Parabola Volume 60, Issue 1 (2024)

Partial coverings and conditions for Sierpiński candidates

Jack W. Leventhal[1]

1 Introduction

In 1958, Raphael M. Robinson [1] found primes of the form $k \cdot 2^n + 1$ for all odd integers $1 < k < 100$ and $0 < n < 512$, with the exception of $k = 47$. Soon after, Polish mathematician Wacław Sierpiński [2] proved that there exist infinitely many odd integers k such that numbers of the form $k \cdot 2^n + 1$ are never prime for any integer n. The values of k with this property have been termed *Sierpiński numbers*.

With the inception of these numbers, Sierpiński set into motion the search to find the least possible value for k, known as the *Sierpiński Problem*. In 1962, John Selfridge showed that no matter the value of n, the number $78557 \cdot 2^n + 1$ is always composite, hence proving that $k = 78557$ is a Sierpiński number. It is still conjectured today to be the smallest Sierpiński number. Assuming that this is true, 271129 is hypothesized to be the second smallest Sierpiński number, a search known as the *Extended Sierpiński Problem*. According to PrimeGrid [5], a program working to solve the aforementioned Sierpiński problems, there are five candidates left in the Sierpiński problem:

$$21181\,,\ 22699\,,\ 24737\,,\ 55459 \quad \text{and} \quad 67607\,.$$

The Extended Sierpiński Problem has eight possible candidate solutions:

$$91549\,,\ 131179\,,\ 163187\,,\ 200749\,,\ 209611\,,\ 227723\,,\ 229673 \quad \text{and} \quad 238411\,.$$

Any prime value of $k \cdot 2^n + 1$, for any k, would eliminate k as a candidate.

This paper introduces a new methodology to find necessary conditions for a prime counterexample, alleviating the search for them, and therefore eases the process of eliminating candidates in the Sierpiński problems.

2 Definitions and procedure

The process for generating restrictions for Sierpiński candidates allows us to greatly reduce the work necessary to solve the Sierpiński problems. Wolfram Alpha [4] will prove useful for computations. First and foremost, we introduce the notions of residue classes and covering systems and sets — covering systems having first been introduced by Paul Erdős [3] in 1950. Calculations for these concepts will be provided following their introduction.

[1]Jack W. Leventhal is a senior at Wilton High School, CT, USA.

Definition 1. A *residue class* $a \pmod{m}$ is the set of integers with the same remainder as a when divided by the modulus m.

For instance, all even numbers are members of the residue class $0 \pmod{2}$, as they all leave a remainder of zero when divided by the modulus, here 2. Residue classes like this will act as the building blocks for covering systems.

Definition 2. A *partial covering system* is a set of residue classes

$$\{\, c_1 \pmod{m_1}\,,\ \ldots\,,\ c_j \pmod{m_j} \,\}\,.$$

Definition 3. A *covering system* is a partial covering system whose union of residue classes contains every integer.

Covering systems are closely tied to covering sets, both of which will be employed to further narrow the search for counterexamples and remove Sierpiński candidates from their respective problems.

Definition 4. Given Sierpiński candidate k, define the covering set S_k to be the smallest set of prime numbers such that, for each non-negative integer n, $k \cdot 2^n + 1$ is divisible by at least one prime in S_k.

For the remaining Sierpiński candidates, partial covering systems (and their accompanying covering sets) will be utilized.

Definition 5. For Sierpiński candidate k, let P_k be the smallest set of prime numbers such that, for all non-negative integers $r \leq n$, the number $k \cdot 2^r + 1$ is divisible by at least one prime in P_k.

Now, we will construct certain partial covering systems and sets. First, choose an arbitrary prime p and find the smallest positive integer m such that $2^m \equiv 1 \pmod{p}$; it is not difficult to show that such an integer will always exist.

Next, for a selected Sierpiński candidate k and the chosen prime p, we can calculate the portion of the partial covering system yielded by p as follows. Solving the congruence $k \cdot 2^n + 1 \equiv 0 \pmod{p}$ for n yields a congruence of the form $n \equiv x_p \pmod{p}$, with x_p being the principal value which satisfies the congruence. These solutions allow one to discover which values of n are divisible by p due to the fact that, if $k \cdot 2^{x_p} + 1 \equiv 0 \pmod{p}$, then the following holds true:

$$k \cdot 2^{x_p + mx} + 1 \equiv k \cdot 2^{x_p}(2^m)^x + 1 \equiv k \cdot 2^{x_p} 1^x + 1 \equiv k \cdot 2^{x_p} + 1 \equiv 0 \pmod{p}\,.$$

In other words, if $n \equiv x_p \pmod{p}$ is satisfied, then adding multiples of p, or mp, to the exponent will still cause n to be divisible by p.

This process for constructing a covering system and set can be exemplified by the Sierpiński number 78557. While it has a covering system rather than a partial covering system, the same process is applicable and begins as follows.

Starting with the smallest odd prime 3, we find the smallest positive integer m such that $2^m \equiv 1 \pmod{3}$. This happens to be 2. Thus, the modulus for the residue class produced by 3 is $m = 2$. Next, solving the congruence $78557 \cdot 2^n + 1 \equiv 0 \pmod 3$ for n, one obtains $n \equiv 0 \pmod 2$. Hence, we know if $n \equiv 0 \pmod 2$ - that is, if n is even - then $78557 \cdot 2^n + 1$ is divisible by 3. Furthermore, if $78557 \cdot 2^n + 1$ is prime, then n must be odd.

Performing this procedure for the next prime, namely 5, the residue class $1 \pmod 4$ is acquired. Thus, if $n \equiv 1 \pmod 4$, then $78557 \cdot 2^n + 1$ is divisible by 5, and our prime counterexample must result from a value of n from the residue class $3 \pmod 4$. Repeating this procedure for the primes 7, 11 and 13, the resulting residue classes are $1 \pmod 3$, $6 \pmod{10}$ and $11 \pmod{12}$, respectively. However, the residue class produced by the prime 11, $6 \pmod{10}$, is unnecessary as we already showed any even value of n will cause $78557 \cdot 2^n + 1$ to be divisible by 3. So, the residue classes derived from primes 7 and 13 may be incorporated in the covering system, while 11 is not necessary to include.

Continuing with the next few primes, most of the residue classes computed are either rendered irrelevant by prior results, or do not significantly restrict the form of n. However, for the primes 19, 37 and 73, the residue classes calculated - $15 \pmod{18}$, $27 \pmod{36}$ and $3 \pmod 9$, respectively - considerably restrict n. In fact, with all the residue classes, all possible values for n are eliminated. This is how, in 1962, Selfridge proved that 78557 is a Sierpiński number.

For the partial coverings systems that we will generate, the aforesaid congruence $k \cdot 2^n + 1 \equiv 0 \pmod p$ may be solved for some Sierpiński candidate k for primes less than 100, excluding 2, before constructing substantial partial covering systems and sets.

Then, with [4] or [6], one can compute the prime factorization of $k \cdot 2^n + 1$ for the smallest value of n excluded by the partial covering system. The procedure can then be completed for the prime factors supplied and repeated. Thereafter, the primes and congruences acquired may be added to the partial covering set and system respectively if the solutions significantly change the form of n. Otherwise, they may be included in a list of restrictions imposed on n.

3 Results for the Sierpiński problem

For the following Sierpiński candidates, the partial modular covering set and system will be presented below, followed by the form that n must take for $k \cdot 2^n + 1$ to be prime and, finally, tables providing further restrictions on n.

3.1 Candidate 1: 21181

For the first Sierpiński candidate, 21181, begin by testing $p = 3$, which yields $m = 2$, and the congruence $n \equiv 1 \pmod 2$. Thus far, n is restricted to the form $n = 2j$ for some non-negative integer j. Continuing this process with the next few primes, one obtains the following:

p	$n \equiv \cdots$
5	$2 \pmod 4$
7	$0 \pmod 3$
13	$4 \pmod{12}$
17	$0 \pmod 8$

These congruences restrict n to the form $n = 24j + 20$ for non-negative integers j, due to the fact that each congruence comprising the partial covering system, on its own or when paired with another congruence, changes the form of n. Other congruences do not change the form of n, but nonetheless inflict modular conditions on n as well as the value of j. They are as follows:

p	$n \equiv \cdots$	$j \equiv \cdots$
11	$6 \pmod{10}$	$4 \pmod 5$
23	$10 \pmod{11}$	$6 \pmod{11}$
47	$19 \pmod{23}$	$22 \pmod{23}$
71	$15 \pmod{35}$	$10 \pmod{35}$
89	$0 \pmod{11}$	$1 \pmod{11}$

p	$n \equiv \cdots$	$j \equiv \cdots$
157	$40 \pmod{52}$	$3 \pmod{13}$
163	$122 \pmod{162}$	$11 \pmod{27}$
223	$35 \pmod{37}$	$33 \pmod{37}$
683	$8 \pmod{22}$	$5 \pmod{11}$
1013	$56 \pmod{92}$	$13 \pmod{23}$

For each of the remaining candidates, partial covering sets and systems and list of conditions can be assembled in a similar fashion.

3.2 Candidate 2: 22699

p	$n \equiv \cdots$
3	$1 \pmod 2$
5	$0 \pmod 4$
7	$2 \pmod 3$

13	$6 \pmod{12}$
17	$2 \pmod 8$
19	$4 \pmod{18}$
73	$7 \pmod 9$

These congruences restrict n to the form $n = 72j + 46$ for non-negative integers j. Other congruences include:

p	$n \equiv \cdots$	$j \equiv \cdots$
11	$6 \pmod{10}$	$0 \pmod 5$
23	$10 \pmod{11}$	$5 \pmod{11}$
47	$22 \pmod{23}$	$15 \pmod{23}$

53	$14 \pmod{52}$	$1 \pmod{13}$
59	$54 \pmod{58}$	$13 \pmod{29}$
173	$30 \pmod{172}$	$38 \pmod{43}$
233	$17 \pmod{29}$	$0 \pmod{29}$

3.3 Candidate 3: 24737

p	$n \equiv \cdots$
3	$0 \pmod 2$
5	$1 \pmod 4$
7	$0 \pmod 3$
13	$11 \pmod{12}$
17	$3 \pmod 8$

These congruences restrict n to the form $n = 24j + 7$ for non-negative integers j. Other congruences include:

p	$n \equiv \cdots$	$j \equiv \cdots$
11	$9 \pmod{10}$	$3 \pmod 5$
31	$0 \pmod 5$	$2 \pmod 5$
173	$171 \pmod{172}$	$14 \pmod{43}$

3.4 Candidate 4: 55459

p	$n \equiv \cdots$
3	$1 \pmod 2$
5	$0 \pmod 4$
7	$2 \pmod 3$
13	$6 \pmod{12}$

These congruences restrict n to the form $n = 12j + 10$ for non-negative integers j. Other congruences include:

p	$n \equiv \cdots$	$j \equiv \cdots$
11	$2 \pmod{10}$	$1 \pmod 5$
37	$34 \pmod{36}$	$2 \pmod 3$
43	$2 \pmod{14}$	$4 \pmod 7$
47	$0 \pmod{23}$	$3 \pmod{23}$
59	$0 \pmod{58}$	$4 \pmod{29}$

83	$24 \pmod{82}$	$8 \pmod{41}$
103	$4 \pmod{51}$	$8 \pmod{17}$
181	$10 \pmod{180}$	$0 \pmod{15}$
613	$154 \pmod{612}$	$12 \pmod{51}$
709	$22 \pmod{708}$	$1 \pmod{59}$
733	$190 \pmod{244}$	$15 \pmod{61}$

3.5 Candidate 5: 67607

The final Sierpiński candidate of the Sierpiński Problem does not have one singular form that n must take for $67607 \cdot 2^n + 1$ to be prime, but rather four as a result of the breadth and structure of the partial covering system. The overarching partial covering set and system will be initially introduced and then listed will be the modular restrictions for each form of n.

p	$n \equiv \cdots$
3	$0 \pmod 2$
5	$1 \pmod 4$
11	$5 \pmod{10}$
13	$7 \pmod{12}$
17	$7 \pmod 8$

19	$11 \pmod{18}$
31	$3 \pmod 5$
37	$15 \pmod{36}$
41	$19 \pmod{20}$
73	$3 \pmod 9$
331	$17 \pmod{30}$

These congruences restrict n to one of the forms $360j_1 + 27$, $360j_2 + 131$, $360j_3 + 171$ and $360j_4 + 251$ for non-negative integers j_1, j_2, j_3 and j_4. Concerning the table below, N/A denotes that, for a particular form of n, no value inputted for the form one is considering will fulfil the congruence introduced by n: the restriction does not apply.

p	$n \equiv \cdots$	$j_1 \equiv \cdots$	$j_2 \equiv \cdots$	$j_3 \equiv \cdots$	$j_4 \equiv \cdots$
23	$4 \pmod{11}$	$4 \pmod{11}$	$2 \pmod{11}$	$8 \pmod{11}$	$9 \pmod{11}$
29	$11 \pmod{28}$	$4 \pmod 7$	$2 \pmod 7$	$5 \pmod 7$	$4 \pmod 7$
43	$9 \pmod{14}$	$1 \pmod 7$	$6 \pmod 7$	$2 \pmod 7$	$1 \pmod 7$
103	$45 \pmod{51}$	$6 \pmod{17}$	N/A	$9 \pmod{17}$	N/A
107	$77 \pmod{106}$	$34 \pmod{53}$	$29 \pmod{53}$	$23 \pmod{53}$	$11 \pmod{53}$
229	$63 \pmod{76}$	$2 \pmod{19}$	$11 \pmod{19}$	$13 \pmod{19}$	$17 \pmod{19}$
283	$33 \pmod{94}$	$29 \pmod{47}$	$12 \pmod{47}$	$38 \pmod{47}$	$43 \pmod{47}$
293	$179 \pmod{292}$	$28 \pmod{73}$	$5 \pmod{73}$	$13 \pmod{73}$	$29 \pmod{73}$
461	$407 \pmod{460}$	$10 \pmod{23}$	N/A	N/A	N/A
491	$87 \pmod{490}$	$41 \pmod{49}$	N/A	N/A	N/A
751	$56 \pmod{375}$	N/A	$5 \pmod{25}$	N/A	$13 \pmod{25}$
3041	$667 \pmod{1520}$	$6 \pmod{38}$	N/A	N/A	N/A

4 Results for the Extended Sierpiński Problem

Quite similar in objective to the Sierpiński Problem, the Extended Sierpiński Problem has eight candidates, for which the same process may be applied.

4.1 Candidate 1: 91549

p	$n \equiv \cdots$
3	$1 \pmod 2$
5	$0 \pmod 4$
7	$1 \pmod 3$
13	$2 \pmod{12}$
17	$2 \pmod 8$

These congruences restrict n to the form $n = 24j + 6$ for non-negative integers j. Other congruences include:

p	$n \equiv \cdots$	$j \equiv \cdots$
11	$8 \pmod{10}$	$3 \pmod 5$
29	$26 \pmod{28}$	$2 \pmod 7$
43	$6 \pmod{14}$	$0 \pmod 7$
47	$11 \pmod{23}$	$5 \pmod{23}$
59	$20 \pmod{58}$	$3 \pmod{29}$
67	$48 \pmod{67}$	$10 \pmod{11}$
89	$6 \pmod{11}$	$0 \pmod{11}$
149	$54 \pmod{148}$	$2 \pmod{37}$
3889	$174 \pmod{648}$	$7 \pmod{27}$

4.2 Candidate 2: 131179

p	$n \equiv \cdots$
3	$1 \pmod 2$
5	$0 \pmod 4$
7	$0 \pmod 3$
13	$10 \pmod{12}$
19	$14 \pmod{18}$
73	$8 \pmod 9$

These congruences restrict n to the form $n = 36j + 2$ for non-negative integers j. Other congruences include:

p	$n \equiv \cdots$	$j \equiv \cdots$
23	$4 \pmod{11}$	$8 \pmod{11}$
71	$12 \pmod{35}$	$10 \pmod{35}$
101	$74 \pmod{100}$	$2 \pmod{25}$
811	$2 \pmod{270}$	$0 \pmod{15}$

4.3 Candidate 3: 163187

p	$n \equiv \cdots$
3	$0 \pmod{2}$
5	$1 \pmod{4}$
7	$1 \pmod{3}$
13	$11 \pmod{12}$
241	$3 \pmod{24}$

These congruences restrict n to the form $n = 24j + 15$ for non-negative integers j. Other congruences include:

p	$n \equiv \cdots$	$j \equiv \cdots$
83	$61 \pmod{82}$	$19 \pmod{41}$
89	$4 \pmod{11}$	$0 \pmod{11}$
107	$87 \pmod{106}$	$3 \pmod{53}$
113	$7 \pmod{28}$	$2 \pmod{7}$
127	$4 \pmod{7}$	$1 \pmod{7}$

139	$69 \pmod{138}$	$8 \pmod{23}$
223	$10 \pmod{37}$	$26 \pmod{37}$
313	$147 \pmod{156}$	$12 \pmod{13}$
433	$39 \pmod{72}$	$1 \pmod{3}$
521	$135 \pmod{260}$	$5 \pmod{65}$
631	$18 \pmod{45}$	$2 \pmod{15}$

4.4 Candidate 4: 200749

p	$n \equiv \cdots$
3	$1 \pmod{2}$
5	$0 \pmod{4}$
7	$1 \pmod{3}$
13	$2 \pmod{12}$
17	$6 \pmod{8}$

These congruences restrict n to the form $n = 24j + 18$ for non-negative integers j. Other congruences include:

p	$n \equiv \cdots$	$j \equiv \cdots$
11	$0 \pmod{10}$	$3 \pmod{5}$
23	$5 \pmod{11}$	$10 \pmod{11}$
59	$38 \pmod{58}$	$25 \pmod{29}$
73	$0 \pmod{9}$	$0 \pmod{3}$
83	$72 \pmod{82}$	$33 \pmod{41}$
139	$90 \pmod{138}$	$3 \pmod{23}$

4.5 Candidate 5: 209611

p	$n \equiv \cdots$
3	$1 \pmod{2}$
5	$2 \pmod{4}$
7	$1 \pmod{3}$
13	$0 \pmod{12}$
17	$4 \pmod{8}$

These congruences restrict n to the form $n = 24j + 8$ for non-negative integers j. Other congruences include:

p	$n \equiv \cdots$	$j \equiv \cdots$
11	$6 \pmod{10}$	$2 \pmod{5}$
19	$14 \pmod{18}$	$1 \pmod{3}$
29	$0 \pmod{28}$	$2 \pmod{7}$
47	$8 \pmod{23}$	$0 \pmod{23}$

59	$54 \pmod{58}$	$14 \pmod{29}$
79	$26 \pmod{39}$	$4 \pmod{13}$
151	$8 \pmod{15}$	$0 \pmod{5}$
307	$80 \pmod{102}$	$3 \pmod{17}$
593	$44 \pmod{148}$	$20 \pmod{37}$

4.6 Candidate 6: 227723

p	$n \equiv \cdots$
3	$0 \pmod{2}$
5	$3 \pmod{4}$
7	$0 \pmod{3}$
13	$5 \pmod{12}$
17	$1 \pmod{8}$

These congruences restrict n to the form $n = 24j + 13$ for non-negative integers j. Other congruences include:

p	$n \equiv \cdots$	$j \equiv \cdots$
11	$5 \pmod{10}$	$3 \pmod{5}$
53	$17 \pmod{52}$	$11 \pmod{13}$
73	$1 \pmod{9}$	$1 \pmod{3}$
107	$55 \pmod{106}$	$15 \pmod{53}$
139	$37 \pmod{138}$	$1 \pmod{23}$
409	$121 \pmod{204}$	$13 \pmod{17}$

4.7 Candidate 7: 229673

p	$n \equiv \cdots$
3	$0 \pmod 2$
5	$3 \pmod 4$
7	$1 \pmod 3$
13	$5 \pmod{12}$
19	$9 \pmod{18}$
37	$21 \pmod{36}$

These congruences restrict n to the form $n = 36j+33$ for non-negative integers j. Other congruences include:

p	$n \equiv \cdots$	$j \equiv \cdots$
11	$3 \pmod{10}$	$0 \pmod 5$
41	$5 \pmod{20}$	$2 \pmod 5$
47	$19 \pmod{23}$	$6 \pmod{23}$
59	$39 \pmod{58}$	$5 \pmod{29}$
67	$27 \pmod{66}$	$9 \pmod{11}$
71	$17 \pmod{35}$	$13 \pmod{35}$
83	$49 \pmod{82}$	$5 \pmod{41}$
139	$39 \pmod{138}$	$4 \pmod{23}$
163	$141 \pmod{162}$	$3 \pmod 9$
199	$42 \pmod{99}$	$3 \pmod{11}$
571	$93 \pmod{114}$	$8 \pmod{19}$

4.8 Candidate 8: 238411

p	$n \equiv \cdots$
3	$1 \pmod 2$
5	$2 \pmod 4$
7	$2 \pmod 3$
13	$4 \pmod{12}$

These congruences restrict n to the form $n = 12j$ for non-negative integers j. Other congruences include:

p	$n \equiv \cdots$	$j \equiv \cdots$
11	$2 \pmod{10}$	$1 \pmod 5$
19	$0 \pmod{18}$	$0 \pmod 3$
53	$16 \pmod{52}$	$10 \pmod{13}$
83	$6 \pmod{82}$	$21 \pmod{41}$
103	$9 \pmod{51}$	$5 \pmod{17}$
131	$116 \pmod{130}$	$53 \pmod{65}$
197	$184 \pmod{196}$	$48 \pmod{49}$
283	$16 \pmod{94}$	$17 \pmod{47}$
353	$16 \pmod{88}$	$16 \pmod{22}$
373	$180 \pmod{372}$	$15 \pmod{31}$
409	$180 \pmod{204}$	$15 \pmod{17}$
421	$216 \pmod{420}$	$18 \pmod{35}$
1201	$264 \pmod{300}$	$22 \pmod{25}$

Thus, the enumeration of partial covering sets and systems and restrictions for each Sierpiński candidate in the Sierpiński and extended Sierpiński problem is complete.

5 Overview of results

The prior sections provide further insight for those engaged with the Sierpiński Problem and the Extended Sierpiński Problem, heavily restricting the form of n. The table below lists the form(s) that n must take to obtain a counterexample for a Sierpiński candidate k, the first five being part of the Sierpiński Problem and the next eight being part of the Extended Sierpiński Problem. For additional restrictions on n for each Sierpiński candidate, please see the subsection devoted to it, either in Section 3 for the Sierpiński Problem or in Section 4 for the Extended Sierpiński Problem.

k	$n = \cdots$
21181	$24j + 20$
22699	$72j + 46$
24737	$24j + 7$
55459	$12j + 10$
67607	$360j + 27\,,\ 360j + 131\,,\ 360j + 171\,,\ 360j + 251$
91549	$24j + 6$
131179	$36j + 2$
163187	$24j + 15$
200749	$24j + 18$
209611	$24j + 8$
227723	$24j + 13$
229673	$36j + 33$
238411	$12j$

With these results, prime computing programs may now more efficiently work to resolve the Sierpiński problems. For each Sierpiński candidate, the number of primes which must be checked can be cut down quite significantly, fulfilling the initially stated goal of this paper.

6 Acknowledgements

The author extends his gratitude to those at Parabola whose suggestions improved the quality and overall presentation of this paper. The author would also like to thank all those involved with the development of prime computing programs and the continued efforts of many to resolve ongoing projects concerning primes.

References

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

[2] W. Sierpiński, Sur un problème concernant les nombres $k \cdot 2^n + 1$, *Elem. Math.* **15** (1960), 73–74.

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

[4] WolframAlpha, https://www.wolframalpha.com/, last accessed on 2024-01-08.

[5] PrimeGrid, http://www.primegrid.com/forum_thread.php?id=1647, last accessed on 2024-01-08.

[6] dCode, Prime Factors Decomposition on dCode.fr, https://www.dcode.fr/prime-factors-decomposition, last accessed on 2024-01-08.