#A52 INTEGERS 17 (2017)

PRIMES IN SHIFTED SUMS OF LUCAS SEQUENCES

Lenny Jones
Department of Mathematics, Shippensburg University, Shippensburg, Pennsylvania
lkjone@ship.edu

Lawrence Somer
Department of Mathematics, Catholic University of America, Washington, D.C.
somer@cua.edu

Received: 2/8/17, Revised: 7/30/17, Accepted: 10/25/17, Published: 11/10/17

Abstract

For any $a_1, a_2, b \in \mathbb{Z}$, with $b \neq 0$, we define

$$\mathcal{W}_{a_1,a_2} := \mathcal{U}(a_1, b) + \mathcal{U}(a_2, b),$$

where $\mathcal{U}(a_i, b)$ is the Lucas sequence of the first kind defined by

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

and the nth term of $\mathcal{W}_{a_1,a_2}$ is the sum of the nth terms of $\mathcal{U}(a_1, b)$ and $\mathcal{U}(a_2, b)$. In this article, we prove that there exist infinitely many integers b and $a_1, a_2 > 0$, with $b(a_1 + a_2) \equiv 1 \pmod 2$, for which there exist infinitely many positive integers k such that each term of both of the shifted sequences $|\mathcal{W}_{a_1,a_2} \pm k|$ is composite and no single prime divides all terms of these sequences. We also show that when $b = 1$, there exist infinitely many integers $a \neq 0$ for which there exist infinitely many positive integers k such that both of the shifted sequences $\mathcal{W}_{1,a} \pm k$ also possess this primefree property.

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 also require that $\mathcal{S} + k$ is not a constant sequence, and that no single prime divides all terms of $\mathcal{S} + k$. Several authors have investigated finding infinitely many values of k for various sequences $\mathcal{S}$ such that the shifted sequences $\mathcal{S} + k$ and $\mathcal{S} - k$ are simultaneously primefree [8, 10, 7]. Such values of k are also related to a generalization of a conjecture of Polignac [2, 9]. In this article, we investigate this primefree situation where the sequence to be shifted is actually a sum of Lucas sequences. For nonzero $a, b \in \mathbb{Z}$, we let

$$\mathcal{U} := \mathcal{U}(a, b) = (u_n)_{n=0}^{\infty}$$

denote the Lucas sequence of the first kind defined by

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

Definition 1. For a fixed nonzero integer b, and any pair (a_1, a_2) of integers, we define

$$\mathcal{W}_{a_1,a_2} := \mathcal{U}(a_1, b) + \mathcal{U}(a_2, b),$$

where $\mathcal{W}_{a_1,a_2} = (w_n)_{n=0}^{\infty}$, and w_n is the sum of the nth term of $\mathcal{U}(a_1, b)$ and the nth term of $\mathcal{U}(a_2, b)$.

One reason we have chosen to investigate shifted sums of these particular sequences is that the Lucas sequences have a long and rich history commencing in 1878 with the papers of Lucas [12, 13, 14]. Consequently, they are much better understood than many other sequences. For example, the terms of the Lucas sequences that possess a primitive divisor (primes that divide a term but do not divide any prior term) are completely known, thanks to the work of many mathematicians beginning with Carmichael [3] in 1913 and culminating with the deep results of Bilu, Hanrot and Voutier [1] in 2001. Another important aspect of the Lucas sequences that is particularly useful in our investigations is the concept of periodicity modulo a prime, which is explained in detail in Section 2.

Our main results are the following:

Theorem 2. *Let b be a fixed odd integer. Then there exist infinitely many pairs (a_1, a_2) of positive integers, with $a_1 + a_2$ odd, for which there exist infinitely many positive integers k such that each of the shifted sequences $\mathcal{W}_{a_1,a_2} \pm k$ is primefree.*

Theorem 3. *Let $b = 1$ and let $p \notin \{2, 17, 19\}$ be prime. If $a \equiv m \pmod{646p}$, where $0 \leq m \leq 646p - 1$, and m satisfies one of the 16 systems of congruences*

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv -1 \pmod{p} \\ x &\equiv r \pmod{17}, \quad \text{where } r \in \{\pm 1, \pm 4, \pm 5, \pm 6\} \\ x &\equiv \pm 4 \pmod{19}, \end{aligned} \tag{2}$$

then there exist infinitely many positive integers k such that each of the sequences $\mathcal{W}_{1,a} \pm k$ is primefree.

In particular, if $p = 3$ in Theorem 3, then there exist infinitely many positive integers k such that each of the sequences $\mathcal{W}_{1,a} \pm k$ is primefree for every $a \equiv m$

(mod 1938), where

$$m \in \{80, 566, 650, 764, 794, 878, 992, 1106, 1220, \\ 1364, 1478, 1592, 1706, 1790, 1820, 1934\}.$$

2. Preliminaries

We let $\mathcal{U}$ be the Lucas sequence, as defined in (1). Although most often we write u_n for the nth term of $\mathcal{U} := \mathcal{U}(a,b)$, occasionally we write $u_n(a,b)$, or $u_n(a)$ when b is fixed, for contextual clarity. We define the *discriminant* $D(a,b)$ of $\mathcal{U}(a,b)$ as

$$D(a,b) := a^2 + 4b.$$

For a fixed b, when the context is clear, we simply write $D(a)$ instead of $D(a,b)$, as in the proof of Theorem 3.

Next, we present some basic nomenclature and facts concerning the periodicity of $\mathcal{U}$ modulo a prime p, most of which can be found in [5]. We say that $\mathcal{U}$ is *purely periodic* modulo p if there exists $t \in \mathbb{N}$ such that

$$u_{n+t} \equiv u_n \pmod{p} \tag{3}$$

for all $n \geq 0$. The minimal value of t (if it exists) such that (3) holds, is called the *least period*, or simply the *period*, of $\mathcal{U}$ modulo p, and we denote it as $P_p := P_p(\mathcal{U}(a,b))$. It is well–known that $\mathcal{U}$ is purely periodic modulo p if $b \not\equiv 0 \pmod{p}$ (see, for example, [4]), and we assume throughout this article that this condition holds. The *restricted period* of $\mathcal{U}$ modulo a prime p, which we denote $R_p := R_p(\mathcal{U}(a,b))$, is the least positive integer r such that

$$u_r \equiv 0 \pmod{p} \quad \text{and} \quad u_{n+r} \equiv M_p u_n \pmod{p}$$

for all $n \geq 0$, and some nonzero residue $M_p := M_p(\mathcal{U}(a,b))$ modulo p, called the *multiplier* of $\mathcal{U}$ modulo p. In addition, $P_p \equiv 0 \pmod{R_p}$, and $E_p := E_p(U(a,b)) = P_p/R_p$ is the order of M_p modulo p [4]. Furthermore, if $j \geq 0$ is a fixed integer, then it is easy to see that

$$u_{n+jR_p} \equiv (M_p)^j u_n \pmod{p},$$

for all $n \geq 0$. We also define $\Gamma_p := \Gamma_p(\mathcal{U}(a,b))$ to be the *cycle* of $\mathcal{U}$ modulo p. The previously-discussed ideas can be extended easily to the sequence $\mathcal{W}_{a_1,a_2}$ and we do so in the sequel. For brevity of notation, we occasionally write simply D, P, R, M, E and Γ for the previously defined quantities when the context is clear.

The following lemma gives some facts concerning the symmetry appearing in Γ. A proof can be found in [15].

Lemma 1. *Let p be an odd prime and let $j \geq 0$ be a fixed integer. Then*

$$u_{Rj-n} \equiv (-1)^{n+1} M^j u_n b^{-n} \pmod{p} \quad \textit{for } 0 \leq n \leq Rj$$
$$u_{Pj-n} \equiv (-1)^{n+1} u_n b^{-n} \pmod{p} \quad \textit{for } 0 \leq n \leq Pj$$

For an odd prime p, we recall the *Legendre symbol*

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a quadratic residue modulo } p \\ -1 & \text{if } x \text{ is a quadratic nonresidue modulo } p \\ 0 & \text{if } x \equiv 0 \pmod{p}. \end{cases}$$

Lemma 2. *Let $\mathcal{U}(a, b)$ be a Lucas sequence as defined in (1), and let p be an odd prime. Then*

1. $R > 1$
2. $u_n \equiv 0 \pmod{p}$ *if and only if* $n \equiv 0 \pmod{R}$
3. $p - \left(\frac{D}{p}\right) \equiv 0 \pmod{R}$
4. *if* $D \not\equiv 0 \pmod{p}$*, then* $\frac{p-\left(\frac{D}{p}\right)}{2} \equiv 0 \pmod{R}$ *if and only if* $\left(\frac{-b}{p}\right) = 1$
5. *if* $\left(\frac{D}{p}\right) = 1$*, then* $p \equiv 1 \pmod{P}$.

Proof. Note that $R > 1$ since $u_1 = 1$. A proof of parts (2) and (4) can be found in [11], while a proof of parts (3) and (5) can be found in [3]. □

The following lemma follows from Lemma 3 in [6].

Lemma 3. *Let $b \neq 0$ be a fixed integer, and let $a > 0$ be an integer such that $D(a, b) > 0$. Then the sequence $\mathcal{U}(a, b)$ is nondecreasing for $n \geq 0$ and strictly increasing for $n \geq 2$.*

Lemma 4. *Let $b \neq 0$ be a fixed integer. Let $u_n(a, b)$ denote the nth term of $\mathcal{U}(a, b)$. Then*

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

Proof. This follows from the Binet formulas for $\mathcal{U}(a, b)$ and $\mathcal{U}(-a, b)$. □

3. The Proof of Theorem 2

Proof of Theorem 2. Let b be a fixed odd integer. Let p be an odd prime such that $\left(\frac{-b}{p}\right) = 1$ and let $A_1 \in \mathbb{Z}$, with $1 \leq A_1 \leq p-1$ be a solution to

$$x^2 \equiv -b \pmod{p}. \tag{4}$$

Note that $A_2 = p - A_1$ is also a solution to (4). Without loss of generality, assume that $A_1 \equiv 0 \mod 2$, so that $A_2 \equiv 1 \pmod{2}$. Let

$$a_1 \equiv A_1 \pmod{2p} \quad \text{and} \quad a_2 \equiv A_2 \pmod{2p}$$

be positive integers with $(a_1, a_2) \neq (A_1, A_2)$, such that

$$D(a_1, b) > 0 \quad \text{and} \quad D(a_2, b) > 0. \tag{5}$$

Then $a_1 = A_1 + z_1 p$ and $a_2 = A_2 + z_2 p$, for some even integers $z_1, z_2 > 0$. Since

$$\begin{aligned} \mathcal{U}(a_1, b) &\equiv (0, 1, 0, 1, 0, 1, \ldots) \pmod{2} \quad \text{and} \\ \mathcal{U}(a_2, b) &\equiv (0, 1, 1, 0, 1, 1, \ldots) \pmod{2}, \end{aligned}$$

we see that

$$P_2\left(\mathcal{U}(a_1, b)\right) = 2 \quad \text{and} \quad P_2\left(\mathcal{U}(a_2, b)\right) = 3.$$

Thus,

$$P_2(W_{a_1,a_2}) = 6 \quad \text{and} \quad \Gamma_2(W_{a_1,a_2}) = [0, 0, 1, 1, 1, 0]. \tag{6}$$

Since $a_1^2 + b \equiv 0 \pmod{p}$ and $a_2 \equiv -a_1 \pmod{p}$, we have by Lemma 4 that

$$\begin{aligned} \mathcal{U}(a_1, b) \pmod{p} = \big(&0, 1, a_1, 0, M, a_1 M, 0, M^2, a_1 M^2, 0, \\ &M^3, a_1 M^3, 0, M^4, a_1 M^4, 0, \ldots\big) \end{aligned} \tag{7}$$

and

$$\begin{aligned} \mathcal{U}(a_2, b) \pmod{p} = \big(&0, 1, -a_1, 0, -M, a_1 M, 0, M^2, -a_1 M^2, 0, \\ &-M^3, a_1 M^3, 0, M^4, -a_1 M^4, 0, \ldots\big), \end{aligned} \tag{8}$$

where $M \equiv a_1 b \not\equiv 0 \pmod{p}$ is the multiplier of $\mathcal{U}(a_1, b)$ modulo p. Then both $\mathcal{U}(a_1, b)$ and $\mathcal{U}(a_2, b)$ have restricted period modulo p equal to 3. Let w_n be the nth term of $\mathcal{W}_{a_1,a_2}$. From (7) and (8), we see for $j \geq 0$ that

$$\begin{aligned} w_{6j} \equiv w_{6j+2} \equiv w_{6j+3} \equiv w_{6j+4} \equiv 0 \pmod{p}, \\ w_{6j+1} \equiv 2M^{2j} \pmod{p} \quad \text{and} \quad w_{6j+5} \equiv 2a_1 M^{2j+1} \pmod{p}. \end{aligned} \tag{9}$$

It now follows from (6) and (9) that

$$w_n \equiv \begin{cases} 0 \pmod{2} & \text{when } n \equiv 0,1,5 \pmod{6} \\ 0 \pmod{p} & \text{when } n \equiv 0,2,3,4 \pmod{6}. \end{cases} \tag{10}$$

For any

$$k \in \mathcal{A} = \left\{ 2pz \;\middle|\; z \geq 1 \right\},$$

we conclude from (10) that each term of $\mathcal{W}_{a_1,a_2} + k$ is divisible by at least one prime in $\{2, p\}$. By (5) and Lemma 3, we deduce that $\mathcal{W}_{a_1,a_2}$ is strictly increasing for $n \geq 0$. Thus, for any sufficiently large choice of $k \in \mathcal{A}$, it follows that $\mathcal{W}_{a_1,a_2}+k$ is primefree. Observe that the gap between consecutive terms of $\mathcal{W}_{a_1,a_2}$ is increasing, while the gap between consecutive terms in the arithmetic progression $\mathcal{A}$ is fixed. This phenomenon allows us to choose $k \in \mathcal{A}$ sufficiently large so that for some N, we have

$$w_N < k < w_{N+1}, \quad k - w_N > p \quad \text{and} \quad w_{N+1} - k > p.$$

Consequently, no term of either sequence $\mathcal{W}_{a_1,a_2} \pm k$ is zero or prime. □

We give an example to illustrate Theorem 2.

Example 1. Let $b = 3$ and $p = 13$. Note that $\left(\frac{-3}{13}\right) = 1$. Let $A_1 = 6$ and $A_2 = 7$. Then

$$A_1^2 \equiv A_2^2 \equiv -3 \pmod{13} \quad \text{and} \quad A_2 = 13 - A_1.$$

Let

$$a_1 = 32 \equiv A_1 \pmod{26} \quad \text{and} \quad a_2 = 33 \equiv A_2 \pmod{26}.$$

Observe that

$$(32, 33) \neq (6, 7), \quad D(32, 3) > 0 \quad \text{and} \quad D(33, 3) > 0.$$

Then, some simple calculations reveal:

$$\Gamma_2(W_{32,33}) = [0, 0, 1, 1, 1, 0], \tag{11}$$

$$\mathcal{U}(32, 3) \pmod{13} = (0, 1, 6, 0, 5, 4, 0, 12, 7, 0, 8, 9, 0, 1, 6, 0, 5, \ldots), \tag{12}$$

$$\mathcal{U}(33, 3) \pmod{13} = (0, 1, 7, 0, 8, 4, 0, 12, 6, 0, 5, 9, 0, 1, 7, 0, 8, \ldots). \tag{13}$$

Adding (12) and (13) we see that

$$\Gamma_{13}(W_{32,33}) = [0, 2, 0, 0, 0, 8, 0, 11, 0, 0, 0, 5]. \tag{14}$$

Then, by layering two juxtaposed copies of (11) on top of one copy of (14), we have

n	0	1	2	3	4	5	6	7	8	9	10	11
$\Gamma_2(\mathcal{W}_{32,33})$	0	0	1	1	1	0	0	0	1	1	1	0
$\Gamma_{13}(\mathcal{W}_{32,33})$	0	2	0	0	0	8	0	11	0	0	0	5

from which we can deduce (10). Finally, choosing

$$k \in \mathcal{A} = \left\{ 26z \;\middle|\; z \geq 1 \right\},$$

with k sufficiently large, we see from (10) that each term of each sequence $|\mathcal{W}_{32,33} \pm k|$ is divisible by, but not equal to, at least one prime in $\{2, 13\}$.

4. The Proof of Theorem 3

The Proof of Theorem 3. Let $p \notin \{2, 17, 19\}$ be prime, let $b = 1$, and suppose that a is an integer such that $a \equiv m \pmod{646p}$, where $0 \leq m \leq 646p - 1$, and m satisfies one of the 16 systems of congruences in (2). Recall that

$$\mathcal{W}_{1,a} := \mathcal{U}(1,1) + \mathcal{U}(a,1),$$

where $\mathcal{U}(1,1)$ is the Fibonacci sequence. Let $u_n(1)$ denote the nth term of $\mathcal{U}(1,1)$, and let $u_n(a)$ denote the nth term of $\mathcal{U}(a,1)$.

Since $a \equiv 0 \pmod 2$, it follows that $w_n \equiv 0 \pmod 2$ exactly when $n \equiv 0, 1, 5 \pmod 6$. Since $a \equiv -1 \pmod p$, we have from Lemma 4 that $w_n \equiv 0 \pmod p$ if $n \equiv 0 \pmod 2$. By inspection,

$$\left(\frac{D(a)}{17}\right) = -1 \Longleftrightarrow a \equiv m \pmod{17}, \quad \text{where} \quad m \in \{\pm 1, \pm 4, \pm 5, \pm 6\}.$$

Then, by Lemma 2, we have that $u_{9n}(a) \equiv 0 \pmod{17}$ for all $n \geq 0$, if $\left(\frac{D(a)}{17}\right) = -1$. Consequently,

$$w_{9n} \equiv 0 \pmod{17} \text{ for all } n \geq 0,$$

if $a \equiv m \pmod{17}$, where $m \in \{\pm 1, \pm 4, \pm 5, \pm 6\}$. Again by inspection, $u_3(1) = 2$, $u_3(\pm 4) = 17$ and

$$\left(\frac{D(1)}{19}\right) = \left(\frac{5}{19}\right) = 1 = \left(\frac{D(\pm 4)}{19}\right) = \left(\frac{1}{19}\right).$$

It now follows from Lemma 2 that if $a \equiv m \pmod{19}$, where $m \in \{1, \pm 4\}$, then

$$R_{19} \equiv 2 \pmod 4, \quad 18 \equiv 0 \pmod{P_{19}} \quad \text{and} \quad M \equiv 1 \pmod{19}.$$

Thus, from Lemma 1, if $n \equiv m \pmod{18}$, where $m \in \{3, 15\}$, we see that

$$u_n(1) \equiv 2 \pmod{19} \quad \text{and} \quad u_n(\pm 4) \equiv 17 \pmod{19}.$$

Hence, $w_n \equiv 2 + 17 \equiv 0 \pmod{19}$. In summary, we have shown

$$w_n \equiv \begin{cases} 0 \pmod{2} & \text{when } n \equiv 0, 1, 5 \pmod{6} \\ 0 \pmod{p} & \text{when } n \equiv 0 \pmod{2} \\ 0 \pmod{17} & \text{when } n \equiv 0 \pmod{9} \\ 0 \pmod{19} & \text{when } n \equiv 3, 15 \pmod{18}, \end{cases} \tag{15}$$

which implies that w_n is divisible by at least one prime in the set $\{2, p, 17, 19\}$, for all $n \geq 0$. Then, using an argument similar to the one used in the proof of Theorem 2, it can be shown that for any sufficiently large value of z, no term of each of the sequences $|\mathcal{W}_{1,a} \pm k|$ is zero or prime, where

$$k = 2 \cdot p \cdot 17 \cdot 19 \cdot z = 646pz.$$

Consequently, each of the sequences $\mathcal{W}_{1,a} \pm k$ is primefree provided

$$a \equiv m \pmod{646p}, \quad \text{with} \quad 0 \leq m \leq 646p - 1,$$

and m satisfies one of the 16 systems of congruences in (2). □

We give an example to illustrate Theorem 3.

Example 2. Let $p = 3$. Then by Theorem 3, there exist infinitely many positive integers $k = 1938z$ such that each of the sequences $\mathcal{W}_{1,a} \pm k$ is primefree for every $a \equiv m \pmod{1938}$, where

$$m \in \{80, 566, 650, 764, 794, 878, 992, 1106, 1220, \\ 1364, 1478, 1592, 1706, 1790, 1820, 1934\}.$$

Remark 1. The smallest nonnegative value of m that satisfies all the congruences in a particular system in (2) for any prime $p \notin \{2, 17, 19\}$ is $m = 4$, when $p = 5$.

Acknowledgements The authors thank the referee for the suggestions that improved the paper.

References

[1] Y. 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.

[2] K. Bresz, L. Jones, A. Lamarche and M. Markovich, A problem related to a conjecture of Polignac, *Integers* **16** (2016), Paper No. A43, 8 pp.

[3] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. Math.* **15** (1913) 30–70.

[4] R. D. Carmichael, On sequences of integers defined by recurrence relations, *Quart. J. Pure Appl. Math.* **48** (1920), 343–372.

[5] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, **104**, American Mathematical Society, (2003).

[6] P. Hilton, J. Pedersen and L. Somer, On Lucasian numbers, *Fibonacci Quart.* **35** (1997), 43–47.

[7] D. Ismailescu, L. Jones and T. Phillips, Primefree shifted Lucas sequences of the second kind, *J. Number Theory* **173** (2017), 87–99.

[8] D. Ismailescu and 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.

[9] L. Jones, Fibonacci variations of a conjecture of Polignac, *Integers* **12** (2012), no. 4, 659–667.

[10] L. Jones, Primefree shifted Lucas sequences, *Acta Arith.* **170** (2015), no. 3, 287–298.

[11] D. H. Lehmer, An extended theory of Lucas' functions, *Ann. Math.* **31** (1930), 419–448.

[12] E. Lucas, Theorie des Fonctions Numeriques Simplement Periodiques (French), *Amer. J. Math.* **1** (1878), no. 2, 184–196.

[13] E. Lucas, Theorie des Fonctions Numeriques Simplement Periodiques (French), *Amer. J. Math.* **1** (1878), no. 3, 197–240.

[14] E. Lucas, Theorie des Fonctions Numeriques Simplement Periodiques (French), *Amer. J. Math.* **1** (1878), no. 4, 289–321.

[15] L. Somer, Upper bounds for frequencies of elements in second-order recurrences over a finite field, *Applications of Fibonacci numbers*, Vol. **5** (St. Andrews, 1992), 527–546, Kluwer Acad. Publ., Dordrecht, (1993).