#A36 INTEGERS 10 (2010), 423-436

POWERS OF SIERPIŃSKI NUMBERS BASE B

Chris K. Caldwell[1]
Department of Mathematics and Statistics, University of Tennessee at Martin, Martin, TN 38238, USA
caldwell@utm.edu

Takao Komatsu[2]
Department of Mathematical Sciences, Hirosaki University, Hirosaki, Japan
komatsu@cc.hirosaki-u.ac.jp

Received: 7/13/09, Revised: 12/24/09, Accepted: 4/20/10, Published: 9/8/10

Abstract

A Sierpiński number is a positive odd integer k such that $k \cdot 2^n + 1$ is composite for all $n > 0$. It has been shown by Filaseta *et al.* that given any integer $R > 0$, there are integers k for which $k, k^2, k^3, \ldots, k^R$ are each Sierpiński numbers. In this paper we seek to generalize this to bases other than 2.

1. Introduction

In 1960, W. Sierpiński [17] proved there are infinitely many odd integers k for which $k \cdot 2^n + 1$ is composite for all integers $n > 0$. Such odd numbers k are called *Sierpiński numbers*. In 1962, Selfridge [unpublished] found what is now believed to be the least Sierpiński number, $k = 78557$. Both did this by finding a finite set of primes S, called a cover (or covering set), for which each term of $k \cdot 2^n + 1$ ($n > 0$) is divisible by at least one element of S.

Sierpiński's original cover [17] was based on the factorization of Fermat numbers $F_n = 2^{2^n} + 1$. We repeat the construction here because it is central to the proofs below. First, $2^{2^n} \equiv -1 \pmod{F_n}$, so we know $\mathrm{ord}_p(2) = 2^{n+1}$ (the order of 2 modulo p) for any divisor $p > 1$ of F_n. (This also means the Fermat numbers are pairwise relatively prime.) Taking advantage of the fact that F_5 factors into $641 \cdot 6700417 = p_1 \cdot q_1$, we have the following implications.

[1]The first author would like to thank Wilfrid Keller for his advice and inspiration.
[2]The second author was partially supported by the Grant-in-Aid for Scientific Research (C) (No. 18540006) from the Japan Society for the Promotion of Science.

$$\left\{\begin{array}{llll} n \equiv 2^0 \pmod{2^1}, & k \equiv 1 \pmod{F_0} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{F_0} \\ n \equiv 2^1 \pmod{2^2}, & k \equiv 1 \pmod{F_1} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{F_1} \\ n \equiv 2^2 \pmod{2^3}, & k \equiv 1 \pmod{F_2} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{F_2} \\ n \equiv 2^3 \pmod{2^4}, & k \equiv 1 \pmod{F_3} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{F_3} \\ n \equiv 2^4 \pmod{2^5}, & k \equiv 1 \pmod{F_4} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{F_4} \\ n \equiv 2^5 \pmod{2^6}, & k \equiv 1 \pmod{p_1} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{p_1} \\ n \equiv 0 \pmod{2^6}, & k \equiv -1 \pmod{q_1} & \Longrightarrow & k \cdot 2^n + 1 \equiv 0 \pmod{q_1}. \end{array}\right. \tag{1}$$

Using the Chinese Remainder Theorem to solve for k yields an arithmetic sequence of values k for which the associated sequences $k \cdot 2^n + 1$ $(n > 0)$ are each covered by the set $\{F_0, F_1, F_2, F_3, F_4, p_1, q_1\}$. Adding $k \equiv 1 \pmod 2$ to the mix will ensure that the resulting k values are all odd, hence Sierpiński numbers.

In this construction it does not matter that the first five terms were prime, it would still work if they were composite. Also, rather than stop with F_5 (as Sierpiński did), we could stop with any composite F_n which is (at least) partially factored. Finally, this cover has an even more interesting property: not only are the k values so constructed Sierpiński numbers, but so are their odd powers:

$$k, k^3, k^5, k^7, \ldots, k^{2n+1}, \ldots. \tag{2}$$

It is natural then to ask if we can fill in the gaps in this sequence of powers, and find a k for which *all* powers of k are Sierpiński numbers. This avenue was first explored for the usual Sierpiński numbers by Chen [6], and then completely solved by Filaseta *et al.* [9]. The main goal of this paper is to generalize this work to bases other than 2 by proving the following two analogs of their results.

Theorem 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 $k^t b^n + 1$ $(n > 0)$ are each divisible by at least two distinct primes for all positive integers t not divisible by 2^r.*

Theorem 2. *Let $b > 1$ be an integer. For every positive integer R, there exist infinitely many integers k for which each of $k^t b^{bn} + 1$ $(n > 0,\ 1 \le t \le R)$ have at least two distinct prime divisors.*

These will be shown in Sections 3 and 4 respectively.

We end this introduction with a definition. Brunner *et al.* [5] generalized the Sierpiński numbers to other bases b as follows.

Definition 3. A *generalized 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 $n > 0$.

They also proved that such b-Sierpiński numbers exist for every base $b > 1$, conjectured the least b-Sierpiński number for $2 \leq b \leq 100$, and proved those conjectures for 34 of these bases [5]. (Notice that this definition is even a slight generalization within base 2.)

The restriction $\gcd(k+1, b-1) = 1$ in the definition rules out the trivial covers—those cases where a single prime divides every term $k \cdot b^n+1$ ($n > 0$). For example if k and b are odd, then all terms are divisible by 2. Bowen [4] used such trivial covers to settle virtually all bases, but those currently studying the problem (such as Barnes' Internet group [2] and those applying specific cases such as Bosma [3]) rule out these trivial covers.

The definition of the (usual) Sierpiński numbers requires that k be odd. This is done to avoid the Fermat numbers. The only primes of the form $2^m 2^n + 1$ (with m and n integers) are the Fermat primes. It is possible (as mentioned in the famous footnote of Hardy and Wright [11]) that there may be only finitely many Fermat primes. If the Fermat primes F_0, F_1, F_2, F_3 and F_4 are all there are, then the smallest positive integer k for which $k \cdot 2^n + 1$ ($n > 0$) are all composite would be $2^{16} = 65536$. This would make $k = 65536$, not Selfridge's $k = 78557$, the least "Sierpiński number," but requiring Sierpiński numbers to be odd avoids this issue.

In the general case, it is again helpful to avoid the corresponding generalized Fermat numbers $F_n(b) = b^{2^n} + 1$ (these numbers are discussed, for example, in [7]). Hence Definition 3 requires that k is not a rational power of b. For the reader's convienence, we include a proof that this condition is necessary and sufficient (Theorem 14).

Finally, the intriguing paper of Jones [13] also considers many bases, but rather than fix the base b and seek k, he essentially does the reverse, creating non-trivial covers for each case. Since he never seeks the least choice of multiplier, the issues of trivial covers and Generalized Fermat numbers are inapplicable.

2. Erdös' Cover Conjecture

Before proving our main theorems, we digress to discuss the fate of a conjecture of Erdös, and its strengthening by Filaseta *et al.*, in this new setting. Erdös [8] introduced the use of covers to disprove the de Polignac conjecture. Apparently Erdös believed that all Sierpiński numbers came from coverings [10, Section F13], so the following conjecture must also hold.

Conjecture 4. If k is a Sierpiński number, then the smallest prime divisor of $k \cdot 2^n + 1$ is bounded as n tends to infinity.

This conjecture was called into doubt by Izotov [12] and then by Filaseta *et al.* [9]. They each gave examples of Sierpiński numbers that arose from a combination of a partial cover and a factorization for the rest of the terms. For the generalized case we are able to show this conjecture fails.

Theorem 5. *There are integers $b > 1$, and b-Sierpiński numbers k, for which the least prime factor of $k \cdot b^n + 1$ is unbounded as n tends to infinity.*

Proof. Note $8 \cdot 27^n + 1 = (2 \cdot 3^n + 1)(4 \cdot 3^{2n} - 2 \cdot 3^n + 1)$ $(n > 0)$, so every term in this sequence is a composite number. It is clear that 8 meets the other requirements in Definition 3 and so is a Sierpiński number base 27. Let $N > 0$ be an integer. For every prime $q \leq N$, we know that $q-1$ divides $N!$, so $8 \cdot 27^{N!} + 1 \equiv 9 \pmod{q}$. Since 3 does not divide any term of this sequence, this shows that no prime less than or equal to N can divide $8 \cdot 27^{N!} + 1$, hence the smallest prime divisor of $8 \cdot 27^n + 1$ is unbounded as n tends to infinity. □

It would be trivial to construct an infinite number of such examples for Theorem 5, but just one suffices to make the point.

So how is this related to the focus of our paper (Sierpiński numbers which are rth powers for $r > 1$)? As Filaseta *et al.* presented their evidence against Conjecture 4, they offered the following stronger version.

Conjecture 6. If k is a Sierpiński number that is not of the form l^r for some integers $l \geq 1$ and $r > 1$, then the smallest prime divisor of $k \cdot 2^n + 1$ is bounded as n tends to infinity.

If we generalize this conjecture by just replacing 2 by b, then it is unlikely to be true. For example, let $b = 240$, $m = 4732988$, and $k = 4bm^4$. It is easy to check that $k \cdot b^n + 1$ is divisible by 241 if n is even, and is divisible by 57601 if $n \equiv 1 \pmod{4}$. When $n \equiv 3 \pmod{4}$, write $n = 4j + 3$, then

$$k \cdot b^n + 1 = (2m^2 b^{2j+2} + 2mb^{j+1} + 1)(2m^2 b^{2j+2} - 2mb^{j+1} + 1). \tag{3}$$

So each term of the sequence $k \cdot b^n + 1$ $(n > 1)$ is composite, and as $\gcd(k+1, b-1) = 1$, k is a b-Sierpiński number.

Note that when $n = 63$, the two factors in Eq. (3) are each 90-digit primes. So *if the prime factors of $k \cdot b^n + 1$ are bounded* as n tends to infinity, then this sequence has a cover $\mathcal{P}$ which must contain one (or both) of these primes. The order of b modulo these primes p, q are $(p-1)/120$ and $(q-1)/60$ respectively.

By the following theorem of D. Schleicher [16], this means the cover $\mathcal{P}$ contains at least 65,371,156,178,359,310,155,826 primes!

Theorem 7 (Schleicher). *Let $e = \text{lcm}(e_1, e_2, \ldots, e_s)$ have the prime decomposition $e = \prod q_j^{\alpha_j}$. If $e_1, e_2, \ldots, e_s$ forms an irreducible covering pattern of period e with s minimal, then $s \geq 1 + \sum \alpha_j(q_j - 1)$.*

Even though it is heuristically unlikely that both terms in Eq. (3) are again simultaneously prime, there seems to be no a priori limit on the lower bound of their factors as n approaches infinity. We choose to state our version of Conjecture 6 as a question.

Open Question If k is a b-Sierpiński number that is not of the form $l^r b^s$ for some integers $l \geq 1$, $r > 1$, and $s \geq 1$, is the smallest prime divisor of $k \cdot b^n + 1$ unbounded as n tends to infinity?

3. Proof of Theorem 1

To motivate our method of proof, let us first add the terms k^2, k^6, k^{10}, k^{14}, ..., to the (regular) Sierpiński numbers listed in Eq. (2). Write $F_6 = p_2 q_2$ where $p_2 = 274177$ and $q_2 = 67280421310721$. Add the following to the congruences in Eq. (1).

$$\begin{aligned} n \equiv 2^6 \pmod{2^7}, \quad k \equiv 1 \pmod{p_2} \quad &\Longrightarrow \quad k \cdot 2^n + 1 \equiv 0 \pmod{p_2} \\ n \equiv 0 \pmod{2^7}, \quad k \equiv 2^{2^5} \pmod{q_2} \quad &\Longrightarrow \quad k \cdot 2^n + 1 \equiv 0 \pmod{q_2} \end{aligned} \tag{4}$$

If $2^7 \nmid n$, then for all integers $t > 0$, $k^t 2^n + 1 \equiv 0 \pmod{p}$ for the correct choice of $p \in \{F_0, F_1, F_2, F_3, F_4, p_1, p_2\}$. If instead $2^7 | n$, then q_1 divides $k^t 2^n + 1$ for odd t, and q_2 divides $k^t 2^n + 1$ for $t \equiv 2 \pmod 4$ (since $q_1 \mid k + 1$ and $q_2 \mid k^2 + 1$). These last congruences are key—we need k^t to be congruent to -1 at the correct times. This can be arranged by making k congruent to the correct power of the base b (for example, $k \equiv 2^{2^5}$ in the last case of *both* Eq. (1) and (4)).

By using multiple composite terms, we may use the same construction to find k for which k^t is also a b-Sierpiński for all t except those divisible by high powers of 2. This was done by Filaseta *et al.* [9] for the regular Sierpiński numbers, and virtually the same argument works here. We begin with a modified version of Theorem 1.

Theorem 8. *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 is an arithmetic progression of integers k such that $k^t b^n + 1$ $(n > 0)$ are composite for each integer 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. (Note $r_m = 0$ if b is even; also $r_m = 1$ if b is odd and $m > 0$.) 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 $b + 1 = 2^{r_0}$. We have ruled out this case, so 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 that for $i > 0$ we have

$$b^{2^i} - 1 = (b-1)(b+1)(b^2+1)(b^4+1)\cdots(b^{2^{i-1}}+1), \tag{5}$$

so $b, b-1$, and $F'_m(b)$ $(m \geq 0)$ are pairwise relatively prime. By the Chinese Remainder Theorem there is an arithmetic sequence of 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, where

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

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

If $i \le m_w$, 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 $b^{2^i}-1$ by Eq. (5). Thus d divides $b^{2^i n'}-1$ and it follows that

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

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 . 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

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

Table 1: k such that k^t is a 5-Sierpiński number when $2^r \nmid t$

form	number	form	number
$2^{2^m}+1$	238	$6^{2^m}+1$	222
$(3^{2^m}+1)/2$	256	$10^{2^m}+1$	232
$(5^{2^m}+1)/2$	246	$12^{2^m}+1$	230

Table 2: Number of generalized Fermat numbers known to be composite

the cofactor as the second "prime." Table shows that there are 246 known composite generalized Fermat numbers $F_m(5)$ (Keller [14]), so there are 5-Sierpiński numbers k for which $k, k^2, k^3, \ldots, k^{2^{246}-1}$ are all 5-Sierpiński numbers.

Next, Theorem 1 states that the terms of the sequence $k \cdot b^n + 1$ are not only composite, but have (at least) two distinct prime divisors. Towards this end we prove the following.

Lemma 9. *Let $L > 0$, $b \geq 2$, and $r \geq 3$ be integers. Then there is a positive integer $N = N(L, b, r)$ such that for each integer $k > N$ and every integer $n > 0$, $k^r b^n + 1$ has a prime factor greater than L.*

Proof. With L and r fixed as in the lemma we must show there are only finitely many integers $n > 0$ for which $k^r b^n + 1$ contains no prime factors greater than L; i.e.,

$$k^r b^n + 1 = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m} \tag{6}$$

where the p_i are the primes less than or equal to L. Writing $e_i = q_i r + r_i$ and $n = q_0 r + r_0$ where q_i and r_i are non-negative integers satisfying $r_i < r$ $(0 \leq i \leq m)$, Eq. (6) is

$$p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} (p_1^{q_1} p_2^{q_2} \cdots p_m^{q_m})^r - b^{r_0} (k b^{q_0})^r = 1. \tag{7}$$

Thus n satisfies one of a finite number of Thue equations $Ax^r - By^r = 1$ (with r^m choices of A and r for B). Each such equation has only finitely many solutions [15, Chpt. 22]. □

Proof of Theorem 1. By Theorem 8, we have infinitely many integers k such that $k^t b^n + 1$ $(n > 0,\ 2^r \nmid t)$ are all divisible by a prime in the cover constructed in that proof. Let L be the largest prime in that cover. These primes also cover $k^{3t} b^n + 1$ $(n > 0,\ 2^r \nmid t)$, so we may complete the proof by applying Lemma 9. □

4. Removing the Dependence on Factorization

In this section we will show that we can do away with the need to know factors of generalized Fermat numbers for those bases of the form b^b. Remember that the key to Sierpiński's original cover (and our extension above) was finding a multiplier k which, when raised to the correct power of two, gave us -1 modulo some prime. Lemma 11 will help provide that term. First we need to recall a pivotal result of A. S. Bang [1].

Theorem 10 (Bang's Theorem). *Let b and n be positive integers with $b \geq 2$. Then $b^n - 1$ has a primitive divisor unless $b = 2$ and $n = 6$; or $b + 1$ is a power of 2 and $n = 2$.*

Lemma 11. *Let $b > 1$ and $s > 1$ be integers. Let q be an odd prime which does not divide b. Then there is an odd primitive prime divisor p of $b^{bq2^s} - 1$. Any such divisor satisfies the following:*

(i) $\mathrm{ord}_p(b) = bq2^s$

(ii) *the prime p does not divide $F_n(b)$ or $F_n(b^b)$ for any $n \geq 0$*

(iii) *there is an integer e for which $e^{b2^s} \equiv -1 \pmod{p}$*

Proof. The prime 2 can not be a primitive divisor of $b^n - 1$ for $n > 1$, so the existence of an odd prime divisor p follows from Bang's Theorem (Theorem 10). Since p is a primitive divisor of $b^{bq2^s} - 1$, it does not divide $b^t - 1$ for any $t < bq2^s$, proving (i). Note q is odd and does not divide b, so q does not divide the order of b modulo any divisor of $F_n(b)$ or $F_n(b^b)$, so (ii) now follows from (i). Also (i) implies $bq2^s$ divides $p - 1$, so in particular, $s > 1$ implies $(p-1)(b-1) \equiv 0 \pmod 8$, and $p \equiv 1 \pmod b$. The Jacobi symbol satisfies $(b|p) = (p|b) = (1|b) = 1$. This means there is an integer x for which $x^2 \equiv b \pmod p$, so $e = x^q$ then has order $2^{s+1}b$ by part (i). Thus $e^{2^s b} \equiv -1 \pmod p$, giving (iii). □

Now we may presents a version of Theorem 1 which does not require us to know the factors of generalized Fermat numbers. (This is slightly stronger than the version Theorem 2 stated in the introduction.)

Theorem 12. *Let $b > 1$ be an integer. For every positive integer R, there exist infinitely many integers k for which each of $k, k^2, k^3, \ldots, k^R$ are each b^b-Sierpiński numbers, and the associated terms $k^t(b^b)^n + 1$ ($n > 0$, $1 \leq t \leq R$) each have at least two distinct prime divisors.*

Proof. So that we may apply Lemma 11, we will prove there are infinitely many integers k for which

$$k^{4b}(b^b)^n+1, k^{8b}(b^b)^n+1, k^{12b}(b^b)^n+1, \ldots, k^{4bR}(b^b)^n+1 \tag{8}$$

each have at least two distinct prime divisors for each positive integer n. These multipliers k^{4b} will then meet the requirements of our theorem.

The terms in Eq. (8) have the form $k^r(b^b)^n+1$ with r a multiple of $4b$. Write $r = 2^s br'$ where r' is odd. Note that s and r' are functions of r, $s \geq 2$ and $2^{s-2}r' \leq R$. Below we will find a cover $\mathcal{P}_r$ for a fixed value of r (with variable n), and the final cover will be the union of the covers for each r.

Choose an odd prime $q = q(r)$ such that $\gcd(q, r'b) = 1$, and the primes $q(r)$ are distinct for each r. Let M be the maximum of $\{s(r)+q(r)-1\}$ over the values of r.

Note that b^b+1 is not a power of 2, so we may begin our cover just like Sierpiński did, setting

$$k \equiv 1 \pmod{p_j} \qquad \text{for } 0 \leq j \leq M, \tag{9}$$

where $p_j > 1$ is any odd divisor of $F_j(b^b)$. If $n \equiv 2^j \pmod{2^{j+1}}$ for some $j \leq s+q-2$, then $n = 2^j n'$ for some odd integer n', and it follows that

$$k^r(b^b)^n+1 \equiv 1^r(-1)^{n'}+1 \equiv 0 \pmod{p_j}.$$

The set of congruences in Eq. (9) will be used as part of the cover for every r, though not every r will require all of them.

This leaves

$$n \equiv 0 \pmod{2^{s+q-1}},$$

which we will cover with a different set of congruences for each $r \leq 4bR$. Now n must satisfy one of the $q = q(r)$ congruences

$$n \equiv j2^{s+q-1} \pmod{2^{s+q-1}q} \qquad \text{for } 0 \leq j \leq q-1.$$

As $2q$ and r' are relatively prime, we know $j2^{s+q-1}$ and $jr'2^{s+q-1}$ produce the same set of residues modulo $2^{s+q-1}q$, so n must satisfy one of

$$n \equiv jr'2^{s+q-1} \pmod{2^{s+q-1}q} \qquad \text{for } 0 \leq j \leq q-1. \tag{10}$$

Lemma 11 tells us that for each j there is a prime divisor $\hat{p}_j = \hat{p}_j(r)$ of $b^{2^{s+j}bq}-1$ together with an integer $e_j = e_j(r)$ such that $e_j^{2^{s+j}b} \equiv -1 \pmod{\hat{p}_j}$. To the cover started in Eq. (9) we now add

$$k \equiv e_j^{2^j} b^{-j2^{q-1}} \pmod{\hat{p}_j} \qquad \text{for } 0 \leq j \leq q-1. \tag{11}$$

By Equation (10), for each j we now may write n as $jr'2^{s+q-1}+2^{s+q-1}qQ$ for some integer Q. So modulo $\hat{p}_j$ we now have

$$\begin{aligned} k^r(b^b)^n &\equiv (e_j^{2^j} b^{-j2^{q-1}})^{2^s br'} (b^b)^{jr'2^{s+q-1}+2^{s+q-1}qQ} \\ &\equiv (e_j^{2^{s+j}br'})(b^{-jbr'2^{s+q-1}} b^{jbr'2^{s+q-1}}) b^{2^{s+q-1}bqQ} \\ &\equiv (e_j^{2^{s+j}b})^{r'}(1)(b^{2^{s+j}bq})^{2^{q-j-1}Q} \equiv (-1)^{r'} 1^{2^{q-j-1}Q} \equiv -1. \end{aligned} \tag{12}$$

So $\hat{p}_j$ divides $k^r(b^b)^n+1$.

Thus, for all $n>0$, $k^r(b^b)^n+1$ has a divisor among the set

$$\mathcal{P}_r = \{p_0, p_1, \ldots, p_{s+q-1}, \hat{p}_0, \hat{p}_1, \ldots, \hat{p}_{q-1}\}.$$

By Lemma 11, $\hat{p}_j(r)$ is an odd prime for which b has the order $2^{s+j}bq(r)$. Since the primes $q(r)$ are distinct, these primes (as j and r vary) are all distinct. They also do not divide b or $b-1$, so we may apply the Chinese Remainder Theorem to show there are infinitely many solutions to the system of congruences defined by

$$k \equiv 0 \pmod{b-1} \qquad \text{and} \qquad k \equiv 1 \pmod{b} \tag{13}$$

and those in Eq. (9) and (11) (for each r). These two additional congruences (Eq. (13)) ensure that $\gcd(k-1, b+1) = 1$ and k is not a rational power of b.

Thus for k sufficiently large, k^r is a b-Sierpiński number for each r. If our desire is solely to show these numbers are b-Sierpiński numbers, sufficiently large means larger than the maximum L of the primes used to form the covers $\mathcal{P} = \cup\mathcal{P}_r$ where the union is over $r \in \{4, 8, 12, \ldots 4R\}$. If we wish to prove the stronger statement that each of the numbers $k^r(b^b)^n+1$ have *at least two* distinct prime divisors, we can use Lemma 9 with this same maximal prime L, to define an appropriate lower bound for k. □

We would have liked to use b, rather than b^b, in the previous theorem, but we needed $(b|p) = 1$ in Lemma 4.4. This requires b in the exponent of the Mersenne term, so also in the exponent of the multiplier k. Finally, this requires b divide the exponent of b, so that terms cancel appropriately in Eq. (12).

5. Additional Proofs

In this last section we prove the result mentioned at the end of Section 1. We begin with an elementary lemma.

Lemma 13. *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 14. *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 13, 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 (not necessarily odd) integer 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 that

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

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

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

□

References

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

[2] G. Barnes, Sierpiński conjecture reservations, May 2008, `http://gbarnes017.googlepages.com/Sierp-conjecture-reserves.htm`.

[3] 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; *MR* 2278921.

[4] R. Bowen, The sequence $ka^n + 1$ is composite for all n, *Amer. Math. Monthly,* **71**:2 (1964), 175–176.

[5] A. Brunner, C. Caldwell, D. Krywaruczenko & C. Lownsdale, Generalizing Sierpiński numbers to base b, New Aspects of Analytic Number Theory, Proceedings of RIMS, Kyoto University, Kyoto, October 27–29, 2008. Surikaisekikenkyusho Kokyuroku (2009). Kyoto University, Research Institute for Mathematical Sciences, Kyoto, April 2009, 69–79.

[6] 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; *MR* 1955419.

[7] H. Dubner & W. Keller, Factors of generalized Fermat numbers, *Math. Comput.*, **64** (1995) 397-405; *MR* 1270618.

[8] P. Erdös, On integers of the form $2^k + p$ and some related problems, *Summa Brasil. Math.*, **2** (1950) 113-123; *MR* 0044558.

[9] 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.

[10] R. K. Guy, *Unsolved Problems in Number Theory* (3rd ed.), Problem Books in Mathematics, Springer-Verlag, New York, 2004; *MR* 2076335.

[11] G. H. Hardy & E. M. Wright, *An introduction to the theory of numbers*, (5th ed.), Oxford University Press, New York, 1979; *MR* 81i:10002.

[12] A. S. Izotov, A note on Sierpiński numbers, *Fibonacci Quart.*, **33** (1995), 206–207; *MR* **96f**:11020.

[13] L. Jones, Variations on a theme of Sierpiński, *J. Integer Seq.*, **10** (2007), Article 07.4.4, 15 pp. (electronic); *MR* 2304362.

[14] W. Keller, Factors of generalized Fermat numbers found after Björn & Riesel, `http://www1.uni-hamburg.de/RRZ/W.Keller/GFNfacs.html`, Jan. 2009.

[15] L. J. Mordell, *Diophantine equations,* Pure and Applied Mathematics, **30**, Academic Press, New York, 1969.

[16] D. Schleicher, unpublished notes, 1991.

[17] 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.