Nonlinear Sierpiński and Riesel numbers

Carrie Finch\textsuperscript{a}, Joshua Harrington\textsuperscript{b}, Lenny Jones\textsuperscript{c,}\textsuperscript{*}

\textsuperscript{a} Mathematics Department, Washington and Lee University, Lexington, VA 24450, United States
\textsuperscript{b} Department of Mathematics, University of South Carolina, Columbia, SC 29208, United States
\textsuperscript{c} Department of Mathematics, Shippensburg University, Shippensburg, PA 17257, United States

A R T I C L E   I N F O

Article history:
Received 19 September 2011
Revised 10 June 2012
Accepted 30 August 2012
Available online xxxx
Communicated by Michael A. Bennett

MSC:
11B83
11Y05

Keywords:
Sierpiński number
Riesel number
Composite number

ABSTRACT

In 1960, Sierpiński proved that there exist infinitely many odd positive integers \( k \) such that \( k \cdot 2^n + 1 \) is composite for all positive integers \( n \). Such values of \( k \) are known as Sierpiński numbers. Extending the ideas of Sierpiński to a nonlinear situation, Chen showed that there exist infinitely many positive integers \( k \) such that \( k' \cdot 2^n + d \) is composite for all positive integers \( n \), where \( d \in \{-1, 1\} \), provided that \( r \) is a positive integer with \( r \not\equiv 0, 4, 6, 8 \pmod{12} \). Filaseta, Finch and Kozek improved Chen’s result by completely lifting the restrictions on \( r \) when \( d = 1 \), and they asked if a similar result exists if \( k' \) is replaced by \( f(k) \), where \( f(x) \) is an arbitrary nonconstant polynomial in \( \mathbb{Z}[x] \). In this article, we address this question when \( f(x) = ax^r + bx + c \in \mathbb{Z}[x] \). In particular, we show, for various values of \( a, b, c, d \) and \( r \), that there exist infinitely many positive integers \( k \) such that \( f(k) \cdot 2^n + d \) is composite for all integers \( n \geq 1 \). When \( d = 1 \) or \( -1 \), we refer to such values of \( k \) as nonlinear Sierpiński or nonlinear Riesel numbers, respectively.

© 2012 Published by Elsevier Inc.

1. Introduction

The following concept, originally due to Erdős [6], is instrumental in establishing all results in this article.

\textbf{Definition 1.1.} A \textit{covering} of the integers is a system of congruences \( n \equiv z_i \pmod{m_i} \) such that every integer satisfies at least one of the congruences. A covering is said to be a \textit{finite covering} if the covering contains only finitely many congruences.

\* Corresponding author.
E-mail address: ljone@ship.edu (L. Jones).

0022-314X/$ – see front matter © 2012 Published by Elsevier Inc.
http://dx.doi.org/10.1016/j.jnt.2012.08.019
Remark 1.2. Since all coverings in this paper are finite coverings, we omit the word “finite”.

Quite often when a covering is used to solve a problem, there is a set of prime numbers associated with the covering. In the situations occurring in this article, for each congruence \( n \equiv z_i \pmod{m_i} \) in the covering, there exists a corresponding prime \( p_i \), such that \( 2^{m_i} \equiv 1 \pmod{p_i} \), and \( p_j \neq p_i \) for all \( j \neq i \). Because of this correspondence, we indicate the covering using a set \( C \) of ordered triples \((z_i, m_i, p_i)\). We abuse the definition of a covering slightly by referring to the set \( C \) as a “covering”.

In 1960, using a particular covering, Sierpiński [16] published a proof of the fact that there exist infinitely many odd positive integers \( k \) such that \( k \cdot 2^n + 1 \) is prime for all natural numbers \( n \). Any such value of \( k \) is called a Sierpiński number. Since then, several authors [1–5,7–13] have investigated generalizations and variations of this result. We should also mention a paper of Riesel [15], which actually predates the paper of Sierpiński, in which Riesel proves a similar result for the sequence \( k \cdot 2^n - 1 \). We include a proof of Sierpiński’s original theorem since it provides an easy introduction to the techniques used in this paper.

Theorem 1.3. (See Sierpiński [16].) There exist infinitely many odd positive integers \( k \) such that \( k \cdot 2^n + 1 \) is composite for all integers \( n \geq 1 \).

Proof. Consider the covering

\[ C = \{(1, 2, 3), (2, 4, 5), (4, 8, 17), (8, 16, 257), (16, 32, 65537), (32, 64, 641), (0, 64, 6700417)\} \]

To illustrate exactly how \( C \) is used to prove this result, start with the triple \((1, 2, 3) \in C\). We want \( k \cdot 2^n + 1 \equiv 0 \pmod{3} \) when \( n \equiv 1 \pmod{2} \). But \( k \cdot 2^n + 1 \equiv k \cdot 2 + 1 \pmod{3} \) when \( n \equiv 1 \pmod{2} \), which tells us that \( k \cdot 2^n + 1 \) is divisible by 3 if \( k \equiv 1 \pmod{3} \). Continuing in this manner gives us the system

\[
\begin{align*}
    k &\equiv 1 \pmod{3}, \\
    k &\equiv 1 \pmod{5}, \\
    k &\equiv 1 \pmod{17}, \\
    k &\equiv 1 \pmod{257}, \\
    k &\equiv 1 \pmod{65537}, \\
    k &\equiv 1 \pmod{641}, \\
    k &\equiv -1 \pmod{6700417}.
\end{align*}
\]

Since we require that \( k \) be odd, we add the congruence \( k \equiv 1 \pmod{2} \) to our system, and then using the Chinese remainder theorem, we get the solution

\[ k \equiv 15511380746462593381 \pmod{2 \cdot 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 \cdot 641 \cdot 6700417}. \]

Therefore, for any integer \( n \geq 1 \) and any such \( k \), we have that at least one prime from the set \( \{3, 5, 17, 257, 641, 65537, 6700417\} \) is a divisor of \( k \cdot 2^n + 1 \). \( \square \)

In this article we are concerned with variations of Theorem 1.3 which are nonlinear in nature, replacing the variable \( k \) with a nonlinear polynomial in \( k \). The investigation into such nonlinear situations began with Chen [4], who showed that for any positive integer \( r \neq 0, 4, 6, 8 \pmod{12} \), there exist infinitely many odd positive integers \( k \) such that \( k^r \cdot 2^n + d \) is composite for all integers \( n \geq 1 \), where \( d \in \{-1, 1\} \). He conjectured that the result is true for all positive integers \( r \). Recently, Filaseta,
Finch and Kozek [8] have been able to lift all restrictions on $r$ when $d = 1$ to verify Chen's conjecture in this case, and they showed that the conjecture is also true for $r = 4$ and $r = 6$ when $d = −1$. (More recently, Finch, Groth, Jones and Mugabe have verified Chen's conjecture for $r = 8$ and $r = 12$ when $d = −1$.) In their paper [8], Filaseta, Finch and Kozek also asked if infinitely many positive integers $k$ can be found such that $f(k) \cdot 2^{n} + 1$ is composite for all integers $n \geq 1$, where $f(x)$ is any nonconstant polynomial in $\mathbb{Z}[x]$. In this article we focus on the situation when $f(x) = ax^r + bx + c \in \mathbb{Z}[x]$, where $a \geq 1$. If, for such a particular polynomial $f(x)$ and an integer $d$, we can prove there exist infinitely many positive integers $k$ such that $f(k) \cdot 2^{n} + d$ is composite for all integers $n \geq 1$, then we say that particular value of $r$ can be captured. The $r$-density for a particular polynomial $f(x)$ is simply the density of the set of captured values of $r$. Our main focus in this article is when $d \in \{−1, 1\}$. For any nonlinear polynomial $f(x)$, we call the integer $k$ a nonlinear Sierpiński number if $f(k) \cdot 2^{n} + 1$ is composite for all integers $n \geq 1$, and a nonlinear Riesel number if $f(k) \cdot 2^{n} − 1$ is composite for all integers $n \geq 1$. A list of the results established in this article follows.

**Theorem 1.4.** Let $f(x) = x^r + x + c \in \mathbb{Z}[x]$, where $0 \leq c \leq 100$.

- **(Nonlinear Sierpiński Numbers)** For any positive integer $r$ and any

\[
c \in \{1, 3, 4, 5, 6, 8, 10, 11, 12, 15, 17, 19, 20, 22, 26, 27, 29, 31, 32, 34, 38, 40, 41, 45, 46, 47, 48, 50, 53, 55, 57, 59, 60, 62, 64, 67, 68, 71, 74, 76, 78, 81, 82, 83, 85, 87, 88, 89, 92, 94, 95, 96, 97\},
\]

there exist infinitely many positive integers $k$ such that $f(k) \cdot 2^{n} + 1$ is composite for all integers $n \geq 1$.

- **(Nonlinear Riesel Numbers)** For any positive integer $r$, and any

\[
c \in \{2, 5, 8, 9, 11, 12, 13, 14, 16, 17, 20, 21, 22, 23, 24, 27, 29, 30, 32, 35, 36, 37, 38, 39, 40, 41, 44, 50, 51, 53, 56, 58, 59, 60, 61, 62, 65, 66, 67, 68, 69, 71, 72, 74, 77, 80, 81, 82, 83, 84, 85, 86, 87, 89, 92, 93, 95, 97, 98\},
\]

there exist infinitely many positive integers $k$ such that $f(k) \cdot 2^{n} − 1$ is composite for all integers $n \geq 1$.

**Theorem 1.5.** Let $f(x) = ax^r + c \in \mathbb{Z}[x]$, where $a \geq 1$, and let $d$ be an odd integer. If $a$ is not divisible by any element in the set of primes

\[
\{3, 5, 7, 11, 13, 17, 19, 37, 41, 73, 257, 641, 65537, 286721, 3602561, 96645260801, 67280421310721\},
\]

then there exist infinitely many positive integers $k$ such that $f(k) \cdot 2^{n} + d$ is composite for all integers $n \geq 1$, either when $r \equiv \pm 1$ (mod 6), or when both $r \equiv 3$ (mod 6) and $r$ is not divisible by any element in the set of primes

\[
\{5, 7, 11, 13, 29, 47, 373, 433, 23669, 2998279\}.
\]

**Theorem 1.6.** Let $f(x) = x^r + 1$.

- **(Nonlinear Sierpiński Numbers)** There exist infinitely many positive integers $k$ such that $f(k) \cdot 2^{n} + 1$ is composite for all integers $n \geq 1$ when either $r \not\equiv 0$ (mod 8) and $r \not\equiv 0$ (mod 17449), or when $r \not\equiv z$ (mod 30) where $z \in \{0, 6, 12, 15, 18, 24\}$.
- (Nonlinear Riesel Numbers) There exist infinitely many positive integers $k$ such that $f(k) \cdot 2^n - 1$ is composite for all integers $n \geq 1$ when $r \neq 0 \pmod{6}$.

**Theorem 1.7.**

- Let $f(x) = x^r + 1$. There exists a set $S$ of $r$-density $8/33$, such that for each $r \in S$, there exist infinitely many positive integers $k$ for which $f(k)$ is odd, and both $f(k) \cdot 2^n + 1$ and $f(k) \cdot 2^n - 1$ are composite for all integers $n \geq 1$.
- Let $f(x) = x^r + x + 1$. There exists a set $S$ with $r$-density approximately $0.47$, such that for each $r \in S$, there exist infinitely many positive integers $k$ for which $f(k)$ is odd, and both $f(k) \cdot 2^n + 1$ and $f(k) \cdot 2^n - 1$ are composite for all integers $n \geq 1$.

For each positive integer $c \leq 100$ not listed in the Sierpiński part of Theorem 1.4, the $r$-density is no smaller than $2/3$, and for each positive integer $c \leq 100$ not listed in the Riesel part, the $r$-density is no smaller than $0.749$. Since the $r$-densities for the Riesel part and Sierpiński part of Theorem 1.4 are similar, we provide in Table 1 the approximate $r$-densities only for the Sierpiński part. The value of $c = 100$ here is simply an arbitrary stopping point. The methods used in the proof of Theorem 1.4 can be applied to larger values of $c$ as well as other polynomials.

Theorem 1.5 is a more general theorem in that the values of the parameters $a$, $c$ and $d$ are not fixed. In some sense, Theorem 1.5 generalizes the work of Filaseta, Finch and Kozek [8] since their work is the special case of $a = d = 1$ and $c = 0$ in Theorem 1.5. However, we are not able to achieve an $r$-density of $1$ in this case using our methods. In the specific case of $a = c = d = 1$ in Theorem 1.5, the $r$-density is slightly less than $0.42$. Applying the techniques used to prove Theorem 1.4 to this special case, this density improves to $2/3$. The proof of the first part of Theorem 1.6 uses a different approach and improves this density to slightly more than $0.94$. Although we do not provide the details here, it can be shown that by combining all of these results, the $r$-density in this case can be improved to slightly less than $0.96$.

Theorem 1.7 addresses the following natural question. Given a specific polynomial $f(x)$, do there exist infinitely many positive integers $k$ such that both $f(k) \cdot 2^n + 1$ and $f(k) \cdot 2^n - 1$ are simultaneously composite for all integers $n \geq 1$? That is, are there positive integers that are both nonlinear Sierpiński numbers and nonlinear Riesel numbers? For certain polynomials and sets with positive $r$-density, this question is answered affirmatively in Section 3 where the proof of Theorem 1.7 is given.

**Remark 1.8.** Computer computations in this article were done using either MAGMA, Maple or a C++ program written by Professor Simon Levy in the computer science department at Washington and Lee University.

2. **Proofs of the theorems**

We begin with some preliminaries from finite group theory that are useful in establishing some of the main results in this paper.

**Lemma 2.1.** Let $G$ be a finite abelian group, and suppose that $r$ is a positive integer such that $\gcd(|G|, r) = 1$. Then the map $\theta_r : G \rightarrow G$ defined by $\theta_r(x) = x^r$ is an automorphism of $G$.

**Proof.** Since $G$ is abelian, $\theta_r$ is clearly a homomorphism. The kernel of $\theta$ is $K = \{x \in G \mid x^r = 1\}$. Since the order of any $x \in K$ divides both $r$ and $|G|$, it follows that $K$ is trivial, which proves the lemma. \(\square\)

The following corollary is immediate from Lemma 2.1.

**Corollary 2.2.** Let $p$ be a prime, and let $(\mathbb{Z}_p)^*$ denote the group of units modulo $p$. For any positive integer $r$ with $\gcd(r, p - 1) = 1$, let $\theta_r$ be the automorphism of $(\mathbb{Z}_p)^*$ defined by $\theta_r(x) = x^r$, and let $\hat{\theta}_r$ be the extension
of the map \( \theta_r \) to the commutative multiplicative monoid \( \mathbb{Z}_p \) by defining \( \widehat{\theta}_r(0) = 0 \). If \( \gcd(r, p - 1) = 1 \), then \( \widehat{\theta}_r \) is a bijection on \( \mathbb{Z}_p \).

The next corollary extends the previous ideas to generate subsets \( S \) of \( \mathbb{Z}_p \) which are fixed under \( \widehat{\theta}_r \) for certain values of \( r \).

**Corollary 2.3.** Let \( p \) be a prime, and suppose that \( p - 1 = q^2m \), where \( q \) is a prime such that \( m \equiv 0 \pmod{q} \). Let

\[
S = \widehat{\theta}_{q^2}(\mathbb{Z}_p) = (\widehat{\theta}_q)^2(\mathbb{Z}_p).
\]

Then \( \widehat{\theta}_q(S) = S \). Moreover, each such set \( S \) is nonempty since \( 0 \in S \).

**Proof.** The kernel of the homomorphism \( \theta_q \) on \( \theta_{q^2}(\mathbb{Z}_p^*) \) is trivial. \( \square \)

The following lemma is used in the proofs of both Theorem 1.5 and Theorem 1.6.

**Lemma 2.4.** Let \( C = \{(z_i, m_i, p_i)\} \) be a covering. Let \( r \) be a positive integer such that \( \gcd(r, p_i - 1) = 1 \) for all \( i \), and let \( a > 0 \) be an integer that is not divisible by \( p_i \) for all \( i \). Then, for any integers \( c \) and \( d \), with \( d \) odd, there exist infinitely many positive integers \( k \) such that \((a \cdot k^r + c) \cdot 2^n + d \) is composite for all integers \( n \geq 1 \).

**Proof.** Let \((z_i, m_i, p_i) \in C \). For each \( i \), \( \widehat{\theta}_r \) is a bijection on \( \mathbb{Z}_{p_i} \) by Corollary 2.2, and since \( a \) is invertible mod \( p_i \), we have that there exists \( v_i \in \mathbb{Z}_{p_i} \) such that

\[
v_i^r \equiv a^{-1}(-d \cdot 2^{-n} - c) \equiv a^{-1}(-d \cdot 2^{-z_i} - c) \pmod{p_i}.
\]

Then we use the Chinese remainder theorem to solve the system of congruences \( k \equiv v_i \pmod{p_i} \). Since \( C \) is a covering, we have shown that, for any positive integer \( n \), the term \((a \cdot k^r + c) \cdot 2^n + d \) is divisible by at least one prime \( p_i \), which completes the proof of the lemma. \( \square \)

### 2.1. Theorem 1.4

We first outline in more generality the procedure used in the proof of Theorem 1.4. Let \( C = \{(z_i, m_i, p_i)\} \) be a covering, where \( p_i \) is odd for all \( i \). Recall that \( 2^{m_i} \equiv 1 \pmod{p_i} \), and that no prime \( p_i \) is repeated. Then \( 2^n \equiv 2^{z_i} \pmod{p_i} \) when \( n \equiv z_i \pmod{m_i} \). Define \( L_C := \text{lcm}_i(p_i - 1) \). Note that \( L_C \) is independent of the list of residues in \( C \). Let

\[
f(x) = x^r + x^e + a_{e-1}x^{e-1} + \cdots + a_1x + a_0
\]

be a nonconstant polynomial with integer coefficients, where \( e \) is a fixed nonnegative integer. The coefficient on \( x^e \) is 1 to exclude the possibility that \( f(x) \equiv 0 \pmod{p_i} \) for some \( i \), when \( r \leq e \). We wish to determine the values of \( r \) for which there exist infinitely many positive integers \( k \) such that \( s_n := f(k) \cdot 2^n + d \) is composite for all integers \( n \geq 1 \), for a fixed \( d \in \{-1, 1\} \). We use \( C \) to examine the behavior of \( s_n \) modulo each \( p_i \), and then piece together the results using the Chinese remainder theorem. We only need to check values of \( r \) with \( 0 \leq r \leq L_C - 1 \). We proceed as follows. Let \( r \) be a fixed integer with \( 0 \leq r \leq L_C - 1 \). Then, for each \( i \), when \( r \leq e \), we calculate the values \( f(k) \), with \( 0 \leq k \leq p_i - 1 \), to determine whether there is a \( k \) such that \( f(k) \equiv -d2^{-z_i} \pmod{p_i} \). If so, then we know there exists \( \beta_i \) such that \( k \equiv \beta_i \pmod{p_i} \) is a solution to \( s_n \equiv 0 \pmod{p_i} \) when \( n \equiv z_i \pmod{m_i} \). Continuing in this manner, if \( \beta_i \) exists for each \( i \), then we can use the Chinese remainder theorem to solve the resulting system of congruences in \( k \). Thus, in this case, we have captured that particular value of \( r \), which contributes a value of \( 1/L_C \) to the total density. This process can be repeated for every list of residues for which a covering exists. In addition, this process can be repeated for coverings
with different lists of moduli. To combine all of these results in a sensible manner, one must take care since the values of \( r \) captured using one list of moduli must be “meshed” with the values of \( r \) captured using a different list of moduli. This can be done by examining values of \( r \) (mod \( L \)), where \( L = \text{lcm}_C L_j \), for all coverings \( C \) under consideration. Then the density of the set of captured values of \( r \) will be the cardinality of the union of these various sets divided by \( L \). We call this density a Sierpiński \( r \)-density or Riesel \( r \)-density for this particular polynomial \( f(x) \), depending on whether \( d = 1 \) or \( d = -1 \), respectively.

**Remark 2.5.** Note that if \( a_0 \equiv 1 \) (mod 2) or \( a_{e-1} + \cdots + a_1 + a_0 \equiv 1 \) (mod 2) in (2.1), then adding, respectively, the additional congruence \( k \equiv 0 \) (mod 2) or \( k \equiv 1 \) (mod 2) to the system of congruences for \( k \) will ensure that \( f(k) \) is odd.

**Proof of Theorem 1.4.** Consider the following lists:

\[
M_1 = [2, 3, 4, 9, 12, 18, 36], \quad P_1 = [3, 7, 5, 73, 13, 19, 37],
\]
\[
M_2 = [2, 3, 4, 8, 12, 24], \quad P_2 = [3, 7, 5, 17, 13, 241],
\]
\[
M_3 = [2, 3, 4, 5, 10, 12, 15, 20, 60], \quad P_3 = [3, 7, 5, 31, 11, 13, 151, 41, 61],
\]

where each \( M_j \) is a list of moduli to be used to construct a covering, and \( P_j \) is the list of corresponding primes. Here \( L = 3600 \). Let \( N_j \) be the total number of coverings having \( M_j \) as the list of moduli. Then \( N_1 = 144, N_2 = 48 \) and \( N_3 = 2880 \). For each \( d \in \{-1, 1\} \), apply the procedure outlined above to the polynomials \( f(x) = x^r + x + c \), with \( 0 \leq c \leq 100 \), using these 3072 coverings to get the results contained in the statement of the theorem. □

It may be that not all lists of moduli \( M_j \) above, or all coverings for a particular list of moduli, are needed to achieve the results for a certain value of \( c \) in Theorem 1.4. For example, it can be shown for \( c = 1 \) that only 24 of the coverings with the moduli \( M_1 \) are needed to prove that the Sierpiński \( r \)-density is 1.

<table>
<thead>
<tr>
<th>( c )</th>
<th>( r )-Density</th>
<th>( c )</th>
<th>( r )-Density</th>
<th>( c )</th>
<th>( r )-Density</th>
<th>( c )</th>
<th>( r )-Density</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.8247</td>
<td>27</td>
<td>0.9997</td>
<td>51</td>
<td>0.8333</td>
<td>72</td>
<td>0.8314</td>
</tr>
<tr>
<td>2</td>
<td>0.8333</td>
<td>28</td>
<td>0.8333</td>
<td>52</td>
<td>0.9164</td>
<td>73</td>
<td>0.9994</td>
</tr>
<tr>
<td>3</td>
<td>0.9997</td>
<td>30</td>
<td>0.8331</td>
<td>54</td>
<td>0.7500</td>
<td>75</td>
<td>0.9167</td>
</tr>
<tr>
<td>7</td>
<td>0.8333</td>
<td>33</td>
<td>0.9942</td>
<td>56</td>
<td>0.8333</td>
<td>77</td>
<td>0.8333</td>
</tr>
<tr>
<td>9</td>
<td>0.6667</td>
<td>34</td>
<td>0.9997</td>
<td>57</td>
<td>0.9997</td>
<td>79</td>
<td>0.8333</td>
</tr>
<tr>
<td>10</td>
<td>0.9997</td>
<td>35</td>
<td>0.8333</td>
<td>58</td>
<td>0.8331</td>
<td>80</td>
<td>0.9969</td>
</tr>
<tr>
<td>13</td>
<td>0.8314</td>
<td>36</td>
<td>0.9167</td>
<td>60</td>
<td>0.9997</td>
<td>81</td>
<td>0.9997</td>
</tr>
<tr>
<td>14</td>
<td>0.8331</td>
<td>37</td>
<td>0.8331</td>
<td>61</td>
<td>0.9942</td>
<td>84</td>
<td>0.6667</td>
</tr>
<tr>
<td>15</td>
<td>0.9997</td>
<td>38</td>
<td>0.9997</td>
<td>62</td>
<td>0.9997</td>
<td>86</td>
<td>0.8333</td>
</tr>
<tr>
<td>16</td>
<td>0.8333</td>
<td>39</td>
<td>0.7500</td>
<td>63</td>
<td>0.8333</td>
<td>87</td>
<td>0.9997</td>
</tr>
<tr>
<td>20</td>
<td>0.8333</td>
<td>40</td>
<td>0.9997</td>
<td>65</td>
<td>0.8331</td>
<td>90</td>
<td>0.9167</td>
</tr>
<tr>
<td>21</td>
<td>0.8333</td>
<td>42</td>
<td>0.7500</td>
<td>66</td>
<td>0.9167</td>
<td>91</td>
<td>0.8331</td>
</tr>
<tr>
<td>22</td>
<td>0.9997</td>
<td>43</td>
<td>0.9975</td>
<td>67</td>
<td>0.9997</td>
<td>93</td>
<td>0.8331</td>
</tr>
<tr>
<td>23</td>
<td>0.8333</td>
<td>44</td>
<td>0.8319</td>
<td>69</td>
<td>0.7494</td>
<td>98</td>
<td>0.8331</td>
</tr>
<tr>
<td>24</td>
<td>0.7478</td>
<td>49</td>
<td>0.8333</td>
<td>70</td>
<td>0.8317</td>
<td>99</td>
<td>0.7497</td>
</tr>
<tr>
<td>25</td>
<td>0.9769</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100</td>
<td>0.8286</td>
</tr>
</tbody>
</table>

### 2.2. Theorem 1.5

The strategy here is to use Lemma 2.4 exclusively to determine which values of \( r \) can be captured in the general situation \((a \cdot k^r + c) \cdot 2^n + d\), where \( a, c, d \in \mathbb{Z} \), with \( a > 0 \) and \( d \) odd. However, since a corresponding odd prime \( p_i \) in any covering is such that \( p_i - 1 \equiv 0 \) (mod 2), Lemma 2.4 alone is ineffective in addressing any even value of \( r \).
Remark 2.6. Note that if \( c \equiv 1 \pmod{2} \) or \( a + c \equiv 1 \pmod{2} \), then adding, respectively, the additional congruence \( k \equiv 0 \pmod{2} \) or \( k \equiv 1 \pmod{2} \) to the system of congruences for \( k \) will ensure that \( f(k) = a \cdot k^r + c \) is odd.

Proof of Theorem 1.5. Suppose first that \( r \equiv \pm 1 \pmod{6} \), and consider the covering

\[
C_1 = \{(1, 2, 3), (0, 3, 7), (0, 4, 5), (5, 9, 73), (10, 12, 13), (2, 18, 19), (26, 36, 37)\}.
\]

For each \((z_i, m_i, p_i) \in C_1\), note that \( a \not\equiv 0 \pmod{p_i} \) and that \( p_i - 1 \not\equiv 0 \pmod{q} \) for any prime \( q \geq 5 \). Since \( \gcd(r, 6) = 1 \), the first part of the theorem is established.

Now suppose that \( r \equiv 3 \pmod{6} \), and consider the covering

\[
C_2 = \{(1, 2, 3), (0, 4, 5), (2, 8, 17), (6, 10, 11), (14, 16, 257), (18, 20, 41),
(6, 32, 65537), (22, 64, 641), (118, 128, 67280421310721),
(310, 320, 3602561), (182, 640, 286721), (54, 640, 96645260801)\}.
\]

It is easy to check using a computer that \( C_2 \) is indeed a covering. For each \((z_i, m_i, p_i) \in C_2\), note that \( a \not\equiv 0 \pmod{p_i} \). In addition, the union of the sets of odd prime divisors of \( p_i - 1 \) for all \( i \) is precisely

\[\{5, 7, 11, 13, 29, 47, 373, 433, 23669, 2998279\}.
\]

Invoking Lemma 2.4 completes the proof. \( \Box \)

2.3. Theorem 1.6

While the hypotheses of Lemma 2.4 are sufficient in addressing a particular value of \( r \), they are not necessary, as we see in Theorem 1.6 where we consider the special case of \( f(x) = x^r + 1 \).

Proof of Theorem 1.6. We first prove the Sierpiński half of the theorem. Suppose that \( r \) is not divisible by either 8 or 17449, and consider the covering

\[
C = \{(0, 2, 3), (1, 4, 5), (3, 8, 17), (7, 16, 257), (15, 32, 65537),
(31, 64, 641), (63, 64, 6700417)\}.
\]

The covering \( C \) gives rise to the system of congruences

\[
k^r \equiv 1 \pmod{3},
\]
\[
k^r \equiv 1 \pmod{5},
\]
\[
k^r \equiv 1 \pmod{17},
\]
\[
k^r \equiv 1 \pmod{257},
\]
\[
k^r \equiv 1 \pmod{65537},
\]
\[
k^r \equiv 1 \pmod{641},
\]
\[
k^r \equiv -3 \pmod{6700417}.
\]
It is clear that $k \equiv 1 \pmod{p_i}$ is a solution to each of the first six congruences above. To see that the last congruence has a solution, first note that

$$(-3)^{6700416/12} \equiv 1 \pmod{6700417}.$$ 

Let $d = \gcd(r, 6700416)$. Since $r \not\equiv 0 \pmod{8}$ and $r \not\equiv 0 \pmod{17449}$, we have that $d$ divides 12. Thus,

$$1 \equiv 1 \frac{12}{d} \equiv (-3)^{6700416/12} \pmod{6700417}.$$ 

Hence, it follows from the generalization of Euler’s criterion for $r$th power residues [14] that there exists a value $k$ such that

$$k^r \equiv -3 \pmod{6700417}.$$ 

Using the Chinese remainder theorem completes the proof for these values of $r$.

To establish the second part of the Sierpiński half of Theorem 1.6, first consider the covering

$$C_1 = \{1, 2, 3, 1, 3, 7, 2, 4, 5, 3, 9, 73, 8, 12, 13, 0, 18, 19, 24, 36, 37\}.$$ 

Since $p_i - 1 \equiv 0 \pmod{2}$ for each $p_i$ in $C_1$, we see that $\theta_2$ is not an automorphism of $(\mathbb{Z}/p_i)\times$. However, for each $i$, by Corollary 2.3, there exists a nonempty subset $S_i$ of $\mathbb{Z}/p_i$ such that

$$(\hat{\theta}_2)^j(S_i) = \hat{\theta}_2(S_i) = S_i$$

for all positive integers $j$. That is, for any nonnegative integers $j$ and $n$, there exists $u_i \in \mathbb{Z}/p_i$ such that $(u_i^{2^j} + 1) \cdot 2^n + 1 \equiv 0 \pmod{p_i}$ provided that $-2^{-n} - 1 \equiv -2^{-z_i} - 1 \pmod{p_i}$ is an element of $S_i$ for each value of $i$.

Now let $r = 2^j m$, where $\gcd(m, 6) = 1$ and $j \geq 0$. Note that the set of all prime divisors of $p_i - 1$ for all $p_i$ in $C_1$ is $\{2, 3\}$. Therefore, for each $i$, there exists, by Corollary 2.2, $v_i \in \mathbb{Z}/p_i$ such that $v_i^{m} \equiv u_i \pmod{p_i}$. Consequently,

$$v_i^r = v_i^{2^j m} = \left(v_i^m\right)^{2^j} \equiv (u_i)^{2^j} \equiv -2^{-z_i} - 1 \pmod{p_i}.$$ 

Thus, we can use the Chinese remainder theorem to solve the system of seven congruences $k \equiv v_i \pmod{p_i}$ to get infinitely many positive integers $k$ such that $(k^r + 1) \cdot 2^n + 1$ is composite for all integers $n \geq 1$. The values of $r \pmod{30}$ captured in this stage are

$$\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26, 28, 29\}.$$ 

Next, consider the covering

$$C_2 = \{(1, 2, 3), (0, 4, 5), (0, 5, 31), (2, 8, 17), (4, 10, 11), (10, 12, 13), (6, 15, 151), (18, 20, 41), (14, 24, 241), (42, 60, 61)\}.$$ 

Here we have that $p_i - 1 \equiv 0 \pmod{3}$ for some values of $i$ so that $\theta_3$ is not an automorphism of $(\mathbb{Z}/p_i)\times$ for these values of $i$. However, as was the case for $\theta_2$ above, by Corollary 2.3 there exists a nonempty subset $S_i$ of $\mathbb{Z}/p_i$ such that
for all positive integers \( j \). That is, for any nonnegative integers \( j \) and \( n \), there exists \( u_i \in \mathbb{Z}_{p_i} \) such that 
\[(u_i^{3j} + 1) \cdot 2^n + 1 \equiv 0 \pmod{p_i}\]
provided that \(-2^{-n} - 1 \equiv 2^{-z_i} - 1 \pmod{p_i} \) is an element of \( S_i \) for each value of \( i \).

Now let \( r = 3^jm \), where \( \gcd(m, 30) = 1 \) and \( j \geq 0 \). Note that the set of all prime divisors of \( p_i - 1 \) for all \( i \) is \( \{2, 3, 5\} \). Hence, for each \( i \), Corollary 2.2 implies the existence of \( v_i \in \mathbb{Z}_{p_i} \) such that \( v_i^{3j} \equiv u_i \pmod{p_i} \). Therefore,
\[v_i = v_i^{3jm} = (v_i^{m})^{3j} \equiv (u_i)^{3j} \equiv -2^{-z_i} - 1 \pmod{p_i}.
\]
Thus, we can apply the Chinese remainder theorem to solve the system of eleven congruences \( k \equiv v_i \pmod{p_i} \) to get infinitely many positive integers \( k \) such that \( (k^2 + 1) \cdot 2^n + 1 \) is composite for all integers \( n \geq 1 \). The values of \( r \pmod{30} \) captured in this stage are \( \{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29\} \).

Combining the results from the two coverings used here completes the proof of the Sierpiński part of the theorem.

Since the Riesel half of this theorem can be established using either the methods used in the proof of Theorem 1.4 or the methods used in the proof of the second part of the Sierpiński half of this theorem, we omit the details. \( \Box \)

**Remark 2.7.** The techniques used in the proof of the first part of the Sierpiński half of Theorem 1.6 do not improve the result in the Riesel half of Theorem 1.6.

3. Simultaneous nonlinear Sierpiński and Riesel numbers

In this section we are concerned with determining a set of \( r \) values of positive density for which infinitely many positive integers \( k \) exist such that both \( f(k) \cdot 2^n + 1 \) and \( f(k) \cdot 2^n - 1 \) are composite for all integers \( n \geq 1 \), where \( f(x) = x^r + 1 \) or \( f(x) = x^r + x + 1 \).

**Proof of Theorem 1.7.** First let \( f(x) = x^r + 1 \). We use the following coverings:

\[C_S = \{ (0, 2, 3), (1, 3, 7), (8, 9, 73), (11, 18, 19), (5, 36, 37), (23, 36, 109), (4, 5, 31), (5, 10, 11), (12, 15, 151), (21, 30, 331), (33, 60, 61), (3, 60, 1321) \}\]

and

\[C_R = \{ (1, 2, 3), (0, 4, 5), (6, 8, 17), (10, 16, 257), (6, 12, 13), (2, 24, 241), (34, 48, 97) \}\]

The covering \( C_S \) is used to construct nonlinear Sierpiński numbers, while the covering \( C_R \) is used to construct nonlinear Riesel Numbers. Since \( k^2 \equiv 1 \pmod{3} \) in both cases, and no other prime in \( C_S \) appears in \( C_R \), these two coverings are consistent, and we can construct a single system of congruences in \( k^2 \) so that any solution \( k \) will be simultaneously a nonlinear Sierpiński number and a nonlinear Riesel number. Let \( \mathcal{P} = \{ p_i - 1 | p_i \in C_S \text{ or } p_i \in C_R \} \). Then, for a fixed value of \( r < \text{lcm}(\mathcal{P}) \), we examine the values of \( k \) with \( 0 \leq k \leq p_i - 1 \) for each prime \( p_i \). This process produces the conclusion of the theorem in this case.

Now, let \( f(x) = x^r + x + 1 \). Using the sets of moduli in \( C_S \) and \( C_R \) above, we construct a set of coverings for the Sierpiński case and a set of coverings for the Riesel case, such that each of the 1592
pairs \((S, R)\), where \(S\) is a Sierpiński covering and \(R\) is a Riesel covering, is consistent as explained above. Let \((S, R)\) be such a consistent Sierpiński–Riesel covering pair. For each element \((z, m, p) \in S\), we first solve the congruence \(x = -2^{-z} - 1 \pmod{p}\). Then we determine the values of \(r\), with \(1 \leq r \leq p - 1\) for which there exists a value of \(k\), with \(0 \leq k \leq p - 1\), such that \(k^r + k = x \pmod{p}\). This process generates a set of “good” \(r\)-values for each prime \(p\). We repeat this procedure for each element \((z', m', p') \in R\), with the modification that in this case we solve the congruence \(x = 2^{-z'} - 1 \pmod{p'}\), and we get a set of “good” \(r\)-values for each prime \(p'\). Thus, we have sets

\[
GS_1, GS_2, \ldots, GS_5, GR_1, GR_2, \ldots, GR_t,
\]

where \(GS_i\) is a set of “good” Sierpiński \(r\)-values, and \(GR_j\) is a set of “good” Riesel \(r\)-values. The next step is to find the intersection of all these sets. We start by finding the intersection of \(GS_1\) and \(GS_2\). Suppose that \(p\) is the prime corresponding to the set \(GS_1\) and \(q\) is the prime corresponding to the set \(GS_2\). For each pair \((a, b) \in GS_1 \times GS_2\), if \(a \equiv b \pmod{g}\), where \(g = \gcd(p - 1, q - 1)\), then we can use the generalized Chinese remainder theorem to find a solution \(x\) to the system \(x \equiv a \pmod{p - 1}\) and \(x \equiv b \pmod{q - 1}\), which gives an element in the intersection \(W = GS_1 \cap GS_2\). Next, we find the intersection \(W \cap GS_3\). We continue in this manner to determine the set of all values of \(r\) captured using this particular pair \((S, R)\). The union of these sets of \(r\)-values for all pairs \((S, R)\) in our collection yields the result of the theorem. \(\square\)

**Remark 3.1.** The technique of using multiple pairs of consistent coverings in the proof of Theorem 1.7 for the case when \(f(x) = x^2 + x + 1\) does not seem to improve the \(r\)-density in the case when \(f(x) = x^2 + 1\).

**Remark 3.2.** The two coverings \(C_S\) and \(C_R\) used in the proof of Theorem 1.7 were used by Filaseta, Finch and Kozek [8] to determine the smallest known positive integer that is simultaneously a Sierpiński number and a Riesel number.

### 4. Comments and conclusions

The methods used in this paper differ from both the approach used previously by Chen, and the approach used by Filaseta, Finch and Kozek. In fact, the techniques used by Filaseta, Finch and Kozek to achieve \(r\)-density 1 are not applicable in Theorem 1.4, Theorem 1.6 and the majority of cases in Theorem 1.5. We should point out that both the paper of Chen [4] and the paper of Filaseta, Finch and Kozek [8] contain the stronger result that each term in the sequence \(k^r \cdot 2^n + 1\) actually has at least two distinct prime divisors. Unfortunately, their methods used to establish this fact seem inapplicable here as well.

### Acknowledgment

The authors thank the referee for the many valuable suggestions that contributed to the improvement of this paper.

### References


