A preliminary (longer) version appeared as [1]. An early success of the method was the complete factorization of the 617-decimal digit Fermat number $F_{11} = 2^{2^{11}} + 1$; see [3, 4].

References

[1] R. P. Brent, "Some integer factorization algorithms using elliptic curves", Report CMA-R32-85, Centre for Mathematical Analysis, ANU, September 1985, 20 pp. rpb097.

[2] R. P. Brent, "Some integer factorization algorithms using elliptic curves", *Proc. Ninth Australian Computer Science Conference*, special issue of *Australian Computer Science Communications* 8 (1986), 149–163. Retyped (with corrections and postscript) in LaTeX 1998. rpb102.

[3] R. P. Brent, "Factorization of the eleventh Fermat number (preliminary report)", *AMS Abstracts* 10 (1989), 89T-11-73. rpb113.

[4] 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.

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

1991 *Mathematics Subject Classification.* Primary 11A51; Secondary 11Y05, 11Y11, 11Y16, 14H52, 68Q22, 68Q25.

Key words and phrases. Factorization, integer factorization, Monte Carlo algorithm, elliptic curve method, ECM, analysis of algorithms.

CR Categories. F.2.

rpb102a typeset using AMS-LaTeX.