ACTA ARITHMETICA
170.3 (2015)

Primefree shifted Lucas sequences

by

Lenny Jones (Shippensburg, PA)

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 $(s_n+k)_{n\geq 0}$. Several classic problems in number theory can be viewed as examining the occurrence of primes in such shifted sequences. For example, if $\mathcal{S} = (2^n)_{n\geq 0}$, then the question of whether there are only finitely many Fermat primes is equivalent to asking whether there are only finitely many primes in the shifted sequence $\mathcal{S}+1$. Also, the conjecture that there exist infinitely many Mersenne primes is equivalent to the statement that the shifted sequence $\mathcal{S}-1$ contains infinitely many primes. Another famous conjecture in number theory states that there are infinitely many primes in the shifted sequence $\mathfrak{P}+k$ for any fixed positive even integer k, where $\mathfrak{P}$ is the sequence of prime numbers. The case $k=2$ is known as the twin-prime conjecture, while the cases $k>2$ are related to Dickson's conjecture (see [4]) and Schinzel's hypothesis H (see [17]).

In 2014, Yitang Zhang [21] shocked the mathematical community by proving unconditionally that there exists some $k \leq 70\,000\,000$ such that $\mathfrak{P}+k$ contains infinitely many primes. Since then, various researchers have been chiseling away at Zhang's upper bound. As of the writing of this paper, the best known unconditional result is that $k \leq 246$, due to the Polymath8 project [15], which was initiated by T. Tao.

We define a sequence $\mathcal{S} = (s_n)_{n\geq 0}$ to be *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 $\mathcal{S}$. Many examples of primefree sequences exist in the literature. One of the earliest is the shifted sequence $(2^n-7629217)_{n\geq 0}$, which was found by Erdős [5] in 1950. Erdős actually constructed an arithmetic progression of integer values of k such that each of the sequences $(2^n-k)_{n\geq 0}$ is primefree. This arithmetic progression of values of k provides infinitely many counterexamples to a conjecture of Alphonse de Polignac. In 1849, Polignac [14] conjectured that every odd integer >1 can be written in the

2010 *Mathematics Subject Classification*: Primary 11B37, 11B39; Secondary 11B83.
Key words and phrases: Lucas sequences, primefree, coverings.

DOI: 10.4064/aa170-3-5

form $2^n + p$ for some integer $n \geq 0$ and some prime p. Polignac later realized that this conjecture is false, and he found several counterexamples. Much earlier, Euler had given the counterexample 959 in a letter to Christian Goldbach [9].

Two other well-known primefree sequences in the literature are due, respectively, to Hans Riesel and Wacław Sierpiński. In 1956, Riesel [16] found infinitely many odd integers k in arithmetic progression such that the sequence $(k \cdot 2^n - 1)_{n \geq 0}$ is primefree. Any such odd positive integer k is called a *Riesel number*. It is conjectured that 509203 is the smallest Riesel number. For the current status of this conjecture, see `www.prothsearch.net/rieselprob.html`. In 1960, Sierpiński [18] showed that there exist infinitely many odd positive integers k in arithmetic progression such that the sequence $(k \cdot 2^n + 1)_{n \geq 0}$ is primefree. Any such odd positive integer k is called a *Sierpiński number*. It is conjectured that 78557 is the smallest Sierpiński number. For the current status of this conjecture, see `www.seventeenorbust.com`.

At first glance, there might appear to be no connection among the sequences found by Erdős, Riesel and Sierpiński. However, it turns out that the method used in any one of these situations to produce the values of k can actually be used to produce values of k in the other situations as well. Indeed, all three of these problems can be considered as constructing primefree shifted sequences of the form $(2^n + k)_{n \geq 0}$. For an explanation of this connection, see [8].

A somewhat natural question to ask is whether there exist infinitely many integers k such that, for each of these values of k, both of the shifted sequences $(2^n + k)_{n \geq 0}$ and $(2^n - k)_{n \geq 0}$ are simultaneously primefree. The affirmative answer to this question was first given by Brier [8, 20]. Along these lines, we prove the following result.

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

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

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

REMARK 1.2. We point out that showing there are infinitely many values of k such that both of the sequences $\mathcal{U}_1 \pm k$ are primefree (the shifted Fibonacci numbers) was handled recently by Ismailescu and Shim [11].

The primefree part of Theorem 1.1 extends previous work [12] of the author for the single shifted sequence $\mathcal{U}_a - k$ when $a = 1$ to all other values of a, and establishes the following conjecture of Ismailescu and Shim [11] for the specific sequences $\mathcal{U}_a$.

CONJECTURE 1.3. *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.*

Most calculations in this article were performed using Maple.

2. Preliminaries. While the common underlying process used in the construction of the sequences of Erdős, Riesel and Sierpiński (as described in Section 1) must be adapted somewhat to the individual sequence, there are two basic ideas central to the general method. The first of these ideas is a concept due to Erdős [5].

DEFINITION 2.1. 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. We write a covering $\mathcal{C}$ as a set of ordered pairs $\{(r_i, m_i)\}$.

A second crucial component used in this process is the notion of a primitive divisor.

DEFINITION 2.2. Let $\mathcal{S}$ be a sequence. A *primitive divisor* of the term $s_n \in \mathcal{S}$ is a prime number p such that $s_n \equiv 0 \pmod{p}$ but $s_m \not\equiv 0 \pmod{p}$ for all $m < n$.

REMARK 2.3. Some authors allow a primitive divisor of s_n to be any divisor $d > 1$ of s_n such that d is coprime to s_m for all $m < n$. For example, see [7]. Also, for Lucas (and Lehmer) sequences, Bilu, Hanrot and Voutier [2] use a slightly modified version of Definition 2.2 which includes an additional restriction. For example, in the Lucas sequence case, they require that a primitive divisor p must satisfy $(\alpha - \beta)^2 \not\equiv 0 \pmod{p}$, where α and β are zeros of the characteristic polynomial. We do not require this additional restriction in this paper.

Our main focus here is on certain Lucas sequences of the first kind.

DEFINITION 2.4. Let $a \in \mathbb{Z}$, and let $\mathcal{U}_a = (u_n)_{n\geq 0}$ denote the *Lucas sequence of the first kind* defined by

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

REMARK 2.5. Note for $a > 0$, we have

$$u_n(-a) = (-1)^{n-1} u_n(a),$$

where $u_n(-a)$ is the nth term of $\mathcal{U}_{-a}$ and $u_n(a)$ is the nth term of $\mathcal{U}_a$.

The following theorem is a special case of a much more general result that is the culmination of work initiated by Carmichael [3] and completed by others [2].

THEOREM 2.6. *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):*

$$(a, 0), (a, 1), (1, 2), (1, 6), (1, 12), (3, 6).$$

It is well known that the sequence $\mathcal{U}_a$ is purely periodic modulo a prime [6]. The *period* of $\mathcal{U}_a$ modulo a prime p, which we denote $\mathcal{P}_p := \mathcal{P}_p(a)$, is the smallest positive integer h such that $u_h \equiv 0 \pmod{p}$ and $u_{h+1} \equiv 1 \pmod{p}$. We define the *rank of apparition* of p in $\mathcal{U}_a$ to be the least positive integer r such that $u_r \equiv 0 \pmod{p}$, and we denote it as $\mathcal{R}_p := \mathcal{R}_p(a)$. We refer to the actual list of residues that occur modulo p from index 0 to index $h-1$ as the *cycle of $\mathcal{U}_a$ modulo p*. For example, if $a = 1$ and $p = 3$, then $\mathcal{P}_3 = 8$ and the cycle of $\mathcal{U}_1$ modulo 3 is $[0, 1, 1, 2, 0, 2, 2, 1]$. We label the positions in the cycle starting at 0, so that the residue at position 4 is 0 in our example. Also, $\mathcal{R}_3 = 4$ here.

The following theorem is a generalization to $\mathcal{U}_a$ of a theorem for $\mathcal{U}_1$ due to Vinson [19]. We omit the proof since it is identical to Vinson's proof when $a \not\equiv 0 \pmod{p}$, and obvious when $a \equiv 0 \pmod{p}$.

THEOREM 2.7. *Let p be a prime. Then*

(1) *If $a \equiv 0 \pmod{p}$, then $\mathcal{P}_p = \mathcal{R}_p = 2$.*
(2) *If $a \not\equiv 0 \pmod{p}$, then*

$$\mathcal{P}_p = \begin{cases} \mathcal{R}_p = 3 & \text{if } p = 2, \\ \mathcal{R}_p & \text{if } \mathcal{R}_p \equiv 2 \pmod{4} \text{ and } p \neq 2, \\ 2\mathcal{R}_p & \text{if } \mathcal{R}_p \equiv 0 \pmod{4} \text{ and } p \neq 2, \\ 4\mathcal{R}_p & \text{if } \mathcal{R}_p \equiv 1 \pmod{2} \text{ and } p \neq 2. \end{cases}$$

REMARK 2.8. Note that if p is a primitive divisor of u_n, then $\mathcal{R}_p = n$.

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

DEFINITION 2.9. Let x be a variable and let $\widehat{\mathcal{U}}_x = (\widehat{u}_n)_{n \geq 0}$ be the sequence of polynomials in x defined by

$$\widehat{u}_0 = 0, \quad \widehat{u}_1 = 1, \quad \text{and} \quad \widehat{u}_n = x\widehat{u}_{n-1} + \widehat{u}_{n-2} \quad \text{for } n \geq 2.$$

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

$$\widehat{u}_m \equiv 0 \pmod{f(x)} \quad \text{and} \quad \widehat{u}_{m+1} \equiv 1 \pmod{f(x)}.$$

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 $\widehat{\mathcal{U}}_x$ 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 2.10. The polynomials $\widehat{u}_n$ in Definition 2.9 are known as the *Fibonacci polynomials* [13].

It is clear from Definition 2.9 that $\widehat{\mathcal{P}}_f$ is finite if and only if $f(x)$ divides $\widehat{u}_n$ for some n. However, as noted by Hoggatt and Long [10], not every monic irreducible polynomial appears as a factor of some $\widehat{u}_n$. When $f(x)$ is a factor of $\widehat{u}_n$ for some n, one can define the rank of apparition of $f(x)$, and a generic version of Theorem 2.7 holds modulo $f(x)$. Although such a complete generic theory is not required here, the following extension of the definition of a primitive divisor is useful.

DEFINITION 2.11. A *generic primitive divisor* of $\widehat{u}_n$ is a monic irreducible polynomial $f(x)$ of positive degree such that $\widehat{u}_n \equiv 0 \pmod{f(x)}$ but $\widehat{u}_m \not\equiv 0 \pmod{f(x)}$ for all indices $m < n$.

REMARK 2.12. The primitive divisors in Definition 2.11 are also known as *fibotomic* polynomials [13].

Note that Theorem 2.6 guarantees the existence of a primitive divisor of $\widehat{u}_n$, other than the possible exceptions listed there. In reality, the only exceptions in the generic situation are $n = 0$ and $n = 1$, since we do see that x, $x^2 + 1$, $x^2 + 3$ and $x^4 + 4x^2 + 1$ are primitive divisors of $\widehat{u}_2$, $\widehat{u}_3$, $\widehat{u}_6$ and $\widehat{u}_{12}$ respectively. It can also be shown that each term $\widehat{u}_n$ has exactly one primitive divisor [13], and so we denote it as $f_n(x)$. Consequently, the primitive divisors of $\mathcal{U}_a$ 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 $\widehat{\mathcal{P}}_f$.

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 $\mathcal{U}_a \pm k$ has at least two distinct prime factors.

THEOREM 2.13. *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*

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

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, we first describe, for any integer $a \geq 1$, a general process that can be used when searching for infinitely many integers k such that the single sequence $\mathcal{U}_a + k$ is primefree. The idea is to build a covering $\mathcal{C} = \{(r_i, m_i)\}$, where $m_i = \mathcal{P}_p$ for some

primitive divisor p of $u_{\mathcal{R}_p} \in \mathcal{U}_a$, and r_i is a position in the cycle of residues modulo p. Then, when $n \equiv r_i \pmod{m_i}$, we have

$$u_n + k \equiv u_{r_i} + k \pmod{p}.$$

Solving the congruence $u_{r_i} + k \equiv 0 \pmod{p}$ for k gives us a value of k such that the term $u_n + k$ in $\mathcal{U}_a + k$ 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 because of other congruences arising from other moduli. If p and q are two primitive divisors of the same term, say $u_N \in \mathcal{U}_a$, then $N = \mathcal{R}_p = \mathcal{R}_q$ and $\mathcal{P}_p = \mathcal{P}_q$ by Theorem 2.7. Thus, we can also reuse the modulus $m_i = \mathcal{P}_p$ in our covering as many times as there are distinct primitive divisors of u_N.

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 the primitive divisors. Thus, for each of these values of k in the arithmetic progression, every term in $\mathcal{U}_a + k$ is divisible by at least one prime in the finite set $\mathcal{D}_a$ of primitive divisors used. Since for k sufficiently large in the arithmetic progression, every term of $\mathcal{U}_a + k$ is larger than the largest prime in $\mathcal{D}_a$, we have successfully found infinitely many integers k such that the sequence $\mathcal{U}_a + k$ is primefree. These methods were employed in [12] and [11] for $a = 1$, and certainly this approach seems plausible on a case-by-case basis for any particular value of $a \geq 1$. However, it is 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 here is that we also require the sequence $\mathcal{U}_a - k$ to be primefree. Because of this added restriction, we need to build two coverings: $\mathcal{C}^+ = \{(r_i, m_i)\}$ for the sequence $\mathcal{U}_a + k$, and $\mathcal{C}^- = \{(s_i, t_i)\}$ for the sequence $\mathcal{U}_a - k$. The coverings $\mathcal{C}^+$ and $\mathcal{C}^-$ must be compatible in the sense that if $m_i = t_i$, and we use the same primitive divisor 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 primitive divisor

$p = 19$. The cycle of $\mathcal{U}_9$ modulo $p = 19$ is

$$[0, 1, 9, 6, 6, 3, 14, 15, 16, 7, 3, 15, 5, 3, 13, 6, 10, 1] \tag{3.1}$$

so that $\mathcal{P}_{19} = 18$. Since the residue $\rho = 6$ appears at locations 3, 4 and 15, we can use the three congruences $(3, 18)$, $(4, 18)$ and $(15, 18)$ to build one of the coverings $\mathcal{C}^+$ or $\mathcal{C}^-$. If we choose to use these congruences for $\mathcal{C}^+$, then we can in fact use only $(14, 18)$ for $\mathcal{C}^-$ in this situation, since 14 is the only location in the cycle (3.1) for which the residue $-\rho = -6 \equiv 13 \pmod{19}$ appears.

Proof of Theorem 1.1. In light of Remark 2.5, we can restrict our attention to $a \geq 0$. We begin with the special case $a = 0$, where $\mathcal{U}_0 = (0, 1, 0, 1, \ldots)$. Let $k \equiv 21 \pmod{2310}$. It is then easy to see that $|\pm k|$ and $|1 \pm k|$ are all divisible by at least two distinct primes from the set $\{2, 3, 5, 7, 11\}$, and so the theorem is true for $a = 0$.

We focus first on the primefree part of the theorem. As mentioned earlier, the case $a = 1$ was handled recently by Ismailescu and Shim [11], so we assume now that $a \geq 2$. We use the ideas of generic cycle and generic primitive divisor from Section 2 to construct 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 for any particular value of a with $a \geq 2$. For each index N_i in the list

$$N = [2, 3, 4, 5, 8, 9, 12, 15, 20, 24, 36, 45, 60]$$

of 13 specific indices, we calculate the generic primitive divisor $F_i := f_{N_i}(x)$ of $\widehat{u}_{N_i}$, and the generic period $\widehat{\mathcal{P}}_i := \widehat{\mathcal{P}}_{F_i}$, for each i with $1 \leq i \leq 13$. This information is provided in Table 1. Observe in the list N that we have avoided the exceptional cases given in Theorem 2.6. In particular, we have not used the index 6.

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

$$\widehat{\mathcal{P}} = [2, 12, 8, 20, 16, 36, 24, 60, 40, 48, 72, 80, 180, 120].$$

To do so, we examine for each i what residues appear, and where they appear, in the generic cycle $\Gamma_i := \Gamma_{F_i}$ of $\widehat{\mathcal{U}}_x$ modulo F_i.

For example, for $i = 2$, we have $N_2 = 3$, $F_2 = x^2 + 1$ and $\widehat{\mathcal{P}}_2 = 12$. Then

$$\Gamma_2 = [0, 1, x, 0, x, -1, 0, -1, -x, 0, -x, 1].$$

Since the residue $\rho = 0$ appears in the following four locations: 0 (mod 12), 3 (mod 12), 6 (mod 12) and 9 (mod 12) in Γ_2, we can, and do, use the modulus 12 four times in $\widehat{\mathcal{C}}^+$ with the residues 0, 3, 6 and 9. Since $-\rho = 0$, we can, and do, use the same congruences in $\widehat{\mathcal{C}}^-$.

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

N	F	$\widehat{\mathcal{P}}$
2	x	2
3	x^2+1	12
4	x^2+2	8
5	x^4+3x^2+1	20
8	x^4+4x^2+2	16
9	$x^6+6x^4+9x^2+1$	36
12	x^4+4x^2+1	24
15	$x^8+9x^6+26x^4+24x^2+1$	60
20	$x^8+8x^6+19x^4+12x^2+1$	40
24	$x^8+8x^6+20x^4+16x^2+1$	48
36	$x^{12}+12x^{10}+54x^8+112x^6+105x^4+36x^2+1$	72
45	$x^{24}+24x^{22}+252x^{20}+1521x^{18}+5832x^{16}+14823x^{14}+25298x^{12}$ $+28743x^{10}+21087x^8+9393x^6+2250x^4+216x^2+1$	180
60	$x^{16}+16x^{14}+105x^{12}+364x^{10}+714x^8+784x^6+440x^4+96x^2+1$	120

As a second example, for $i=9$, we have $N_9=20$, $F_9=x^8+8x^6+19x^4+12x^2+1$ and $\widehat{\mathcal{P}}_9=40$. The generic cycle Γ_9 of $\widehat{\mathcal{U}}_x$ modulo F_9 is given in Table 2, with the location in Γ_9 of each generic residue.

Continuing in this manner, we build the coverings $\widehat{\mathcal{C}}^+$ and $\widehat{\mathcal{C}}^-$:

$$\begin{aligned}\widehat{\mathcal{C}}^+ = \{&(0,2),(0,12),(3,12),(6,12),(9,12),(3,8),(5,8),(0,20),(5,20),\\ &(10,20),(15,20),(7,16),(9,16),(17,36),(19,36),(7,24),\\ &(17,24),(29,60),(31,60),(17,40),(23,40),(1,48),(47,48),\\ &(25,72),(47,72),(41,180),(139,180),(47,120),(73,120)\},\end{aligned}$$

$$\begin{aligned}\widehat{\mathcal{C}}^- = \{&(0,2),(0,12),(3,12),(6,12),(9,12),(1,8),(7,8),(0,20),(5,20),\\ &(10,20),(15,20),(1,16),(15,16),(1,36),(35,36),(5,24),\\ &(19,24),(1,60),(59,60),(3,40),(37,40),(23,48),(25,48),\\ &(11,72),(61,72),(49,180),(131,180),(13,120),(107,120)\}.\end{aligned}$$

Since the exceptional cases given in Theorem 2.6 have been avoided, it follows that for any positive integer $a\geq 2$, there exists a primitive divisor p_i of the term u_{N_i} in $\mathcal{U}_a$. This prime p_i is a divisor of $F_i(a)$, and therefore the coverings $\widehat{\mathcal{C}}^+$ and $\widehat{\mathcal{C}}^-$ can be applied to this specialized situation. This process results in a system of congruences for k modulo each prime in the finite set $\mathcal{D}_a$ of primitive divisors used. Using the Chinese remainder theorem to solve this system gives an arithmetic progression of values of k such that each term in both sequences $\mathcal{U}_a\pm k$ is divisible by at least one prime from $\mathcal{D}_a$.

Table 2. Generic residues in Γ_9

Location	Generic residue	Location	Generic residue
0	0	20	0
1	1	21	-1
2	x	22	$-x$
3	x^2+1	23	$-x^2-1$
4	x^3+2x	24	$-x^3-2x$
5	x^4+3x^2+1	25	$-x^4-3x^2-1$
6	x^5+4x^3+3x	26	$-x^5-4x^3-3x$
7	$x^6+5x^4+6x^2+1$	27	$-x^6-5x^4-6x^2-1$
8	$x^7+6x^5+10x^3+4x$	28	$-x^7-6x^5-10x^3-4x$
9	$-x^6-4x^4-2x^2$	29	$x^6+4x^4+2x^2$
10	$2x^5+8x^3+4x$	30	$-2x^5-8x^3-4x$
11	$x^6+4x^4+2x^2$	31	$-x^6-4x^4-2x^2$
12	$x^7+6x^5+10x^3+4x$	32	$-x^7-6x^5-10x^3-4x$
13	$-x^6-5x^4-6x^2-1$	33	$x^6+5x^4+6x^2+1$
14	x^5+4x^3+3x	34	$-x^5-4x^3-3x$
15	$-x^4-3x^2-1$	35	x^4+3x^2+1
16	x^3+2x	36	$-x^3-2x$
17	$-x^2-1$	37	x^2+1
18	x	38	$-x$
19	-1	39	1

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

We turn to showing that there exist infinitely many values of k such that every term of both of the sequences $\mathcal{U}_a \pm k$ 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 $\mathcal{U}_a \pm k$ are primefree. If not every term of the sequences $\mathcal{U}_a \pm k$ has at least two distinct prime divisors, then we have $k = |u_n \pm p^m|$ for some term $u_n \in \mathcal{U}_a$, some prime $p \in \mathcal{D}_a$, the finite set of primitive divisors used to construct the arithmetic progression containing k, and some integer $m \geq 2$. We can write

$$u_n = c\alpha^n + (-c)\beta^n,$$

where $\alpha = (a + \sqrt{a^2+4})/2$, $\beta = (a - \sqrt{a^2+4})/2$ and $c = 1/(\alpha - \beta)$. Note that $|\beta| < 1$, and thus $u_n = c\alpha^n + o(1)$. Therefore,

$$k = |u_n \pm p^m| = c\alpha^n |1 \pm c^{-1}\alpha^{-n}p^m| + o(1). \tag{3.2}$$

If k is small, say $k < .5\max\{c\alpha^n, p^m\}$, then $c\alpha^n \in (p^m/2, 2p^m)$. Hence,

$$n \asymp m. \tag{3.3}$$

If $c^{-1}\alpha^{-n}p^m = \pm 1$, then

$$\alpha^{2n} = c^{-2}p^{2m} \in \mathbb{Q},$$

which is impossible for $n \neq 0$. Therefore, we can apply Theorem 2.13, with $\xi_1 = \pm c$, $\xi_2 = \alpha$, $\xi_3 = p$, $b_1 = -1$, $b_2 = -n$ and $b_3 = m$, to the expression $|1 \pm c^{-1}\alpha^{-n}p^m|$, to get

$$|1 \pm c^{-1}\alpha^{-n}p^m| > (\max\{m, n\})^{-C} \tag{3.4}$$

for some constant C. Thus, from (3.3), (3.2) and (3.4), we obtain

$$k \gg \frac{\alpha^n}{\max\{m, n\}^C} \gg \frac{\max\{\alpha^n, p^m\}}{\max\{m, n\}^C}. \tag{3.5}$$

If $T \geq k$, then $\log T \gg \max\{m, n\}$ from (3.5), and so there are only $O((\log T)^2)$ 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 $k \neq |u_n \pm p^m|$ for all n, m and primes $p \in \mathcal{D}_a$, and the proof is complete. ∎

The following corollary is an immediate consequence of Theorem 1.1.

Corollary 3.1. *For all integers a, Conjecture* 1.3 *is true for the Lucas sequences $\mathcal{U}_a$.*

Remark 3.2. The type of plus/minus symmetry that appears in Table 2 for Γ_9 only seems to occur when $\widehat{\mathcal{P}}_f \equiv 0 \pmod 4$.

We give an example to illustrate the application of the first part of Theorem 1.1.

Example 3.3 ($a = 2$; the Pell numbers). We use the coverings $\widehat{\mathcal{C}}^+$ and $\widehat{\mathcal{C}}^-$ with the list N and the list

$$P = [2, 5, 3, 29, 17, 197, 11, 269, 19, 1153, 73, 6481, 601]$$

of corresponding primitive divisors. Note that when u_{N_i} has more than one primitive divisor, we have chosen the smallest primitive divisor of u_{N_i} for the list P. Using the Chinese remainder theorem to solve the resulting system of congruences

$$\begin{aligned} &k \equiv 0 \pmod 2, && k \equiv 1 \pmod{269},\\ &k \equiv 0 \pmod 5, && k \equiv 5 \pmod{19},\\ &k \equiv 1 \pmod 3, && k \equiv 1152 \pmod{1153},\\ &k \equiv 0 \pmod{29}, && k \equiv 47 \pmod{73}, \end{aligned}$$

$$k \equiv 1 \pmod{17}, \qquad k \equiv 2267 \pmod{6481},$$
$$k \equiv 1 \pmod{197}, \qquad k \equiv 496 \pmod{601},$$
$$k \equiv 7 \pmod{11},$$

for k gives an arithmetic progression of values of k such that both of the sequences $\mathcal{U}_2 \pm k$ are primefree. The smallest positive value of k in this arithmetic progression is

$$k = 10124756384607912952120.$$

4. Final comments. Since the only primitive divisor of $\widehat{u}_{N_i}$ in $\widehat{\mathcal{U}}_x$ 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 $\mathcal{U}_a$. Quite often, in practice, $F_i(a)$ will have more than a single prime factor that is a primitive divisor of u_{N_i} in $\mathcal{U}_a$. 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 Lucas sequences. Unfortunately, it appears that the generic periodicity used for the sequences $\widehat{\mathcal{U}}_x$ in the proof of Theorem 1.1 fails for more general situations.

Acknowledgements. The author thanks the referee for the many excellent suggestions, and especially for providing the argument to prove that there exist infinitely many values of k such that every term in both of the sequences $\mathcal{U}_a \pm k$ has at least two distinct prime divisors.

References

[1] A. Baker, *Transcendental Number Theory*, 2nd ed., Cambridge Math. Library, Cambridge Univ. Press, Cambridge, 1990.

[2] Yu. Bilu, G. Hanrot, and 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] *Dickson's conjecture*, http://en.wikipedia.org/wiki/Dickson's_conjecture.

[5] P. Erdős, *On integers of the form* $2^k + p$ *and some related problems*, Summa Brasil. Math. 2 (1950), 113–123.

[6] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence Sequences*, Math. Surveys Monogr. 104, Amer. Math. Soc., Providence, RI, 2003.

[7] G. Everest, S. Stevens, D. Tamsett, and T. Ward, *Primes generated by recurrence sequences*, Amer. Math. Monthly 114 (2007), 417–431.
[8] 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.
[9] P.-H. Fuss, *Correspondance Mathématique et Physique de Quelques Célèbres Géomètres du XVIIIème Siècle*, I, II, Johnson Reprint Corp., New York, 1968.
[10] V. E. Hoggatt Jr. and C. T. Long, *Divisibility properties of generalized Fibonacci polynomials*, Fibonacci Quart. 12 (1974), 113–120.
[11] D. Ismailescu and P. C. Shim, *On numbers that cannot be expressed as a plus-minus weighted sum of a Fibonacci number and a prime*, Integers 14 (2014), #A65, 12 pp.
[12] L. Jones, *Fibonacci variations of a conjecture of Polignac*, Integers 12 (2012), 659–667.
[13] D. Levy, *The irreducible factorization of Fibonacci polynomials over* $\mathbb{Q}$, Fibonacci Quart. 39 (2001), 309–319.
[14] A. de Polignac, *Recherches nouvelles sur les nombres premiers*, C. R. Acad. Sci. Paris Math. 29 (1849), 397–401, 738–739.
[15] *The "bounded gaps between primes" Polymath project—a retrospective*, arXiv:1409.8361v1 [math.HO].
[16] H. Riesel, *Några stora primtal*, Elementa 39 (1956), 258–260.
[17] *Schinzel's hypothesis H*, http://en.wikipedia.org/wiki/Schinzel's_hypothesis_H.
[18] W. Sierpiński, *Sur un problème concernant les nombres* $k \cdot 2^n + 1$, Elem. Math. 15 (1960), 73–74.
[19] J. Vinson, *The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence*, Fibonacci Quart. 1 (1963), no. 2, 37–45.
[20] E. W. Weisstein, *Brier Number*, http://mathworld.wolfram.com/BrierNumber.html.
[21] Y. Zhang, *Bounded gaps between primes*, Ann. of Math. 179 (2014), 1121–1174.

Lenny Jones
Department of Mathematics
Shippensburg University
Shippensburg, PA 17257, U.S.A.
E-mail: lkjone@ship.edu

Received on 18.10.2014
and in revised form on 12.5.2015 (7968)