#A61 INTEGERS 21 (2021)

ON BINOMIAL COEFFICIENTS ASSOCIATED WITH SIERPIŃSKI AND RIESEL NUMBERS

Ashley Armbruster
Department of Mathematics, Frostburg State University, Maryland
aarmbruster0@frostburg.edu

Grace Barger
Department of Mathematics, Salem College, North Carolina
grace.barger@salem.edu

Sofya Bykova
Department of Mathematics, Cornell University, New York
sab444@cornell.edu

Tyler Dvorachek
Department of Mathematics, University of Wisconsin-Green Bay, Wisconsin
dvortj19@uwgb.edu

Emily Eckard
Department of Mathematics, Mount St. Mary's University, Maryland
e.m.eckard@email.msmary.edu

Joshua Harrington
Department of Mathematics, Cedar Crest College, Pennsylvania
joshua.harrington@cedarcrest.edu

Yewen Sun
Department of Mathematics, University of California, Santa Barbara, California
yewen@ucsb.edu

Tony W. H. Wong
Department of Mathematics, Kutztown University of Pennsylvania, Pennsylvania
wong@kutztown.edu

Received: 9/28/20, Accepted: 5/28/21, Published: 6/3/21

Abstract

In this paper, we investigate the existence of Sierpiński numbers and Riesel numbers as binomial coefficients. We show that for any odd positive integer r, there exist infinitely many Sierpiński numbers and Riesel numbers of the form $\binom{k}{r}$. Let $S(x)$ be the number of positive integers r satisfying $1 \leq r \leq x$ for which $\binom{k}{r}$ is a Sierpiński number for infinitely many k. We further show that the value $S(x)/x$ gets arbitrarily close to 1 as x tends to infinity. Generalizations to base a-Sierpiński numbers and base a-Riesel numbers are also considered. In particular, we prove that there exist infinitely many positive integers r such that $\binom{k}{r}$ is simultaneously a base a-Sierpiński and base a-Riesel number for infinitely many k.

1. Introduction

In 1956, Riesel [11] showed that if $k \equiv 509203 \pmod{1184810}$, then for any natural number n, the value $k \cdot 2^n - 1$ is composite. Today we say that k is a Riesel number if k is an odd positive integer such that $k \cdot 2^n - 1$ is composite for all natural numbers n. Using methods similar to Riesel, Sierpiński [12] showed in 1960 that there are infinitely many odd positive integers k such that $k \cdot 2^n + 1$ is composite for all natural numbers n; values of k satisfying this property are now known as Sierpiński numbers.

In 2003, Chen [5] showed that if $r \not\equiv 0, 4, 6, 8 \pmod{12}$, then there exist infinitely many odd positive integers k such that k^r is a Sierpiński number. Chen's result was later extended by Filaseta, Finch, and Kozek [7] for all positive integers r. In their article, Filaseta, Finch, and Kozek asked the following question.

Question 1. Let $f \in \mathbb{Z}[x]$. Does there exist an integer k such that $f(k)$ is a Sierpiński number?

This question has been studied by various authors. For example, Finch, Harrington, and Jones [8] studied this question for $f(x) \in \{x^r + x + c, ax^r + c, x^r + 1, x^r + x + 1\}$ and Emadian, Finch-Smith, and Kallus [6] studied this question for $f(x) = 384x^3 + 432x^2 + 112x - 5$. Other authors considered Question 1 for polynomials $f \in \mathbb{Q}[x]$. Of particular note is the existence of infinitely many Sierpiński numbers in the sequence of triangular numbers and other polygonal numbers. Recall that for $s \geq 3$, the x-th s-gonal number is given by

$$P_s(x) = \frac{s-2}{2}x^2 - \frac{s-4}{2}x.$$

Question 1 with respect to $P_s(x)$ has been studied by Baczkowski et al. [2] and Baczkowski and Eitner [3].

In this article, we study Question 1 with respect to the polynomial

$$\binom{x}{r} = \frac{x(x-1)(x-2)\cdots(x-(r-1))}{r!}$$

where r is a fixed positive integer. Notice that the case $\binom{x}{2}$ has been previously studied since $\binom{x}{2} = P_3(x-1)$. Of course, $\binom{x}{r}$ is more commonly referred to as the *binomial coefficient* function. We begin our investigation on the existence of Sierpiński binomial coefficients for general r in Section 3, and extend some of these results to base a-Sierpiński and a-Riesel binomial coefficients in Section 4.

2. Preliminary Results, Definitions, and Notation

Throughout this article, we use $[a, b]$ to denote the set of integers x such that $a \leq x \leq b$.

For our investigation, we will make use of the following concept, originally introduced by Erdős.

Definition 1. A *covering system* of the integers is a finite collection of congruences such that every integer satisfies at least one congruence from the set.

In this article, we will primarily use covering systems of the form:

$$\begin{aligned} 0 \pmod{2^\tau} &\qquad \text{where } \tau \text{ is a positive integer} \\ 2^{\ell-1} \pmod{2^\ell} &\qquad \text{for each } 1 \le \ell \le \tau. \end{aligned} \tag{1}$$

Many of the proofs in this article rely heavily on the following two theorems, originally due to Zsigmondy [13] and Lucas [10], respectively.

Theorem 2 (Zsigmondy's Theorem)**.** *Let a and b be relatively prime positive integers with $a > b$. Then for any integer $n \ge 2$, there exists a prime p such that p divides $a^n - b^n$ and p does not divide $a^{\widetilde{n}} - b^{\widetilde{n}}$ for any $\widetilde{n} < n$, with the exceptions*

- *$(a, b) = (2, 1)$ and $n = 6$; and*
- *$a + b$ is a power of 2 and $n = 2$.*

Theorem 3 (Lucas' Theorem)**.** *Let p be a prime, and let m and n be nonnegative integers. Let the base p representations of m and n be $m = \sum_{i=0}^{j} m_i p^i$ and $n = \sum_{i=0}^{j} n_i p^i$, respectively, where $m_i, n_i \in [0, p-1]$ for all $i \in [0, j]$. Then*

$$\binom{m}{n} \equiv \prod_{i=0}^{j} \binom{m_i}{n_i} \pmod{p}.$$

3. Sierpiński Binomial Coefficients

Lemma 1. *Let p be a prime, and let r be a nonnegative integer. Let j be the smallest nonnegative integer such that $r < p^{j+1}$. Then for all positive integers k such that $k \equiv r \pmod{p^{j+1}}$, we have*

$$\binom{k}{r} \equiv 1 \pmod{p}.$$

Proof. Let the base p representations of r and k be $r = \sum_{i=0}^{j'} r_i p^i$ and $k = \sum_{i=0}^{j'} k_i p^i$, respectively, where $j \le j'$, $k_i = r_i \in [0, p-1]$ for all $i \in [0, j]$, $r_i = 0$ for all $i \in [j+1, j']$, and $k_i \in [0, p-1]$ for all $i \in [j+1, j']$. By Theorem 3,

$$\binom{k}{r} \equiv \left(\prod_{i=0}^{j} \binom{k_i}{r_i}\right) \left(\prod_{i=j+1}^{j'} \binom{k_i}{r_i}\right) \equiv \left(\prod_{i=0}^{j} \binom{r_i}{r_i}\right) \left(\prod_{i=j+1}^{j'} \binom{k_i}{0}\right) \equiv 1 \pmod{p}.$$

□

The following three lemmas are verified computationally by Mathematica. The code for these lemmas is included in Appendix A, Appendix B, and Appendix C, respectively.

Lemma 2. *Let $p = 641$, and let*

$$\begin{aligned}\mathcal{G} = \{\gamma \in [1, p-1] : \gamma \text{ is odd}\} \cup \{&2, 6, 8, 10, 12, 22, 24, 30, 32, 34, 44, 46, 48, 52, 56, 66,\\ &70, 74, 80, 84, 86, 94, 100, 102, 104, 110, 118, 120, 134, 136, 140, 144, 146, 160,\\ &162, 174, 176, 182, 184, 190, 194, 198, 200, 202, 208, 222, 224, 236, 248, 250,\\ &252, 260, 270, 292, 294, 304, 312, 318, 334, 336, 338, 348, 366, 368, 374, 402,\\ &414, 424, 426, 454, 474, 530, 546, 552, 578\}.\end{aligned}$$

Then there exists a function $\kappa : \mathcal{G} \to [0, p-1]$ such that for every $r \in \mathcal{G}$,

$$\binom{\kappa(r)}{r} \equiv -1 \pmod{p}.$$

Lemma 3. *Let $p = 641$. Recall $\mathcal{G}$ defined in Lemma 2. Then there exist a function $\widetilde{\kappa} = (\widetilde{\kappa}', \widetilde{\kappa}'') : [1, 515]^2 \to [0, p-1]^2$ such that for every ordered pair $(r', r'') \in [1, 515]^2$,*

$$\binom{\widetilde{\kappa}'(r', r'')}{r'}\binom{\widetilde{\kappa}''(r', r'')}{r''} \equiv -1 \pmod{p}.$$

Lemma 4. *Let $\mathcal{P}$ be the following set of primes p that divides $2^{2^{\tau-1}} + 1$ for some $\tau \in \mathbb{N}$ such that $\left(2^{2^{\tau-1}} + 1\right)/p$ is divisible by another prime distinct from p:*

$$\{641, 114689, 274177, 319489, 974849, 2424833,\\ 6700417, 13631489, 26017793, 45592577, 63766529\}.$$

Then for every $r \in [1, 640]$, there exists $p \in \mathcal{P}$ and $k \in \mathbb{N}$ such that

$$\binom{k}{r} \equiv -1 \pmod{p}.$$

Lemma 5. *Let $p = 641$. Recall $\mathcal{G}$ and κ defined in Lemma 2, and recall $\widetilde{\kappa} = (\widetilde{\kappa}', \widetilde{\kappa}'')$ defined in Lemma 3. Let r be a nonnegative integer with base p representation $r = \sum_{i=0}^{j} r_i p^i$, where $r_i \in [0, p-1]$ for all $i \in [0, j]$.*

(a) *If there exists $i_0 \in [0, j]$ such that $r_{i_0} \in \mathcal{G}$, then for all positive integers k such that $k \equiv r + (\kappa(r_{i_0}) - r_{i_0})p^{i_0} \pmod{p^{j+1}}$, we have*

$$\binom{k}{r} \equiv -1 \pmod{p}.$$

(*b*) *If there exist* $i_1, i_2 \in [0, j]$ *such that* $r_{i_1}, r_{i_2} \in [1, 515]$*, then for all positive integers* k *such that* $k \equiv r + (\widetilde{\kappa}'(r_{i_1}, r_{i_2}) - r_{i_1})p^{i_1} + (\widetilde{\kappa}''(r_{i_1}, r_{i_2}) - r_{i_2})p^{i_2} \pmod{p^{j+1}}$*, we have*

$$\binom{k}{r} \equiv -1 \pmod{p}.$$

Proof. (*a*) Let the base p representation of k be $k = \sum_{i=0}^{j'} k_i p^i$, where $j \le j'$, $k_i = r_i$ for all $i \in [0, j] \setminus \{i_0\}$, $k_{i_0} = \kappa(r_{i_0})$, and $k_i \in [0, p-1]$ for all $i \in [j+1, j']$. Furthermore, define $r_i = 0$ for all $i \in [j+1, j']$. By Theorem 3,

$$\begin{aligned}\binom{k}{r} \equiv \left(\prod_{i=0}^{j}\binom{k_i}{r_i}\right)\left(\prod_{i=j+1}^{j'}\binom{k_i}{r_i}\right) &\equiv \left(\prod_{\substack{i=0\\ i\neq i_0}}^{j}\binom{r_i}{r_i}\right)\binom{\kappa(r_{i_0})}{r_{i_0}}\left(\prod_{i=j+1}^{j'}\binom{k_i}{0}\right)\\ &\equiv -1 \pmod{p}.\end{aligned}$$

(*b*) Let the base p representation of k be $k = \sum_{i=0}^{j'} k_i p^i$, where $j \le j'$, $k_i = r_i$ for all $i \in [0, j] \setminus \{i_1, i_2\}$, $k_{i_1} = \widetilde{\kappa}'(r_{i_1}, r_{i_2})$, $k_{i_2} = \widetilde{\kappa}''(r_{i_1}, r_{i_2})$, and $k_i \in [0, p-1]$ for all $i \in [j+1, j']$. Furthermore, define $r_i = 0$ for all $i \in [j+1, j']$. By Theorem 3,

$$\binom{k}{r} \equiv \left(\prod_{\substack{i=0\\ i\notin\{i_1,i_2\}}}^{j}\binom{r_i}{r_i}\right)\binom{\widetilde{\kappa}'(r_{i_1}, r_{i_2})}{r_{i_1}}\binom{\widetilde{\kappa}''(r_{i_1}, r_{i_2})}{r_{i_2}}\left(\prod_{i=j+1}^{j'}\binom{k_i}{0}\right) \equiv -1 \pmod{p}.$$

$\square$

Theorem 4. *Let* $p = 641$*, and recall* $\mathcal{G}$ *defined in Lemma* 2*. Let* r *be a nonnegative integer with base* p *representation* $r = \sum_{i=0}^{j} r_i p^i$*, where* $r_i \in [0, p-1]$ *for all* $i \in [0, j]$*, such that at least one of the following conditions is satisfied:*

(*i*) *there exists* $i_0 \in [0, j]$ *such that* $r_{i_0} \in \mathcal{G}$*; or*

(*ii*) *there exists* $i_1, i_2 \in [0, j]$ *such that* $r_{i_1}, r_{i_2} \in [1, 515]$*.*

Then there exist infinitely many positive integers k *such that* $\binom{k}{r}$ *is a Sierpiński number.*

Proof. Let $p_0 = 641$, $p_1 = 3$, $p_2 = 5$, $p_3 = 17$, $p_4 = 257$, $p_5 = 65537$, and $p_6 = 6700417$. Note that for each $\ell \in [1, 6]$,

$$p_\ell \mid 2^{2^\ell} - 1 \text{ and } p_\ell \nmid 2^{2^{\widetilde{\ell}}} - 1 \text{ for any } \widetilde{\ell} < \ell,$$

so we also have $2^{2^{\ell-1}} \equiv -1 \pmod{p_\ell}$.

Consider the covering system in Equation (1) with $\tau = 6$. Suppose that $n \equiv 2^{\ell-1} \pmod{2^\ell}$ for some $\ell \in [1, 6]$. Then

$$2^n = \left(2^{2^\ell}\right)^t \cdot 2^{2^{\ell-1}} \equiv 1^t \cdot (-1) \equiv -1 \pmod{p_\ell}$$

for some nonnegative integer t. Hence,

$$\binom{k}{r} \cdot 2^n + 1 \equiv -\binom{k}{r} + 1 \pmod{p_\ell}.$$

Let j_ℓ be the smallest nonnegative integer such that $r < p_\ell^{j_\ell+1}$ for each $\ell \in [1, 6]$. By Lemma 1, if

$$k \equiv r \pmod{p_\ell^{j_\ell+1}}, \tag{2}$$

then $\binom{k}{r} \cdot 2^n + 1 \equiv 0 \pmod{p_\ell}$.

Since Equation (1) is a covering system, if $n \not\equiv 2^{\ell-1} \pmod{2^\ell}$ for any $\ell \in [1, 6]$, then $n \equiv 0 \pmod{2^6}$. Note that $p_0 \mid 2^{2^6} - 1$, so $2^n \equiv 1 \pmod{p_0}$ and

$$\binom{k}{r} \cdot 2^n + 1 \equiv \binom{k}{r} + 1 \pmod{p_0}.$$

Let j_0 be the smallest nonnegative integer such that $r < p_0^{j_0+1}$. Recall the function κ defined in Lemma 2. By Lemma 5(a), if condition (i) of this theorem is satisfied and

$$k \equiv r + (\kappa(r_{i_0}) - r_{i_0})p_0^{i_0} \pmod{p_0^{j_0+1}}, \tag{3}$$

then $\binom{k}{r} \cdot 2^n + 1 \equiv 0 \pmod{p_0}$.

Hence, for any natural number n, if the congruence in Equation (2) is satisfied for each $\ell \in [1, 6]$ and the congruence in Equation (3) is satisfied, then $\binom{k}{r} \cdot 2^n + 1$ is divisible by some prime p_ℓ with $0 \le \ell \le 6$. Using Lemma 1, we ensure that $\binom{k}{r}$ is odd by further requiring $k \equiv r \pmod{2^{j+1}}$, where j is the smallest nonnegative integer such that $r < 2^{j+1}$. By the Chinese remainder theorem, there are infinitely many such integers k. Choosing k so that $\binom{k}{r} \ge p_6$ ensures that $\binom{k}{r}$ is a Sierpiński number.

If condition (ii) of this theorem is satisfied, then the same argument applies by replacing Lemma 5(a) and Equation (3) with Lemma 5(b) and the congruence

$$k \equiv r + (\widetilde{\kappa}'(r_{i_1}, r_{i_2}) - r_{i_1})p_0^{i_1} + (\widetilde{\kappa}''(r_{i_1}, r_{i_2}) - r_{i_2})p_0^{i_2} \pmod{p_0^{j_0+1}}.$$

$\square$

The following corollary follows from Theorem 4(i) since every odd positive integer must have an odd digit in its base p representation.

Corollary 1. *Let r be an odd positive integer. Then there exist infinitely many positive integers k such that $\binom{k}{r}$ is a Sierpiński number.*

There are 245 integers $r \in [1, 2563]$ that do not satisfy the conditions in Theorem 4. Nonetheless, we can tackle these values of r in the following theorem.

Theorem 5. *Let $r \in [1, 2563]$. Then there exist infinitely many positive integers k such that $\binom{k}{r}$ is a Sierpiński number.*

Proof. If $r \in [641, 2563]$, then the conclusion follows from Theorem 4(i) since the base p representation of r contains the digits 1, 2, or 3, which are in $\mathcal{G}$ defined in Lemma 2.

Suppose that $r \in [1, 640]$. Let $\mathcal{P}$ be the set of primes defined in Lemma 4. By Lemma 4, there exist $p_0 \in \mathcal{P}$ and $k' \in \mathbb{N}$ such that $\binom{k'}{r} \equiv -1 \pmod{p_0}$. By the definition of $\mathcal{P}$, there is some integer $\tau \geq 5$ and some prime $p_\tau \neq p_0$ such that p_0 and p_τ both divide $2^{2^{\tau-1}} + 1$. Consequently, p_0 and p_τ are both prime factors of $2^{2^\tau} - 1$. By Theorem 2, for each $\ell \in [1, \tau - 1]$, let p_ℓ be a prime such that

$$p_\ell \mid 2^{2^\ell} - 1 \text{ and } p_\ell \nmid 2^{2^{\widetilde{\ell}}} - 1 \text{ for any } \widetilde{\ell} < \ell,$$

so we also have $2^{2^{\ell-1}} \equiv -1 \pmod{p_\ell}$. Note that p_0 and p_τ are distinct from p_ℓ for all $\ell \in [1, \tau-1]$. This is because $2^{2^\ell} \equiv 1 \pmod{p_\ell}$, implying that $2^{2^{\tau-1}} \equiv 1 \pmod{p_\ell}$, while $2^{2^{\tau-1}} \equiv -1 \pmod{p_0}$ and $2^{2^{\tau-1}} \equiv -1 \pmod{p_\tau}$.

Consider the covering system in Equation (1). Suppose that $n \equiv 2^{\ell-1} \pmod{2^\ell}$ for some $\ell \in [1, \tau]$. Let j_ℓ be the smallest nonnegative integer such that $r < p^{j_\ell+1}$. Similar to the argument presented in proof of Theorem 4, by Lemma 1, if

$$k \equiv r \pmod{p_\ell^{j_\ell+1}}, \tag{4}$$

then $\binom{k}{r} \cdot 2^n + 1 \equiv 0 \pmod{p_\ell}$.

Since Equation (1) is a covering system, if $n \not\equiv 2^{\ell-1} \pmod{2^\ell}$ for any $\ell \in [1, \tau]$, then $n \equiv 0 \pmod{2^\tau}$. Note that $r < p_0$, so by the definition of k', for all $k \in \mathbb{N}$ such that

$$k \equiv k' \pmod{p_0}, \tag{5}$$

we have $\binom{k}{r} \equiv -1 \pmod{p_0}$, which implies that $\binom{k}{r} \cdot 2^n + 1 \equiv 0 \pmod{p_0}$.

The result follows by letting $k \geq \max\{p_0, p_1, \ldots, p_\tau\}$ satisfy the congruence relations in Equation (4) for all $\ell \in [1, \tau]$, Equation (5), and $k \equiv r \pmod{2^{j+1}}$, where j is the smallest nonnegative integer such that $r < 2^{j+1}$. $\square$

There are $641^2 - 1 = 410880$ one-digit or two-digit positive integers $\overline{r'r''}$ in base 641, and from the code given in Appendix B, only $3771 - 1 = 3770$ of them do not have any solution $(x', x'') \in [0, 640]^2$ for the equation

$$\binom{x'}{r'}\binom{x''}{r''} \equiv -1 \pmod{641}.$$

For a positive integer x, let $S(x)$ be the number of $r \in [1, x]$ such that $\binom{k}{r}$ is a Sierpiński number for infinitely many positive integers k. Then $S(410880)/410880 > 99\%$, and the next theorem addresses $S(x)/x$ as x tends to infinity.

Theorem 6. *The density $S(x)/x$ gets arbitrarily close to 1 as x tends to infinity.*

Proof. Let $p = 641$. Note that the cardinality of $\mathcal{G}$, which is defined in Lemma 2, is 395. Hence, the number of integers less than p^{j+1} such that no digit comes from $\mathcal{G}$ when expressed in base p is

$$1 - \frac{S(p^{j+1}-1)}{p^{j+1}-1} \leq \frac{(p-395)^{j+1}-1}{p^{j+1}-1},$$

which tends to 0 as j tends to infinity. □

4. Generalizations of Sierpiński and Riesel Binomial Coefficients

In 2009, Brunner et al. [1] generalized the concept of a Sierpiński number in the following way.

Definition 2. For a positive integer a, we call a positive integer k an *a-Sierpiński number* if $\gcd(k+1, a-1) = 1$, k is not a power of a, and $k \cdot a^n + 1$ is composite for all natural numbers n.

The following is an analogous definition for an a-Riesel number.

Definition 3. For a positive integer a, we call a positive integer k an *a-Riesel number* if $\gcd(k-1, a-1) = 1$, k is not a power of a, and $k \cdot a^n - 1$ is composite for all natural numbers n.

The next theorem is a generalization of Corollary 1.

Theorem 7. *Let a and r be positive integers such that $a+1$ is not a power of 2 and r is odd. Further assume that there exists a positive integer τ such that $a^{2^\tau}-1$ is divisible by distinct primes p_0 and p_τ, where neither p_0 nor p_τ divides $a^{2^{\widetilde{\ell}}}-1$ for any $\widetilde{\ell} \in [0, \tau-1]$. Then each of the following holds:*

- (a) *there exist infinitely many positive integers k such that $\binom{k}{r}$ is an a-Sierpiński number;*
- (b) *there exist infinitely many positive integers k such that $\binom{k}{r}$ is an a-Riesel number.*

Proof. For each $\ell \in [1, \tau]$, let p_ℓ be a prime such that

$$p_\ell \mid a^{2^\ell} - 1 \text{ and } p_\ell \nmid a^{2^{\widetilde{\ell}}} - 1 \text{ for any } \widetilde{\ell} \in [0, \ell-1],$$

so we also have $a^{2^{\ell-1}} \equiv -1 \pmod{p_\ell}$. Note that such primes exist by Theorem 2. Let $p_{\tau+1}, p_{\tau+2}, \ldots, p_\sigma$ be all the prime factors of $a-1$. Further let $p_{\sigma+1}$ be a prime factor of a. Note that p_ℓ are all distinct for $\ell \in [0, \sigma+1]$ since $\gcd(a, a^{\widetilde{\ell}}-1) = 1$ for all positive integers $\widetilde{\ell}$. For each $\ell \in [0, \sigma+1]$, let j_ℓ be the smallest positive integer satisfying $r < p_\ell^{j_\ell+1}$.

Using the Chinese remainder theorem, let k satisfy the following congruences:

$$\begin{aligned} k &\equiv 0 \pmod{p_\ell^{j_\ell}} \text{ for each } \ell \in [\tau+1, \sigma] \text{ and} \\ k &\equiv r \pmod{p_{\sigma+1}^{j_{\sigma+1}+1}}. \end{aligned} \tag{6}$$

It follows from Theorem 3 that $\binom{k}{r} \equiv 0 \pmod{p_\ell}$ for each $\ell \in [\tau+1, \sigma]$ and $\binom{k}{r} \equiv 1 \pmod{p_{\sigma+1}}$. Consequently, $\gcd\left(\binom{k}{r} - 1, a-1\right) = \gcd\left(\binom{k}{r} + 1, a-1\right) = 1$ and $\binom{k}{r}$ is not a power of a.

For each $\ell \in [0, \tau]$, if

$$k \equiv r \pmod{p_\ell^{j_\ell+1}}, \tag{7}$$

then $\binom{k}{r} \equiv 1 \pmod{p_\ell}$ by Lemma 1. Let $\sum_{i=0}^{j_\ell} r_{\ell i} p_\ell^i$ be the base p_ℓ representation of r. Since r is an odd integer, there exists an $i_0 \in [0, j_\ell]$ such that $r_{\ell i_0}$ is odd. By Theorem 3, if

$$k \equiv r + (p_\ell - 1 - r_{\ell i_0}) p_\ell^{i_0} \pmod{p_\ell^{j_\ell+1}}, \tag{8}$$

then $\binom{k}{r} \equiv \binom{p_\ell - 1}{r_{\ell i_0}} \equiv -1 \pmod{p_\ell}$.

Consider the covering system in Equation (1). If $n \equiv 2^{\ell-1} \pmod{2^\ell}$ for some $\ell \in [1, \tau]$, then $a^n \equiv -1 \pmod{p_\ell}$, and if $n \equiv 0 \pmod{p_0}$, then $a^n \equiv 1 \pmod{p_0}$. Thus, using the Chinese remainder theorem to choose k so that

- $\binom{k}{r} \geq \max\{p_0, p_1, \ldots, p_\tau\}$;
- k satisfies Equation (7) for each $\ell \in [1, \tau]$; and
- k satisfies Equation (8) when $\ell = 0$,

we ensure that for any natural number n, $\binom{k}{r} a^n + 1$ is composite and divisible by p_ℓ for some $\ell \in [0, \tau]$. Similarly, using the Chinese remainder theorem to choose k so that

- $\binom{k}{r} \geq \max\{p_0, p_1, \ldots, p_\tau\}$;
- k satisfies Equation (7) when $\ell = 0$; and
- k satisfies Equation (8) for each $\ell \in [1, \tau]$,

we ensure that for any natural number n, $\binom{k}{r} a^n - 1$ is composite and divisible by p_ℓ for some $\ell \in [0, \tau]$. Thus, the proof is finished by recalling that k satisfies the congruences in Equation (6). □

For a positive integer x, let $R(x)$ be the number of $r \in [1,x]$ such that $\binom{k}{r}$ is a Riesel number for infinitely many positive integers k. The following theorem follows similarly to Theorem 6.

Theorem 8. *The density $R(x)/x$ gets arbitrarily close to 1 as x tends to infinity.*

In 2001, Chen [4] introduced the concept of a $(2,1)$-primitive m-covering. This concept was extended to the following definition by Harrington [9] in 2015.

Definition 4. A covering system $\mathcal{C} = \{q_\ell \pmod{m_\ell}\}_{\ell=1}^{\tau}$ is called an (a,b)*-primitive m-covering* if every integer satisfies at least m congruences of $\mathcal{C}$ and there exist distinct primes $p_1, p_2, \ldots, p_\tau$ such that for each $\ell \in [1,\tau]$,

$$p_\ell \mid a^{m_\ell} - b^{m_\ell} \text{ and } p_\ell \nmid a^{\widetilde{\ell}} - b^{\widetilde{\ell}} \text{ for any } \widetilde{\ell} < m_\ell.$$

Furthermore, a covering system $\mathcal{C}$ is called an (a,b)*-primitive disjoint m-covering* if $\mathcal{C}$ is an (a,b)-primitive m-covering that can be partitioned into m disjoint (a,b)-primitive 1-covering systems.

Harrington [9] showed that if a and b are relatively prime integers such that $a+b$ is not a power of 2, then there exists an (a,b)-primitive disjoint 3-covering. Thus, the following theorem provides immediate results when $m = 3$.

Theorem 9. *Let a be a positive integer for which there exists an $(a,1)$-primitive m-covering $\mathcal{C}$. Then there exist infinitely many positive integers r for which each of the following holds:*

(a) *there exist infinitely many positive integers k such that* $\gcd\left(\binom{k}{r}+1, a-1\right) = 1$, *$\binom{k}{r}$ is not a power of a, and $\binom{k}{r}\cdot a^n+1$ has at least m distinct prime divisors for all natural numbers n;*

(b) *there exist infinitely many positive integers k such that* $\gcd\left(\binom{k}{r}-1, a-1\right) = 1$, *$\binom{k}{r}$ is not a power of a, and $\binom{k}{r}\cdot a^n-1$ has at least m distinct prime divisors for all natural numbers n; and*

(c) *if $\mathcal{C}$ is an $(a,1)$-primitive disjoint m-covering, then there exist infinitely many positive integers k such that* $\gcd\left(\binom{k}{r}+1, a-1\right) = \gcd\left(\binom{k}{r}-1, a-1\right) = 1$, *$\binom{k}{r}$ is not a power of a, $\binom{k}{r}\cdot a^n+1$ and $\binom{k}{r}\cdot a^n-1$ are composite, and each of $\binom{k}{r}\cdot a^n+1$ and $\binom{k}{r}\cdot a^n-1$ has at least $\lfloor m/2 \rfloor$ distinct prime divisors for all natural numbers n.*

Proof. Let $\mathcal{C} = \{q_\ell \pmod{m_\ell}\}_{\ell=1}^{\tau}$ be an $(a,1)$-primitive m covering with distinct primes $p_1, p_2, \ldots, p_\tau$ given by Definition 4. Let $p_{\tau+1}, p_{\tau+2}, \ldots, p_\sigma$ be all the prime factors of $a-1$. Further let $p_{\sigma+1}$ be a prime factor of a. Note that p_ℓ are all distinct for $\ell \in [1, \sigma+1]$ due to Definition 4 and that $\gcd(a, a^{\widetilde{\ell}} - 1) = 1$ for all positive integers $\widetilde{\ell}$.

(a) By the Chinese remainder theorem, there exists a positive integer R such that

$$R \equiv \begin{cases} a^{-q_\ell} \pmod{p_\ell} & \text{for all } \ell \in [1, \tau]; \\ 0 \pmod{p_\ell} & \text{for all } \ell \in [\tau+1, \sigma]; \\ 1 \pmod{p_{\sigma+1}}. \end{cases} \tag{9}$$

Let J_1 be the smallest nonnegative integer such that $R < p_\ell^{J_1+1}$ for all $\ell \in [1, \sigma+1]$. Again by the Chinese remainder theorem, there exist infinitely many positive integers $r > R$ such that $r \equiv 1 \pmod{p_\ell^{J_1+1}}$ for all $\ell \in [1, \sigma+1]$. For each such r, let J_2 be the smallest nonnegative integer such that $r < p_\ell^{J_2+1}$ for all $\ell \in [1, \sigma+1]$. Once again by the Chinese remainder theorem, there exist infinitely many positive integers $k > r$ such that $k \equiv r+R-1 \pmod{p_\ell^{J_2+1}}$ for all $\ell \in [1, \sigma+1]$. For each such k, let J_3 be the smallest nonnegative integer such that $k < p_\ell^{J_3+1}$ for all $\ell \in [1, \sigma+1]$. For each $\ell \in [1, \sigma+1]$, let the base p_ℓ representations of R, r, and k be $R = \sum_{i=0}^{J_1} R_{\ell i} p_\ell^i$, $r = 1 + \sum_{i=J_1+1}^{J_2} r_{\ell i} p_\ell^i$, and $k = \sum_{i=0}^{J_1} R_{\ell i} p_\ell^i + \sum_{i=J_1+1}^{J_2} r_{\ell i} p_\ell^i + \sum_{i=J_2+1}^{J_3} k_{\ell i} p_\ell^i$, respectively. By Theorem 3,

$$\binom{k}{r} \equiv \binom{R_{\ell 0}}{1} \left(\prod_{i=1}^{J_1} \binom{R_{\ell i}}{0} \right) \left(\prod_{i=J_1+1}^{J_2} \binom{r_{\ell i}}{r_{\ell i}} \right) \left(\prod_{i=J_2+1}^{J_3} \binom{k_{\ell i}}{0} \right) \equiv R_{\ell 0} \equiv R \pmod{p_\ell}.$$

Therefore, $\gcd\left(\binom{k}{r} + 1, a-1\right) = 1$ since $\binom{k}{r} + 1 \equiv 1 \pmod{p_\ell}$ for all $\ell \in [\tau+1, \sigma]$, and $\binom{k}{r}$ is not a power of a since $\binom{k}{r} \equiv 1 \pmod{p_{\sigma+1}}$. Lastly, since $\mathcal{C}$ is an $(a,1)$-primitive m covering, for each natural number n, there exist distinct $\ell_1, \ell_2, \ldots, \ell_m \in [1, \tau]$ such that $n \equiv q_{\ell_\iota} \pmod{m_{\ell_\iota}}$ for all $\iota \in [1, m]$. Thus, for each $\iota \in [1, m]$,

$$\binom{k}{r} \cdot a^n - 1 \equiv R\left((a^{m_{\ell_\iota}})^t a^{q_{\ell_\iota}}\right) - 1 \equiv a^{-q_{\ell_\iota}} a^{q_{\ell_\iota}} - 1 \equiv 0 \pmod{p_{\ell_\iota}}$$

for some nonnegative integer t.

(b) This proof resembles the proof of part (a) after replacing Equation (9) by

$$R \equiv \begin{cases} -a^{-q_\ell} \pmod{p_\ell} & \text{for all } \ell \in [1, \tau]; \\ 0 \pmod{p_\ell} & \text{for all } \ell \in [\tau+1, \sigma]; \\ 1 \pmod{p_{\sigma+1}}. \end{cases}$$

(c) Let $\mathcal{C}$ be partitioned into $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_m$, where $\mathcal{C}_\lambda = \{q_{\lambda\ell} \pmod{m_{\lambda\ell}}\}_{\ell=1}^{\tau_\lambda}$ for each $\lambda \in [1, m]$, and $\tau_1 + \tau_2 + \cdots + \tau_\lambda = \tau$. Let $\{p_{\lambda 1}, p_{\lambda 2}, \ldots, p_{\lambda \tau_\lambda} : \lambda \in [1, m]\}$ be given by Definition 4. A similar proof as from part (a) applies after replacing

Equation (9) by

$$R \equiv \begin{cases} a^{-q_{\lambda\ell}} \pmod{p_{\lambda\ell}} & \text{for all } \ell \in [1, \tau_\lambda],\ \text{where } \lambda \in [1, \lfloor m/2 \rfloor]; \\ -a^{-q_{\lambda\ell}} \pmod{p_{\lambda\ell}} & \text{for all } \ell \in [1, \tau_\lambda],\ \text{where } \lambda \in [\lceil m/2 \rceil + 1, m]; \\ 0 \pmod{p_\ell} & \text{for all } \ell \in [\tau + 1, \sigma]; \\ 1 \pmod{p_{\sigma+1}}. \end{cases}$$

□

5. Concluding Remarks

Theorem 7 shows that for any integer $a \geq 2$ and any odd positive integer r, there are infinitely many a-Sierpiński numbers and infinitely many a-Riesel numbers of the form $\binom{k}{r}$. Theorems 4 and 5 show that there are infinitely many Sierpiński numbers of the form $\binom{k}{r}$ for most even positive integers r; however, it is unknown if there are Sierpiński numbers of the form $\binom{k}{r}$ for an arbitrary even positive integer r. Thus, we present the following conjecture.

Conjecture 1. For any positive integer r, there exist infinitely many positive integers k for which $\binom{k}{r}$ is simultaneously a Sierpiński number and a Riesel number.

We end this section with the following question regarding Catalan numbers. Recall that the k-th Catalan number is $\frac{1}{k+1}\binom{2k}{k}$.

Question 10. Are there infinitely many Catalan numbers that are either Sierpiński numbers or Riesel numbers?

The constructions in this paper rely on fixing a positive integer r prior to finding k values for which $\binom{k}{r}$ is either Sierpiński or Riesel. Hence, a new technique might be required in order to tackle the existence of Sierpiński or Riesel Catalan numbers.

Acknowledgement. These results are based on work supported by the National Science Foundation under grant numbered DMS-1852378.

References

[1] A. Brunner, C. Caldwell, D. Krywaruczenko, and C. Lownsdale, Generalizing Sierpiński numbers to base b, *New Aspects of Analytic Number Theory, Proceedings of RIMS, Surikaisekikenkyusho Kokyuroku* (2009), 69–79.

[2] D. Baczkowski, J. Eitner, C. Finch, M. Kozek, and B. Suminski, Polygonal, Sierpiński, and Riesel numbers, *J. Integer Seq.* **18** (2015), Article 15.8.1.

[3] D. Baczkowski and J. Eitner, Polyonal-Sierpiński-Riesel sequences with terms having at least two distinct prime divisors, *Integers* **16** (2016), Article A40.

[4] Y.G. Chen, On integers of the form $k-2^n$ and $k2^n+1$, *J. Number Theory* **89** (2001), 121–125.

[5] Y.G. Chen, On integers of the form $k^r - 2^n$ and $k^r 2^n + 1$, *J. Number Theory* **98** (2003), 310–319.

[6] E. Emadian, C. Finch-Smith, and M. Kallus, Ruth-Aaron pairs containing Riesel or Sierpiński numbers, *Integers* **18** (2018), Article A72.

[7] M. Filaseta, C. Finch, and M. Kozek, On powers associated with Sierpiński numbers, Riesel numbers, and Polignac's conjecture, *J. Number Theory* **128** (2008), 1916–1940.

[8] C. Finch, J. Harrington, and L. Jones, Nonlinear Sierpiński and Riesel numbers, *J. Number Theory* **133** (2013), 534–544.

[9] J. Harrington, Two questions concerning coverings systems of the integers, *Int. J. Number Theory* **11** (2015), 1739–1750.

[10] E. Lucas, Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un module premier, *Bull. Soc. Math. France* **6** (1878), 49–54.

[11] H. Riesel, Några stora primal, *Elementa* **39** (1956), 258–260.

[12] W. Sierpiński, Sure un problème concernant les nombres $k2^n + 1$, *Elem. Math.* **15** (1960), 73–74.

[13] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsch. Math. Phys.* **3** (1892), 265–284.

A. Appendix: Mathematica Code for Lemma 2

```
p = 641;
good = Complement[ Table[
     If[ Or @@ Table[ Mod[Binomial[k, r], p] == p - 1, {k, p - 1}], r],
  {r, 0, p - 1}], {Null}]
```

The output good is our desired set $\mathcal{G}$.

B. Appendix: Mathematica Code for Lemma 3

The variables p and good are defined in the code given in Appendix A.

```
bad = Complement[ Table[r, {r, 0, p - 1}], good];
badbad = {};
Do[ If[ Not[ Or @@ Flatten[
  Table[ Mod[Binomial[k1, bad[[r1]]] * Binomial[k2, bad[[r2]]], p] == p - 1,
     {k1, p - 1}, {k2, p - 1}]]]],
  badbad = Append[badbad, {bad[[r1]], bad[[r2]]}]],
```

```
  {r1, Length[bad]}, {r2, Length[bad]}];
Or @@ Table[ 1 <= badbad[[i, 1]] <= 515 && 1 <= badbad[[i, 2]] <= 515,
  {i, Length[badbad]}]
```

The variable `badbad` contains all ordered pairs of $(r', r'') \in [0, 640]^2$ that fail to satisfy our desired equation. If we want to further investigate by using `Length[badbad]`, the number of ordered pairs of $(r', r'') \in [0, 640]^2$ that fail to satisfy our desired equation is 3771. However, the final output is `False`, showing that there are no unordered pairs $\{r', r''\} \subseteq [1, 515]$ that fails to satisfy our desired equation.

C. Appendix: Mathematica Code for Lemma 4

```
plist = {641, 114689, 274177, 319489, 974849, 2424833, 6700417, 13631489,
  26017793, 45592577, 63766529};
And @@ Table[Or @@ Table[
  Solve[Product[k - j, {j, 0, r - 1}]/r!  == p - 1, k, Modulus -> p] != {},
  {p, plist}], {r, 640}]
```

The output is `True`, showing that every $r \in [1, 640]$ satisfies our desired equation.