Journal of Number Theory 173 (2017) 87–99

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Primefree shifted Lucas sequences of the second kind

Dan Ismailescu[a], Lenny Jones[b,*], Tristan Phillips[b]

[a] *Department of Mathematics, Hofstra University, Hempstead, NY, USA*
[b] *Department of Mathematics, Shippensburg University, PA, USA*

ARTICLE INFO

Article history:
Received 4 January 2016
Received in revised form 1 September 2016
Accepted 2 September 2016
Available online 9 November 2016
Communicated by D. Goss

MSC:
primary 11B37, 11B39
secondary 11B83

Keywords:
Lucas sequences
Primefree
Coverings

ABSTRACT

We say a sequence $\mathcal{S} = (s_n)_{n \geq 0}$ is *primefree* if $|s_n|$ is not prime for all $n \geq 0$ and, to rule out trivial situations, we require that no single prime divides all terms of $\mathcal{S}$. Recently, the second author showed that there exist infinitely many integers k such that both of the shifted sequences $\mathcal{U} \pm k$ are simultaneously primefree, where $\mathcal{U}$ is a particular Lucas sequence of the first kind. In this article, we prove an analogous result for the Lucas sequences $\mathcal{V}_a = (v_n)_{n \geq 0}$ of the second kind, defined by

$$v_0 = 2, \quad v_1 = a, \quad \text{and} \quad v_n = av_{n-1} + v_{n-2}, \quad \text{for } n \geq 2,$$

where a is a fixed integer. More precisely, we show that for any integer a, there exist infinitely many integers k such that both of the shifted sequences $\mathcal{V}_a \pm k$ are simultaneously primefree. This result provides additional evidence to support a conjecture of Ismailescu and Shim. Moreover, we show that there are infinitely many values of k such that every term of both of the shifted sequences $\mathcal{V}_a \pm k$ has at least two distinct prime factors.

* Corresponding author.
E-mail addresses: Dan.P.Ismailescu@hofstra.edu (D. Ismailescu), lkjone@ship.edu (L. Jones), tp7924@ship.edu (T. Phillips).

http://dx.doi.org/10.1016/j.jnt.2016.09.016

1. Introduction

For a given sequence $\mathcal{S} = (s_n)_{n\geq 0}$, and $k \in \mathbb{Z}$, we let $\mathcal{S} + k$ denote the k-shifted sequence $(s_n + k)_{n\geq 0}$. We say that $\mathcal{S}+k$ is *primefree* if $|s_n + k|$ is not prime for all $n \geq 0$ and, to rule out trivial situations, we require that no single prime divides all terms of $\mathcal{S} + k$. Recently, the second author [8] showed that there exist infinitely many integers k such that both of the shifted sequences $\mathcal{U}_a \pm k$ are simultaneously primefree, where $\mathcal{U}_a = (u_n)_{n\geq 0}$ is the Lucas sequence of the first kind defined by

$$u_0 = 0, \quad u_1 = 1, \quad \text{and} \quad u_n = au_{n-1} + u_{n-2}, \quad \text{for } n \geq 2, \tag{1.1}$$

with a a fixed integer. The second author also showed in [8] that infinitely many values of k exist such that each term of both primefree shifted sequences has at least two distinct prime divisors.

In this article, using techniques similar to the methods used in [8], we establish an analogous result for certain Lucas sequences of the second kind. In particular, we prove

Theorem 1.1. *For any $a \in \mathbb{Z}$, there exist infinitely many integers k, such that both of the shifted sequences $\mathcal{V}_a \pm k$ are primefree, where $\mathcal{V}_a$ is the Lucas sequence $(v_n)_{n\geq 0}$ of the second kind, defined by*

$$v_0 = 2, \quad v_1 = a, \qquad \textit{and} \qquad v_n = av_{n-1} + v_{n-2}, \quad \textit{for } n \geq 2.$$

Moreover, there exist infinitely many values of k such that every term in both of the primefree shifted sequences $\mathcal{V}_a \pm k$ has at least two distinct prime factors.

We should point out that Theorem 1.1 provides additional evidence to support the following conjecture of Ismailescu and Shim [6].

Conjecture 1.2. *Let $(x_n)_{n\geq 0}$ be an integer sequence defined by a second order recurrence relation $x_{n+2} = ax_{n+1} + bx_n$, where a and b are integers. Further assume that $\lim_{n\to\infty} |x_n| = \infty$. Then there exist integers k that cannot be written in the form $\pm x_n \pm p$ for any n and any prime p.*

Maple and Magma were used to perform some of the calculations in this article.

2. Preliminaries

Our main focus in this article is on certain Lucas sequences of the second kind.

Definition 2.1. Let $a \in \mathbb{Z}$, and let $\mathcal{V}_a = (v_n)_{n\geq 0}$ denote the *Lucas sequence of the second kind* defined by

$$v_0 = 2, \quad v_1 = a, \quad \text{and} \quad v_n = av_{n-1} + v_{n-2}, \quad \text{for } n \geq 2.$$

Remark 2.2. We note two items:

(1) For $a > 0$, we have that

$$v_n(-a) = (-1)^n v_n(a),$$

where $v_n(-a)$ is the nth term of $\mathcal{V}_{-a}$ and $v_n(a)$ is the nth term of $\mathcal{V}_a$. Thus, we need only consider the situations with $a \geq 0$

(2) For all $n \geq 1$, the sequence $\mathcal{V}_a$ is related to the sequence $\mathcal{U}_a$, defined in (1.1), by the relationship $v_n = u_{2n}/u_n$.

We require several key ingredients in our process. The first ingredient is the notion of a primitive divisor. For the sequence $\mathcal{V}_a$, we define a *primitive divisor* of the term v_n to be a prime number p such that $v_n \equiv 0 \pmod{p}$ but $v_m \not\equiv 0 \pmod{p}$ for all $m < n$. The following theorem concerning primitive divisors of Lucas sequences of the first kind, as defined in (1.1), is a special case of a much more general theorem that is the culmination of work initiated by Carmichael [3] and completed by others [2].

Theorem 2.3. *Let $a \geq 1$ be an integer. Then every term u_n of $\mathcal{U}_a$ has a primitive divisor with the following exceptions, which are indicated as ordered pairs $[a, n]$:*

$$[a, 0], [a, 1], [1, 2], [1, 6], [1, 12], [3, 6].$$

Because of item (2) in Remark 2.2, the primitive divisors of $\mathcal{V}_a$ are intimately related to the primitive divisors of $\mathcal{U}_a$, and therefore we have the following.

Corollary 2.4. *Let $a \geq 1$ be an integer. Then every term v_n of $\mathcal{V}_a$ has a primitive divisor with the following exceptions, which are indicated as ordered pairs $[a, n]$:*

$$[2^c, 1], [1, 3], [1, 6], [3, 3]$$

where $c \geq 0$ is an integer.

Remark 2.5. Unlike $\mathcal{U}_a$, it is not always true that a particular prime will appear as the primitive divisor of some term in $\mathcal{V}_a$. See, for example, [9].

A second ingredient needed for our methods is the concept of periodicity of $\mathcal{V}_a$. It is well known that the sequence $\mathcal{V}_a$ is purely periodic modulo a prime p [5]. The *period* of $\mathcal{V}_a$ modulo p, which we denote $\mathcal{P}_p := \mathcal{P}_p(a)$, is the smallest positive integer h such that $v_h \equiv 2 \pmod{p}$ and $v_{h+1} \equiv a \pmod{p}$. We refer to the actual list of residues that occur modulo p from index 0 to index $h - 1$ as the *cycle of $\mathcal{V}_a$ modulo p*. For example, if $a = 1$ and $p = 3$, then $\mathcal{P}_3 = 8$ and the cycle of $\mathcal{V}_1$ modulo 3 is $[2, 1, 0, 1, 1, 2, 0, 2]$. We label the positions in the cycle starting at 0, so that the residue at position 6 is 0 in our example.

To facilitate our approach in this article, it is convenient to make the following definitions.

Definition 2.6. Let x be a variable and let $\widehat{\mathcal{V}}_x = (\widehat{v}_n)_{n\geq 0}$ be the sequence of polynomials in x defined by

$$\widehat{v}_0 = 2, \quad \widehat{v}_1 = x, \qquad \text{and} \qquad \widehat{v}_n = x\widehat{v}_{n-1} + \widehat{v}_{n-2}, \quad \text{for } n \geq 2.$$

For a monic polynomial $f(x) \in \mathbb{Z}[x]$, we define the *generic period* modulo $f(x)$ of $\widehat{\mathcal{V}}_x$, denoted $\widehat{\mathcal{P}}_f$, to be the smallest positive integer m, if it exists, such that

$$\widehat{v}_m \equiv 2 \pmod{f(x)} \qquad \text{and} \qquad \widehat{v}_{m+1} \equiv x \pmod{f(x)}.$$

If such an integer m does not exist, we define $\widehat{\mathcal{P}}_f = \infty$. When $\widehat{\mathcal{P}}_f$ is finite, we call the list of residues modulo $f(x)$ that appear, in order starting at index 0 up to index $\widehat{\mathcal{P}}_f - 1$, the *generic cycle of* $\widehat{\mathcal{V}}_x$ *modulo* $f(x)$, and we denote it as Γ_f. For a given positive integer a, we also let $\Gamma_f|_{x=a}$ denote this generic cycle specialized at $x = a$.

Remark 2.7. The polynomials $\widehat{v}_n$ in Definition 2.6 are known as the *Lucas polynomials*.

Definition 2.8. A *generic primitive divisor* of $\widehat{v}_n$ is a monic irreducible polynomial $f(x)$ of positive degree such that $\widehat{v}_n \equiv 0 \pmod{f(x)}$ but $\widehat{v}_m \not\equiv 0 \pmod{f(x)}$ for all indices $m < n$.

Note that Corollary 2.4 guarantees the existence of a primitive divisor of $\widehat{v}_n$, other than the possible exceptions listed there. In reality, there are no exceptions in the generic situation since we see that x, x^2+3, and x^4+4x^2+1 are generic primitive divisors of $\widehat{v}_1$, $\widehat{v}_3$ and $\widehat{v}_6$ respectively. It can also be shown that each term $\widehat{v}_n$ has exactly one generic primitive divisor [10], and so we denote it as $f_n(x)$. Consequently, the primitive divisors of $\mathcal{V}_a$ occur as prime divisors of $f_n(a)$. Also, if we let p be a prime divisor of $f_n(a)$, then $\mathcal{P}_p$ is a divisor of $\widehat{\mathcal{P}}_f$.

A third ingredient we require is a concept originally due to Erdős [4].

Definition 2.9. A *(finite) covering system* $\mathcal{C}$, or simply a *covering*, of the integers is a system of $t < \infty$ congruences $x \equiv r_i \pmod{m_i}$, with $m_i > 1$ for all $1 \leq i \leq t$, such that every integer n satisfies at least one of these congruences.

In this article, we represent a covering $\mathcal{C}$ as a set of ordered pairs $\{(r_i, m_i)\}$, where $x \equiv r_i \pmod{m_i}$ is a congruence in $\mathcal{C}$. Additionally, associated to each congruence $(r_i, m_i) \in \mathcal{C}$ is a corresponding prime p_i, where m_i is the period of the particular Lucas sequence $\mathcal{V}_a$ modulo p_i.

Finally, in this section we present, without proof, a lower bound on linear forms in logarithms, due to Baker [1]. This result is necessary to establish the existence of infinitely many values of k in Theorem 1.1, such that every term in both of the shifted sequences $\mathcal{V}_a \pm k$ has at least two distinct prime factors.

Theorem 2.10. *Let $\xi_1, \ldots, \xi_t \in \mathbb{C} \setminus \{0, 1\}$ be algebraic numbers, and let $b_1, \ldots, b_t$ be rational integers such that $\xi_1^{b_1} \cdots \xi_t^{b_t} \neq 1$. Then*

$$\left| \xi_1^{b_1} \cdots \xi_t^{b_t} - 1 \right| \geq B^{-C},$$

where $B = \max(|b_1|, \ldots, |b_t|)$ and C is an effectively computable constant depending on t and the heights of $\xi_1, \ldots, \xi_t$.

3. The proof of Theorem 1.1

Before we begin the proof of Theorem 1.1, we first describe, for any fixed integer $a \geq 1$, a general process that can be used in the situation of finding infinitely many integers k such that the single sequence $\mathcal{V}_a + k$ is primefree. The idea is to build a covering $\mathcal{C} = \{(r_i, m_i)\}$, where $m_i = \mathcal{P}_p$ for some prime p, and r_i is a position in the cycle of residues modulo p. Then, when $n \equiv r_i \pmod{m_i}$, we have that

$$v_n + k \equiv v_{r_i} + k \pmod{p}.$$

Solving the congruence $v_{r_i} + k \equiv 0 \pmod{p}$ for k gives us a value of k such that the term $v_n + k$ in $\mathcal{V}_a + k$ is divisible by p whenever $n \equiv r_i \pmod{m_i}$. For k sufficiently large, $u_n + k$ will be larger than p, and hence composite. If the residue ρ that appears at location r_i is repeated at another location, say s_i, in a single cycle modulo p, then we can also use the congruence (s_i, m_i) in our covering since the resulting congruences for k modulo p will be consistent. In fact, we can repeat the particular modulus m_i in our covering as many times as ρ appears in a single cycle modulo p. Note, however, that the repeated use of a single modulus in this manner might not always be beneficial in building the covering if the new locations produce congruences that are redundant with other congruences arising from other moduli. If we are fortunate enough to be able to build a covering using these ideas, then we can use the Chinese remainder theorem to piece together the values of k found for each prime to get an infinite arithmetic progression of values of k modulo the product of all primes in $\mathcal{D}_a$, the finite set of primes used to build the covering. Thus, for each of these values of k in the arithmetic progression, we have that every term in $\mathcal{V}_a + k$ is divisible by at least one prime in $\mathcal{D}_a$. Since for k sufficiently large in the arithmetic progression, every term of $\mathcal{V}_a + k$ is larger than the largest prime in $\mathcal{D}_a$, we have successfully found infinitely many integers k such that the sequence $\mathcal{V}_a + k$ is primefree. These methods were employed in [7,8], and in [6] for $a = 1$, where all the primes used were, in fact, primitive divisors. In light of Remark 2.5, building a covering in the situation of $\mathcal{V}_a$ appears potentially more difficult than for $\mathcal{U}_a$, if we require all primes used to be primitive divisors. However, there is no necessity to avoid primes that are not primitive divisors since our main concern is the periods of these primes, which are used as moduli in the coverings. Nevertheless, it is still unclear whether this approach would be successful for every such value of a. In particular, can a suitable covering be built for any integer $a \geq 1$?

An additional complication is that we also require the sequence $\mathcal{V}_a - k$ to be primefree. Because of this added restriction, we need to build two coverings: $\mathcal{C}^+ = \{(r_i, m_i)\}$ for the sequence $\mathcal{V}_a + k$, and $\mathcal{C}^- = \{(s_i, t_i)\}$ for the sequence $\mathcal{V}_a - k$. The coverings $\mathcal{C}^+$ and $\mathcal{C}^-$ must be compatible in the sense that if $m_i = t_i$, and if we use the same prime p when we solve for k using each of the congruences (r_i, m_i) and (s_i, t_i), then we must have

$$u_{s_i} \equiv -u_{r_i} \pmod{p}.$$

As an example, suppose that $a = 9$, and that we use the prime $p = 19$. The cycle of $\mathcal{V}_9$ modulo $p = 19$ is

$$[2, 9, 7, 15, 9, 1, 18, 11, 3, 0, 3, 8, 18, 18, 9, 4, 7, 10] \tag{3.1}$$

so that $\mathcal{P}_{19} = 18$. Since the residue $\rho = 9$ appears at locations 1, 4 and 14, we can use the three congruences $(1, 18)$, $(4, 18)$ and $(14, 18)$ to build one of the coverings $\mathcal{C}^+$ or $\mathcal{C}^-$. If we choose to use these congruences for $\mathcal{C}^+$, then we can use only the congruence $(17, 18)$ for $\mathcal{C}^-$ in this situation, since 17 is the only location in the cycle (3.1) for which the residue $-\rho = -9 \equiv 10 \pmod{19}$ appears. Of course, we are not forced here into choosing these particular congruences. There are other possibilities. One such alternative is that we could use the congruence $(9, 18)$ in both $\mathcal{C}^+$ or $\mathcal{C}^-$, since the residue is 0 at location 9 of (3.1).

Proof of Theorem 1.1. In light of item (1) of Remark 2.2, we can restrict our attention to $a \geq 0$. We begin with the case $a = 0$, which is somewhat trivial and misleading due to the fact that

$$\mathcal{V}_0 = (2, 0, 2, 0, \ldots)$$

has period 2 with cycle $[2, 0]$ modulo any odd prime. Consequently, we have

$$\mathcal{C}^+ = \mathcal{C}^- = \{(0, 2), (1, 2)\}.$$

We choose to use the primes 3, 5, 7 and 11 for $\mathcal{C}^+$, and the primes 3, 5, 13 and 19 for $\mathcal{C}^-$, where 3 and 5 correspond to the congruence $(1, 2)$ in both coverings. This choice gives us the following system of congruences for k:

$$\begin{array}{lll} k \equiv 0 \pmod{3} & k \equiv 5 \pmod{7} & k \equiv 2 \pmod{13} \\ k \equiv 0 \pmod{5} & k \equiv 9 \pmod{11} & k \equiv 2 \pmod{19}. \end{array}$$

To ensure that k is odd (to avoid a trivial situation), we add the congruence $k \equiv 1 \pmod 2$ to the system. Solving this system gives $k \equiv 4695 \pmod{570570}$. Then it is easy to see that $|\pm k|$ and $|2 \pm k|$ are all divisible by at least two primes from the set $\{3, 5, 7, 11, 13, 19\}$.

Now we let $a \geq 1$, and we focus first on the primefree part of the theorem. We treat the cases $a \in \{1, 2, 3, 4\}$ individually.

Suppose first that $a = 1$. We use the list of primes

$$P = [2, 3, 5, 7, 17, 19, 23, 47, 107, 103681],$$

and the corresponding list of periods

$$\mathcal{P} = [3, 8, 4, 16, 36, 18, 48, 32, 72, 144]$$

as moduli to build the coverings. Note that the least common multiple of these moduli is 288. Examining the cycles produced by these primes, and using the strategy outlined earlier in this section, we build the coverings:

$$\begin{aligned}
\mathcal{C}^+ = \{&(1,3),(2,3),(2,8),(6,8),(3,4),(4,16),(12,16),(21,36),\\
&(33,36),(9,18),(8,32),(24,32),(0,72),(48,144),(96,144)\},\\
\mathcal{C}^- = \{&(1,3),(2,3),(2,8),(6,8),(1,4),(4,16),(12,16),\\
&(15,36),(3,36),(9,18),(0,48),(8,32),(24,32)\}.
\end{aligned}$$

From these coverings, we create the following system of congruences for k:

$$\begin{array}{ll}
k \equiv 1 \pmod{2} & k \equiv 0 \pmod{19}\\
k \equiv 0 \pmod{3} & k \equiv 2 \pmod{23}\\
k \equiv 1 \pmod{5} & k \equiv 0 \pmod{47}\\
k \equiv 0 \pmod{7} & k \equiv 105 \pmod{107}\\
k \equiv 4 \pmod{17} & k \equiv 1 \pmod{103681}
\end{array}$$

Using the Chinese remainder theorem to solve this system gives

$$k = 37906473446751$$

as the smallest positive solution.

Next, suppose that $a = 2$. In this case, to avoid the trivial situation of having every term in the shifted sequences divisible by 2, we cannot use the prime 2. The construction of the covering then becomes a bit more difficult. We use the list of primes

$$P = [3, 5, 7, 11, 17, 73, 97, 179, 197, 199, 577, 1009, 1153, 13729, 1523089],$$

and the corresponding list of periods

$$\mathcal{P} = [8, 12, 6, 24, 16, 72, 96, 72, 36, 18, 32, 144, 48, 96, 144]$$

as moduli to build the coverings. As in the case $a = 1$, the least common multiple of these moduli is 288. We proceed as before to build the coverings:

$$\begin{aligned}\mathcal{C}^+ = \{&(2,8),(6,8),(0,12),(1,12),(5,12),(3,6),(23,24),(4,16),(12,16),(43,72),\\&(32,96),(64,96),(7,72),(23,36),(31,36),(1,18),(8,32),(24,32),\\&(11,144),(35,48),(16,96),(80,96),(107,144)\},\\ \mathcal{C}^- = \{&(2,8),(6,8),(7,12),(11,12),(3,6),(0,24),(1,24),(4,16),(12,16),\\&(29,72),(16,96),(80,96),(65,72),(5,36),(13,36),(17,18),(8,32),(24,32),\\&(133,144),(13,48),(32,96),(64,96),(37,144)\}.\end{aligned}$$

From these coverings, we create a system of congruences for k. To completely avoid values of k such that every term in the shifted sequences is even, we add the additional congruence $k \equiv 1 \pmod 2$:

$$\begin{array}{ll} k \equiv 1 \pmod{2} & k \equiv 59 \pmod{179} \\ k \equiv 0 \pmod{3} & k \equiv 82 \pmod{197} \\ k \equiv 3 \pmod{5} & k \equiv 197 \pmod{199} \\ k \equiv 0 \pmod{7} & k \equiv 0 \pmod{577} \\ k \equiv 2 \pmod{11} & k \equiv 915 \pmod{1009} \\ k \equiv 0 \pmod{17} & k \equiv 96 \pmod{1153} \\ k \equiv 40 \pmod{73} & k \equiv 13728 \pmod{13729} \\ k \equiv 1 \pmod{97} & k \equiv 110880 \pmod{1523089} \end{array}$$

Using the Chinese remainder theorem to solve this system gives

$$k = 45902855345456873184678819298233$$

as the smallest positive solution.

Next, suppose that $a = 3$. We use the primes $P = [2, 3, 5, 13]$, together with the corresponding periods $\mathcal{P} = [3, 2, 12, 4]$ as moduli, and proceed as before to construct the coverings:

$$\mathcal{C}^+ = \{(1,3),(2,3),(1,2),(0,12),(2,4)\},$$

$$\mathcal{C}^- = \{(1,3),(2,3),(1,2),(6,12),(0,4)\}.$$

These coverings give rise to the following system of congruences for k:

$$\begin{array}{ll} k \equiv 1 \pmod{2} & k \equiv 3 \pmod{5} \\ k \equiv 0 \pmod{3} & k \equiv 2 \pmod{13}. \end{array}$$

Table 1
Indices N, primitive divisors F and generic periods $\widehat{\mathcal{P}}$.

N	F	$\widehat{\mathcal{P}}$
2	x^2+2	8
3	x^2+3	6
4	x^4+4x^2+2	16
6	x^4+4x^2+1	24
8	$x^8+8x^6+20x^4+16x^2+2$	32
9	$x^6+6x^4+9x^2+3$	18
12	$x^8+8x^6+20x^4+16x^2+1$	48
18	$x^{12}+12x^{10}+54x^8+112x^6+105x^4+36x^2+1$	72
36	$x^{24}+24x^{22}+252x^{20}+1520x^{18}+5814x^{16}+14688x^{14}$ $+24752x^{12}+27456x^{10}+19305x^8+8008x^6+1716x^4+144x^2+1$	144

Table 2
Non-primitive divisors G_i and their generic periods $\widehat{\mathcal{P}}$.

i	G_i	$\widehat{\mathcal{P}}$
1	x^2+1	12
2	x^2+4	4
3	$x^6+6x^4+9x^2+1$	36

Solving this system, using the Chinese remainder theorem, produces the solution $k \equiv 93 \pmod{390}$. It is interesting to note (and easy to show) that $k = 93$ is actually the smallest positive integer such that both of the sequences $\mathcal{V}_3 \pm k$ are primefree.

Now suppose that $a \geq 4$. We use the ideas of generic cycle and generic primitive divisor from Section 2 to aid in the construction of two "generic" coverings $\widehat{\mathcal{C}}^+$ and $\widehat{\mathcal{C}}^-$. These coverings are actual coverings of the integers, but they are generic in the sense that they can be used to achieve the desired result upon specialization at any particular value of a. To complete these coverings, we also require the use of three generic moduli, G_1, G_2 and G_3, that are not generic primitive divisors of any term of $\widehat{\mathcal{V}}_x$.

For each index N_i in the list

$$N = [2, 3, 4, 6, 8, 9, 12, 18, 36], \tag{3.2}$$

we calculate the generic primitive divisor $F_i := f_{N_i}(x)$ of $\widehat{v}_{N_i}$, and the generic period $\widehat{\mathcal{P}}_i := \widehat{\mathcal{P}}_{F_i}$ for each i with $1 \leq i \leq 9$. This information is provided in Table 1. Note that, by the restrictions on a, we have avoided the exceptional cases, as given in Corollary 2.4, in the list (3.2). Observe that the additional polynomials G_i required to complete the coverings are listed in Table 2.

We now construct the coverings $\widehat{\mathcal{C}}^+$ and $\widehat{\mathcal{C}}^-$ using as our moduli the elements of the complete list of generic periods:

$$\widehat{\mathcal{P}} = [8, 6, 16, 24, 32, 18, 48, 72, 144, 12, 4, 36].$$

Observe that the least common multiple of the elements in $\widehat{\mathcal{P}}$ is 288. To construct $\widehat{\mathcal{C}}^+$ and $\widehat{\mathcal{C}}^-$, we begin with the elements F_i of Table 1 and examine for each i what residues

Table 3
Generic residues in Γ_4.

Location	Generic residue	Location	Generic residue
0	2	12	-2
1	x	13	$-x$
2	x^2+2	14	$-x^2-2$
3	x^3+3x	15	$-x^3-3x$
4	1	16	-1
5	x^3+4x	17	$-x^3-4x$
6	0	18	0
7	x^3+4x	19	$-x^3-4x$
8	-1	20	1
9	x^3+3x	21	$-x^3-3x$
10	$-x^2-2$	22	x^2+2x
11	x	23	$-x$

appear, and where they appear, in the generic cycle $\Gamma_i := \Gamma_{F_i}$ of $\widehat{\mathcal{V}}_x$ modulo F_i. For example, for $i=1$, we have

$$N_i = N_1 = 2, \quad F_i = F_1 = x^2+2 \quad \text{and } \widehat{\mathcal{P}}_i = \widehat{\mathcal{P}}_1 = 8.$$

Then

$$\Gamma_1 = [2, x, 0, x, -2, -x, 0, -x].$$

Since the residue $\rho = 0$ appears in the locations 2 and 6 in Γ_1, we can, and do, use the congruences $(2, 8)$ and $(6, 8)$ to build both $\widehat{\mathcal{C}}^+$ and $\widehat{\mathcal{C}}^-$. As a second example, for $i=4$, we have

$$N_i = N_4 = 6, \quad F_i = F_4 = x^4+4x^2+1 \quad \text{and } \widehat{\mathcal{P}}_i = \widehat{\mathcal{P}}_4 = 24.$$

The generic cycle Γ_4 of $\widehat{\mathcal{V}}_x$ modulo F_4 is given in Table 3, with the location in Γ_4 of each generic residue. We can, and do, use the two congruences $(8, 24)$ and $(16, 24)$ to build $\widehat{\mathcal{C}}^+$, since in both locations 8 and 16 of Γ_4, the residue is the same, namely $\rho = -1$. We could, although we choose not to, use the two congruences $(4, 24)$ and $(20, 24)$ to build $\widehat{\mathcal{C}}^-$, since in both locations 4 and 20 of Γ_4, the residue is $-\rho = 1$. We continue in this manner with the remainder of the elements in Table 1. Note that, for any value of $a \geq 4$, $F_i|_{x=a}$ has at least one odd primitive divisor p_i, and that these primes are all distinct by the definition of primitive divisor.

After examining all elements F_i of Table 1, we move to the elements G_i of Table 2. Let q_i be an odd prime divisor of $G_i|_{x=a}$. To see that such primes exist, we examine the solutions to the Diophantine equations $\mathcal{D}_i : G_i = 2^y$. We see that $\mathcal{D}_1$ has no solutions modulo 4, and so the only solution to $\mathcal{D}_1$ is $(x, y) = (1, 1)$. Similarly, reduction modulo 16 shows that the only solution to $\mathcal{D}_2$ is $(x, y) = (2, 3)$; and finally, reduction modulo 2 shows that the only solution to $\mathcal{D}_3$ is $(x, y) = (0, 0)$. Hence, the existence of the primes q_i are guaranteed here since $a \geq 4$. Moreover, it is straightforward, although somewhat tedious, to show that the odd primes q_i are distinct, and also different from the odd primes p_i. There are only 30 pairs that need to be checked since we already know that the primes p_i are distinct. We give an example to illustrate how this process is accomplished. We know that some odd prime q_2 divides a^2+4 and some odd prime p_3 divides a^4+4a^2+2. Suppose that $d = \gcd(a^2+4, a^4+4a^2+2)$. Then d divides $(a^2+4)^2-(a^4+4a^2+2) = 4a^2+12$, and hence d divides $4(a^2+4)-(4a^2+12) = 4$. Thus, we can conclude that $q_2 \neq p_3$.

Then, we examine the generic cycles of $\widehat{\mathcal{V}}_x$ modulo the polynomials G_i. For example,

$$v_n \equiv -a \pmod{G_1} \quad \text{for} \quad n \equiv 7, 11 \pmod{12} \quad \text{and}$$
$$v_n \equiv a \pmod{G_1} \quad \text{for} \quad n \equiv 1, 5 \pmod{12}.$$

Consequently, we add the congruences $(7, 12)$ and $(11, 12)$ to $\mathcal{C}^+$, and the congruences $(1, 12)$ and $(5, 12)$ to $\mathcal{C}^-$. Continuing in this manner yields the coverings:

$$\begin{aligned}\mathcal{C}^+ = \{&(2,8),(6,8),(3,6),(4,16),(12,16),(8,24),(16,24),(8,32),(24,32),\\&(6,18),(12,18),(0,144),(7,12),(11,12),(1,4)\},\end{aligned} \tag{3.3}$$

$$\begin{aligned}\mathcal{C}^- = \{&(2,8),(6,8),(3,6),(4,16),(12,16),(8,32),(24,32),(16,48),(32,48),\\&(24,72),(48,72),(1,12),(5,12),(3,4),(0,36)\}.\end{aligned} \tag{3.4}$$

From these coverings, we derive the following system of congruences for k:

$$\begin{array}{llll} k \equiv 0 & \pmod{p_1} & k \equiv -1 & \pmod{p_7} \\ k \equiv 0 & \pmod{p_2} & k \equiv -1 & \pmod{p_8} \\ k \equiv 0 & \pmod{p_3} & k \equiv -2 & \pmod{p_9} \\ k \equiv 1 & \pmod{p_4} & k \equiv a & \pmod{q_1} \\ k \equiv 0 & \pmod{p_5} & k \equiv -a & \pmod{q_2} \\ k \equiv 1 & \pmod{p_6} & k \equiv 2 & \pmod{q_3}. \end{array} \tag{3.5}$$

We add the congruence $k \equiv 1 \pmod 2$ to the system (3.5) to avoid the trivial situation in which all terms of the shifted sequences are divisible by 2. Then, for any specific value of a, we can use the Chinese remainder theorem to solve this system to get an infinite arithmetic progression of odd values of k such that each term in both sequences $\mathcal{V}_a \pm k$ is divisible by at least one prime from the set

$$P_a := \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_8, p_9, q_1, q_2, q_3\}.$$

Since there are infinitely many values of k in this arithmetic progression such that $|v_n - k| > p$ and $|v_n + k| > p$ for all n, where $p = \max_{p \in P_a} \{p\}$, the proof that the sequences $\mathcal{V}_a \pm k$ are primefree is complete.

We turn now to showing that there exist infinitely many values of k such that every term of both of the sequences $\mathcal{V}_a \pm k$ has at least two distinct prime divisors. The case $a = 0$ has already been addressed, so assume that $a \geq 1$ is fixed, and that k is an element of an arithmetic progression such that both sequences $\mathcal{V}_a \pm k$ are primefree. If not every term of the sequences $\mathcal{V}_a \pm k$ has at least two distinct prime divisors, then

$$k = |v_n \pm p^m|$$

for some term $v_n \in \mathcal{V}_a$, some prime $p \in P_a$ and some integer $m \geq 2$. Since $v_n = \alpha^n + \beta^n$, where $\alpha = \left(a + \sqrt{a^2+4}\right)/2$ and $\beta = \left(a - \sqrt{a^2+4}\right)/2$, we have

$$k = \alpha^n \left|1 \pm \alpha^{-n} p^m\right| + o(1),$$

since $|\beta| < 1$. Note that $\alpha^{-n}p^m \neq \pm 1$. Therefore, we can apply Theorem 2.10, with $\xi_1 = \alpha$, $\xi_2 = p$, $b_1 = -n$ and $b_2 = m$, to the expression $|1 \pm \alpha^{-n}p^m|$ to get

$$k \gg \frac{\max\{\alpha^n, p^m\}}{\max\{m,n\}^C}, \tag{3.6}$$

for some constant C. If $T \geq k$ is some large real number, then $\log T \gg \max\{m,n\}$ from (3.6), and so there are only $O\left((\log T)^2\right)$ such possibilities for k. Since k is in an arithmetic progression, there are $\gg T$ values for k up to T. Thus, for T sufficiently large, there exists some value of k such that $k \neq |v_n \pm p^m|$ for all n, m and primes $p \in P_a$, and the theorem is established. $\square$

Remark 3.1. The part of the proof of Theorem 1.1 for $a \geq 4$ actually works for $a = 3$ as well, but we presented the case $a = 3$ separately since that special treatment led to the determination of the smallest such positive value of k that works for $a = 3$, namely $k = 93$.

The following corollary is an immediate consequence of Theorem 1.1.

Corollary 3.2. *For all integers a, Conjecture 1.2 is true for the Lucas sequences $\mathcal{V}_a$.*

We give an example to illustrate Theorem 1.1 when $a \geq 4$.

Example 3.3. $a = 5$

We use the coverings (3.3) and (3.4), together with the list

$$P = [3, 7, 727, 11, 528527, 19603, 264263, 937, 147639149571513601, 13, 29, 17]$$

of primes $p_1, \ldots, p_9, q_1, q_2, q_3$. Note that when there was more than one choice of a prime p_i as a primitive divisor of $F_i|_{x=5}$, or a prime q_i as a divisor of $G_i|_{x=5}$, we chose only the smallest such prime to construct the list P. For example, although $v_{18} \in \mathcal{V}_5$ has the two primitive divisors 937 and 136691, we choose to use only 937. Then, with the addition of the congruence $k \equiv 1 \pmod 2$, we use the Chinese remainder theorem to solve the resulting system (3.5) of congruences for k to get an infinite arithmetic progression of odd positive values of k such that both of the sequences $\mathcal{V}_5 \pm k$ are simultaneously primefree. The smallest positive value of k in this arithmetic progression is

$$k = 785752477092532495678103253704193081314976951.$$

4. Final comments

Since the only primitive divisor of $\widehat{v}_{N_i}$ in $\widehat{\mathcal{V}}_x$ is F_i, we could only use a single primitive divisor for each N_i to build the coverings $\widehat{\mathcal{C}}^+$ and $\widehat{\mathcal{C}}^-$ in the proof of Theorem 1.1. However, this situation represents a worst-case scenario in $\mathcal{V}_a$. Quite often, in practice, $F_i(a)$ will have more than a single prime factor that is a primitive divisor of v_{N_i} in $\mathcal{V}_a$. In this case, we can reuse the modulus $\mathcal{P}_i$ with the new primitive divisor, which yields a smaller covering system with a smaller least common multiple, and quite possibly, a smaller positive value of k. Additionally, it can happen that there are better choices for the residues in $\Gamma_f|_{x=a}$ with which to build the covering. This phenomenon can also reduce the smallest positive value of k.

A natural question to ask is whether the "generic" process used in the proof of Theorem 1.1 can be extended to handle more general sequences. It seems that if the periods of the sequence modulo the primes are "well-behaved", then it is conceivable that such techniques could be used successfully. However, we leave this possibility for future research.

Acknowledgment

The authors thank the referee for the many valuable suggestions.

References

[1] A. Baker, Transcendental Number Theory, second edition, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1990.
[2] Y. Bilu, G. Hanrot, P.M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, with an appendix by M. Mignotte, J. Reine Angew. Math. 539 (2001) 75–122.
[3] R.D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, Ann. of Math. 15 (1913) 30–70.
[4] P. Erdős, On integers of the form $2^k + p$ and some related problems, Summa Brasil. Math. (1950) 113–123.
[5] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, Recurrence Sequences, vol. 104, American Mathematical Society, 2003.
[6] D. Ismailescu, P. Shim, On numbers that cannot be expressed as a plus-minus weighted sum of a Fibonacci number and a prime, Integers 14 (2014), paper No. A65, 12 pp.
[7] L. Jones, Fibonacci variations of a conjecture of Polignac, Integers 12 (4) (2012) 659–667.
[8] L. Jones, Primefree shifted Lucas sequences, Acta Arith. 170 (3) (2015) 287–298.
[9] J. Lagarias, The set of primes dividing the Lucas numbers has density 2/3, Pacific J. Math. 118 (2) (1985) 449–461.
[10] D. Levy, The irreducible factorization of Fibonacci polynomials over $\mathbb{Q}$, Fibonacci Quart. 39 (4) (2001) 309–319.