2008

On powers associated with Sierpiński numbers, Riesel numbers and Polignac's conjecture

Mark Kozek

Michael Filaseta

Carrie Finch

Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 128 (2008) 1916–1940
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

On powers associated with Sierpiński numbers, Riesel numbers and Polignac's conjecture ☆

Michael Filaseta [a,*], Carrie Finch [b], Mark Kozek [c]

[a] *Department of Mathematics, University of South Carolina, Columbia, SC 29208, USA*
[b] *Mathematics Department, Washington and Lee University, Lexington, VA 24450, USA*
[c] *Department of Mathematics, Whittier College, Whittier, CA 90608, USA*

Received 2 January 2007; revised 25 February 2008

Available online 24 April 2008

Communicated by C. Pomerance

Abstract

We address conjectures of P. Erdős and conjectures of Y.-G. Chen concerning the numbers in the title. We obtain a variety of related results, including a new smallest positive integer that is simultaneously a Sierpiński number and a Riesel number and a proof that for every positive integer r, there is an integer k such that the numbers $k, k^2, k^3, \ldots, k^r$ are simultaneously Sierpiński numbers.

Keywords: Covering system; Polignac's conjecture; Riesel number; Sierpiński number

1. Introduction

A Sierpiński number is a positive odd integer k with the property that $k \cdot 2^n + 1$ is composite for all positive integers n. A Riesel number is a positive odd integer k with the property that $k \cdot 2^n - 1$ is composite for all positive integers n. In 1849, A. de Polignac [6] conjectured that every positive odd integer k can be written as a sum of a prime and a power of two. It is well known that Polignac's conjecture is not true. What has become of interest here are positive odd integers k

☆ The authors express their appreciation to the National Science Foundation and the National Security Agency for support during the research for this paper.
* Corresponding author.
E-mail addresses: filaseta@math.sc.edu (M. Filaseta), finchc@wlu.edu (C. Finch), mkozek@whittier.edu (M. Kozek).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2008.02.004

for which $|k - 2^n|$ is composite for all positive integers n. In this section, we briefly discuss our main results concerning these various numbers k, leaving motivational and background material for the next section.

The existence of k as in each of the three concepts above has historically been associated with covering systems. A covering system or covering, for short, is a finite system of congruences $x \equiv a_j \pmod{m_j}$, $1 \leqslant j \leqslant r$, such that every integer satisfies at least one of the congruences. P. Erdős [9, Section F13] apparently believed that Sierpiński numbers and covering systems are so strongly connected that he conjectured that every Sierpiński number must be obtainable from an argument involving a covering. This is formulated more precisely as Conjecture 1 in the next section. The formulation of what is meant by being obtainable by a covering argument, though, is not so much of interest to us here as an example of a Sierpiński number given by A. Izotov [10], which suggests that this conjecture of Erdős is incorrect. One goal of this paper is to elaborate on these ideas and to produce similar examples of Sierpiński numbers, Riesel numbers and positive odd integers k for which $|k - 2^n|$ is composite for all positive integers n. These examples fall into infinite classes of k that are likely not obtainable by covering arguments. We make some attempt to determine small examples of such k. However, we note that a "proof" that any of our examples cannot arise from a covering argument seems out of reach. On the other hand, our explanations for why they likely do not arise from a covering argument will hopefully be convincing.

The examples discussed above arise from considering k that are squares and fourth powers. This naturally leads to recent investigations of Y.-G. Chen [3]. One of our main results in this paper resolves a conjecture of Chen that for each positive integer r, there are infinitely many Sierpiński numbers that are rth powers. His conjecture was actually the stronger assertion that such rth powers k are not only such that $k \cdot 2^n + 1$ is composite for each positive integer n but further such that $k \cdot 2^n + 1$ has at least two *distinct* prime divisors for each positive integer n. We establish the following even stronger assertion.

Theorem 1. *For every positive integer R, there exist infinitely many positive odd numbers k such that each of the numbers*

$$k2^n + 1,\ k^2 2^n + 1,\ k^3 2^n + 1,\ \ldots,\ k^R 2^n + 1$$

has at least two distinct prime factors for each positive integer n.

The analogous conjectures with powers associated with Riesel numbers and Polignac's conjecture remain open. We obtain some partial results in this direction, and in particular we resolve these analogous conjectures for fourth powers and sixth powers, the two smallest powers that were not resolved by the work of Chen.

We close this section with some open problems. We begin with one suggested by Theorem 1. We do not know whether there is a k such that the infinite list $k, k^2, k^3, \ldots$ are all simultaneously Sierpiński numbers. Note that this is the same as asking whether there is a positive odd integer k such that all of the numbers of the form $2^i k^j + 1$, where i and j are positive integers, are composite.

Let $f(x)$ be an arbitrary nonconstant polynomial in $\mathbb{Z}[x]$. Must there be infinitely many integers k such that $f(k) \cdot 2^n + 1$ is composite for all positive integers n? Suppose $g(x)$ is another nonconstant polynomial in $\mathbb{Z}[x]$. Are there infinitely many integers k such that $f(k) \cdot 2^n + 1$ and $g(k) \cdot 2^n + 1$ are both composite for all positive integers n?

In connection to the conjecture of Erdős alluded to earlier, the following struck us as particularly interesting. Is it possible to find a method for determining whether a given k has the property that the smallest prime divisor of $k \cdot 2^n + 1$ is bounded? Can one even prove that the smallest prime divisor of $5 \cdot 2^n + 1$ is not bounded as n tends to infinity? One can answer this question affirmatively if 5 is replaced by a smaller positive integer. For example, given any x, there is a positive integer n such that $2^n - 1$ is divisible by every odd prime $\leqslant x$. It follows that for this n, the smallest prime factor of $3 \cdot 2^n + 1$ is $> x$. Thus, the smallest prime divisor of $3 \cdot 2^n + 1$ cannot be bounded as n tends to infinity. A similar question along these lines is the following: can one prove that the smallest prime divisor of $11 \cdot 2^n - 1$ is not bounded as n tends to infinity?

2. Background

W. Sierpiński [12] observed the following implications:

$$\begin{aligned}
n \equiv 1 \pmod 2, \quad k \equiv 1 \pmod 3 &\implies k \cdot 2^n + 1 \equiv 0 \pmod 3,\\
n \equiv 2 \pmod 4, \quad k \equiv 1 \pmod 5 &\implies k \cdot 2^n + 1 \equiv 0 \pmod 5,\\
n \equiv 4 \pmod 8, \quad k \equiv 1 \pmod{17} &\implies k \cdot 2^n + 1 \equiv 0 \pmod{17},\\
n \equiv 8 \pmod{16}, \quad k \equiv 1 \pmod{257} &\implies k \cdot 2^n + 1 \equiv 0 \pmod{257},\\
n \equiv 16 \pmod{32}, \quad k \equiv 1 \pmod{65537} &\implies k \cdot 2^n + 1 \equiv 0 \pmod{65537},\\
n \equiv 32 \pmod{64}, \quad k \equiv 1 \pmod{641} &\implies k \cdot 2^n + 1 \equiv 0 \pmod{641},\\
n \equiv 0 \pmod{64}, \quad k \equiv -1 \pmod{6700417} &\implies k \cdot 2^n + 1 \equiv 0 \pmod{6700417}.
\end{aligned}$$

The moduli appearing in the congruences involving k are 7 primes, the first (perhaps only) 5 Fermat primes $F_n = 2^{2^n} + 1$ for $0 \leqslant n \leqslant 4$ and the two prime divisors of F_5. The congruences for n on the left form a covering of the integers, and hence it follows that any k satisfying the congruences on k above has the property that, for any positive integer n, the number $k \cdot 2^n + 1$ is divisible by one of these 7 primes. We add the condition $k \equiv 1 \pmod 2$ to ensure that k is odd. Then the Chinese Remainder Theorem implies that there are infinitely many Sierpiński numbers given by

$$k \equiv 155113807464625933 81 \pmod{2 \cdot 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 \cdot 641 \cdot 6700417}.$$

This congruence establishes that a positive proportion of the positive integers are in fact Sierpiński numbers. For convenience in this paper, we will refer to the construction of Sierpiński numbers as above as Sierpiński's construction. We also note that this construction of Sierpiński relies on the fact that F_5 is composite.

In 1962, John Selfridge (unpublished) found what is believed to be the smallest Sierpiński number, namely $k = 78557$. His argument is based on the following implications:

$$\begin{aligned}
n \equiv 0 \pmod 2, \quad k \equiv 2 \pmod 3 &\implies k \cdot 2^n + 1 \equiv 0 \pmod 3,\\
n \equiv 1 \pmod 4, \quad k \equiv 2 \pmod 5 &\implies k \cdot 2^n + 1 \equiv 0 \pmod 5,\\
n \equiv 3 \pmod 9, \quad k \equiv 9 \pmod{73} &\implies k \cdot 2^n + 1 \equiv 0 \pmod{73},
\end{aligned}$$

$$\begin{aligned} n \equiv 15 \pmod{18}, \quad k \equiv 11 \pmod{19} &\implies k \cdot 2^n + 1 \equiv 0 \pmod{19}, \\ n \equiv 27 \pmod{36}, \quad k \equiv 6 \pmod{37} &\implies k \cdot 2^n + 1 \equiv 0 \pmod{37}, \\ n \equiv 1 \pmod{3}, \quad k \equiv 3 \pmod{7} &\implies k \cdot 2^n + 1 \equiv 0 \pmod{7}, \\ n \equiv 11 \pmod{12}, \quad k \equiv 11 \pmod{13} &\implies k \cdot 2^n + 1 \equiv 0 \pmod{13}. \end{aligned}$$

There have been attempts to prove that 78557 is the smallest Sierpiński number. In this regards, the web page http://www.seventeenorbust.com contains the current up-to-date information. The research for this page, under the name of Seventeen or Bust, was started by L. Helm and D. Norris in March of 2002 when there were 17 numbers < 78557 which were not yet eliminated from being Sierpiński numbers. The idea is to establish that each $k < 78557$ is not a Sierpiński number by finding a prime of the form $k \cdot 2^n + 1$. As of this writing, there remain 6 values of $k < 78557$ which are unresolved by the Seventeen or Bust project, namely

$$10223,\ 21181,\ 22699,\ 24737,\ 55459,\ 67607.$$

There are justifications for the belief that each of these 6 numbers is not a Sierpiński number. Recall that the Sierpiński numbers k found by Sierpiński have the property that for each positive integer n, the number $k \cdot 2^n + 1$ is divisible by one of 7 primes. Similarly, the Sierpiński numbers determined by the argument of Selfridge have this same property (though the primes are different). If one believes that Sierpiński numbers are related to coverings as the above examples suggest, then it would follow that the following conjecture of P. Erdős [9] (Section F13) holds.

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

We define

$$\operatorname{ord}_p(2) = m \text{ if } m \in \mathbb{Z}^+ \text{ is minimal such that } 2^m \equiv 1 \pmod{p}.$$

In other words, $\operatorname{ord}_p(2) = m$ means that m is the order of 2 modulo p. It is of some interest to note also that the congruences $n \equiv a \pmod{m}$, $k \equiv b \pmod{p}$ appearing to the left of each implication above is such that $\operatorname{ord}_p(2) = m$. This further suggests that a Sierpiński number k should have the property that for each positive integer n, the number $k \cdot 2^n + 1$ is divisible by a prime p for which $\operatorname{ord}_p(2) = m$ is not too large. What is more important here is that m is a modulus of the related covering which in turn would suggest the prime divisors of m should not be large. Computations can be used to show that the 6 numbers k listed above are likely not Sierpiński numbers since each has the property that the prime divisors of $k \cdot 2^n + 1$ do not seem to belong to a finite list and do not seem to have the property that 2 has a small order or an order consisting of small prime divisors modulo these primes. For example, it is not difficult to check that $10223 \cdot 2^n + 1$ is divisible by one of the primes 3, 5, 7 and 13 unless $n \equiv 5 \pmod{12}$. Although, one can (is bound) to find patterns among these n as well, like 11 divides every fifth one, a quick look at the prime divisors for $n \equiv 5 \pmod{12}$ reveals little to suggest 10223 is the result of a covering. For example, we find the following early examples of the smallest prime p dividing $10223 \cdot 2^n + 1$ and the orders of 2 modulo p among the $n \equiv 5 \pmod{12}$.

Table 1

n	Smallest prime	Factorization of order of 2
77	619033	$2 \cdot 25793$
101	45677096693	$2^2 \cdot 31 \cdot 368363683$
137	1904660910466121	$2^2 \cdot 5 \cdot 1559 \cdot 4733 \cdot 6453199$

We keep such tables in this paper short; they are intended to indicate some of the behavior we observed for the k tested and, in general, a similar behavior was observed for many other choices of n but with the smallest prime not quite as large as those listed. One could consider other primes dividing $10223 \cdot 2^n + 1$ besides the smallest prime with the hope that their orders would be smaller or involve smaller primes, but this also does not seem to help.

This discussion has seemingly caused us to go off course of the focus of this paper which is to consider Sierpiński and related numbers which are rth powers for some $r > 1$. But in fact, the above leads exactly to this topic. A nice observation of A. Izotov [10] is that the given motivation for 10223 not being a Sierpiński number, and similarly for the other numbers below 78557 which have not yet been eliminated as Sierpiński numbers, is somewhat in error. More precisely, it is highly likely that Erdős's Conjecture 2 is wrong.

To understand Izotov's idea, we return to Sierpiński's construction and simply remove the congruence $n \equiv 2 \pmod 4$ and the corresponding condition $k \equiv 1 \pmod 5$. So we have a simplified system of congruences on n which no longer covers the integers. Now, suppose we can find an odd number k that satisfies only the remaining conditions on k in Sierpiński's construction and also that $k = \ell^4$ for some integer $\ell > 1$. Observe that if $n = 4u + 2$ for some nonnegative integer u, then

$$k \cdot 2^n + 1 = 4\big(\ell \cdot 2^u\big)^4 + 1 = \big(\ell^2 \cdot 2^{2u+1} + \ell \cdot 2^{u+1} + 1\big)\big(\ell^2 \cdot 2^{2u+1} - \ell \cdot 2^{u+1} + 1\big). \quad (1)$$

Thus, whenever $n \equiv 2 \pmod 4$, we obtain that $k \cdot 2^n + 1$ is composite and seemingly for reasons not associated with a covering but rather due to the fact that $4x^4 + 1$ has a nontrivial factorization in $\mathbb{Z}[x]$. This is the idea. Some modifications are needed for if $\ell \not\equiv 0 \pmod 5$ in this construction, then $k = \ell^4 \equiv 1 \pmod 5$ and $k \cdot 2^{4u+2} + 1$ will have 5 as a factor. In other words, we will be in the situation of Sierpiński's original construction. It should be noted here that each of the congruences $k \equiv b \pmod p$ in Sierpiński's construction satisfies $k \equiv \ell^4 \pmod p$ for some integer ℓ. In the case that $b = 1$, one can take $\ell = 1$; in the last congruence where $b = -1$ and $p = 6700417$, one can take $\ell = 2^8$ since 6700417 is a prime divisor of $2^{32} + 1$. We consider, however,

$$\ell \equiv 1 \pmod 2, \qquad \ell \equiv 2 \pmod 3,$$
$$\ell \equiv 0 \pmod 5, \qquad \ell \equiv 13 \pmod{17},$$
$$\ell \equiv 256 \pmod{257}, \qquad \ell \equiv 1 \pmod{65537},$$
$$\ell \equiv 640 \pmod{641}, \qquad \ell \equiv 3376382 \pmod{6700417}.$$

This particular choice of congruences gives the least ℓ based on Izotov's construction. The solution to these congruences is

$$\ell \equiv 734110615000775 \pmod{2 \cdot 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 \cdot 641 \cdot 6700417}.$$

Thus, any ℓ of this form has the property that $k = \ell^4$ is a Sierpiński number, and it seems likely that these give rise to counterexamples to Conjecture 2. We have already discussed how computations can suggest that a value of k is not a Sierpiński number based on a covering argument by producing $k \cdot 2^n + 1$ which have large prime divisors p each with 2 having a large order modulo p. Table 2 below gives evidence then that $k = \ell^4$ with $\ell = 734110615000775$ does not arise from a covering argument, that is, that it is a true counterexample to Conjecture 2.

Table 2

n	Smallest prime	Factorization of order of 2
14	271933097	$2593 \cdot 13109$
118	2476352353	$2^2 \cdot 3 \cdot 3391 \cdot 7607$
334	376843822247957	$2^2 \cdot 7 \cdot 79 \cdot 733 \cdot 1031 \cdot 225431$

Given that the k that was used to create Table 2 is considerably larger than the k used to create Table 1, one might suspect that the primes appearing in Table 2 should be larger. We note, however, that the k used in Table 2 only has a chance of producing a large smallest prime factor when $n \equiv 2 \pmod 4$ and in this case we know that $k \cdot 2^n + 1$ splits as a product of two numbers of relatively equal size. There was not an analogous splitting situation for the k used to create Table 1.

Before proceeding, we clarify that we are not suggesting that any of the remaining 6 values in the Seventeen or Bust project are actually Sierpiński numbers. One can easily check that none of these 6 values is of the form ℓ^r where $r > 1$, and it seems likely to us that the following revision of Conjecture 2 holds.

Conjecture 3. *If k is a Sierpiński number that is not of the form ℓ^r for some integers $\ell \geqslant 1$ and $r > 1$, then the smallest prime divisor of $k \cdot 2^n + 1$ is bounded as n tends to infinity.*

Motivated by the work of Izotov and in the spirit of Selfridge's example of a Sierpiński number, in the next section we discuss small examples of Sierpiński and Riesel numbers and for Polignac's conjecture that do not appear to arise from coverings. The constructions of examples for Riesel numbers and Polignac's conjecture are new. In this regard, it is of some interest to quote the first edition of [9] (Springer-Verlag, New York, 1981, Section F13) which mentions the following:

> *Erdős also formulates the following conjecture. Consider all the arithmetic progressions of odd numbers, no term of which is of the form $2^k + p$. Is it true that all these progressions can be obtained from covering congruences*? *Are there infinitely many integers, not of the form $2^k + p$, which are not in such progressions*?

Our work suggests strongly that the answer to the second question is, "Yes."

We turn to background on Riesel numbers and Polignac's problem. First we clarify that the use of coverings for finding k such that $k \cdot 2^n - 1$ is composite for each positive integer n and the use of coverings for finding k such that $|k - 2^n|$ is composite for each positive integer n are essentially equivalent. More precisely, let k be an integer, and let $\mathcal{P}$ be a finite set of odd primes. Then $k \cdot 2^n - 1$ has a prime divisor from the set $\mathcal{P}$ for all positive integers n if and only if $|k - 2^n|$ has a prime divisor from the set $\mathcal{P}$ for all positive integers n. We state this as a lemma that allows

us to move from one problem to the next. For later purposes in the paper, we state it with a little more generality.

Lemma 4. *Let $\mathcal{S}$ be the set of integers, the set of even integers or the set of odd integers, let $\mathcal{P}$ be a finite set of odd primes, and let k be an integer. Suppose that for every sufficiently large $n \in \mathcal{S}$ there is a $p \in \mathcal{P}$ for which*

$$k \cdot 2^n - 1 \equiv 0 \pmod{p}. \tag{2}$$

Then for each $n \in \mathcal{S}$ there is a $p \in \mathcal{P}$ for which

$$k - 2^n \equiv 0 \pmod{p}. \tag{3}$$

Similarly, if for every sufficiently large $n \in \mathcal{S}$ there is a $p \in \mathcal{P}$ satisfying (3)*, then for every $n \in \mathcal{S}$ there is a $p \in \mathcal{P}$ satisfying* (2)*.*

Proof. We consider the first implication. Let n be an arbitrary element of $\mathcal{S}$. Put

$$m_p = \operatorname{ord}_p(2), \quad \text{for } p \in \mathcal{P}.$$

Set

$$N = 2M \cdot \left(\prod_{p \in \mathcal{P}} m_p \right) - n,$$

where M is an arbitrary integer. Observe that $n \in \mathcal{S}$ implies that $N \in \mathcal{S}$. We take M sufficiently large so that N is large enough to guarantee that

$$k \cdot 2^N - 1 \equiv 0 \pmod{p}$$

for some $p \in \mathcal{P}$. This congruence implies

$$k \cdot 2^{-n} - 1 \equiv 0 \pmod{p}.$$

We multiply both sides of the congruence by 2^n to obtain

$$k - 2^n \equiv 0 \pmod{p}.$$

This establishes the first part of the lemma. The second part follows along similar lines. □

We note that it is possible for $k \cdot 2^n - 1$ or $|k - 2^n|$ above to be an element of $\mathcal{P}$. For that reason, we are *not* claiming that k is a Riesel number if and only if k is an odd positive integer for which $|k - 2^n|$ is composite for all positive integers n. We are not even claiming that this is true when we restrict ourselves to such k that can be obtained from coverings. However, the above lemma does allow us *often* to conclude that a k that has been shown to be a Riesel number is also an odd positive integer k for which $|k - 2^n|$ is composite for all positive integers n and vice versa. A. Schinzel has also obtained a connection between Sierpiński numbers and Riesel numbers. The

connection is not as direct as above, and we do not give the details here. The interested reader can see [8] or [13] for details.

H. Riesel [11] showed that if

$$k \equiv 509203 \pmod{11184810},$$

then k is what has been defined as a Riesel number. It is believed that 509203 is in fact the smallest Riesel number. As of this writing, there remain 70 odd positive integers $k < 509203$ which have not been established as being or not being Riesel numbers. Of these k, the number 2293 is the smallest. The web page http://www.prothsearch.net/rieselprob.html maintains up-to-date information.

Eric Brier (1998, unpublished) showed that there are infinitely many numbers which are simultaneously Sierpiński and Riesel numbers. His example had 41 digits, and Yves Gallot (2000, unpublished) later found an example with 27 digits. We note that Y.-G. Chen [4] has recently obtained some related results. We obtain here a smaller example with 24 digits.

Theorem 5. *A positive proportion of the positive integers are simultaneously Sierpiński and Riesel numbers. The number* 143665583045350793098657 *is one such number.*

The first part of this result is not new and follows from Brier's work. For a proof of Theorem 5, we provide appropriate coverings. One covering will show that if k satisfies certain conditions, then k is a Sierpiński number. The other will show that if certain other conditions are satisfied by k, then k is a Riesel number. It will be an easy task to then justify that all the conditions can simultaneously be satisfied by k. We give the details to help clarify the approach we use throughout this paper.

Proof. Each row of Table 3 indicates a residue class $a \pmod m$ for n and a corresponding residue class $b \pmod p$ for k such that, for every positive integer $n \equiv a \pmod m$, the number $k \cdot 2^n + 1$ is divisible by p. Each row of Table 4 indicates a residue class $a \pmod m$ for n and a corresponding residue class $b \pmod p$ for k such that, for every positive integer $n \equiv a \pmod m$, the number $k \cdot 2^n - 1$ is divisible by p. For each table, the congruences $x \equiv a \pmod m$ given by the residue classes $a \pmod m$ for n form a covering. We justify these remarks.

Table 3

Classes for n	Classes for k
1 (mod 2)	1 (mod 3)
0 (mod 3)	6 (mod 7)
4 (mod 9)	41 (mod 73)
10 (mod 18)	10 (mod 19)
16 (mod 36)	4 (mod 37)
34 (mod 36)	105 (mod 109)
2 (mod 5)	23 (mod 31)
8 (mod 10)	7 (mod 11)
5 (mod 15)	33 (mod 151)
14 (mod 30)	2 (mod 331)
56 (mod 60)	45 (mod 61)
26 (mod 60)	16 (mod 1321)

Table 4

Classes for n	Classes for k
0 (mod 2)	1 (mod 3)
3 (mod 4)	2 (mod 5)
5 (mod 8)	8 (mod 17)
1 (mod 16)	129 (mod 257)
5 (mod 12)	11 (mod 13)
9 (mod 24)	233 (mod 241)
25 (mod 48)	48 (mod 97)

Observe that the least common multiple of the moduli m for the residue classes $a \pmod m$ for n in Table 3 is 180. We can establish then that the 12 congruences $x \equiv a \pmod m$ form a covering by simply checking if each element of $\{0, 1, \ldots, 179\}$ satisfies one of the 12 congruences. Indeed, if this is the case, then an arbitrary integer u can be written in the form $u = 180q + r$ where $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, 179\}$ so that u and r are congruent modulo any of the 12 moduli m. It follows that u will satisfy whichever of these congruences that r satisfies. To justify the entries $a \pmod m$ and $b \pmod p$ in a row of Table 3, one checks that $\operatorname{ord}_p(2) = m$ and that $b2^a + 1 \equiv 0 \pmod p$. For if this holds, then

$$n \equiv a \pmod m, \quad k \equiv b \pmod p \quad \Longrightarrow \quad k2^n + 1 \equiv b2^a + 1 \equiv 0 \pmod p.$$

In this manner, one can therefore justify that any k as in Table 3 is indeed a Sierpiński number. An analogous argument works to justify that any k as in Table 4 is a Riesel number, though the argument in this case is somewhat easier since the number of congruences to consider is smaller and the least common multiple of the moduli for n in Table 4 is 48. Finally, observe that the prime moduli p appearing for the residue classes for k in Tables 3 and 4 are distinct except in the case that $p = 3$. In this case, both tables indicate that we want $k \equiv 1 \pmod 3$. We add the condition $k \equiv 1 \pmod 2$. The Chinese Remainder Theorem and a calculation now establish Theorem 5. □

Small positive odd integers which are not the sum of a power of 2 and a prime are easy to come by. This list begins

$$127,\ 149,\ 251,\ 331,\ 337,\ 373,\ 509.$$

These numbers are all prime. The smallest composite odd number that is not a power of 2 plus a prime is 905. As mentioned in the opening paragraph, the real interest here is in odd positive integers k with the property that $|k - 2^n|$ is not prime for all positive integers n. As a consequence of Lemma 4, the smallest known such k is 509203. In 1950, J.G. van der Corput [14] and Erdős [7] independently showed that a positive proportion of the odd positive integers k have the property that $|k - 2^n|$ is not prime for all positive integers n. Erdős's argument was based on a covering, and in fact his paper introduced the idea of applying covering systems to problems in number theory.

In the final two sections of this paper, we address two recent conjectures of Y.-G. Chen [3]:

Conjecture 6. *For any positive integer r, there exist infinitely many positive odd numbers k such that $k^r 2^n + 1$ has at least two distinct prime factors for all positive integers n.*

Conjecture 7. *For any positive integer r, there exist infinitely many positive odd numbers k such that $k^r - 2^n$ has at least two distinct prime factors for all positive integers n.*

He resolves these conjectures in the case that r is odd and in the case that r is twice an odd number and $3 \nmid r$. As he notes, the least r for which his arguments do not apply are $r = 4$ and $r = 6$. We will show that Conjecture 6 is true in general and that Conjecture 7 holds in the special cases $r = 4$ and $r = 6$. Our arguments will in fact resolve Conjecture 7 for a set of integers r with positive density with each r divisible by 4 and another set r having positive density and each r divisible by 6. The full strength of Conjecture 7 remains open.

Next, we turn to a result associated with Conjecture 6. We include the proof here as it draws from some of the discussion above and is fairly simple. The material in the third section can be viewed as a strengthening of the result below and its corollary.

Theorem 8. *Suppose there exist at least r composite Fermat numbers $F_m = 2^{2^m} + 1$. Then there are infinitely many positive odd integers k such that if t is a positive integer not divisible by 2^r, then k^t is a Sierpiński number.*

Proof. We will use that F_m cannot be of the form u^s where u and s are positive integers and $s > 1$. To see this, assume otherwise. Then $2^{2^m} = u^s - 1$ has $u - 1$ as a factor. Hence, $u = 2^v + 1$ for some integer $v \geqslant 1$. This implies $2^{2^m} + 1 = (2^v + 1)^s$. The rest of the argument can be completed in a few different ways. In particular, we obtain an immediate contradiction from Bang's theorem [1] that there is a primitive prime divisor of $2^a + 1$ for every integer $a > 3$.

Let $m_0 < m_1 < \cdots < m_{r-1}$ be positive integers for which F_{m_j} is composite for each j. Since no F_{m_j} is of the form u^s with $s > 1$, we deduce that each F_{m_j} has at least two distinct prime factors, say p_j and q_j. We use also that the Fermat numbers F_m, for $m \geqslant 0$, are odd and pairwise coprime.

By the Chinese Remainder Theorem, there is an infinite arithmetic progression of positive integers k satisfying the following congruences:

$$k \equiv \begin{cases} 1 \pmod 2, & \\ 1 \pmod{F_m} & \text{for } 0 \leqslant m < m_{r-1} \text{ and } m \notin \{m_0, \ldots, m_{r-1}\}, \\ 1 \pmod{p_j} & \text{for } 0 \leqslant j \leqslant r-1, \\ 2^{2^{m_j - j}} \pmod{q_j} & \text{for } 0 \leqslant j \leqslant r-1. \end{cases}$$

We prove that any such k satisfying these congruences, other than possibly the least one, also satisfies the condition in the theorem.

Let t be a positive integer not divisible by 2^r. Then we can write $t = 2^w t'$ where w and t' are integers with $0 \leqslant w \leqslant r-1$, $t' > 0$ and t' odd. We want $k^t \cdot 2^n + 1$ to be composite for each positive integer n. Fix a positive integer n. We complete the proof by showing that $k^t \cdot 2^n + 1$ is divisible by some number from the set

$$\mathcal{S} = \left\{F_m \colon 0 \leqslant m < m_w,\ m \notin \{m_0, \ldots, m_w\}\right\} \cup \{p_j \colon 0 \leqslant j \leqslant w\} \cup \{q_w\}.$$

Since each k satisfying the congruences above, other than the least one, is greater than the product of the elements of $\mathcal{S}$, we can deduce then that each such k satisfies that $k^t \cdot 2^n + 1$ is composite for all positive integers n.

Fix i to be the nonnegative integer such that $n = 2^i n'$ where n' is an odd integer. Let

$$d = \begin{cases} F_i & \text{if } i < m_w \text{ and } i \notin \{m_0, m_1, \ldots, m_w\}, \\ p_j & \text{if } i = m_j \text{ for some } j \in \{0, 1, \ldots, w\}, \\ q_w & \text{if } i > m_w. \end{cases}$$

Observe that if $i \leqslant m_w$, then d divides $2^{2^i} + 1$ and, hence, $2^{2^i n'} + 1$. Therefore,

$$k^t 2^n + 1 \equiv k^t 2^{2^i n'} + 1 \equiv 2^{2^i n'} + 1 \equiv 0 \pmod d.$$

Now, suppose $i > m_w$. Then

$$k^t \equiv 2^{2^{m_w - w} 2^w t'} \equiv \left(2^{2^{m_w}}\right)^{t'} \equiv (-1)^{t'} \equiv -1 \pmod{d}.$$

Note that in this case d divides $2^{2^{m_w}} + 1$ and, hence, $2^{2^i} - 1$, since this latter number is the product of F_m for $0 \leqslant m < i$. Thus, d divides $2^{2^i n'} - 1$, which implies

$$k^t 2^n + 1 \equiv -\left(2^{2^i n'} - 1\right) \equiv 0 \pmod{d}.$$

Hence, for each positive integer n, the number $k^t 2^n + 1$ is divisible by an element of $\mathcal{S}$. The theorem follows. □

Given the current status of composite Fermat numbers at http://www.prothsearch.net/fermat.html there are 231 known positive integers m for which $F_m = 2^{2^m} + 1$ is composite. By Theorem 8, there is a positive integer k such that k^t is a Sierpiński number for every $t < 2^{231}$. Hence, we have

Corollary 9. *There is a k such that all of the numbers $k, k^2, k^3, \ldots, k^{3.45 \cdot 10^{69}}$ are simultaneously Sierpiński numbers.*

3. Small examples associated with Conjecture 2

We begin with a variation on Izotov's construction, described in the previous section, to exhibit a relatively small odd positive integer ℓ such that $k = \ell^4$ is a Sierpiński number and with the property that k seemingly does not arise from a covering system. Following the idea of Izotov, we determine k such that whenever $n \not\equiv 2 \pmod 4$, the value of $k \cdot 2^n + 1$ is divisible by a prime from a fixed finite set $\mathcal{P}$ of primes. For $n \equiv 2 \pmod 4$, we rely on the fact that $k = \ell^4$ to deduce that $k \cdot 2^n + 1$ is composite based on (1). We obtain values of ℓ by applying the Chinese Remainder Theorem with congruences having moduli coming from the set $\mathcal{P}$ together with the congruences $\ell \equiv 1 \pmod 2$ and $\ell \equiv 0 \pmod 5$. As before, the congruence $\ell \equiv 1 \pmod 2$ insures that k is odd, and the congruence $\ell \equiv 0 \pmod 5$ insures that the smallest prime divisor of $k \cdot 2^n + 1$ as n varies is not always from the set $\mathcal{P} \cup \{5\}$. To obtain a small value of ℓ, we simply looked for an appropriate set $\mathcal{P}$ which had the property that the product of the primes in $\mathcal{P}$ is as small as we could find. As with other notable numbers mentioned in this paper, there is no guarantee that the value of ℓ we found in this way is minimal, but the approach is a reasonable one for minimizing or at least reducing the size of ℓ.

Our search led us to taking

$$\mathcal{P} = \{3, 17, 97, 241, 257, 673\}.$$

There are various congruences one can consider based on this choice of $\mathcal{P}$. We searched through these to minimize ℓ and obtained the following:

$$\begin{aligned} n \equiv 1 \pmod 2, \quad \ell \equiv 2 \pmod 3 \quad &\Longrightarrow \quad k \cdot 2^n + 1 \equiv 0 \pmod 3, \\ n \equiv 4 \pmod 8, \quad \ell \equiv 4 \pmod{17} \quad &\Longrightarrow \quad k \cdot 2^n + 1 \equiv 0 \pmod{17}, \\ n \equiv 32 \pmod{48}, \quad \ell \equiv 43 \pmod{97} \quad &\Longrightarrow \quad k \cdot 2^n + 1 \equiv 0 \pmod{97}, \end{aligned}$$

$$n \equiv 0 \pmod{24}, \quad \ell \equiv 8 \pmod{241} \implies k \cdot 2^n + 1 \equiv 0 \pmod{241},$$
$$n \equiv 8 \pmod{16}, \quad \ell \equiv 256 \pmod{257} \implies k \cdot 2^n + 1 \equiv 0 \pmod{257},$$
$$n \equiv 16 \pmod{48}, \quad \ell \equiv 4 \pmod{673} \implies k \cdot 2^n + 1 \equiv 0 \pmod{637}.$$

In the above, $k = \ell^4$. As in the previous section, an implication with $n \equiv a \pmod{m}$ and $\ell \equiv b \pmod{p}$ is justified by checking that $\operatorname{ord}_p(2) = m$ and $b^4 2^a + 1 \equiv 0 \pmod{p}$. Observe that the least common multiple of the moduli for the congruences involving n above is 48. Also, 4 divides 48. We can establish then that these 6 congruences, together with $n \equiv 2 \pmod{4}$, form a covering by simply checking if each element of $\{0, 1, \ldots, 47\}$ satisfies one of the 7 congruences. Combining the congruences on ℓ with $\ell \equiv 1 \pmod{2}$ and $\ell \equiv 0 \pmod{5}$, we obtain the following result.

Theorem 10. *If ℓ is a positive integer satisfying*

$$\ell \equiv 44745755 \pmod{2 \cdot 3 \cdot 5 \cdot 17 \cdot 97 \cdot 241 \cdot 257 \cdot 673},$$

then $k = \ell^4$ is a Sierpiński number.

The number 44745755 should be compared to the 15 digit number arising from Izotov's construction. What we cannot conclude but would nevertheless like to give some justification for is that $k = 44745755^4$, which was constructed by making use of the fact that $4x^4 + 1$ factors in $\mathbb{Z}[x]$, cannot be obtained from a covering argument. As in the previous section, we give some evidence of this in Table 5 by looking at the smallest prime factors of $k \cdot 2^n + 1$ for various n and the order of 2 modulo these primes.

Table 5

n	Smallest prime	Factorization of order of 2
54	5719237	$2^2 \cdot 3 \cdot 476603$
90	64450569241	$3^6 \cdot 5 \cdot 139 \cdot 15901$
214	338100368290543455397	$2^2 \cdot 28175030690878621283$

We turn now to finding examples of Riesel numbers that do not appear to arise from coverings. What we use here is simply that $k \cdot 2^n - 1$ is composite if $n = 2u$ and $k = \ell^2$ where u and ℓ are positive integers with $\ell > 1$ since

$$k \cdot 2^n - 1 = \ell^2 \cdot 2^{2u} - 1 = \big(\ell \cdot 2^u + 1\big)\big(\ell \cdot 2^u - 1\big).$$

The idea then is to find a collection of congruences for n such that whenever n is odd, then n satisfies at least one of the congruences. In other words, the congruences when combined with $n \equiv 0 \pmod{2}$ form a covering. This seemingly puts us in a better position than we were in with the Sierpiński numbers where the factorization of $4x^4 + 1$ left us with wanting to find a collection of congruences such that every integer $n \not\equiv 2 \pmod{4}$ satisfies at least one of the congruences. However, the situation with Riesel numbers is actually more complicated. For Sierpiński numbers, the congruences $n \equiv 1 \pmod{2}$ and $\ell \equiv 2 \pmod{3}$ immediately gave us that whenever $n \equiv 1 \pmod{2}$, the number $\ell^4 2^n + 1$ is divisible by 3. Thus, we were only left with finding a

Table 6

Classes for n	Classes for ℓ
2 (mod 3)	4 (mod 7)
5 (mod 8)	12 (mod 17)
0 (mod 5)	30 (mod 31)
11 (mod 20)	15 (mod 41)
14 (mod 35)	66 (mod 71)
7 (mod 48)	84 (mod 97)
15 (mod 28)	100 (mod 113)
2 (mod 7)	64 (mod 127)
12 (mod 15)	92 (mod 151)
19 (mod 24)	153 (mod 241)
9 (mod 16)	223 (mod 257)
59 (mod 70)	9 (mod 281)
18 (mod 21)	52 (mod 337)
33 (mod 64)	31 (mod 641)
31 (mod 48)	236 (mod 673)
3 (mod 60)	34 (mod 1321)
75 (mod 84)	11729 (mod 14449)
69 (mod 105)	575 (mod 29191)
17 (mod 32)	2056 (mod 65537)
1 (mod 64)	5012354 (mod 6700417)

collection of congruences such that every integer $n \equiv 3 \pmod 4$ satisfies at least one of the congruences. For Riesel numbers, such a simplification in the integers n that need to be considered is not possible.

Our investigations led us to a set $\mathcal{P}$ of 20 primes for the Riesel numbers, namely

$$\mathcal{P} = \{7, 17, 31, 41, 71, 97, 113, 127, 151, 241, 257, 281, 337, 641, 673, 1321, 14449, 29191, 65537, 6700417\}.$$

Rather than displaying a list of implications, we simplify our presentation with Table 6 which consists of two columns, one column for the congruence involving n and the second column for the corresponding congruence involving ℓ. The least common multiple of the moduli for the congruences involving n is 6720. Thus, one can confirm that the 20 congruences on n together with $n \equiv 0 \pmod 2$ form a covering of the integers simply by checking that each integer in the set $\{0, 1, \ldots, 6719\}$ satisfies at least one of the 21 congruences. Hence, if ℓ satisfies each of the congruences in the second column of Table 6 and the congruence $\ell \equiv 1 \pmod 2$, then ℓ^2 is a Riesel number. We deduce

Theorem 11. *There are infinitely many squares that are Riesel numbers. One such Riesel number is*

$$3896845303873881175159314620808887046066972469809^2.$$

As noted earlier, the first sentence of this theorem is not new; it is a consequence of the work of Y.-G. Chen [3]. The significance here is that the above square, say ℓ^2, appears not to arise from a covering argument. The square is the least one that we found with our methods, though given the complexity of the covering, it is certainly possible that smaller ones exist. Analogous

to before, in Table 7 we give some information on the factorization of $\ell^2 \cdot 2^n - 1$ to support our belief that ℓ^2 cannot be obtained from a covering argument. The size of ℓ is rather large here and we quickly came to numbers that were hard to factor, so only two rows are indicated in the table. The computations for other values of n also suggest that the number ℓ does not arise from coverings; for example, a quick sieve using the first 20000 primes indicated that for $n \leqslant 25000$, there are at least 170 different values for the minimum prime factor of $\ell^2 2^n - 1$ and 59 different n for which $\ell^2 2^n - 1$ did not have a prime factor among the first 20000 primes.

Table 7

n	Smallest prime	Factorization of order of 2
118	22138187	$2 \cdot 7 \cdot 1581299$
166	666829	$2^2 \cdot 3^2 \cdot 18523$

Let $k = \ell^2$ be the Riesel number in Theorem 11. Observe that $\ell^2 - 2^{2u} = (\ell + 2^u)(\ell - 2^u)$. As each of $\ell + 1$ and $\ell - 1$ is not a power of 2, we have that $|\ell - 2^u| > 1$ for each positive integer u. Take $\mathcal{S}$ to be the set of odd numbers in Lemma 4. One checks that $k + p$ and $k - p$ are not powers of 2 for each $p \in \mathcal{P}$. We deduce that k has the property that $|k - 2^n|$ is composite for all positive integers n. Information on the factorization of $|\ell^2 - 2^n|$ to support our belief that ℓ^2 cannot be obtained from a covering argument for this problem is given in Table 8. (Note also that Lemma 4 with $S = \mathbb{Z}$ implies that if the least prime divisor of $|\ell^2 - 2^n|$ is bounded a n tends to infinity, then the least prime divisor of $|\ell^2 2^n - 1|$ is bounded as n tends to infinity.)

Table 8

n	Smallest prime	Factorization of order of 2
7	13883	$2 \cdot 11 \cdot 631$
314	9344182730989	$2^2 \cdot 3 \cdot 111240270607$

4. The resolution of Conjecture 6

In this section, we establish Theorem 1. Recall that Sierpiński's construction relied upon the fact that F_5 has two prime factors. Our proof of Theorem 8 showed how this idea could be extended but still relied on the existence of composite Fermat numbers, requiring us then to only obtain a result like Theorem 1 with R bounded. Thus, we will want to obtain a covering here by another method. We will introduce new congruences making use of primitive prime divisors of the Mersenne numbers $M_n = 2^n - 1$. To clarify, a prime p is said to be a primitive prime divisor of $2^n - 1$, independent of the expression that may be used for n in the exponent, if p divides $2^n - 1$ and p does not divide $2^t - 1$ for every positive integer $t < n$. An important result due to Bang [1] is the following:

Lemma 12. *For each positive integer $n > 6$, there exists a primitive prime divisor of $2^n - 1$.*

Our next lemma clarifies the information about primitive prime divisors of $2^n - 1$ that we will use.

Lemma 13. *Let q be an odd prime and let $s > 2$ be an integer. Then there exists a primitive prime divisor p of $2^{q2^s} - 1$. Furthermore, any such p satisfies the following*:

(i) *The order of* 2 *modulo* p *is* $q2^s$.
(ii) $p \nmid F_i$ *for every* $i \geqslant 0$.
(iii) *There exists an integer* e *such that* $e^{2^s} \equiv -1 \pmod{p}$.

Proof. Lemma 12 implies the existence of a primitive prime divisor p of $2^{q2^s} - 1$. To see (i), note that since p is a primitive prime divisor of $2^{q2^s} - 1$, p does not divide $2^t - 1$ for all $t < q2^s$. For (ii), combine (i) with the fact that 2 has order 2^{i+1} modulo prime divisors of F_i. To obtain (iii), notice that since $s > 2$, we obtain from (i) that $p \equiv 1 \pmod 8$. This implies 2 is a square modulo p; that is, there is an integer a with $a^2 \equiv 2 \pmod p$. Let $e = a^q$. One checks that $\operatorname{ord}_p(e) = 2^{s+1}$ from which (iii) follows. □

Once we have constructed our covering of the integers, our system of congruences that describe k, and our finite set of primes $\mathcal{P}$, we will use the following lemma to guarantee the existence of at least two distinct prime divisors of $k^r 2^n + 1$ for each n.

Lemma 14. *Given* $P > 0$*, an integer* $r \geqslant 3$ *and* C *and* D *nonzero integers, there is a positive integer* $Y = Y(P, r, C, D)$ *such that if* k *is an odd integer with* $|k| > Y$ *and* n *is a positive integer, then* $Ck^r 2^n + D$ *has a prime factor that is greater than* P.

Proof. Fix P, r, C and D as in the lemma. It suffices to show that there are only finitely many ordered pairs (k, n) such that

$$Ck^r 2^n + D = p_1^{f_1} \cdots p_t^{f_t}, \tag{4}$$

where the p_i are all the distinct primes less $\leqslant P$ and the f_i are nonnegative integers. We put $n = rn_1 + n_0$ and $f_i = ru_i + v_i$ for each $i \in \{1, 2, \ldots, t\}$ where $n_1, u_1, u_2, \ldots, u_t \in \mathbb{Z}$ and $n_0, v_1, v_2, \ldots, v_t \in \{0, 1, \ldots, r-1\}$. Then

$$p_1^{v_1} \cdots p_t^{v_t} \big(p_1^{u_1} \cdots p_t^{u_t}\big)^r - 2^{n_0} C \big(2^{n_1} k\big)^r = D. \tag{5}$$

Observe that $Ax^r - By^r = D$, where $r \geqslant 3$ and A, B and D are nonzero integers, is a Thue equation which has finitely many solutions in integers x and y. We take $A = p_1^{v_1} \cdots p_t^{v_t}$ and $B = 2^{n_0} C$. There are r^t possibilities for A depending on the v_i and r possibilities for B depending on n_0. We deduce that there are finitely many possibilities for $p_1^{u_1} \cdots p_t^{u_t}$ and $2^{n_1} k$ in (5) and, consequently, finitely many pairs (k, n) satisfying (4). □

To establish Theorem 1, we may suppose that k is an 8th power. In other words, it suffices to show that there exist infinitely many positive odd numbers k such that each of the numbers

$$k^8 2^n + 1,\ k^{16} 2^n + 1,\ k^{24} 2^n + 1,\ \ldots,\ k^{8R} 2^n + 1$$

has at least two distinct prime factors for each positive integer n. We consider then the positive integers $r \leqslant 8R$ that are divisible by 8. Define integers $s = s(r)$ and $r' = r'(r)$, with r' odd, by the relation $r = 2^s r'$. Let $q = q(r)$ be an odd prime with $(r', q) = 1$. We furthermore take the various $q(r)$ as r varies so that they are distinct. We start our covering of the integers with the congruences

$$n \equiv 2^i \pmod{2^{i+1}}, \quad \text{for } 0 \leqslant i \leqslant \max\big\{s(r) + q(r) - 2\big\}, \tag{6}$$

where the maximum is over the positive integers $r \leqslant 8R$ divisible by 8. For each i as above, fix a prime divisor p_i of $F_i = 2^{2^i} + 1$. Observe that for each i, if

$$n \equiv 2^i \pmod{2^{i+1}} \quad \text{and} \quad k \equiv 1 \pmod{p_i},$$

then

$$k^r 2^n + 1 \equiv 0 \pmod{p_i}.$$

The idea is to complete the covering system which began with the congruences in (6) by making use of different congruences depending on the value of r. With r fixed as above, we note that the congruences in (6) together with

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

form a covering of the integers. Recall here that s and q depend on r. Note that this covering of the integers only makes use of the congruences in (6) corresponding to $0 \leqslant i \leqslant s+q-2$. Also, every integer n that satisfies $n \equiv 0 \pmod{2^{s+q-1}}$ must satisfy one of the q congruences

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

Since q and r' are coprime odd numbers, the set of residues classes modulo $2^{s+q-1}q$ represented by

$$0,\ 2^{s+q-1},\ 2 \cdot 2^{s+q-1},\ \ldots,\ (q-1)2^{s+q-1}$$

is identical to the set of residue classes modulo $2^{s+q-1}q$ represented by

$$0,\ r'2^{s+q-1},\ r'2 \cdot 2^{s+q-1},\ \ldots,\ r'(q-1)2^{s+q-1},$$

so it suffices to complete our covering with the q congruences

$$n \equiv jr'2^{s+q-1} \pmod{2^{s+q-1}q}, \quad \text{for } 0 \leqslant j \leqslant q-1.$$

From Lemma 13, for each $j \in \{0, 1, \ldots, q-1\}$, there is a primitive prime divisor $\hat{p}_j = \hat{p}_j(r)$ of the Mersenne number $M_{2^{s+j}q}$ and an integer $e_j = e_j(r)$ such that $e_j^{2^{s+j}} \equiv -1 \pmod{\hat{p}_j}$. We show that for each $j \in \{0, 1, \ldots, q-1\}$ if

$$n \equiv jr'2^{s+q-1} \pmod{2^{s+q-1}q} \quad \text{and} \quad k \equiv 2^{-j \cdot 2^{q-1}} e_j^{2^j} \pmod{\hat{p}_j},$$

then

$$k^r 2^n + 1 \equiv 0 \pmod{\hat{p}_j}.$$

Indeed, defining the integer N by $n = 2^{s+q-1}qN + jr'2^{s+q-1}$, this follows from

$$\begin{aligned} k^r 2^n + 1 &\equiv \left(2^{-j\cdot 2^{q-1}} e_j^{2^j}\right)^{2^s r'} 2^{2^{s+q-1} qN + jr' 2^{s+q-1}} + 1 \\ &\equiv \left(e_j^{2^{s+j}}\right)^{r'} \cdot \left(2^{2^{s+j} q}\right)^{2^{q-1-j} N} + 1 \\ &\equiv (-1)^{r'} + 1 \equiv 0 \pmod{\hat{p}_j}. \end{aligned}$$

We summarize the above. For each $r \leqslant 8R$ that is a multiple of 8, the congruences

$$\begin{aligned} n &\equiv 2^i \pmod{2^{i+1}}, \quad \text{for } 0 \leqslant i \leqslant s+q-2, \\ n &\equiv jr' 2^{s+q-1} \pmod{2^{s+q-1} q}, \quad \text{for } 0 \leqslant j \leqslant q-1 \end{aligned}$$

form a covering of the integers. If k satisfies the congruences

$$\begin{aligned} k &\equiv 1 \pmod{p_i}, \quad \text{for } 0 \leqslant i \leqslant s+q-2, \\ k &\equiv 2^{-j\cdot 2^{q-1}} e_j^{2^j} \pmod{\hat{p}_j}, \quad \text{for } 0 \leqslant j \leqslant q-1, \end{aligned}$$

then for each positive integer n, the number $k^r 2^n + 1$ is divisible by some prime in the set

$$\mathcal{P}_r = \{p_0, p_1, \ldots, p_{s+q-2}, \hat{p}_0, \hat{p}_1, \ldots, \hat{p}_{q-1}\}.$$

Furthermore, Lemma 13 guarantees that the primes in $\mathcal{P}_r$ are distinct.

Recall that $\hat{p}_j(r)$ is a prime, necessarily odd, for which 2 has order $2^{s+j} q(r)$. Since the $q(r)$ are distinct, we deduce that the values of $\hat{p}_j(r)$ as j and r vary are all distinct. By the Chinese Remainder Theorem, there are infinitely many positive integers k satisfying

$$\begin{aligned} k &\equiv 1 \pmod 2, \\ k &\equiv 1 \pmod{p_i}, \quad \text{for } 0 \leqslant i \leqslant \max\{s(r) + q(r) - 2\}, \\ k &\equiv 2^{-j\cdot 2^{q(r)-1}} e_j(r)^{2^j} \pmod{\hat{p}_j(r)} \quad \text{for } r \in \{8, 16, 24, \ldots, 8R\} \text{ and } 0 \leqslant j \leqslant q(r)-1. \end{aligned}$$

We deduce that any such k has the property that, for every positive integer n, the numbers

$$k^8 2^n + 1,\ k^{16} 2^n + 1,\ k^{24} 2^n + 1,\ \ldots,\ k^{8R} 2^n + 1$$

each have a prime divisor from the set

$$\mathcal{P} = \bigcup \mathcal{P}_r,$$

where the union is over $r \in \{8, 16, 24, \ldots, 8R\}$. We apply Lemma 14 for each r with P being the maximum element of $\mathcal{P}$, $C = 1$ and $D = 1$. Hence, we see that if k is sufficiently large satisfying the congruences above, then for every positive integer n, the numbers

$$k^8 2^n + 1,\ k^{16} 2^n + 1,\ k^{24} 2^n + 1,\ \ldots,\ k^{8R} 2^n + 1$$

each have a prime divisor in $\mathcal{P}$ and a prime divisor not in $\mathcal{P}$. This establishes Theorem 1.

5. New cases of Conjecture 7

In this section, we address the two special cases of Conjecture 7 with $r = 4$ and $r = 6$. Corollaries of the arguments below will address some other new cases of this conjecture. We begin with the case $r = 4$.

Theorem 15. *There exist infinitely many positive odd numbers k such that*

$$k^4 - 2^n$$

has at least two distinct prime factors for each positive integer n.

With the intent of applying Lemma 4, we work with $k^4 2^n - 1$. We make use of two simple lemmas.

Lemma 16. *Let r be a positive integer, let p be an odd prime, and let a be an arbitrary integer. Suppose that 2 is an rth power modulo p and that the order of 2 modulo p is m. Then there exists an integer $b = b(p, a)$ such that if $k \equiv b \pmod{p}$ and $n \equiv a \pmod{m}$, then $k^r 2^n - 1$ is divisible by p.*

Proof. Let c be such that $c^r \equiv 2 \pmod{p}$. Since p is odd, p does not divide c. If $n \equiv a \pmod{m}$, then

$$k^r 2^n - 1 \equiv k^r 2^a - 1 \equiv \left(kc^a\right)^r - 1 \pmod{p}.$$

The lemma follows by taking $b \equiv c^{-a} \pmod{p}$. □

Lemma 17. *Let r be a positive integer, let p be an odd prime and let $g = \gcd(r, p-1)$. Then 2 is an rth power modulo p if and only if $2^{(p-1)/g} \equiv 1 \pmod{p}$.*

Proof. The condition $2^{(p-1)/g} \equiv 1 \pmod{p}$ is equivalent to 2 being a gth power modulo p. There are integers x and y such that $rx + (p-1)y = g$. If a is an integer for which $2 \equiv a^g \pmod{p}$, then $2 \equiv a^{rx+(p-1)y} \equiv (a^x)^r \pmod{p}$, so 2 is an rth power modulo p. Since $g \mid r$, we also have that if 2 is an rth power modulo p, then 2 is a gth power modulo p. This completes the proof. □

Lemma 16 motivates our approach. We take $r = 4$. If $n \equiv 0 \pmod{2}$ and $k \equiv 1 \pmod{3}$, then $k^r 2^n - 1$ is divisible by 3. We take $a_1 = 0$, $m_1 = 2$ and $p_1 = 3$. For $n \equiv 1 \pmod{2}$, we find distinct odd primes $p_2, \ldots, p_t$, with 2 a fourth power modulo each p_i, and build on the congruence $n \equiv a_1 \pmod{m_1}$ to form a covering of the integers

$$n \equiv a_i \pmod{m_i} \quad \text{for } 1 \leqslant i \leqslant t,$$

such that $m_i = \operatorname{ord}_{p_i}(2)$ for each i. The tables in [2] provide an excellent source for finding the primes p for which 2 has a prescribed order m modulo p. One simply looks up the primitive prime factors of $2^m - 1$ appearing in these tables. Thus, [2] helped us determine the primes to initially consider as well as the moduli, with their multiplicities, that we could use for the

covering. Lemma 17, with $r = 4$, enabled us to quickly simplify these lists so that only primes p for which 2 is a fourth power modulo p were considered. We tabulate the results of our work in the 63 rows of Table 9. In the ith row, we list a congruence on n of the form $n \equiv a_i \pmod{m_i}$, a list $[e_1, e_2, e_3, e_4, e_5]$ of exponents to clarify the factorization

$$m_i = 2^{e_1}3^{e_2}5^{e_3}7^{e_4}11^{e_5},$$

and a prime p_i. To conserve space in the tables, we note here that

$$p_{38} = 204856883529738048676023 1,$$
$$p_{63} = 14768784307009061644318236958041601.$$

Lemma 18. *The congruences $n \equiv a_i \pmod{m_i}$ listed in Table 9 form a covering of the integers. Also, the primes p_i are distinct, $\operatorname{ord}_{p_i}(2) = m_i$ for each i, and 2 is a fourth power modulo p_i for each $i \geqslant 2$.*

One can verify the second statement in Lemma 18 directly. In particular, to test whether 2 is a fourth power modulo p_i, observe that, in the notation of Lemma 17, we have

$$2^{(p_i-1)/g} \equiv 1 \pmod{p_i} \quad \Longleftrightarrow \quad m_i \text{ divides } (p_i - 1)/g. \tag{7}$$

Thus, for $r = 4$, Lemma 17 implies that 2 is a fourth power modulo p_i if and only if the largest power of 2 dividing the product of $\gcd(4, p_i - 1)$ and m_i divides $p_i - 1$.

We explain next a method for verifying the first part of Lemma 18.

The least common multiple of the moduli in Table 9 is $2^5 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11 = 997920$. To verify that the congruences on n form a covering one can check that each of $0, 1, \ldots, 997919$ satisfies one of these congruences (computationally, this is not difficult). To reduce the amount of work needed to verify Lemma 18, one can proceed as follows. The congruences in rows 28 to 45 of Table 9 are the only congruences where the moduli have 11 as a prime factor. To reduce the least common multiple of the moduli of the covering, one can first verify that these 18 congruences together with the congruences in rows 23 and 24 cover 5 modulo 18, that is that every integer which is 5 modulo 18 satisfies one of the congruences on n in rows 28 to 45 or in rows 23 and 24. The least common multiple of the moduli for these 20 congruences is 3960. One can check directly that the 220 residues $18j + 5$, for $0 \leqslant j \leqslant 219$, modulo 3960 that correspond to 5 modulo 18 are covered by these 20 congruences. Once this is confirmed, we can replace the congruences in rows 28 to 45 with $n \equiv 5 \pmod{18}$, eliminating 11 from the prime factors of our moduli and reducing the least common multiple of the moduli to 90720.

To further reduce the work needed to verify Lemma 18, we similarly observe that rows 10 through 23 of Table 9 cover the residue 7 modulo 18 and these include the only congruences whose moduli have 7 as a prime factor. To verify that these 14 congruences cover 7 modulo 18, one need only check the 35 residues modulo 630 that make up 7 modulo 18. Once this is established, we can replace the congruences in rows 10 to 22 with $n \equiv 7 \pmod{18}$, eliminating 7 from the prime factors of our moduli and reducing the least common multiple of the moduli to 12960. From here, it is a simple computation to establish that these congruences do indeed cover the integers.

Table 9

Row	Congruence	Exponents of prime factors of m_i	Prime p_i
1	$n \equiv 0 \pmod 2$	[1,0,0,0,0]	3
2	$n \equiv 0 \pmod 3$	[0,1,0,0,0]	7
3	$n \equiv 1 \pmod 9$	[0,2,0,0,0]	73
4	$n \equiv 4 \pmod{27}$	[0,3,0,0,0]	262657
5	$n \equiv 49 \pmod{108}$	[2,3,0,0,0]	246241
6	$n \equiv 103 \pmod{108}$	[2,3,0,0,0]	279073
7	$n \equiv 13 \pmod{81}$	[0,4,0,0,0]	2593
8	$n \equiv 40 \pmod{81}$	[0,4,0,0,0]	71119
9	$n \equiv 67 \pmod{81}$	[0,4,0,0,0]	97685839
10	$n \equiv 0 \pmod 7$	[0,0,0,1,0]	127
11	$n \equiv 1 \pmod{21}$	[0,1,0,1,0]	337
12	$n \equiv 16 \pmod{63}$	[0,2,0,1,0]	92737
13	$n \equiv 52 \pmod{63}$	[0,2,0,1,0]	649657
14	$n \equiv 25 \pmod{126}$	[1,2,0,1,0]	77158673929
15	$n \equiv 26 \pmod{35}$	[0,0,1,1,0]	71
16	$n \equiv 47 \pmod{70}$	[1,0,1,1,0]	281
17	$n \equiv 103 \pmod{105}$	[0,1,1,1,0]	29191
18	$n \equiv 19 \pmod{105}$	[0,1,1,1,0]	106681
19	$n \equiv 97 \pmod{210}$	[1,1,1,1,0]	664441
20	$n \equiv 181 \pmod{210}$	[1,1,1,1,0]	1564921
21	$n \equiv 223 \pmod{315}$	[0,2,1,1,0]	870031
22	$n \equiv 34 \pmod{315}$	[0,2,1,1,0]	983431
23	$n \equiv 0 \pmod 5$	[0,0,1,0,0]	31
24	$n \equiv 11 \pmod{15}$	[0,1,1,0,0]	151
25	$n \equiv 2 \pmod{45}$	[0,2,1,0,0]	631
26	$n \equiv 38 \pmod{45}$	[0,2,1,0,0]	23311
27	$n \equiv 29 \pmod{90}$	[1,2,1,0,0]	18837001
28	$n \equiv 0 \pmod{11}$	[0,0,0,0,1]	23
29	$n \equiv 1 \pmod{11}$	[0,0,0,0,1]	89
30	$n \equiv 2 \pmod{33}$	[0,1,0,0,1]	599479
31	$n \equiv 47 \pmod{66}$	[1,1,0,0,1]	20857
32	$n \equiv 5 \pmod{99}$	[0,2,0,0,1]	199
33	$n \equiv 59 \pmod{99}$	[0,2,0,0,1]	153649
34	$n \equiv 50 \pmod{99}$	[0,2,0,0,1]	33057806959
35	$n \equiv 18 \pmod{55}$	[0,0,1,0,1]	881
36	$n \equiv 29 \pmod{55}$	[0,0,1,0,1]	3191
37	$n \equiv 7 \pmod{55}$	[0,0,1,0,1]	201961
38	$n \equiv 107 \pmod{165}$	[0,1,1,0,1]	p_{38}
39	$n \equiv 173 \pmod{330}$	[1,1,1,0,1]	415365721
40	$n \equiv 239 \pmod{495}$	[0,2,1,0,1]	991
41	$n \equiv 9 \pmod{44}$	[2,0,0,0,1]	2113
42	$n \equiv 383 \pmod{396}$	[2,2,0,0,1]	15975607282273
43	$n \equiv 65 \pmod{132}$	[2,1,0,0,1]	4327489
44	$n \equiv 43 \pmod{88}$	[3,0,0,0,1]	353
45	$n \equiv 263 \pmod{264}$	[3,1,0,0,1]	7393
46	$n \equiv 17 \pmod{144}$	[4,2,0,0,0]	577
47	$n \equiv 89 \pmod{144}$	[4,2,0,0,0]	487824887233
48	$n \equiv 3 \pmod{16}$	[4,0,0,0,0]	257
49	$n \equiv 107 \pmod{288}$	[5,2,0,0,0]	1153
50	$n \equiv 251 \pmod{288}$	[5,2,0,0,0]	278452876033
51	$n \equiv 35 \pmod{162}$	[1,4,0,0,0]	135433

(*continued on next page*)

Table 9 (*continued*)

Row	Congruence	Exponents of prime factors of m_i	Prime p_i
52	$n \equiv 89 \pmod{162}$	[1,4,0,0,0]	272010961
53	$n \equiv 629 \pmod{1296}$	[4,4,0,0,0]	10369
54	$n \equiv 413 \pmod{432}$	[4,3,0,0,0]	209924353
55	$n \equiv 53 \pmod{216}$	[3,3,0,0,0]	33975937
56	$n \equiv 125 \pmod{216}$	[3,3,0,0,0]	138991501037953
57	$n \equiv 107 \pmod{180}$	[2,2,1,0,0]	54001
58	$n \equiv 23 \pmod{240}$	[4,1,1,0,0]	394783681
59	$n \equiv 143 \pmod{240}$	[4,1,1,0,0]	46908728641
60	$n \equiv 39 \pmod{160}$	[5,0,1,0,0]	414721
61	$n \equiv 79 \pmod{160}$	[5,0,1,0,0]	44479210368001
62	$n \equiv 119 \pmod{480}$	[5,1,1,0,0]	23041
63	$n \equiv 479 \pmod{480}$	[5,1,1,0,0]	p_{63}

For each $i \geqslant 2$, we choose c_i so that $c_i^4 \equiv 2 \pmod{p_i}$. Recall that $\operatorname{ord}_{p_i}(2) = m_i$. One checks that, for such i, if

$$n \equiv a_i \pmod{m_i} \quad \text{and} \quad k \equiv c_i^{-a_i} \pmod{p_i},$$

then $k^4 2^n - 1$ is divisible by p_i. This was essentially our proof of Lemma 16.

Let k be an integer satisfying

$$k \equiv c_i^{-a_i} \pmod{p_i} \quad \text{for } 2 \leqslant i \leqslant 63$$

and

$$k \equiv 1 \pmod{6}.$$

The Chinese Remainder Theorem guarantees the existence of infinitely many such integers k corresponding to a congruence modulo $M = 2p_1 \cdots p_{63}$. We deduce that each such k has the property that $k^4 2^n + 1$ has a prime factor in

$$\mathcal{P} = \{p_1, p_2, \ldots, p_{63}\}$$

for each positive integer n.

To establish Theorem 15, we apply Lemma 4 with $\mathcal{S} = \mathbb{Z}$ to deduce that there is an infinite arithmetic progression of odd integers k such that $k^4 - 2^n$ is divisible by at least one prime from $\mathcal{P}$ for each positive integer n.

Next, we address finding a prime divisor of $k^4 - 2^n$ that is not in $\mathcal{P}$. We make use of the following theorem of Darmon and Granville [5].

Theorem 19. *Let A, B and C be nonzero integers. Let p, q and r be positive integers for which $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. Then the generalized Fermat equation $Ax^p + By^q = Cz^r$ has only finitely many solutions in integers x, y and z with* $\gcd(x, y, z) = 1$.

Lemma 20. *Given $P > 0$, an integer $r \geqslant 2$ and C and D nonzero integers, there is a positive integer $Y = Y(P, r, C, D)$ such that if k is an odd integer with $|k| > Y$ and n is a positive integer, then $C2^n + Dk^r$ has a prime factor greater than P.*

Proof. Fix P, r, C and D as in the lemma. It suffices to show that there are only finitely many ordered pairs (k, n) with k odd such that

$$C2^n + Dk^r = p_1^{f_1} \cdots p_t^{f_t}, \tag{8}$$

where the p_i are all the distinct primes less $\leqslant P$ and the f_i are nonnegative integers. Suppose (8) holds with k odd. We put $n = 5n_1 + n_0$ and $f_i = 5u_i + v_i$ for each $i \in \{1, 2, \ldots, t\}$ where $n_1, u_1, u_2, \ldots, u_t \in \mathbb{Z}$ and $n_0, v_1, v_2, \ldots, v_t \in \{0, 1, \ldots, 4\}$. Then

$$2^{n_0} C\left(2^{n_1}\right)^5 + Dk^r = p_1^{v_1} \cdots p_t^{v_t} \left(p_1^{u_1} \cdots p_t^{u_t}\right)^5. \tag{9}$$

Observe that $Ax^5 + Dy^r = Bz^5$, where $r \geqslant 2$ and A, B and D are nonzero integers, is a generalized Fermat equation with the sum of the reciprocals of the exponents < 1 and, hence, has finitely many solutions in integers x, y and z, with $\gcd(x, y, z) = 1$, by Theorem 19. Since k is odd, we have $\gcd(2^{n_1}, k, p_1^{u_1} \cdots p_t^{u_t}) = 1$. We take $A = 2^{n_0} C$ and $B = p_1^{v_1} \cdots p_t^{v_t}$. There are 5 possibilities for A depending on n_0 and 5^t possibilities for B depending on the v_j. We deduce that there are finitely many possibilities for 2^{n_1}, k and $p_1^{u_1} \cdots p_t^{u_t}$ as in (9) and, consequently, finitely many pairs (k, n) satisfying (8). □

Using Lemma 20, with $P = \max\{p_i\}$, $r = 4$, $C = -1$ and $D = 1$, we see that if k is sufficiently large, then for each positive integer n, we have that $k^4 - 2^n$ has a prime divisor outside the set $\mathcal{P} = \{p_1, \ldots, p_{63}\}$. Theorem 15 now follows.

We address some corollaries of the above. Rather than using Lemma 20, we could work with $k^4 2^n - 1$ and appeal to Lemma 14. This would give the following.

Corollary 21. *There exist infinitely many positive odd numbers k such that*

$$k^4 2^n - 1$$

has at least two distinct prime factors for each positive integer n.

Using Lemma 4, one can take the k appearing in Corollary 21 to be the same as the k appearing in Theorem 15. Suppose that m is a positive integer relatively prime to $p - 1$ for all $p \in \mathcal{P}$. Setting $r = 4m$, we get $\gcd(r, p - 1) = \gcd(4, p - 1)$ for each $p \in \mathcal{P}$. Lemma 17 now implies that 2 is an rth power for each $p \in \mathcal{P}$ with $p > 3$. Making use of the covering given in Lemma 18 and applying Lemma 16 and Lemma 20 or Lemma 14 as above, we obtain the following.

Corollary 22. *There is a set $\mathcal{T}$ of positive integers r having positive asymptotic density with the following properties*:

(i) *If* $r \in \mathcal{T}$, *then* $4 \mid r$.
(ii) *For each* $r \in \mathcal{T}$, *there exist infinitely many positive odd numbers* k *such that each of the numbers*

$$k^r - 2^n,\ k^r 2^n - 1$$

has at least two distinct prime factors for each positive integer n.

We now use the same idea to resolve the case $r = 6$.

Theorem 23. *There exist infinitely many positive odd numbers* k *such that*

$$k^6 - 2^n$$

has at least two distinct prime factors for each positive integer n.

The procedure is analogous to the procedure used to prove Theorem 15, with the exception that we want $r = 6$ in Lemmas 16 and 17. If an integer n is divisible by 2 or 3, then it satisfies one of the two congruences $n \equiv 0 \pmod 2$ and $n \equiv 0 \pmod 3$. We set $k \equiv 1 \pmod 3$ and $k \equiv 1 \pmod 7$ so n satisfying these congruences also satisfy $k^6 2^n - 1$ is divisible by at least one of 3 and 7. Next, we take 2 to be a sixth power modulo any of the remaining primes $p_3, \dots, p_t$. We identify such primes using the tables in [2] and Lemma 17 with $r = 6$. We note that the use of Lemma 17 to determine whether 2 is a sixth power modulo some prime p_i with 2 of order m_i can be simplified by taking advantage of (7) with $g = \gcd(6, p_i - 1)$. In particular, one only needs to consider the largest powers of 2 and 3 dividing m_i and $p_i - 1$.

We make use of a table to display our covering as before. For this table, we set

$$p_{28} = 432363203127002885506543172618401,$$
$$p_{33} = 841798420776578620118678896 81,$$
$$p_{41} = 342124938170536803983033419004621122511 6161.$$

Lemma 24. *The congruences* $n \equiv a_i \pmod{m_i}$ *listed in Table* 10 *form a covering of the integers. Also, the primes* p_i *are distinct,* $\operatorname{ord}_{p_i}(2) = m_i$ *for each* i, *and* 2 *is a sixth power modulo* p_i *for each* $i \geqslant 3$.

The least common multiple of the moduli in the tables is $2^5 \cdot 3 \cdot 5^2 \cdot 7 = 16800$; to verify that the congruences form a covering one checks that each of the residues modulo 16800 satisfies at least one of the congruences. Lemma 24 and Theorem 23 then follow.

Analogous to the case $r = 4$, we also obtain the following corollaries.

Corollary 25. *There exist infinitely many positive odd numbers* k *such that*

$$k^6 2^n - 1$$

has at least two distinct prime factors for each positive integer n.

Table 10

Row	Congruence	Exponents of prime factors of m_i	Prime p_i
1	$n \equiv 0 \pmod 2$	[1,0,0,0]	3
2	$n \equiv 0 \pmod 3$	[0,1,0,0]	7
3	$n \equiv 0 \pmod 5$	[0,0,1,0]	31
4	$n \equiv 1 \pmod{20}$	[2,0,1,0]	41
5	$n \equiv 11 \pmod{40}$	[3,0,1,0]	61681
6	$n \equiv 7 \pmod 8$	[3,0,0,0]	17
7	$n \equiv 27 \pmod{80}$	[4,0,1,0]	4278255361
8	$n \equiv 3 \pmod{16}$	[4,0,0,0]	257
9	$n \equiv 3 \pmod 7$	[0,0,0,1]	127
10	$n \equiv 2 \pmod{35}$	[0,0,1,1]	122921
11	$n \equiv 57 \pmod{70}$	[1,0,1,1]	281
12	$n \equiv 21 \pmod{28}$	[2,0,0,1]	113
13	$n \equiv 27 \pmod{35}$	[0,0,1,1]	71
14	$n \equiv 117 \pmod{140}$	[2,0,1,1]	7416361
15	$n \equiv 25 \pmod{56}$	[3,0,0,1]	15790321
16	$n \equiv 53 \pmod{112}$	[4,0,0,1]	5153
17	$n \equiv 109 \pmod{112}$	[4,0,0,1]	54410972897
18	$n \equiv 11 \pmod{32}$	[5,0,0,0]	65537
19	$n \equiv 123 \pmod{160}$	[5,0,1,0]	414721
20	$n \equiv 13 \pmod{25}$	[0,0,2,0]	601
21	$n \equiv 8 \pmod{25}$	[0,0,2,0]	1801
22	$n \equiv 53 \pmod{200}$	[3,0,2,0]	340801
23	$n \equiv 73 \pmod{200}$	[3,0,2,0]	401
24	$n \equiv 93 \pmod{400}$	[4,0,2,0]	1601
25	$n \equiv 293 \pmod{400}$	[4,0,2,0]	82471201
26	$n \equiv 153 \pmod{200}$	[3,0,2,0]	3173389601
27	$n \equiv 173 \pmod{400}$	[4,0,2,0]	25601
28	$n \equiv 373 \pmod{400}$	[4,0,2,0]	p_{28}
29	$n \equiv 193 \pmod{200}$	[3,0,2,0]	2787601
30	$n \equiv 59 \pmod{160}$	[5,0,1,0]	44479210368001
31	$n \equiv 233 \pmod{336}$	[4,1,0,1]	2017
32	$n \equiv 169 \pmod{240}$	[4,1,1,0]	46908728641
33	$n \equiv 149 \pmod{280}$	[3,0,1,1]	p_{33}
34	$n \equiv 65 \pmod{224}$	[5,0,0,1]	358429848460993
35	$n \equiv 177 \pmod{224}$	[5,0,0,1]	2689
36	$n \equiv 29 \pmod{210}$	[1,1,1,1]	1564921
37	$n \equiv 253 \pmod{336}$	[4,1,0,1]	25629623713
38	$n \equiv 113 \pmod{224}$	[5,0,0,1]	183076097
39	$n \equiv 289 \pmod{480}$	[5,1,1,0]	23041
40	$n \equiv 1429 \pmod{1680}$	[4,1,1,1]	4841172001
41	$n \equiv 69 \pmod{560}$	[4,0,1,1]	p_{41}
42	$n \equiv 209 \pmod{224}$	[5,0,0,1]	449
43	$n \equiv 769 \pmod{1120}$	[5,0,1,1]	86800001
44	$n \equiv 349 \pmod{560}$	[4,0,1,1]	557761
45	$n \equiv 41 \pmod{336}$	[4,1,0,1]	1538595959564161
46	$n \equiv 89 \pmod{840}$	[3,1,1,1]	755667361
47	$n \equiv 229 \pmod{560}$	[4,0,1,1]	4481
48	$n \equiv 369 \pmod{1120}$	[5,0,1,1]	16824641
49	$n \equiv 509 \pmod{560}$	[4,0,1,1]	736961

Corollary 26. *There is a set $\mathcal{T}'$ of positive integers r having positive asymptotic density with the following properties*:

(i) *If $r \in \mathcal{T}'$, then $6 \mid r$.*
(ii) *For each $r \in \mathcal{T}'$, there exist infinitely many positive odd numbers k such that each of the numbers*

$$k^r - 2^n,\ k^r 2^n - 1$$

has at least two distinct prime factors for each positive integer n.

In conclusion, we note that the r that are in the sets $\mathcal{T}$ and $\mathcal{T}'$ of Corollaries 22 and 26 are not covered by the work of Chen in [3].

References

[1] A.S. Bang, Taltheoretiske Undersgelser, Tidsskrift for Mat. 4 (1886) 70–80, 130–137.
[2] J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, S.S. Wagstaff Jr., Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$, Up to High Powers, third ed., Contemp. Math., vol. 22, Amer. Math. Soc., Providence, 2002 (available online).
[3] Y.-G. Chen, On integers of the forms $k^r - 2^n$ and $k^r 2^n + 1$, J. Number Theory 98 (2003) 310–319.
[4] Y.-G. Chen, On integers of the forms $k \pm 2^n$ and $k2^n \pm 1$, J. Number Theory 125 (2007) 14–25.
[5] H. Darmon, A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. 27 (1995) 513–544.
[6] A. de Polignac, Recherches nouvelles sur les nombres premiers, C. R. Acad. Sci. Paris Math. 29 (1849) 397–401, 738–739.
[7] P. Erdős, On integers of the form $2^k + p$ and some related problems, Summa Brasil. Math. 2 (1950) 113–123.
[8] M. Filaseta, Coverings of the integers associated with an irreducibility theorem of A. Schinzel, in: Number Theory for the Millennium, II, Urbana, IL, 2000, A K Peters, Natick, MA, 2002, pp. 1–24.
[9] R.K. Guy, Unsolved Problems in Number Theory, third ed., Problem Books in Math., Springer-Verlag, New York, 2004.
[10] A.S. Izotov, A note on Sierpiński numbers, Fibonacci Quart. 33 (1995) 206–207.
[11] H. Riesel, Några stora primtal, Elementa 39 (1956) 258–260.
[12] W. Sierpiński, Sur un problème concernant les nombres $k \cdot 2^n + 1$, Elem. Math. 15 (1960) 73–74.
[13] R.G. Stanton, H. Williams, Computation of some number-theoretic coverings, in: Combinatorial Mathematics, VIII, Geelong, 1980, in: Lecture Notes in Math., vol. 884, Springer, 1981, pp. 8–13.
[14] J.G. van der Corput, On de Polignac's conjecture, Simon Stevin 27 (1950) 99–105.