ON PRIMES IN LUCAS SEQUENCES

LAWRENCE SOMER AND MICHAL KŘÍŽEK

Abstract. Consider the Lucas sequence $u(a, b) = \{u_n(a, b)\}$ and the companion Lucas sequence $v(a, b) = \{v_n(a, b)\}$ which both satisfy the second order recursion relation

$$w_{n+2} = aw_{n+1} - bw_n$$

with initial terms $u_0 = 0$, $u_1 = 1$, and $v_0 = 2$, $v_1 = a$, respectively. We give both necessary and sufficient tests and also necessary tests for the primality of $|u_n|$ and $|v_n|$. For those tests which are only necessary, we show that these tests are not sufficient by means of a simple criterion using the Legendre symbol. These results are specialized to the Fibonacci numbers $\{F_n\}$ and to the Lucas numbers $\{L_n\}$. In particular, we generalize a result of Drobot giving criteria for F_p not to be prime, where p is a prime, to the Lucas numbers $\{L_n\}$.

1. Introduction

As usual, let $\{L_n\}$ denote the sequence of Lucas numbers which satisfy the same recursion relation as the sequence of Fibonacci numbers $\{F_n\}$ and have initial terms $L_0 = 2$ and $L_1 = 1$. Throughout this paper, p will always denote a prime and ε will be assumed to be a member of the set $\{-1, 1\}$. It is well-known that F_n or L_m can be prime only if $n = 4$, n is prime, $m = 0$, m is prime, or m is a power of 2. These observations are consequences of the fact that $F_0 = 0$, $F_1 = 1$, $L_0 = 2$, $L_1 = 1$, $\{F_n\}$ is increasing for $n \geq 2$, $\{L_m\}$ is increasing for $m \geq 1$, $F_i \mid F_n$ for $i \notin \{0, 2\}$ if and only if $i \mid n$, and $L_j \mid L_m$ for $j, m \geq 1$ if and only if $j \mid m$ and m/j is odd. There are 33 known values of n for which F_n is prime (see [22]) with the largest value being $n = 81839$. The first 12 values of n for which F_n is prime are

$$n = 3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83.$$

In addition, there exist 43 known values of m for which L_m is prime (see [23]) with the largest value being $m = 56003$. The first 13 values of m for which L_m is prime are

$$m = 0, 2, 4, 5, 7, 8, 11, 13, 16, 17, 19, 31, 37.$$

It is conjectured that F_n and L_m are prime for infinitely many values of n and m (see [14, pp. 362–364]). However, Drobot [7] proved the following theorem giving simple conditions for F_p to be composite.

Theorem 1.1. (Drobot) *Suppose that* $p > 7$, $p \equiv 2$ *or* $4 \pmod 5$, *and* $2p-1$ *is also a prime. Then* $2p - 1 \mid F_p$ *and* $F_p > 2p - 1$ *and thus composite.*

Example 1.2. Making use of Appendix A.3 of [9], we see that

$$37 \mid F_{19} = 4181 = 37 \cdot 113,$$
$$73 \mid F_{37} = 24157817 = 73 \cdot 149 \cdot 2221,$$
$$157 \mid F_{79} = 14472334024676221 = 157 \cdot 92180471494753,$$

and

$$193 \mid F_{97} = 83621143489848422977 = 193 \cdot 389 \cdot 3084989 \cdot 361040209.$$

In this paper, we will prove the following complementary result to Theorem 1.1 providing values of n for which n is equal to a prime or a power of 2 and L_n is composite. We recall that the number $M_p = 2^p - 1$ is called a *Mersenne number.* If $2^p - 1$ itself is prime, then it is called a *Mersenne prime.*

Theorem 1.3.

(i) Suppose that $p \equiv 29 \pmod{30}$ and $2p+1$ is also prime. Then $2p+1 \mid L_p$ and $2p+1 < L_p$.

(ii) Suppose that $p \equiv 3 \pmod 4$ and $2^p - 1$ is a Mersenne prime. Then $2^p - 1 \mid L_{2^{p-1}}$. Moreover, $2^p - 1 < L_{2^{p-1}}$ when $p > 3$.

Example 1.4. By the use of Appendix A.4 in [9], we see that

$$59 \mid L_{29} = 1149851 = 59 \cdot 19489,$$
$$179 \mid F_{89} = 3980154972736918051 = 179 \cdot 22235502640988369,$$

and

$$2^7 - 1 = 127 \mid L_{2^6} = L_{64} = 23725150497407 = 127 \cdot 186812208641.$$

The next assertion, Theorem 1.5, which concerns Mersenne primes, presents a similar result to that of Theorem 1.1. This result was proved by Euler and independently by Lagrange. A proof of Theorem 1.5 is given in [14, pp. 90–91].

Theorem 1.5. (Euler and Lagrange) *Let $p > 3$ be a prime such that $p \equiv 3 \pmod 4$ and $2p + 1$ is also prime. Then $2p + 1 \mid M_p$ and M_p is composite.*

The primality of Mersenne numbers is of interest because of their well-known relationship to even perfect numbers.

2. Lucas Sequences and Companion Lucas Sequences

We will prove Theorems 1.1 and 1.3 by treating them as special cases of more general results, Theorems 3.15, 3.18, and 3.20, involving Lucas sequences and companion Lucas sequences. Let $u(a, b) = \{u_n(a, b)\}$ called a *Lucas sequence,* and $v(a, b) = \{v_n(a, b)\}$ called a *companion Lucas sequence*, denote the recurrences satisfying the second-order recursion relation

$$w_{n+2} = aw_{n+1} - bw_n \tag{2.1}$$

with initial terms $u_0 = 0$, $u_1 = 1$ and $v_0 = 2$, $v_1 = a$, respectively, where a and b are integers. Associated with $u(a, b)$ and $v(a, b)$ is the characteristic polynomial

$$f(x) = x^2 - ax + b \tag{2.2}$$

with characteristic roots α, β and discriminant $D = a^2 - 4b = (\alpha - \beta)^2$. By the Binet formulas,

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{if } D \neq 0, \tag{2.3}$$

$$u_n = n\alpha^{n-1} \quad \text{if } D = 0, \tag{2.4}$$

and

$$v_n = \alpha^n + \beta^n. \tag{2.5}$$

Example 2.1. For later reference, we make use of the recursion relation given in (2.1) to derive the first six terms of both $u(a, b)$ and $v(a, b)$ in terms of a and b:

$$\begin{aligned} &u_0 = 0, \quad u_1 = 1, \quad u_2 = a, \quad u_3 = a^2 - b, \\ &u_4 = a^3 - 2ab = a(a^2 - 2b), \quad u_5 = a^4 - 3a^2b + b^2, \end{aligned} \tag{2.6}$$

$$\begin{aligned} &v_0 = 2, \quad v_1 = a, \quad v_2 = a^2 - 2b, \quad v_3 = a^3 - 3ab = a(a^2 - 3b), \\ &v_4 = a^4 - 4a^2b + 2b^2, \quad v_5 = a^5 - 5a^3b + 5ab^2. \end{aligned} \tag{2.7}$$

The sequences $u(a, b)$ and $v(a, b)$ are called *degenerate* if $\alpha\beta = 0$ or α/β is a root of unity. Note that $u_n(a, b) = 0$ or $v_n(a, b) = 0$ for some $n > 0$ only if $u(a, b)$ or $v(a, b)$ is degenerate. Since α and β are zeros of a monic polynomial of degree 2 over the rationals, α/β can be an nth root of unity only if $n = 1, 2, 3, 4$, or 6.

In the next section, along with other results, we will determine all cases in which $u(a, b)$ or $v(a, b)$ is degenerate and $|u_n(a, b)|$ or $|v_n(a, b)|$ is prime for $n \geq 0$. For reference, the following proposition (proved in [21, p. 613]) lists all cases in which $u(a, b)$ and $v(a, b)$ are degenerate.

Proposition 2.2. *Let N be a nonzero integer. Then both $u(a, b)$ and $v(a, b)$ are degenerate if and only if $ab = 0$ or (a, b) is of the form (N, N^2), $(2N, 2N^2)$, $(3N, 3N^2)$, or $(2N, N^2)$.*

Lemma 2.3. *Let $u(a, b)$ and $v(a, b)$ be degenerate sequences for which $\gcd(a, b) = 1$. Let $n \geq 0$ and $k \geq 0$. Then*

(i) *$(a, b) = (0, \varepsilon)$, $(\varepsilon, 0)$, $(\varepsilon, 1)$, or $(2\varepsilon, 1)$.*
(ii) *If $(a, b) = (0, \varepsilon)$, then $u_{2k} = 0$ and $u_{2k+1} = (-\varepsilon)^k$, while $v_{2k} = 2(-\varepsilon)^k$ and $v_{2k+1} = 0$.*
(iii) *If $(a, b) = (\varepsilon, 0)$, then $u_0 = 0$ and $u_n = \varepsilon^{n+1}$ for $n \geq 1$, while $v_0 = 2$ and $v_n = \varepsilon^n$ for $n \geq 1$.*
(iv) *If $(a, b) = (\varepsilon, 1)$, then $u_{3k} = 0$, $u_{3k+1} = (-\varepsilon)^k$, and $u_{3k+2} = -(-\varepsilon)^{k+1}$, while $v_{3k} = 2(-\varepsilon)^k$, $v_{3k+1} = -(-\varepsilon)^{k+1}$, and $v_{3k+2} = -(-\varepsilon)^k$.*
(v) *If $(a, b) = (2\varepsilon, 1)$, then $u_n = n\varepsilon^{n+1}$, while $v_n = 2\varepsilon^n$.*

Proof. Part (i) follows from Proposition 2.2. Parts (ii)–(v) can be established through induction. □

Definition 2.4. Let $\{w_n\}_{n=0}^{\infty}$ be a sequence of integers. Then p is a *primitive* prime divisor of w_n for $n \geq 1$ if $p \mid w_n$ and either $n = 1$ or $n \geq 2$ and $p \nmid w_1 w_2 \cdots w_{n-1}$.

In this paper, we will be interested in finding indices n for which $|u_n(a, b)| = p$ or $|v_n(a, b)| = p$. A key tool for accomplishing this is the following theorem, which is proved in Theorems C, 1.3, and 1.4 by Bilu, Hanrot, and Voutier in [1].

Theorem 2.5. *Consider the nondegenerate Lucas sequence $u(a, b)$ for which $\gcd(a, b) = 1$.*

(i) *If $n > 30$, then u_n has a primitive prime divisor.*
(ii) *If $n \leq 30$, then u_n has a primitive prime divisor if it is not the case that $n \in \{1, \ldots, 8, 10, 12, 13, 18, 30\}$.*
(iii) *If $n \in \{5, 7, 8, 10, 12, 13, 18, 30\}$, then there exist exactly 38 terms such that $u_n(a, b)$ has no primitive prime divisor. These terms are given in Table 1 below, which is extracted from Table 1 on page 78 of [1].*

Table 1. Values for which the sequence $u_n(a,b)$ has no primitive prime divisor when $n \in \{5, 7, 8, 10, 12, 13, 18, 30\}$.

n	(a,b)
5	$(\pm1, 2)$, $(\pm1, 3)$, $(\pm12, 55)$, $(\pm12, 377)$
7	$(\pm1, 5)$
8	$(\pm1, 2)$, $(\pm2, 7)$
10	$(\pm2, 3)$, $(\pm5, 7)$, $(\pm5, 18)$
12	$(\pm1, -1)$, $(\pm1, 2)$, $(\pm1, 3)$, $(\pm1, 4)$, $(\pm1, 5)$, $(\pm2, 15)$
13	$(\pm1, 2)$
18	$(\pm1, 2)$
30	$(\pm1, 2)$

Remark 2.6. For $n \in \{1, 2, 3, 4, 6\}$ there exist infinitely many terms such that $u_n(a,b)$ has no primitive prime divisor. As contrasted to our Definition 2.4 of a primitive divisor, Bilu, Hanrot, and Voutier in [1] define p to be a primitive divisor of u_n if $p \nmid u_n$, but $p \nmid Du_1u_2 \cdots u_{n-1}$.

Propositions 3.1–3.4 and Theorems 3.5 and 3.9 will give both necessary and sufficient conditions for $|u_n(a,b)|$ or $|v_n(a,b)|$ to be prime, while Theorems 3.7 and 3.10 will provide only necessary conditions for $|u_n(a,b)|$ or $|v_n(a,b)|$ to be prime. Theorems 3.15, 3.18, and 3.20 will give simple criteria involving the Legendre symbol to show that these necessary conditions given in Theorems 3.7 and 3.10 for the primality of $|u_n(a,b)|$ or $|v_n(a,b)|$ are not sufficient. Examples 3.17, 3.19, 3.23, and 3.24 will provide specific instances to show that the criteria given in Theorems 3.15, 3.18, and 3.20 for the compositeness of certain terms are indeed satisfied in particular cases. Further criteria based on known results will be given to show that for very particular Lucas sequences $u(a,b)$, the necessary conditions given in Theorem 3.7 for the primality of $|u_n(a,b)|$ are not sufficient.

Lemmas 2.7 and 2.9 and Theorem 2.8 give known properties of the sequences $u(a,b)$ and $v(a,b)$ that we will need for our later proofs.

Lemma 2.7. *Consider the sequences $u(a,b)$ and $v(a,b)$.*

(i) *If $m \mid n$, then $u_m \mid u_n$.*
(ii) *If $m \mid n$ and n/m is odd, then $v_m \mid v_n$.*
(iii) $u_n(-a,b) = (-1)^{n+1}u_n(a,b)$.
(iv) $v_n(-a,b) = (-1)^n v_n(a,b)$.
(v) $u_{2n} = u_n v_n$.
(vi) $v_n^2 - Du_n^2 = 4b^n$.
(vii) *If $p \nmid 2b$, then $p \nmid \gcd(u_n, v_n)$.*
(viii) *If $p \nmid 2bD$, then $p \mid u_{p-(D/p)}$, where (D/p) denotes the Legendre symbol and $(D/p) = 0$ if $p \mid D$.*
(ix) *If $p \nmid 2bD$, then $p \mid u_{(p-(D/p))/2}$ if and only if $(b/p) = 1$.*
(x) *If $p \nmid 2bD$, then $p \mid v_{(p-(D/p))/2}$ if and only if $(b/p) = -1$.*
(xi) *If $p \nmid 2bD$ and p is a primitive divisor of u_n, then $p = kn \pm 1$ for some $k \geq 1$.*
(xii) *If $p \nmid 2b$ and p is a primitive divisor of v_n, then $p = 2kn \pm 1$ for some $k \geq 1$.*
(xiii) *If $\gcd(a,b) = 1$, then $\gcd(u_n, b) = \gcd(v_n, b) = 1$ for $n \geq 1$.*

Proof. Parts (i)–(vi) follow from the Binet formulas (2.3), (2.4), and (2.5). Part (vii) follows from part (vi). Part (viii) is proved in [6, pp. 44-45] and part (ix) is proved in [11, p. 441]. Parts (xi) and (xii) are proved in [11, p. 425]. Part (xiii) is proved in [6, p. 35]. We now prove part (x). Suppose that $(b/p) = -1$. By (v),

$$u_{p-(D/p)} = u_{(p-(D/p))/2} \cdot v_{(p-(D/p))/2}. \tag{2.8}$$

By (viii), $p \mid u_{p-(D/p)}$. It now follows from (2.8) and part (ix) that $p \mid v_{(p-(D/p))/2}$.

Conversely, suppose that $p \mid v_{(p-(D/p))/2}$. Then $p \nmid u_{(p-(D/p))/2}$ by part (vii). Thus, $(b/p) = -1$ by part (ix). □

Theorem 2.8. *Consider the sequences* $u(a,b)$ *and* $v(a,b)$*, where* $\gcd(a,b) = 1$ *and* $ab \neq 0$*. Let* $m = 2^r m'$ *and* $n = 2^s n'$*, where* m' *and* n' *are odd, and* $r, s \geq 0$*. Let* $d = \gcd(m,n)$*. Then*

(i) $\gcd(u_m, u_n) = |u_d|$,

(ii) $\gcd(v_m, v_n) = \begin{cases} v_d, & \text{if } r = s; \\ 1 \text{ or } 2, & \text{if } r \neq s, \end{cases}$

(iii) *The value of* $\gcd(v_m, v_n)$ *is even if and only if* b *is odd and either* a *is even or* $3 \mid d$*.*

The proof of Theorem 2.8 is given in [13].

Lemma 2.9. Let $u(a,b)$ and $v(a,b)$ be nondegenerate sequences for which $\gcd(a,b) = 1$. Then $|u_n| = 1$ for $n > 1$ or $|v_n| = 1$ for $n \geq 1$ only in the following instances:

(i) $n = 1$, $a = \pm 1$, $v_1 = \pm 1$,
(ii) $n = 2$, $a = \pm 1$, $u_2 = \pm 1$,
(iii) $n = 2$, a is odd, $b = (a^2 \pm 1)/2$, $v_2 = \pm 1$,
(iv) $n = 3$, $b = a^2 \pm 1$, $u_3 = \pm 1$,
(v) $n = 4$, $a = \pm 1$, $b = 2$, $v_4 = 1$,
(vi) $n = 5$, $(a,b) = (\pm 1, 2)$, $(\pm 1, 3)$, $(\pm 12, 55)$, or $(\pm 12, 377)$, $u_5 = \pm 1$,
(vii) $n = 7$, $a = \pm 1$, $b = 5$, $u_7 = 1$,
(viii) $n = 13$, $a = \pm 1$, $b = 2$, $u_{13} = -1$.

This is proved in [12, pp. 253–254].

3. Main Results

Propositions 3.1 and 3.2 determine exactly when $|u_n(a,b)|$ and $|v_m(a,b)|$ are primes for $0 \leq n \leq 4$ and $0 \leq m \leq 3$ based on simple constraints on the parameters a and b.

Proposition 3.1. *Consider the Lucas sequence* $u(a,b)$*. Let* $1 \leq n \leq 4$*. Then* $|u_n(a,b)| = p$ *for some prime* p *if and only if one of the following three conditions holds:*

(i) $n = 2$ *and* $a = \pm p$*,*
(ii) $n = 3$ *and* $b = a^2 \pm p$*,*
(iii) $n = 4$*,* p *is odd and one of the following conditions holds:*
  (a) $a = \pm 1$ *and* $b = (1 + \varepsilon p)/2$*,*
  (b) $a = \varepsilon p$ *and* $b = (p^2 \pm 1)/2$*.*

Proof. It is obvious that n cannot be equal to 0 or 1. Parts (i) and (ii) follow from (2.6) in Example 2.1. Part (iii) is proved in Theorem 2.10 of [19]. □

Proposition 3.2. *Consider the companion Lucas sequence* $v(a,b)$*. Let* $0 \leq m \leq 3$*. Then* $|v_m(a,b)| = p$ *for some prime* p *if and only if one of the following four conditions holds:*

(i) $m = 0$ *and* $p = 2$*,*

(ii) *$m = 1$ and $a = \pm p$,*
(iii) *$m = 2$, $a \equiv p \pmod 2$, and $b = (a^2 \pm p)/2$,*
(iv) *$m = 3$ and one of the following holds:*
  (a) *$\varepsilon p \equiv 1 \pmod 3$, $a = \pm 1$, and $b = (1 - \varepsilon p)/3$,*
  (b) *$p \not\equiv 0 \pmod 3$, $a = \varepsilon p$, and $b = (p^2 - 1)/3$.*

Proof. Part (i) is obvious. Parts (ii) and (iii) follow from (2.7) in Example 2.1. It is evident that in part (iii), we must have $a \equiv p \pmod 2$ in order for b to be an integer.

By the expression for $v_3(a, b)$ in (2.7), we see that either $|a| = 1$ or $|a| = p$. If $|a| = 1$, then $a^2 - 3b = \varepsilon p$, which implies that $b = (1 - \varepsilon p)/3$. It is clear that b is an integer if and only if $\varepsilon p \equiv 1 \pmod 3$. If $|a| = p$, then $a^2 - 3b = \pm 1$, which implies that $b = (p^2 \pm 1)/3$. It is evident that $p \not\equiv 0 \pmod 3$, since b is an integer. Thus, $p^2 \equiv 1 \pmod 3$, which implies that $b = (p^2 - 1)/3$ in order for b to be an integer. □

By virtue of Proposition 3.1 and 3.2, we will usually assume that $n \geq 5$ and $m \geq 4$ in examining the primality of $|u_n(a, b)|$ and $|v_m(a, b)|$.

Proposition 3.3. *Consider the sequences $u(a, b)$ and $v(a, b)$ and let $\gcd(a, b) = d > 1$. Then*

(i) *$|u_n(a, b)|$ is never prime for $n \geq 4$,*
(ii) *$|v_m(a, b)|$ is never prime for $m \geq 3$.*

Proof. It follows by induction using the recursion relations defining $u(a, b)$ and $v(a, b)$ that $d^k \mid u_n(a, b)$ for $n \geq 2k$ and $d^k \mid v_m(a, b)$ for $m \geq 2k - 1$. Thus, $d^2 \mid u_n(a, b)$ for $n \geq 4$ and $d^2 \mid v_m(a, b)$ for $m \geq 3$. □

In light of Proposition 3.3, we will assume from here on that $\gcd(a, b) = 1$. The remaining results not proved in this section will be proved in Section 5.

Proposition 3.4. *Suppose that $u(a, b)$ and $v(a, b)$ are both degenerate and that $\gcd(a, b) = 1$. Then*

(i) *$(a, b) = (0, \varepsilon)$, $(\varepsilon, 0)$, $(\varepsilon, 1)$, or $(2\varepsilon, 1)$.*
(ii) *If $(a, b) = (0, \varepsilon)$, then $|u_n|$ is never prime, while $|v_n|$ is prime if and only if $2 \mid n$. In particular, $|v_{2n}| = 2$ for $n \geq 0$.*
(iii) *If $(a, b) = (\varepsilon, 0)$, then $|u_n|$ is never prime, whereas $|v_n|$ is prime if and only if $n = 0$. In particular, $v_0 = 2$.*
(iv) *If $(a, b) = (\varepsilon, 1)$, then $|u_n|$ is never prime, whereas $|v_n|$ is prime if and only if $3 \mid n$. In particular, $|v_{3n}| = 2$ for $n \geq 0$.*
(v) *Suppose that $(a, b) = (2\varepsilon, 1)$. Then $|u_n|$ is prime if and only if n is prime. In particular, $|u_p| = p$ for each prime p. Moreover, $|v_n| = 2$ for $n \geq 0$ and $|v_n|$ is prime for all n.*

The proof of Proposition 3.4 follows immediately from Lemma 2.3.

By virtue of Proposition 3.4, from now on, we will only consider nondegenerate sequences $u(a, b)$ and $v(a, b)$ for which $\gcd(a, b) = 1$.

Theorem 3.5. *Consider the nondegenerate Lucas sequence $u(a, b)$, where $\gcd(a, b) = 1$. Suppose that $n \geq 6$ is composite and that $n \neq 9$. Then $|u_n(a, b)|$ is prime if and only if one of the following cases holds:*

(i) *$|u_6(\pm 1, 2)| = 5$,*
(ii) *$|u_8(\pm 1, 2)| = 3$,*
(iii) *$|u_{10}(\pm 1, 2)| = 11$,*
(iv) *$|u_{10}(\pm 1, 3)| = 31$,*

(v) $u_{15}(\pm 1, 2) = -89$,
(vi) $u_{25}(\pm 1, 2) = -4049$,
(vii) $u_{25}(\pm 1, 3) = 282001$,
(viii) $|u_{26}(\pm 1, 2)| = 181$,
(ix) $u_{65}(\pm 1, 2) = -335257649$.

This is proved in the proof of Theorem 3.1 on pages 254–256 of [12].

Remark 3.6. We note that in Theorem 3.5, only in part (ii) is the prime value p of $|u_n(a,b)|$ not a primitive divisor of $u_n(a,b)$. In this case, $|u_8(\pm 1, 2)| = |u_4(\pm 1, 2)| = 3$. Obviously, $|u_n(a,b)|$ or $|v_n(a,b)|$ can be equal to a prime only if either all prime divisors of $u_n(a,b)$ or $v_n(a,b)$ are primitive or all prime divisors of $u_n(a,b)$ or $v_n(a,b)$ are not primitive. We will use this observation in finding all instances in which $|u_n(a,b)|$ or $|v_n(a,b)|$ can possibly be prime.

Theorem 3.7 complements Theorem 3.5 by finding a necessary condition for $|u_n(a,b)|$ to be prime in the remaining cases in which $n \geq 5$ and either n is prime or $n = 9$.

Theorem 3.7. *Consider the nondegenerate Lucas sequence $u(a,b)$, where* $\gcd(a,b) = 1$. *Suppose that $n \geq 5$ is prime or $n = 9$. Then $|u_n(a,b)| > 1$ and each prime divisor of $u_n(a,b)$ is primitive if and only if one of the two conditions below is satisfied. In particular, $|u_n(a,b)|$ can be prime in this case only if condition (i) or condition (ii) holds:*

(i) *$n \geq 5$ is prime and $u_n(a,b) \neq 1$, which occurs if and only if $(n,a,b) \neq (5,\pm 1,2)$, $(5,\pm 1,3)$, $(5,\pm 12,55)$, $(5,\pm 12,377)$, $(7,\pm 1,5)$, or $(13,\pm 1,2)$,*
(ii) *$n = 9$ and $u_3(a,b) = \pm 1$, which occurs if and only if $b = a^2 \pm 1$.*

Proof. By Theorem 2.8 (i) and the fact that $u_1 = 1$, we see that each prime divisor of u_n is primitive if n is prime.

Now suppose that $n = 9$. If $p \mid u_3$, then by Lemma 2.7 (i), $p \mid u_9$ and p is not a primitive divisor of u_9. It now follows from Theorem 2.8 (i) that each prime divisor of u_9 is primitive if $u_3 = \pm 1$.

The assertions concerning when $u_n(a,b) = \pm 1$ for n a prime follow from Lemma 2.9. □

Remark 3.8. We conjecture that for each prime $p \geq 5$, there exist infinitely many nondegenerate Lucas sequences $u(a,b)$ for which $|u_p(a,b)|$ is prime.

We also conjecture that there exist infinitely many nondegenerate Lucas sequences $u(a,b)$ for which $|u_9(a,b)|$ is prime. By Theorem 3.7 (ii), $|u_9(a,b)|$ can be prime only if (a,b) is of the form $(M, M^2+\varepsilon)$ for some nonzero integer M. By Theorem 2.14 on p. 200 of [19],

$$|u_9(M, M^2+\varepsilon)| = 3(M^2+\varepsilon)((M^2+\varepsilon)^2 - 1) - \varepsilon. \tag{3.1}$$

In Example 5.3 on pages 212–213 of [19], we searched for prime values of $|u_9(M, M^2+\varepsilon)|$ given in (3.1) for $1 \leq |M| \leq 386$. We found 121 such prime values given by 242 ordered pairs $(M, M^2+\varepsilon)$. The largest prime value found was

$$|u(\pm 380, 144401)| = 9032996815106399.$$

Theorem 3.9. *Let us consider the nondegenerate companion Lucas sequence $v(a,b)$, where* $\gcd(a,b) = 1$. *Suppose that $n \geq 4$. Then $v_n(a,b)$ has no primitive prime divisor if and only if*

$$\begin{aligned}(n,a,b) =& (4,\pm 1,2),\ (4,\pm 2,7),\ (5,\pm 2,3),\ (5,\pm 5,7),\ (5,\pm 5,18),\ (6,\pm 1,-1),\\ & (6,\pm 1,2),\ (6,\pm 1,3),\ (6,\pm 1,4),\ (6,\pm 1,5),\ (6,\pm 2,15),\ (9,\pm 1,2),\ \text{or } (15,\pm 1,2).\end{aligned}$$

In particular, $|v_n(a,b)| = p$, where p is not a primitive divisor of $v_n(a,b)$ if and only if one of the following four cases holds:

(i) $v_4(\pm 2, 7) = 2$,
(ii) $|v_5(\pm 2, 3)| = 2$,
(iii) $v_6(\pm 1, 4) = -7$,
(iv) $|v_9(\pm 1, 2)| = 5$.

Theorem 3.10. *Let us consider the nondegenerate companion Lucas sequence $v(a, b)$, where $\gcd(a, b) = 1$. Suppose that $n \geq 4$. Then $|v_n(a, b)| > 1$ and each prime divisor of $v_n(a, b)$ is primitive if and only if one of the four conditions below holds. In particular, $|v_n(a, b)| = p$, where p is a primitive divisor of $v_n(a, b)$ only if one of the conditions (i)–(iv) is satisfied.*

(i) *n is prime and $v_1 = \pm 1$, which occurs if and only if $a = \pm 1$.*
(ii) *$n = 2^k$ for some $k \geq 2$, $2 \nmid a$, and $n \neq 4$ if $(a, b) = (\pm 1, 2)$.*
(iii) *$n = 2p$ for some prime p, $v_2 = \pm 1$ which occurs if and only if a is odd and $b = (a^2 \pm 1)/2$, and it is not the case that $p = 3$ and a and b are odd.*
(iv) *$(a, b) = (\pm 1, 2)$ and $n = 4p$. In this case, $v_4(\pm 1, 2) = 1$.*

Proof. Throughout this proof, we assume that $v(a, b)$ is nondegenerate and $\gcd(a, b) = 1$. Suppose that there exists an integer m such that $1 \leq m < n$, $m \mid n$, n/m is odd, and $|v_m| > 1$. Then $v_m \mid v_n$ by Lemma 2.7 (ii). Let $p \mid v_m$. Then $p \mid v_n$ and p is not a primitive divisor of v_n. We also observe by Lemma 2.8 (iii) that if $v_1 = a$ is even, then $2 \mid v_n$ for all $n \geq 0$. We further notice by Lemma 2.8 (iii) that if $p = 3$ and a and b are odd, then 2 divides both $v_3(a, b)$ and $v_6(a, b)$ and 2 is not a primitive divisor of $v_6(a, b)$. We also note by Lemma 2.9 that $v_n(a, b)$ can equal ± 1 if and only if $(n, a, b) = (1, \pm 1, r)$, $(2, 2s + 1, ((2s + 1)^2 \pm 1)/2)$, or $(4, \pm 1, 2)$, where r and s are arbitrary integers. It now follows that $|v_n(a, b)| > 1$ and each prime divisor of v_n is primitive only if one of the conditions (i)–(iv) holds.

Conversely, we suppose that one of the conditions (i)–(iv) holds. By Theorem 2.8 (iii), v_n is odd. It then follows from Theorem 2.8 (ii) and our above arguments that $|v_n(a, b)| > 1$ and each prime divisor of v_n is primitive if one of the conditions (i)–(iv) holds. □

Remark 3.11. We conjecture that for any fixed integer $n \geq 4$, which satisfies one of conditions (i)–(iii), there exist infinitely many nondegenerate companion Lucas sequences $v(a, b)$ such that $|v_n(a, b)|$ is prime. We also conjecture that there exist infinitely many primes p such that $|v_{4p}(\pm 1, 2)|$ is prime.

Example 3.12. To lend some support for the conjectures in Remark 3.11, we examine the sequence $v(1, 2)$ for which $v_1 = 1$, $2 \nmid a$, and $v_4 = 1$, and also look at the sequence $v(3, 5)$ for which $v_1 = 1$, $2 \nmid a$, and $v_2 = -1$.

By inspection, we see that $|v_n(1, 2)|$ is prime for the following 25 values of n such that $|v_n(1, 2)| < 10^{16}$:

$$\begin{aligned} n =& 0,\ 2,\ 3,\ 5,\ 7,\ 8,\ 9,\ 11,\ 12,\ 13,\ 16,\ 17,\ 19,\ 20,\ 23,\ 32,\ 37, \\ & 41,\ 43,\ 47,\ 61,\ 67,\ 76,\ 83,\ 92. \end{aligned}$$

Moreover, by examination, we observe that $|v_n(3, 5)|$ is prime for the following values of n such that $|v_n(3, 5)| < 10^{14}$:

$$n = 0,\ 1,\ 8,\ 10,\ 14,\ 16,\ 34.$$

We also note by [4] that if α and β as usual denote the characteristic roots of $v(a, b)$ is prime, then $v_{2^{19}}(a, b) = v_{524288}(a, b)$ is prime when

$$(\alpha, \beta) = (475856, 1),\ (356926, 1),\ (341112, 1),\ \text{or}\ (75898, 1)$$

and $v_{2^{18}}(a,b) = v_{262144}(a,b)$ is prime when

$$(\alpha, \beta) = (773620, 1),\ (676754, 1),\ (525094, 1),\ (361658, 1),\ (145310, 1)\,(40734, 1),\ \text{or}\ (24518, 1).$$

In Theorems 3.15, 3.18, and 3.20, we show by the use of the Legendre symbol that the necessary conditions for the primality of $|u_n(a,b)|$ or $|v_n(a,b)|$ given in Theorems 3.7 and 3.10 are not sufficient. Before presenting these theorems, we will need the following result.

Theorem 3.13. *Let $u(a,b)$ and $v(a,b)$ be the nondegenerate sequences for which $\gcd(a,b) = 1$ with discriminant $D = a^2 - 4b$. There exist positive integer constants C_1 and C_2, which are dependent on a and b if $D < 0$ and are independent of a and b if $D > 0$, such that if $n \geq C_1$ and $m \geq C_2$, then $|u_n(a,b)| > 2n + 1$ and $|v_m(a,b)| > 2m + 1$. Moreover, if $D > 0$, then the following hold, where C_1' and C_2' are the least such positive integer constants C_1 and C_2, respectively.*

(i) $C_1' = 2$ *or* 3 *except for the following cases:*
  (a) $(a,b) = (\pm 1, -1)$, $C_1' = 8$;
  (b) $(a,b) = (\pm 1, -2)$, $C_1' = 6$;
  (c) $(a,b) = (\pm 1, -3)$ *or* $(\pm 1, -4)$, $C_1' = 5$;
  (d) $(a,b) = (\pm 1, -5)$, $(\pm 1, -6)$, $(\pm 2, -1)$, $(\pm 2, -2)$, $(\pm 2, -3)$, *or* $(\pm 3, 2)$, $C_1' = 4$.

(ii) $C_2' = 1$ *or* 2 *except for the following cases:*
  (a) $(a,b) = (\pm 1, -1)$, $C_2' = 6$;
  (b) $(a,b) = (\pm 1, -2)$, $C_2' = 4$;
  (c) $(a,b) = (\pm 3, 2)$, $C_2' = 3$.

Remark 3.14. Based on the examination of many sequences $u(a,b)$ and $v(a,b)$, we conjecture that if $u(a,b)$ and $v(a,b)$ are nondegenerate sequences for which $\gcd(a,b) = 1$, and $D < 0$, then C_1 and C_2 are absolute constants independent of a and b, and that $C_1' \leq 14$ and $C_2' \leq 10$. Moreover, we conjecture that $C_1' = 14$ if and only if $(a,b) = (\pm 1, 2)$, and $C_2' = 10$ if and only if $(a,b) = (\pm 1, 2)$. In particular, we note that

$$u_{13}(\pm 1, 2) = -1,\ |u_{14}(\pm 1, 2)| = 91,\ u_{15}(\pm 1, 2) = -89,\ |u_{16}(\pm 1, 2)| = 93,\ \text{and}\ u_{17}(\pm 1, 2) = 271,$$

whereas

$$|v_9(\pm 1, 2)| = 5,\ v_{10}(\pm 1, 2) = 57,\ |v_{11}(\pm 1, 2)| = 67,\ v_{12}(\pm 1, 2) = -47,\ \text{and}\ |v_{13}(\pm 1, 2)| = 181.$$

Theorem 3.15. *Let $u(a,b)$ be a nondegenerate Lucas sequence and let $p \geq C_1'$, where C_1' is as defined in Theorem 3.13.*

(i) *If $2p - 1$ is also a prime, $(b/(2p-1)) = 1$, and $(D/(2p-1)) = -1$, then $2p - 1 \mid u_p$ and $|u_p|$ is composite.*
(ii) *If $2p + 1$ is a prime, $(b/(2p+1)) = 1$, and $(D/(2p+1)) = 1$, then $2p + 1 \mid u_p$ and $|u_p|$ is composite.*

Proof. The assertions that $2p - 1 \mid u_p$ if (i) holds and $2p + 1 \mid u_p$ if (ii) is satisfied are proved in [18]. It then follows from Theorem 3.13 that $|u_p|$ is composite if $p \geq C_1'$. □

Remark 3.16. In the original presentation of Theorem 3.15 in [18], there was the additional condition that $p \nmid b$. However, the proof of Theorem 3.15 given in [18] shows that this constraint is not necessary. Theorem 1.1 was proved in [18] by the use of Theorem 3.15.

Example 3.17. Consider the nondegenerate Lucas sequence $u(1, -5)$ with discriminant $D = 21$. Then we can find primes satisfying each of the conditions of Theorem 3.15.

Primes satisfying the conditions of Theorem 3.15 (i): Let p be a prime such that $p \equiv 1 \pmod{30}$, $p \equiv 0$, 2, or $3 \pmod 7$, and $2p-1$ is also a prime. Then $2p-1 \equiv 1 \pmod{60}$. Hence, $2p-1$ is congruent to $1 \pmod 3$, $1 \pmod 4$, $1 \pmod 5$, and $3, 5$, or $6 \pmod 7$. Thus, by the law of quadratic reciprocity,

$$\Big(\frac{b}{2p-1}\Big) = \Big(\frac{-5}{2p-1}\Big) = \Big(\frac{-1}{2p-1}\Big)\Big(\frac{5}{2p-1}\Big) = 1 \cdot \Big(\frac{2p-1}{5}\Big) = \Big(\frac{1}{5}\Big) = 1,$$

as desired. Moreover,

$$\Big(\frac{D}{2p-1}\Big) = \Big(\frac{21}{2p-1}\Big) = \Big(\frac{3}{2p-1}\Big)\Big(\frac{7}{2p-1}\Big) = \Big(\frac{2p-1}{3}\Big)\Big(\frac{2p-1}{7}\Big) = \Big(\frac{1}{3}\Big)(-1) = -1.$$

Therefore, the conditions of Theorem 3.15 (i) hold, and $2p-1 \mid u_p$. The ordered pairs $(p, 2p-1)$ with $p < 1000$ satisfying the constraints of Theorem 3.15 (i) are

$$(31, 61), \ (331, 661), \ \text{and } (661, 1321).$$

We observe explicitly that

$$61 \mid u_{31}(1, -5) = 14415648500221 = 61 \cdot 1427 \cdot 5021 \cdot 32983.$$

Primes satisfying the conditions of Theorem 3.15 (ii): Let p be a prime such that $p \equiv 11$ or $23 \pmod{30}$, $p \equiv 1$, 2, or $6 \pmod 7$, and $2p+1$ is a prime. Then $2p+1 \equiv 23$ or $47 \pmod{60}$. Therefore, $2p+1$ is congruent to $2 \pmod 3$, $3 \pmod 4$, 2 or $3 \pmod 5$, and $3, 5$, or $6 \pmod 7$. Hence, by the law of quadratic reciprocity,

$$\Big(\frac{b}{2p+1}\Big) = \Big(\frac{-5}{2p+1}\Big) = \Big(\frac{-1}{2p+1}\Big)\Big(\frac{5}{2p+1}\Big) = (-1) \cdot \Big(\frac{2p+1}{5}\Big) = (-1)(-1) = 1$$

as desired. Furthermore,

$$\Big(\frac{D}{2p+1}\Big) = \Big(\frac{21}{2p+1}\Big) = \Big(\frac{3}{2p+1}\Big)\Big(\frac{7}{2p+1}\Big) = -\Big(\frac{2p+1}{3}\Big)\Big[-\Big(\frac{2p+1}{7}\Big)\Big] = 1 \cdot 1 = 1,$$

as desired. Therefore, the conditions of Theorem 3.15 (ii) are satisfied, and $2p+1 \mid u_p$. The ordered pairs $(p, 2p+1)$ with $p < 1000$ satisfying the constraints of Theorem 3.15 (ii) are:

$(23, 47)$, $(41, 83)$, $(83, 167)$, $(113, 227)$, $(191, 383)$, $(233, 467)$, $(251, 503)$, $(281, 563)$,
$(293, 587)$, $(443, 887)$, $(491, 983)$, $(653, 1307)$, $(743, 1487)$, and $(953, 1907)$.

In particular, we see that

$$47 \mid u_{23}(1, -5) = 3912125981 = 47 \cdot 827 \cdot 100649.$$

Finally, we find by inspection that $u_n(1, -5)$ is prime for $0 \le n \le 31$ only in the following cases:

$$u_4 = 11, \quad u_5 = 41, \quad u_{17} = 8275601.$$

Theorem 3.18 shows that the necessary conditions given in Theorem 3.7 (ii) for $u_9(a, b)$ to be prime are not sufficient.

Theorem 3.18. *Let $u(a, b) = u(a, a^2 \pm 1)$ be a nondegenerate Lucas sequence for which $|a| \ge 2$. Then $u_3(a, b) = \pm 1$.*

(i) *Suppose that $b = a^2 - 1$. If $a \equiv \pm 3$ or $\pm 4 \pmod{17}$, then $17 \mid |u_9(a, a^2 - 1)|$ and $|u_9(a, a^2 - 1)|$ is composite. If $a \equiv \pm 5 \pmod{19}$, then $19 \mid u_9(a, a^2 - 1)$ and $|u_9(a, a^2 - 1)|$ is again composite.*

(ii) *Suppose that $b = a^2 + 1$. If $a \equiv \pm 1$ or $\pm 5 \pmod{17}$, then $17 \mid u_9(a, a^2 + 1)$ and $|u_9(a, a^2 + 1)|$ is composite. If $a \equiv \pm 4$ or $\pm 5 \pmod{19}$, then $19 \mid u_9(a, a^2 + 1)$ and $|u_9(a, a^2 + 1)|$ is composite.*

(iii) *Suppose that* $b = a^2 - 1$. *If*

$$a \equiv 14,\ 71,\ 81,\ 157,\ 166,\ 242,\ 252,\ \textit{or}\ 309 \pmod{323},$$

then $17 \cdot 19 = 323 \mid u_9(a, a^2 - 1)$ *and* $|u_9(a, a^2 - 1)|$ *is composite.*

(iv) *Suppose that* $b = a^2 + 1$. *If*

$$a \equiv 5,\ 33,\ 52,\ 80,\ 90,\ 118,\ 137,\ 148,\ 175,\ 186,$$

$$205,\ 233,\ 243,\ 271,\ 290,\ \textit{or}\ 318 \pmod{323},$$

then $323 \mid u_9(a, a^2 + 1)$ *and* $|u_9(a, a^2 + 1)|$ *is composite.*

Proof. We see from (3.1) in Remark 3.8 that

$$|u_9(a, a^2 \pm 1)| \geq 3(2^2 - 1)((2^2 - 1)^2 - 1) + 1 = 73$$

for $|a| \geq 2$. Thus, $|u_9(a, a^2 \pm 1)|$ is composite if 17 or 19 divides $u_9(a, a^2 \pm 1)$. We now prove parts (i)–(iv) together.

First suppose that $b = a^2 - 1$. Then by Lemma 2.7 (ix), if

$$\left(\frac{b}{17}\right) = \left(\frac{a^2 - 1}{17}\right) = 1 \quad \text{and} \quad \left(\frac{D}{17}\right) = \left(\frac{-3a^2 + 4}{17}\right) = -1, \tag{3.2}$$

then

$$17 \mid u_{(17-(D/17))/2} = u_9(a, a^2 - 1).$$

By inspection, we find that (3.2) holds if $a \equiv \pm 3$ or $\pm 4 \pmod{17}$.

We also see by Lemma 2.7 (ix) that if

$$\left(\frac{b}{19}\right) = \left(\frac{a^2 - 1}{19}\right) = 1 \quad \text{and} \quad \left(\frac{D}{19}\right) = \left(\frac{-3a^2 + 4}{19}\right) = 1, \tag{3.3}$$

then

$$19 \mid u_{(19-(D/19))/2} = u_9(a, a^2 - 1).$$

By examination, we observe that (3.3) is satisfied when $a \equiv \pm 5 \pmod{19}$. Thus, part (i) is proved.

It now follows from part (i) and the Chinese Remainder Theorem that part (iii) holds. For example, if

$$a \equiv 3 \pmod{17} \quad \text{and} \quad a \equiv 5 \pmod{19}, \tag{3.4}$$

then both (3.2) and (3.3) hold. It then follows that

$$17 \cdot 19 = 323 \mid u_9(a, a^2 - 1).$$

We see by the Chinese Remainder Theorem that (3.4) holds if $a \equiv 309 \pmod{323}$. The other 7 cases are handled similarly using the Chinese Remainder Theorem.

Now suppose that $b = a^2 + 1$. It follows from Lemma 2.7 (ix) that if

$$\left(\frac{b}{17}\right) = \left(\frac{a^2 + 1}{17}\right) = 1 \quad \text{and} \quad \left(\frac{D}{17}\right) = \left(\frac{-3a^2 - 4}{17}\right) = -1, \tag{3.5}$$

then

$$17 \mid u_{(17-(D/17))/2} = u_9(a, a^2 + 1).$$

By inspection, we see that (3.5) hold if $a \equiv \pm 1$ or $\pm 5 \pmod{17}$.

We further observe by Lemma 2.7 (ix) that if

$$\left(\frac{b}{19}\right) = \left(\frac{a^2 + 1}{19}\right) = 1 \quad \text{and} \quad \left(\frac{D}{19}\right) = \left(\frac{-3a^2 - 4}{19}\right) = 1, \tag{3.6}$$

then

$$19 \mid u_{(19-(D/19))/2} = u_9(a, a^2+1).$$

By inspection, we see that (3.6) is satisfied when $a \equiv \pm 4$ or $\pm 5 \pmod{19}$. Therefore, part (ii) holds.

Finally, it follows from part (ii) and the Chinese Remainder Theorem that part (iv) holds. □

Example 3.19. In (3.7) and (3.8), we find terms $u_9(a, a^2 \pm 1)$ such that u_9 is divisible by 17, 19, and a large prime having 12 digits. In (3.9) and (3.10), we present terms $u_9(a, a^2 \pm 1)$ that are divisible by 5 primes including 17 and 19;

$$u_9(157, 24648) = 44922747483433 = 17 \cdot 19 \cdot 139079713571, \tag{3.7}$$

$$u_9(175, 30626) = 86177142371249 = 17 \cdot 19 \cdot 266802298363, \tag{3.8}$$

$$u_9(137, 18770) = 19838739342689 = 17 \cdot 19 \cdot 37 \cdot 20123 \cdot 82493, \tag{3.9}$$

$$u_9(186, 34597) = 124232887378727 = 17 \cdot 19 \cdot 541 \cdot 2699 \cdot 263411. \tag{3.10}$$

Before presenting Theorem 3.20 we need to discuss primes of the form $2^k + 1$. It is easy to see that $2^k + 1$ can be prime only if $k = 2^m$ for some $m \geq 0$. Such primes are called *Fermat primes* and will be denoted by $\overline{F}_m = 2^{2^m} + 1$. Their properties are given in [10]. The only known Fermat primes $\overline{F}_m$ are those for which $m \in \{0, 1, 2, 3, 4\}$. We have the following consecutive Fermat numbers (which may or may not be prime):

$$\overline{F}_{m+1} = 2^{2^{m+1}} + 1 = \left(2^{2^m}\right)^2 + 1 = (\overline{F}_m - 1)^2 + 1. \tag{3.11}$$

Theorem 3.20. *Let $v(a, b)$ be a nondegenerate companion Lucas sequence with* $\gcd(a, b) = 1$. *Let C_2' be defined as in Theorem 3.13.*

(i) *Suppose that $a = \pm 1$. If $p \geq C_2'$ and $2p - 1$ is a prime such that*

$$\left(\frac{b}{2p-1}\right) = \left(\frac{D}{2p-1}\right) = -1,$$

then $2p - 1 \mid v_p$ and $|v_p|$ is composite.

(ii) *Suppose that $a = \pm 1$. If $p \geq C_2'$ and $2p + 1$ is a prime such that*

$$\left(\frac{b}{2p+1}\right) = -1 \quad \text{and} \quad \left(\frac{D}{2p+1}\right) = 1,$$

then $2p + 1 \mid v_p$ and $|v_p|$ is composite.

(iii) *Suppose that $2 \nmid a$. Let p be a prime such that $2^{p-1} \geq C_2'$. Let $M_p = 2^p - 1$ be a Mersenne prime such that*

$$\left(\frac{b}{M_p}\right) = \left(\frac{D}{M_p}\right) = -1.$$

Then $M_p \mid v_{2^{p-1}}$ and $|v_{2^{p-1}}|$ is composite.

(iv) *Suppose that $2 \nmid a$. Let m be a nonnegative integer such that $\overline{F}_m$ is a Fermat prime such that*

$$\left(\frac{b}{\overline{F}_m}\right) = -1 \quad \text{and} \quad \left(\frac{D}{\overline{F}_m}\right) = 1.$$

Then $\overline{F}_m \mid v_{2^r}$, where $r = 2^m - 1$, and v_{2^r} is composite.

(v) *Suppose that* $b = (a^2 \pm 1)/2$ *and thus* $v_2 = \pm 1$. *Let* p *be a prime such that* $2p \geq C_2'$. *If* $4p - 1$ *is a prime such that*

$$\left(\frac{b}{4p-1}\right) = \left(\frac{D}{4p-1}\right) = -1,$$

then $4p - 1 \mid v_{2p}$ *and* $|v_{2p}|$ *is composite.*

(vi) *Suppose that* $b = (a^2 \pm 1)/2$ *and thus* $v_2 \pm 1$. *Let* p *be a prime such that* $2p \geq C_2'$. *If* $4p + 1$ *is a prime such that*

$$\left(\frac{b}{4p+1}\right) = -1 \quad \text{and} \quad \left(\frac{D}{4p+1}\right) = 1,$$

then $4p + 1 \mid v_{2p}$ *and* $|v_{2p}|$ *is composite.*

Proof. The assertions about compositeness follow from Theorem 3.13. By Lemma 2.7 (x) we have

(i) $2p - 1 \mid v_{(2p-1+1)/2} = v_p$,
(ii) $2p + 1 \mid v_{(2p+1-1)/2} = v_p$,
(iii) $2^p - 1 \mid v_{(2^p-1+1)/2} = v_{2^{p-1}}$,
(iv) $\overline{F}_m \mid v_{(\overline{F}_m-1)/2} = v_{2^r}$, where $r = 2^m - 1$,
(v) $4p - 1 \mid v_{(4p-1+1)/2} = v_{2p}$,
(vi) $4p + 1 \mid v_{(4p+1-1)/2} = v_{2p}$.

□

Remark 3.21. We note that in Theorem 3.20, we do not have a criterion involving the Legendre symbol for determining primes of the form $8p \pm 1$ such that

$$8p \pm 1 \mid v_{4p}(\pm 1, 2).$$

The reason is that if we use Lemma 2.7 (x) as we did in the proofs of parts (i)–(vi) of Theorem 3.20, we must have that

$$\left(\frac{b}{8p \pm 1}\right) = \left(\frac{2}{8p \pm 1}\right) = -1.$$

However, by the law of quadratic reciprocity,

$$\left(\frac{2}{8p \pm 1}\right) = 1.$$

Remark 3.22. Theorems 1.1, 1.3, 1.5, 3.15, and 3.20 discuss primes p such that $2p \pm 1$ is also a prime. Primes p such that $2p+1$ is prime are called *Sophie Germain primes of the first kind*, while primes p for which $2p - 1$ is prime are called *Sophie Germain primes of the second kind*. By inspection, we see that the first few Sophie Germain primes of the first kind are

$$2,\ 3,\ 5,\ 11,\ 23,\ 29,\ 41,\ 53,\ 83,\ 89,\ 113,\ 131, \ldots,$$

whereas the first few Sophie Germain primes of the second kind are

$$2,\ 3,\ 7,\ 19,\ 31,\ 37,\ 79,\ 97,\ 139,\ 157,\ 199,\ 211, \ldots.$$

According to [5], the largest known Sophie Germain prime of the first kind is

$$18543637900515 \cdot 2^{666667} - 1$$

with 200701 digits, while we find from [3] that the largest known Sophie Germain prime of the second kind is

$$648309 \cdot 2^{148310} + 1$$

with 44652 digits.

The following example shows that there exist nondegenerate companion Lucas sequence $v(a, b)$ for which each of the conditions (i)–(iv) of Theorem 3.20 can be satisfied for certain primes.

Example 3.23. Consider the nondegenerate companion Lucas sequence $v(1, -5)$ with discriminant $D = 21$. Then we can find primes satisfying each of the conditions (i)–(iv) of Theorem 3.20.

Primes satisfying the conditions of Theorem 3.20 (i): Let p be a prime such that $p \equiv 7$ or $19 \pmod{30}$, $p \equiv 0, 2,$ or $3 \pmod 7$, and $2p-1$ is also a prime. Then $2p - 1 \equiv 13$ or $37 \pmod{60}$. Hence, $2p - 1$ is congruent to $1 \pmod 3$, $1 \pmod 4$, 2 or $3 \pmod 5$, and $3, 5,$ or $6 \pmod 7$. Thus, by the law of quadratic reciprocity,

$$\Big(\frac{b}{2p-1}\Big) = \Big(\frac{-5}{2p-1}\Big) = \Big(\frac{-1}{2p-1}\Big)\Big(\frac{5}{2p-1}\Big) = 1 \cdot \Big(\frac{2p-1}{5}\Big) = -1,$$

as desired. Moreover,

$$\Big(\frac{D}{2p-1}\Big) = \Big(\frac{21}{2p-1}\Big) = \Big(\frac{3}{2p-1}\Big)\Big(\frac{7}{2p-1}\Big) = \Big(\frac{2p-1}{3}\Big)\Big(\frac{2p-1}{7}\Big) = \Big(\frac{1}{3}\Big)\Big(\frac{2p-1}{7}\Big) = -1.$$

Thus, the conditions of Theorem 3.20 (i) are fulfilled, and $2p - 1 \mid v_p$. The ordered pairs $(p, 2p - 1)$ with $p < 1000$ satisfying the constraints of Theorem 3.20 (i) are:

$$(7, 13),\ (37, 73),\ (79, 157),\ (157, 313),\ (199, 397),\ (367, 733),\ (499, 997),$$

$$(577, 1153),\ (619, 1237),\ (829, 1657),\ (877, 1753), \quad \text{and} \quad (997, 1993).$$

We observe explicitly that $13 \mid v_7(1, -5) = 1261 = 13 \cdot 97$.

Primes satisfying the conditions of Theorem 3.20 (ii): Let p be a prime such that $p \equiv 29 \pmod{30}$, $p \equiv 1, 2,$ or $6 \pmod 7$, and $2p + 1$ is also a prime. Then $2p + 1 \equiv 59 \pmod{60}$. Therefore, $2p + 1$ is congruent to $2 \pmod 3$, $3 \pmod 4$, $4 \pmod 5$, and $3, 5,$ or $6 \pmod 7$. By the law of quadratic reciprocity, we have

$$\Big(\frac{b}{2p+1}\Big) = \Big(\frac{-5}{2p+1}\Big) = \Big(\frac{-1}{2p+1}\Big)\Big(\frac{5}{2p+1}\Big) = (-1) \cdot \Big(\frac{2p+1}{5}\Big) = -1,$$

as required. Furthermore,

$$\Big(\frac{D}{2p+1}\Big) = \Big(\frac{21}{2p+1}\Big) = \Big(\frac{3}{2p+1}\Big)\Big(\frac{7}{2p+1}\Big) = \Big[-\Big(\frac{2p+1}{3}\Big)\Big]\Big[-\Big(\frac{2p+1}{7}\Big)\Big] =$$

$$\Big[-\Big(\frac{2}{3}\Big)\Big]\Big[-\Big(\frac{2p+1}{7}\Big)\Big] = 1 \cdot 1 = 1,$$

as desired. Therefore, the conditions of Theorem 3.20 (ii) hold, and $2p + 1 \mid v_p$. The ordered pairs $(p, 2p + 1)$ with $p < 1000$ satisfying the constraints of Theorem 3.20 (ii) are

$$(29, 59),\ (239, 479),\ (359, 719),\ (419, 839),\ \text{and } (659, 1319).$$

In particular, we see that

$$59 \mid v_{29}(1, -5) = 8478772712071 = 59 \cdot 347 \cdot 8293 \cdot 49939.$$

Primes satisfying the conditions of Theorem 3.20 (iii): Suppose that $p \equiv 5 \pmod{12}$ and $M_p = 2^p - 1$ is a Mersenne prime. Then $M_p \equiv 3 \pmod 4$. We claim that

$$\Big(\frac{b}{M_p}\Big) = \Big(\frac{-5}{M_p}\Big) = \Big(\frac{D}{M_p}\Big) = \Big(\frac{21}{M_p}\Big) = -1.$$

Let $p = 12k + 5$. By Fermat's Little Theorem and the law of quadratic reciprocity,

$$\Big(\frac{-5}{M_p}\Big) = \Big(\frac{-1}{2^p-1}\Big)\Big(\frac{5}{2^p-1}\Big) = (-1)\Big(\frac{2^p-1}{5}\Big) = -\Big(\frac{2^{12k}\cdot 2^5 - 1}{5}\Big) = -\Big(\frac{1\cdot 32 - 1}{5}\Big) = -1.$$

Moreover,

$$\begin{aligned}\Big(\frac{21}{M_p}\Big) &= \Big(\frac{3}{2^p-1}\Big)\Big(\frac{7}{2^p-1}\Big) = \Big[-\Big(\frac{2^p-1}{3}\Big)\Big]\Big[-\Big(\frac{2^p-1}{7}\Big)\Big] \\ &= (-1)\Big(\frac{1\cdot 32-1}{3}\Big)(-1)\Big(\frac{1\cdot 32-1}{7}\Big) = (-1)\Big(\frac{1}{3}\Big)(-1)\Big(\frac{3}{7}\Big) = -1,\end{aligned}$$

as desired. Hence, $2^p - 1 \mid v_{2^{p-1}}$ in these cases.

There are 18 known Mersenne primes M_p with $p \equiv 5 \pmod{12}$ (see [2]), namely those primes p for which

$$p = 5,\ 17,\ 89,\ 521,\ 4253,\ 9689,\ 9941,\ 11213,\ 19937,\ 21701,\ 859433,$$
$$1398269,\ 2976221,\ 3021377,\ 6972593,\ 32582657,\ 43112609,\ \text{and } 57885161.$$

In particular, we observe that

$$M_5 = 2^5 - 1 = 31 \mid v_{2^4} = v_{16} = 13590431 = 31 \cdot 438401.$$

Primes satisfying the conditions of Theorem 3.20 (iv): Let $\overline{F}_m = 2^{2^m} + 1$ be a Fermat prime with $m \geq 2$. We will show that

$$\Big(\frac{b}{\overline{F}_m}\Big) = \Big(\frac{-5}{\overline{F}_m}\Big) = -1.$$

and

$$\Big(\frac{D}{\overline{F}_m}\Big) = \Big(\frac{21}{\overline{F}_m}\Big) = 1.$$

By use of (3.11) and induction, we find that

$$\begin{aligned}\overline{F}_m &\equiv 2 \pmod 3 \quad \text{for } m \geq 1,\\ \overline{F}_m &\equiv 1 \pmod 4 \quad \text{for } m \geq 1,\\ \overline{F}_m &\equiv 2 \pmod 5 \quad \text{for } m \geq 2,\\ \overline{F}_m &\equiv 3 \pmod 7 \quad \text{for } m \geq 0 \text{ and } m \text{ even},\end{aligned}$$

and

$$\overline{F}_m \equiv 5 \pmod 7 \quad \text{for } m \geq 1 \text{ and } m \text{ odd}.$$

Thus, by the law of quadratic reciprocity,

$$\Big(\frac{3}{\overline{F}_m}\Big) = \Big(\frac{\overline{F}_m}{3}\Big) = \Big(\frac{5}{\overline{F}_m}\Big) = \Big(\frac{\overline{F}_m}{5}\Big) = \Big(\frac{7}{\overline{F}_m}\Big) = \Big(\frac{\overline{F}_m}{7}\Big) = -1$$

for $m \geq 2$. Hence, for $m \geq 2$,

$$\Big(\frac{-5}{\overline{F}_m}\Big) = \Big(\frac{-1}{\overline{F}_m}\Big)\Big(\frac{5}{\overline{F}_m}\Big) = 1 \cdot (-1) = -1$$

and

$$\Big(\frac{21}{\overline{F}_m}\Big) = \Big(\frac{3}{\overline{F}_m}\Big)\Big(\frac{7}{\overline{F}_m}\Big) = (-1)(-1) = 1,$$

as desired. Thus, $2^{2^m}+1 \mid v_{2^r}$, where $r = 2^m - 1$, when $\overline{F}_m$ is a prime for $m \geq 2$. Thus, by examination, we see that

$$\begin{aligned}
&\overline{F}_2 = 17 \mid v_8(1,-5) = 3791 = 17 \cdot 223,\\
&\overline{F}_3 = 257 \mid v_{128}(1,-5), \quad \text{and}\\
&\overline{F}_4 = 65537 \mid v_{2^{15}}(1,-5) = v_{32768}(1,-5).
\end{aligned}$$

Finally, we find by inspection that $v_n(1,-5)$ is prime for $0 \leq n \leq 30$ only in the following cases, for which we must have that n is equal to 0, a prime, or a power of 2:

$$v_0 = 2,\ v_2 = 11,\ v_4 = 71,\ v_5 = 151,\ v_{11} = 79531,\ v_{17} = 37883311,\ v_{23} = 17926283491.$$

Example 3.24. *Consider the nondegenerate companion Lucas sequence $v(3,5)$ with discriminant $D = -11$ and for which $v_2 = -1$. We show that we can find primes satisfying each of the conditions (v) and (vi) of Theorem 3.20.*

Primes satisfying the conditions of Theorem 3.20 (v): Let p be a prime such that $p \geq C_2'$, $p \equiv 11$ or $17 \pmod{30}$, $p \equiv 0, 2, 5, 9,$ or $10 \pmod{11}$, and $4p-1$ is also a prime. Then $4p-1 \equiv 43$ or $67 \pmod{120}$. Hence, $4p-1$ is congruent to $3 \pmod 4$, 2 or $3 \pmod 5$, and 2, 6, 7, 8, or $10 \pmod{11}$. Thus, by the law of quadratic reciprocity,

$$\begin{aligned}
\Big(\frac{b}{4p-1}\Big) &= \Big(\frac{5}{4p-1}\Big) = \Big(\frac{4p-1}{5}\Big) = -1\\
= \Big(\frac{D}{4p-1}\Big) &= \Big(\frac{-11}{4p-1}\Big) = \Big(\frac{-1}{4p-1}\Big)\Big(\frac{11}{4p-1}\Big) = (-1)\Big[-\Big(\frac{4p-1}{11}\Big)\Big] = -1,
\end{aligned}$$

as desired. Therefore, the conditions of Theorem 3.20 (v) are satisfied and $4p-1 \mid v_{2p}$. The ordered pairs $(p, 4p-1)$ with $p < 1000$ satisfying the constraints of Theorem 3.20 (v) are:

$$(11,43),\ (71,283),\ (131,523),\ (137,547),\ (197,787),\ (431,1723),\ (467,1867),$$
$$(797,3187),\ (827,3307),\ (911,3643),\ \text{and}\ (977,3907).$$

We observe explicitly that

$$43 \mid v_{22}(3,5) = 87113399 = 43 \cdot 307 \cdot 6599.$$

Primes satisfying the conditions of Theorem 3.20 (vi): Let p be a prime such that $p \geq C_2'$, $p \equiv 13$ or $19 \pmod{30}$, $p \equiv 0, 1, 2, 6,$ or $9 \pmod{11}$, and $4p+1$ is a prime. Then $4p+1 \equiv 53$ or $77 \pmod{120}$. Thus, $4p+1$ is congruent to $1 \pmod 4$, 2 or $3 \pmod 5$, and $1, 3, 4, 5,$ or $9 \pmod{11}$. By the law of quadratic reciprocity we then have that

$$\Big(\frac{b}{4p+1}\Big) = \Big(\frac{5}{4p+1}\Big) = \Big(\frac{4p+1}{5}\Big) = -1$$

and

$$\Big(\frac{D}{4p+1}\Big) = \Big(\frac{-11}{4p+1}\Big) = \Big(\frac{-1}{4p+1}\Big)\Big(\frac{11}{4p+1}\Big) = 1 \cdot \Big(\frac{4p+1}{11}\Big) = 1,$$

as desired. Hence, the conditions are satisfied and $4p+1 \mid v_{2p}$. The ordered pairs $(p, 4p+1)$ with $p < 1000$ and satisfying the constraints of Theorem 3.20 (vi) are

$$(13,53),\ (79,317),\ (163,653),\ (193,773),\ (199,797),\ (409,1637),$$

$$(673, 2693),\ (739, 2957),\ (853, 3413),\ \text{and } (919, 3677).$$

In particular,

$$53 \mid v_{26}(3, 5) = -2353852801 = -53 \cdot 157 \cdot 282881.$$

The following proofs show that we can consider Theorems 1.3 and 1.5 to be corollaries of Theorem 3.20.

Proof of Theorem 1.3. We note that for $\{L_m\} = v(1, -1)$, we have that $b = -1$ and $D = 5$. It follows from Theorem 3.13 (ii) that $L_n > 2n + 1$ for $n \geq 6$.

(i) Suppose that $p \equiv 29 \pmod{30}$ and $2p+1$ is also a prime. Then $2p+1 \equiv 59 \pmod{60}$. Thus, $2p + 1 \equiv 3 \pmod 4$ and $2p + 1 \equiv 4 \pmod 5$. We then see that

$$\Big(\frac{b}{2p+1}\Big) = \Big(\frac{-1}{2p+1}\Big) = -1$$

and

$$\Big(\frac{D}{2p+1}\Big) = \Big(\frac{5}{2p+1}\Big) = \Big(\frac{2p+1}{5}\Big) = \Big(\frac{4}{5}\Big) = 1.$$

It now follows from Theorem 3.20 (ii) that $2p+1 \mid L_p$ which implies that $L_p > 2p+1$, since $p \geq 29$.

(ii) Suppose that $p \equiv 3 \pmod 4$ and $2^p - 1$ is a Mersenne prime. Let $p = 4k + 3$. By Fermat's Little Theorem,

$$2^p - 1 = 2^{4k}2^3 - 1 \equiv 1 \cdot 2^3 - 1 \equiv 2 \pmod 5.$$

Clearly, $2^p - 1 \equiv 3 \pmod 4$. It now follows by the law of quadratic reciprocity that

$$\Big(\frac{b}{2^p-1}\Big) = \Big(\frac{-1}{2^p-1}\Big) = -1, \quad \Big(\frac{D}{2^p-1}\Big) = \Big(\frac{5}{2^p-1}\Big) = \Big(\frac{2^p-1}{5}\Big) = \Big(\frac{2}{5}\Big) = -1.$$

We now see from Theorem 3.20 (iii) that $2^p - 1 \mid L_{2^{p-1}}$, and it follows from Theorem 3.13 (ii) that $L_{2^{p-1}} > 2^{p-1}$, since $2^{p-1} > 6$ when $p > 3$. □

Proof of Theorem 1.5. Let $p > 3$, $p \equiv 3 \pmod 4$, and $2p + 1$ equal to a prime. Consider the companion Lucas sequence $v(1, -2)$ with characteristic roots $\alpha = 2$, $\beta = -1$, and discriminant $D = (\alpha - \beta)^2 = 3^2 = 9$. By (2.5), $v_n = 2^n + (-1)^n$. Hence, $v_n = 2^n - 1$ when n is odd. It follows that

$$v_p = M_p = 2^p - 1.$$

Since $p \equiv 3 \pmod 4$, we find that $2p+1 \equiv 7 \pmod 8$. We now observe by the law of quadratic reciprocity that

$$\Big(\frac{b}{2p+1}\Big) = \Big(\frac{-2}{2p+1}\Big) = \Big(\frac{-1}{2p+1}\Big)\Big(\frac{2}{2p+1}\Big) = -1 \cdot 1 = -1$$

and

$$\Big(\frac{D}{2p+1}\Big) = \Big(\frac{9}{2p+1}\Big) = 1.$$

It now follows from Theorem 3.20 (ii), Theorem 3.13 (ii), and the fact that $p > 6$ that

$$2p + 1 \mid v_p = M_p$$

and M_p is composite. □

We now present some known results for which $|u_p(a, b)|$ is known to be composite in some special cases, where $u(a, b)$ is nondegenerate and $\gcd(a, b) = 1$.

Theorem 3.25. *Let $u(a,b)$ be a nondegenerate Lucas sequence with discriminant D for which* $\gcd(a,b)=1$. *Let $p \geq 5$ be a prime such that $p \mid D$. Then $p \mid u_p$. Moreover, $|u_p|$ is composite except in the following cases for which $|u_p(a,b)| = p$:*

(i) $p=5$; $(a,b,D) = (\pm 1,-1,5),\ (\pm 1,4,-15),\ (\pm 2,11,-40)$.

(ii) $p=7$; $(a,b,D) = (\pm 1,2,-7)$.

Proof. By Lemma 2.7 (viii), $p \mid u_p$. It now follows from Table 1 in [1] that $|u_p| > p$ except if condition (i) or condition (ii) is satisfied. □

Theorem 3.26. *Let $u(a,b)$ be a nondegenerate Lucas sequence for which* $\gcd(a,b)=1$ *and $b = M^2$ for some positive integer M. If $D > 0$, then $|u_p(a,b)|$ is composite for $p \geq 5$. If $D < 0$, then there exists a positive integer C_3, dependent on a and b, such that if $p \geq C_3$, then $|u_p(a,b)|$ is composite.*

Proof. When $D > 0$, it was shown in [15] and [16] that $u_n(a,b)$ has two primitive divisors for $n \geq 5$ an odd integer. When $D < 0$, it was proven in [16] that there exists a positive integer C_3 such that if n is odd and greater than or equal to C_3, then $|u_n(a,b)|$ has two primitive prime divisors. The result now follows. □

Remark 3.27. Both the papers [15] and [16] showed that if $D > 0$ and b is a square, then according to their definition of a primitive prime divisor, $u_n(a,b)$ has two primitive prime divisors for $n \geq 5$ except for the terms $u_5(\pm 3,1) = 55$. However, by our definition of a primitive prime divisor, $u_5(\pm 3,1)$ has the two primitive prime divisors 5 and 11.

Before presenting our next result concerning sequences $u(a,b)$ for which $|u_p|$ is known to be composite for all but at most five primes p, we need the following lemma.

Lemma 3.28. *Let $u(a_1,b_1)$ and $v(a_1,b_1)$ be nondegenerate sequences with characteristic roots α, β and discriminant D, where* $\gcd(a_1,b_1)=1$. *Let $u(a,b)$ and $v(a,b)$ be sequences with characteristic roots α^k and β^k, where $k \geq 2$ is an integer. Then $a = v_k(a_1,b_1)$ and $b = b^k$. Moreover, $u(a,b)$ and $v(a,b)$ are nondegenerate sequences for which* $\gcd(a,b)=1$. *Further,*

$$u_n(a,b) = \frac{u_{kn}(a_1,b_1)}{u_k(a_1,b_1)} \quad \text{and} \quad v_n(a,b) = v_{kn}(a_1,b_1) \tag{3.12}$$

for $n \geq 0$.

Proof. Clearly, $u(a,b)$ and $v(a,b)$ are nondegenerate, since $u(a_1,b_1)$ and $v(a_1,b_1)$ are. We note that

$$u_n(a,b) = \frac{\alpha^{kn}-\beta^{kn}}{\alpha^k-\beta^k} = \frac{u_{kn}(a_1,b_1)}{u_k(a_1,b_1)} \quad \text{and} \quad v_n(a,b) = \alpha^{kn}+\beta^{kn} = v_{kn}(a_1,b_1).$$

Then

$$a = \alpha^k+\beta^k = v_k(a_1,b_1) \quad \text{and} \quad b = (\alpha\beta)^k = b^k.$$

It now follows from Lemma 2.7 (xiii) that $\gcd(a,b)=1$. □

Theorem 3.29. *Suppose that $v(a_1,b_1)$ is a nondegenerate companion Lucas sequence for which* $\gcd(a_1,b_1)=1$. *Let $k \geq 2$ and let $a = \pm v_k(a_1,b_1) = 1$ and $b = b_1^k$. Then $u(a,b)$ is a nondegenerate Lucas sequence for which* $\gcd(a,b)=1$. *Let $p \geq 5$ denote an arbitrary prime. Then $|u_p(a,b)|$ has at least two distinct primitive prime divisors and thus is composite if and only if one of the following three conditions is satisfied:*

(i) *k has at least two distinct prime divisors;*

(ii) *$k = q^i$, where $i \geq 2$ and $p \neq q$;*
(iii) *$k = q$, $p \neq q$, and $u_p(a_1, b_1) \neq \pm 1$, which occurs if and only if*

$$(p, a_1, b_1) \neq (5, \pm 1, 2),\ (5, \pm 1, 3),\ (5, \pm 12, 55),\ (5, \pm 12, 377),\ (7, \pm 1, 5),\ \text{or}\ (13, \pm 1, 2).$$

This follows from Lemmas 2.9 and 3.28 in this paper and from the proof of Theorem 3.5 in [12].

Theorem 3.30 shows that the necessary condition for $|u_n(a, b)|$ to be prime given in Theorem 3.7 (i) fails spectacularly as a necessary and sufficient test for primality in the following sense. Given any arbitrary large integer C, we can find a nondegenerate sequence $u(a, b)$ for which $u_p(a, b)$ has at least C distinct primitive prime divisors for all but finitely many primes p.

Theorem 3.30. *Let C be a positive integer. Let $v(a_1, b_1)$ be a nondegenerate companion Lucas sequence for which $\gcd(a_1, b_1) = 1$. Let $k \geq 2$ be an integer for which $\tau(k) \geq C+3$, where $\tau(k)$ denotes the number of positive divisors of k. Let $a = \pm v_k(a_1, b_1)$ and $b = b_1^k$. Then $u(a, b)$ is a nondegenerate Lucas sequence for which $\gcd(a, b) = 1$. Moreover, if $p \geq 5$ is any prime not dividing k, then $u_p(a, b)$ has at least C distinct primitive prime divisors.*

Proof. By Lemma 3.28, $u(a, b)$ is nondegenerate and $\gcd(a, b) = 1$. By Theorem 2.5 (ii) and Table 1 of Theorem 2.5, we see that there exist at least C positive divisors d_i of k, $i \leq i \leq C$, such that $u_{pd_i}(a_1, b_1)$ has a primitive prime divisor p_i, where $p \geq 5$ and $p \nmid k$. Let $e_i = \gcd(pd_i, k)$. Then $e_i < pd_i$, since $pd_i \nmid k$.

Suppose that $p_i \mid u_k(a_1, b_1)$. Then by Theorem 2.8 (i), $p_i \mid u_{e_i}(a_1, b_1)$, which contradicts the fact that p_i is a primitive divisor of $u_{pd_i}(a_1, b_1)$. Thus, $p_i \nmid u_k(a_1, b_1)$ for $i = 1, 2, \ldots, C$. Noting that $d_i \mid k$, we see by Lemma 2.7 (i) that

$$p_i \mid u_p(a, b) = \frac{u_{pk}(a_1, b_1)}{u_k(a_1, b_1)}.$$

By the proof of Theorem 3.7, any prime divisor of $u_p(a, b)$ is primitive. The result now follows. □

Remark 3.31. As contrasted to the situation concerning the Lucas sequence

$$\{u_n(v_k(a, b), b^k)\}_{n=0}^{\infty} = \left\{ \frac{u_{kn}(a, b)}{u_k(a, b)} \right\}_{n=0}^{\infty},$$

which was dealt with in Lemma 3.28 and Theorems 3.29 and 3.30, we can treat the companion Lucas sequences $\{v_n(v_k(a, b), b^k)\}_{n=0}^{\infty}$ by only considering results involving the general companion Lucas sequence $\{v_n(a, b)\}_{n=0}^{\infty}$. The reason is that

$$\{v_n(v_k(a, b), b^k)\}_{n=0}^{\infty} = \{v_{kn}(a, b)\}_{n=0}^{\infty}.$$

4. Auxiliary Results

We will need the following results for the proofs of Theorems 3.9 and 3.13.

Lemma 4.1. *Consider the nondegenerate sequences $u(a, b)$ and $v(a, b)$, where $\gcd(a, b) = 1$. Suppose that $v_n(a, b)$ has no primitive prime divisor. Then $u_{2n}(a, b)$ has no primitive prime divisor.*

Proof. Let p be a prime divisor of $u_{2n}(a, b)$. Since $u_{2n}(a, b) = u_n(a, b)v_n(a, b)$ by Lemma 2.7 (v), we see that $p \mid u_n$ or $p \mid v_n$. If $p \mid u_n$, then p is not a primitive divisor of u_{2n} by definition. If $p \mid v_n$, then $p \mid v_m$ for some m such that $1 \leq m < n$, since v_n has no primitive prime divisor by hypothesis. Then $p \mid u_{2m} = u_m v_m$. Since $2m < 2n$, we see that p is not a primitive divisor of u_{2n} in this case also. □

Lemma 4.2. *Let $u(a,b)$ and $v(a,b)$ be nondegenerate sequences for which $D > 0$. Then $|u_n|$ is increasing for $n \geq 2$ and $|v_n|$ is increasing for $n \geq 1$. Further, if $a > 0$ then $u_n > 0$ for $n \geq 1$ and $v_n > 0$ for $n \geq 0$. Moreover, if $b \geq 1$, then $|a| \geq 3$, $|u_{n+1}| > |au_n/2|$, and $|v_{n+1}| > |av_n/2|$ for $n \geq 1$.*

This follows from the proof of Lemma 3 in [8].

Theorem 4.3. *Let $u(a,b)$ and $v(a,b)$ be nondegenerate sequences with characteristic roots α and β, where $|\alpha| \geq |\beta|$. Then $|\alpha| > 1$ and there exist computable positive constants C_3, C_4, C_5, and C_6, dependent on a and b, such that if $n \geq C_3$, then*

$$|u_n(a,b)| \geq |\alpha|^{n - C_4 \log n}, \tag{4.1}$$

while if $n \geq C_5$, then

$$|v_n(a,b)| \geq |\alpha|^{n - C_6 \log n}. \tag{4.2}$$

This follows from Lemma 5 of [17].

Theorem 4.4. *Let $u(a,b)$ and $v(a,b)$ be nondegenerate sequences. Let $w(a,b) = u(a,b)$ or $v(a,b)$. For an integer m, let $P(m)$ denote the largest prime divisor of m, where by convention, $P(-1) = P(0) = P(1) = 1$. Then there exists a computable positive constant C_7, dependent on a and b, such that if $n \geq C_7$, then*

$$P(w_n(a,b)) > n \exp(\log /(104 \log\log n)). \tag{4.3}$$

In particular,

$$\lim_{n\to\infty} \frac{P(w_n)}{n} = \infty. \tag{4.4}$$

This follows from Theorem 1.1 of [20].

5. Proofs of Theorems 3.9 and 3.13

Proof of Theorem 3.9. Suppose that $n \geq 4$ and $v_n(a,b)$ has no primitive prime divisor. Then by Lemma 4.1 and Theorem 2.5 (i) and (ii), $u_{2n}(a,b)$ has no primitive prime divisor, which can occur only if $2n \in \{8, 10, 12, 18, 30\}$. Table 1 of Theorem 2.5 lists all cases in which $u_{2n}(a,b)$ has no primitive prime divisor for $2n \in \{8, 10, 12, 18, 30\}$. By examination of these cases, we see that $v_n(a,b)$ has no primitive prime divisor if (n,a,b) is one of the ordered triplets listed in Theorem 3.9.

By inspection of the values of $v_n(a,b)$ in all these cases, we see that $|v_n(a,b)| = p$, where $n \geq 4$ and p is not a primitive divisor of $v_n(a,b)$ if and only if one of the conditions (i)–(iv) is satisfied. □

Proof of Theorem 3.13. We prove all the parts of the theorem together. Let $w(a,b) = u(a,b)$ or $v(a,b)$, where $w(a,b)$ is nondegenerate and $\gcd(a,b) = 1$. First suppose that $D < 0$. It follows from Theorem 4.3 or Theorem 4.4 that the constants C_1 and C_2 both exist.

Now suppose that $D > 0$. By Lemma 2.7 (ii) and (iii), we can assume that $a > 0$. Then by Lemma 4.2, $w_n > 0$ for $n \geq 1$ and w_n is increasing for $n \geq 2$. Suppose further that $b \leq -1$. It is evident that

$$w_{n+2} \geq w_{n+1} + w_n \tag{5.1}$$

for $n \geq 0$. We also observe from (5.1) that if $n \geq 1$, $w_n > 2n+1$, and $w_{n+1} > 2(n+1)+1 = 2n+3$, then

$$w_{n+2} \geq w_{n+1} + w_n > 2(n+2)+1 = 2n+5. \tag{5.2}$$

Next suppose that $b \geq 1$. We see that $a \geq 3$, since $D = a^2 - 4b > 0$. Then by Lemma 4.2,

$$w_{n+1} > aw_n/2 \tag{5.3}$$

for $n \geq 1$. It now follows from (5.3) that if $n \geq 1$ and $w_n > 2n+1$, then

$$w_{n+1} > 3w_n/2 > 2(n+1)+1 = 2n+3. \tag{5.4}$$

Now suppose that $w(a,b) = u(a,b)$ and $b \leq -1$. If $a = 1$, $b \leq -7$, or $a = 2$, $b \leq -4$, or $a \geq 3$, then by (2.6),

$$u_3 = a^2 - b \geq 8 > 2 \cdot 3 + 1 \tag{5.5}$$

and

$$u_4 = a(a^2 - 2b) \geq 15 > 2 \cdot 4 + 1. \tag{5.6}$$

Hence, by (5.2), we see that $C_1' = 2$ or 3 in these cases, since $u_1 = 1$.

We next consider the case in which $w(a,b) = u(a,b)$ and $b \geq 1$. Then $a \geq 3$. Since $D = a^2 - 4b > 0$, we find that if $a = 3$, then $b = 1$ or 2. Moreover, if $n \geq 1$ and either $a = 3$, $b = 1$ or $a \geq 4$, then we get (5.5). Thus, by (5.4), we observe that $C_1' = 2$ or 3 in these cases. By inspection of the remaining cases in which $a = 1$, $-6 \leq b \leq -1$, or $a = 2$, $-3 \leq b \leq -1$, or $a = 3$, $b = 2$, and the use of (5.2) and (5.4), we see that each of parts (a), (b), (c), and (d) of (i) holds.

We now suppose that $w(a,b) = v(a,b)$ and $b \leq -1$. If $a = 1$, $b \leq -3$ or $a \geq 2$, then by (2.7),

$$v_2 = a^2 - 2b \geq 6 > 2 \cdot 2 + 1$$

and

$$v_3 = a(a^2 - 3b) \geq 10 > 2 \cdot 3 + 1.$$

Thus, by (5.2), we find that $C_2' = 1$ or 2 in these cases.

We finally suppose that $w(a,b) = v(a,b)$ and $b \geq 1$. We see that $a \geq 3$. If $a = 3$, $b = 1$ or $a \geq 4$, then by (2.7),

$$v_2 = a^2 - 2b \geq 7 > 2 \cdot 2 + 1.$$

It now follows from (5.4) that $C_2' = 1$ or 2 in these cases. The only remaining cases to consider are $a = 1$, $b = -1$ or -2, or $a = 3$, $b = -2$. By examination of these cases, we see that parts (a), (b), and (c) of (ii) all hold. □

6. Acknowledgement

The authors would like to thank Walter Carlip (State Univ. of New York at Bimghamton) for extensive calculations using GAP and *Mathematica* and Cameron L. Stewart (University of Waterloo) for providing two references. This paper was supported by Projects RVO 67985840 and P101/14-020675.

References

[1] Y. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math., **539** (2001), 75–122.

[2] C. K. Caldwell, *Mersenne primes: history, theorems and lists*, `http://primes.utm.edu/mersenne/`.

[3] C. K. Caldwell, *The top twenty, Cunningham chains (2nd kind)*, `http://primes.utm.edu/top20/page.php?id=20`.

[4] C. K. Caldwell, *The top twenty, Generalized Fermat*, `http://primes.utm.edu/top20/page.php?id=12`.

[5] C. K. Caldwell, *The top twenty, Sophie Germain (p)*, `http://primes.utm.edu/top20/page.php?id=2`.

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

[7] V. Drobot, *On primes in the Fibonacci sequences*, The Fibonacci Quarterly, **38.1** (2000), 71–72.

[8] P. Hilton, J. Pedersen, and L. Somer, *On Lucasian numbers*, The Fibonacci Quarterly, **35.1** (1997), 43–47.

[9] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, John Wiley & Sons, Inc., New York, 2001.

[10] M. Křížek, F. Luca, L. Somer, *17 Lectures on Fermat Numbers: From Number Theory to Geometry*, CMS Books in Mathematics, Vol. 9, Springer-Verlag, New York, 2001.

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

[12] F. Luca and L. Somer, *Lucas sequences for which* $4 \mid \phi(|u_n|)$ *for almost all* n, The Fibonacci Quarterly, **44.3** (2006), 249–263.

[13] W. L. McDaniel, *The G.C.D. in Lucas sequences and Lehmer number sequences*, The Fibonacci Quarterly, **29.1** (1991), 24–29.

[14] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996.

[15] A. Rotkiewicz, *On Lucas numbers with two intrinsic divisors*, Bull. Acad. Polon. Sér. Math. Astr. Phys., **10** (1962), 229–232.

[16] A. Schinzel, *On primitive prime factors of Lehmer numbers I*, Acta Arith., **8** (1963), 213–223.

[17] T. N. Shorey and C. L. Stewart, *On the Diophantine equation* $ax^{2t} + bx^t y + cy^2 = d$ *and pure powers in recurrence sequences*, Math. Scand., **52** (1983), 24–36.

[18] L. Somer, *Generalization of a theorem of Drobot*, The Fibonacci Quarterly, **40.4** (2002), 435–437.

[19] L. Somer and M. Křížek, *Prime Lehmer and Lucas numbers with composite indices*, The Fibonacci Quarterly, **51.3** (2013), 194–214.

[20] C. L. Stewart, *On divisors of Lucas and Lehmer numbers*, to appear in Acta Mathematica.

[21] M. Ward, *Prime divisors of second order recurring sequences*, Duke Math. J., **21** (1954), 607–614.

[22] E. W. Weisstein, *Fibonacci prime*, `http://mathworld.wolfram.com/FibonacciPrime.html`.

[23] E. W. Weisstein, *Lucas prime*, `http://mathworld.wolfram.com/LucasPrime.html`.

MSC2010: 11B39, 11A41, 11A51

Department of Mathematics, Catholic University of America, Washington, D.C. 20064
E-mail address: somer@cua.edu

Institute of Mathematics, Academy of Sciences, Žitná 25, CZ – 115 67 Prague 1, Czech Republic
E-mail address: krizek@math.cas.cz