SUCCINCT PROOFS OF PRIMALITY FOR THE FACTORS OF SOME FERMAT NUMBERS

RICHARD P. BRENT

Abstract

We give short and easily verified proofs of primality for the factors of the Fermat numbers F_5, F_6, F_7 and F_8.

Comments

Only the Abstract is given here. The full paper appeared as [2]. The main result is a simpler proof of primality of the larger factor of F_8 than is given in [1]. Proofs of primality of the factors of F_9, F_{10} and F_{11} may be found in [3].

References

[1] 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.

[2] 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.

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

Department of Computer Science, Australian National University, Canberra

1991 *Mathematics Subject Classification.* Primary 10-04, 10A25, 10A40; Secondary 10A05, 10A10, 65C05, 68-04.

Key words and phrases. Factorization, Fermat numbers, primality testing, primitive root, Monte Carlo methods.

Received January 15, 1981.

rpb066a typeset using $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX.