AN IMPROVED MONTE CARLO FACTORIZATION ALGORITHM

RICHARD P. BRENT

Abstract

Pollard's Monte Carlo factorization algorithm usually finds a factor of a composite integer N in $O(N^{1/4})$ arithmetic operations. The algorithm is based on a cycle-finding algorithm of Floyd. We describe a cycle-finding algorithm which is about 36 percent faster than Floyd's (on the average), and apply it to give a Monte Carlo factorization algorithm which is similar to Pollard's but about 24 percent faster.

Comments

Only the Abstract is given here. A preliminary version appeared as [2] and the full paper appeared as [1]. The result improved the efficiency of Pollard's "rho" method [4]. A further modification was used to factor the eighth Fermat number [3].

References

[1] R. P. Brent, "An improved Monte Carlo factorization algorithm", *BIT* 20 (1980), 176-184. MR 82a:10007, Zbl 439.65001. rpb051

[2] R. P. Brent, *Analysis of some new cycle finding and factorization algorithms*, Technical Report TR-CS-79-11, DCS, ANU (November 1979), 10 *pp.*

[3] R. P. Brent and J. M. Pollard, "Factorization of the eighth Fermat number", *Math. Comp.* 36 (1981), 627-630. MR 83h:10014. rpb061

[4] J. M. Pollard, "A Monte Carlo method for factorization", *BIT* 15 (1975), 331–334. MR 52 #13611.

Department of Computer Science, Australian National University, Canberra, ACT 2600

1991 *Mathematics Subject Classification.* Primary 11Y05, 11A51; Secondary 11Y16, 11Y55, 68Q25.
Key words and phrases. Cycle finding, factorization, Monte Carlo, Pollard rho.
Manuscript received December 14, 1979.

rpb051a typeset using $\mathcal{AMS}$-LaTeX.