

Six New Factors of Fermat Numbers

By Gary B. Gostin and Philip B. McLaughlin, Jr.

Abstract. A new prime factor is given for each of the Fermat numbers F_{29} , F_{36} , F_{99} , F_{147} , F_{150} , and F_{201} . A summary of search limits and recent results is included.

In the past few years several investigators [1]–[11] have found many new prime factors of the Fermat numbers $F_m = 2^{2^m} + 1$. The increased availability and speed of computing equipment have allowed the search limits for factors of these numbers to be extended significantly. In tables below, we include the known search limits and all of the results that have been obtained since H. C. Williams' 1978 paper [12] was published.

Using the method outlined by Hallyburton and Brillhart [8], we tested integers of the form $k \cdot 2^n + 1$, k odd, as factors of the Fermat numbers F_m , $9 \leq m \leq n - 2$, for the ranges shown in Table 1. During our search the following new prime factors were found:

$$\begin{aligned}
 &1120049 \cdot 2^{31} + 1 | F_{29}, \\
 &3759613 \cdot 2^{38} + 1 | F_{36}, \\
 &16233 \cdot 2^{104} + 1 | F_{99}, \\
 &3125 \cdot 2^{149} + 1 | F_{147}, \\
 &5439 \cdot 2^{154} + 1 | F_{150}, \\
 &4845 \cdot 2^{204} + 1 | F_{201}.
 \end{aligned}$$

The factors of F_{36} and F_{150} are the second known for these numbers.

TABLE 1
Intervals covered by the authors for $k \cdot 2^n + 1$, k odd.

n		n	
25	$2^{22} < k < 2^{23}$	104–113	$10^3 < k < 2^{18}$
26–27	$2^{21} < k < 2^{23}$	114–135	$10^3 < k < 2^{17}$
28	$2^{20} < k < 2^{23}$	136–143	$10^3 < k < 2^{16}$
29–40	$10^6 < k < 2^{23}$	144–176	$10^3 < k < 2^{15}$
41	$10^6 < k < 2^{22}$	177	$10^3 < k < 2^{14}$
42–55	$10^6 < k < 2^{21}$	178–242	$10^3 < k < 2^{13}$
56–102	$10^6 < k < 2^{20}$	243–245	$10^3 < k < 2^{255-n}$
103	$10^3 < k < 2^{19}$		

Received December 17, 1980; revised March 19, 1981.

1980 *Mathematics Subject Classification.* Primary 10A25, 10A40; Secondary 10–04.

Key words and phrases. Fermat numbers, factorization.

©1982 American Mathematical Society
 0025-5718/81/0000-1121/\$02.25

Note. We did not test the range $2^{15} < k < 2^{16}$ for $n = 120, 128,$ or 136 . These intervals were covered by H. Suyama. See Table 2.

The first-named author programmed the method in assembly language on a Motorola MC6800 microprocessor. To test a trial divisor $d_k = k \cdot 2^n + 1$ as a factor, the residue $2^{2^m} \pmod{d_k}$ was calculated for $9 \leq m \leq n - 2$. The number of trial divisors were reduced by sieving through a set of modulo p_i counters, where p_i is the i th prime, $2 \leq i \leq 31$. Counter i , upon counting down to zero, would signify division of d_k by p_i , and the counter would be reset to p_i . This program has been running, with only brief interruptions, since September, 1979.

The second-named author programmed the method in HPL (a machine-specific language) on a Hewlett-Packard 9825 desktop computer. To reduce the number of trial divisors d_k , the values of k were sieved. This consisted of computing and storing, for a given value of n , the quantities $c_i = -(p_i + 1)/2^n \pmod{p_i}$, where p_i is the i th prime. It is easy to show that p_i divides $d_k = k \cdot 2^n + 1$ if, and only if, $k \pmod{p_i} = c_i$. Thus only those d_k 's for which $k \pmod{p_i} \neq c_i, 2 \leq i \leq L$, where L was variable up to 1300, were tested as possible factors. This program has been running almost continuously since January, 1980.

TABLE 2
Search limits for $k \cdot 2^n + 1, k$ odd, $3 \leq k < L_k$.

n	L_k	Recent investigators
11-23	2^{47-n}	Montgomery ($n < 15$) [9], Gostin [7]
24	2^{24}	Hallyburton & Brillhart [8]
25-40	2^{23}	Baillie ($k < 10^6$) [2], [3]
41	2^{22}	
42-55	2^{21}	
56-102	2^{20}	
103	2^{19}	
104-113	2^{18}	Suyama ($k < f$) [10], [11]
114-135	2^{17}	
136-144	2^{16}	
145-177	$\max(2^{15}, f)^*$	
178-243	$\max(2^{13}, f)$	
244-418	$\max(1000, f)$	Baillie [2], [3]
419-600	1000	
601-1000	280	
1001-1500	150	
1501-4000	30	

* $f = 2^{16-r}$, where $r = n \pmod{8}, 0 \leq r < 7$.

Note. The exponent n has been searched up to 8000 for $k = 7, 17, 27,$ and 29 , and up to 10000 for $k = 5$ [6].

It is interesting to note that full multiple-precision division is not necessary when computing residues modulo d_k . Instead, given the previous residue $2^{2^{i-1}} \pmod{d_k} = r_{i-1}$, $0 < r_{i-1} < d_k$, calculate r_{i-1}^2 , and then compute q_i and r'_i , where $r_{i-1}^2 = q_i(k \cdot 2^n) + r'_i$, $0 \leq r'_i < k \cdot 2^n$. When using a base-2 number system, this division can be reduced to division by k and some shift operations. The next residue is now easily obtained: $r_i = r'_i - q_i \pmod{d_k}$. Moreover, $-k \cdot 2^n \leq r'_i - q_i < k \cdot 2^n$, so that at most a single addition of d_k is required to force $0 < r_i < d_k$.

TABLE 3
Recent factors of the form $k \cdot 2^n + 1$ of F_m , and related results.

m	k	n	Date	Discoverer
8	604944512477	11	1980	R. P. Brent [4]
8	p^*		1980	R. P. Brent, H. C. Williams [5]
11	c^{**}		1979	S. S. Wagstaff (see [7])
12	c		1979	S. S. Wagstaff (see [7])
13	c		1979	S. S. Wagstaff (see [7])
17	59251857	19	1978	G. B. Gostin [7]
29	1120049	31	1980	G. B. Gostin, P. B. McLaughlin
36	3759613	38	1981	G. B. Gostin, P. B. McLaughlin
93	92341	96	1979	R. Baillie [2]
99	16233	104	1979	G. B. Gostin, P. B. McLaughlin, H. Suyama [10]
147	3125	149	1979	G. B. Gostin, P. B. McLaughlin
150	5439	154	1980	G. B. Gostin, P. B. McLaughlin, H. Suyama [10]
201	4845	204	1980	G. B. Gostin, P. B. McLaughlin
215	32111	217	1980	H. Suyama [10]
255	629	257	1979	R. Baillie [2]
287	5915	289	1980	H. Suyama [10]
298	247	302	1979	R. Baillie [2]
329	1211	333	1981	H. Suyama [10]
416	8619	418	1981	H. Suyama [11]
544	225	547	1979	R. Baillie [2]
692	717	695	1979	A. O. L. Atkin, N. W. Rickert [1]
1551	291	1553	1979	A. O. L. Atkin, N. W. Rickert [1]
2023	29	2027	1979	Atkin, Rickert, Cormack, Williams [1], [6]
2456	85	2458	1979	A. O. L. Atkin, N. W. Rickert [1]
3310	5	3313	1979	Atkin, Rickert, Cormack, Williams [1], [6]
4724	29	4727	1979	G. V. Cormack, H. C. Williams [6]
6537	17	6539	1979	G. V. Cormack, H. C. Williams [6]

* cofactor is prime.

** cofactor is composite.

The time required to cover the different intervals in Table 1 varied considerably. To test a single trial divisor on the 9825 took about 4 seconds for n near 40, 25

seconds for n near 100, and about 150 seconds for n near 175. For any particular n , the time spent searching ranged anywhere from 50–75 hours each for n in the range 144–176, to up to 10 days or more for n in the range 25–40. The two machines used had quite similar computation speeds.

In Table 2 above, we give a summary of the search limits known to us for factors of Fermat numbers. The names of recent researchers other than the authors, some of whose work has not been published previously, are included.

Samuel Wagstaff has informed us that Hiromi Suyama, working independently in Japan, has also discovered the factors of F_{99} and F_{150} mentioned above. In addition, he has found four other new factors of Fermat numbers. These, as well as all of the other factors and related results that have been published since Williams' paper [12], are listed in Table 3. We understand that a full account of Suyama's work will be published elsewhere.

The reader should note an error in [12]. In Table 4 on p. 135, the fifth entry should read "30 127589 33", not "30 127589 30".

There are now 85 prime factors known for 71 composite Fermat numbers. In addition, one other Fermat number and five cofactors are known to be composite.

Finally, there is a well-known conjecture that the Fermat numbers are square-free. We tested all of the known prime factors p of F_m , $9 < m < 2456$, to determine if p^2 divided F_m . No such factor was found. In each case, the residue $R = 2^{2^m} \pmod{p^2}$ was subsequently divided by p to verify that $R \pmod{p} = -1$. The test for $85 \cdot 2^{2458} + 1$ took about 165 hours. To our knowledge, the three largest factors in Table 3 have not been so tested.

Acknowledgement. The authors wish to thank Robert Baillie, Peter Montgomery, and Hiromi Suyama for their contributions to this paper, and Samuel Wagstaff for supplying helpful suggestions and information.

Note Added in Proof. We have extended our search to the following limits:

n	L_k
22	35750886
25–27	2^{24}
145–181	2^{16}
247–702	2^{10}
703–819	2^9

Intervals already covered were bypassed. In addition, Hiromi Suyama has searched $419 \leq n \leq 575$ for $k < f$ (see Table 2). No new factors were discovered.

571 Havencrest Lane
Coppell, Texas 75019

919 Northwood #7604
Baytown, Texas 77521

1. A. O. L. ATKIN & N. W. RICKERT, "Some factors of Fermat numbers," *Abstracts Amer. Math. Soc.*, v. 1, 1980, p. 211.
2. ROBERT BAILLIE, "New primes of the form $k \cdot 2^n + 1$," *Math. Comp.*, v. 33, 1979, pp. 1333–1336.
3. ROBERT BAILLIE, Personal communication via S. S. Wagstaff, Jr.

4. R. P. BRENT, "Factorization of the eighth Fermat number," *Abstracts Amer. Math. Soc.*, v. 1, 1980, p. 565.
5. R. P. BRENT & J. M. POLLARD, "Factorization of the eighth Fermat number," *Math. Comp.*, v. 36, 1981, pp. 627–630.
6. G. V. CORMACK & H. C. WILLIAMS, "Some very large primes of the form $k \cdot 2^n + 1$," *Math. Comp.*, v. 35, 1980, pp. 1419–1421.
7. GARY B. GOSTIN, "A factor of F_{17} ," *Math. Comp.*, v. 35, 1980, pp. 975–976.
8. JOHN C. HALLYBURTON, JR. & JOHN BRILLHART, "Two new factors of Fermat numbers," *Math. Comp.*, v. 29, 1975, pp. 109–112. For a correction, see *Math. Comp.*, v. 30, 1976, p. 198.
9. PETER MONTGOMERY, Personal communication.
10. HIROMI SUYAMA, "Searching for prime factors of Fermat numbers with a microcomputer," *BIT* (Japanese), v. 13, 1981, pp. 240–245.
11. HIROMI SUYAMA, Personal Communication; published with permission.
12. H. C. WILLIAMS, "Primality testing on a computer," *Ars Combin.*, v. 5, 1978, pp. 127–185.