FACTORIZATION OF THE EIGHTH FERMAT NUMBER

RICHARD P. BRENT AND JOHN M. POLLARD

Abstract

We describe a Monte Carlo factorization algorithm which was used to factorize the Fermat number $F_8 = 2^{256} + 1$. Previously, F_8 was known to be composite, but its factors were unknown.

Comments

Only the Abstract is given here. The full paper appeared as [2]. For a succinct proof of primality of the larger factor q_8 of F_8, see [3].

At the time of this paper, Lenstra's elliptic curve method (ECM) had not been invented. Thus, a modification of Pollard's "rho" method [1] was used to factor F_8 and several Mersenne numbers [4]. For the factorization of a larger Fermat number by ECM, see [5].

The smaller factor of F_8 is 1238926361552897. The epigram

I am now entirely persuaded to employ the method,
a handy trick, on gigantic composite numbers

may appeal to readers who wish to memorize this factor.

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 and J. M. Pollard, "Factorization of the eighth Fermat number", *Mathematics of Computation* 36 (1981), 627–630. MR 83h:10014. Also appeared as Report TR-CS-80-12, Department of Computer Science, ANU, (September 1980), 7 pp. A preliminary announcement appeared in *AMS Abstracts* 1 (1980), 565, 80T–A212. rpb061.

[3] R. P. Brent, "Succinct proofs of primality for the factors of some Fermat numbers", *Mathematics of Computation* 38 (1982), 253–255. MR 82k:10002. rpb066.

[4] R. P. Brent, "New factors of Mersenne numbers (preliminary report)", *AMS Abstracts* 2 (1981), 367, 81T–10–246; part II, *ibid* 3 (1982), 132, 82T–10–22; part III, *ibid* 4 (1983), 197, 83T–10–138. rpb067.

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

(Brent) Department of Computer Science, Australian National University, Canberra

(Pollard) Plessey Telecommunications, Taplow Court, Maidenhead, Berkshire, England

1991 *Mathematics Subject Classification.* Primary 11-04; Secondary 11A51, 11K45, 11Y05, 11Y11, 65C05.

Key words and phrases. Fermat numbers, factorization, Monte Carlo methods.

We thank H. C. Williams for proving the primality of q_8, D. H. Lehmer and Daniel Shanks for their assistance, and the Australian National University for the provision of computer time.

Received September 18, 1980.

rpb061a typeset using $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX.