MATHEMATICS OF COMPUTATION
VOLUME 37, NUMBER 155
JULY 1981

The Problem of Sierpiński Concerning $k \cdot 2^n + 1$

By Robert Baillie, G. Cormack and H. C. Williams

Abstract. Let k_0 be the least odd value of k such that $k \cdot 2^n + 1$ is composite for all $n \geqslant 1$. In this note, we present the results of some extensive computations which restrict the value of k_0 to one of 119 numbers between 3061 and 78557 inclusive. Some new large primes are also given.

We assume throughout that k is odd, positive and that $n \geqslant 1$. Sierpiński proved [5], [6] that there are infinitely many values of k such that $k \cdot 2^n + 1$ is composite for all n, by showing that, for

$$k \equiv 1 \pmod{(2^{32} - 1) \cdot 641} \quad \text{and} \quad k \equiv -1 \pmod{6700417},$$

every integer in the sequence $k \cdot 2^n + 1$ is divisible by at least one of the primes in the "covering set" $\{3, 5, 17, 257, 641, 65537, 6700417\}$. There are smaller values of k than those in Sierpiński's arithmetic progression, which still have this covering set. The least of these is $k = 201\ 44650\ 31451\ 65177$. For this k, we have

$$\begin{array}{llll}
k \cdot 2^{2n} + 1 \equiv 0 & \pmod{3} & k \cdot 2^{16n+7} + 1 \equiv 0 & \pmod{257} \\
k \cdot 2^{4n+1} + 1 \equiv 0 & \pmod{5} & k \cdot 2^{32n+31} + 1 \equiv 0 & \pmod{65537} \\
k \cdot 2^{8n+3} + 1 \equiv 0 & \pmod{17} & k \cdot 2^{64n+47} + 1 \equiv 0 & \pmod{641}
\end{array}$$

$$k \cdot 2^{64n+15} + 1 \equiv 0 \pmod{6700417}.$$

Sierpiński also points out that one of the primes 3, 5, 7, 13, 17, 241 will divide $k \cdot 2^n + 1$ for certain other values of k. The least of these is 271129. Finally, he mentions that the problem of determining the least value k_0 of k such that $k \cdot 2^n + 1$ is always composite is unsolved. This problem was posed again by Guy [3].

We have not considered the possibility that k be even here because any power of 2 which divides k can be absorbed into the 2^n part of the expression $k \cdot 2^n + 1$. Hence, we would only need to consider $k = 2^r$ and $k2^n + 1 = 2^{n+r} + 1$. The only primes of this form are the Fermat primes $2^{2^m} + 1$. If $r < 16$, we know that there is a prime of the form $2^{n+r} + 1$; however, if $r = 16$ ($k = 65536$), it is not known whether or not there is a prime of this form. Certainly, there is none with $n < 10^6$. In this case there is no finite covering, but it may well be true that there are no primes.

In 1962, J. L. Selfridge (unpublished) discovered that one of the primes 3, 5, 7, 13, 19, 37, 73 always divides $78557 \cdot 2^n + 1$. He also remarks [4] that there exists a prime of the form $k \cdot 2^n + 1$ for any $k < 383$ and that $383 \cdot 2^n + 1$ is composite for all $n < 2313$. In 1976, N. S. Mendelsohn and B. Wolk (unpublished) found that

Received August 29, 1980; revised October 27, 1980.
1980 *Mathematics Subject Classification.* Primary 10–04, 10A25.

$383 \cdot 2^n + 1$ is composite for all $n \leqslant 4017$. Thus, at that time it was known that k_0 exists and that $383 \leqslant k_0 \leqslant 78557$.

If $K(x)$ is the number of odd $k \leqslant x$ such that $k \cdot 2^n + 1$ is prime for some n, then Sierpiński's proof [5] implies that $K(x) < x/2$ for all sufficiently large x. Erdös and Odlyzko [2] show that there is a positive constant c such that $K(x) > cx$ for $x \geqslant 1$.

In this note, we report on some extensive calculations which have further restricted the possible value of k_0. These calculations, which required several hundred hours of CPU time, were performed on the AMDAHL 470-V7 computer at the University of Manitoba and the CDC 6500 at the Computer-Based Education Research Laboratory at the University of Illinois.

For each odd value of k ($383 \leqslant k < 78557$), we attempted to find a prime of the form $k \cdot 2^n + 1$. When $k < 10000$, we searched for such a prime with n up to at least 8000. For $k > 10000$, we searched for such a prime with $n \leqslant 2000$. For large values of n, we often used the methods of Cormack and Williams [1] to find these primes. We summarize our results for $k < 10000$ in Table 1. The eight values of k here are the only ones less than 10000 for which no prime of the form $k \cdot 2^n + 1$ is known. Also, for these values of k, no prime of this form exists for $n \leqslant B$.

TABLE 1

k	B	k	B
3061	16000	5897	8170
4847	8102	7013	8105
5297	8070	7651	8080
5359	8109	8423	8000

During these computations, we found some rather large primes. We give those with $n \geqslant 3000$ in Table 2. For each k, the value of n given is the least n such that $k \cdot 2^n + 1$ is prime.

TABLE 2

k	n	k	n
383	6393	7957	5064
2897	9715	8543	5793
6313	4606	9323	8313
7493	5249		

In Table 3, we give all the 110 values of k ($10000 < k < 78557$) such that $k \cdot 2^n + 1$ is composite for all $n \leqslant 2000$.

TABLE 3

10223,	10583,	10967,	12527,	13787,	14027,	16519,	16817,	16987,	17597,
17701,	18107,	18203,	19021,	19249,	20851,	21167,	21181,	22699,	23779,
24151,	24737,	25171,	25339,	25819,	25861,	27653,	27923,	28433,	30091,
31951,	32161,	32393,	33661,	34565,	34711,	34999,	35987,	36781,	36983,
37561,	38029,	39079,	39781,	40547,	42257,	43429,	44131,	44903,	45737,
46157,	46159,	46187,	46403,	46471,	47179,	47897,	47911,	48833,	49219,
50693,	51617,	51917,	52771,	52909,	53941,	54001,	54739,	54767,	55459,
56543,	57503,	59569,	60443,	60541,	60829,	62093,	62761,	63017,	63379,
64007,	64039,	65057,	65477,	65567,	65791,	67193,	67607,	67759,	67913,
70261,	71417,	71671,	71869,	72197,	73189,	73253,	74191,	74221,	74269,
74959,	75841,	76261,	76759,	76969,	77267,	77341,	77521,	77899,	78181

There are only 118 values of $k < 78557$ that need to be tested further. There does not appear to be any reason to believe that any of these produce only composite values of $k \cdot 2^n + 1$. Unlike the values of k where $k \cdot 2^n + 1$ is known to always be composite, these k seem to have no small covering set. For these k, it may just be that the density of primes in the sequence $\{k \cdot 2^n + 1\}$ is small so that they must be searched up to large values of n. It would be interesting to see how many of these 118 k values could be eliminated by a large, fast computer like the CRAY-1.

Computer-Based Education Research Laboratory
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

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

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

1. G. Cormack & H. C. Williams, "Some very large primes of the form $k \cdot 2^m + 1$," *Math. Comp.*, v. 35, 1980, pp. 1419–1421.

2. P. Erdös & A. M. Odlyzko, "On the density of odd integers of the form $(p - 1)2^{-n}$ and related questions," *J. Number Theory*, v. 11, 1979, pp. 257–263.

3. R. K. Guy, "Some unsolved problems," in *Computers in Number Theory* (A. O. L. Atkin and B. J. Birch, Eds.), Academic Press, New York, 1971, pp. 415–422.

4. J. L. Selfridge, "Solution to problem 4995," *Amer. Math. Monthly*, v. 70, 1963, p. 101.

5. W. Sierpiński, "Sur un problème concernant les nombres $k \cdot 2^n + 1$," *Elem. Math.*, v. 15, 1960, pp. 73–74; Corrigendum, v. 17, 1962, p. 85.

6. W. Sierpiński, 250 *Problems in Elementary Number Theory*, American Elsevier, New York, 1970, p. 10 and p. 64.