FACTORIZATION OF THE ELEVENTH FERMAT NUMBER (PRELIMINARY REPORT)

RICHARD P. BRENT

Abstract

Of the Fermat numbers $F_n = 2^{2^n} + 1$, only F_1 to F_4 are known to be prime; certainly F_5 to F_{21} are composite. However, the only complete factorizations known until now are those of F_5 (Euler), F_6 (Landry), F_7 (Morrison and Brillhart, 1975), and F_8 (Brent and Pollard, 1981). This abstract announces the complete factorization of the 617-digit Fermat number $F_{11} = 2^{2^{11}} + 1$. In fact

$$F_{11} = 319489 \cdot 974849 \cdot 167988556341760475137 \cdot 3560841906445833920513 \cdot p_{564}$$

where the two 6-digit factors were already known (Cunningham, 1899), the 21-digit and 22-digit prime factors were found using the two-phase elliptic curve algorithm on a Fujitsu VP100 computer, and p_{564} is a 564-decimal digit prime (primality proof by F. Morain, using the method of Atkin).

Comments

The abstract appeared as [2]. For a description of the computational method and related work, see [1, 3, 4]. The primality test of Atkin and Morain is described in [5].

References

[1] 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. rpb097.

[2] R. P. Brent, "Factorization of the eleventh Fermat number (preliminary report)", *AMS Abstracts* 10 (1989), 89T-11-73. rpb113a.

[3] 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.

[4] R. P. Brent, "Primality testing and integer factorisation", *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. rpb120.

[5] F. Morain, *Courbes elliptiques et tests de primalité*, thesis, Université de Lyon I, 1990. Available by anonymous ftp from `ftp.inria.fr` .

Computer Sciences Laboratory, Australian National University, Canberra

1991 *Mathematics Subject Classification.* Primary 11-04; Secondary 11A51, 11Y05, 11Y11, 14H52.

Key words and phrases. Fermat number, factorization, elliptic curve method, ECM, primality test.

The provision of computer time by the ANU Supercomputer Facility is gratefully acknowledged.

Submitted 21 December 1988.

rpb113a typeset using $\mathcal{AMS}$-LaTeX.