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 report appeared as [1]. A revision appeared as [2].

Errata

1. Equations (7.3) and (7.7) have obvious (easily corrected) errors.
2. In equation (1.1), the "$(1+o(1))$" factor should be *inside* the exponential.

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. rpb102.

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.

rpb097a typeset using $\mathcal{AMS}$-LaTeX.