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 $3 \leq k \leq 29$ 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 $m \geq n + 2$ 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 $k \leq 149$ and $m \leq 1500$. Only 25 of these primes are factors
of Fermat numbers, and of these, 21 have $k \leq 29$. In this note, we describe the results
of searching for all primes of the form $k \cdot 2^m + 1$ with $k \leq 29$ and $m \leq r$. 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 $4 \times 10^6$. 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 $0 \leq m \leq 100$ and stored in a table; next, all values of $-k^{-1}2^{-100n} \pmod{p}$ ($0 \leq n \leq 100$) 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 tech-
nique 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 multipli-
cation. This algorithm allows two $n$-bit numbers to be multiplied in three $\frac{3}{2}n$ bit multi-
lications, 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:

$$5 \cdot 2^{3313} + 1 \mid F_{3310}.$$
It is interesting to note that of the 15 primes, of the form \( k \cdot 2^m + 1 \) for \( k = 5 \) and \( m \leq 10000 \), seven are factors of Fermat numbers. The reason for this high density of Fermat factors is unknown.

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

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 \( F_{4724} \), 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.

