MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 129
JANUARY 1975, PAGES 109–112

Two New Factors of Fermat Numbers

By John C. Hallyburton, Jr. and John Brillhart

Dedicated to D. H. Lehmer on his 70th birthday

Abstract. A new prime factor is given for each of the Fermat numbers F_{12} and F_{13} (none was previously known for F_{13}). The factoring method used and its machine implementation are discussed. A short table of factors and a current status list are also included.

In recent years various investigators have used computers to search for prime factors of the Fermat numbers $F_m = 2^{2^m} + 1$, $m \geqslant 7$ (see Selfridge [10], Robinson [7]–[9], Riesel [6], Brillhart [1], Wrathall [12], Morrison and Brillhart [3], [4]). In our investigation we have found two new factors, namely:

$$190274191361 = 11613415 \cdot 2^{14} + 1 \quad \text{and} \quad 2710954639361 = 41365885 \cdot 2^{16} + 1,$$

which divide F_{12} and F_{13}, respectively. Previously, three prime factors of F_{12} had been discovered, while F_{13} was only known to be composite (see Paxson [5]).

It is well known that any prime factor of F_m has the form $k \cdot 2^{m+2} + 1$, $m \geqslant 2$. In searching for such a factor, we can try dividing F_m by each d_k of this form for k less than some search limit L_m. Many composite d_k can, of course, be eliminated as trial divisors in advance by sieving on the arithmetic sequence $\{d_k\}$ with small, odd primes (in our program the odd primes less than 500 were used).

To discover whether a d_k which has survived the sieving is a factor of F_m, we calculate $F_m(\text{mod } d_k)$ by the usual powering method—here only a sequence of squarings and reductions.

Since the residues r_i of the powers $2^{2^i}(\text{mod } d_k)$, $i \leqslant m$, will necessarily be computed in this calculation, it is clear we should check to see if $r_i \equiv -1(\text{mod } d_k)$ for each i, $8 \leqslant i \leqslant m$, thereby determining in one stroke if d_k is a factor of *any* of these F_i. It should be remarked, however, that k is always taken to be odd. Thus, if F_m has a prime factor $k \cdot 2^{n+2} + 1$ with k odd and $n > m$, then this factor can only be discovered during the search for factors of F_n. For example, the factor of F_{13} was found during the investigation of F_{14}, since in this case $n - m = 1$.

This procedure was coded in COMPASS assembly language for the CDC 6400 at

Received May 20, 1974.
AMS (MOS) subject classifications (1970). Primary 10A25, 10A40; Secondary 10–04.
Key words and phrases. Fermat numbers, factoring.

TABLE 1. *Search limits*

$1 \leqslant k \leqslant L_m$, k odd

m	L_m
8	1542455295
9–13	16777215
14	792008373
15–22	16777215

TABLE 2. *Factors of* F_m, $5 \leqslant m \leqslant 22$

m	Prime Factors	Date	Discoverer
5	641	1732	Euler
5	6700417	1732	Euler
6	274177	1880	Landry
6	67280421310721	1880	Landry, LeLasseur, Gérardin
7	59649589127417217	1970	Morrison, Brillhart
7	5704689200685129054721	1970	Morrison, Brillhart
8	c	1909	Morehead, Western
9	2424833	1903	Western
9	c*	1967	Brillhart
10	45592577	1953	Selfridge
10	6487031809	1962	Brillhart
10	c*	1967	Brillhart
11	319489	1899	Cunningham
11	974849	1899	Cunningham
12	114689	1877	Lucas, Pervouchine
12	26017793	1903	Western
12	63766529	1903	Western
12	190274191361	1974	Hallyburton, Brillhart
13	2710954639361	1974	Hallyburton, Brillhart
14	c	1961	Selfridge, Hurwitz
15	1214251009	1925	Kraitchik
16	825753601	1953	Selfridge
17	?		
18	13631489	1903	Western
19	70525124609	1962	Riesel
19	646730219521	1963	Wrathall
20	?		
21	4485296422913	1963	Wrathall
22	?		

? = character of F_m is unknown.

c = number is composite. (* = previously unpublished results found on the IBM 7094 at the Bell Telephone Laboratories at Holmdel, New Jersey.)

TABLE 3. *Status list*

m	Character of F_m
0, 1, 2, 3, 4	Prime
5, 6, 7	Composite and completely factored
10^+, 11, 12^*, 19, 30, 38	Two or four* factors known (+ = cofactor is composite)
9^+, 13, 15, 16, 18, 21, 23, 25, 26, 27, 32, 36, 39, 42, 52, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 250, 267, 268, 284, 316, 452, 1945	Only one prime factor known
8, 14	Composite but no factor known
17, 20, 22, 24, 28, 29, 31, etc.	Character unknown

the University of Arizona Computer Center and was run for 150 hours at lowest priority.

It should be pointed out that there is a problem with running a low-priority job, which requires considerable memory, on a large processor like the CDC 6400. To maximize running time the program should always remain in core, i.e., it should not use so much space that other jobs (all of higher priority) continually cause it to be swapped onto a disk because of their memory requirements. On the other hand, the sieve, which the program uses, should occupy enough memory to avoid its continually having to be remade.

To solve this problem, we usually ran the program only on weekends, holidays, or late at night (when only nightowl system programmers were around). By asking, we could get a good idea of their memory requirements and scale our own space request accordingly. In addition to this, pieces of the sieve (64 words at a time—the minimum possible on this machine) were returned to the system, after they had been read, to further increase the likelihood that the job would remain in core. (The sieve was stored in reverse order, adjacent to the program, to facilitate this return.) When reading the sieve was completed, a new memory request was automatically made and a new section of the sieve was constructed. In general, the sieve required between half a million and a million bits.

In this investigation only F_m for $8 \leqslant m \leqslant 22$ were considered. The search limits on k that were used in each case are listed on Table 1. A limitation of 2^{48} was placed on $d_k = k \cdot 2^{m+2} + 1$ so that a remainder $(\text{mod } d_k)$ would be less than this amount—a convenient size for double-precision squaring on the CDC 6400.

All known factors of these F_m were rediscovered and are given with their discoverer and date in Table 2 (dates after 1925 are the dates of discovery).

Acknowledgements. The authors would like to express their gratitude to the staff and management of the University of Arizona Computer Center for their support of this project.

Department of Computer Science
University of Arizona
Tucson, Arizona 85721

Department of Mathematics
University of Arizona
Tucson, Arizona 85721

1. JOHN BRILLHART, "Some miscellaneous factorizations," *Math. Comp.*, v. 17, 1963, pp. 447–450.

2. ALEXANDER HURWITZ & J. L. SELFRIDGE, "Fermat numbers and perfect numbers," *Notices Amer. Math. Soc.*, v. 8, 1961, p. 601, Abstract #587-104.

3, MICHAEL A. MORRISON & JOHN BRILLHART, "The factorization of F_7," *Bull. Amer. Math. Soc.*, v. 77, 1971, p. 264. MR 42 #3012.

4. MICHAEL A. MORRISON & JOHN BRILLHART, "A method of factoring and the factorization of F_7," *Math. Comp.*, v. 29, 1975, pp. 183-205 (this issue).

5. G. A. PAXSON, "The compositeness of the thirteenth Fermat number," *Math. Comp.*, v. 15, 1961, p. 420. MR 23 #A1578.

6. HANS RIESEL, "A factor of the Fermat number F_{19}," *Math. Comp.*, v. 17, 1963, p. 458.

7. RAPHAEL M. ROBINSON, "Mersenne and Fermat numbers," *Proc. Amer. Math. Soc.*, v. 5, 1954, pp. 842–846. MR 16, 335.

8. RAPHAEL M. ROBINSON, "Factors of Fermat numbers," *MTAC*, v. 11, 1957, pp. 21–22. MR 19, 14.

9. 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. MR 20 #3097.

10. J. L. SELFRIDGE, "Factors of Fermat numbers," *MTAC*, v. 7, 1953, pp. 274–275.

11. J. L. SELFRIDGE & ALEXANDER HURWITZ, "Fermat numbers and Mersenne numbers," *Math. Comp.*, v. 18, 1964, pp. 146–148. MR 28 #2991.

12. CLAUDE P. WRATHALL, "New factors of Fermat numbers," *Math. Comp.*, v. 18, 1964, pp. 324–325. MR 29 #1167.