Parabola Volume 56, Issue 2 (2020)

A modular arithmetic analysis of the Sierpiński Number Problem

Arya R. Kondur[1]

1 Introduction

The term "Sierpiński number" comes from renowned Polish mathematician Wacław Sierpiński. However, the work involved dates to an earlier mathematician by the name of Raphael M. Robinson. In 1958, Robinson [2] developed a table of prime numbers of the form $k2^n + 1$ and in doing so, he found primes for all values of k less than 100 except for $k = 47$.

Following this discovery, Sierpiński [4] then proved in 1960 that there are infinitely many odd integers k such that $k2^n + 1$ is not prime for any integers n. This is a fascinating result and it led to the search for the least possible such value of k, or in colloquial terms, the least *Sierpiński number*. This search is called the *Sierpiński Number Problem*. In 1962, John Selfridge proved that $k = 78557$ was a Sierpiński number. This was done mainly through private correspondence with Paul Erdős, who commented on this result in [1]. Selfridge's proof used the concept of a covering set, which we shall discuss in the following section. Selfridge went beyond this proof and conjectured that this value was the least Sierpiński number. At the time, and even currently, $k = 78557$ is the least known Sierpiński number.

However, there still remain five numbers - 21181, 22699, 24737, 55459, 67607 - that could be even smaller Sierpiński numbers. To eliminate any of these numbers, it suffices to find a value of $k2^n + 1$ that is prime. Many computational techniques [4] are being used despite the obstacles caused by the increasing size of prime numbers. Thus, in this paper, we aim to complete two tasks. First, prove theorems that will allow us to simplify the Sierpiński Number Problem. Second, develop a searching method for prime numbers that would aid the current sequential searching techniques.

[1] Arya R. Kondur is a student at Monta Vista High School, California, USA.

2 Introductory theorems and definitions

We shall start with the most simple definition relating to Sierpiński numbers, which is that of covering sets. David Wells [5] has given an apt definition, but we tailor it to our needs here.

Definition 1. *Given a Sierpiński number k, let C_k denote a* covering set *for k: this is a smallest possible set of distinct prime numbers such that, for all $n \in \mathbb{N}$, at least one element in C_k divides $k2^n + 1$.*

Each Sierpiński number has a partial covering set, which is a subset of its full covering set. A more formal definition is given below.

Definition 2. *Given a Sierpiński number k and a positive integer n, let $P_{n,k}$ denote a* partial covering set *for k: this is a smallest possible set of distinct prime numbers such that, for all $m \leq n$, at least one element in S divides $k2^n + 1$. A* partial covering set *is the smallest possible set of distinct prime numbers such that for all positive integers $m \leq n$ at least one element in $P_{n,k}$ divides $k2^m + 1$.*

For some positive integers, there exists a covering set such that each element will repeat as a divisor of $k2^n + 1$ in a cyclic pattern.

Definition 3. *Let k be a positive integer. A prime number p is said to* cycle by *a positive integer d with respect to k if and only if p divides $k2^{n+d} + 1$ whenever p divides $k2^n + 1$ for any n. A covering set C_k (resp., partial covering set $P_{n,k}$) is said to* cycle by *a positive integer d with respect to k if and only if p cycles by d with respect to k for each element $p \in C_k$ (resp., $c \in P_{n,k}$).*

For each prime p, let $F(p)$ be the smallest positive integer such that $2^d \equiv 1 \pmod{p}$.

Theorem 4. *For all positive integers k and d, each prime p cycles by $dF(p)$ with respect to k.*

Proof. Suppose that $k2^n + 1 \equiv 0 \pmod{p}$. Then

$$k2^{n+dF(p)} + 1 \equiv k2^n 2^{dF(p)} + 1 \equiv k2^n \left(2^{F(p)}\right)^d + 1 \equiv k2^n 1^d + 1 \equiv k2^n + 1 \equiv 0 \pmod{p}.$$

By Definition 3, p cycles by $dF(p)$ with respect to k. □

Now, we shall define two sets that will be used throughout the rest of this paper:

$$M_k = \{F(c) \ : \ c \in C_k\}$$
$$M_{n,k} = \{F(m) \ : \ m \in P_{n,k}\}$$

Note that $M_{n,k}$ is a subset of M_k. Also, let L_k be the least common multiple of the elements in M_k and let $L_{n,k}$ be the least common multiple of the elements in $M_{n,k}$.

Theorem 5. *For each positive integer k, C_k cycles by L_k with respect to k, and $C_{n,k}$ cycles by $L_{n,k}$ with respect to k.*

Proof. Let $p \in C_k$. By definition, L_k is a multiple of $F(p)$, so $L_k = dF(p)$ for some positive integer d. By Theorem 4, p cycles by L_k with respect to k. The second claim is proved similarly. □

Definition 6. *For all integers n and k, let $D_{n,k}$ be the set of prime divisors of $k2^n + 1$. An* optimal divisor *of $k2^n + 1$, denoted by $\sigma_{n,k}$, is an element $p \in D_{n,k}$ with smallest value $F(p)$.*

In other words, out of all the elements $d \in D_{n,k}$, the value $F(d)$ is minimized when $d = \sigma_{n,k}$. This leads to the following theorem.

Theorem 7. *For all positive integers n and Sierpiński numbers k, $\sigma_{n,k} \in C_k$.*

Proof. By definition, a covering set C_k must be smallest possible, so each element in C_k must cycle by the least number possible. By Theorem 5, C_k will cycle by L_k, which is the least common multiple of the elements in M_k. In order for L_k to be minimal, $\sigma_{n,k}$ must belong to C_k. □

This concludes the discussion of the basic definitions and theorems needed to further the analysis of the Sierpiński numbers.

3 Application to possible Sierpiński numbers

At the date of writing this paper, there remain five integers still in contention to be named the smallest Sierpiński number. In the following subsections, we analyze each number in more detail using the theorems and definitions established in Section 2. For the following table, keep in mind the notation $F(x)$ first mentioned in Theorem 4.

Odd prime divisor p	$F(p)$	Odd prime divisor p	$F(p)$
3	2	37	36
5	4	41	20
7	3	43	14
11	10	47	23
13	12	53	52
17	8	59	58
19	18	61	60
23	11	67	66
29	28	71	35
31	5	73	9

Table 1: The 20 smallest odd primes and their multiplicative orders

The above table will prove to be useful in the following subsections, in which we delve deeper into the cyclic patterns in the five remaining cases that represent possible Sierpiński numbers.

3.1 Case 1: $k = 21181$

Consider the expression $k2^n + 1$ for $k = 21181$. For $n = 1$, the expression yields 42363, which is divisible by 3. By Table 1, we know that 3 cycles by 2, so the expression $21181 \cdot 2^n + 1$ will be divisible by 3 for $n = 1, 3, 5$, and so on (i.e. $21181 \cdot 2^n + 1$ is divisible by 3 when $n = 2q + 1$ for some nonnegative integer q). Here, we say the *cyclic pattern* of 3 for 21181 is $n = 2q + 1$. Similarly, the expression is divisible by 5 for $n = 2$ and 5 cycles by 4, as per Table 1. Thus, $21181 \cdot 2^n + 1$ is divisible by 5 when $n = 4q + 2$ for some nonnegative integer q.

Note that in the table below, not all values of n are displayed. This is because many are included in a previously established cyclic pattern. For example, $n = 3$ is not shown since it is included in the cyclic pattern for the optimal divisor 3, which is $n = 2q + 1$ (i.e. $n = 2q + 1 = 3$ when $q = 1$).

n	$D_{n,21181}$	$\sigma_{n,21181}$	$F(\sigma_{n,21181})$	$P_{n,21181}$	$L_{n,21181}$
1	$\{3\}$	3	2	$\{3\}$	2
2	$\{5\}$	5	4	$\{3, 5\}$	4
4	$\{13, 131, 199\}$	13	12	$\{3, 5, 13\}$	12
8	$\{17, 467, 683\}$	17	8	$\{3, 5, 13, 17\}$	24
12	$\{7, 941\}$	7	3	$\{3, 5, 7, 13, 17\}$	24
20	$\{83077\}$	83077	1932	$\{3, 5, 7, 13, 17, 83077\}$	3864
44	$\{89, 353, 2887237, 4107893\}$	89	11	$\{3, 5, 7, 13, 17, 89, 83077\}$	42504
68	$\{342467, 27897143\}$	342467	342466	$\{3, 5, 7, 13, 17, 89, 83077, 342467\}$	7278087432

Table 2: $k = 21181$

Note that starting with n = 20, new values are added to $C_{n,21181}$ every 24 iterations of n. This is because the subset $\{3, 5, 7, 13, 17\}$ cycles by 24, but none of the elements cover values of n where $n = 24q + 20$. This observation will be explored further in the following subsections.

3.2 Case 2: $k = 22699$

Table 3 addresses the case $k = 22699$. Note that, starting with $n = 118$, new values are added to $C_{n,22699}$ every 72 iterations of n.

n	$D_{n,22699}$	$\sigma_{n,22699}$	$F(\sigma_{n,22699})$	$P_{n,22699}$	$L_{n,22699}$
1	$\{3, 37\}$	3	2	$\{3\}$	2
2	$\{7, 17, 109\}$	7	3	$\{3, 7\}$	6
4	$\{5, 19\}$	5	4	$\{3, 5, 7\}$	12
6	$\{11, 13\}$	11	10	$\{3, 5, 7, 11\}$	60
10	$\{17, 23\}$	17	8	$\{3, 5, 7, 11, 17\}$	120
22	$\{19, 47, 1721, 61949\}$	19	18	$\{3, 5, 7, 11, 17, 19\}$	360
30	$\{13,173,63841,169753\}$	13	12	$\{3, 5, 7, 11, 13, 17, 19\}$	360
70	$\{73, 239, 3884047\}$	73	9	$\{3, 5, 7, 11, 13, 17, 19, 73\}$	360
118	$\{53, 547, 2022359\}$	53	52	$\{3, 5, 7, 11, 13, 17, 19, 53, 73\}$	4680
190	$\{84884846681\}$	84884846681	42442423340	$\{3,5,7,11,13,17,19,53,73,84884846681\}$	Too large

Table 3: $k = 22699$

3.3 Case 3: $k = 24737$

Table 4 addresses the case $k = 24737$. Note that, starting with $n = 55$, new values are initially added to $C_{n,24737}$ every 24 iterations of n.

n	$D_{n,24737}$	$\sigma_{n,24737}$	$F(\sigma_{n,24737})$	$P_{n,24737}$	$L_{n,24737}$
1	$\{5\}$	5	4	$\{5\}$	4
2	$\{3\}$	3	2	$\{3, 5\}$	4
3	$\{7, 17\}$	7	3	$\{3, 5, 7\}$	12
7	$\{907\}$	907	906	$\{3, 5, 7, 907\}$	1812
10	$\{13, 17\}$	17	8	$\{3, 5, 7, 17, 907\}$	3624
23	$\{13, 97, 599, 274723\}$	13	12	$\{3, 5, 7, 13, 17, 907\}$	3624
31	$\{503, 12689\}$	503	251	$\{3, 5, 7, 13, 17, 503, 907\}$	909624
55	$\{31, 112967, 4461227\}$	31	5	$\{3, 5, 7, 13, 17, 31, 503, 907\}$	4548120
79	$\{11, 7177613\}$	11	10	$\{3, 5, 7, 11, 13, 17, 31, 503, 907\}$	4548120
103	$\{2118089\}$	2118089	264761	$\{3, 5, 7, 11, 13, 17, 31, 503, 907, 2118089\}$	$\approx 1.20 \cdot 10^{12}$

Table 4: $k = 24737$

3.4 Case 4: $k = 55459$

Table 5 addresses the case $k = 55459$. It may seem that new values are added every 36 iteration of n, but by expanding the table, we see this is not the case. The next two points at which new values are added to $C_{n,55459}$ are $n = 118$ and $n = 130$. It is clear now that there is no clear pattern here. This means that to check for points where new values are added, we must keep incrementing n by 12.

n	$D_{n,55459}$	$\sigma_{n,55459}$	$F(\sigma_{n,55459})$	$P_{n,55459}$	$L_{n,55459}$
1	$\{3\}$	3	2	$\{3\}$	2
2	$\{7, 11, 43, 67\}$	7	3	$\{3, 7\}$	6
4	$\{5, 103\}$	5	4	$\{3, 5, 7\}$	12
6	$\{13\}$	13	12	$\{3, 5, 7, 13\}$	12
10	$\{181, 211, 1487\}$	181	180	$\{3, 5, 7, 13, 181\}$	180
22	$\{11, 709, 1151, 25913\}$	11	10	$\{3, 5, 7, 11, 13, 181\}$	180
34	$\{37\}$	37	36	$\{3, 5, 7, 11, 13, 37, 181\}$	180
46	$\{47, 19477, 208889, 20408747\}$	47	23	$\{3, 5, 7, 11, 13, 37, 47, 181\}$	4140
58	$\{43, 59\}$	43	14	$\{3, 5, 7, 11, 13, 37, 43, 47, 181\}$	28980
94	$\{467\}$	467	466	$\{3, 5, 7, 11, 13, 37, 43, 47, 181, 467\}$	6752340

Table 5: $k = 55459$

3.5 Case 5: $k = 67607$

Table 5 addresses the case $k = 67607$. This fifth and final case is a bit more interesting than the previous four cases. Here, we see that starting with $n = 19$, new values are added to $C_{n,67607}$ every 8 or 16 iterations of n. However, this pattern is broken following $n = 59$, since the next time a new value is added is for $n = 99$. Following this, the next time is $n = 131$. There doesn't seem to be a clear cut pattern here, so the conclusions discussed in the following section may not entirely apply to $k = 67607$.

n	$D_{n,67607}$	$\sigma_{n,67607}$	$F(\sigma_{n,67607})$	$P_{n,67607}$	$L_{n,67607}$
1	$\{5\}$	5	4	$\{5\}$	4
2	$\{3, 109\}$	3	2	$\{3, 5\}$	4
4	$\{31, 73, 239\}$	31	5	$\{3, 5, 31\}$	20
7	$\{13, 17\}$	17	8	$\{3, 5, 17, 31\}$	40
11	$\{19, 29\}$	19	18	$\{3, 5, 17, 19, 31\}$	360
19	$\{13, 41\}$	13	12	$\{3, 5, 13, 17, 19, 31\}$	360
27	$\{198017\}$	198017	99008	$\{3, 5, 13, 17, 19, 31, 198017\}$	4455360
35	$\{11, 22129\}$	11	10	$\{3, 5, 11, 13, 17, 19, 31, 198017\}$	4455360
51	$\{37, 43, 4027\}$	43	14	$\{3, 5, 11, 13, 17, 19, 31, 43, 198017\}$	4455360
59	$\{23, 41\}$	23	11	$\{3, 5, 11, 13, 17, 19, 23, 31, 43, 198017\}$	49008960

Table 6: $k = 67607$

This concludes our recording of data regarding certain aspects and characteristics of the five possible Sierpiński numbers. With these tables, for each $k2^n + 1$, we recorded values of n, the divisor set for the certain n, the actual optimal divisor, the multiplicative order of 2 modulo the optimal divisor, the partial covering set for the certain n, and the least common multiples of $M_{n,k}$ (which was not explicitly recorded, but can be found using $P_{n,k}$ which was recorded).

4 Discussion of Results

The results of Section 3 provide adequate guidance to further the exploration into four of the five cases and understand if they are Sierpiński numbers. For $k = 21181$, it suffices to check only values of n that satisfy $n = 24q + 20$ for some integer q. Thus, it is only necessary to check approximately $\frac{1}{24}$ (about 4%) of all positive numbers n.

Similar approaches can be made for the cases detailed in Subsections 3.2 and 3.3. For $k = 22699$, it suffices to check only values of n that satisfy $n = 72q + 118$ for some integer q. Thus, it is only necessary to check approximately $\frac{1}{72}$ (about 1.44%) of all natural numbers n. For $k = 24737$, it suffices to check only values of n that satisfy $n = 24q + 55$ for some integer q. Thus, it is only necessary to check approximately $\frac{1}{24}$ (about 1.4%) of all natural numbers n.

In the previous three cases, it is clear the search for a prime by sequentially checking values of n could be cut down significantly. However, for the cases detailed in Subsections 3.4 and 3.5, the lack of pattern demonstrates that we can only check values of n in increments of 8 or 12. Specifically, for $k = 55459$ it suffices to check only values of $n = 12q + 22$ for some integer q. For $k = 67607$, we only need to check values of

$n = 8q + 11$ for some integer q. In both these cases, we see that it is only necessary to check approximately $\frac{1}{12}$ (about 8.3%) and $\frac{1}{8}$ (exactly 12.5%) of all natural numbers n, respectively.

Despite this, we must say that it is highly unlikely for any of the remaining numbers to actually be Sierpiński numbers. The values of $L_{n,k}$ increase at a rapid rate that does not occur with any known Sierpiński numbers. Returning to the main focus of this paper, we claim to have accomplished our purpose, which was twofold: first, to establish theorems that might help in better understanding the Sierpiński Number Problem and how to solve it; and second, to formulate a novel searching pattern for possible primes in the expressions of Sierpiński numbers that would improve basic sequential searching.

References

[1] P. Erdős and A.M. Odlyzko, On the density of odd integers of the form $(p-1)2^{-n}$ and related questions, *J. Number Theory* **11** (1979), 257–263.

[2] R.M. Robinson, A report on primes of the form $k2^n + 1$ and on factors of Fermat numbers, *Proc. Amer. Math. Soc.* **9** (1958), 673–681.

[3] PrimeGrid, *SeventeenOrBust*, (last accessed 2020-08-12) `http://primegrid.com/forum_thread.php?id=1647`.

[4] W. Sierpiński, Sur un problème concernant les nombre, *Elemente der Mathematik* **15** (1960), 73–74.

[5] D. Wells, *Prime Numbers: The Most Mysterious Figures in Math*, John Wiley & Sons, Inc., Hoboken, NJ, 2005.