MATHEMATICS OF COMPUTATION, VOLUME 35, NUMBER 152
OCTOBER 1980, PAGES 1419–1421

Some Very Large Primes of the Form $k \cdot 2^m + 1$

By G. V. Cormack and H. C. Williams

Abstract. Several large primes of the form $k \cdot 2^m + 1$ with $3 \leqslant k \leqslant 29$ and $m > 1500$ are tabulated and four new factors of Fermat numbers are presented.

It is well known that any factor of the Fermat number $F_n = 2^{2^n} + 1$ must have the form $k \cdot 2^m + 1$ where $m \geqslant n + 2$ and k is odd. Baillie [1] has extended the earlier tables of Robinson [6] and Matthew and Williams [5] to include all primes of the above form for odd $k \leqslant 149$ and $m \leqslant 1500$. Only 25 of these primes are factors of Fermat numbers, and of these, 21 have $k \leqslant 29$. In this note, we describe the results of searching for all primes of the form $k \cdot 2^m + 1$ with $k \leqslant 29$ and $m \leqslant r$. Here r is at least 4,000 and, in certain special cases, is as large as 8,000 or 10,000.

The numbers to be tested for primality were first sieved by solving the congruence

$$2^m \equiv -k^{-1} \pmod{p}$$

for all primes p less than 4×10^6. This was done by making use of a modification of an algorithm mentioned by Knuth [4, p. 9]. All values of $2^m \pmod{p}$ were computed for $0 \leqslant m \leqslant 100$ and stored in a table; next, all values of $-k^{-1}2^{-100n} \pmod{p}$ ($0 \leqslant n \leqslant 100$) were computed and looked up in the table by hashing. When a match was found, $k2^{m+100n} + 1$ was known to be divisible by p. This preliminary sieving technique eliminated about 90% of all the numbers.

The remaining numbers were tested for primality by using the test of Proth; see Robinson [6]. Since the numbers involved in this testing are very large, the algorithm of recursive bisection (Knuth [3, p. 258]) was used to increase the speed of multiplication. This algorithm allows two n-bit numbers to be multiplied in three $\frac{1}{2}n$ bit multiplications, provided n is a power of 2. For $n = 8192$, this technique is 4.8 times faster than the usual multiplication algorithm.

Also, advantage was taken of the special form of the numbers in order to reduce the problem of division by $k \cdot 2^m + 1$ to that of division by k. The results of our computations are presented in Table 1 below. These calculations were performed in over 100 CPU hours on an AMDAHL 470-V7 computer.

The upper bound on the range of m was increased beyond 4000 when it was felt that the density of Fermat number factors in the sequence $\{k2^m + 1, m = 2, 3, \ldots, 4000\}$ was large enough that there was a good chance of finding another such factor. Four of these primes are divisors of Fermat numbers. They are:

$$5 \cdot 2^{3313} + 1 \mid F_{3310},$$

Received November 30, 1979; revised March 3, 1980.
1980 *Mathematics Subject Classification.* Primary 10A25, 10A40, 10–04.

$$29 \cdot 2^{2027} + 1 \mid F_{2023},$$

$$29 \cdot 2^{4727} + 1 \mid F_{4724},$$

$$17 \cdot 2^{6539} + 1 \mid F_{6537}.$$

It is interesting to note that of the 15 primes, of the form $k \cdot 2^m + 1$ for $k = 5$ and $m \leqslant 10000$, seven are factors of Fermat numbers. The reason for this high density of Fermat factors is unknown.

TABLE 1

k	Range of m	All values of m such that $k \cdot 2^m + 1$ is prime
3	$1500 < m \leqslant 4000$	2208, 2816, 3168, 3189, 3912
5	$2000 < m \leqslant 10000$	3313, 4687, 5947
7	$1500 < m \leqslant 8000$	1804, 2256, 6614
9	$1500 < m \leqslant 4000$	2297, 2826, 3230, 3354, 3417, 3690
11	$1500 < m \leqslant 4000$	3225
13	$1500 < m \leqslant 4000$	
15	$1500 < m \leqslant 4000$	2808, 2875, 3128, 3888
17	$1500 < m \leqslant 8000$	2163, 3087, 5355, 6539, 7311
19	$1500 < m \leqslant 4000$	2038
21	$1500 < m \leqslant 4000$	1532, 1613, 1969, 2245, 2733
23	$1500 < m \leqslant 4000$	1961, 3929
25	$1500 < m \leqslant 4000$	1640, 3314, 3904, 3938
27	$1500 < m \leqslant 8000$	3080, 3322, 6419, 7639
29	$1500 < m \leqslant 8000$	2027, 3627, 4727, 5443, 7927

Mention should be made of the fact that A. O. L. Atkin and Rickert [7] independently discovered the factors of F_{3310} and F_{2023} given above. He has also discovered three other new factors of Fermat numbers. These factors, taken with those reported above and Gostin's [2] factor of F_{17}, bring the number of Fermat numbers known to be composite to 64.

Finally, it should be noted that, for each prime of the form $3r2^m + 1$ in Table 1, the number $3r2^m - 1$ was also tested for primality. Unfortunately, no pair of large twin primes was found.

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2

1 ROBERT BAILLIE, "New primes of the form $k \cdot 2^n + 1$," *Math. Comp.*, v. 33, 1979, pp. 1333–1336.

2. G. B. GOSTIN, "A factor of F_{17}," *Math. Comp.*, v. 34, 1980, pp. 975–976.

3. DONALD E. KNUTH, *The Art of Computer Programming*, Vol. II, *Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 1969.

4. DONALD E. KNUTH, *The Art of Computer Programming,* Vol. III, *Sorting and Searching,* Addison-Wesley, Reading, Mass., 1969.

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

6. R. 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.

7. A. O. L. ATKIN & N. W. RICKERT, "Some factors of Fermat numbers," *Abstracts Amer. Math. Soc.,* v. 1, 1980, p. 211.