LUCAS-SIERPIŃSKI AND LUCAS-RIESEL NUMBERS

DANIEL BACZKOWSKI, OLAOLU FASORANTI, AND CARRIE E. FINCH

Abstract. In this paper, we show that there are infinitely many Sierpiński numbers in the sequence of Lucas numbers. We also show that there are infinitely many Riesel numbers in the sequence of Lucas numbers. Finally, we show that there are infinitely many Lucas numbers that are not a sum of two prime powers.

1. Introduction

In 1960, W. Sierpiński [8] showed that there are infinitely many odd positive integers k with the property that $k \cdot 2^n + 1$ is composite for all positive integers n. Such an integer k is called a Sierpiński number in honor of Sierpiński's work. Two years later, J. Selfridge (unpublished) showed that 78557 is a Sierpiński number. To this day, this is the smallest known Sierpiński number. As of this writing, there are six candidates smaller than 78557 to consider: 10223, 21181, 22699, 24737, 55459, 67607. See `http://www.seventeenorbust.com` for the most up-to-date information.

Riesel numbers are defined in a similar way: an odd positive integer k is Riesel if $k \cdot 2^n - 1$ is composite for all positive integers n. These were first investigated by H. Riesel in 1956 [7]. The smallest known Riesel number is 509203. As of this writing there are 62 remaining candidates smaller that 509203 to consider. See `http://www.prothsearch.net/rieselprob.html` for the most recent information.

The usual approach for constructing Sierpiński or Riesel numbers is to use a covering – a finite set of congruences with the property that every integer satisfies at least one of the congruences.

Consider the implications in Table 1 below.

$$\begin{array}{lcll}
n \equiv 0 \pmod 2 & \& & k \equiv 1 \pmod 3 & \implies k \cdot 2^n - 1 \equiv 0 \pmod 3 \\
n \equiv 0 \pmod 3 & \& & k \equiv 1 \pmod 7 & \implies k \cdot 2^n - 1 \equiv 0 \pmod 7 \\
n \equiv 1 \pmod 4 & \& & k \equiv 3 \pmod 5 & \implies k \cdot 2^n - 1 \equiv 0 \pmod 5 \\
n \equiv 11 \pmod{12} & \& & k \equiv 2 \pmod{13} & \implies k \cdot 2^n - 1 \equiv 0 \pmod{13} \\
n \equiv 7 \pmod{36} & \& & k \equiv 4 \pmod{73} & \implies k \cdot 2^n - 1 \equiv 0 \pmod{73} \\
n \equiv 19 \pmod{36} & \& & k \equiv 18 \pmod{37} & \implies k \cdot 2^n - 1 \equiv 0 \pmod{37} \\
n \equiv 31 \pmod{36} & \& & k \equiv 13 \pmod{19} & \implies k \cdot 2^n - 1 \equiv 0 \pmod{19}
\end{array}$$

Table 1

The congruences for n listed in Table 1 cover all possibilities for n; that is, this set of congruences forms a covering. As the moduli of the congruences involving k are relatively prime, the Chinese Remainder Theorem allows us to combine all of the congruences for k into one statement: $k \equiv 33737173 \pmod{3 \cdot 7 \cdot 5 \cdot 13 \cdot 73 \cdot 37 \cdot 19}$. For any of the infinitely many positive integer values of k in this arithmetic progression, we have that $k \cdot 2^n - 1$ has a prime divisor from the set $\mathcal{S} = \{3, 5, 7, 13, 19, 37, 73\}$. Moreover, as k is large enough, $k \cdot 2^n - 1$ can-

not be equal to any element of $\mathcal{S}$, and hence $k \cdot 2^n - 1$ must be composite. Therefore, each such k is a Riesel number.

Luca and Mejía-Huguet take this one step further, finding Riesel and Sierpiński numbers embedded in the Fibonacci sequence [4]. That is, they replace k with F_k, where $F_0 = 0$, $F_1 = 1$ and $F_i = F_{i-1} + F_{i-2}$ for $i \geq 2$. First, to ensure F_k is odd, note that the only Fibonacci numbers which are even are those satisfying $k \equiv 0 \pmod 3$. In order to have F_k be a Riesel number (using the covering in Table 1), each of the congruences $k \equiv a \pmod m$ from Table 1 must be replaced with $F_k \equiv a \pmod m$ and subsequently solved for k. We denote these solutions as $\mathcal{A}(a, m) = \{k : F_k \equiv a \pmod m\}$. Observe the fact that the Fibonacci numbers (or more generally any linear homogeneous recurrence relation with rational coefficients) are eventually periodic modulo m with period say $p(m)$ (cf. [1]). Note that a sequence considered modulo m may have a non-repeating part at the beginning of the sequence, but this is not the case in the Fibonacci sequence. Hence, if $k \in \mathcal{A}(a, m)$, then every integer in the congruence $k \pmod{p(m)}$ is also in $\mathcal{A}(a, m)$. These are computed below:

$$\begin{aligned}
\mathcal{A}(1,3) &= \{1,2,7\} \pmod 8 \\
\mathcal{A}(1,7) &= \{1,2,6,15\} \pmod{16} \\
\mathcal{A}(3,5) &= \{4,6,7,13\} \pmod{20} \\
\mathcal{A}(2,13) &= \{3,25\} \pmod{28} \\
\mathcal{A}(4,73) &= \{53,95\} \pmod{148} \\
\mathcal{A}(18,37) &= \{10,15,28,61\} \pmod{76} \\
\mathcal{A}(13,19) &= \{7,11\} \pmod{18}.
\end{aligned} \tag{1.1}$$

When we implement the Chinese Remainder Theorem, we find that the intersection of the sets in (1.1) contains the following residue classes:

$$k \equiv 947887, 1735247, 1807873, \text{ or } 2595233 \pmod{3543120}.$$

Since these residue classes for k do not include any multiples of 3, all such F_k are odd. We deduce F_k is both a Riesel number and a Fibonacci number. Thus, there are infinitely many Riesel numbers in the Fibonacci sequence.

The sequence of Lucas numbers L_k follows the same recurrence relation as the Fibonacci numbers ($L_i = L_{i-1} + L_{i-2}$), but with different initial values ($L_0 = 2$ and $L_1 = 1$). In Sections 2 and 3, we show that Luca and Mejía-Huguet's results for Riesel and Sierpiński numbers, respectively, hold for the sequence of Lucas numbers. In addition, Luca and Stănică [6] showed there are infinitely many Fibonacci numbers that are not the sum of two prime powers. In the final section of this paper, we show there are also infinitely many Lucas numbers with this property.

2. Lucas-Riesel Numbers

We define the sequence of Lucas numbers in the usual way: $L_0 = 2$, $L_1 = 1$, and $L_i = L_{i-1} + L_{i-2}$ for $i \geq 2$. Consider the implications in Table 2.

$$\begin{array}{lcll}
n \equiv 1 \pmod 2 & \& & L_k \equiv 2 \pmod 3 & \implies L_k \cdot 2^n - 1 \equiv 0 \pmod 3 \\
n \equiv 2 \pmod 4 & \& & L_k \equiv 4 \pmod 5 & \implies L_k \cdot 2^n - 1 \equiv 0 \pmod 5 \\
n \equiv 4 \pmod 8 & \& & L_k \equiv 16 \pmod{17} & \implies L_k \cdot 2^n - 1 \equiv 0 \pmod{17} \\
n \equiv 8 \pmod{16} & \& & L_k \equiv 256 \pmod{257} & \implies L_k \cdot 2^n - 1 \equiv 0 \pmod{257} \\
n \equiv 32 \pmod{48} & \& & L_k \equiv 3 \pmod{13} & \implies L_k \cdot 2^n - 1 \equiv 0 \pmod{13} \\
n \equiv 28 \pmod{36} & \& & L_k \equiv 34 \pmod{37} & \implies L_k \cdot 2^n - 1 \equiv 0 \pmod{37} \\
n \equiv 16 \pmod{36} & \& & L_k \equiv 4 \pmod{73} & \implies L_k \cdot 2^n - 1 \equiv 0 \pmod{73} \\
n \equiv 112 \pmod{288} & \& & L_k \equiv 365 \pmod{1153} & \implies L_k \cdot 2^n - 1 \equiv 0 \pmod{1153} \\
n \equiv 256 \pmod{288} & \& & L_k \equiv 2167 \pmod{6337} & \implies L_k \cdot 2^n - 1 \equiv 0 \pmod{6337} \\
n \equiv 0 \pmod 3 & \& & L_k \equiv 1 \pmod 7 & \implies L_k \cdot 2^n - 1 \equiv 0 \pmod 7
\end{array}$$

TABLE 2

As before, the congruences for n in Table 2 form a covering. The implications also produce a fixed residue class of integers L_k that are Riesel numbers whenever L_k is odd. Our aim is to show this set of implications holds for all k in some arithmetic progression. We can then deduce the existence of infinitely many Lucas numbers which are also Riesel numbers.

We begin by noting that the only Lucas numbers which are even are those satisfying $k \equiv 0 \pmod 3$. In order to have L_k be a Riesel number (using this covering), we would need to solve $L_k \equiv a \pmod m$ for k in each row of the Table 2. We denote this set of solutions as $\mathcal{B}(a, m) = \{k : L_k \equiv a \pmod m\}$. These sets are computed in (2.1).

We use that the Lucas numbers are periodic modulo m. In fact, the period of the Lucas numbers modulo m divides the period of the Fibonacci numbers modulo m [9]. Thus, the modulus that appears in each $\mathcal{B}(a, m)$-set in (2.1) is actually the period of the Fibonacci numbers modulo m.

$$\begin{array}{rcl}
\mathcal{B}(2,3) & = & \{0,5,7\} \pmod 8 \\
\mathcal{B}(4,5) & = & \{3\} \pmod 4 \\
\mathcal{B}(16,17) & = & \{12,19,24,35\} \pmod{36} \\
\mathcal{B}(256,257) & = & \{172,259,344,515\} \pmod{516} \\
\mathcal{B}(3,13) & = & \{2,7,26\} \pmod{28} \\
\mathcal{B}(34,37) & = & \{36,40,51,63\} \pmod{76} \\
\mathcal{B}(4,73) & = & \{3,71\} \pmod{148} \\
\mathcal{B}(365,1153) & = & \{499,655\} \pmod{2308} \\
\mathcal{B}(2167,6337) & = & \{115,5748,6223,6928\} \pmod{12676} \\
\mathcal{B}(1,7) & = & \{1,7\} \pmod{16}
\end{array} \tag{2.1}$$

Now it can be checked that if k modulo 55716312432816 is congruent to one of the following 16 integers:

$$\begin{array}{cccc}
17304307932583, & 19044893268919, & 20236745429047, & 21977330765383, \\
23580842262103, & 25321427598439, & 26513279758567, & 28253865094903, \\
38386155880135, & 40126741216471, & 41318593376599, & 43059178712935, \\
44662690209655, & 46403275545991, & 47595127706119, & 49335713042455,
\end{array}$$

then k lies in the intersection of the $\mathcal{B}(a, m)$ sets. Finally, since none of these congruences for k includes any multiples of 3, all such L_k are odd. Thus, L_k is both a Riesel number and a Lucas number. Hence, there are infinitely many Riesel numbers in the sequence of Lucas numbers.

3. Lucas-Sierpiński Numbers

In this section, we show how the covering from Table 2 in Section 2 can be utilized to find infinitely many k such that L_k is a Sierpiński number. Consider the implications in Table 3.

$n \equiv 1 \pmod 2$	&	$L_k \equiv 1 \pmod 3$	$\Longrightarrow$	$L_k \cdot 2^n + 1 \equiv 0 \pmod 3$
$n \equiv 2 \pmod 4$	&	$L_k \equiv 1 \pmod 5$	$\Longrightarrow$	$L_k \cdot 2^n + 1 \equiv 0 \pmod 5$
$n \equiv 4 \pmod 8$	&	$L_k \equiv 1 \pmod{17}$	$\Longrightarrow$	$L_k \cdot 2^n + 1 \equiv 0 \pmod{17}$
$n \equiv 8 \pmod{16}$	&	$L_k \equiv 1 \pmod{257}$	$\Longrightarrow$	$L_k \cdot 2^n + 1 \equiv 0 \pmod{257}$
$n \equiv 32 \pmod{48}$	&	$L_k \equiv -3 \pmod{13}$	$\Longrightarrow$	$L_k \cdot 2^n + 1 \equiv 0 \pmod{13}$
$n \equiv 28 \pmod{36}$	&	$L_k \equiv 3 \pmod{37}$	$\Longrightarrow$	$L_k \cdot 2^n + 1 \equiv 0 \pmod{37}$
$n \equiv 16 \pmod{36}$	&	$L_k \equiv -4 \pmod{73}$	$\Longrightarrow$	$L_k \cdot 2^n + 1 \equiv 0 \pmod{73}$
$n \equiv 112 \pmod{288}$	&	$L_k \equiv -365 \pmod{1153}$	$\Longrightarrow$	$L_k \cdot 2^n + 1 \equiv 0 \pmod{1153}$
$n \equiv 256 \pmod{288}$	&	$L_k \equiv -2167 \pmod{6337}$	$\Longrightarrow$	$L_k \cdot 2^n + 1 \equiv 0 \pmod{6337}$
$n \equiv 0 \pmod 3$	&	$L_k \equiv -1 \pmod 7$	$\Longrightarrow$	$L_k \cdot 2^n + 1 \equiv 0 \pmod 7$

Table 3

The congruences for n in the table form a covering; these are the same congruences as in Table 2. These implications show that if L_k satisfied all of these congruences simultaneously, then L_k is a Sierpiński number, as long as L_k is odd.

To show there exist infinitely many integers k satisfying all of the implications in Table 2, we begin by recalling that the only Lucas numbers which are even are those satisfying $k \equiv 0 \pmod 3$. As before, the sets $\mathcal{B}(a, m)$ are computed in the table below:

$$\begin{aligned}
\mathcal{B}(1,3) &= \{0,5,7\} \pmod 8 \\
\mathcal{B}(1,5) &= \{3\} \pmod 4 \\
\mathcal{B}(1,17) &= \{12,19,24,35\} \pmod{36} \\
\mathcal{B}(1,257) &= \{172,259,344,515\} \pmod{516} \\
\mathcal{B}(-3,13) &= \{2,7,26\} \pmod{28} \\
\mathcal{B}(3,37) &= \{36,40,51,63\} \pmod{76} \\
\mathcal{B}(-4,73) &= \{3,71\} \pmod{148} \\
\mathcal{B}(-365,1153) &= \{499,655\} \pmod{2308} \\
\mathcal{B}(-2167,6337) &= \{115,5748,6223,6928\} \pmod{12676} \\
\mathcal{B}(-1,7) &= \{1,7\} \pmod{16}.
\end{aligned} \tag{3.1}$$

Now it can be checked that k lies in the intersection of the $\mathcal{B}(a, m)$ sets if $k \pmod{55716312432816}$ is in one of the following 32 residue classes:

3563460609625,	5304045945961,	6380599390361,	6495898106089,
8121184726697,	8236483442425,	9313036886825,	9839994939145,
11053622223161,	11580580275481,	12657133719881,	12772432435609,
14397719056217,	14513017771945,	15589571216345,	17330156552681,
27462447337913,	29203032674249,	30394884834377,	32135470170713,
33738981667433,	35479567003769,	36671419163897,	38197925094889,
38412004500233,	39938510431225,	41130362591353,	42870947927689,
44474459424409,	46215044760745,	47406896920873,	49147482257209.

Again, these congruences for k do not include any $k \equiv 0 \pmod 3$, so all such L_k are odd. Hence, we deduce L_k is both a Sierpiński number and a Lucas number. Thus, there are infinitely many Sierpiński numbers in the sequence of Lucas numbers.

4. Lucas Numbers That are Not a Sum of Two Prime Powers

Luca and Stănică [6] showed there exist infinitely many Fibonacci numbers that are not a sum of two prime powers. That is, they are not of the form $p^a + q^b$ with primes p and q and non-negative integers a and b. In this section, we prove an analogous result for the Lucas numbers. In particular, we prove the following theorem.

Theorem 4.1. *There are infinitely many Lucas numbers L_n that cannot be represented as $p^a + q^b$ for some primes p and q and nonnegative integers a and b.*

To prove the theorem, we begin by observing the congruences shown in Table 4. Again, we note that the congruences involving n form a covering of the integers.

$$\begin{array}{lcl}
n \equiv 1 \pmod 2 & \& & L_k \equiv 2^1 \pmod 3 \\
n \equiv 2 \pmod 4 & \& & L_k \equiv 2^2 \pmod 5 \\
n \equiv 4 \pmod 8 & \& & L_k \equiv 2^4 \pmod{17} \\
n \equiv 8 \pmod{16} & \& & L_k \equiv 2^8 \pmod{257} \\
n \equiv 16 \pmod{32} & \& & L_k \equiv 2^{16} \pmod{65537} \\
n \equiv 32 \pmod{64} & \& & L_k \equiv 2^{32} \pmod{641} \\
n \equiv 0 \pmod{64} & \& & L_k \equiv 2^0 \pmod{6700417}
\end{array}$$

Table 4

The solutions for k in each of the congruences involving L_k in Table 4 are, respectively,

$$\begin{aligned}
\mathcal{B}(2,3) &= \{0,5,7\} \pmod 8 \\
\mathcal{B}(2^2,5) &= \{3\} \pmod 4 \\
\mathcal{B}(2^4,17) &= \{12,19,24,35\} \pmod{36} \\
\mathcal{B}(2^8,257) &= \{172,259,344,515\} \pmod{516} \\
\mathcal{B}(2^{16},65537) &= \{7283,14563\} \pmod{14564} \\
\mathcal{B}(2^{32},641) &= \{1,319\} \pmod{640} \\
\mathcal{B}(1,6700417) &= \{6700419,13400835\} \pmod{13400836}.
\end{aligned} \tag{4.1}$$

Observe that the intersection of the sets above is nonempty; in fact, every integer congruent modulo 3021228124801920 to one of the following 4 integers:

$$799976513568959, \quad 878044423770559, \quad 2550328108096319, \quad 2628396018297919$$

is in the intersection of the $\mathcal{B}$-sets listed in (4.1).

Note all such k are not divisible by 3, so L_k is odd. To complete the proof, suppose now that such a Lucas number L_k can be expressed as a sum of two prime powers: $L_k = p^a + q^b$. As L_k is odd, we must have $L_k = 2^a + q^b$. Since the congruences for n in Table 4 form a covering of the integers, a must fit into a residue class expressed in one of the rows of the table. Suppose we have $a \equiv a_i \pmod{b_i}$, where $n \equiv a_i \pmod{b_i}$ and $L_k \equiv 2^{a_i} \pmod{p_i}$ is a row in Table 4.

Observe $2^{b_i} \equiv 1 \pmod{p_i}$. We deduce that $L_k \equiv 2^a \pmod{p_i}$. In particular, $p_i \mid (L_k - 2^a)$. However, $L_k - 2^a = q^b$, so that $q = p_i$. Thus, $q \in \{3,5,17,257,65537,641,6700417\}$. Recall Lucas numbers can be expressed as $L_k = \alpha^k + \beta^k$, where $\alpha = \frac{1}{2}(1+\sqrt{5})$ and $\beta = \frac{1}{2}(1-\sqrt{5})$. The equation $\alpha^k + \beta^k = 2^a + q^b$ can be rewritten as an $\mathcal{S}$-unit equation known to have only

finitely many solutions (k, a, b) (cf. [2, 3, 5]). Thus, if we take k sufficiently large, there are no solutions to $L_k = 2^a + q^b$ for $q \in \{3, 5, 17, 257, 65537, 641, 6700417\}$. We deduce if k is sufficiently large and in the intersection of the $\mathcal{B}$-sets, then L_k is a Lucas number that is not a sum of two prime powers.

5. Acknowledgements

The authors wish to thank the referee for the valuable suggestions. This work was completed while the second author was an R. E. Lee Summer Scholar at Washington and Lee University. He wishes to thank the Christian Johnson Foundation for supporting the R. E. Lee Scholar program. In addition, the third author was supported by Washington and Lee University's Lenfest Grant during the writing of this article. She gratefully acknowledges the support of Mr. Gerry Lenfest for this program. Finally, the third author expresses her gratitude to the staff of the Gray-Lester Library at Stuart Hall School for the workspace and their support while writing this article.

References

[1] H. T. Engstrom, *Periodicity in sequences defined by linear recurrence relations*, Proceedings of the National Academy of Sciences of the United States of America, 16 (10), 1930, 663–665.
[2] J.-H. Evertse, K. Győry, C. L. Stewart, and R. Tijdeman, *S-Unit equations and their applications*, New Advances in Transcendence Theory, (Durham, 1986), 110–174, Cambridge Univ. Press, Cambridge, 2988.
[3] J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. Math., **155** (2002), 1–30.
[4] F. Luca and V. J. Mejía Huguet, *Fibonacci-Riesel and Fibonacci-Sierpiński numbers*, The Fibonacci Quarterly, **46/47.3** (2008/2009), 216–219.
[5] F. Luca and P. Stănică, *Fibonacci numbers of the form $p^a \pm p^b$*, Proceedings of the Eleventh International Conference on Fibonacci Numbers and their Applications, Congr. Numer., **194** (2009), 177–183.
[6] F. Luca and P. Stănică, *Fibonacci numbers that are not sums of two prime powers*, Proceedings of AMS, **133** (2005), 1887–1890.
[7] H. Riesel, *Några stora primtal*, Elementa, **39** (1956), 258–260.
[8] W. Sierpiński, *Sur un problème concernant les nombres $k2^n + 1$*, Elem. Math., **15** (1960), 73–74.
[9] D. D. Wall, *Fibonacci series modulo m*, Amer. Math. Monthly, **67** (1960), 525–532.

MSC2010: 11B39, 11B25, 11B50, 11P32

Mathematics Department, The University of Findlay, Findlay, OH 45840
E-mail address: baczkowski@findlay.edu

Mathematics Department, Washington and Lee University, Lexington, VA 24450
E-mail address: fasorantio12@mail.wlu.edu

Mathematics Department, Washington and Lee University, Lexington, VA 24450
E-mail address: finchc@wlu.edu