GENERALIZED SIERPIŃSKI NUMBERS BASE b

AMY BRUNNER†, CHRIS K. CALDWELL, DANIEL KRYWARUCZENKO†,
AND CHRIS LOWNSDALE†

Abstract. Sierpiński proved that there are infinitely many odd integers k such that $k \cdot 2^n+1$ is composite for all $n \geq 0$. These k are now called Sierpiński numbers. We define a Sierpiński number base b to be an integer $k > 1$ for which $\gcd(k+1, b-1) = 1$, k is not a rational power of b, and $k \cdot b^n+1$ is composite for all $n > 0$. We discuss ways that these can arise, offer conjectured least Sierpiński number in each of the bases $2 < b \leq 100$ (34 are proven), and show that all bases b admit Sierpiński numbers. We also show that under certain circumstances there are base b Sierpiński numbers k for which $k, k^2, k^3, ..., k^{2^r-1}$ are each base b Sierpiński numbers.

1. Introduction and History

In 1958, R. M. Robinson [26] formed a table of primes of the form $k \cdot 2^n+1$ for odd integers $1 \leq k < 100$ and $0 \leq n \leq 512$. He found primes for all k values except 47. Some then wondered "Is there an odd k value such that $k \cdot 2^n+1$ is always composite?" In 1960, W. Sierpiński [29] proved that there were indeed infinitely many such odd integers k. He did this by finding a small set of primes S such that for a suitable choice of k, every term of the sequence $k \cdot 2^n+1$ ($n > 0$) is divisible by a prime in his "cover" S. The values k which make every term in the sequence composite are now called **Sierpiński numbers**. Sierpiński however neither gave a value of k nor sought the least such k.

In 1962, Selfridge [unpublished] showed that $k = 78557$ is also a Sierpiński number, and this is now believed to be the least Sierpiński number. For three decades mathematicians have been testing all of the values of k less than 78557 to prove this conjecture [2, 9, 20, 22]. All values except $10223, 21181, 22699, 24737, 55459$, and 67607 have now been eliminated by finding a prime in the corresponding sequence [18].

There are two standard methods of generalizing Sierpiński numbers. Several have generalized this idea by altering the restrictions on k [10, 11, 14, 21]. For example, one may seek Sierpiński numbers k for which all of $k, k^2, k^3, \ldots, k^r$ are also Sierpiński numbers for arbitrarily large integers r [14]. We will provide a similar (but weaker) result as Theorem 7.1.

On the Internet several groups have generalized Sierpiński's result to other bases b [4, 30, 31]. (See, for example, the results in Table 1.) There was also a short note by Bowen in 1964 [5] which we will mention in the next section. But at the time we began our investigation, none of these presented a systematic study of the generalization or even a careful study of the definition. In this paper we will fill this

Key words and phrases. Sierpiński number, covering set, generalized Fermat number.

†Undergraduate student. The beginning of this work was partially supported by a University of Tennessee at Martin College of Engineering and Natural Sciences undergraduate research grant.

TABLE 1. Conjectured least Sierpiński numbers k base b

b	N	k {cover}	k's not yet eliminated	ref
2	36	78557 $\{3, 5, 7, 13, 19, 37, 73\}$	$\{10223, 21181, 22699, 24737, 55459, 67607\}$	[18]
3	144	125050976086 $\{5, 7, 13, 17, 19, 37, 41, 193, 767\}$	$\{2949008, 4273396, 4660218, 6363484, 8058998, 8182316, \ldots\}$	[4, 6]
4	12	66741 $\{5, 7, 13, 17, 241\}$	$\{18534, 20446, 21181, 22699, 23451, 49474, 55459, 60849, 64494\}$	[18, 31]
5	12	159986 $\{3, 7, 13, 31, 601\}$	$\{6436, 7528, 8644, 10918, 24032, 26798, 29914, 31712, 36412, \ldots\}$	[4]
6	12	174308 $\{7, 13, 31, 37, 97\}$	$\{10107, 13215, 14505, 26375, 31340, 33706, 36772, 50252, 51255, \ldots\}$	[4]
7	24	1112646039348 $\{5, 13, 19, 43, 73, 181, 193, 1201\}$	$\{66936, 95626, 242334, 270636, 303366, 357132, 468552, \ldots\}$	[4]

gap by providing a definition and then extending the studied bases systematically to include all of the bases up through 100.

We will prove that Sierpiński numbers exist for all bases $b > 1$, and offer conjectured least Sierpiński numbers for the bases $2 < b \leq 100$. For 34 of these bases we are able to prove that the conjectured values are indeed the least.

2. Generalizing Sierpiński numbers to base b

A Sierpiński number is an odd integer k such that $k \cdot 2^n+1$ is composite for all $n > 0$. Before generalizing this definition of a Sierpiński number to other bases b, there are a couple of things we must consider.

First, when generalizing a definition it is traditional to exclude any cases that are too trivial. So we begin by requiring that the sequence $k \cdot b^n + 1$ $(n = 0, 1, 2, \ldots)$ does have not a "one-cover." That is, there is no single prime p which divides every value of the sequence. For example, if k and b are odd, then 2 divides every term (and in fact if 2 divides any one term of any sequence it divides them all).

Theorem 2.1 (1-covers)**.** *The prime p divides $k \cdot b^n+1$ for all non-negative integers n if and only if p divides* $\gcd(k+1, b-1)$.

Proof. First, suppose p divides $k \cdot b^n+1$ for all n, then it does so for $n = 0$ and 1, that is p divides $k + 1$ and $k \cdot b+1$. Subtracting these we see p divides $k(b - 1)$ so p divides $\gcd(k+1, b-1)$. If instead p divides $\gcd(k+1, b-1)$, then $k \cdot b^n+1 \equiv k+1 \equiv 0 \pmod{p}$. □

In 1964, Bowen [5] showed there where choices of k for which $k \cdot b^n+1$ is composite for all $n \geq 0$, but he did so by using 1-covers for all bases except those which are a power of 2 plus one.

Second, some have suggested that the restriction "k odd" appears in the above definition because any factor of 2 in k can be absorbed into the exponent n, but consider the number $2^m 2^n+1$ for some fixed positive integers m and n. If this number is to be prime, then it must be a Fermat number $F_n = 2^{2^n} + 1$ and so $n+m$ must be a power of two. It is widely suspected that there are only finitely many Fermat primes, which would mean there would be infinitely many even Sierpiński

TABLE 2. $k \cdot b^n + 1$ is infinitely often a generalized Fermat ‡

b	k	b	k
6	6, 36, 216, 1296, 7776, 46656	46	46, 2116
8	2, 4, 8, 16, 32	48	48
10	10, 100, 1000	52	52, 2704
12	12, 144	58	58, 3364
16	16, 256, 4096, 65536	60	60, 3600
18	18, 324	64	4, 16
22	22, 484	66	66, 4356, 287496, 18974736
24	24, 576, 13824	70	70, 4900
26	26	72	72
28	28, 784	78	78, 6084
30	30	80	80
32	2, 4, 8	82	82, 6724
36	36, 1296	88	88
40	40, 1600, 64000	96	96, 9216
42	42, 1764	100	100
2	2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536		
4	4, 16, 64, 256, 1024, 4096, 16384, 65536		

‡ Just those smaller than conjectured least base b Sierpiński and with $\gcd(k+1, b-1) = 1$.

numbers that are a power of 2. If the only Fermat numbers are the five known, then $2^{16}2^n + 1$ would be composite for $n > 0$, and therefore $2^{16} = 65536$ would be the least Sierpiński number, not Selfridge's 78557.

Since the existence of infinitely many Fermat primes is undecidable at this point in time, it seems best to define generalized Sierpiński numbers in such a way as to exclude the Fermat numbers and, for bases other than powers of 2, to exclude the generalized Fermat numbers $F_n(b) = b^{2^n} + 1$ [12]. At the end of this section (Theorem 2.3) we will show that this is equivalent to *adding* the requirement that k is not a rational power of b ($k \neq b^{\frac{p}{q}}$ for integers $p \geq 0$ and $q > 0$), and hence that $k > 1$. Those values so omitted are listed in Table 2.

Combining these considerations we generalize Sierpiński numbers as follows.

Definition 2.2. Let $b > 1$ be an integer. A **Sierpiński number base** b (or b-**Sierpiński**) is an integer $k > 1$ for which $\gcd(k+1, b-1) = 1$, k is not a rational power of b, and $k \cdot b^n + 1$ is composite for all $n > 0$.

Notice that this definition extends the definition of Sierpiński numbers in base 2 as well as the larger integer bases—yet still 78557 likely remains the least possible 2-Sierpiński number.

We end this section by showing we have properly characterized those pairs k and b which may generate infinitely many generalized Fermat numbers. Recall that the order of b modulo a relatively prime integer p, denoted $\text{ord}_p(b)$, is the least positive integer m for which p divides $b^m - 1$. So in particular $\text{ord}_p(b)$ divides $\phi(p)$ (Euler's ϕ function of p).

Lemma 2.1. *Let $e > 1$, $f > 0$ and $c \neq 0$ be integers. Write $e = 2^n e'$ where e' is odd. Then $\gcd(c^f - 1, c^e + 1) > 1$ if and only if c is odd or 2^{n+1} divides f.*

Proof. Let $d = \gcd(c^f - 1, c^e + 1)$. First note that 2 divides d if and only if c is odd, so assume c is even. Note that since e' is odd, $c^{2^n} + 1$ divides $c^e + 1$. If 2^{n+1} divides f, then $c^{2^n} + 1$ divides d. Conversely, if any odd prime p divides d, then $\mathrm{ord}_p(c)$ divides both $2e$ and f, but not e. This means 2^{n+1} divides $\mathrm{ord}_p(c)$ and therefore divides f. □

Theorem 2.3. *Let $b > 1$ and $k > 0$ be integers for which $\gcd(k + 1, b - 1) = 1$. There is an integer $c > 1$ for which $k \cdot b^n + 1 = F_r(c)$ for infinitely many integer values of r and n, if and only if k is a rational power of b.*

Proof. Let $b > 1$ and $k > 0$ be fixed integers for which $\gcd(k + 1, b - 1) = 1$.

Suppose there is an integer c for which $k \cdot b^n + 1$ ($n > 1$) is the generalized Fermat number $F_r(c)$ for infinitely many pairs of integers r and n. Choose two such pairs (r, n) and (s, m) with $n < m$. Then

$$k \cdot b^n + 1 = c^{2^r} + 1 \qquad \text{and} \qquad k \cdot b^m + 1 = c^{2^s} + 1.$$

Thus $b^{m-n} = c^{2^s - 2^r}$, and it follows $b = c^{\frac{2^s - 2^r}{m-n}}$, $k = c^{\frac{m2^r - n2^s}{m-n}}$, and therefore k is a rational power of b (and both are rational powers of c).

Conversely, suppose k is a rational power of b, say $k = b^{e/f}$ for relatively prime integers e and f with $e \geq 0$ and $f > 0$. Then because b is an integer, $b = c^f$ and $k = c^e$ for some integer c. Write $f = 2^t f'$ where f' is an odd integer. Now $\gcd(c^f - 1, c^e + 1) = 1$, so by Lemma 2.1 c is even and the power of 2 which divides e is at least as great as the power of 2 which divides f. So we may write $e = 2^t e'$ for some integer (not necessarily odd) e'. Note that if r is any positive multiple of $\mathrm{ord}_{f'}(2)$, then $e' \equiv e' 2^r \pmod{f'}$, so we may solve the following for a positive integer $n = n(r)$:

$$e' + f'n = e' 2^r.$$

So it follows

$$e + fn = 2^t(e' + f'n) = e' 2^{r+t},$$

and there are infinitely many choices of r and n for which

$$k \cdot b^n + 1 = c^{e+fn} + 1 = c^{e' 2^{r+t}} + 1 = F_{r+t}(c^{e'}).$$

□

3. N-covers: Covers and theorems

The use of covers was introduced by Paul Erdös in 1950 [13].

Definition 3.1. A **cover** for the sequence $k \cdot b^n + 1$ ($n > 0$) is a finite set of primes $S = \{p_1, p_2, \ldots p_m\}$ for which each element of the sequence is divisible by a prime in S. We ask that covers be minimal in the sense that no subset of S will also cover the sequence. S is called an **N-cover** if N is the least positive integer for which each prime p in S divides $k \cdot b^n + 1$ if and only if p divides $k \cdot b^{n+N} + 1$. We will call this integer N the **period of the cover** S. Finally, we will say that **the base b has an N-cover** if there is an integer k for which $k \cdot b^n + 1$ has a non-trivial N-cover ($N > 1$).

Erdös apparently believed that all Sierpiński numbers arise from covers [16, Section F13]. That is probably not the case [14]. In section 5 we will show that not all b-Sierpiński numbers arise from covers. In practice, though, most small examples do come from covers.

There are two basic ways of constructing covers: Sierpiński's approach of using the Fermat numbers (generalized Fermat numbers in our case) and Selfridge's use of factors of $b^n - 1$. We begin with the latter.

Theorem 3.2. *Every element of an N-cover S of $k \cdot b^n+1$ divides b^N-1.*

Proof. Choose $p \in S$. This p must divide $k \cdot b^n+1$ for some $n \leq N$. It then also divides $k \cdot b^{n+N}+1$, so divides their difference $k \cdot b^n(b^N-1)$. Since p does not divide $k \cdot b^n$, this completes the proof. □

For example, Selfridge's Sierpiński 78557 arises from the cover $\{3, 5, 7, 13, 19, 37, 73\}$. Each prime of this cover divides $2^{36}-1$, so to prove 78557 is a Sierpiński number base 2, it is sufficient to show that each of the first 36 terms in the sequence $78557 \cdot 2^n+1$ $(n > 0)$ are divisible by one of these seven primes.

The previous theorem also tells us that for every element p of an N-cover of $k \cdot b^n+1$, $\mathrm{ord}_p(b)$ divides N. It is easy to show $N = \mathrm{lcm}_{p \in S}(\mathrm{ord}_p(b))$.

Unless we say otherwise, in the rest of this article "N-cover" will mean non-trivial N cover, that is $N > 1$. Note that if S is an N-cover for one k, b pair, then it is also a cover for infinitely many other multipliers k and bases b.

Theorem 3.3. *An N-cover S of $k \cdot b^n + 1$ is also a cover of $K \cdot B^n + 1$ for all integers $K \equiv k, B \equiv b \pmod P$ where P is the product of the primes in the cover S.*

It follows by Dirichlet's theorem that there are infinitely many prime multipliers, and infinitely many prime bases covered by any given N-cover.

In what follows it will be helpful to recall the cyclotomic polynomials $\Phi_n(x)$. These are defined by

$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)} \qquad \text{and so} \qquad x^n - 1 = \prod_{d|n} \Phi_d(x).$$

This makes $\Phi_n(x)$ the "primitive part" of $x^n - 1$ when factoring, and the $\phi(n)$ zeros of $\Phi_n(x)$ are the primitive n^{th} roots of unity. For integers n and b greater than one, if a prime p divides $\Phi_n(b)$ but not n, then $p \equiv 1 \pmod n$.

Theorem 3.2 can now be greatly sharpened for more specific values of N.

Theorem 3.4. *Let p be a prime number. The sequence base b has a p-cover S if and only if $\Phi_p(b)$ has at least p distinct prime divisors greater than p.*

Proof. Suppose first S is a p-cover of $k \cdot b^n+1$. So there is an element of S which divides each element of $T = \{k \cdot b^1+1, k \cdot b^2+1, \ldots, k \cdot b^p+1\}$. If q is an element of S, the $\mathrm{ord}_q(b)$ must divide the period of S, which is p. This order can not be one, or $\{q\}$ would be a trivial cover, so $\mathrm{ord}_q(b) = p$ and therefore $p \mid q - 1$. This means q can only divide one element of T, hence there are at least p primes in S. Finally, these primes do not divide $b - 1$, so they each divide $(b^p - 1)/(b - 1) = \Phi_p(b)$.

On the other hand, if $\Phi_p(b)$ has the p distinct prime divisors: $q_1, q_2, q_3, \ldots, q_p$, each greater than p, then none divide $b - 1$ so we can use the Chinese Remainder

Theorem to show they form a p-cover by solving the system of linear equations

$$\begin{aligned} k \cdot b^1 + 1 &\equiv 0 \pmod{q_1} \\ k \cdot b^2 + 1 &\equiv 0 \pmod{q_2} \\ &\vdots \\ k \cdot b^p + 1 &\equiv 0 \pmod{q_p} \end{aligned}$$

for the multiplier k. □

For example, the base b has a 2-cover if and only if $b+1$ has at least two distinct odd prime divisors. Examples of this include $b = 14$, 20, 29, 32, 34, 38, 41, 44, 50, 54, 56, 59, 62, 64, 65, 68, 69, 74, 76, 77, 83, 84, 86, 89, 90, 92, 94, 98 ... For all of these listed bases except 68 and 86, we have proven the 2-cover generates the least generalized Sierpiński number base b (see Table 5). Bowen [5] also used 2-covers to address the bases $b = 2^s + 1$ where $s \neq 2^m + 1$ and $s > 5$.

Similarly, the base b has a 3-cover if and only if $\Phi_3(b) = b^2 + b + 1$ has at least three distinct divisors greater than 3. The first such bases are $b = 74$, 81, 87, 100, 102, 107, 121, and 135. Of those bases $b \leq 100$, only for 100 does the 3-cover yield the least generalized Sierpiński number. Bases 74, 81, and 87 have 3-covers, but these produce larger multipliers k than can be generated by other methods.

The minimal base for longer prime period covers grows quickly: (p, minimal base b) = $(2, 14), (3, 74), (5, 339), (7, 2601), (11, 32400)$, and $(13, 212574)$.

The structure of composite period covers are more interesting. For example, 4-covers usually arise from an odd prime factor p for which the base b has order 2 (a divisor of $\Phi_2(b) = b + 1$), and two primes q_1, q_2 for which b has order 4 (divisors of $\Phi_4(b) = b^2 + 1$). Then the terms of the sequence $k \cdot b^n + 1$ ($n = 1, 2, \ldots$) are divisible by the primes of the 4-cover in a pattern like

$$\underbrace{p,\ q_1,\ p,\ q_2,}\ \underbrace{p,\ q_1,\ p,\ q_2,}\ \cdots.$$

So one choice of k could be found by solving the following system.

$$\begin{aligned} k \cdot b^1 + 1 &\equiv 0 \pmod{p} \\ k \cdot b^2 + 1 &\equiv 0 \pmod{q_1} \\ k \cdot b^4 + 1 &\equiv 0 \pmod{q_2} \end{aligned}$$

For 29 of the bases in Table 5, 4-covers provide the least known b-Sierpiński numbers.

Most 6-covers involve four primes. Often one prime in the cover, say p, has period 2 ($\mathrm{ord}_p(b) = 2$), and there are three more of orders 3 or 6, say q_1, q_2, q_3, dividing the terms of $k \cdot b^n + 1$ in a pattern similar to

$$\underbrace{p,\ q_1,\ p,\ q_2,\ p,\ q_3,}\ \underbrace{p,\ q_1,\ p,\ q_2,\ p,\ q_3,}\ \cdots.$$

Most bases have a 12-cover. One way one of these can arise is if each of $\Phi_2(b)$, $\Phi_3(b)$, $\Phi_4(b)$, $\Phi_6(b)$ and $\Phi_{12}(b)$ have a primitive divisor, call them p_2, p_3, p_4, p_6 and

p_{12} respectively. Then by solving the following system for k

$$\begin{aligned} k \cdot b^1 + 1 &\equiv 0 \pmod{p_2} \\ k \cdot b^2 + 1 &\equiv 0 \pmod{p_3} \\ k \cdot b^4 + 1 &\equiv 0 \pmod{p_4} \\ k \cdot b^6 + 1 &\equiv 0 \pmod{p_6} \\ k \cdot b^{10} + 1 &\equiv 0 \pmod{p_{12}} \end{aligned}$$

we have the divisibility pattern

$$\underbrace{p_2,\ p_3,\ p_2,\ p_4,\ p_2,\ p_6,\ p_2,\ p_3,\ p_2,\ p_{12},\ p_2,\ p_4,}\ \cdots$$

Many other such patterns are possible with these five primes, but this one is sufficient to prove the following.

Theorem 3.5. *Every base $b > 2$ which is not a Mersenne number has a 12-cover.*

The proof follows immediately from the congruences above and Bang's result [3] that $b^N - 1$ has a primitive divisor except when $N = 2$ and b is a Mersenne number ($2^n - 1$, n a positive integer); or $N = 6$ and $b = 2$.

We can also use Bang's theorem on the Mersenne numbers by using a 144-cover: choose a primitive divisor p of $\Phi_n(b)$ and then solve the system of congruences $k \cdot b^e + 1 \equiv 0 \pmod{p}$ for each of the pairs $(n, e) = (3, 1), (4, 2), (6, 3), (8, 5), (9, 8), (12, 12), (16, 20), (18, 11), (24, 32), (36, 23), (48, 92)$, and $(72, 41)$. Similar systems are easily found for bases such as 120 and 180, but these require more primes. With Dirichlet's Theorem we now have the following.

Theorem 3.6. *There are infinitely many prime generalized Sierpiński numbers for every base b.*

Finally, when searching for possible covers the following results can be very useful.

Theorem 3.7. *If S is an N-cover of $k \cdot b^n+1$, then $\sum_{p \in S} \frac{1}{\mathrm{ord}_p(b)} \geq 1$*

Theorem 3.8. *If there is a non-trivial cover for $k \cdot b^n+1$, then $k+1$ has an odd prime divisor.*

The first of these was used by Stanton [32] in his analysis of possible covers for the $b = 2$ case.

4. A Simple Program and Known Results

Theorem 3.2 can be turned into a surprisingly effective program to find N-covers by looping on k until one is found for which $\gcd(k \cdot b^n+1, b^N-1) > 1$ for each of $k = 1, 2, \ldots N$. If this is done with a fairly large round value of N, such as 5040, then most small covers with relatively small k (say less than 10^8) will be easily spotted.

Daniel Adler, at the time a student at University of Tennessee at Martin, was enlisted to write a program `Sierpiński` in `C++` using the multiprecision package `GMP`[1]. When the program finds an N-cover, it outputs k and a vector of length N

[1] `http://gmplib.org/`

where the i^{th} component is $\gcd(k \cdot b^i+1, b^N-1)$ $(1 \le i \le N)$. From this it was a simple hand calculation to find the actual covering set of primes.

This program was run on the 16 nodes of our Beowulf cluster for about 80-CPU days to find the constants k and the associated covers in the first columns of Table 5 except for $b = 3$, 7 and 15. Some individual values (e.g., 71), required substantially longer search times.

The program `Sierpiński` has several limitations. First, one must know something of N in advance because the program is set up to seek all covers with period N dividing a specified constant. For Table 5 we usually sought periods dividing $7! = 5040$. It is possible that we missed some covers for smaller k values.

Second, the program `Sierpiński` only seeks values of k belonging to covers. Such k values are Sierpiński numbers base b, but there may be smaller b-Sierpiński numbers that do not arise from covers. We will discuss this in the next section.

Finally, the program `Sierpiński` is too slow to find the least covers for bases like 3. For those bases we may begin by factoring b^N-1 for various small values of N and construct covers as described in the previous section. For example, Brennen [7] used this method to find 3574321403229074 (48-cover) for $b = 3$. (This improved earlier results of Bowen [5] and Saouter [28].) With an improved algorithm Bosma [6] reduced this to $k = 125050976086$ (144-cover).

5. Polynomial Factorization and Partial Factorization

Another way that generalized Sierpiński numbers can arise is through factorization as polynomials. For example, when $b = 27$ and $k = 8$, each term factors as a difference of cubes:

$$8 \cdot 27^n+1 = (2 \cdot 3^n+1)(4 \cdot 3^{2n}-2 \cdot 3^n+1).$$

Similarly 8 is b^3-Sierpiński number for all positive multiples of 3. Such b-Sierpiński numbers arise whenever b is a perfect cube.

Consider also the factorization $4x^4 + 1 = (2x^2 + 2x + 1)(2x^2 - 2x + 1)$. Anytime b is fourth power and the multiplier k is 4 times a fourth power, every term of the sequence $k \cdot b^n + 1$ will all factor in this manner. Small examples for which this factorization generates the least known generalized Sierpiński numbers base b include $(k, b) = (2500, 16)$, and $(2500, 81)$.

The cases where the least Sierpiński numbers arise by polynomial factorization are marked by ♯ in Table 5.

A final possibility is a "partial factorization," where part of the sequence is covered by a set of primes, and the remainder of the terms factor as above. For example, the least known b-Sierpiński number for base $b = 63$, $k = 3511808$, comes from the partial 3-cover $\{37, 109\}$ (which divide $3511808 \cdot 63^n + 1$ when $n \equiv 1, 2 \pmod 3$) and the factorable $x^3 + 1$ (for $n \equiv 0 \pmod 3$). This was discussed for the usual base 2 Sierpiński numbers by Izotov [19] (see also [14]).

Another example is $k \cdot 2070^n + 1$ whose least base b Sierpiński appears to be 324. Here $324 \cdot 2070^n + 1$ factors as $4x^4 + 1$ when $n \equiv 0 \pmod 4$, and then values of $n \not\equiv 0 \pmod 4$ are covered by $\{17, 19\}$. To prove 324 is the least Sierpiński base 2070, we must find a prime for each of the following values of k : 77, 96, 132, 153, and 305. All others are known to generate primes.

The generalized Fermat numbers base b allow neither factorizations nor finite covers, yet it seems very likely that there are bases b such that all $F_n(b)$ $(n \ge 0)$

are composite. These have been excluded by our definition, but we see no reason that there could not be other examples of b-Sierpiński numbers that have neither covers nor factorizations. (This same possibility is addressed for base 2 in [19, 14]).

6. Checking the Results

The conjectured minimal values in Table 5 were compared against the published results [4, 31] and against the results of Robert Gerbicz's program which finds covers very quickly[2].

To prove the multipliers k conjectured in Table 5 are the least b-Sierpiński numbers is "simple:" just find a prime of the form $K \cdot b^n + 1$ $(n > 0)$ for each potential $K < k$. Though conceptually trivial, the amount of effort this can take may be truly massive! This is shown by the original case $b = 2$, still unsettled after 45 years, and is still one of the larger distributive computing projects: Seventeen or Bust [18]. The largest prime that they have had to find so far to eliminate a k value was $19249 \cdot 2^{13018586} + 1$ with 3,918,990 digits. They estimate they may need to search to an exponent of $n = 3,400,000,000,000$ just to get a 50% chance of finishing of the remaining cases [17].

To eliminate these small K values, we began with a Maple program. We then used `OpenPFGW` [25] for anything larger than a dozen digits. This was done in two passes: the first to trial factor by small primes and perform a probable primality test (this took about five CPU years). Second we reran `OpenPFGW` on our list of probable primes to provide classical $n \pm 1$ primality proofs [8].

We compared against all published sources that we could find, especially [4, 31]. For many of the smaller bases, Barnes [4] has results from more extensive searches than ours—so we include those results in Table 5 also. When comparing tables it is necessary to be sensitive of the variety of different definitions of generalized Sierpiński numbers being used.

7. Can $k, k^2, k^3, \ldots$ all be b-Sierpiński numbers?

Sierpiński's original construction [29] was based on the factorization of Fermat numbers. Because $2^{2^n} \equiv -1 \pmod{F_n}$, we know $\mathrm{ord}_p(2) = 2^{2^{n+1}}$ for any divisor $d > 1$ of F_n (this also means the Fermat numbers are pairwise relatively prime). So taking advantage of the fact that $F_5 = 641 \cdot 6700417 = p \cdot q$, we have the following implications.

$$\begin{array}{llll}
n \equiv 2^0 \pmod{2^1}, & k \equiv 1 \pmod{F_0} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{F_0} \\
n \equiv 2^1 \pmod{2^2}, & k \equiv 1 \pmod{F_1} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{F_1} \\
n \equiv 2^2 \pmod{2^3}, & k \equiv 1 \pmod{F_2} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{F_2} \\
n \equiv 2^3 \pmod{2^4}, & k \equiv 1 \pmod{F_3} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{F_3} \\
n \equiv 2^4 \pmod{2^5}, & k \equiv 1 \pmod{F_4} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{F_4} \\
n \equiv 2^5 \pmod{2^6}, & k \equiv 1 \pmod{p} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{p} \\
n \equiv 0 \pmod{2^6}, & k \equiv -1 \pmod{q} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{q}
\end{array}$$

Using the Chinese Remainder Theorem to solve for k yields a cover of $k \cdot 2^n + 1$ $\{F_0, F_1, F_2, F_3, F_4, p, q\}$ with period 64. In this construction it does not matter that the first five terms were prime, it would still work if they were composite. Rather than stop with F_5 (as Sierpiński did), we could then stop with any F_n for which at least one proper factor p is known and let $q = \frac{F_n}{p}$.

[2] `http://robert.gerbicz.googlepages.com/coveringsets`

This cover has another interesting property: not only are the k so constructed Sierpiński numbers, but so are k^t for any odd integer $t > 1$. It turns out that by using multiple different composite terms we may use essentially the same construction to find k for which k^t is also prime for t divisible by low powers of 2. This was done by Filaseta *et al.* [14] for the regular Sierpiński numbers, and virtually the same argument works here.

Theorem 7.1. *Let $b > 1$ be an integer for which $b+1$ is not a power of 2. If there are at least r generalized Fermat numbers $F_m(b) = b^{2^m} + 1$ which are each divisible by at least two distinct odd primes, then there are infinitely many integers k such that k^t is a b-Sierpiński number for all positive integers t not divisible by 2^r.*

Proof. Define the integer $F'_m(b)$ by $F_m(b) = 2^{r_m} F'_m(b)$ with $r_m \geq 0$ and $F'_m(b)$ odd. In what follows we need the fact that $F'_m(b)$ has at least one prime factor. This is the case unless $F'_m(b) = 1$. If $F'_m(b) = 1$, then b is odd. It follows that $m = 0$; otherwise $b^{2^m} + 1 \equiv 2 \pmod 8$. So $F'_m(b) = 1$ implies $b + 1 = 2^{r_0}$. For the rest of the proof we assume $b + 1$ is not a power of 2 (hence $F'_m(b) > 1$).

Let $m_0 < m_1 < \cdots < m_{r-1}$ be non-negative integers for which the generalized Fermat numbers $F_{m_j}(b)$, hence $F'_{m_j}(b)$, each have at least two distinct odd prime factors, say p_j and q_j. Note these primes are all different as $b, b-1$, and $F'_m(b)$ $(m \geq 0)$ are pairwise relatively prime.

By the Chinese Remainder Theorem there are infinitely many solutions to the following set of congruences.

$$k \equiv \begin{cases} 0 \pmod{b-1} & \\ 1 \pmod{b} & \\ 1 \pmod{F'_m(b)} & \text{for } 0 \leq m < m_{r-1} \text{ and } m \notin \{m_0, \ldots, m_{r-1}\} \\ 1 \pmod{p_j} & \text{for } 0 \leq j \leq r-1 \\ b^{2^{m_j - j}} \pmod{q_j} & \text{for } 0 \leq j \leq r-1. \end{cases}$$

We further restrict k to those solutions which are greater than each of the moduli above. The first of these modular restrictions guarantees $\gcd(k+1, b-1) = 1$, and the second guarantees that $\gcd(k, b) = 1$, so k is not a rational power of b.

Given any positive integer t not divisible by 2^r, say $t = 2^w t'$ where t' is odd and $0 \leq w < r$, we must show $k^t b^n + 1$ is composite for each positive integer n. Fix a positive integer n and let $n = 2^i n'$ where n' is odd. We may complete this proof by showing $k^t b^n + 1$ is divisible by

$$d = \begin{cases} F'_m(b) & \text{if } i < m_w \text{ and } m \notin \{m_0, \ldots, m_w\} \\ p_j & \text{if } i = m_j \text{ for some } j \text{ with } 0 \leq j \leq w \\ q_w & \text{if } i > m_w. \end{cases}$$

Since $d < k < k^t b^n + 1$, this will show the latter term is composite.

If $i \leq m_w$, then d divides $b^{2^i} + 1$ which divides $b^{2^i n'} + 1 = b^n + 1$. Because $k \equiv 1 \pmod d$, it follows d divides $k^t b^n + 1$.

If instead $i > m_w$, then

$$k^t \equiv (b^{2^{m_w - w}})^{2^w t'} \equiv (b^{2^{m_w}})^{t'} \equiv (-1)^{t'} \equiv -1 \pmod{q_w}.$$

Now $d = q_w$ divides $b^{2^{m_w}} + 1$ which divides

$$b^{2^i} - 1 = (b-1)(b+1)(b^2+1)(b^4+1)\cdots(b^{2^{i-1}}+1).$$

TABLE 3. k such that k^t is a 5-Sierpiński when $2^r \nmid t$

k	r
23140626796	1
3352282631064632411056	2
384540718547995072480673753524 96	3
29561279723339852323228218644200579458754257589 6	4
120225001038617128761545808 5\ 38672401747715293327992755292222232423161027929 6	5
4833\ 96281140918612511630787705875212985273405983905\ 51285269605666567127384967113451342752950905745 6	6
18081740848967\ 53044039134711401288516658002520824319923798573\ 21066068822042818728981135699573582776134982055 6	7

Thus d divides $b^{2^i n'} - 1$ and it follows

$$k^t \cdot b^n + 1 \equiv -(b^n - 1) \equiv 0 \pmod{d}.$$

This completes the proof of the theorem. □

For example, when $b = 5$, $F'_m(b)$ is prime for $m = 0, 1$, and 2. It is composite (with distinct prime divisors) for $m_0 = 3, m_1 = 4, \ldots, m_{10} = 13$. If we let q_j be the smallest prime factor of $F'_{m_j}(b)$ and p_j be the second smallest, then we get the b-Sierpiński numbers in Table 3. Of course, as noted in the discussion before the proof, rather than use prime factors, we may use any two relatively prime (non-trivial) proper divisors. So it is sufficient to know any odd prime divisor and, after checking that the given generalized Fermat is not a power of that prime, use the cofactor as the second "prime." Table 4 shows that there are 244 known composite generalized Fermat numbers $F_n(5)$, so there are 5-Sierpiński k for which $k, k^2, k^3, ..., k^{2^{244}-1}$ are all Sierpiński numbers (from [23]).

TABLE 4. Number of generalized Fermat numbers known to be composite

form	number	form	number
$2^{2^m} + 1$	235	$6^{2^m} + 1$	220
$(3^{2^m} + 1)/2$	256	$10^{2^m} + 1$	230
$(5^{2^m} + 1)/2$	244	$12^{2^m} + 1$	223

8. CONCLUSIONS

Of the many possible generalizations of the Sierpiński numbers, we have discussed what seemed the most natural to us. It would be interesting, but difficult, to study the generalized Fermat cases that we excluded in our definition. It seems likely that bases b can be found so that the least Sierpiński number is arbitrarily large. One can also ask the reverse question: given a value k, can we find a base b for which

k is a base b Sierpiński? A partial answer has been provided by one of the authors [24].

Note that every cover of a sequence of the form $k \cdot b^n + 1$ $(n > 0)$ is also a cover of a sequence $k' \cdot b^n - 1$ $(n > 0)$, and vice versa. Positive odd integers k for which $k \cdot b^n - 1$ are composite for all $n > 0$ are called Riesel numbers after an article by Riesel [27] in 1956 (so the Riesel numbers predate the Sierpiński numbers). Thus another generalization to study would be the generalized Riesel numbers (k which make $k \cdot b^n - 1$ composite for all $n > 0$ with suitable restrictions on k and b); as well as the numbers that are both b-Riesels and b-Sierpińskis. Part of this work is being done informally by Barnes and others [4], as are restrictive cases like seeking the smallest b-Sierpiński numbers which are prime.

A. de Polignac conjectured (and quickly retracted) the guess that every positive odd number can be written in the form $2^n + p$ for a prime p and integer $n > 0$. He did this even though Euler had previously shown that this was not the case for 127 or 929 [1]. Again every cover of $k \cdot b^n + 1$ $(n > 0)$ is also a cover of a sequence $b^n + k$ $(n > 0)$, and vice versa.

References

1. L. Babai, C. Pomerance & P. Vértesi, The mathematics of Paul Erdös, *Notices of the AMS*, **45**:1 (January 1998), 19–31.
2. R. Baillie, G. V. Cormack & H. C. Williams, The problem of Sierpiński concerning $k{\cdot}2^n{+}1$ *Math. Comput.*, **37** (1981) 229–231; corrigendum, **39** (1982) 308.
3. A. S. Bang, Taltheoretiske Undersøgelser, *Tidsskrift for Mat.*, **5(4)** (1886), 70–80, 130–137.
4. G. Barnes, Sierpiński conjecture reservations, May 2008, `http://gbarnes017.googlepages.com/Sierp-conjecture-reserves.htm`.
5. R. Bowen, The sequence $ka^n + 1$ composite for all n, *Math. Monthly,* **71**:2 (1964), 175–176.
6. W. Bosma, Some computational experiments in number theory. In *Discovering Mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pp. 1–30. Springer-Verlag, Berlin, 2006.
7. J. Brennen, PrimeForm e-mail discussion list, May 16, 2002, `http://tech.groups.yahoo.com/group/primenumbers/message/7147`.
8. J. Brillhart, D.H. Lehmer & J.L. Selfridge, New primality criteria and factorizations of $2^m \pm 1$, *Math. Comp.*, **29** (1975) 620–647.
9. D. A. Buell & J. Young, Some large primes and the Sierpiński problem, SRC Technical Report 88-004, Supercomputing Research Center, Lanham, MD, May 1988.
10. Y. G. Chen, On integers of the forms $k^r - 2^n$ and $k^r 2^n + 1$, *J. Number Theory*, **98**:2 (2003), 310–319.
11. Y. G. Chen, On integers of the forms $k \pm 2^n$ and $k2^n \pm 1$, *J. Number Theory*, **125**:1 (2007), 14–25, *MR* 2333115.
12. H. Dubner & W. Keller, Factors of generalized Fermat numbers, *Math. Comput.*, **64** (1995) 397-405, *MR* 1270618.
13. P. Erdös, On integers of the form $2^k + p$ and some related problems, *Summa Brasil. Math.*, **2** (1950) 113-123, *MR* 0044558.
14. M. Filaseta, C. Finch & M. Kozek, On powers associated with Sierpiński numbers, Riesel numbers and Polignac's conjecture, *J. Number Theory*, **128**:7 (2008)1916–1940, *MR* 2423742.
15. Y. Gallot, Proth.exe, `primes.utm.edu/programs/gallot/`, July 2005.
16. R. K. Guy, *Unsolved Problems in Number Theory* (3rd ed.), Problem Books in Mathematics, Springer-Verlag, New York, 2004.
17. L. Helm, P. Moore, P. Samidoost & G. Woltman, Resolution of the mixed Sierpiński problem, *INTEGERS: Elec. J. Comb. Num. Th.*, to appear.
18. L. Helm & D. Norris, Seventeen or Bust–a distributed attack on the Sierpiński problem, `http://www.seventeenorbust.com/`.
19. A. S. Izotov, A note on Sierpiński numbers, *Fibonacci Quart.*, **33** (1995) 206–207; *MR* **96f**:11020.

20. G. Jaeschke, On the smallest k such that all $k \cdot 2^N + 1$ are composite, *Math. Comput.*, **40** (1983) 381–384; *MR* **84k**:10006; corrigendum, **45** (1985) 637; *MR* **87b**:11009.
21. L. Jones, Variations on a theme of Sierpiński, *J. Integer Seq.*, **10** (2007).
22. W. Keller, Factors of Fermat numbers and large primes of the form $k{\cdot}2^n{+}1$, *Math. Comput.*, **41** (1983) 661–673; *MR* **85b**:11119; II (incomplete draft, 92-02-19).
23. W. Keller, Factors of generalized Fermat numbers found after Björn & Riesel, `http://www1.uni-hamburg.de/RRZ/W.Keller/GFNfacs.html`, Oct. 2008.
24. D. Krywaruczenko, A reverse Sierpiński number problem, *Rose-Hulman Undergrad. Math. J.* (electronic) to appear.
25. C. Nash & J. Fougeron, OpenPFGW (Open source software), `http://tech.groups.yahoo.com/group/primeform/`.
26. 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.*, **9** (1958) 673–681; *MR* **20** #3097.
27. H. Riesel, Några stora primtal (Swedish: Some large primes), *Elementa*, **39** (1956) 258–260.
28. Y. Saouter, A Fermat-like sequence and primes of the form $2h \cdot 3^n + 1$, Research Report 2728, Nov. 1995, `citeseer.ist.psu.edu/saouter95fermatlike.html`.
29. W. Sierpiński, Sur un problème concernant les nombres $k{\cdot}2^n{+}1$, *Elem. Math.*, **15** (1960) 73–74; *MR* **22** #7983; corrigendum, **17** (1962) 85.
30. N. Sloane, The on-line encyclopedia of integer sequences, Conjectured smallest Sierpiński numbers, `www.research.att.com/~njas/sequences/A123159`.
31. R. Smith, Sierpiński and Riesel bases 6 to 18, Conjectured smallest Sierpiński numbers, `www.mersenneforum.org/showthread.php?t=6895`, August 2007.
32. R. G. Stanton, Further results on covering integers of the form $1 + k \cdot 2^N$ by primes, *Combinatorial mathematics, VIII* (*Geelong*, 1980), *Springer Lecture Notes in Math.*, **884** (1981) 107–114; *MR* **84j**:10009.

Table 5: Conjectured Least Sierpiński Numbers k base b

b	N	k {cover}	k's not yet eliminated	ref
8	4	47 $\{3,5,13\}$	**proven**	
9	6	2344 $\{5,7,13,73\}$	$\{2036\}$	
10	6	9175 $\{7,11,13,73\}$	$\{7666\}$	[4]
11	6	1490 $\{3,7,19,37\}$	**proven**	[4]
12	4	521 $\{5,13,29\}$	$\{404\}$	
13	4	132 $\{5,7,17\}$	**proven**	
14	2	4 $\{3,5\}$	**proven**	
15	24	91218919470156 $\{13,17,113,211,241,1489,3877\}$	$\{114258,148458,215432,405556,424074,\ldots\}$	
16	♯	2500	**proven**	
17	4	278 $\{3,5,29\}$	$\{244\}$	[4]
18	4	398 $\{5,13,19\}$	$\{122\}$	
19	12	765174 $\{5,7,13,127,769\}$	$\{634,1446,2526,2716,3714,4506,\ldots\}$	
20	2	8 $\{3,7\}$	**proven**	
21	4	1002 $\{11,13,17\}$	**proven**	
22	4	6694 $\{5,23,97\}$	$\{1611,1908,4233,5128\}$	[4]
23	4	182 $\{3,5,53\}$	$\{8,68\}$	
24	12	30651 $\{5,7,13,73,79\}$	$\{319,621,656,821,1099,1851,1864,2164,2351,2586,3031,3051,3404,3526,\ldots\}$	
25	6	262638 $\{7,13,31,601\}$	$\{222,5550,6082,6436,7528,8644,10218,10918,12864,12988,13026,13548,\ldots\}$	
26	6	221 $\{3,7,19,37\}$	$\{32,65,155\}$	
27	♯	8	**proven**	
28	4	4554 $\{5,29,157\}$	$\{871,2377,3394,4233,4552\}$	
29	2	4 $\{3,5\}$	**proven**	
30	6	867 $\{7,13,19,31\}$	$\{278,588\}$	
31	12	6360528 $\{7,13,19,37,331\}$	$\{10366,13240,69120,70612,76848,99450,101980,122806,124812,\ldots\}$	
32	2	10 $\{3,11\}$	**proven**	
33	4	1854 $\{5,17,109\}$	$\{766,1678,1818\}$	
34	2	6 $\{5,7\}$	**proven**	
35	6	214018 $\{3,13,97,397\}$	$\{46,1610,2006,2272,2588,3046,3700,3812,5518,8632,8800,9542,10222,\ldots\}$	
36	6	1886 $\{13,31,37,43\}$	**proven**	
37	4	2604 $\{5,19,137\}$	$\{94,1272,1866,2224\}$	
38	2	14 $\{3,13\}$	**proven**	
39	6	166134 $\{5,7,223,1483\}$	$\{2264,2414,2434,3254,3986,4226,\ldots\}$	
40	6	826477 $\{7,41,223,547\}$	$\{4468,7092,9964,11112,18285,\ldots\}$	
41	2	8 $\{3,7\}$	**proven**	
42	4	13372 $\{5,43,353\}$	$\{116,988,1117,1421,2794,2903,3046,3226,3897,4127,4297,4643,\ldots\}$	
43	4	2256 $\{5,11,37\}$	$\{166,648\}$	

‡ partial factorization, ♯ factorization

Table 5: Conjectured Least Sierpiński Numbers k base b – Continued

b	N	k {cover}	k's not yet eliminated	ref
44	2	4 $\{3,5\}$	**proven**	
45	6	53474 $\{7,19,23,109\}$	$\{474,1908,2444,3106,4530,4990,$ $6510,6586,6624,7108,8026,9774,\ldots\}$	
46	6	14992 $\{7,19,47,103\}$	$\{892,976,1132,1798,3261,3477,$ $3961,4842,5395,6015,6391,6816,\ldots\}$	
47	4	8 $\{3,5,13\}$	**proven**	
48	6	1219 $\{7,13,61,181\}$	$\{29,36,62,153,422,1174\}$	
49	12	2944 $\{5,19,73,181,193\}$	$\{1134,1414,1456,2694,2746\}$	
50	2	16 $\{3,17\}$	**proven**	
51	6	5183582 $\{7,13,379,2551\}$	$\{5498,6280,6696,7682,8126,8412,\ldots\}$	
52	4	28674 $\{5,53,541\}$	$\{1483,1591,2386,3181,3232,3418,5619,$ $5776,5988,6147,6891,7147,8638,\ldots\}$	
53	4	1966 $\{3,5,281\}$	$\{1816,1838,1862,1892\}$	
54	2	21 $\{5,11\}$	**proven**	
55	4‡	2500 $\{7,17\}$	$\{1980,2274\}$	
56	2	20 $\{3,19\}$	**proven**	
57	4	1188 $\{5,13,29\}$	$\{378\}$	
58	4	43071 $\{5,59,673\}$	$\{222,787,886,1102,1923,2182,2656,2713,$ $3246,3511,3541,4021,5274,6046,\ldots\}$	
59	2	4 $\{3,5\}$	**proven**	
60	4	16957 $\{13,61,277\}$	$\{853,1646,2075,2497,4025,4406,4441,$ $5064,5767,6772,7262,7931,8923,\ldots\}$	
61	6	15168 $\{7,13,31,97\}$	$\{1570,1642,3390,3442,3936,6852,7348,$ $8710,8772,8902,9208,9268,9952,\ldots\}$	
62	2	8 $\{3,7\}$	**proven**	
63	3‡	3511808 $\{37,109\}$	$\{3092,3230,4106,7622,\ldots\}$	
64	2	51 $\{5,13\}$	**proven**	
65	2	10 $\{3,11\}$	**proven**	
66	24	21314443 $\{7,17,37,67,$ $73,4357\}$	$\{470,2076,4153,5442,6835,13201,$ $17035,\ldots\}$	
67	4	18342 $\{5,17,449\}$	$\{154,460,1494,2196,2362,2806,2872,$ $2874,3384,4062,4618,4996,5668,\ldots\}$	
68	2	22 $\{3,23\}$	$\{12,17\}$	
69	2	6 $\{5,7\}$	**proven**	
70	4	11077 $\{13,29,71\}$	$\{3762,4119,5608,9231,10438\}$	
71	18	5917678826 $\{3,19,37,73,$ $1657,5113\}$	$\{172,502,508,1942,2782,3776,4490,5002,$ $5078,5266,5330,5632,5950,6338,\ldots\}$	
72	4	731 $\{5,61,73\}$	$\{493,647\}$	
73	4	1444 $\{5,13,37\}$	$\{778,1344\}$	
74	2	4 $\{3,5\}$	**proven**	
75	6	4086 $\{7,13,19,61\}$	$\{2336,2564,3782\}$	
76	2	43 $\{7,11\}$	**proven**	
77	2	14 $\{3,13\}$	**proven**	
78	4	186123 $\{5,79,1217\}$	$\{2371,4820,4897,5294,5531,6353,\ldots\}$	

‡ partial factorization, ♯ factorization

Table 5: Conjectured Least Sierpiński Numbers k base b – Continued

b	N	k {cover}	k's not yet eliminated	ref
79	6	2212516 $\{5, 7, 43, 6163\}$	$\{24, 594, 724, 1086, 1654, 1774, 1896, \ldots\}$	
80	12	1039 $\{3, 7, 13, 43, 173\}$	$\{86, 92, 166, 188, 295, 326, 370, 433, 472, 556$ $623, 628, 692, 770, 778, 787, 818, 857, 968\}$	
81	♯	2500	$\{558, 1650, 2036, 2182, 2350, 2378\}$	
82	12	19587 $\{5, 7, 13, 37, 83\}$	$\{1251, 1327, 1570, 1716, 1798, 1908, 2251,$ $2352, 2461, 2491, 2731, 2989, 3342, \ldots\}$	
83	2	8 $\{3, 7\}$	**proven**	
84	2	16 $\{5, 17\}$	**proven**	
85	6	346334170 $\{37, 43, 193,$ $2437\}$	$\{7612, 11740, 27168, 31776, 32550, 34014,$ $35088, 36508, 43474, 48204, 50352, \ldots\}$	
86	2	28 $\{3, 29\}$	$\{8\}$	
87	6	274 $\{7, 11, 19, 31\}$	$\{32\}$	
88	12	4093 $\{5, 7, 31, 37, 89\}$	$\{192, 244, 958, 978, 1452, 1585, 1678, 1779,$ $2007, 2617, 2838, 3396, \ldots\}$	
89	2	4 $\{3, 5\}$	**proven**	
90	2	27 $\{7, 13\}$	**proven**	
91	4	89586 $\{23, 41, 101\}$	$\{252, 1678, 2008, 6970, 8902, 11706, 12306,$ $14236, 22932, 23520, 26472, 29488, \ldots\}$	
92	2	32 $\{3, 31\}$	**proven**	
93	4	24394 $\{5, 47, 173\}$	$\{62, 306, 706, 866, 894, 902, 1652, 2208,$ $2678, 3218, 3244, 3384, 3750, 3996, \ldots\}$	
94	2	39 $\{5, 19\}$	**proven**	
95	6	41354 $\{3, 7, 13, 229\}$	$\{244, 376, 692, 790, 848, 908, 926, 1004,$ $1012, 1024, 1096, 1312, 1396, 1662, \ldots\}$	
96	4	353081 $\{13, 97, 709\}$	$\{1262, 2952, 3028, 4461, \ldots\}$	
97	4	15996 $\{5, 7, 941\}$	$\{120, 202, 538, 666, 736, 762, 1042, 1044,$ $1098, 1114, 1156, 1252, 1308, 1518, \ldots\}$	
98	2	10 $\{3, 11\}$	**proven**	
99	4	684 $\{5, 13, 29\}$	$\{284\}$	
100	3	2469 $\{7, 13, 37\}$	$\{64, 433, 684, 922, 2145\}$	

‡ partial factorization, ♯ factorization

University of Tennessee at Martin
E-mail address: caldwell@utm.edu