Journal of Integer Sequences, Vol. 10 (2007),
Article 07.4.4

Variations on a Theme of Sierpiński

Lenny Jones
Department of Mathematics
Shippensburg University
Shippensburg, Pennsylvania 17257
USA
lkjone@ship.edu

Abstract

Using an idea of Erdős, Sierpiński proved that there exist infinitely many odd positive integers k such that $k \cdot 2^n + 1$ is composite for all positive integers n. In this paper we give a brief discussion of Sierpiński's theorem and some variations that have been examined, including the work of Riesel, Brier, Chen, and most recently, Filaseta, Finch and Kozek. The majority of the paper is devoted to the presentation of some new results concerning our own variations of Sierpiński's original theorem.

1 Introduction

In 1960, using an idea of Erdős, Sierpiński [15] proved that there exist infinitely many odd positive integers k such that $k \cdot 2^n + 1$ is composite for all positive integers n. Such values of k are called Sierpiński numbers. The smallest such integer produced by Sierpiński's method is $k = 15511380746462593381$. In 1962, however, John Selfridge proved that the value $k = 78557$ has the property that $k \cdot 2^n + 1$ is composite for all positive integers n. The problem of determining the smallest such value of k is known as *Sierpiński's Problem*. Selfridge conjectured that $k = 78557$ is indeed the smallest such value of k. To establish this claim, one needs to show that for each positive integer $k < 78557$, there exists a positive integer n such that $k \cdot 2^n + 1$ is prime. Currently, there remain only eight unresolved cases: $k = 10223$, 19249, 21181, 22699, 24737, 33661, 55459, and 67607. For the most recent progress on this problem, we refer the interested reader to the distributed computing project known as *Seventeen or Bust*, which can be found at the website www.seventeenorbust.com. The name of this project indicates that when it was started, only 17 values of k were unresolved.

In 1956, four years prior to Sierpiński's original paper, Riesel [12] proved that there are infinitely many odd positive integers k such that $k \cdot 2^n - 1$ is composite for all positive integers n. Such values of k are called Riesel numbers, and the problem of finding the smallest Riesel number is known as *Riesel's Problem.* To date, the smallest known Riesel number is $k = 509203$. Although Riesel and Sierpiński used the same methods, and Riesel's result predates Sierpiński's, it is curious that the result of Riesel did not originally garner as much focus as Sierpiński's theorem. This is conceivably due, in part, to the fact that Selfridge popularized Sierpiński's problem by taking an active role in its solution. A related problem, due to Brier, is to determine the smallest odd positive integer k such that both $k \cdot 2^n + 1$ and $k \cdot 2^n - 1$ are composite for all positive integers n. Currently, the smallest known Brier number is $k = 143665583045350793098657$, which was found recently by Filaseta, Finch and Kozek [9]. Both the problems of Riesel and Brier now have dedicated enthusiasts in pursuit of their solutions. More recently, some modifications of the theorems of Sierpiński and Riesel have been investigated by Chen [4, 5, 6, 7], and Filaseta, Finch and Kozek [9]. These recent results also show that the set of all values of k for which each term of the sequence contains at least m distinct prime divisors, for certain fixed integers $m \geq 2$, contains an infinite arithmetic progression or contains a subset that can be obtained from an infinite arithmetic progression.

The main purpose of this paper is to present some results concerning new variations of Sierpiński's theorem. In particular, our main result, Theorem 4.12, provides a true generalization of Sierpiński's original theorem. A by-product of the proof is that the sets of values of k that are produced all contain an infinite arithmetic progression. We are not concerned here in any case with determining the smallest such value of k, although in certain situations this can be done quite easily.

2 Definitions and Preliminaries

In this section we present some definitions and results which are used in the sequel.

Definition 2.1. For any sequence $\{s_n\}_{n=1}^{\infty}$ of positive integers, we call a prime divisor q of the term s_n a *primitive prime divisor* of s_n, if q does not divide s_m for any $m < n$.

Remark. A term s_n can have more than one primitive prime divisor, or none at all. See Theorem 2.2 and Theorem 4.9.

The following result is originally due to Bang [1].

Theorem 2.2. *Let a and n be positive integers with $a \geq 2$. Then $a^n - 1$ has a primitive prime divisor with the following exceptions:*

- *$a = 2$ and $n = 6$*
- *$a + 1$ is a power of 2 and $n = 2$.*

Many other proofs of Theorem 2.2 and its generalizations have been published. Two of the most well-known papers are due to Zsigmondy [16], and Birkhoff and Vandiver [3]. More recently, along these lines, Bilu, Hanrot and Voutier [2] have settled completely the question of primitive prime divisors in Lucas and Lehmer sequences by showing that, for all $n > 30$, the n–th term of any Lucas or Lehmer sequence has a primitive prime divisor.

The following concept is due to Erdős.

Definition 2.3. A *finite covering* is a finite system of congruences $x \equiv a_i \pmod{m_i}$, with $1 \le i \le t$, such that every integer satisfies at least one of the congruences.

Note that we simply use the word "covering" here to indicate a finite covering, since we are not concerned with infinite coverings. An example of a covering in which the modulii are not distinct is given below.

Example 2.4.

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 3 \pmod{4} \end{aligned}$$

The following example is a covering with distinct modulii.

Example 2.5.

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 0 \pmod{3} \\ x &\equiv 0 \pmod{5} \\ x &\equiv 1 \pmod{6} \\ x &\equiv 0 \pmod{7} \\ x &\equiv 1 \pmod{10} \\ x &\equiv 1 \pmod{14} \\ x &\equiv 2 \pmod{15} \\ x &\equiv 2 \pmod{21} \\ x &\equiv 23 \pmod{30} \\ x &\equiv 4 \pmod{35} \\ x &\equiv 5 \pmod{42} \\ x &\equiv 59 \pmod{70} \\ x &\equiv 104 \pmod{105} \end{aligned}$$

There are still many unsolved problems regarding coverings. Two of the most famous open questions are the following: [10]

1. Does there exist a covering in which all moduli are odd, distinct and greater than one?

2. Can the minimum modulus in a covering with distinct moduli be arbitrarily large?

Question 2. was first posed by Erdős [8], and he offers posthumously \$1000 for a solution.

3 Sierpiński's Theorem

To illustrate a basic technique used in this paper, we present a proof of the original theorem of Sierpiński [15] from 1960, stated below as Theorem 3.1.

Theorem 3.1. *There exist infinitely many odd positive integers k such that $k \cdot 2^n + 1$ is composite for all positive integers n.*

Proof. Consider the following covering $n \equiv a_i \pmod{m_i}$:

i	1	2	3	4	5	6	7
a_i	1	2	4	8	16	32	0
m_i	2	4	8	16	32	64	64.

For each i, when $n \equiv a_i \pmod{m_i}$ and $k \equiv b_i \pmod{p_i}$ (from below),

i	1	2	3	4	5	6	7
b_i	1	1	1	1	1	1	-1
p_i	3	5	17	257	65537	641	6700417,

it is easy to check that $k \cdot 2^n + 1$ is divisible by p_i. Now, apply the Chinese Remainder Theorem to the system $k \equiv b_i \pmod{p_i}$. Then, for any such solution k, each $k \cdot 2^n + 1$ is divisible by at least one prime from the set $\mathcal{C} = \{3, 5, 17, 257, 641, 65537, 6700417\}$. $\square$

Remarks.

- The set $\mathcal{C}$ in the proof of Theorem 3.1 is called a *covering set* associated with the covering.
- Observe that a consequence of the method of proof of Theorem 3.1 is that the set of all odd positive integers k such that $k \cdot 2^n + 1$ is composite for all positive integers n contains an infinite arithmetic progression.

While the proof of Theorem 3.1 is straightforward, the choice of the covering is the crucial and delicate step. What makes this particular covering useful is the fact that the Fermat number $2^{2^5} + 1$ has two distinct prime divisors. A priori, it is conceivable that there are other coverings that could be used to prove Theorem 3.1. In fact, Selfridge produced the smaller value $k = 78557$ by using the covering:

$$\begin{aligned}
n &\equiv 0 \pmod{2}\\
n &\equiv 1 \pmod{4}\\
n &\equiv 3 \pmod{36}\\
n &\equiv 15 \pmod{36}\\
n &\equiv 27 \pmod{36}\\
n &\equiv 7 \pmod{12}\\
n &\equiv 11 \pmod{12}
\end{aligned}$$

and associated covering set $\{3, 5, 7, 13, 19, 37, 73\}$.

The following questions come to mind upon examining the proof of Theorem 3.1.

- *From among the coverings that can be used to prove Theorem 3.1, which covering produces the smallest value of k?*
  As mentioned in Section 1, Selfridge conjectured that $k = 78557$ is the smallest value of k such that $k \cdot 2^n + 1$ is composite for all positive integers n. This problem is still unsolved.

- *Is it possible to prove Theorem 3.1, and perhaps produce a value of k smaller than $k = 78557$, using a method that does not involve a covering set?*
  For example, in Section 4.2, a covering set is not needed to prove Theorem 4.2.

- *Are there Sierpiński-like problems that cannot be solved using coverings?*
  Erdős [10] conjectured that all sequences of the form $d \cdot 2^n + 1$, with d fixed and odd, that contain no primes, can be obtained from coverings. There is evidence [11], however, to suggest that this conjecture might not be true.

4 Variations of Sierpiński's Theorem

4.1 Some Recent Variations

Certain variations of Theorem 3.1 have been concerned with the number of distinct prime divisors that can occur in the factorization of $k \cdot 2^n + 1$. In particular, if $m \geq 2$ is some fixed integer, does there exist a set of odd positive integers k that contains an infinite arithmetic progression such that, for each k, the integer $k \cdot 2^n + 1$ has at least m distinct prime divisors for all positive integers n? In 2001, Chen [6] answered this question in the affirmative for $m = 3$.

Chen [7] also proved the following theorem in 2003.

Theorem 4.1. *Let r be a positive integer with $r \not\equiv 0, 4, 6, 8 \pmod{12}$. Then the set of odd positive integers k such that $k^r 2^n + 1$ has at least two distinct prime divisors for all positive integers n contains an infinite arithmetic progression.*

Because of the presence of the exponent r, we can think of Theorem 4.1 as a nonlinear variation of Sierpiński's original theorem. Nevertheless, coverings still play a crucial role in the proof, although other techniques are also employed by Chen. Recently, the restrictions on r in Theorem 4.1 have been overcome by Filaseta, Finch and Kozek [9]. Again, while coverings are used in their proof, additional methods are utilized. Chen's paper [7] also contains an analogous result for integers of the form $k^r - 2^n$ with the same restrictions on r. In this situation however, the recent work of Filaseta, Finch and Kozek [9] disposes of only the cases when $r = 4$ or $r = 6$.

4.2 Some New Variations

We first present a theorem that deviates somewhat from previous investigations in the sense that here the "multiplier" k is fixed. The proof uses a covering and an algebraic factorization, rather than an associated covering set. A similar approach was employed by Izotov [11] to give a different proof of Theorem 3.1.

Theorem 4.2. *Let $k \geq 2$ be a fixed integer and let $f(x) \in \mathbb{Z}[x]$ be a polynomial with positive leading coefficient such that $f(-1) \geq 2$. Then the set of all positive integers b such that $kf(b)b^n+1$ is composite for all positive integers n contains an infinite arithmetic progression.*

Proof. For any positive integer c, let $b = c(k^2f(-1)^2-1)-1$. Then, when n is odd, we have

$$kf(b)b^n + 1 \equiv kf(-1)(-1)^n + 1 \equiv 0 \pmod{kf(-1)-1};$$

and when n is even, we have

$$kf(b)b^n + 1 \equiv kf(-1)(-1)^n + 1 \equiv 0 \pmod{kf(-1)+1}.$$

Since $f(x)$ has a positive leading coefficient, there exists N such that $kf(b)b+1 > kf(-1)+1$ for all $c > N$, eliminating the possibility that $kf(b)b^n+1$ is prime for any positive integer n. □

The following corollary is immediate from Dirichlet's theorem on primes in an arithmetic progression.

Corollary 4.3. *Assume the hypotheses of Theorem 4.2. Then there exist infinitely many prime numbers p such that $kf(p)p^n+1$ is composite for all positive integers n.*

If certain further restrictions are imposed on the polynomial $f(x)$ in Theorem 4.2, a lower bound can be placed on the number of prime divisors of each term in the sequence of Theorem 4.2. More precisely, we have the following:

Theorem 4.4. *In addition to the hypotheses of Theorem 4.2, let $m \geq 2$ be a fixed integer and let z be an odd positive integer such that the number of divisors of z is $m+1$. If $f(-1) = k^{z-1}$, then the set of all positive integers b such that $kf(b)b^n+1$ has at least m distinct prime divisors for all positive integers n contains an infinite arithmetic progression.*

Proof. Since $m \geq 2$, we have that $z > 2$. Then, by Theorem 2.2, $kf(-1)-1 = k^z-1$ has at least m distinct prime divisors. Thus, when n is odd, $kf(b)b^n+1$ has at least m distinct prime divisors since, from the proof of Theorem 4.2, we have that $kf(-1)-1$ divides $kf(b)b^n+1$. Also, by Theorem 2.2, $k^{2z}-1$ has at least m distinct prime divisors. Consequently, $kf(-1)+1 = k^z+1$ has at least m distinct prime divisors. Therefore, when n is even, $kf(b)b^n+1$ has at least m distinct prime divisors since, from the proof of Theorem 4.2, we have that $kf(-1)+1$ divides $kf(b)b^n+1$. □

As before, we have the following corollary immediately from Dirichlet's theorem.

Corollary 4.5. *Assume the hypotheses of Theorem 4.4. Then there exist infinitely many prime numbers p such that $kf(p)p^n+1$ has at least m distinct prime divisors for all positive integers n.*

While Theorem 4.2 is interesting, it does not generalize Theorem 3.1. The following conjecture, however, is a natural generalization of Theorem 3.1.

Conjecture 4.6. *Let $a, m \geq 2$ be fixed integers. For any positive integer n, define*

$$b_n := a^{(m-1)n} + a^{(m-2)n} + \cdots + a^n.$$

Then the set of all positive integers k such that $kb_n + 1$ is composite for all positive integers n contains an infinite arithmetic progression.

Remark. Note that $a = m = 2$ in Conjecture 4.6 is Sierpiński's original result, Theorem 3.1.

It was our hope to find a proof of Conjecture 4.6. Unfortunately, known general techniques seem to fall short of achieving this goal. In particular, the major stumbling block seems to be that little is known concerning the number of primitive prime divisors in sequences whose terms are of the form $a^m - 1$. Despite this lack of additional insight, we are able to prove Conjecture 4.6 in many situations (see Theorem 4.12).

We digress now for a brief discussion about the number of primitive prime divisors in sequences whose terms are of the form $a^m - 1$, by first stating Conjecture 4.7, whose truth is adequate to supply a proof of Conjecture 4.6, which is given at the end of this section.

Conjecture 4.7. *Let $a \geq 2$ be an integer and let p be a prime. Then there exists a positive integer t such that $a^{p^t} - 1$ has at least two distinct primitive prime divisors. Equivalently, there exists a positive integer z such that $\left(a^{p^z} - 1\right) / (a - 1)$ has at least $z + 1$ distinct prime divisors.*

The best known result in the direction of Conjecture 4.7 is given below as Theorem 4.9, which is a special case of a theorem of Schinzel [13]. We need the following definition.

Definition 4.8. For any integer a, we define the *square-free kernel* of a, denoted $\mathcal{K}(a)$, to be a divided by its largest square factor.

Theorem 4.9. *Let $a \geq 2$ and $m \geq 3$ be integers. Let $e = 1$ if $\mathcal{K}(a) \equiv 1 \pmod 4$, and let $e = 2$ if $\mathcal{K}(a) \equiv 2, 3 \pmod 4$. If $m/\left(e\mathcal{K}(a)\right)$ is an odd integer, then $a^m - 1$ has at least two distinct primitive prime divisors, with the following exceptions:*

$$\begin{aligned} a &= 2, \quad m \in \{4, 12, 20\} \\ a &= 3, \quad m = 6 \\ a &= 4, \quad m = 3. \end{aligned}$$

The following conjecture is related to Conjecture 4.7.

Conjecture 4.10. *Let $a \geq 2$ be a positive integer and let p be a prime. Let $\Phi_p(x)$ denote the p–th cyclotomic polynomial. Then there exists a positive integer t such that $\Phi_p(a^{p^{t-1}})$ has at least two distinct prime divisors.*

Since $a^{p^t} - 1 = \left(a^{p^{t-1}} - 1\right) \Phi_p \left(a^{p^{t-1}}\right)$, it follows from Theorem 2.2 that, when $a \not\equiv 1 \pmod p$, Conjecture 4.10 is equivalent to Conjecture 4.7. Along these lines, for $p \neq 3$, a result of Schinzel and Tijdeman [14] implies that there are at most finitely many triples (x, y, m) of integers, with $x \geq 1$ and $y, m \geq 2$, such that $\Phi_p(x) = y^m$. Consequently, if Conjecture 4.10 is not true, then $\Phi_p(a^{p^{t-1}})$ is prime for all sufficiently large t, which seems quite implausible. Computer evidence suggests that, most likely, the following somewhat stronger statement is true.

Conjecture 4.11. *Let $a \geq 2$ be a positive integer. Then $\Phi_p(a^{p^2})$ has at least two distinct prime divisors for all sufficiently large primes p.*

We turn now to our main result stated below as Theorem 4.12.

Theorem 4.12. *Let $a, m \geq 2$ be fixed integers. For any positive integer n, define*

$$b_n := a^{(m-1)n} + a^{(m-2)n} + \cdots + a^n.$$

Then the set of all positive integers k such that $kb_n + 1$ is composite for all positive integers n contains an infinite arithmetic progression, with the possible exception of the situation when m and a satisfy the following conditions:

- *m is a prime such that $m \equiv 1 \pmod{12}$ and $m \equiv 1 \pmod{q}$ for all prime divisors q of $a - 1$,*
- *a is not of the form c^2 or mc^2 for some integer $c \geq 2$.*

We restate Theorem 4.12 in a less succinct manner since the proof is organized according to the cases indicated in the restatement.

Theorem 4.12. (**Restated**)*Let $a, m \geq 2$ be fixed integers. For any positive integer n, define*

$$b_n := a^{(m-1)n} + a^{(m-2)n} + \cdots + a^n.$$

Then, in each of the following cases, the set of all positive integers k such that $kb_n + 1$ is composite for all positive integers n contains an infinite arithmetic progression:

1. *There is a prime q that divides $a - 1$ but does not divide $m - 1$*
2. *m is composite*
3. *$m = 2$*
4. *m is an odd prime with $m \not\equiv 1 \pmod{12}$*
5. *$m/(e\mathcal{K}(a))$ is an odd integer, where $\mathcal{K}(a)$, e, m and a are as given in Definition 4.8 and Theorem 4.9.*

The approach we use to prove Theorem 4.12 is, for the most part, a straightforward modification of Sierpiński's original method. For each case, we start by choosing a covering. We choose a corresponding covering set of primes to impose various congruence conditions on k to guarantee the proper divisibility of each of the terms $kb_n + 1$ by some prime in the covering set. Then we apply the Chinese Remainder Theorem to the set of congruence conditions on k to find the values of k that satisfy all conditions simultaneously. The tricky steps, as always in this process, are choosing the appropriate covering and corresponding covering set. While the techniques used in the proof of each case are similar, we provide most of the details in each situation. We point out that no attempt is made, at this time, to choose the covering or the covering set in any optimal manner. As previously mentioned, Sierpiński's original theorem is the special case of $a = m = 2$ in Theorem 4.12.

Note that the parts in Theorem 4.12, as they are presented in the restated version, are not mutually exclusive. For example, part (3) is just a combination of a special case of part (1) and Theorem 3.1. We list this $m = 2$ case separately in the attempt to categorize the cases according to whether m is prime or not. Although there is some overlap among the parts in Theorem 4.12, no part is a subset of any other. For example, the case $a = 6$, $m = 13$ is handled in part (1) and no other, while the case $a = 4$, $m = 13$ is addressed in part (5) and no other. Note also that, if a is odd and m is even in Theorem 4.12, then $kb_n + 1$ is even for any odd positive integer k, and the theorem is trivially true. Since most of the arguments given in the proof of Theorem 4.12 are general enough, it is often not necessary to distinguish the trivial situations from the nontrivial situations. The drawback to this more general approach, however, is that sometimes in the trivial situations we are providing an unnecessarily complicated or inefficient proof. Nevertheless, we have chosen the more general path rather than deciding in every case which situations qualify as truly trivial.

We need the following lemma for the proof of Theorem 4.12.

Lemma 4.13. *Let $a \geq 2$ be an integer, and let $m \geq 6$ be a composite integer. Then there exists a prime q such that all of the following hold:*

- *q divides $a^m - 1$*
- *q is not a primitive divisor of $a^m - 1$*
- *q does not divide $m - 1$.*

Proof. First suppose that m is not the square of a prime. Write $m = xy$ with $1 < x < y < m$ and $y \neq 6$. Note that $y > 2$, so that $a^y - 1$ has a primitive prime divisor q. Then q divides $a^m - 1$ but is not a primitive prime divisor of $a^m - 1$. Since q is a primitive prime divisor of $a^y - 1$, we have that $q - 1 = zy = zm/x$ for some positive integer z. If q divides $m - 1$, then $m - 1 = wq$ for some positive integer w. Combining these facts gives

$$m - 1 = w\left(\frac{zm}{x} + 1\right), \tag{1}$$

which implies that $w < x$, or equivalently $w + 1 < x + 1$. Rearranging (1) yields

$$y(x - wz) = \frac{m}{x}(x - wz) = w + 1,$$

so that $y \leq w + 1$. Therefore, it follows that $y < x + 1$, contradicting the fact that $x < y$.

Now suppose that $m = p^2$ for some prime $p \geq 3$. Let q be a primitive prime divisor of $a^p - 1$. Then q divides $a^{p^2} - 1$ but is not a primitive prime divisor of $a^{p^2} - 1$. Suppose that q divides $p^2 - 1$. Since q is a primitive prime divisor of $a^p - 1$, we have that p divides $q - 1$, and so $p < q$. Then, since q divides $p^2 - 1 = (p - 1)(p + 1)$, it follows that $q = p + 1$, which is impossible since $p \geq 3$. ∎

Proof of Theorem 4.12. The proof of part (1) is trivial since, if there exists a prime q that divides $a - 1$ but does not divide $m - 1$, then, for any $k \equiv -1/(m - 1) \pmod{q}$, we have that $kb_n + 1 \equiv 0 \pmod{q}$ for all n. Also, note that

$$kb_n + 1 = k(a^{(m-1)n} + \cdots + a^n) + 1 \geq ka^n + 1 \geq a + 1 > q,$$

so that no term kb_n+1 is actually equal to the prime q.

To prove part (2), consider first the case when $m \geq 6$, and write $m = xy$ with $1 < x < y < m$ and $y \neq 6$. For now, we exclude the particular case of $a = 2$ and $m = 6$. Let q be a primitive prime divisor of $a^y - 1$, which exists since $y > 2$ and $y \neq 6$. Let r be a primitive prime divisor of $a^m - 1$, which exists since $m > 2$ and $a \neq 2$ when $m = 6$. We use the covering $n \equiv 0, 1, 2, \ldots, m-1 \pmod{m}$. When $n \equiv 1, 2, \ldots, m-1 \pmod{m}$, we have that $a^n - 1 \not\equiv 0 \pmod{r}$, since r is a primitive prime divisor of $a^m - 1$. Consequently,

$$\begin{aligned} b_n + 1 &= \frac{(a^n)^m - 1}{a^n - 1} \\ &= \frac{(a^m)^n - 1}{a^n - 1} \\ &= \frac{(a^m - 1)\left((a^m)^{n-1} + \cdots + 1\right)}{a^n - 1} \\ &\equiv 0 \pmod{r}. \end{aligned}$$

Therefore, if $k \equiv 1 \pmod{r}$, it follows that $kb_n + 1 \equiv 0 \pmod{r}$. Also, since

$$b_1 + 1 = \frac{a^{xy} - 1}{a - 1} = \frac{(a^y - 1)\left(a^{y(x-1)} + \cdots + 1\right)}{a - 1} \equiv 0 \pmod{q},$$

we see that

$$kb_n + 1 \geq b_n + 1 \geq b_1 + 1 \geq qr > r,$$

and so kb_n+1 is never equal to the prime r. When $n \equiv 0 \pmod{m}$, we have that $b_n \equiv m-1 \pmod{q}$. From the proof of Lemma 4.13, $m - 1 \not\equiv 0 \pmod{q}$. Hence, $kb_n + 1 \equiv 0 \pmod{q}$ if $k \equiv -1/(m-1) \pmod{q}$. Also, since $b_n > a^y - 1 \geq q$, the term $kb_n + 1$ is never equal to the prime q. Now apply the Chinese Remainder Theorem to the system of congruences

$$\begin{aligned} k &\equiv 1 \pmod{r} \\ k &\equiv -1/(m-1) \pmod{q} \end{aligned}$$

to finish the proof of the theorem for composite $m \geq 6$, with the exception of the case $a = 2$ and $m = 6$. For this particular case, we have that $b_n + 1 = 2^{6n} - 1 \equiv 0 \pmod{3}$ and $b_n > 3$ for all n. Hence, if $k \equiv 1 \pmod{3}$, then $kb_n + 1 \equiv 0 \pmod{3}$, and is never equal to 3, for all n.

Suppose now that $m = 4$. As mentioned in the discussion prior to Lemma 4.13, the theorem is trivially true if a is odd, so we assume that a is even. For $a \geq 4$, we use the covering $n \equiv 0, 1, 2, 3 \pmod{4}$. Let r be a primitive prime divisor of $a^4 - 1$. If $a \equiv 4 \pmod{6}$, let q be a primitive prime divisor of $a^2 - 1$, which exists since $a + 1$ is not a power of 2. Note that $q \neq 3$ since 3 divides $a - 1$. If $a \equiv 0, 2 \pmod{6}$, let q be any prime divisor of $a-1$. Observe that $q \neq 3$ here as well. Thus, when $n \equiv 1, 2, 3 \pmod{4}$, we see that $b_n \equiv -1 \pmod{r}$, and consequently, $kb_n + 1 \equiv 0 \pmod{r}$ if $k \equiv 1 \pmod{r}$. Also, since

$$kb_n + 1 > ka^{2n} + 1 \geq a^2 + 1 \geq r,$$

it follows that $kb_n + 1$ is never equal to the prime r. When $n \equiv 0 \pmod 4$, we have that $b_n \equiv 3 \pmod q$, and therefore $kb_n + 1 \equiv 0 \pmod q$ if $k \equiv -1/3 \pmod q$. As above, it is easy to see that $kb_n + 1$ is never equal to the prime q. Then apply the Chinese Remainder Theorem to the system of congruences

$$\begin{array}{rcll} k & \equiv & 1 & \pmod r \\ k & \equiv & -1/3 & \pmod q. \end{array}$$

For the case $a = 2$, we use the covering

$$\begin{array}{rcll} n & \equiv & 1, 2, 3 & \pmod 4 \\ n & \equiv & 0 & \pmod 8 \\ n & \equiv & 4 & \pmod{16} \\ n & \equiv & 12 & \pmod{32} \\ n & \equiv & 28 & \pmod{64} \\ n & \equiv & 60 & \pmod{64} \end{array}$$

and the corresponding covering set $\{5, 17, 257, 65537, 641, 6700417\}$, which lead to the system of congruences

$$\begin{array}{rcll} k & \equiv & 1 & \pmod 5 \\ k & \equiv & 11 & \pmod{17} \\ k & \equiv & 1 & \pmod{257} \\ k & \equiv & 4368 & \pmod{65537} \\ k & \equiv & 400 & \pmod{641} \\ k & \equiv & 6135898 & \pmod{6700417}, \end{array}$$

having $k = 4331277253353619796$ as its smallest solution. This completes the proof of part (2).

Part (3) is just a special case of part (1) when $a \geq 3$, and it is just Theorem 3.1 when $a = 2$.

To prove part (4), let m be an odd prime p, and assume first that $p \equiv 3 \pmod 4$. We use the covering

$$\begin{array}{rcll} n & \equiv & 1, 2, \ldots, p-1 & \pmod p \\ n & \equiv & 0 & \pmod{2p} \\ n & \equiv & p & \pmod{4p} \\ n & \equiv & 3p & \pmod{4p}. \end{array}$$

Let q be a primitive prime divisor of $a^p - 1$. When $n \equiv 1, 2, \ldots, p-1 \pmod p$, we have that $b_n \equiv -1 \pmod q$, which implies that $kb_n + 1 \equiv 0 \pmod q$ if $k \equiv 1 \pmod q$. Therefore, since

$$kb_n + 1 \geq b_n + 1 \geq b_1 + 1 = a^{p-1} + a^{p-2} + \cdots + 1 \geq q,$$

we conclude that q is a proper divisor of $kb_n + 1$ when $k \equiv 1 \pmod q$ with $k > 1$. In fact, $kb_n + 1$ is never actually equal to the prime q since forthcoming conditions on k preclude the possibility that $k = 1$. Now let r be a primitive prime divisor of $a^{2p} - 1$, except in the case $a = 2$ and $p = 3$, where we let $r = 3$. With the exception of the case $a = 2$ and $p = 3$, note that $p < r$ since $2p$ divides $r - 1$. So, in any case, when $n \equiv 0 \pmod{2p}$, we see that $b_n \equiv p - 1 \not\equiv 0 \pmod r$. Thus, $kb_n + 1 \equiv 0 \pmod r$, if $k \equiv -1/(p-1) \pmod r$. Note that if $k = 1$, then $p \equiv 0 \pmod{r}$, which is impossible, unless $a = 2$ and $p = r = 3$. Hence, $k > 1$ unless $a = 2$ and $p = r = 3$. Now let s be a primitive prime divisor of $a^{4p} - 1$. Then, $a^p - 1 \not\equiv 0 \pmod{s}$, and when $n \equiv p \pmod{4p}$, we have $b_n > s$ and

$$b_n \equiv \frac{a^p \left(a^{p(p-1)} - 1\right)}{a^p - 1} \not\equiv 0 \pmod{s},$$

since $p \equiv 3 \pmod{4}$. Next, let u be a primitive prime divisor of $a^4 - 1$. Then, when $n \equiv 3p \pmod{4p}$, we have $b_n > u$ and

$$b_n \equiv \frac{a^{3p} \left(a^{3p(p-1)} - 1\right)}{a^{3p} - 1} \not\equiv 0 \pmod{u},$$

since $p \equiv 3 \pmod{4}$. Finally, apply the Chinese Remainder Theorem to the system of congruences

$$\begin{array}{rcll} k & \equiv & 1 & \pmod{q} \\ k & \equiv & -1/(p-1) & \pmod{r} \\ k & \equiv & -(a^p - 1)/\left(a^p \left(a^{p(p-1)} - 1\right)\right) & \pmod{s} \\ k & \equiv & -(a^{3p} - 1)/\left(a^{3p} \left(a^{3p(p-1)} - 1\right)\right) & \pmod{u}. \end{array}$$

Note that when $a = 2$ and $p = r = 3$, we have that $s = 13$. Therefore, the third congruence above is $k \equiv 11 \pmod{13}$, which implies that $k \neq 1$. This completes the proof when $p \equiv 3 \pmod{4}$.

Now suppose that $p \equiv 5 \pmod{12}$. We use the covering

$$\begin{array}{rcll} n & \equiv & 1, 2, \ldots, p-1 & \pmod{p} \\ n & \equiv & 0 & \pmod{2p} \\ n & \equiv & p & \pmod{6p} \\ n & \equiv & 3p & \pmod{6p} \\ n & \equiv & 5p & \pmod{6p}. \end{array}$$

We let $\{q, r, s, u, v\}$ be the corresponding covering set of primes, where q, r, s, u and v are, respectively, primitive prime divisors of $a^p - 1$, $a^{2p} - 1$, $a^3 - 1$, $a^{3p} - 1$ and $a^{6p} - 1$. As above, similar arguments show the following for any n:

- b_n is larger than the corresponding prime from the covering set
- b_n is not divisible by the corresponding prime from the covering set (using the fact that $p \not\equiv 1 \pmod{12}$).

To finish the proof when $p \equiv 5 \pmod{12}$, apply the Chinese Remainder Theorem to the following system of congruences for k:

$$\begin{array}{rcll} k & \equiv & 1 & \pmod{q} \\ k & \equiv & -1/(p-1) & \pmod{r} \\ k & \equiv & -(a^p - 1)/\left(a^p \left(a^{p(p-1)} - 1\right)\right) & \pmod{s} \\ k & \equiv & -1/(p-1) & \pmod{u} \\ k & \equiv & -(a^{5p} - 1)/\left(a^{5p} \left(a^{5p(p-1)} - 1\right)\right) & \pmod{v}. \end{array}$$

This completes the proof of part (4).

Finally, for the proof of part (5), suppose that $m/(e\mathcal{K}(a))$ is an odd integer, where $\mathcal{K}(a)$, e, m and a are as given in Definition 4.8 and Theorem 4.9. Note that the exceptions mentioned in Theorem 4.9 are addressed in parts (2) and (4) of this theorem. We can assume that m is odd, since part (2) of this theorem handles the cases when $m \geq 4$ is even. We use the covering $n \equiv 0, 1, 2, \ldots, m-1 \pmod{m}$. From Theorem 4.9, we have that $a^m - 1$ has at least two distinct primitive prime divisors. Let q and r be two such divisors. When $n \equiv 1, 2, \ldots, m-1 \pmod{m}$, we have that $b_n \equiv -1 \pmod{q}$, and when $n \equiv 0 \pmod{m}$, we have that $b_n \equiv m-1 \pmod{r}$. It is easily verified that b_n is greater than each of the primes q and r. Then, we use the Chinese Remainder Theorem to solve the system of congruences:

$$\begin{array}{rcll} k & \equiv & 1 & \pmod{q} \\ k & \equiv & -1/(m-1) & \pmod{r}, \end{array}$$

which completes the proof of the theorem.

□

Remark. For the case $a = 2$ and $m = 4$ in part (2) of Theorem 4.12, we can also use the covering and corresponding covering set that Sierpiński used in his original problem, namely:

$$\begin{array}{rcll} n & \equiv & 1 & \pmod{2} \\ n & \equiv & 2 & \pmod{4} \\ n & \equiv & 4 & \pmod{8} \\ n & \equiv & 8 & \pmod{16} \\ n & \equiv & 16 & \pmod{32} \\ n & \equiv & 32 & \pmod{64} \\ n & \equiv & 0 & \pmod{64} \end{array}$$

and $\{3, 5, 17, 257, 65537, 641, 6700417\}$, which lead to the system of congruences

$$\begin{array}{rcll} k & \equiv & 1 & \pmod{3} \\ k & \equiv & 1 & \pmod{5} \\ k & \equiv & 1 & \pmod{17} \\ k & \equiv & 1 & \pmod{257} \\ k & \equiv & 1 & \pmod{65537} \\ k & \equiv & 1 & \pmod{641} \\ k & \equiv & 2233472 & \pmod{6700417}. \end{array}$$

The smallest solution is $k = 10340920497641728921$.

We now give a proof of Conjecture 4.6 assuming the truth of Conjecture 4.7.

Proof of Conjecture 4.6 assuming Conjecture 4.7. For composite m, the given proof of Theorem 4.12 suffices. So, assume that $m = p$ is prime. Conjecture 4.7 implies that there exists a positive integer t such that $a^{p^t} - 1$ has at least two distinct primitive prime divisors: q_t and q_{t+1}. We use the covering

$$
\begin{array}{rcll}
n & \equiv & 1, 2, \ldots, p-1 & \pmod{p} \\
n & \equiv & p, 2p, \ldots, (p-1)p & \pmod{p^2} \\
\vdots & \vdots & \vdots & \vdots \\
n & \equiv & p^{t-2}, 2p^{t-2}, \ldots, (p-1)p^{t-2} & \pmod{p^{t-1}} \\
n & \equiv & p^{t-1}, 2p^{t-1}, \ldots, (p-1)p^{t-1} & \pmod{p^t} \\
n & \equiv & 0 & \pmod{p^t}
\end{array}
$$

with the corresponding covering set $\{q_1, q_2, \ldots, q_{t+1}\}$ of primes, where q_j is a primitive prime divisor of $a^{p^j} - 1$, for $1 \le j \le t-1$. Then, when $n \equiv p^{j-1}, 2p^{j-1}, \ldots, (p-1)p^{j-1} \pmod{p^j}$, for any $1 \le j \le t$, we have that

$$
b_n + 1 \equiv \frac{a^{zp^j} - 1}{a^{zp^{j-1}} - 1} \equiv 0 \pmod{q_j},
$$

for any $z \in \{1, 2, \ldots, p-1\}$. Also, when $n \equiv 0 \pmod{p^t}$, we have that $b_n \equiv p-1 \pmod{q_{t+1}}$. Since $p - 1 < p \le p^t < q_{t+1}$, it follows that $b_n \not\equiv 0 \pmod{q_{t+1}}$. These conditions imply that, whenever k satisfies the system of congruences

$$
\begin{array}{rcll}
k & \equiv & 1 & \pmod{q_j} \qquad 1 \le j \le t \\
k & \equiv & -1/(p-1) & \pmod{q_{t+1}},
\end{array}
$$

all terms $kb_n + 1$ are composite. Again, by the Chinese Remainder Theorem, there exist infinitely many such positive integers k, and the proof is complete. $\square$

5 Acknowledgments

The author thanks the referees for the valuable suggestions.

References

[1] A.S. Bang, Taltheoretiske Unders§ogelser, *Tidsskrift for Mat.* **5(4)** (1886), 70–80, 130–137

[2] Yu. Bilu, G. Hanrot, P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, With an appendix by M. Mignotte, *J. Reine Angew. Math.* **539** (2001), 75–122.

[3] G. D. Birkhoff and H. S. Vandiver, On the integral divisors of $a^n - b^n$, *Ann. of Math. (Second Series)* **5** (1903-1904), 173-180.

[4] Yong-Gao Chen, On integers of the form $2^n \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, *Proc. Amer. Math. Soc.* **128** (2000), 1613–1616.

[5] Yong-Gao Chen, On integers of the form $k2^n + 1$, *Proc. Amer. Math. Soc.* **129** (2001), 355–361.

[6] Yong-Gao Chen, On integers of the forms $k - 2^n$ and $k2^n + 1$, *J. Number Theory* **89** (2001), 121–125.

[7] Yong-Gao Chen, On integers of the forms $k^r - 2^n$ and $k^r 2^n + 1$, *J. Number Theory* **98** (2003), 310–319.

[8] P. Erdős, On integers of the form $2^k + p$ and some related problems, *Summa Brasil. Math.* **2** (1950), 113–123.

[9] Michael Filaseta, Carrie Finch and Mark Kozek, *On powers associated with Sierpinski numbers, Riesel numbers and Polignac's conjecture*, (submitted).

[10] Richard K. Guy, *Unsolved Problems in Number Theory, third edition*, Sringer-Verlag, 2004.

[11] Anatoly S. Izotov, A note on Sierpiński numbers, *Fibonacci Quart.* **33** (1995), 206–207.

[12] H. Riesel, Några stora primtal, *Elementa* **39** (1956), 258–260.

[13] A. Schinzel, On primitive prime factors of $a^n - b^n$, *Proc. Cambridge Philos. Soc.* **58** (1962), 555–562.

[14] A. Schinzel and R. Tijdeman, On the equation $y^m = P(x)$, *Acta Arith.* **31** (1976), 199–204.

[15] W. Sierpiński, Sur un problème concernant les nombres $k2^n + 1$, *Elem. d. Math.* **15** (1960), 73–74.

[16] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatshefte f—r Math. u. Phys.* **3** (1892), 265–284.

2000 *Mathematics Subject Classification*: Primary 11B25, 11B07; Secondary 11B99.
Keywords: Sierpiński number; arithmetic progression; primitive divisor.

Received November 14 2006; revised version received April 14 2007. Published in *Journal of Integer Sequences*, April 14 2007.

Return to Journal of Integer Sequences home page.