MATHEMATICS OF COMPUTATION
VOLUME 38, NUMBER 157
JANUARY 1982

Succinct Proofs of Primality for the Factors of Some Fermat Numbers

By 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.

1. Introduction. The Fermat numbers $F_k = 2^{2^k} + 1$ are prime for $1 \leqslant k \leqslant 4$ and have exactly two prime factors for $5 \leqslant k \leqslant 8$. Here we give 'succinct' [7] and easily verified proofs of primality for the prime factors of F_k, $5 \leqslant k \leqslant 8$. We assume that the primality of integers smaller than 10^7 is easy to check [5].

To prove that an integer p is prime, it is sufficient to find an integer x such that

$$x^{p-1} = 1 \pmod p$$

and, for all prime divisors q of $p - 1$,

$$x^{(p-1)/q} \neq 1 \pmod p.$$

Then x is a primitive root $(\operatorname{mod} p)$. The difficulty in finding such proofs lies in factorizing $p - 1$; see e.g. [4].

2. Proofs of Primality. In Table 1 we give the least positive primitive root $(\operatorname{mod} p_k)$ and the complete factorization of $p_k - 1$ for the primes p_k listed in Table 2. Using Table 1, it is easy to verify that $p_{20}, \ldots, p_1$ are in fact prime. Since

$$\begin{aligned} F_5 &= 641 \cdot 6700417 && \text{(Euler)},\\ F_6 &= 274177 \cdot p_1 && \text{(Landry)},\\ F_7 &= p_2 \cdot p_3 && \text{(Morrison and Brillhart [6])}, \end{aligned}$$

and

$$F_8 = p_8 \cdot p_9 \qquad \text{(Brent and Pollard [3])},$$

this completes the required primality proofs.

Received January 15, 1981.
1980 *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.

TABLE 1
Primitive roots and factorizations

k	primitive root (mod p_k)	factorization of $p_k - 1$
1	3	$2^8 \cdot 5 \cdot 47 \cdot 373 \cdot 2998279$
2	3	$2^9 \cdot p_4$
3	21	$2^9 \cdot 3^5 \cdot 5 \cdot 12497 \cdot p_6$
4	2	$2 \cdot 7 \cdot 449 \cdot p_5$
5	6	$2 \cdot 3^3 \cdot 181 \cdot 1896229$
6	2	$2 \cdot 3 \cdot 2203 \cdot p_7$
7	3	$2^3 \cdot 6939437$
8	3	$2^{11} \cdot 157 \cdot p_{10}$
9	43	$2^{11} \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot p_{11} \cdot p_{12}$
10	6	$2^6 \cdot 5 \cdot 719 \cdot 16747$
11	17	$2 \cdot 1789 \cdot 10079 \cdot 876769$
12	11	$2^4 \cdot 3 \cdot 8861 \cdot p_{13} \cdot p_{14} \cdot p_{15}$
13	2	$2^2 \cdot 7 \cdot 223 \cdot 1699$
14	2	$2 \cdot 3^2 \cdot 16879 \cdot p_{16}$
15	5	$2 \cdot 20939 \cdot p_{18}$
16	11	$2 \cdot p_{17}$
17	2	$2 \cdot 13 \cdot 1604753$
18	5	$2^2 \cdot 3^2 \cdot p_{19}$
19	3	$2^4 \cdot 5 \cdot 7 \cdot p_{20}$
20	2	$2 \cdot 23 \cdot 29^2 \cdot 283$

TABLE 2
Primes related to factors of Fermat numbers

k	p_k
1	67280421310721
2	59649589127497217
3	5704689200685129054721
4	116503103764643
5	18533742247
6	733803839347
7	55515497
8	1238926361552897
9	93461639715357977769163558199606896584051237541638188580280321
10	3853149761
11	31618624099079
12	1057372046781162536274034354686893329625329
13	10608557
14	25353082741699
15	9243081088796207
16	83447159
17	41723579
18	220714482277
19	6130957841
20	10948139

3. Comments. The larger factor p_9 of F_8 was first proved to be prime by H. C. Williams, using the method of [8]. At that time the complete factorization of $p_9 - 1$ was not known.

To obtain Table 1 we had to factorize several large integers. All nontrivial factorizations given in Table 1 were obtained using the Monte Carlo method of [2], implemented with the MP package [1]. The most difficult factorizations were those of the 56-digit integer $p_{11}p_{12}$ and the 30-digit integer $p_{14}p_{15}$. The numbers of arithmetic operations required for these factorizations were approximately as predicted by the probabilistic analysis of [2].

Acknowledgement. We thank the Australian National University for the provision of computer time.

Department of Computer Science
Australian National University
Canberra, A.C.T. 2600, Australia

1. R. P. Brent, "Algorithm 524: MP, A Fortran multiple-precision arithmetic package," *ACM Trans. Math. Software*, v. 4, 1978, pp. 71–81.

2. R. P. Brent, "An improved Monte Carlo factorization algorithm," *BIT*, v. 20, 1980, pp. 176–184.

3. R. P. Brent & J. M. Pollard, "Factorization of the eighth Fermat number," *Math. Comp.*, v. 36, 1981, pp. 627–630.

4. D. E. Knuth, *The Art of Computer Programming*, Vol. 2, Addison-Wesley, Menlo Park, 1969, Sec. 4.5.4.

5. D. N. Lehmer, *List of Prime Numbers from* 1 *to* 10,006,721, Hafner, New York, 1956.

6. M. A. Morrison & J. Brillhart, "A method of factoring and the factorization of F_7," *Math. Comp.*, v. 29, 1975, pp. 183–208.

7. V. R. Pratt, "Every prime has a succinct certificate," *SIAM J. Comput.*, v. 4, 1975, pp. 214–220.

8. H. C. Williams & J. S. Judd, "Some algorithms for prime testing using generalized Lehmer functions," *Math. Comp.*, v. 30, 1976, pp. 867–886.