FACTORIZATION OF THE TENTH AND ELEVENTH FERMAT NUMBERS

RICHARD P. BRENT

Abstract

We describe the complete factorization of the tenth and eleventh Fermat numbers. The tenth Fermat number is a product of four prime factors with 8, 10, 40 and 252 decimal digits. The eleventh Fermat number is a product of five prime factors with 6, 6, 21, 22 and 564 decimal digits. We also note a new 27-decimal digit factor of the thirteenth Fermat number. This number has four known prime factors and a 2391-decimal digit composite factor. All the new factors reported here were found by the elliptic curve method (ECM). The 40-digit factor of the tenth Fermat number was found after about 140 Mflop-years of computation. We discuss aspects of the practical implementation of ECM, including the use of special-purpose hardware, and note several other large factors found recently by ECM.

Comments

Only the Abstract is given here. The full report appeared as [1]. A shorter version (omitting the factor of F_{13}) appeared as [2]. The factor of F_{13} is mentioned in [3].

References

[1] R. P. Brent, *Factorization of the tenth and eleventh Fermat numbers,* Technical Report TR-CS-96-02, CSL, ANU, Feb. 1996, 25 pp. `ftp://discus.anu.edu.au/pub/Brent/rpb161tr.dvi.gz`. rpb161tr

[2] R. P. Brent, "Factorization of the tenth Fermat number", *Math. Comp.* 68 (1999), 429–451. rpb161

[3] R. P. Brent, R. E. Crandall, K. Dilcher and C. Van Halewyn, "Three new factors of Fermat numbers", *Mathematics of Computation* S 0025-5718(00)01207-2 (published electronically 1 March 2000). rpb175

Computer Sciences Laboratory, Australian National University, Canberra, ACT 0200

E-mail address: `rpb@cslab.anu.edu.au`

Date: 21 February 1996.

1991 *Mathematics Subject Classification.* 11Y05, 11B83, 11Y55; Secondary 11-04, 11A51, 11Y11, 11Y16, 14H52, 65Y10, 68Q25.

Key words and phrases. computational number theory, Cunningham project, ECM, elliptic curve method, factorization, Fermat number, F_{10}, F_{11}, F_{12}, F_{13}, integer factorization.

rpb161a typeset using $\mathcal{AMS}$-LaTeX.