# LUCAS SEQUENCES CONTAINING FEW PRIMES

MARK BRODERIUS AND JOHN GREENE

Abstract. Whereas proving that a Lucas sequence contains infinitely many primes is a difficult problem, there are many Lucas sequences that contain no primes or finitely many primes. We give two families of Lucas sequences containing only finitely many primes. We conjecture that all other Lucas sequences without obvious obstructions contain infinitely many primes.

## 1. Introduction

It is well known [1, 4, 7] that for positive integers $a$ and $d$, an arithmetic sequence $a$, $a+d$, $a+2d$, ... contains infinitely many primes when $\gcd(a,d)=1$, exactly one prime when $a$ is prime and $\gcd(a,d)>1$, and no primes when $a$ is not prime and $\gcd(a,d)>1$. A similar classification can be made if one does not restrict $a$ and $d$ to the positive integers, assuming numbers such as $-7$ are viewed as primes. If one translates to recurrence relations, we could say that prime numbers in the recurrence

$$a_0 = a, \quad a_n = a_{n-1} + d \quad \text{for } n \geq 1$$

are well understood. However, even the slightest generalization, say to

$$a_0 = a, \quad a_n = ca_{n-1} + d \quad \text{for } n \geq 1$$

makes the problem intractable with current methods. For example, when $c=2$, $a=0$, $d=1$, and $a_n = 2^n - 1$, we have the Mersenne numbers. Heuristically [10], one expects infinitely many primes in this sequence, but at present there is no proof.

The nonhomogeneous recurrence above can be converted to a second order homogeneous recurrence relation, $a_n = (c+1)a_{n-1} - ca_{n-2}$. In this paper, we look at primes in more general second order homogeneous recurrence relations. Again, with one trivial exception, we are unable to prove that any such sequence contains infinitely many primes, but there are sequences that contain no primes or few primes. We attempt to categorize some of these sequences here.

Following usual conventions [7, 8], for integers $P$ and $Q$, we define the Lucas sequence $U_n = U_n(P,Q)$ by

$$U_0 = 0, \quad U_1 = 1, \quad U_n = PU_{n-1} - QU_{n-2} \text{ for } n \geq 2. \tag{1.1}$$

Associated with sequences $U_n$ are sequences $V_n$ satisfying the same recurrence, but with initial conditions $V_0 = 2$ and $V_1 = P$. If the characteristic polynomial of the recurrence, $z^2 - Pz + Q$, has zeros $x$ and $y$, then

$$\begin{cases} U_n = \frac{x^n - y^n}{x-y}, & V_n = x^n + y^n, \quad \text{if } x \neq y; \\ U_n = nx^{n-1}, & V_n = 2x^n, \quad \text{if } x = y. \end{cases} \tag{1.2}$$

When stressing $x$ and $y$, we write $U_n(x+y, xy)$, because $P = x+y$ and $Q = xy$.

Just as $a$ and $d$ must be relatively prime for arithmetic sequences to contain infinitely many primes, $P$ and $Q$ must be relatively prime for Lucas sequences to contain infinitely

many primes. This is because if $d = \gcd(P, Q)$, then $d^{\lfloor n/2 \rfloor}$ divides $U_n(P, Q)$. Thus, for $n \geq 4$, $U_n(P, Q)$ cannot be prime unless $P$ and $Q$ are relatively prime, a fact we use throughout this paper. However, even when $P$ and $Q$ are relatively prime, we show that certain Lucas sequences contain only finitely many primes. That is, although it is beyond current techniques to prove any Lucas sequences other than $U_n(2, 1)$ or $U_n(-2, 1)$ contain infinitely many primes, we have the following negative results.

**Theorem 1.1.** *If $P$ and $Q$ are integers and $Q$ is a square, then the sequence $U_n(P, Q)$ contains only finitely many primes.*

**Theorem 1.2.** *If $x$ and $y$ are complex numbers, not both 1 and not both -1, for which $xy$ and $x + y$ are integers and $k > 1$ is an integer, then $U_n(x^k + y^k, x^k y^k)$ contains only finitely many primes.*

When $x$ and $y$ are real, we can say more.

**Theorem 1.3.** *If $P^2 > 4Q$ and $Q$ a square, then $U_n(P, Q)$ can only be prime when $n = 2$.*

**Theorem 1.4.** *Suppose $x$ and $y$ are real, $xy$ and $x + y$ are integers, and $k > 1$ is an integer. Then, $U_n(x^k + y^k, x^k y^k)$ can only be prime when $n = p$ and $k = p^r$ for some prime $p$ and positive integer $r$.*

Lucas sequences satisfy a large number of identities. We will make use of the following identities.

$$U_{m+n} = U_m U_{n+1} - Q U_{m-1} U_n, \tag{1.3}$$

$$U_{2n+1} = U_{n+1}^2 - Q U_n^2, \tag{1.4}$$

$$U_n(x + y, xy) = x U_{n-1}(x + y, xy) + y^{n-1}. \tag{1.5}$$

Of these, formula (1.3) is well-known [7, (IV.4), p. 57] and formula (1.4) is an immediate consequence of it (with $m = n + 1$). Formula (1.5) follows easily from formula (1.2). We need the following connections between the sequences $U_n$ and $V_n$ [7, (IV.2), p. 56, (IV.11), p. 59].

$$V_n = U_{n+1} - Q U_{n-1} \tag{1.6}$$

$$U_n = \sum_{k=1}^{\lceil n/2 \rceil} Q^{k-1} V_{n+1-2k} = V_{n-1} + Q V_{n-3} + Q^2 V_{n-5} + \cdots . \tag{1.7}$$

Lucas sequences are divisibility sequences. That is, they satisfy the arithmetic property:

$$U_k \text{ divides } U_n \quad \text{when} \quad k \text{ divides } n. \tag{1.8}$$

A simple calculation using formula (1.2) gives the following formula.

$$U_{km}(x + y, xy) = U_k(x + y, xy) U_m(x^k + y^k, x^k y^k). \tag{1.9}$$

Because $x^k + y^k = V_k(x + y, xy)$ is an integer, $U_{km}$ can be explicitly written as $U_k$ times an integer. An iteration of formula (1.9) gives

$$U_n(x^k + y^k, x^k y^k) = \frac{U_n(x + y, xy)\, U_k(x^n + y^n, x^n y^n)}{U_k(x + y, xy)}. \tag{1.10}$$

When $P$ and $Q$ are relatively prime, the result in (1.8) can be strengthened to

$$\gcd(U_m, U_n) = U_{\gcd(m,n)}, \tag{1.11}$$

as found in [7, (IV.26), p. 64]. In particular, if $\gcd(m, n) = 1$, then $\gcd(U_m, U_n) = 1$, when $P$ and $Q$ are relatively prime.

Given complex numbers $x$ and $y$, we define the $n$th cyclotomic number for $x$ and $y$ to be

$$\Phi_n(x,y) = \prod_{\substack{\gcd(r,n)=1 \\ 1\le r\le n}} (x - \zeta^r y),$$

where $\zeta$ is a primitive $n$th root of unity. Cyclotomic numbers have the following properties [7, p. 82], [9].

**Theorem 1.5.** *If $x$ and $y$ are zeros of $z^2 - Pz + Q$, then*

a. *for all natural numbers $n$, $\Phi_n(x,y)$ is an integer,*

b. *for all natural numbers $n$, $U_n(P,Q) = \prod_{d|n,\, d>1} \Phi_d(x,y)$.*

Critical to this study, we need a condition on the growth of cyclotomic numbers. With $\phi(n)$ representing Euler's totient function, we quote the following result from Stewart [9], Theorem 4.2.

**Theorem 1.6.** *If $xy$ and $(x+y)^2$ are integers and $x/y$ is not a root of unity, then there is an effectively computable positive number $c$ for which*

$$|\Phi_n(x,y)| > |x|^{\phi(n)/2} \tag{1.12}$$

*for all $n > c$.*

At the other extreme, it is easy to characterize the cases where $U_n$ is small.

**Theorem 1.7.** *Let $S$ be the set $\{(0,0),(\pm1,0),(0,\pm1),(\pm1,1)\}$. Then, $|U_n(P,Q)| \le 1$ for all $n$ if and only if $(P,Q) \in S$.*

*Proof.* It is easy to see that for $(P,Q)$ in the given set, $|U_n(P,Q)|$ is 0 or 1 for every $n$. In the other direction, because $U_2(P,Q) = P$, we must have $|P| \le 1$. Because $U_n(-P,Q) = (-1)^n U_n(P,Q)$, without loss of generality, let $P$ be 0 or 1. If $P = 0$, then $U_3 = -Q$ forces $Q = 0, \pm 1$. If $P = 1$, then $U_3 = 1 - Q$ forces $Q = 0$ or $Q = 2$. Finally, if $(P,Q) = (1,2)$, then $|U_4| = 3 > 1$. □

Most of our attention is focused on Lucas sequences $U_n(P,Q)$ where $n$ is prime. This is because, as mentioned in Theorem 2.1, there is a known finite list of composite $n$ for which $U_n(P,Q)$ can be prime. In Section 3, we compare heuristic estimates to our data. We prove Theorem 1.1 and Theorem 1.2 in Section 4. In Section 5, we prove Theorem 1.3 and Theorem 1.4. We conclude this section by characterizing those Lucas sequences for which $x/y$ is a root of unity. This material is well-known, but we include it here in our notation.

**Lemma 1.8.** *If $P$ and $Q$ are integers, then $x/y$ is a root of unity if and only if $P^2 = kQ$, where $k \in \{0,1,2,3,4\}$.*

*Proof.* It is easy to see that $x/y$ is a root of unity when $P^2 = kQ$ with $k \in \{0,1,2,3,4\}$.

On the other hand, suppose that $x/y$ is a root of unity. Because $x/y$ is at worst quadratic, if $x/y = e^{2\pi ij/m}$ for relatively prime integers $j$ and $m$, then $\phi(m)$ is 1 or 2, because the degree of $e^{2\pi ij/m}$ is $\phi(m)$. Consequently, $m$ has one of the values 1, 2, 3, 4, or 6. If $m = 1$, then $x = y$ and $P^2 = 4Q$. If $m = 2$, $x = -y$ and $P = 0$. When $m = 4$, $P = (1 \pm i)y$ and $Q = \pm iy^2$ gives $P^2 = 2Q$. When $m = 3$, $x$ is $\omega y$ or $\omega^2 y$, where $\omega$ is a primitive cube root of unity. In each case, $P^2 = Q$. Finally, if $m = 6$, then $x = -\omega y$ or $x = -\omega^2 y$. In either case, $P^2 = 3Q$. □

**Theorem 1.9.** *If $P$ and $Q$ are relatively prime and $x/y$ is a root of unity, then $(P,Q) \in \{(0,\pm1),(\pm1,1),(\pm2,1)\}$.*

*Proof.* If $P = 0$, then $Q = \pm 1$. If $P \neq 0$ and $P^2 = kQ$, then any prime divisor of $Q$ is also a divisor of $P$. This forces $Q = 1$. By Lemma 1.8, $P = \pm 1$ if $k = 1$, and $P = \pm 2$ if $k = 4$, and these are the only possibilities. □

## 2. Lucas Primes with Composite Index

Because Lucas sequences are divisibility sequences, one might think $n$ must be prime for $U_n$ to be prime. A Wikipedia article [11] makes this explicit claim. However, even among the Fibonacci numbers, $F_4 = 3$. Prime Lucas numbers of composite index are mostly classified.

**Theorem 2.1.** *For composite $n$, a Lucas number $U_n(P, Q)$ can only be prime for*

$$n \in \{4, 6, 8, 9, 10, 15, 25, 26, 65\}.$$

*Moreover, for $n \in \{6, 8, 10, 15, 25, 26, 65\}$, there are only finitely many $P, Q$ for which $U_n(P, Q)$ is prime, and this list of $(n, P, Q)$ is known.*

*Proof.* The proof, with the list of values $(n, P, Q)$, is given in Theorem 3.1 of [6]. □

When $P^2 - 4Q > 0$, we can say more.

**Theorem 2.2.** *If $P$ and $Q$ are integers and $P^2 - 4Q > 0$, then $U_n$ is composite for all composite $n > 4$.*

*Proof.* As mentioned in Lemma 5.1, for $P^2 - 4Q > 0$, $U_n$ is increasing for all $n \geq 2$. Thus, for $n = km$ with $k \geq m > 1$, by hypothesis, $k > 2$, so $U_n > U_k > 1$. Because $U_n$ has $U_k$ as a factor, $U_n$ is composite. □

Because $U_4(P, Q) = P(P^2 - 2Q)$, this expression is prime for infinitely many $(P, Q)$. In particular, $U_4\big(1, \frac{1}{2}(1 \pm q)\big)$ is prime for all odd primes $q$ and $U_4\big(P, \frac{1}{2}(P^2 \pm 1)\big)$ is prime, whenever $P$ is an odd prime.

We have a partial characterization of $P, Q$ for which $U_9$ is prime.

**Theorem 2.3.** *For integers $P > 0$ and $Q$, $U_9(P, Q)$ is prime if and only if one of the two conditions hold:*

$$Q = P^2 + 1 \qquad \textit{and} \qquad 3P^6 + 9P^4 + 6P^2 - 1 \qquad \textit{is prime,}$$

*or*

$$Q = P^2 - 1 \qquad \textit{and} \qquad 3P^6 - 9P^4 + 6P^2 + 1 \qquad \textit{is prime.}$$

*Proof.* We have $U_9(P, Q) = (P^2 - Q)(P^6 - 6P^4Q + 9P^2 - Q^3)$. This second expression can be written as $(P^3 - 3PQ)^2 - Q^3$, or $m^2 - n^3$ for some integers $m$ and $n$. Now $m^2 = n^3 - 1$ has $m = 0$, $n = 1$ as its only integer solution and $m^2 = n^3 + 1$ has only $(m, n) = (-1, 0), (0, \pm 1), (2, \pm 3)$ as integer solutions. These results date back to Euler, see [2, pp. 533–534]. None of the solutions to $m^2 = n^3 \pm 1$ lead to a case where $|P^6 - 6P^4Q + 9P^2 - Q^3| = 1$, with $P, Q$ integers and $P > 0$. Thus, to be prime, we need $P^2 - Q = \pm 1$, which leads to the given characterization. □

By Bouniakowski's conjecture [1, Hypothesis H, p. 15], we expect infinitely many cases of $P, Q$ for which $U_9$ is prime.

## 3. Heuristic Expectations

Let $p$ be a prime number. In [10], it is stated that the expected probability that a Mersenne number $M_p = 2^p - 1$ be prime is

$$e^\gamma \frac{\log(2p)}{\log M_p},$$

where $\gamma$ is the Euler-Mascheroni constant. The argument is as follows (see [10] or [1, p. 23] for a more careful argument). First, by the Prime Number Theorem, the expected probability that a random number $N$ is prime is $\frac{1}{\log N}$. However, $M_p$ is not a random number. Any prime divisor of $M_p$ must be congruent to 1 modulo $p$. Thus, $M_p$ is not divisible by any prime $q < 2p + 1$. This is expected to increase the probability that $M_p$ be prime by a factor of $\prod_{q<2p+1} \frac{q}{q-1}$, and this product is asymptotic to $e^\gamma \log(2p)$ by Mertens Theorem [1, Theorem 1.4.2, p. 32].

In the case where $P$ and $Q$ are relatively prime, if $p$ does not divide $Q$ or $D$, then one should have the same heuristic probability that $U_p(P, Q)$ is prime. That is, aside from the exceptions named in Theorem 1.1 and Theorem 1.2, one expects $U_p(P, Q)$ to be prime with probability

$$e^\gamma \frac{\log(2p)}{\log |\, U_p \,|}. \tag{3.1}$$

For $1 \le P \le 100$, $-100 \le Q \le 100$, and $1 \le n \le 1000$, we found all pairs $(P, Q, n)$ where $n$ is prime and $U_n(P, Q)$ is a probable prime. We tested our data against heuristic expectations in two different ways. First, for each prime $p < 1000$ we added $\frac{\log(2p)}{\log |U_p|}$ over all $P, Q$ in our range to get an "expected" number of primes $U_p$, and compared this against the actual number of prime $U_p$ in our data set. A least squares fit gave

$$\frac{\text{Actual number of prime } U_p}{\text{Estimated number of prime } U_p} = 1.632 - .000036p.$$

Because we left off the scaling factor $e^\gamma \approx 1.781$, we expected the constant term to be closer to 1.781. However, this fit did not take Theorem 1.1 or Theorem 1.2 into account. When we modified our expectation to only sum over those $P, Q$ not subject to these theorems, the constant rose to 1.733, still a bit below $e^\gamma$. This might be because of the influence of the smallest primes $p$. If we exclude the first 10 primes, the fit becomes $1.771 - .000030p$.

We also examined the total number of primes found in our search vs. the expected number. All told, we found 43,683 triples $(P, Q, p)$ for which $p$ is prime and $U_p(P, Q)$ is a probable prime. Summing the expression in (3.1) over all triples $(P, Q, p)$ gives 54,053, off by about 24%. There are two confounding effects: the effect of small primes, and the effect of those $(P, Q)$ known to contain only finitely many primes in their Lucas sequences. If we ignore the first 10 primes, and those $(P, Q)$ covered by Theorem 1.1 or Theorem 1.2, the expected number of primes (found by summing (3.1) over the allowable $(P, Q)$ with $p > 29$) was 22,834 and the number of primes found in our search was 22,352, pretty good matches.

## 4. Proofs of Theorem 1.1 and Theorem 1.2

*A Proof of Theorem 1.2.* As usual, without loss of generality, we may assume $P > 0$. Moreover, we need not consider any $(P, Q)$ in $S$, the set in Theorem 1.7, and we may assume $\gcd(P, Q) = 1$. Because we are assuming $x$ and $y$ are not both 1, by Theorem 1.9, we may assume $x/y$ is not a root of unity. Recalling formula (1.10),

$$U_n(x^k + y^k, x^k y^k) = \frac{U_n(x + y, xy)\, U_k(x^n + y^n, x^n y^n)}{U_k(x + y, xy)},$$

we fix $k$, so $C = |U_k(x+y, xy)|$ is a fixed nonzero integer. By Theorem 1.6, $|U_n(x+y,xy)| \geq |\Phi_n(x,y)| > C$ for $n$ sufficiently large. Similarly,

$$U_k(x^n+y^n, x^n y^n) = \frac{U_{kn}(x+y,xy)}{U_k(x+y,xy)} = \frac{\prod_{d|kn,\, d>1} \Phi_d(x,y)}{\prod_{d|n,\, d>1} \Phi_d(x,y)}$$

is divisible by $|\Phi_{kn}(x,y)| > C$ for sufficiently large $n$. Thus, $U_n(x^k+y^k, x^k y^k)$ is composite for all large $n$. □

*A Proof of Theorem 1.1.* We may again ignore cases where $P$ or $Q$ is 0, or when $|P| = |Q| = 1$. Let $x$ and $y$ be zeros of $z^2 - Pz + Q$, and select complex numbers $u$ and $v$ satisfying $u^2 = x$ and $v^2 = y$. Then, $(u+v)^2 = P + 2Q$, an integer, and Theorem 1.6 applies. By Theorem 2.1, only finitely many primes can occur when $n$ is even, so we restrict our attention to odd $n$. By formula (1.4), if $n = 2m+1$, then $U_n = (U_{m+1} - \sqrt{Q}U_m)(U_{m+1} + \sqrt{Q}U_m)$. That is, $U_n$ is the product of two integers. We have

$$\begin{aligned} U_{m+1} + \sqrt{Q}U_m &= \frac{x^{m+1} - y^{m+1}}{x-y} + uv\frac{x^m - y^m}{x-y} \\ &= \frac{u^{2m+1} - v^{2m+1}}{u-v} = U_{2m+1}(u+v, uv) \end{aligned}$$

and

$$U_{m+1} - \sqrt{Q}U_m = \frac{u^{2m+1} + v^{2m+1}}{u+v} = \frac{U_{4m+2}(u+v,uv)}{U_{2m+1}(u+v,uv)}.$$

By Theorem 1.5, $\Phi_{2m+1}(u,v)$ divides $U_{m+1} + \sqrt{Q}U_m$ and $\Phi_{4m+2}(u,v)$ divides $U_{m+1} - \sqrt{Q}U_m$. By Theorem 1.6, for sufficiently large $n$, each term is larger than 1. Consequently, $U_n$ is composite for all large $n$. □

## 5. The Real Case

In this section, we provide elementary proofs (that is, proofs not relying on the theory of linear forms in logarithms of algebraic numbers) for Theorem 1.3 and Theorem 1.4. We assume that $x$ and $y$, the zeros of $z^2 - Pz + Q$ are real. That is, we assume $P^2 - 4Q \geq 0$.

**Lemma 5.1.** *If $P \neq 0$ and $P^2 > 4Q$, then $|U_n(P,Q)|$ is a strictly increasing function of $n$ for $n \geq 2$ and $|V_n(P,Q)|$ is increasing for all $n \geq 1$.*

*Proof.* This is the result of Lemma 3 from [5]. □

*A Proof of Theorem 1.3.* Without loss of generality, we may assume $P > 0$ and $x > y > 0$. Now, $P^2 - 4Q = (P - 2\sqrt{Q})(P + 2\sqrt{Q}) > 0$. Thus, $P > 2\sqrt{Q}$. In particular, $P \geq 3$. Because $U_2 = P$, $U_2$ will be prime when $P$ is prime. Note that $U_3 = P^2 - Q = (P - \sqrt{Q})(P + \sqrt{Q})$. Because $P - \sqrt{Q} > \sqrt{Q} \geq 1$, both factors are larger than 1, showing $U_3$ is never prime. Similarly, because $P \geq 3$ and $U_4 = P(P^2 - 2Q)$, $U_4$ is not prime. Thus, by Theorem 2.2, $U_n$ will not be prime for any composite $n$. Suppose $n$ is prime and $n > 3$. Since $n$ is odd, $n = 2k+1$ for some $k \geq 2$ and $U_n = (U_{k+1} - \sqrt{Q}U_k)(U_{k+1} + \sqrt{Q}U_k)$. This second term is an integer larger than 1. For the first,

$$U_{k+1} - \sqrt{Q}U_k = xU_k - \sqrt{xy}U_k + y^k = \sqrt{x}(\sqrt{x} - \sqrt{y})U_k + y^k.$$

Note that

$$(\sqrt{x} - \sqrt{y})^2 = x + y - 2\sqrt{xy} = P - 2\sqrt{Q} \geq 1.$$

Consequently, $\sqrt{x} > 1$, $\sqrt{x} - \sqrt{y} \geq 1$, $U_k \geq U_2 > 1$, and $y^k$ is positive. Thus, $U_{k+1} - \sqrt{Q}U_k > 1$, so $U_n$ is not prime. This completes the proof. □

We next study $U_k(x^n + y^n, x^n y^n)$ as a function of $n$.

**Lemma 5.2.** *If $x > y > 0$, then*

$$U_k(x^n + y^n, x^n y^n) > U_k(x^{n-1} + y^{n-1}, x^{n-1} y^{n-1})$$

*for all $k \geq 2$ and $n \geq 2$.*

*Proof.* Because $y > 0$, we have $Q > 0$, meaning $Q \geq 1$. Thus, $Q^i \geq Q^j$ for all $i > j$. Also, $V_k(x^n, y^n) = V_{kn}(x, y) > V_{kn-k}(x, y) = V_k(x^{n-1}, y^{n-1})$, provided $n > 1$ by Lemma 5.1. Using equation (1.7), we have

$$\begin{aligned} U_k(x^n, y^n) &= \sum_{j=1}^{\lceil k/2 \rceil} Q^{n(j-1)} V_{k+1-2j}(x^n + y^n, x^n y^n) \\ &> \sum_{j=1}^{\lceil k/2 \rceil} Q^{(n-1)(j-1)} V_{k+1-2j}(x^{n-1} + y^{n-1}, x^{n-1} y^{n-1}) \\ &= U_k(x^{n-1} + y^{n-1}, x^{n-1} y^{n-1}), \end{aligned}$$

as desired. □

The same proof shows a little more.

**Lemma 5.3.** *For all $x > y$, if $n$ is even, then $U_k(x^n, y^n) > U_k(x^m, y^m)$ for all $0 < m < n$.*

*Proof.* We have

$$\begin{aligned} U_k(x^m + y^m, x^m y^m) &= \sum_{j=1}^{\lceil k/2 \rceil} Q^{m(j-1)} V_{k+1-2j}(x^m + y^m, x^m y^m) \\ &\leq \sum_{j=1}^{\lceil k/2 \rceil} |Q|^{m(j-1)} V_{k+1-2j}(x^m + y^m, x^m y^m) \\ &< \sum_{j=1}^{\lceil k/2 \rceil} |Q|^{n(j-1)} V_{k+1-2j}(x^n + y^n, x^n y^n) \\ &= \sum_{j=1}^{\lceil k/2 \rceil} Q^{n(j-1)} V_{k+1-2j}(x^n + y^n, x^n y^n) \\ &= U_k(x^n + y^n, x^n y^n). \end{aligned}$$

□

Finally, we have the following theorem.

**Theorem 5.4.** *For all $n > 1$ and $k > 1$,*

$$|U_k(x^n + y^n, x^n y^n)| > |U_k(x^{n-1} + y^{n-1}, x^{n-1} y^{n-1})|.$$

*Proof.* Without loss of generality, we may assume $P > 0$, $x > y$, and $x > 0$. We have verified the result for $y > 0$ and also for $n$ even, so suppose $n$ is odd and $y < 0$. Then, $Q < 0$. The proof follows by induction on $k$. When $k = 0$, $U_k(x^n, y^n) = 0 = U_k(x, y)$, and when $k = 1$, $U_k(x^n, y^n) = 1 = U_k(x, y)$. Moreover, $U_2(x^n, y^n) = x^n + y^n > x + y = U_2(x, y)$. Assuming

that $U_m(x^n, y^n) > U_m(x^{n-1}, y^{n-1})$ for all $m$ with $2 \le m \le k-1$, by the defining recurrence (1.1), we have

$$\begin{aligned} U_k(x^n, y^n) &= V_n(x,y)U_{k-1}(x^n, y^n) - Q^n U_{k-2}(x^n, y^n) \\ &= V_n(x,y)U_{k-1}(x^n, y^n) + |Q|^n U_{k-2}(x^n, y^n) \\ &> V_{n-1}(x,y)U_{k-1}(x^{n-1}, y^{n-1}) + |Q|^{n-1} U_{k-2}(x^{n-1}, y^{n-1}) \\ &> V_{n-1}(x,y)U_{k-1}(x^{n-1}, y^{n-1}) - Q^{n-1} U_{k-2}(x^{n-1}, y^{n-1}) \\ &= U_k(x^{n-1}, y^{n-1}), \end{aligned}$$

as desired. □

*A Proof of Theorem 1.4.* Without loss of generality, we assume $P > 0$ and $x > y$, $x > 0$. First note that

$$U_4(x^k + y^k, x^k y^k) = V_k(x+y, xy)V_{2k}(x+y, xy),$$

so by Lemma 5.1, $U_4(x^k + y^k, x^k y^k)$ is not prime. Consequently, by Theorem 2.2, we may restrict ourselves to the case where $n$ is a prime number. By formula (1.10), Lemma 5.1, and Theorem 5.4, when $n > k$, $U_n(x^k + y^k, x^k y^k)$ is composite. For $n \le k$, suppose $k$ is divisible by a prime $q \ne n$, say $k = qm$. An application of formula (1.10) with variables $x^m$ and $y^m$ and with $q$ in place of $k$ gives

$$\begin{aligned} U_n(x^k + y^k, x^k y^k) &= U_n((x^m)^q + (y^m)^q, ((xy)^m)^q) \\ &= \frac{U_n(x^m + y^m, x^m y^m)U_q(x^{mn} + y^{mn}, (xy)^{mn})}{U_q(x^m + y^m, x^m y^m)}. \end{aligned}$$

Because $q$ is prime to $n$, $U_q$ is prime to $U_n$ in this product, so $U_q(x^m + y^m, x^m y^m)$ properly divides $U_q(x^{mn} + y^{mn}, (xy)^{mn})$, showing $U_n(x^k + y^k, x^k y^k)$ is composite. Thus, for $U_n(x^k + y^k, x^k y^k)$ to be prime, it must be that $n$ is prime and $k$ is a power of $n$. This completes the proof. □

## 6. Comments

With regard to Theorem 1.2 and Theorem 1.4, when $n = p$ and $k = p^m$ for some prime $p$ and positive integer $m$, then

$$U_p(x^{p^m} + y^{p^m}, x^{p^m} y^{p^m}) = \Phi_{p^m}(x, y).$$

As a consequence of the Bouniakowski's conjecture [1, Hypothesis H, p. 15], for any fixed $p$ and $m$, we expect this polynomial to be prime for infinitely many $x$ and $y$.

In our data, as is to be expected, the slower $U_n$ grew with $n$, the more primes tended to occur in the sequence. Because $U_n(2,1) = n$, this sequence produces a prime for all 168 primes $n < 1000$. The sequence $U_n(1,2)$ was prime for 33 values of $n$ and $U_n(2,5)$ was prime for 24 values. These sequences are aided because $x$ and $y$ are complex, so the oscillating nature of $U_n$ gives many small values. For real $x$ and $y$, the best performers were the Fibonacci numbers ($(P,Q) = (1,-1)$) and $U_n(2,-1)$, each prime for 21 values of $n$.

At the other extreme, in our search, we found 658 pairs $(P,Q)$ with $1 \le P \le 100$, $-100 \le Q \le 100$, $\gcd(P,Q) = 1$ for which $U_n(P,Q)$ was composite for all $n \le 1000$. Taking into account Theorem 1.1, Theorem 1.2, and expanding the search to all $n \le 10,000$, the number of pairs $(P,Q)$ dropped to 97. If we include cases where $P$ is prime, so $U_2(P,Q)$ is prime, but $U_n$ is not prime for any other values of $n \le 10,000$, then there were 156 examples. The examples with smallest $P$ and $|Q|$ were $(6,-29)$ and $(13,-19)$. Is there something special about $U_n(6,-29)$ or $U_n(5,33)$ that they should never be prime for $n \ge 3$? We suspect that

this was a statistical artifact. That is, we tested $12,174$ pairs $(P, Q)$ so, even if it is likely that a given sequence contain primes, it is not surprising that some did not, in a limited search up to only $n = 10,000$.

Ronald L. Graham [3] exhibited a Fibonacci-like sequence ($A_n = A_{n-1} + A_{n-2}$, but with specific, well chosen initial conditions) that contained no primes. His method used covering congruences to show that there was a list of 18 primes with the property that each $A_n$ was divisible by at least one of those primes. Such an approach is not possible here due to formula (1.11), which forbids the existence of a finite set of primes with at least one dividing each sufficiently large $U_n$. Consequently, we think Theorem 1.1 and Theorem 1.2 are the only obstructions to infinitely many primes in a Lucas sequence. That is, we make the following conjecture.

**Conjecture 1.** *If $x$ and $y$ are complex numbers, where $P = x + y$ and $Q = xy$ are relatively prime integers and*

- $(P, Q) \notin \{(0, \pm 1), (\pm 1, 1), (\pm 2, 1)\}$,
- *$Q$ is not a square,*
- *there are no complex numbers $\alpha$ and $\beta$ with the property that $\alpha + \beta$ and $\alpha\beta$ are integers and for some integer $k > 1$, $x = \alpha^k$, $y = \beta^k$,*

*then there are infinitely many prime numbers $p$ for which $U_p(P, Q)$ is prime.*

## References


[1] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer-Verlag, New York, 2001.

[2] L. E. Dickson, *History of the Theory of Numbers*, Vol. II, Chelsea, Bronx, 1971.

[3] R. L. Graham, *A Fibonacci-like sequence of composite numbers*, Math. Mag., **37** (1964), 322–324.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Claredon Press, Oxford, UK, 1979.

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

[6] 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.

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

[8] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, 2nd ed., Birkhauser, Boston, 1994.

[9] C. L. Stewart, *On divisors of Lucas and Lehmer numbers*, Acta Math., **211** (2013), 291–314.

[10] S. Wagstaff, *Divisors of Mersenne numbers*, Math. Comp., **40** (1983), 385–397.

[11] Wikipedia contributors, *Lucas sequence — Wikipedia, The Free Encyclopedia*, 2020, https://en.wikipedia.org/w/index.php?title=Lucassequence&oldid=917524700, accessed 22-October-2019.


MSC2020: 11B39, 11A41, 11B37

Department of Mathematics and Statistics, University of Minnesota–Duluth, Duluth, MN 55812

Department of Mathematics and Statistics, University of Minnesota–Duluth, Duluth, MN 55812

*Email address*: jgreene@d.umn.edu