MATHEMATICS OF COMPUTATION
VOLUME 41, NUMBER 164
OCTOBER 1983, PAGES 661–673

# Factors of Fermat Numbers and Large Primes of the Form $k \cdot 2^n + 1$

By Wilfrid Keller

**Abstract.** A new factor is given for each of the Fermat numbers $F_{52}$, $F_{931}$, $F_{6835}$, and $F_{9448}$. In addition, a factor of $F_{75}$ discovered by Gary Gostin is presented. The current status for all $F_m$ is shown in a table. Primes of the form $k \cdot 2^n + 1$, $k$ odd, are listed for $31 \leq k \leq 149$, $1500 < n \leq 4000$, and for $151 \leq k \leq 199$, $1000 < n \leq 4000$. Some primes for even larger values of $n$ are included, the largest one being $5 \cdot 2^{13165} + 1$. Also, a survey of several related questions is given. In particular, values of $k$ such that $k \cdot 2^n + 1$ is composite for every $n$ are considered, as well as odd values of $h$ such that $3h \cdot 2^n \pm 1$ never yields a twin prime pair.

**1. Introduction.** The search for factors of Fermat numbers $F_m = 2^{2^m} + 1$ has been unusually intense in the last few years. Various investigators succeeded in discovering new factors. A summary of results obtained since 1978 was given recently by Gostin and McLaughlin [10]. Actually, something more had been accomplished, for we had been gathering some additional material during that same period of time. Thus, the following three new factors,

$$1985 \cdot 2^{933} + 1 \mid F_{931},$$

$$19 \cdot 2^{6838} + 1 \mid F_{6835},$$

$$19 \cdot 2^{9450} + 1 \mid F_{9448},$$

had already been found in 1980, 1978, and 1980, respectively. While this paper was being revised for the second time, we found another new factor,

$$21626655 \cdot 2^{54} + 1 \mid F_{52},$$

the second one known for that Fermat number. Furthermore, we are for the first time presenting the factor

$$3447431 \cdot 2^{77} + 1 \mid F_{75}$$

discovered by Gary Gostin, and we are pleased at having been expressly authorized to do so.

In the following, we shall give a full account of our investigation, which has gradually extended to several related questions. We shall also report on some further computational efforts in searching for factors of Fermat numbers.

Generally, two different ways of organizing that search are in use, both relying on the well-known fact that any factor of $F_m$ has the form $k \cdot 2^n + 1$, where $n \geq m + 2$

Received March 12, 1981; revised July 16, 1982 and February 8, 1983.
1980 *Mathematics Subject Classification.* Primary 10A25, 10A40; Secondary 10–04.
*Key words and phrases.* Fermat numbers, numbers of Ferentinou-Nicolacopoulou, factoring, trial division, large primes, covering set of divisors, twin primes.

©1983 American Mathematical Society
0025-5718/83 $1.00 + $.25 per page

and $k$ is odd. Throughout this paper, let $k$ always denote an odd integer. The two ways are:

*Trial division.* For fixed $n$, look for all $k$ less than some search limit $L_n$ to see if $k \cdot 2^n + 1$ divides some $F_m$, $m \leqslant n - 2$. In [12, p. 109], it was described how this is conveniently done.

*Tabulation of primes.* For fixed $k$, list all primes of the form $k \cdot 2^n + 1$ for $n$ up to some limit $N_k$. Then, for each prime $k \cdot 2^n + 1$ found, look to see if it divides some $F_m$, $m \leqslant n - 2$. For reference, see [20, p. 673] and [8, p. 1419].

In both cases, the size of the quantities involved in the computation is essentially that of the particular number tested as a possible factor.

Trial division is best suited if the index $m$ of the numbers $F_m$ to be investigated is small compared with the limit $L_n$ on $k$. Most recently this method has successfully been used for values $n \leqslant 420$ by Gostin and McLaughlin, and by Suyama, see [10], [23]. On the other hand, tabulation of primes of the form $k \cdot 2^n + 1$ becomes attractive if large limits $N_k$ on $n$ are envisaged. The primes in a sequence $\{k \cdot 2^n + 1\}$ for fixed $k$ are of interest in their own right, due to the irregularity and increasing sparseness of primes in such a sequence. The first substantial table was presented by Robinson [20] in 1958. His table has successively been extended by Matthew and Williams [17], Baillie [3], and Cormack and Williams [8]. A further extension was announced by Atkin and Rickert [2]. In each case, factors of Fermat numbers $F_m$ were discovered for $m \geqslant 255$. We have been following both the outlined ways in our search, as will be described in subsequent sections.

It should be pointed out that occasionally other methods of factoring have been used. The celebrated factorizations of $F_7$ and $F_8$ have been achieved through the continued fraction algorithm of Morrison and Brillhart [18], in the first case, and the Monte Carlo algorithm of Brent and Pollard [6], in the latter. However, such methods certainly do not apply unless the index $m$ of $F_m$ is quite small, since they demand an effective handling of numbers whose size is comparable to that of $F_m$ itself.

**2. Factors of Fermat Numbers.** Including the five new factors given here, there are now 90 known prime factors $k \cdot 2^n + 1$ of 75 different Fermat numbers $F_m$. The difference $n - m$ being always at least 2, it actually takes the values 2, 3, 4, 5, 6, 7, 8 with frequencies 47, 26, 11, 1, 2, 2, 1, respectively. The current status of the investigation of Fermat numbers was last displayed in 1975 [12], so it seems appropriate to give an updated version of the status list in Table 1. A complete list of the factors themselves may be assembled from Tables 3 and 4 of [24] (note the correction given in [10, p. 648]), Table 3 of [10], and the above Introduction.

Most of the factors $k \cdot 2^n + 1$ are 'small' in that $k < 2^n$. Those factors are easily proved prime by Proth's theorem (see [20, p. 673]), while 'succinct' proofs for the 12 factors having $k > 2^n$ require some additional information about $k$, as it was given by Brent [5] for 7 of these. For the other 5, corresponding to $F_m$ with $m = 10, 10, 12, 13, 17$, such proofs might be added without difficulty.

None of the known prime factors $p$ gives rise to a square factor $p^2$ of a Fermat number $F_m$. For the major part of them, this has been shown in [10]. We completed the test for the remaining factors

$$p = 5 \cdot 2^{3313} + 1, \quad 29 \cdot 2^{4727} + 1, \quad 17 \cdot 2^{6539} + 1,$$

and the five new ones given above. Except for the factors of $F_{52}$, $F_{75}$, and $F_{9448}$, these primes were independently tested by Philip McLaughlin (personal communication). In each case, the computed residue $R = F_m \bmod p^2$ correctly proved to be divisible by $p$.

The square factors of Fermat numbers have recently been characterized by Ribenboim [19] as follows: If the prime $k \cdot 2^n + 1$ divides some $F_m$, then $p^2$ also is a factor of $F_m$ if and only if $p$ satisfies the Wieferich congruence $2^{p-1} \equiv 1 \pmod{p^2}$; cf. [16]. Another necessary condition for $p^2$ to divide $F_m$ is $k^{p-1} \equiv 1 \pmod{p^2}$.

TABLE 1
*Status list*

| Values of m | Character of $F_m$ |
|---|---|
| 0, 1, 2, 3, 4 | Prime |
| 5, 6, 7, 8 | Composite and completely factored |
| 12* | Four prime factors known |
| 10*, 11*, 19, 30, 36, 38, 52, 150 | Two prime factors known |
| 9*, 13*, 15, 16, 17, 18, 21, 23, 25, 26, 27, 29, 32, 39, 42, 55, 58, 62, 63, 66, 71, 73, 75, 77, 81, 91, 93, 99, 117, 125, 144, 147, 201, 207, 215, 226, 228, 250, 255, 267, 268, 284, 287, 298, 316, 329, 416, 452, 544, 556, 692, 744, 931, 1551, 1945, 2023, 2456, 3310, 4724, 6537, 6835, 9448 | Only one prime factor known |
| 14 | Composite but no factor known |
| 20, 22, 24, 28, 31, 33, 34, 35, etc. | Character unknown |

*Cofactor known to be composite

**3. The Numbers of Ferentinou-Nicolacopoulou.** Let $a$ be an integer, $a \geq 2$. The numbers $F_{a,m} = a^{a^m} + 1$, which generalize the Fermat numbers $F_m = F_{2,m}$, were introduced by Ferentinou-Nicolacopoulou in 1963 and, more recently, some divisibility properties for them have been established by Ribenboim [19]. If $a$ is restricted to the even integers, then the numbers $F_{a,m}$, $m \geq 1$, show a structure very similar to that of Fermat numbers. First, for $a$ fixed, the numbers $F_{a,m}$ are pairwise relatively prime. Secondly, any prime factor $p$ of $F_{a,m}$ has the form $p = k \cdot 2^n + 1$, where $n > m$; more precisely, if $a = b \cdot 2^c$, $b$ odd, then $n \geq cm + 1$. Finally, if the prime $p$ divides some $F_{a,m}$, then $p^2$ also is a factor of $F_{a,m}$ if and only if $p$ satisfies the congruence $a^{p-1} \equiv 1 \pmod{p^2}$.

Let us recall the elementary fact which implies that $2^N + 1$ cannot be a prime unless $N = 2^m$: If $N$ has an odd factor $u > 1$, $N = uv$, and if $c \geq 2$, then $c^v + 1$

properly divides $c^N + 1$ (cf. [13, Theorem 17]). With this in mind, we distinguish three cases regarding the index $a$ of the numbers $F_{a,m}$:

(i) If $a = uv$ with an odd $u > 1$, then $a^{a^m/u} + 1$ is a proper factor of $F_{a,m}$.

(ii) If $a = 2^{uv}$ with an odd $u > 1$, then $2^{va^m} + 1$ is a proper factor of $F_{a,m}$.

(iii) If $a = 2^{2^r}$, then $F_{a,m}$ is a Fermat number $F_s$, where $s = r + m \cdot 2^r$.

As a consequence, $F_{a,m}$ can only be a prime if it is a Fermat number.

It seemed that no effective factorization of numbers $F_{a,m}$ had yet been attempted. So we examined a wide range of these numbers numerically. In determining many factors, we were led to the following observations.

Square factors of $F_{a,m}$ are readily found for $m = 1$. Thus, $29^2 \mid F_{14,1}$, $(5 \cdot 37)^2 \mid F_{18,1}$, $17^2 \mid F_{38,1}$, $17^2 \mid F_{40,1}$, $13^2 \mid F_{70,1}$, etc.

Apparently, every prime $p = k \cdot 2^n + 1$ divides $F_{2k,m}$ for some $m < n$, provided $n$ is not too small (in fact, no counterexample was found for $n > 9$). We are indebted to the referee for explaining this as follows: By Fermat's theorem we have $(2k)^{k \cdot 2^n} \equiv 1 \pmod{p}$. Hence, unless $n$ is very small, we have $(2k)^{k \cdot 2^m} \equiv -1 \pmod{p}$ for some $m$ slightly smaller than $n$. Therefore $p$ divides $(2k)^{k \cdot 2^m} + 1$. If $m > 1$, the latter is a proper factor of $F_{2k,m}$ because $(2k)^m/(k \cdot 2^m) = k^{m-1}$ is odd and $2k \geqslant 2$. If, instead, $m = 1$, we at once have $p \mid F_{2k,1}$.

Consider, for instance, the known primes $3 \cdot 2^n + 1$, which occur for

$$n = 1, 2, 5, 6, 8, 12, 18, 30, 36, 41, 66, 189, 201, 209, 276,$$
$$353, 408, 438, 534, 2208, 2816, 3168, 3189, 3912$$

(see [20], [17], [3], [8]). These primes divide the numbers $F_{6,m}$ for

$$m = 0, 1, 1, 4, 6, 10, 16, 27, 34, 38, 64, 185, 195, 203, 273,$$
$$346, 406, 436, 532, 2202, 2812, 3165, 3185, 3909,$$

respectively. The prime $3 \cdot 2^1 + 1 = F_{6,0} = 7$ should be discarded because $m$ was supposed to be positive. Note, however, that

$$F_{6,1} = 46657 = (3 \cdot 2^2 + 1) \cdot (3 \cdot 2^5 + 1) \cdot 37.$$

Numerical evidence suggests something more general: If $p = k \cdot 2^n + 1$, $k$ odd, is a prime number, and if $n$ is not too small, then for every $r = 1, 3, 5, \ldots$ which is not a multiple of $p$ there is an $m_r < n$ such that $p \mid F_{2kr,m_r}$. The explanation that was given for $r = 1$ immediately extends to this observation, since by Fermat's theorem $(2kr)^{k \cdot 2^n} \equiv 1 \pmod{p}$ whenever $(2kr, p) = (r, p) = 1$. Thus $p$ divides infinitely many numbers $F_{a,m}$, $a$ even. As a matter of fact, the prime $p$ is a divisor of $F_{a,m}$ for many additional values of $a$. To give an example, the prime $3 \cdot 2^{41} + 1$ divides $F_{a,m_a}$, where $m_a < 41$, for

$$a = 2, 6^*, 12, 16, 18^*, 30^*, 36, 42^*, 46, 54^*, 58, 60, 62, 66^*, 70, \ldots.$$

The values of $a$ of the form $2 \cdot 3 \cdot r$ corresponding to the above statement are marked with an asterisk.

**4. Searching by Trial Division.** In our search for factors of Fermat numbers we used trial division for all $n$ with $16 \leqslant n \leqslant 1002$, to the limits $K_n$ given in Table 2. All factors known to exist in that range were refound, and the new factors of $F_{52}$ and $F_{931}$ emerged.

Reporting on the first submitted version of this paper, the referee luckily enabled us to join a mutually coordinated action which had already been established between

Gary Gostin, Philip McLaughlin, and Hiromi Suyama (the authors of [10] and [23]) in order to further extend the search by trial division. With kind permission of the named investigators we are presenting in Table 3 the intervals additionally covered by them until very recently. That search produced the new factor of $F_{75}$. The reader should be advised that the reported work is still being continued.

TABLE 2

*Numbers $k \cdot 2^n + 1$, $k$ odd, tested by the author for $1 < k < K_n$ using trial division*

| n | $K_n$ | n | $K_n$ |
|---|---|---|---|
| 16-24 | $2^{32}$ | 103-202 | $10^5$ |
| 25-28 | $2^{56-n}$ | 203-610 | $2 \cdot 10^4$ |
| 29-56 | $2^{27}$ | 611-1002 | $5 \cdot 10^3$ |
| 57-102 | $3 \cdot 10^5$ | | |

TABLE 3

*Intervals for $k \cdot 2^n + 1$, $k$ odd, covered recently by other investigators*

| n | Interval | Investigator |
|---|---|---|
| 57-82 | $2^{20} < k < 2^{22}$ | Gostin |
| 114-134 | $2^{17} < k < 2^{18}$ | McLaughlin |
| 136-171 | $2^{16} < k < 2^{17}$ | McLaughlin |
| 203-231 | $\max(2^{13}, f_n)^* < k < 2^{15}$ | McLaughlin |
| 576-639 | $1 < k < f_n^*$ | Suyama |
| 640-707 | $5 \cdot 10^3 < k < f_n^*$ | Suyama |

* $f_n = 2^{16-(n \bmod 8)}$

TABLE 4

*Overall search limits for $k \cdot 2^n + 1$, $k$ odd, $1 < k < L_n$*

| n | $L_n$ | n | $L_n$ |
|---|---|---|---|
| 11-14 | $2^{47-n}$ | 135-171 | $2^{17}$ |
| 15-24 | $2^{32}$ | 172-202 | $10^5$ |
| 25-28 | $2^{56-n}$ | 203-231 | $\max(2^{15}, f_n)^*$ |
| 29-56 | $2^{27}$ | 232-610 | $\max(2 \cdot 10^4, f_n)^*$ |
| 57-82 | $2^{22}$ | 611-707 | $\max(5 \cdot 10^3, f_n)^*$ |
| 83-102 | $2^{20}$ | 708-1002 | $5 \cdot 10^3$ |
| 103 | $2^{19}$ | 1003-4000 | 200 |
| 104-134 | $2^{18}$ | 4001-8500 | 20 |

* $f_n = 2^{16-(n \bmod 8)}$

The overall search limits $L_n$ for $k \cdot 2^n + 1$ resulting from [10] (Table 2 and Note added in proof) and our Tables 2 and 3 are put together in Table 4. Also included are part of the results obtained for $n > 1002$, which are completely discussed in the next section.

The varying expression for the limits $f_n = 2^{16-(n \bmod 8)}$ encountered in the work of Suyama derives from the fact that he used a microcomputer with an 8-bit word. Let us briefly consider his proceeding (communicated personally): Setting $n = \lfloor n/8 \rfloor \cdot 8 + n \bmod 8$, $K = k \cdot 2^{n \bmod 8}$, and $N = \lfloor n/8 \rfloor$, the trial divisor $k \cdot 2^n + 1$ might be written as $k \cdot 2^n + 1 = K \cdot 256^N + 1$. Now, if $K$ is allowed to occupy two 8-bit words, i.e. $K < 2^{16}$, then $K \cdot 256^N + 1$ is representable by $N + 2$ words, $N - 1$ of which are zero words. The condition imposed on $K$ just means that $k < 2^{16-(n \bmod 8)} = f_n$. As to the convenience of such a representation, cf. Section 8.

**5. Primes of the Form $k \cdot 2^n + 1$.** Of the factors of Fermat numbers we found by tabulation of primes, only the given factors of $F_{6835}$ and $F_{9448}$ are new.

Listing primes of the form $k \cdot 2^n + 1$ for fixed $k$ up to a limit $N_k$, we always tested the numbers in question for all $n$ in the interval $1 \leqslant n \leqslant N_k$, thereby confirming existing tables. Generally, our limits were $N_k = 8500$ for $3 \leqslant k \leqslant 19$, $N_k = 4000$ for $21 \leqslant k \leqslant 199$, and $N_k = 1000$ for $201 \leqslant k \leqslant 1199$. In several cases, which are shown in Table 6, $N_k$ was taken to be much larger. Those primes with $n > 1000$ not published elsewhere are presented in Tables 5 and 6. (Exception to this is the single prime $9 \cdot 2^{5802} + 1$, which already appeared in [2].) The 3964-digit prime $5 \cdot 2^{13165} + 1$ was found on March 25, 1979. Beyond our limits, $k = 27$ and $k = 29$ have been searched by Cormack and Williams to $N_k = 8000$ [8]. It should be noticed that, while $13 \cdot 2^{1000} + 1$ is a prime, no further prime $13 \cdot 2^n + 1$ has been found for $1000 < n \leqslant 17000$ (cf. [17], [3], and [8]).

TABLE 5

*All primes of the form* $k \cdot 2^n + 1$ *for* $31 \leqslant k \leqslant 149$, $1500 < n \leqslant 4000$, *and for* $151 \leqslant k \leqslant 199$, $1000 < n \leqslant 4000$

| k | Values of n | k | Values of n |
|---|---|---|---|
| 31 | 1808, 1944 | 55 | 1996, 2744 |
| 33 | 1630, 3076, 3118 | 57 | 1828 |
| 35 | 2493, 3627 | 59 | 2685 |
| 37 | 1706, 1804, 1904, 2240, | 61 | 3328 |
| | 2632, 3104 | 63 | 2424, 2478, 3024, 3293 |
| 39 | 1602, 2211, 3049 | 65 | 1631, 1737, 1859, 1917, |
| 41 | 1991 | | 1999, 2353, 3477 |
| 43 | 2974, 3022, 3528 | 67 | 1692, 1782, 1870, 3602 |
| 45 | | 69 | 2159, 2290, 2306, 2335, |
| 47 | | | 3379 |
| 49 | 2334 | 71 | 2255 |
| 51 | 1917, 2660, 2967, 3447, | 73 | 1892, 1974, 2210, 3596 |
| | 3659 | 75 | 1615, 2017, 2157 |
| 53 | 1665, 2133, 2765 | 77 | 1639 |

TABLE 5 (*continued*)

| k | Values of n | k | Values of n |
|---|---|---|---|
| 79 | 1766, 2162 | 143 | |
| 81 | 1972, 2624, 2829, 3497, | 145 | 1552, 1968 |
| | 3945, 3995 | 147 | 1731, 2194, 2328, 2568, |
| 83 | 2425, 2773, 3253 | | 2915, 3554 |
| 85 | 2458, 2556, 3638, 3834 | 149 | 1599, 1815, 2499, 2995 |
| 87 | 2324, 2372 | 151 | 1124, 1760 |
| 89 | 1537, 1921, 3217 | 153 | 1001, 1237, 1565, 2665 |
| 91 | | 155 | 1253, 1301, 2449 |
| 93 | 1646, 2032, 2066, 2800, | 157 | 1460, 1776 |
| | 2816 | 159 | 1087, 2478, 3309, 3862 |
| 95 | 1849, 1987, 3437 | 161 | 1453, 3703 |
| 97 | 2026, 2732, 3880 | 163 | 1642 |
| 99 | 1617, 2025 | 165 | 1013, 1407, 1417, 1532, |
| 101 | 3767, 3831 | | 1887, 1902, 1993, 2137, |
| 103 | 3670 | | 2294, 2381, 2509, 3259 |
| 105 | 1631, 3063, 3331, 3461, | 167 | |
| | 3619 | 169 | 1050, 1470, 1478, 1614, |
| 107 | 3087 | | 1970, 2570 |
| 109 | 1574, 2034 | 171 | 1007, 3825, 3837 |
| 111 | 2344 | 173 | |
| 113 | 1541, 2473, 3461 | 175 | 1652, 3254, 3848 |
| 115 | 3048 | 177 | 1032, 1750, 2050, 3980 |
| 117 | 2656, 2851 | 179 | 1511, 1903, 2335, 3063, |
| 119 | 2471, 2773 | | 3459, 3623, 3655 |
| 121 | 1808 | 181 | 3560 |
| 123 | 1677 | 183 | 1289, 1616, 1736, 1994, |
| 125 | 1631, 1895, 2735, 3475 | | 2344, 3024 |
| 127 | 2764 | 185 | 1187, 1337, 2633, 2993, |
| 129 | 2433, 2817, 3165 | | 3963 |
| 131 | 2065, 3553 | 187 | 1926, 2802 |
| 133 | 1588, 1652, 1812, 3012, | 189 | 1445, 1590, 1606, 1861, |
| | 3308 | | 2037, 3538, 3730 |
| 135 | 1523, 1611, 1770, 1923, | 191 | 1249, 1409, 1715, 1995 |
| | 2053, 2099, 2242, 2796 | 193 | 1052, 1070, 1528, 1804, |
| 137 | 1979 | | 2568, 2914, 3712 |
| 139 | | 195 | 1045, 1270, 1861, 3623 |
| 141 | 1745, 1805, 2053, 2372, | 197 | 1175, 3047 |
| | 3375 | 199 | 1302 |

TABLE 6

*Primes of the form* $k \cdot 2^n + 1$ *for* $n > 4000$

| k | Range | Values of n |
|---|---|---|
| 3 | $4000 < n \leq 14000$ | |
| 5 | $10000 < n \leq 18000$ | 13165 |
| 7 | $8000 < n \leq 12000$ | |
| 9 | $4000 < n \leq 8500$ | 4842, 5802, 6937, 7967 |
| 11 | $4000 < n \leq 12000$ | 4543, 10179 |
| 13 | $4000 < n \leq 17000$ | |
| 15 | $4000 < n \leq 8500$ | 4410, 6804, 7050, 7392 |
| 17 | $8000 < n \leq 18000$ | |
| 19 | $4000 < n \leq 12000$ | 4386, 4438, 6838, 7498, 7998, 9450, 11890 |
| 45 | $4000 < n \leq 7000$ | 6146, 6284, 6359, 6923 |
| 47 | $4000 < n \leq 15000$ | 6115 |
| 91 | $4000 < n \leq 6000$ | 5028, 5536 |
| 139 | $4000 < n \leq 13000$ | 12614 |
| 167 | $4000 < n \leq 11000$ | 10183 |
| 173 | $4000 < n \leq 7000$ | 6253 |

The sequences $\{k \cdot 2^n + 1\}$ corresponding to the values $k = 47, 91, 139, 167, 173$ included in Table 6 are those for $k \leq 199$ which have the lowest density of primes for $n \leq 4000$. Below this limit, primes with $k = 47$ occur only for $n = 583$, 1483, and, likewise, primes occur for $k = 91$, $n = 8$, 168, 260, 696, for $k = 139$, $n = 2$, 14, 914, for $k = 167$, $n = 7$, 103, 151, 247, and for $k = 173$, $n = 1$, 13. In each of these cases our search was continued at least until the next prime appeared. Incidentally, the highest densities for fixed $k \leq 199$ and $n \leq 4000$ are observed for $k = 81$ (44 primes), $k = 135$ (41 primes), and $k = 165$ (43 primes). An indication of how such varying densities of primes come about is given in [3, p. 1333].

Among a number of primes obtained for some isolated values of $k > 199$, only the largest one, $271 \cdot 2^{7780} + 1$, seems worth mentioning.

**6. Sierpiński's Problem.** As was seen for $k = 47$, the smallest $n$ for which $k \cdot 2^n + 1$ is prime may be quite large in some cases. But there also exist values of $k$ such that $k \cdot 2^n + 1$ is always composite. For each of the known examples, like $k = 78557$, a covering set of divisors $C = \{p_1, p_2, \ldots, p_s\}$ is associated with the sequence $\{k \cdot 2^n + 1\}$, every term of it being divisible by at least one prime $p_i \in C$ (see [4]). Obviously, if a sequence $\{k_0 \cdot 2^n + 1\}$ has the covering set $C$, then the sequences $\{k_r \cdot 2^n + 1\}$ corresponding to $k_r = k_0 + r \cdot p_1 p_2 \cdots p_s$, $r \geq 0$, have all the same covering set $C$.

The nature of possible covering sets has been studied by Stanton [22], who also presented some unpublished results of Selfridge and van Rees. Stanton proved that a

covering set $C$ of cardinality $s < 6$ cannot occur, and that for $s = 6$ the only possible covering set is $C = \{3, 5, 7, 13, 17, 241\}$. The least $k$ of a sequence $\{k \cdot 2^n + 1\}$ covered by this set of primes is $k = 271129$. Generally, for every specified $s \geqslant 6$ only a finite number (which might be zero) of 'minimal' covering sets having $s$ primes does exist. Selfridge and van Rees found that for $s = 7$ there are just 20 different minimal covering sets. One of these, $C = \{3, 5, 7, 13, 19, 37, 73\}$, is the unique covering set $C$ such that $p_i \leqslant 73$ for all $p_i \in C$. This particular set of primes covers the sequence $\{k \cdot 2^n + 1\}$ for $k = 78557$, the smallest known value of $k$ for which $k \cdot 2^n + 1$ is always composite.

Let $k^*$ denote the smallest $k$ whichever of that kind. The problem of determining $k^*$, first posed by Sierpiński in 1960 [21], remains unsolved. But it has been known for about twenty years that $383 \leqslant k^* \leqslant 78557$, and it is believed that in fact $k^* = 78557$ (for the history of the problem, refer to [4]). The true lower bound for $k^*$ has been increased quite recently to 3061 by Baillie, Cormack and Williams [4]. Moreover, they listed all 120 values of $k < 78557$ for which no prime $k \cdot 2^n + 1$ is known. They showed that $k \cdot 2^n + 1$ is composite for all $n \leqslant 16000$ if $k = 3061$, for all $n \leqslant 8000$ if $k$ assumes one of seven additional values with $3061 < k < 10000$, and for all $n \leqslant 2000$ in the remaining 112 cases. It has since become desirable to eliminate as many of these $k$ as possible by searching for corresponding primes $k \cdot 2^n + 1$ with $n > 2000$. This has thoroughly been accomplished by Jaeschke [14] for $2000 < n \leqslant 3900$, who could thus rule out 30 of the former 120 uncertain candidates for $k^*$.

After redoing and corroborating the reported computations of Baillie, Cormack and Williams, and Jaeschke, we have been able to amplify the scope of that numerical investigation considerably. In Table 7 we give all 21 values of $k$, $10000 < k < 78557$, for which the least prime $k \cdot 2^n + 1$ has its exponent $n$ in the interval $3900 < n \leqslant 8000$. We would like to mention here that the two primes $74221 \cdot 2^{4188} + 1$ and $77267 \cdot 2^{4159} + 1$ had first been discovered by Gerhard Jaeschke (personal communication).

TABLE 7

*The least prime of the form* $k \cdot 2^n + 1$ *for some fixed values of* $k$, $10000 < k < 78557$

| k | n | k | n | k | n |
|---|---|---|---|---|---|
| 18203 | 6141 | 43429 | 4290 | 71869 | 5130 |
| 21167 | 6095 | 46159 | 4790 | 73189 | 4278 |
| 23779 | 5234 | 47911 | 5568 | 73253 | 6889 |
| 25339 | 4438 | 57503 | 5697 | 74221 | 4188 |
| 25861 | 4848 | 60829 | 6398 | 74959 | 4274 |
| 32393 | 4365 | 65477 | 5887 | 77267 | 4159 |
| 36781 | 4824 | 67913 | 5773 | 77341 | 5076 |

We are now left with 69 values of $k < 78557$ such that no prime of the form $k \cdot 2^n + 1$ exists for $n \leqslant 8000$. They may be drawn from Table 2 of [14] taking into account our Table 7. From these 69 values, 24 have been selected to pursue the search at least up to $n = 12000$. Some of these have even been pushed much further. The different bounds $B_k$ on $n$ reached are presented in Table 8. It should be remarked that for any particular $k$, all numbers $k \cdot 2^n + 1$ for $\lfloor B_k/1000 \rfloor \cdot 1000 < n \leqslant B_k$ could be dismissed by finding a small factor. Thus, for example, not a single number $67607 \cdot 2^n + 1$ for $17532 \leqslant n \leqslant 18170$ had to be properly tested for compositeness.

The sieving procedure we used for $1000 < n \leqslant 8000$ comprised the computation of residues modulo $p$ for all primes $p$ less than a certain limit which varied from $5 \cdot 10^4$ to $2 \cdot 10^6$ (the same limits were used for $3 \leqslant k \leqslant 19$; cf. Section 5). Thus, for a fixed $k$, only $t_k$ numbers $k \cdot 2^n + 1$ with $1000 < n \leqslant 8000$ survived our sieving procedure, where $22 \leqslant t_k \leqslant 184$ for all of the above-mentioned 69 values of $k$. Table 8 includes those 21 values of $k$ showing the lowest frequencies $t_k$ (in particular, $t_{67607} = 22$). Besides, we have $t_{3061} = 156$, $t_{5297} = 90$, and $t_{5359} = 73$. For the purpose of comparison, we recorded $t_k = 729, 300, 755, 851, 447, 327, 1032, 219, 280$ for $k = 3, 5, 7, 9, 11, 13, 15, 17, 19$.

While searching for least primes with $n \leqslant 8000$, $n$ was always advanced at full intervals of length 1000, even if a prime appeared. So it could be observed that a least prime occurring for large $n$ might nevertheless be closely followed by another prime. For instance, $47911 \cdot 2^n + 1$ is prime for $n = 5568, 5652$, $52909 \cdot 2^n + 1$ is prime for $n = 3518, 3606$, and $77521 \cdot 2^n + 1$ is prime for $n = 3336, 3360$ (cf. Table 7 and [14, Table 2]). Also, $11027 \cdot 2^n + 1$ is prime for $n = 1075, 1255, 1287, 1403, 1827$ and no other $n \leqslant 2000$.

TABLE 8

*For a given value of k no prime of the form $k \cdot 2^n + 1$ exists for $n \leqslant B_k$*

| k | $B_k$ | k | $B_k$ | k | $B_k$ |
|---|---|---|---|---|---|
| 3061 | 17007 | 21181 | 12091 | 54001 | 12115 |
| 4847 | 12062 | 22699 | 20133 | 60443 | 12260 |
| 5297 | 12030 | 25819 | 12001 | 62093 | 12016 |
| 5359 | 12069 | 27653 | 12344 | 65567 | 20154 |
| 5897 | 20170 | 28433 | 12072 | 67607 | 18170 |
| 7013 | 24160 | 34999 | 12273 | 69109 | 12021 |
| 18107 | 12278 | 39079 | 12249 | 75841 | 12211 |
| 19249 | 18157 | 46157 | 12046 | 77899 | 12209 |

As a result of our experiences with the referred computations, it appears that the Sierpiński problem of determining the least $k$ such that no prime $k \cdot 2^n + 1$ exists is not likely to be settled in the foreseeable future by mere computation, even if the most powerful equipment available today would be applied (cf. [11, p. 43]). That

impression might be supported by the following consideration. Of the 178 values of $k < 78557$ such that $k \cdot 2^n + 1$ is composite for all $n \leqslant 1000$ (see [14, Table 2]), one could eliminate 48, 23, 11, 11, 10, 5, and 0 finding a prime with $n$ in the interval $1000 \cdot i < n \leqslant 1000 \cdot (i + 1)$ for $i = 1, 2, 3, 4, 5, 6, 7$, respectively. The rate of success, so to speak, apparently tends to diminish. On the other hand, the extremely low density of possible candidates $k \cdot 2^n + 1$ for being a prime observed for most of the values of $k$ in Table 8 suggests that the primes sought may lie well beyond the largest prime presently known, in a number of cases.

**7. Twin Primes.** For each prime $k \cdot 2^n + 1$ listed during the search described in Section 5, the corresponding number $k \cdot 2^n - 1$ was checked for primality to see if a pair of twin primes could be detected. Of course, only values of $k$ which are multiples of 3 were to be considered. For $n > 600$ (cf. [3, p. 1333]), the only pairs found were $177 \cdot 2^{1032} \pm 1$, $213 \cdot 2^{726} \pm 1$, and $315 \cdot 2^{767} \pm 1$. Furthermore, the ranges $201 \leqslant k \leqslant 795$, $1000 < n \leqslant 3000$; $801 \leqslant k \leqslant 1197$, $1000 < n \leqslant 2000$; and $1203 \leqslant k \leqslant 1497$, $1 \leqslant n \leqslant 2000$ were searched for twin primes, and the additional pairs $291 \cdot 2^{1553} \pm 1$, $1035 \cdot 2^{1156} \pm 1$, $1065 \cdot 2^{1321} \pm 1$, and $1365 \cdot 2^{829} \pm 1$ were found.

Mention should be made of three considerably larger prime-pairs of that same form $k \cdot 2^n \pm 1$ discovered by Atkin and Rickert in 1979 [1] and 1980 [9]. These primes are $256200945 \cdot 2^{3426} \pm 1$, $347251905 \cdot 2^{2305} \pm 1$, and $1159142985 \cdot 2^{2304} \pm 1$, where all three values of $k$ are divisible by $15015 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$.

The concept of a covering set discussed in the preceding section similarly applies to a sequence $\{3h \cdot 2^n \pm 1\}$, $h$ odd and fixed, which fails to produce any twin pair of primes. The set of primes $C = \{p_1, p_2, \ldots, p_s\}$ will be said to be a covering set for the sequence $\{3h \cdot 2^n \pm 1\}$ if for every $n$ either $3h \cdot 2^n - 1$ or $3h \cdot 2^n + 1$ is divisible by at least one $p_i \in C$. For instance, the sequence $\{3 \cdot 79 \cdot 2^n \pm 1\}$ has the covering set $C = \{5, 7, 13, 17, 19, 241\}$, and $\{3 \cdot 269 \cdot 2^n \pm 1\}$ is covered by $C = \{5, 7, 13, 19, 37, 73\}$. Clearly, there are also infinitely many values of $h$ such that $3h \cdot 2^n \pm 1$ never gives a twin prime pair. On the other hand, for every odd $h$, $1 \leqslant h < 37$, there is a twin prime pair $3h \cdot 2^n \pm 1$ with $n \leqslant 14$. If we denote by $h^*$ the smallest value of $h$ such that $3h \cdot 2^n \pm 1$ never gives a twin prime pair, then we have $37 \leqslant h^* \leqslant 79$. Moreover, $h^*$ could only take one of the values $h = 37, 41, 51, 53, 57, 61, 63, 73, 75, 79$. None of these produces a prime pair for $n \leqslant 4000$. Also, there is no twin pair of the form $3 \cdot 37 \cdot 2^n \pm 1$ for $n \leqslant 20458$. In establishing this result, we discovered the prime $111 \cdot 2^{10883} + 1$; its companion, the composite number $111 \cdot 2^{10883} - 1$, has no divisor less than $10^7$.

**8. The Computations.** Nearly all of the computations reported here were performed on a TELEFUNKEN TR 440 computer using the Rational Arithmetic System [7] developed by Ingo Büchel and the author. That system is entirely written in the TAS assembly language and, in particular, it deals with arbitrarily large integers very efficiently. The system provides a procedure for integer division by a power of 2 based on the binary shift operation. This allows the reduction modulo $k \cdot 2^n + 1$ needed in testing numbers of that form to be done with a running time proportional to $n$ if $n$ is large.

For a description of that reduction algorithm, see [10, p. 647]; the reader may also consult [15, p. 614]. An improvement suggested by Hiromi Suyama (cf. Section 4) is based on the idea of representing $k \cdot 2^n + 1$ as $K \cdot 2^{wN} + 1$, where $w$ is the word length of a binary machine. Thus all shifting operations moving across the word boundaries could be avoided.

Our computing times on the TR 440 were as follows. Trying the divisibility test for $k \cdot 2^n + 1$ through, say, the whole interval $1 < k < 5000$ took about 200, 440, 1700, and 6300 seconds for $n = 100, 200, 500, 1000$, respectively, including the time for the preliminary sieving procedure. For large exponents $n$, the primality test for $k \cdot 2^n + 1$ required about $3.2(10^{-3}n)^3 + 5.9(10^{-3}n)^2$ seconds. In particular, 139 minutes were needed to test the prime $5 \cdot 2^{13165} + 1$. In a later stage of the computations, this could moderately be speeded up by introducing a few steps of the 'recursive bisection' method [15, pp. 278–279] into the squaring operation, which consumes the predominant part of the testing time.

Trial division for $16 \leqslant n \leqslant 56$ was done on a SIEMENS 7 · 882 computer taking advantage of the built-in extended precision floating-point arithmetic.

**Acknowledgements.** The author wishes to thank Gary Gostin, Philip McLaughlin, and Hiromi Suyama for their contributions to this paper. The author also thanks the computer operators for their tireless cooperation in carrying out this project.

Rechenzentrum der Universität Hamburg
Hamburg, Federal Republic of Germany

1. A. O. L. ATKIN & N. W. RICKERT, "On a larger pair of twin primes," *Notices Amer. Math. Soc.*, v. 26, 1979, p. A-373.

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

3. ROBERT BAILLIE, "New primes of the form $k \cdot 2^n + 1$," *Math. Comp.*, v. 33, 1979, pp. 1333–1336. MR **80h**: 10009. Table errata: MTE **585**, *Math. Comp.*, v. 38, 1982, p. 335. MR **82m**: 10013.

4. ROBERT BAILLIE, G. CORMACK & H. C. WILLIAMS, "The problem of Sierpiński concerning $k \cdot 2^n + 1$," *Math. Comp.*, v. 37, 1981, pp. 229–231. MR **83a**: 10006a. Corrigenda: *Math. Comp.*, v. 39, 1982, p. 308. MR **83a**: 10006b.

5. RICHARD P. BRENT, "Succinct proofs of primality for the factors of some Fermat numbers," *Math. Comp.*, v. 38, 1982, pp. 253–255. MR **82k**: 10002.

6. RICHARD P. BRENT & JOHN M. POLLARD, "Factorization of the eighth Fermat number," *Math. Comp.*, v. 36, 1981, pp. 627–630.

7. INGO BÜCHEL & WILFRID KELLER, *Ein Programmsystem für Rationale Arithmetik: Einführung und Beispielsammlung*, Bericht Nr. 8004, Rechenzentrum der Universität Hamburg, April 1980.

8. G. V. CORMACK & H. C. WILLIAMS, "Some very large primes of the form $k \cdot 2^m + 1$," *Math. Comp.*, v. 35, 1980, pp. 1419–1421. MR **81i**: 10011. Table Errata: MTE **586**, *Math. Comp.*, v. 38, 1982, p. 335. MR **82k**: 10011.

9. MARTIN GARDNER, "Mathematical games: Gauss's congruence theory was mod as early as 1801," *Scientific American*, v. 244, #2, February 1981, pp. 14–19.

10. GARY B. GOSTIN & PHILIP B. MCLAUGHLIN, JR., "Six new factors of Fermat numbers," *Math. Comp.*, v. 38, 1982, pp. 645–649.

11. RICHARD K. GUY, *Unsolved Problems in Number Theory*, Springer-Verlag, New York, 1981.

12. JOHN C. HALLYBURTON, JR & JOHN BRILLHART, "Two new factors of Fermat numbers," *Math. Comp.*, v. 29, 1975, pp. 109–112. MR **51** #5460. Corrigendum: *Math. Comp.*, v. 30, 1976, p. 198. MR **52** #13599.

13. G. H. HARDY & E. M. WRIGHT, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Univ. Press, Oxford, 1979.

14. G. JAESCHKE, "On the smallest $k$ such that all $k \cdot 2^n + 1$ are composite," *Math. Comp.*, v. 40, 1983, pp. 381–384.

15. DONALD E. KNUTH, *The Art of Computer Programming*, Vol. 2: *Seminumerical Algorithms*, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

16. D. H. LEHMER, "On Fermat's quotient, base two," *Math. Comp.*, v. 36, 1981, pp. 289–290.

17. G. MATTHEW & H. C. WILLIAMS, "Some new primes of the form $k \cdot 2^n + 1$," *Math. Comp.*, v. 31, 1977, pp. 797–798. MR **55** #12605.

18. MICHAEL A. MORRISON & JOHN BRILLHART, "A method of factoring and the factorization of $F_7$," *Math. Comp.*, v. 29, 1975, pp. 183–205. MR **51** #8017.

19. P. RIBENBOIM, "On the square factors of the numbers of Fermat and Ferentinou-Nicolacopoulou," *Bull. Soc. Math. Grèce (N. S.)*, v. 20, 1979, pp. 81–92.

20. 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.

21. W. SIERPIŃSKI, "Sur un problème concernant les nombres $k \cdot 2^n + 1$," *Elem. Math.*, v. 15, 1960, pp. 73–74. MR **22** #7983. Corrigendum: *Elem. Math.*, v. 17, 1962, p. 85.

22. R. G. STANTON, "Further results on covering integers of the form $1 + k2^n$ by primes," *Lecture Notes in Math.*, Vol. 884: *Combinatorial Mathematics* VIII, Springer-Verlag, Berlin and Heidelberg, 1981, pp. 107–114.

23. HIROMI SUYAMA, "Searching for prime factors of Fermat numbers with a microcomputer," *bit*, v. 13, 1981, pp. 240–245. (Japanese) MR **82c**: 10012.

24. H. C. WILLIAMS, "Primality testing on a computer," *Ars Combin.*, v. 5, 1978, pp. 127–185. MR **80d**: 10002.