# A REVERSE SIERPIŃSKI NUMBER PROBLEM

DAN KRYWARUCZENKO

ABSTRACT. A generalized Sierpiński number base $b$ 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 $n > 0$. Given an integer $k > 0$, we will seek a base $b$ for which $k$ is a generalized Sierpiński number base $b$. We will show that this is not possible if $k$ is a Mersenne number. We will give an algorithm which will work for all other $k$ provided that there exists a composite in the sequence $\{(k^{2^m}+1)/\gcd(k+1, 2)\}_{m=0}^{\infty}$.

## 1. INTRODUCTION

A Sierpiński number $k > 0$ is an odd number such that $k \cdot 2^n + 1$ is composite for all integers $n > 0$. Waclaw Sierpiński, in 1960, proved that there are infinitely many such numbers [12] but found no exact values. (This is a dual of a problem of Euler that Erdös solved in 1950 [6].) In 1962 John Selfridge discovered what may be the smallest Sierpiński number, 78,557. He showed that each term in the sequence $78557 \cdot 2^n + 1$ is divisible by one of the primes in the covering set $\{3, 5, 7, 13, 19, 37, 73\}$. After 45 years of computing there remains only 6 possible numbers less than 78,557 that must be eliminated to prove this is true [9].

In our previous paper [1], we extended the definition of Sierpiński numbers to include other bases (as below) and found Sierpiński numbers for each of the bases $2 \le b \le 100$. We proved that for 33 of the bases, these were the least possible Sierpiński numbers.

**Definition 1.1.** A **Sierpiński number base** $b$ 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 $n > 0$.

The gcd condition is to avoid having a single prime which divides every term of the sequence; these are called trivial covers (or 1-covers). The rational power condition avoids numbers of the form $b^{2^n} + 1$, the generalized Fermat numbers. Some researchers do not exclude these and instead exclude those $k$ which allow polynomial factorization [8]. Others have generalized the notion of Sierpiński numbers by altering the conditions on $k$ without changing the base $b$ [11, 2, 3, 4, 5, 7].

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

This research was completed at the University of Tennessee at Martin under the direction of Dr. Chris K. Caldwell.

**Definition 1.2.** 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 $S$. $S$ is called a **N-cover** if $N$ is the least positive integer for which each prime in $S$ divides $k \cdot b^n+1$ if and only if it divides $k \cdot b^{n+N}+1$. We will call this integer $N$ the **period of the cover** $S$.

In our previous paper we showed that every integer base $b > 1$ admitted a Sierpiński number $k$. In this paper we will reverse the problem and ask for each integer $k > 1$ is there a base $b$ for which $k$ is a Sierpiński number.

Using a program to find Sierpiński numbers for small bases [1] we found that every positive integer less than 3000 is a Sierpiński number (with a cover with period dividing 5040) for some base less than 10,000,000 except for $k = 2, 3, 5, 7, 15, 31, 63, 65, 127, 255, 511, 1023$, and 2047.

A Mersenne is a number of the form $2^m - 1$ where (e.g., $2^8 - 1$). We will show that when $k$ is a Mersenne number, $k \cdot b^n + 1$ can not have a non-trivial cover. Most Sierpiński numbers arise through covers, though it is also possible for them to arise by algebraic factorization or a combination of the two [1]. But it is very unlikely that such factorizations arise when $k$ is a Mersenne [8, 10]. Once we eliminate the Mersenne numbers from the list above we are left with 2, 5, and 65.

It was conjectured that there is no base which makes 2 a Sierpiński number [13]. We will find bases for which 2, 5, and 65 are Sierpiński numbers, and then characterize those $k$ which cannot be Sierpiński numbers.

## 2. Preliminary Theorems

**Theorem 2.1.** *Suppose $k \cdot b^n + 1$ has a cover $S$ with period $N$. Then each prime in $S$ divides $(-k)^N - 1$ and $b^N - 1$.*

*Proof.* Let $S$ be such a cover and let $p \in S$. Then $p$ divides $k \cdot b^n + 1$ for some $n$ with $1 \leq n \leq N$. Since $N$ is our period and $p \in S$ we know $p$ divides $k \cdot b^n + 1$, $k \cdot b^{n+N} + 1$, and their difference $k \cdot b^n(b^N - 1)$, but does not divide $k \cdot b^n$. So $b^N \equiv 1 \pmod{p}$. Now $k \cdot b^n + 1 \equiv 0 \pmod{p}$ so $k \equiv -b^{-n} \pmod{p}$ and $(-k)^N \equiv (b^{-n})^N \equiv 1 \pmod{p}$. □

Notice 2 cannot be a member of a non-trivial cover because if 2 divides $k \cdot b^n + 1$ and 2 divides $b^N - 1$, then 2 divides $\gcd(b - 1, k + 1)$.

**Theorem 2.2.** *If $k$ is a Mersenne number and $n \geq 0$, then $k \cdot b^n + 1$ cannot have a non-trivial cover.*

*Proof.* We will prove the contrapositive. Let S be a non-trivial cover of $k \cdot b^n + 1$ with period $N$. Then there is some odd prime $p \in S$ which divides $k \cdot b^N + 1$. By the previous theorem, $b^N \equiv 1 \pmod{p}$, so $p$ divides $k + 1$. This means $k + 1$ has an odd prime divisor. Therefore, $k + 1$ is not a power of 2. □

These theorem suggests the following approach to finding a base $b$ which makes $k$ a Sierpiński number. First, select a period $N$ for the cover. Then

factor $(-k)^N - 1$. Using each of its prime divisors $p$, we would find a specific $b$ value such that $p$ divides $b^N - 1$, but not $b - 1$, and $p$ divides $k \cdot b^n + 1$ for some $n < N$. If this is possible, then a list could be formed showing the specific $b$ values and $n$ values satisfying the requirements for each prime. After repeating this for each prime, determine whether there is a set of bases and primes such that the entire set of $N$ terms would be covered. If so, we then solve the problem by using the Chinese Remainder Theorem.

We used this method to solve for $b$ when $k = 12$. We have $(-12)^6 - 1 = 7 \cdot 11 \cdot 13 \cdot 19 \cdot 157$. Using the primes 7, 13, and 19 coupled respectively with base residues 4, 3, and 7 for $b$, the Chinese Remainder Theorem gave the result $b = 900$. The primes in the cover $\{7, 13, 19\}$ divide the sequence of terms $12 \cdot 900^n + 1$ with period 3 in the following pattern.

$$\underbrace{7,\ 19,\ 13,}\ \underbrace{7,\ 19,\ 13,}\ \ldots$$

However, with $k = 2$ we ran into difficulties. The approach appeared to fail for all periods $N \leq 60$. For example, when we set our period at 60 (a smooth number which is likely to yield results), we cover either $2 \cdot b^{15} + 1$ or $2 \cdot b^{45} + 1$ but not both. When we set the period at 48, this process would fail at one of these specific $n$ values: $\{3, 9, 17, 15, 21, 27, 33, 39, 41, 45\}$. The key problem is that $k \cdot b^n + 1 \equiv 0 \pmod{p}$ may be impossible to solve for a certain $k$, $n$, and $p$; so we will give an alternative approach in the next section.

## 3. Period length a power of two

We need a few more results before we present our alternate method.

**Theorem 3.1.** *If $n > m \geq 0$, then $\gcd(k^{2^m} + 1, k^{2^n} + 1) = \gcd(k + 1, 2)$.*

*Proof.* Note $k^{2^m} + 1$ is one of the terms on the left of

$$(k-1)(k+1)(k^2+1) \cdot \ldots \cdot (k^{2^{n-1}} + 1) = k^{2^n} - 1 = (k^{2^n} + 1) - 2,$$

so $\gcd(k^{2^m} + 1, k^{2^n} + 1)$ divides 2. If $k$ is even then the greatest common divisor is one; otherwise it is 2. □

**Theorem 3.2.** *If $n > 0$ and $k > 1$, then $k^{2^n} + 1$ has an odd prime factor.*

*Proof.* If $k$ is even, then $k^{2^n} + 1$ is an odd number greater than 1, so we are done. If instead $k$ is odd, then $\gcd(k^{2^n} + 1, 4) = 2$ and $(k^{2^n} + 1)/2$ is an odd number greater than or equal to 5, so again it has an odd prime factor. □

**Theorem 3.3.** *Let $p$ be an odd prime which divides $k^{2^m} + 1$ for some fixed integer $m > 0$. For all odd integers $n$ it is possible to solve $k \cdot b^n + 1 \equiv 0 \pmod{p}$ for a solution $b = (-k)^j$. This solution satisfies $k \cdot b^M + 1 \equiv 0 \pmod{p}$ if and only if $\operatorname{ord}_p(b)$ divides $M - n$.*

*Proof.* Let $m > 0$. From what we are given $(-k)^{2^m} \equiv -1 \pmod{p}$, hence $(-k)^{2^{m+1}} \equiv 1 \pmod{p}$. So we know $-k$ has order $2^{m+1}$ modulo $p$. To solve $k \cdot b^n + 1 \equiv 0 \pmod{p}$ for $b$, let $b = (-k)^j$ for some $j \geq 0$ and solve

$(-k)^{j\cdot n+1} \equiv 1 \pmod{p}$. It is sufficient to solve $j \cdot n+1 \equiv 0 \pmod{\operatorname{ord}_p(-k)}$ which is possible because $n$ and the order of $-k \pmod{p}$ are relatively prime. Note that $j$ must be odd, so the solution $b$ has order $2^{m+1}$ also. □

We are now able to present our new approach as Algorithm 1.

**Algorithm 1**: Find $b$ so that $k$ is a Sierpiński number base $b$

```
1  input k > 1
2  if k is a Mersenne number then
3  |  return "[probably] not possible"
4  else
5  |  m ← −1
6  |  repeat
7  |  |  m ← m + 1
8  |  |  p_m ← the least odd prime which divides k^(2^m)+1
9  |  |  n ← 2^m + 1
10 |  |  solve k · b_m^n + 1 ≡ 0 (mod p_m) for b_m
11 |  until m > 0 and there is another odd prime which divides
   |  k^(2^m)+1
12 |  call this second prime p_{m+1}
13 |  define b_{m+1} by k · b_{m+1} + 1 ≡ 0 (mod p_{m+1})
14 |  find b so that b ≡ b_i (mod p_i) for 0 ≤ i ≤ m + 1, and
   |  gcd(k + 1, b − 1) = 1
15 |  return base b, cover S = {p_0, p_1, ... p_{m+1}}, period 2^{m+1}
16 endif
```

**Theorem 3.4.** *Suppose $k > 1$ is not a Mersenne number. If there is a composite in the sequence*

$$\{(k^{2^m}+1)/\gcd(k+1,2)\}, \qquad (m > 0) \tag{3.1}$$

*then Algorithm 1 will find a base $b$ for which $k$ is a Sierpiński number.*

Before we present the proof, we will illustrate the use of this algorithm with $k = 2$. After the first time through the loop (steps 6 through 11), $m = 0$, $p_0 = 3$, $n = 2$, and $b_0 \equiv 2 \pmod 3$. So after we solve for $b \equiv b_0$, 3 will divide the second term of the sequence $k \cdot b^v + 1$ for $v = \{1, 2, \ldots, \}$ and every other term because $b$ has period 2 modulo 3. This prime begins our cover and at this stage the pattern with which the primes in the cover divides the terms $k \cdot b^v + 1$ for $v = \{1, 2, \ldots, \}$ and looks like the following:

$$\underbrace{\_\_,\ 3,}\ \underbrace{\_\_,\ 3,}\ \ldots$$

That is, 3 divides $2 \cdot b^v + 1$ for $v = 2, 4, 6, \ldots$.

After the second time through the loop, $m = 1$, $p_1 = 5$, $n = 3$, and $b_1 \equiv 3 \pmod 5$. So 5 divides the third term and then every fourth because $2^{1+1} = 4$

is the period of $b_1(mod p_1)$ by Theorem 3.3. So our divisibility pattern now looks like:

$$\underbrace{\_\_,\ 3,\ 5,\ 3,}\ \underbrace{\_\_,\ 3,\ 5,\ 3,}\ \dots$$

After the third time through $p_2 = 17$ and $b_2$ has order 8, so we now have a pattern with period $2^3$

$$\underbrace{\_\_,\ 3,\ 5,\ 3,\ 17,\ 3,\ 5,\ 3,}\ \underbrace{\_\_,\ 3,\ 5,\ 3,\ 17,\ 3,\ 5,\ 3,}\ \dots$$

The primes for iterations four and five are 257 and 65537 see (Table 1), leaving a pattern with period $2^5$.

Notice that each time through the loop the period doubles; however, since we have added just one prime to each stop we are still left with one hole. If we were to ever get a case in which there were two odd primes dividing $k^{2^m}+1$ then we can fill in that hole! In our example, it is the sixth iteration in which this first occurs (when $2^{2^5} + 1 = 641 \cdot 6700417$), so we double the period again but we can also now fill in the last hole. Finally, we solve for $b$ using the Chinese Remainder Theorem. Thus, when $k = 2$, we find $b = 16979062410086072498$ and the cover $\{3, 5, 17, 257, 641, 65537, 6700417\}$ that repeats with period 64.

Similarly, with $k = 5$, we find $b = 140324348$ and the cover $\{3, 13, 17, 313, 11489\}$ with a period of 16. Finally, for $k = 65$, $b = 19030688904264$ with cover $\{3, 17, 113, 2113, 8925313\}$ with a period of 16.

*Proof of Theorem 3.4.* The algorithm starts with an input $k > 1$. If $k$ is a Mersenne number, the algorithm throws it out because of Theorem 2.2. Next, we start the loop with $m = 0$, and find the least odd prime $p_0$ that divides $k + 1$ (we know this exists because $k$ is not a Mersenne). When $m = 0$, it is also possible to solve $k \cdot b_0^2 + 1 \equiv 0 \pmod{p}$, because $k \equiv -1 \pmod{p}$. So if we let $b_0 \equiv -1 \pmod{p}$, then $k \cdot b_0^2 + 1 \equiv 0 \pmod{p}$. Note that if $b \equiv b_0 \pmod{p_0}$ then $p_0$ divides every other term in the sequence $k \cdot b^n + 1$ because $b_0$ has order 2 mod $p_0$.

During the next loop $m = 1$ and we know that $k^{2^1} + 1$ has an odd prime factor (for all $m > 0$) from Theorem 3.2. Thus, we solve $k \cdot b_1^n + 1 \equiv 0 \pmod{p_1}$ for base $b_1$, which is possible (for all $m > 0$) by Theorem 3.3. By Theorem 3.2, we know our solution has order $2^{m+1} = 4$ so we have a pattern

$$\underbrace{\_\_,\ p_0,\ p_1,\ p_0}\ ,\ \underbrace{\_\_,\ p_0,\ p_1,\ p_0,}\ \cdots$$

We repeat this process (steps $6 - 11$) until there are two odd primes which divide $k^{2^m} + 1$. For the first prime $p_m$, the algorithm solves (as usual) $k \cdot b_m^n + 1 \equiv 0 \pmod{p_m}$. With the second prime, $p_{m+1}$, the algorithm solves $k \cdot b_{m+1} + 1 \equiv 0 \pmod{p_{m+1}}$ for base $b_{m+1}$ to fill in the last hole in our pattern. So we have a cover $\{p_1, \dots, p_{m+1}\}$ which divide the terms $k \cdot b^n + 1$ with a pattern determined by Theorem 3.3 to be

$$\underbrace{p_{m+1},\ p_0,\ p_1,\ p_0,\ p_2,\ p_0,\ \dots\ p_m,\ \dots\ p_0,\ p_1,\ p_0}\,.$$

We then use the Chinese Remainder Theorem (step 13) to solve for $b$. However, we must make sure the cover is not trivial so if $\gcd(k+1, b-1) \neq 1$, we can add $p_1 p_2 \cdot \cdots \cdot p_{m+1}$ to $b$ to get $b'$. Now $\gcd(k+1, b'-1) = 1$ by Theorem 3.1. We are then left with a base $b$ that makes $k$ a Sierpiński Number with a cover $S$ and a period equal to $2^{m+1}$. □

TABLE 1. The Algorithm Table

| $m$ | $k^{2^m}+1$ | $p_m$ | $n$ | $b_m \pmod p$ |
|---|---|---|---|---|
| 0 | 3 | 3 | 2 | 2 |
| 1 | 5 | 5 | 3 | 3 |
| 2 | 17 | 17 | 5 | 9 |
| 3 | 257 | 257 | 9 | 129 |
| 4 | 65537 | 65537 | 17 | 32769 |
| 5 | $641 \cdot 6700417$ | 641 | 33 | 321 |
| | | 6700417 | 1 | 3350208 |

## 4. Conclusion

It is highly unlikely that there exists an integer $k$ for which the sequence of generalized Fermat numbers of equation 3.1 are all prime. So given a $k$, we have shown how to find bases $b$ for which $k \cdot b^n + 1$ has non-trivial cover, for all $k$ for which these exist! However, this does not mean our choice of $b$ is the least. Computations have shown that our solution for $k = 5$ is the smallest with period dividing 5040, but we do not know if the others are the smallest.

## References


1. A. Brunner, D. Krywaruczenko, C. Lownsdale & C. Caldwell, The Sierpiński numbers base $b$, in process.
2. Y. 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.
3. Y. Chen, On integers of the form $k2^n + 1$, *Proc. Amer. Math. Soc.* **129** (2001), 355–361.
4. Y. Chen, On integers of the forms $k - 2^n$ and $k2^n + 1$, *J. Number Theory* **89** (2001), 121–125.
5. Y. Chen, On integers of the forms $k^r - 2^n$ and $k^r 2^n + 1$, *J. Number Theory* **98**:2 (2003), 310–319.
6. P. Erdös On integers of the form $2^k + p$ and some related problems, Summa Brasil. Math. #2 (1950), 113-123.
7. M. Filaseta, C. Finch and M. Kozek, *On powers associated with Sierpiński numbers, Riesel numbers and Polignac's conjecture*, (submitted).
8. A. Granville and P. Pleasants, Aurifeuillian Factorization Mathematics of Computation, **75**:253, 497–508.
9. L. Helm & D. Norris, Seventeen or Bust–a distributed attack on the Sierpiński problem, `http://www.seventeenorbust.com/`.
10. A. Izotov, A note on Sierpiński numbers, *Fibonacci Quart.* **33**:3 (1995), 206–207.

11. L. Jones, Variation on a theme of Sierpiński, *J. Integer Seq.,* **10**, (2007), article 07.4.4.
12. W. Sierpiński, Sur un problème concernant les nombres $k \cdot 2^n + 1$, *Elem. Math.*, **15**(1960) 73–74; corrigendum, **17**(1962) 85.
13. R.W. Smith, Personal correspondence.