MATHEMATICS OF COMPUTATION, VOLUME 35, NUMBER 151
JULY 1980, PAGES 975–976

A Factor of F_{17}

By Gary B. Gostin

Abstract. A prime factor is given for F_{17}. The method of factoring and its machine implementation are given.

During the investigation reported here, a new factor of Fermat Number F_{17} was discovered. It is given in Table 1. The factor is significant, since F_{17} is the smallest Fermat number whose character was unknown, and since $17 = F_2$.

The method of factoring is similar to that of Hallyburton and Brillhart [1] and others [3], [4]. To determine whether a $d_k = k \cdot 2^{n+2} + 1$ divides F_n, the congruence $2^{2^n} \equiv -1 \pmod{d_k}$ is tested. This is done by beginning with the residue $r_i = 2^{32}$ for $i = 5$, and computing $r_i^2 \pmod{d_k}$ which becomes r_{i+1}. This operation is repeated $n - 5$ times. For any r_i, d_k divides F_i if $r_i \equiv -1 \pmod{d_k}$. Therefore this method tests to see if d_k divides any F_i for $5 < i \leqslant n$.

TABLE 1. *Factor of* F_{17}

n	Factor
17	$31065037602817 = 59251857 \cdot 2^{19} + 1$

This procedure was written in Compass assembly language for the CDC Cyber 175. The basic test, along with a provision to add a constant to d_k and to repeat the basic test, was written as a subroutine that can be called by Fortran. The subroutine can test up to 131,072 d_k's on a single call. The time to test a d_k is given in Table 2 for three Fermat Numbers.

TABLE 2. *Time to test a* d_k *for* F_n

n	time (microseconds)	# residue calculations
9	7.0	4
13	14.5	8
17	20.8	12

A computer generated sieve was considered for reducing the number of d_k's tested. It was rejected, however, because the cost (time plus memory) of rejecting a d_k, by using the sieve, was more than the cost of running the basic test with d_k. Instead the following method was used.

Received April 16, 1979; revised November 7, 1979.
1980 *Mathematics Subject Classification.* Primary 10A25, 10A40; Secondary 10–04.

If all d_k divisible by 3 or 5, or with k even, are crossed off a list of all d_k's, the pattern of divisors remaining is periodic with a period of thirty. Eight divisors out of each group of thirty will remain. Therefore a search of a sequence of d_k's can be broken down into eight searches, with $30 \cdot 2^{n+2}$ being added to the present divisor to get the next divisor in each test. Thus a sieve by 3 and 5 on a sequence of d_k's (k odd) can be done with no additional computer time. By consulting a table of primes, it is estimated that 60% of the composite d_k's are rejected by this sieve.

All the Fermat numbers from F_8 to F_{46} were examined. A limit of 2^{48} was placed on d_k, but $d_k = 2^{48} + 1$ was factored (thus rejected) by hand. The search limit for each Fermat Number is shown in Table 3. For each F_n, the limit on d_k includes odd values of k tried while examining F_n, and even values of k tried while examining $F_m > n$. Therefore in every case, all divisors up to the limit reported were covered. The total CPU execution time of this program was about seven hours.

TABLE 3. *Search limit for F_n*

n	Limit	
8	$d_k = 2^{41} + 1$	$k = 2^{31}$
9	$d_k = 2^{41} + 1$	$k = 2^{30}$
10	$d_k = 2^{42} + 1$	$k = 2^{30}$
11	$d_k = 2^{43} + 1$	$k = 2^{30}$
12	$d_k = 2^{45} + 1$	$k = 2^{31}$
13	$d_k = 2^{45} + 1$	$k = 2^{30}$
14 – 24	$d_k = 2^{47} + 1$	
25 – 46	$d_k = 2^{48} + 1$	

During the search, two factors for F_{12} and one for F_{11} were also found. These were found by S. Wagstaff at the University of Illinois to be products of smaller known factors. Wagstaff also mentioned that the cofactors of F_{11}, F_{12}, and F_{13} are composite.

I would like to express my thanks to the University of Illinois Computer Center for the use of the Cyber 175, on which the work reported here was done.

13354 Emily Road #136
Dallas, Texas 75240

1. JOHN C. HALLYBURTON, JR. & JOHN BRILLHART, "Two new factors of Fermat numbers," *Math. Comp.*, v. 29, 1975, pp. 109–112.

2. MICHAEL A. MORRISON & JOHN BRILLHART, "A method of factoring and the factorization of F_7, "*Math. Comp.*, v. 29, 1975, pp. 183–205.

3. RAPHAEL M. ROBINSON, "A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers," *Proc. Amer. Math. Soc.*, v. 9, 1958, pp. 673–681.

4. G. MATTHEW & H. C. WILLIAMS, "Some new primes of the form $k \cdot 2^n + 1$," *Math. Comp.*, v. 31, 1977, pp. 797–798.