MATHEMATICS OF COMPUTATION
VOLUME 40, NUMBER 161
JANUARY 1983, PAGES 381-384

On the Smallest k Such That All $k \cdot 2^N + 1$ Are Composite

By G. Jaeschke

Abstract. In this note we present some computational results which restrict the least odd value of k such that $k \cdot 2^n + 1$ is composite for all $n \geqslant 1$ to one of 91 numbers between 3061 and 78557, inclusive. Further, we give the computational results of a relaxed problem and prove for any positive integer r the existence of infinitely many odd integers k such that $k \cdot 2^r + 1$ is prime but $k \cdot 2^v + 1$ is not prime for $v < r$.

Sierpinski's Problem. In 1960 Sierpinski [4] proved that the set S of odd integers k such that $k \cdot 2^n + 1$ is composite for all n has infinitely many elements (we call them 'Sierpinski numbers'). In his proof Sierpinski used as covering set Q_0 the set of the seven prime divisors of $2^{64} - 1$ (a 'covering set' means here a finite set of primes such that every integer of the sequence $k \cdot 2^n + 1$, $n = 1, 2, \ldots$, is divisible by at least one of these primes). All Sierpinski numbers with Q_0 as covering set have at least 18 decimal digits; see [1]. Therefore, the question arises whether there exist smaller Sierpinski numbers $k \in S$. Several authors (for instance [2], [3]) found Sierpinski numbers smaller than 1000000 which are listed in Table 1 together with their coverings. Thus, the smallest Sierpinski number known up to now is $k = 78557$.

For the discussion whether 78557 is actually the smallest Sierpinski number k_0, we define for every odd integer the number ω_k as follows (U = set of odd integers):

$$(1) \qquad \begin{aligned} &\omega_k = \infty && \text{for } k \in S, \\ &\omega_k = \min\{n \mid k \cdot 2^n + 1 \text{ is prime}\} && \text{for } k \in U - S. \end{aligned}$$

Let R be the set of all odd integers $k < 78557$. We inspected all values $k \in R$ in order to determine ω_k. It turned out that

$$\begin{aligned} &\omega_k \geqslant 100 && \text{only for 1002 elements } k \in R, \\ &\omega_k \geqslant 1000 && \text{only for 178 elements } k \in R. \end{aligned}$$

These 178 odd integers k are listed together with ω_k (as far as it is known) in Table 2. The test range for the exponent ω_k for the numbers $k > 10000$ in Table 2 was $\omega_k \leqslant 3900$. In this table the results of the previously published paper of Baillie, Cormack and Williams [1] are included. So there remain only 90 odd integers $k < 78557$ that need to be tested further. Table 2 contains 33 new primes of the form $k \cdot 2^n + 1$ with $n \geqslant 2000$.

A further open question is whether the above-mentioned 11 Sierpinski numbers are the only ones < 1000000.

Received May 16, 1978; revised November 17, 1981 and June 21, 1982.
1980 *Mathematics Subject Classification.* Primary 10A25, 10A40.

TABLE 1

Sierpinski numbers less than 10^6

Sierpinski number	Covering set
78557	Q_1
271129	Q_2
271577	Q_2
327739	Q_4
482719	Q_2
575041	Q_2
603713	Q_2
808247	Q_1
903983	Q_2
934909	Q_3
965431	Q_2

with

$$Q_1 = \{3, 5, 7, 13, 19, 37, 73\}$$
$$Q_2 = \{3, 5, 7, 13, 17, 241\}$$
$$Q_3 = \{3, 5, 7, 13, 19, 73, 109\}$$
$$Q_4 = \{3, 5, 7, 13, 17, 97, 257\}$$

The main part of the calculations reported in this note was performed on an IBM/370 System, Model 158 at the IBM Heidelberg Scientific Center.

Related Problems. In the following we shall discuss two results which are closely related to the problem stated in the title of this paper.

Result 1. The smallest integer k such that all numbers $k \cdot 2^n + 1$ and $k + 2^n$ are composite belongs to the following set C of cardinality 17:

$$C = \{5297, 5359, 7013, 19249, 28433, 32161, 39079, 44131, 47911, \\ 48833, 60443, 62761, 67607, 74191, 75841, 77899, 78557\}.$$

For all $k \in C$ no prime of the form $k + 2^n$ with $n \leqslant 100$ has been found. Thus, if any $k \in C$ has a covering set (with respect to the sequence $k \cdot 2^n + 1$) where all primes are less than 2^{100}, then all numbers $k + 2^n$ are composite (see [5]).

Result 2. The second result is a theorem on the numbers ω_k defined above.

THEOREM. *For any positive integer r there exist infinitely many odd numbers k such that $\omega_k = r$.*

Proof. Assume $r \geqslant 2$, since for $r = 1$ all $k = (p - 1)/2$ with $p \equiv 3 \bmod 4$ yield $\omega_k = 1$. Let T_r denote the set of primes that divide $2^r + 1$ or $2^\rho - 1$ for some ρ with $2 \leqslant \rho \leqslant r$, let $Q_r = \{p_1^{(r)}, \ldots, p_{r-1}^{(r)}\}$ consist of the $r - 1$ smallest odd primes not belonging to T_r, and let w_r be the product of the primes in Q_r and the prime divisors of $2^r + 1$. Let further x_0 be the smallest positive solution x to the following system of congruences:

$$\text{(2)} \qquad x \equiv 1 \mod \prod_{p | 2^r + 1} p$$

$$x \cdot 2^v + 2^{v-1} + 1 \equiv 0 \mod p_{v-1}^{(r)}, \; v = 2, \ldots, r.$$

TABLE 2

Primes $k \cdot 2^{\omega_k} + 1$ with $k < 78557$ and $\omega_k \geqslant 1000$

k	ω_k	k	ω_k	k	ω_k	k	ω_k
383	6393	19249	----	40571	1673	60829	----
881	1027	20851	----	41809	1402	61519	1290
1643	1465	21143	1061	42257	2667	62093	----
2897	9715	21167	----	42409	1506	62761	----
3061	----	21181	----	43429	----	63017	----
3443	3137	21901	1540	43471	1508	63379	2070
3829	1230	22699	----	44131	----	64007	----
4847	----	22727	1371	44629	1270	64039	2246
4861	2492	22951	1344	44903	----	65057	----
5297	----	23701	1780	45713	1229	65477	----
5359	----	23779	----	45737	2375	65539	1822
5897	----	24151	2508	46157	----	65567	----
6319	4606	24737	----	46159	----	65623	1746
6379	1014	24769	1514	46187	----	65791	2760
7013	----	24977	1079	46403	3057	65971	1224
7493	5249	25171	2456	46471	----	67193	----
7651	----	25339	----	47179	2918	67607	----
7909	2174	25343	1989	47897	----	67759	----
7957	5064	25819	----	47911	----	67831	1720
8119	1162	25861	----	48091	1476	67913	----
8269	1150	26269	1086	48323	1369	68393	1901
8423	----	27653	----	48833	----	69107	----
8543	5793	27923	----	49219	----	69109	----
8929	1966	28433	----	----	----	70261	3048
9323	3013	29629	1498	50693	----	71417	----
10223	----	30091	2184	51617	2675	71671	----
10583	2689	31951	3084	51917	----	71869	----
10967	2719	32161	----	52771	----	72197	2171
11027	1075	32393	----	52909	3518	73189	----
11479	1702	32731	1720	53941	----	73253	----
12395	1111	33661	----	54001	----	73849	1202
12527	2435	34037	1671	54739	----	74191	----
13007	1655	34565	3361	54767	----	74221	----
13787	----	34711	----	55459	----	74269	----
14027	----	34999	----	56543	2501	74959	----
16519	3434	35987	2795	56731	1172	75841	----
16817	---	36781	----	56867	1127	76261	2156
16987	2748	36983	----	57647	1259	76759	---
17437	1812	37561	----	57503	----	76969	3702
17597	3799	38029	2778	57949	1058	77267	----
17629	1094	39079	----	58243	1136	77341	----
17701	2700	39241	1120	59569	----	77521	3336
18107	----	39781	----	60443	----	77899	----
18203	---	40547	----	60541	----	78181	----
19021	2608	40553	1077	60737	1411		

Define P_r to be the set of all primes

$$p \equiv x_0 \cdot 2^{r+1} + 2^r + 1 \mod w_r \cdot 2^{r+1}.$$

Then we show

(3) P_r is infinite,

(4) for every $p \in P_r$ we have $\omega_{(p-1)/2^r} = r$.

In order to prove (3) we have only to show that $w_r 2^{r+1}$ and $x_0 \cdot 2^{r+1} + 2^r + 1$ are coprime since then (3) follows from Dirichlet's Prime Number Theorem. If q were a common divisor of these 2 numbers, we would have

$$w_r \equiv 0 \mod q \tag{5}$$

and

$$x_0 \cdot 2^{r+1} + 2^r + 1 \equiv 0 \mod q. \tag{6}$$

We distinguish two cases with respect to (5):

(a) $q \mid 2^r + 1$. Then we have $2^r + 1 \equiv 0 \bmod q$. Hence by (6) $x_0 \equiv 0 \bmod q$, which contradicts the first congruence in (2).

(b) $q \in Q_r$. Then we have $q = p_{v-1}^{(r)}$ for some v with $2 \leqslant v \leqslant r$ and therefore $x_0 \cdot 2^v + 2^{v-1} + 1 \equiv 0 \bmod q$. If this congruence is multiplied by 2^{r+1-v}, we obtain $x_0 \cdot 2^{r+1} + 2^r + 2^{r+1-v} \equiv 0 \bmod q$, and by means of (6) $2^{r+1-v} \equiv 1 \bmod q$ and $q \mid 2^{r+1-v} - 1$, which contradicts the definition of Q_r. Thus, the infinity of P_r is proved.

In order to prove (4) let p be a prime, $p = x_0 \cdot 2^{r+1} + 2^r + 1 + \lambda w_r \cdot 2^{r+1}$ with $\lambda \geqslant 1$ and $k = (p-1)/2^r$. Then $k \cdot 2^r + 1$ is prime, hence $\omega_k \leqslant r$. If we had $1 \leqslant \mu = \omega_k < r$, then $k \cdot 2^\mu + 1$ would be a prime and this would produce a contradiction as follows. From $k \cdot 2^r + 1 = p = x_0 \cdot 2^{r+1} + 2^r + 1 + \lambda w_r \cdot 2^{r+1}$ it follows that $k = 2x_0 + 1 + 2\lambda w_r$, hence $k \cdot 2^\mu + 1 = x_0 \cdot 2^{\mu+1} + 2^\mu + \lambda w_r \cdot 2^{\mu+1} + 1 = x_0 \cdot 2^v + 2^{v-1} + 1 + \lambda w_r \cdot 2^v$ for $v = \mu + 1$, therefore $2 \leqslant v \leqslant r$. But then we have $k \cdot 2^\mu + 1 \equiv 0 \bmod p_{v-1}^{(r)}$ by (2) and $k \cdot 2^\mu + 1$ is not prime. Thus, $\omega_k = r$.

Acknowledgements. The author would like to thank his colleague H. Eberle for valuable comments in editing this paper, and M. Bergen and U. Schauer for their programming assistance.

IBM Scientific Center
Heidelberg, West Germany

1. R. Baillie, G. Cormack & H. C. Williams, "The problem of Sierpinski concerning $k \cdot 2^n + 1$," *Math. Comp.*, v. 37, 1981, pp. 229–231. Corrigenda, *Math. Comp.*, v. 39, 1982, p. 308.

2. N. S. Mendelsohn, "The equation $\phi(x) = k$," *Math. Mag.*, v. 49, 1976, pp. 37–39.

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

4. W. Sierpinski, "Sur un probleme concernant les nombres $k \cdot 2^n + 1$," *Elem. Math.*, v. 15, 1960, pp. 73–74.

5. R. G. Stanton & H. C. Williams, *Further Results on Coverings of the Integers* $1 + k \cdot 2^n$ *by Primes*, Lecture Notes in Math., vol. 884, Combinatorial Mathematics VIII, pp. 107–114, Springer-Verlag, Berlin and New York, 1980.