ON LUCAS AND FROBENIUS PSEUDOPRIMES

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

Michal Křížek
Institute of Mathematics, Czech Academy of Sciences, Prague, Czech Republic
krizek@math.cas.cz

Received: 12/30/24, Revised: 5/22/25, Accepted: 11/3/25, Published: 11/25/25

Abstract

Consider the Lucas sequences $U(P,Q)$ and $V(P,Q)$ which satisfy the linear recurrence relation $W_{n+2} = PW_{n+1} - QW_n$ with initial terms $U_0 = 0$, $U_1 = 1$, and $V_0 = 2$, $V_1 = P$, respectively, where P and Q are integers. We consider pseudoprimes with parameters P and Q related to $U(P,Q)$ and $V(P,Q)$. We extend results obtained by Somer and Křížek (2022) regarding pseudoprimes with parameters P and Q, where P is odd and greater than 0 to those in which the parameter P can also be less than 0 or even. We also obtain infinitely many new examples of pseudoprimes, called the Lucas pseudoprimes with parameters P and Q. We further present results on Frobenius pseudoprimes, which are generalizations of Lucas pseudoprimes.

– *Dedicated to Professor Curtis Cooper on the occasion of his retirement.*

1. Introduction

Let P and Q be integer numbers. Let $U(P,Q)$, called the *Lucas sequence of the first kind* (LSFK), and $V(P,Q)$, called the *Lucas sequence of the second kind* (LSSK), be the sequences satisfying the linear recursion relation

$$W_{n+2} = PW_{n+1} - QW_n \qquad (n \geq 0) \tag{1.1}$$

with discriminant $D = P^2 - 4Q$ and the initial terms W_0 and W_1 are $U_0 = 0$, $U_1 = 1$ and $V_0 = 2$, $V_1 = P$, respectively.

In this paper, we will extend results obtained by Somer and Křížek [22] concerning pseudoprimes related to the Lucas sequences $U(P,Q)$ and $V(P,Q)$. These results are generalized from pseudoprimes with parameters P and Q for which P is greater

DOI: 10.5281/zenodo.17711594

than 0 and odd to additional cases in which P can also be less than 0 or even. We will also obtain infinitely many new cases of one type of pseudoprime defined below in Definition 3.1, called the *Lucas pseudoprimes with parameters P and Q*. We also discuss Frobenius pseudoprimes which are generalizations of Lucas pseudoprimes.

2. Necessary Definitions and Results

To proceed, we will require the following definitions and results. If m is a positive integer, it is easily seen that $U(P,Q)$ and $V(P,Q)$ are purely periodic modulo m when $\gcd(m,Q) = 1$ (see [5, pp. 344–345]). From here on, we assume that $\gcd(m,Q) = 1$. Throughout this paper, p and p_i denote primes and m always represents a positive integer. We denote the period of $U(P,Q)$ modulo m by $\lambda(m)$, that is, $\lambda(m)$ is the least positive integer s such that

$$U_{s+n} \equiv u_n \pmod{m}$$

for all $n \geq 0$. The *rank of appearance* of m in $U(P,Q)$, denoted by $\rho(m)$, is the least positive integer r such that

$$U_r \equiv 0 \pmod{m}.$$

Since $U_0 = 0$ and $U(P,Q)$ is purely periodic modulo m, we see that $\rho(m)$ exists. It is clear that $U_t \equiv 0 \pmod{m}$ if and only if $\rho(m) \mid t$. The prime p is called a *primitive prime divisor* of $U_n(P,Q)$ if $\rho(p) = n$. Equivalently, p is a primitive prime divisor of $U_n(P,Q)$ if $p \mid U_n(P,Q)$, but $p \nmid U_i(P,Q)$ for $1 \leq i \leq n-1$.

Associated with $U(P,Q)$ and $V(P,Q)$ is the characteristic polynomial

$$f(x) = x^2 - Px + Q$$

with discriminant $D = D(P,Q) = P^2 - 4Q$ and characteristic roots

$$\alpha = (P + \sqrt{D})/2 \qquad \text{and} \qquad \beta = (P - \sqrt{D})/2. \tag{2.1}$$

We observe that

$$D = (\alpha - \beta)^2. \tag{2.2}$$

It follows from (2.1), (2.2), the Binet formulas, and the binomial formula that

$$U_n(P,Q) = \frac{\alpha^n - \beta^n}{\sqrt{D}} = \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n}{2k+1} \frac{1}{2^{n-1}} P^{n-(2k+1)} D^k \tag{2.3}$$

and

$$V_n(P,Q) = \alpha^n + \beta^n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} \frac{1}{2^{n-1}} P^{n-2k} D^k. \tag{2.4}$$

The Lucas sequences $U(P,Q)$ and $V(P,Q)$ with characteristic roots α and β are called *degenerate* if $PQ = 0$ or α/β is a root of unity. It follows from the Binet formulas (2.3) and (2.4) that $U_n(P,Q)$ or $V_n(P,Q)$ can be equal to 0 for some $n > 0$ only if $U(P,Q)$ and $V(P,Q)$ are degenerate. Since the characteristic polynomial of $U(P,Q)$ and $V(P,Q)$ is a quadratic polynomial with integer coefficients, one sees that α/β can be a primitive nth root of unity only if $n \in \{1,2,3,4,6\}$. The following theorem determines all degenerate Lucas sequences $U(P,Q)$ and $V(P,Q)$.

Theorem 2.1. *Let M denote an arbitrary nonzero integer. Then the Lucas sequences $U(P,Q)$ and $V(P,Q)$ with characteristic roots α and β are degenerate only in the following cases:*

(i) *$Q = 0$, P is any integer. Then $D = P^2$, $U_n = P^{n-1}$, and $V_n = P^n$ for $n \geq 1$.*

(ii) *$\alpha/\beta = 1$. Then $P = 2M$, $Q = M^2$, and $D = 0$.*

(iii) *$\alpha/\beta = -1$. Then $P = 0$, $Q = M$, and $D = -4M$.*

(iv) *α/β is a primitive cube root of unity. Then $P = M$, $Q = M^2$, and $D = -3M^2$.*

(v) *α/β is a primitive fourth root of unity. Then $P = 2M$, $Q = 2M^2$, and $D = -4M^2$.*

(vi) *α/β is a primitive sixth root of unity. Then $P = 3M$, $Q = 3M^2$, and $D = -3M^2$.*

This is proved in [23, p. 613].

Remark 2.2. Consider the nondegenerate LSFK $U(P,Q)$, where $Q = \pm 1$. We note that by Theorem 2.1, $D = P^2 - 4Q > 0$.

The following Proposition 2.3, Theorem 2.4, Lemmas 2.5–2.9, and Corollary 2.10 will be needed for the proof of our principal results.

Proposition 2.3. *Consider the nondegenerate Lucas sequences $U(P,Q)$ and $V(P,Q)$. Then the following hold:*

(i) *$U_{2n} = U_n V_n$;*

(ii) *$U_{n+1}^2 - U_n U_{n+2} = Q^n$;*

(iii) *if $m \mid n$, then $U_m \mid U_n$;*

(iv) *if $m \mid n$ and n/m is odd, then $V_m \mid V_n$;*

(v) *$P \mid U_{2n}$ for all $n \geq 0$;*

(vi) $P \mid V_n$ *for* n *odd;*

(vii) $U_n(-P,Q) = (-1)^{n+1}U_n(P,Q)$*;*

(viii) $V_n(-P,Q) = (-1)^n V_n(P,Q)$.

Proof. Parts (i)–(iv) and (vii)–(viii) follow from the Binet formulas (2.3) and (2.4). Part (v) follows from part (iii) and part (vi) follows from part (iv) upon noting that $U_2 = V_1 = P$. □

Theorem 2.4. *Consider the LSFK* $U(P,Q)$ *and the LSSK* $V(P,Q)$ *with discriminant* D*. Let* r *and* s *be positive integers.*

(i) *If* $\gcd(r,Q) = 1$*, then* $r \mid U_s$ *if and only if* $\rho(r) \mid s$*;*

(ii) *if* p *is an odd prime and* $p \nmid Q$*, then* $p \mid U_{p-(D/p)}$*, where* (D/p) *is the Legendre symbol and* $(D/p) = 0$ *if* $p \mid D$*;*

(iii) *if* $p \mid D$ *and* $p \nmid Q$*, then* $\rho(p) = p$*;*

(iv) *if* $p \nmid 2QD$*, then* $U_{(p-(D/p))/2}$ *if and only if* $(Q/p) = 1$*;*

(v) *if* $p \nmid Q$*,* $\rho(p^k) = \rho(p)$*, and* $\rho(p^{k+1}) \neq \rho(p)$*, then* $\rho(p^j) = p^{\max(j-k,0)}\rho(p)$ *for* $j \geq 1$*;*

(vi) *if* $\gcd(rs,Q) = 1$ *and* $r \mid s$*, then* $\rho(r) \mid \rho(s)$*;*

(vii) *if* $\gcd(P,Q) = 1$ *and* $d = \gcd(r,s)$*, then* $\gcd(U_r,U_s) = |U_d|$*;*

(viii) *if* $\gcd(r,s) = \gcd(rs,Q) = 1$*, then* $\rho(rs) = \operatorname{lcm}(\rho(r),\rho(s))$*;*

(ix) *if* $\gcd(P,Q) = 1$ *and* $p \mid Q$*, then* $p \nmid U_n$ *for* $n \geq 1$*;*

(x) *if* $\gcd(P,Q) = 1$*, then* $p \equiv (D/p) \pmod{\rho(p)}$.

This follows from the results in [12, pp. 53–74], [4], and [9].

Lemma 2.5. *Consider the LSFK* $U(P,Q)$*, where* $Q \neq 0$*. Let* $W(P,Q)$ *be a recurrence satisfying the recursion relation* (1.1) *with initial terms* W_0 *and* W_1*. Suppose that* $U_t \equiv 0 \pmod{m}$*, where* $\gcd(m,Q) = 1$*. Then*

$$W_{n+t} \equiv U_{t+1}W_n \pmod{m}$$

for all $n \geq 0$.

Proof. It can be shown by induction and use of the linear recursion relation defining both $U(P,Q)$ and $W(P,Q)$ that

$$W_{n+s} = -QW_{n-1}U_s + W_nU_{s+1}.$$

Thus,

$$W_{n+t} \equiv -QW_{n-1}U_t + W_nU_{t+1} \equiv -QW_{n-1} \cdot 0 + W_nU_{t+1} \equiv U_{t+1}W_n \pmod{m}$$

for all $n \geq 0$. □

Lemma 2.6. *Consider the Lucas sequence $U(P,Q)$, where $\gcd(P,Q) = 1$. Let p be a prime such that $p^i \parallel U_2 = P$, where $p^i \parallel U_2$ means that $p^i \mid U_2$, but $p^{i+1} \nmid U_2$. Let n be a positive integer. Then $p^{i+1} \mid U_{2n}$ if and only if $p \mid n$. In particular, $\gcd(U_{2n}/P, P) = 1$ if $\gcd(n, P) = 1$.*

Proof. This follows from Theorem X of [4]. □

Lemma 2.7. *Let $U(P,Q)$ be a Lucas sequence for which $2 \nmid \gcd(P,Q)$.*

(i) *$U(P,Q)$ is purely periodic modulo 2.*

(ii) *Suppose P is odd and Q is even. Then $2 \nmid U_n$ for $n \geq 1$.*

(iii) *Suppose P is even and Q is odd. Then $2 \mid U_n$ if and only $2 \mid n$. Moreover, $2 \mid D$.*

(iv) *Suppose P and Q are both odd. Then $2 \mid U_n$ if and only $3 \mid n$.*

Proof. This follows by inspection of $U(P,Q)$ modulo 2. □

Lemma 2.8. *Let $U(P,Q)$ be a Lucas sequence for which $3 \nmid \gcd(P,Q)$.*

(i) *$U(P,Q)$ is purely periodic modulo 3.*

(ii) *If $3 \mid Q$, then $3 \nmid U_n$ for $n \geq 1$.*

(iii) *If $3 \mid P$, then $\rho(3) = 2$ and $3 \mid U_n$ if and only if $2 \mid n$.*

(iv) *If $3 \nmid P$ and $Q \equiv -1 \pmod 3$, then $\rho(3) = 4$ and $3 \mid U_n$ if and only if $4 \mid n$.*

(v) *If $3 \nmid P$ and $Q \equiv 1 \pmod 3$, then $\rho(3) = 3$ and $3 \mid U_n$ if and only if $3 \mid n$. Moreover, $3 \mid D$.*

Proof. This follows by inspection of $U(P,Q)$ modulo 3. □

Lemma 2.9. *Let $U(P,Q)$ and $V(P,Q)$ be nondegenerate Lucas sequences such that $D > 0$. Then $|U_n|$ is increasing for $n \geq 2$ and $|V_n|$ is increasing for $n \geq 1$. Further, if $P > 0$, then $U_n > 0$ for $n \geq 1$ and $V_n > 0$ for $n \geq 0$. Moreover, if it is not the case that $|P| = -Q = 1$, then $|U_3| \geq 3$.*

This follows from Lemma 3 of [6] and Lemma 2.8 of [10].

The following corollary is immediate from Lemma 2.9.

Corollary 2.10. *Let $U(P,Q)$ be a nondegenerate LSFK such that $D > 0$. Then $\rho(U_n) = n$ for $n \geq 3$.*

3. Pseudoprimes Related to the Lucas Sequences $U(P,Q)$ and $V(P,Q)$

It follows from Theorem 2.4 (ii) and (iv) and the Binet formulas (2.3) and (2.4) that if N is an odd prime such that $\gcd(N, PQD) = 1$, then the following four congruences are all satisfied for the Lucas sequences $U(P,Q)$ and $V(P,Q)$ with discriminant D, where (D/N) denotes the Jacobi symbol (also see [2, pp. 1391, 1392, 1396]):

$$U_{N-(D/N)} \equiv 0 \pmod{N}, \tag{3.1}$$

$$U_N \equiv (D/N) \pmod{N}, \tag{3.2}$$

$$V_N \equiv P \pmod{N}, \tag{3.3}$$

$$V_{N-(D/N)} \equiv 2Q^{1-(D/N))/2} \pmod{N}. \tag{3.4}$$

It also occurs rarely that at least one of the four congruences (3.1)–(3.4) holds if N is a positive odd composite integer. We note that by [2, p. 1392], any two of the four congruences above imply the other two when N is a positive odd integer. We have the following definitions which are given in [16].

Definition 3.1. The positive odd composite integer N is called a *Lucas pseudoprime with parameters P and Q* if $\gcd(N, QD) = 1$ and congruence (3.1) holds. (We simply denote N as a Lucas pseudoprime if the parameters P and Q are understood.)

Definition 3.2. The positive odd composite integer N is called a *Lucas pseudoprime of the second kind with parameters P and Q* if $\gcd(N, QD) = 1$ and congruence (3.2) holds.

Definition 3.3. The positive odd composite integer N is called a *Dickson pseudoprime with parameters P and Q* if $\gcd(N, QD) = 1$ and congruence (3.3) holds.

Definition 3.4. The positive odd composite integer N is called a *Dickson pseudoprime of the second kind with parameters P and Q* if $\gcd(N, QD) = 1$ and congruence (3.4) holds.

For particular pairs of parameters P and Q it is known that there exist infinitely many odd composite integers N that satisfy each of the congruences (3.1)–(3.4) (see Theorem 1 of [14]). This gives rise to the following definition appearing in [16].

Definition 3.5. The positive odd composite integer N is called a *Frobenius pseudoprime with parameters P and Q* if $\gcd(N, PQD) = 1$ and congruences (3.1)–(3.4) all hold.

In [22] we found families of Lucas pseudoprimes and Frobenius pseudoprimes with parameters P and Q in which $P > 0$ and P is odd. In this paper, we will generalize these results by removing the restriction on P and allowing negative values of P as well as permitting P to be even. In both this paper and [22], we give special attention to the situation in which $Q = \pm 1$.

In addition, the definitions of the five types of pseudoprimes given below will be needed for our further work.

Definition 3.6. Let N be a positive odd composite integer and let a be a positive odd integer such that $\gcd(a, N) = 1$. Then N is called a *pseudoprime to the base a* if

$$a^{n-1} \equiv 1 \pmod{N}.$$

Definition 3.7. Let N be a positive odd composite integer and let a be a positive odd integer such that $\gcd(a, N) = 1$. Then N is called an *Euler pseudoprime to the base a* if

$$a^{(N-1)/2} \equiv 1 \pmod{N} \text{ if } (\mathrm{a/N}) = 1$$

or

$$a^{(N-1)/2} \equiv -1 \pmod{N} \text{ if } (\mathrm{a/N}) = -1.$$

It is clear that N is a pseudoprime to the base a if N is an Euler pseudoprime to the base a.

Remark 3.8. Let N be a positive odd integer and let $Q = \pm 1$. Then by the properties of the Jacobi symbol,

$$Q^{(N-1)/2} = (Q/N),$$

and N is always an Euler pseudoprime to the base Q.

Definition 3.9. Consider the LSFK $U(P, Q)$ and the LSSK $V(P, Q)$. The positive odd composite integer N is called an *Euler–Lucas pseudoprime with parameters P and Q* if $\gcd(N, QD) = 1$ and

$$U_{(N-(D/N))/2} \equiv 0 \pmod{N} \text{ if } (Q/N) = 1$$

or

$$V_{(N-(D/N))/2} \equiv 0 \pmod{N} \text{ if } (Q/N) = -1.$$

Definition 3.10. Consider the LSFK $U(P, Q)$ and the LSSK $V(P, Q)$. Let N be a positive odd composite integer such that $\gcd(N, QD) = 1$ and $N - (D/N) = 2^s d$, where d is odd. Then N is called a *strong Lucas pseudoprime with parameters P and Q* if either

(i) $U_d \equiv 0 \pmod{N}$, or

(ii) $V_{2^r d} \equiv 0 \pmod{N}$ for some r with $0 \leq r < s$.

Remark 3.11. It follows from Proposition 2.3 (i) and (iii) that Euler–Lucas pseudoprimes and strong Lucas pseudoprimes are Lucas pseudoprimes.

Theorem 3.12. *Consider the LSFK $U(P,Q)$. Let N be a positive odd composite integer N such that $\gcd(N,QD) = 1$. If N is a strong Lucas pseudoprime, then N is an Euler–Lucas pseudoprime.*

This is proved in Theorem 3 of [2].

Definition 3.13. The positive odd composite integer N is called a *super Lucas pseudoprime with parameters P and Q* if $\gcd(N,QD) = 1$ and each divisor of N greater than 1 is a prime or a Lucas pseudoprime with parameters P and Q. *Super Frobenius pseudoprimes* and *super strong Lucas pseudoprimes with parameters P and Q* are defined similarly.

Theorems 3.14 and 3.16 given below provide necessary and sufficient criteria for an odd composite integer N to be a strong Lucas pseudoprime or a super Lucas pseudoprime.

Theorem 3.14. *Consider the nondegenerate LSFK $U(P,Q)$. Let*

$$N = \prod_{i=1}^{s} p_i^{k_i}$$

be an odd composite integer such that $\gcd(N,PQD) = 1$. Suppose that N is a Lucas pseudoprime. Then $\rho(p_i^{k_i}) = p_i$ for $1 \leq i \leq s$. If N is also a strong Lucas pseudoprime, then $\nu_2(\rho(p_i)) = \nu_2(\rho(p_j))$ for $1 \leq i < j \leq s$, where $\nu_2(m) = i$ if $p^i \mid m$, but $p^{i+1} \nmid m$.

Conversely, if N is a Lucas pseudoprime such that $\nu_2(\rho(p_i)) = \nu_2(\rho(p_j))$ for $1 \leq i < j \leq s$, then N is in addition a strong Lucas pseudoprime.

This is proved in Proposition 2.18 of [22].

Corollary 3.15. *Consider the nondegenerate LSFK $U(P,Q)$. Let N be a Lucas pseudoprime for which $\gcd(N,QD) = 1$. Then, N is in addition a strong Lucas pseudoprime if $\rho(N)$ is odd.*

Proof. By Theorem 2.4 (vi), if $p \mid N$, then $\rho(p) \mid \rho(N)$. The result now follows from Theorem 3.14. □

Theorem 3.16. *Consider the nondegenerate LSFK $U(P,Q)$. Let $p_1, p_2, \ldots, p_s$ be distinct odd primes each relatively prime to QD such that $\rho(p_i^{m_i}) = \rho(p_i)$, but $\rho(p_i^{m_{i+1}}) \neq \rho(p_i)$ for $i \in \{1, \ldots, s\}$. Let*

$$h = \operatorname{lcm}(\rho(p_1), \rho(p_2), \ldots, \rho(p_s)).$$

Let N be an odd composite integer such that

$$N = \prod_{i=1}^{s} p_i^{k_i},$$

where $1 \leq k_i \leq m_i$. Then $\rho(N) = h$ and N is a super Lucas pseudoprime if and only if for each $i = 1, \ldots, s$,

$$p_i \equiv (D/p_i) \pmod{h}.$$

This is proved in Theorem 2.22 of [22].

Theorem 3.17. *Consider the nondegenerate LSFK $U(P,Q)$. Let*

$$N = \prod_{i=1}^{s} p_i^{k_i}$$

be an odd composite integer such that $\gcd(N, PQD) = 1$. Suppose that

$$\rho(p_i^{k_i}) = \rho(p_i) = \rho(p_j^{k_j}) = \rho(p_j) \quad \text{for } 1 \leq i < j \leq s.$$

Then N is a super strong Lucas pseudoprime. Additionally, if $Q = \pm 1$, then N is also a super Frobenius pseudoprime.

This follows from the proof of Proposition 2.23 in [22].

Theorem 3.18. *Consider the nondegenerate LSFK $U(P,Q)$. Suppose that N is an Euler–Lucas pseudoprime with parameters P and Q and that N is also an Euler pseudoprime to the base Q, where $\gcd(N, PQD) = 1$. Then N is a Frobenius pseudoprime.*

This is proved in Theorem 1 of [15].

Theorem 3.19. *Consider the nondegenerate LSFK $U(P,Q)$, where $Q = \pm 1$. Suppose that N is a positive odd composite integer such that $\gcd(N, PD) = 1$. If N is a strong Lucas pseudoprime, then N is a Frobenius pseudoprime.*

Proof. By Theorem 3.12, N is also an Euler–Lucas pseudoprime with parameters P and Q. By Remark 3.8, N is moreover an Euler pseudoprime to the base Q. It now follows from Theorem 3.18 that N is a Frobenius pseudoprime. □

Remark 3.20. In Sections 5 and 6, we investigate when $U_m(P,Q)$ or $U_{2m}(P,Q)/P$ is a Lucas pseudoprime with parameters P and Q for the situation in which m is an odd prime or m is a particular kind of pseudoprime with parameters P and Q. In Section 5, we consider the case in which m is an odd prime. In this case, we shall obtain sharper results by showing that there are fewer constraints on P and Q in order for $|U_m(P,Q)|$ or $|U_{2m}(P,Q)/P|$ to be a Lucas pseudoprime. Not only will we show that $|U_m(P,Q)|$ and $|U_{2m}(P,Q)/P|$ are Lucas pseudoprimes or strong Lucas pseudoprimes or Frobenius pseudoprimes, but we will also see that they are super pseudoprimes of these various types. The results in Section 6 generalize results obtained in [22] from the cases in which the parameter P is positive and odd to additional cases in which P is nonzero or even. In Section 6, we also obtain new examples of Lucas pseudoprimes with parameters P and Q by showing that if $Q = \pm 1$, then $U_{2m}(P,Q)/P$ is a Lucas pseudoprime for the case in which m is a Lucas pseudoprime, not just a Frobenius pseudoprime as was shown in Theorem 3.1 of [22] for the case in which $P > 0$ and P is odd. In Theorems 6.10 and 6.11, we show in addition that there are indeed infinitely many Lucas pseudoprimes with parameters P and $Q = \pm 1$ that are not Frobenius pseudoprimes.

4. Auxiliary Results

We will need the following results before presenting our prinipal results in Sections 5 and 6.

Theorem 4.1 (Carmichael)**.** *Consider the nondegenerate LSFK $U(P,Q)$, where* $\gcd(P,Q) = 1$ *and $D > 0$. Then U_n has a primitive prime divisor if $n \notin \{1, 2, 6, 12\}$.*

This is proved in Theorem XXIII of [4].

Corollary 4.2. *Consider the nondegenerate LSFK $U(P,Q)$, where* $\gcd(P,Q) = 1$ *and $D > 0$. Let $m \geq 5$ be a positive odd integer. Then the following hold:*

(i) *If m is composite, then U_m is composite;*

(ii) *U_{2m}/P is composite.*

Proof. (i) Let $a \geq 3$ be a proper divisor of the odd composite integer m. Then a is odd and $a \leq m$. It follows from Theorem 4.1 that U_a has a primitive prime divisor p_1 and U_m has a primitive prime divisor p_2. We now see that $p_1 p_2 \mid U_m$, and $|U_m|$ is composite.

(ii) By Theorem 4.1, U_m has a primitive prime divisor p_3 and U_{2m} has a primitive prime divisor p_4. Since $P = U_2$, we observe that $\gcd(P, p_3 p_4) = 1$. Consequently, $p_3 p_4 \mid U_{2m}/P$, and $|U_{2m}/P|$ is composite. □

Theorem 4.3 (Bilu, Hanrot, and Voutier)**.** *Let us consider the nondegenerate LSFK $U(P,Q)$, where $\gcd(P,Q)=1$. Then U_n has a primitive prime divisor if $n \neq 1,2,\ldots,8,10,12,13,18$, or 30.*

This is proved in Theorem C and Tables 1 and 3 of [3].

Theorem 4.4. *Consider the nondegenerate LSFK $U(P,Q)$, where $\gcd(P,Q)=1$, and suppose that ℓ is composite. Then $|U_\ell(P,Q)|$ is not composite only if $n \in \{4,6,8,9,10,15,25,26,65\}$. Furthermore, when $n \in \{6,8,10,15,25,26,65\}$, there are only finitely many ordered pairs (P,Q) such that $|U_\ell(P,Q)|$ or $|U_\ell(P,Q)/P|$ is not composite. All such cases are given below.*

(i) $U_6(\pm 1,2) = \pm 5$;

(ii) $U_8(\pm 1,2) = \pm 3$;

(iii) $U_{10}(\pm 1,2) = \pm 11$;

(iv) $U_{10}(\pm 1,3) = \pm 31$;

(v) $U_{10}(\pm 2,3)/2 = \pm 11$;

(vi) $U_{10}(\pm 12,55)/12 = \pm 3739$;

(vii) $U_{15}(\pm 1,2) = -89$;

(viii) $U_{25}(\pm 1,2) = -4049$;

(ix) $U_{25}(\pm 1,3) = 282001$;

(x) $U_{26}(\pm 1,2) = \pm 181$;

(xi) $U_{65}(\pm 1,2) = -335257649$.

In particular, if $|U_\ell(P,Q)|$ is not composite for $\ell \geq 6$ composite, then $D(P,Q) < 0$.

Proof. This follows by inspection from Theorems 2.7 and 2.14 of [20], Lemma 2.21 of [10], the proof of Theorem 3.1 of [10], and Tables 1 and 3 of [3]. □

Theorem 4.5 (Rotkiewicz)**.** *Consider the nondegenerate LSFK $U(P,Q)$, where $Q = \pm 1$. Then there exist infinitely many integers N of the form p_1p_2, where p_1 and p_2 are distinct odd primes, that are simultaneously strong Lucas pseudoprimes and Frobenius pseudoprimes with parameters P and Q.*

This is proved in Theorem 1 of [14].

Theorem 4.6 (Rotkiewicz)**.** *Consider the nondegenerate LSFK $U(P,Q)$, where $Q = \pm 1$. Let a and b be fixed coprime positive integers. Then in the arithmetic progression $ax+b$, there exist infinitely many integers N that are Frobenius pseudoprimes.*

This is proved in Theorem 2 of [14].

Theorem 4.7. *Consider the nondegenerate LSFK's $U(P,Q)$ and $U(-P,Q)$ and LSSK's $V(P,Q)$ and $V(-P,Q)$. Suppose that $N>1$ is a positive odd integer such that $\gcd(N,QD)=1$. Then the following hold:*

(i) *N is a Lucas pseudoprime with parameters P and Q if and only if N is a Lucas pseudoprime with parameters $-P$ and Q;*

(ii) *N is a Lucas pseudoprime of the second kind with parameters P and Q if and only if N is a Lucas pseudoprime of the second kind with parameters $-P$ and Q;*

(iii) *N is a Dickson pseudoprime with parameters P and Q if and only if N is a Dickson pseudoprime with parameters $-P$ and Q;*

(iv) *N is a Dickson pseudoprime of the second kind with parameters P and Q if and only if N is a Dickson pseudoprime of the second kind with parameters $-P$ and Q;*

(v) *N is a Frobenius pseudoprime with parameters P and Q if and only if N is a Frobenius pseudoprime with parameters $-P$ and Q.*

Proof. We see by Proposition 2.3 (vii) and (viii) that

$$U_n(-P,Q)=(-1)^{n+1}U_n(P,Q) \text{ and } V_n(-P,Q)=(-1)^nV_n(P,Q). \tag{4.1}$$

Moreover,

$$D=D(P,Q)=D(-P,Q)=P^2-4Q. \tag{4.2}$$

(i) Suppose that N is a Lucas pseudoprime with parameters P and Q. Then $N-(D/N)$ is even and

$$U_{N-(D(P,Q)/N)}\equiv 0\equiv U_{N-(D(-P,Q)/N)} \pmod N$$

by (4.1) and (4.2), and N is also a Lucas pseudoprime with parameters $-P$ and Q.

(ii) Suppose that N is a Lucas pseudoprime of the second kind with parameters P and Q. Then by (4.1) and (4.2),

$$U_N(P,Q)\equiv (D(P,Q)/N)\equiv U_N(-P,Q)\equiv (D(-P,Q)/N) \pmod N,$$

and N is also a Lucas pseudoprime of the second kind with parameters $-P$ and Q.

(iii) Suppose that N is a Dickson pseudoprime with parameters P and Q. Then by (4.1),

$$V_N(P,Q)\equiv P\equiv -V_N(-P,Q) \pmod N.$$

Hence,

$$V_N(-P,Q) \equiv -P \pmod{N},$$

and N is moreover a Dickson pseudoprime with parameters $-P$ and Q.

(iv) Suppose that N is a Dickson pseudoprime of the second kind with parameters P and Q. Then by (4.1) and (4.2),

$$V_{N-(D(P,Q)/N)} \equiv 2Q^{(1-(D/N))/2} \equiv V_{N-(D(-P,Q)/N)} \pmod{N}$$

and N is furthermore a Dickson pseudoprime of the second kind with parameters $-P$ and Q.

(v) This follows from parts (i)–(iv). □

Remark 4.8. Consider the nondegenerate LSFK's $U(P,Q)$ with discriminant D. In view of Theorem 4.7, we will always just treat the case in which $P > 0$ in our subsequent proofs that numbers of the form $U_m(P,Q)$ or $U_{2m}(P,Q)/P$ are pseudoprimes of various types. We observe by Lemma 2.9 and Theorem 4.7 that if $P > 0$ and $D > 0$, then both $U_n(P,Q)$ and $V_n(P,Q)$ are greater than 0 for all $n \geq 1$.

Lemma 4.9. *Consider the LSFK $U(P,Q)$ with discriminant $D = P^2 - 4Q$ such that $\gcd(P,Q) = 1$. Then $\gcd(P,D) \mid 4$. Moreover, if D' is odd and $D' \mid D$, then $\gcd(P,D') = 1$.*

Proof. Since $\gcd(P,Q) = 1$, it follows that $\gcd(P,D) \mid 4$. As D' is odd and $D' \mid D$, we see that $\gcd(D',P) = 1$. □

Lemma 4.10. *Consider the LSFK $U(P,Q)$ with discriminant $D = P^2 - 4Q$ such that $\gcd(P,Q) = 1$. Suppose that $D = 2^i D_0$, where $i \geq 0$ and D_0 is odd. Let m be an odd integer such that $\gcd(m, PQD) = 1$ and it is the case that $3 \nmid m$ if $P \equiv Q \equiv 1 \pmod{2}$. Let $N_1 = U_m$ and $N_2 = U_{2m}/P$. Then N_1 and N_2 are both odd integers and $\gcd(N_1, D) = \gcd(N_2, D) = 1$.*

Proof. By Proposition 2.3 (v), U_{2m}/P is an integer. By Lemmas 2.6 and 2.7, N_1 and N_2 are both odd. We observe by (2.3) that

$$\begin{aligned} N_1 = U_m(P,Q) &= \sum_{k=0}^{(m-1)/2} \binom{m}{2k+1} \frac{1}{2^{m-1}} P^{m-(2k+1)} D^k \\ &= m\frac{1}{2^{m-1}} P^{m-1} + \binom{m}{3} \frac{1}{2^{m-1}} P^{m-3} D + \dots \\ &\quad + \binom{m}{m-2} \frac{1}{2^{m-1}} P^2 D^{(m-3)/2} + \frac{1}{2^{m-1}} D^{(m-1)/2} \end{aligned} \tag{4.3}$$

and

$$N_2 = U_{2m}(P,Q)/P = \sum_{k=0}^{m-1} \binom{2m}{2k+1} \frac{1}{2^{2m-1}} P^{2m-2k-2} D^k$$
$$= m\frac{1}{2^{2m-2}} P^{2m-2} + \binom{2m}{3} \frac{1}{2^{2m-1}} P^{2m-4} D + \dots$$
$$+ \binom{2m}{2m-3} \frac{1}{2^{2m-1}} P^2 D^{m-2} + \frac{1}{2^{2m-1}} D^{m-1}. \tag{4.4}$$

Noting that D_0 is odd, we see by (4.3) and (4.4) that

$$N_1 = U_m \equiv mP^{m-1}(2^{-1})^{m-1} \pmod{D_0} \tag{4.5}$$

and

$$N_2 = U_{2m}/P \equiv mP^{2m-2}(2^{-1})^{2m-2} \pmod{D_0}. \tag{4.6}$$

Noticing that $\gcd(P, D_0) = 1$ by Lemma 4.9, $\gcd(m, D) = 1$ by hypothesis, and D_0 is odd, we obtain from (4.5) and (4.6) that

$$\gcd(N_1, D_0) = \gcd(N_2, D_0) = 1. \tag{4.7}$$

Since N_1 and N_2 are both odd and $D = 2^i D_0$, we find from (4.7) that $\gcd(N_1, D) = \gcd(N_2, D) = 1$. □

5. Lucas Pseudoprimes of the Form $|U_p(P,Q)|$ or $|U_{2p}(P,Q)/P|$

Theorem 5.1 below shows that given the LSFK $U(P,Q)$, where $\gcd(P,Q) = 1$, we have that $|U_p|$ is a super strong Lucas pseudoprime when $|U_p|$ is composite.

Theorem 5.1. *Let $U(P,Q)$ be a nondegenerate LSFK for which $\gcd(P,Q) = 1$. Let $p \geq 5$ be a prime such that $\gcd(p, PQD) = 1$. Let $N_1 = |U_p(P,Q)|$. Then N_1 is a super strong Lucas pseudoprime if N_1 is composite. Moreover, if $Q = \pm 1$ and N_1 is composite, then N_1 is both a super strong Lucas pseudoprime and a super Frobenius pseudoprime. Furthermore, $|U_p(P,Q)|$ is composite if one of the following holds:*

(i) *Q is a perfect square and $D > 0$. In this case, $|U_p(P,Q)|$ has at least two distinct prime divisors.*

(ii) *If p and $2p+1$ are both primes such that $|U_p(P,Q)| > 2p+1$ and*

$$(D/2p+1) = (Q/2p+1) = 1, \tag{5.1}$$

then $2p+1 \mid |U_p(P,Q)|$. Moreover, if $D > 0$ and (5.1) holds, then $|U_p(P,Q)| > 2p+1$ if it is not the case that $(p,P,Q) = (5, \pm 1, -2)$. Furthermore, if $D < 0$, then there exists a constant C_1 such that $|U_p(P,Q)| > 2p+1$ if $p \geq C_1$.

(iii) *If p and $2p-1$ are both primes such that $|U_p(P,Q)| > 2p-1$,*

$$(D/2p-1) = -1 \quad \textit{and} \quad (Q/2p-1) = 1, \tag{5.2}$$

then $2p-1 \mid |U_p(P,Q)|$. Moreover, if $D > 0$ and (5.2) holds, then $|U_p(P,Q)| > 2p-1$ if it is not the case that $(p,P,Q) = (7,\pm 1,-1)$. Moreover, if $D < 0$, then there exists a constant C_2 such that $|U_p(P,Q)| > 2p+1$ if $p \geq C_2$.

(iv) *Let $U(P_1,Q_1)$ be a nondegenerate LSFK for which $\gcd(P_1,Q_1) = 1$. Let D_1 be the discriminant of $U(P_1,Q_1)$. Let $k \geq 2$ be an integer such that $\gcd(D_1,k) = 1$. Let p be a prime such that $p \nmid kD_1$, $p \geq 5$ if $D > 0$, $p \geq 11$ if $D < 0$, and $p \neq 13$ if $P = \pm 1$, $Q = 2$. Let $P = \pm V_k(P_1,Q_1)$ and $Q = Q_1^k$. Then $\gcd(P,Q) = 1$ and U(P, Q) is a nondegenerate LSFK with discriminant $D = D_1 U_k^2$.*

Moreover, $|U_p(P,Q)|$ is a super strong Lucas pseudoprime with parameters P and Q that is also a super Frobenius pseudoprime with parameters P and Q if $Q_1 = \pm 1$. Let $\omega(k)$ denote the number of distinct prime divisors of k and let $\tau(k)$ denote the number of positive divisors of k. Then $|U_p(P,Q)|$ has at least $\tau(k) \geq 2^{\omega(k)}$ positive divisors.

Proof. It follows from Theorem 3.17 that N_1 is a super strong Lucas pseudoprime if N_1 is composite, while N_1 is both a super strong Lucas pseudoprime and a super Frobenius pseudoprime if $Q = \pm 1$ and N_1 is composite. Part (i) follows from [13] and [17].

Parts (ii) and (iii) follow from Theorem 2 in [18], and Theorem 3.13 in [21]. Part (iv) follows from Tables 1 and 3 of [3] and the proof of Theorem 3.17 of [22]. □

Example 5.2. Given the LSFK $U(P,Q)$, where $\gcd(P,Q) = 1$, the indices n for which $U_n(P,Q)$ are primes appear to be rare. For example, consider the Fibonacci sequence $U(1,1)$. It is shown in the website [24] that there are 34 known Fibonacci primes whose indices are

3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83, 131, 137, 359, 431, 433, 449, 509, 569, 571, 2971, 4723, 5387, 9311, 9677, 14431, 25561, 30757, 35999, 37511, 50833, 81839, 104911.

By comparison, the number of primes less than or equal to 104911 is $\pi(104911) = 10016$.

Theorem 5.3 below shows that if $p \geq 5$ and $U(P,Q)$ is a Lucas sequence for which $\gcd(P,Q) = 1$, then $|U_{2p}/P|$ is a super Lucas pseudoprime with ten exceptions.

Theorem 5.3. *Consider the nondegenerate LSFK $U(P,Q)$, where $\gcd(P,Q) = 1$. Suppose that $p \geq 5$ and $\gcd(p,PQD) = 1$. Then $N_2 = |U_{2p}/P|$ is a super Lucas*

pseudoprime if it is not the case that $(p, P, Q) = (5, \pm 1, 2)$ *or* $(5, \pm 1, 3)$ *or* $(5, \pm 2, 3)$ *or* $(5, \pm 12, 55)$ *or* $(13, \pm 1, 2)$. *Moreover,*

$$|U_{10}(\pm 1, 2)| = 11, |U_{10}(\pm 1, 3)| = 31, |U_{10}(\pm 2, 3)/2| = 11,$$
$$|U_{10}(\pm 12, 55)/12| = 3739, |U_{26}(\pm 1, 2)| = 181, \tag{5.3}$$

which are all primes.

Proof. By Proposition 2.3 (v), $P \mid U_{2p}$. We note that $U_1 = 1$, $U_2 = P$, and $\gcd(p, P) = 1$. It then follows from Lemma 2.6, Proposition 2.3 (iii), and Theorem 2.4 (i) that the only prime divisors of $N_2 = |U_{2p}/P|$ are the primitive prime divisors of U_p and U_{2p}. We now show that if $|U_{2p}/P|$ is composite, then $N_2 = |U_{2p}/P|$ is a super Lucas pseudoprime. Since $N_2 \mid U_{2p}$, it follows that $\rho(N_2) \mid 2p$. Suppose that q_1 is a primitive prime divisor of U_p. By Theorem 2.4 (ii), (iii), and (x), $q_1 \equiv (D/q_1) \pmod{p}$, where $(D/q_1) = \pm 1$, since $p \nmid D$. As $q_1 - (D/q_1)$ is even and p is odd, it follows that $q_1 \equiv (D/q_1) \pmod{2p}$. Further by Theorem 2.4 (ii), (iii), and (x), if q_2 is a primitive prime divisor of U_{2p}, then $q_2 \equiv (D/q_2) \pmod{2p}$, where $(D/q_2) = \pm 1$, since $2p = \rho(q_2)$ is not a divisor of D. We now see by Theorem 3.16 that N_2 is a super Lucas pseudoprime if $|U_{2p}/P|$ is composite.

We now suppose that U_p and U_{2p} both have primitive prime divisors. Since $U_2 = P$, it follows by Proposition 2.3 (iii) and Theorem 2.4 (viii) that $N_2 = |U_{2p}/P|$ is composite and thus is a super Lucas pseudoprime. Now consider the situation in which $p \geq 11$ and $(p, P, Q) \neq (13, \pm 1, 2)$. It follows by Theorem 4.3 and Tables 1 and 3 of [3] that $U_p(P, Q)$ has a primitive divisor p_1 and $U_{2p}(P, Q)$ has a primitive divisor p_2. We now see by our above argument that $|U_{2p}/P|$ is a super Lucas pseudoprime in this case.

We finally suppose that $p = 5$ or 7 or it is the case that $p = 13$, $P = \pm 1$, and $Q = 2$. By or discussion above, $|U_{2p}/P|$ is then a super Lucas pseudoprime if it is composite. We now observe by Theorem 4.3, Tables 1 and 3 of [3], and the proof of Theorem 3.1 of [10] that $|U_{2p}/P|$ is composite if it is not the case that (5.3) holds. □

Remark 5.4. In Theorem 2 of [7], Kiss showed that there is a constant C dependent on P and Q such that $|U_{2p}/P|$ is a super Lucas pseudoprime if $p > C$. In Theorem 5.3 above, we demonstrated that the constant C is an absolute constant, not dependent on P and Q, and that we can take $C = 13$.

6. Lucas Pseudoprimes of the Form $U_m(P, Q)$ or $U_{2m}(P, Q)/P$

Lemma 6.1 below will be a key tool in proving five of our main results, Theorems 6.2, 6.3, 6.5, 6.6, and 6.10.

Lemma 6.1. *Let $U(P,Q)$ be a nondegenerate LSFK for which $\gcd(P,Q)=1$ and $D>0$. Let $m>1$ be an odd integer such that $\gcd(m,PQD)=1$, and $3\nmid m$ if $P\equiv Q\equiv 1 \pmod 2$. Let $N_1=U_m$ and $N_2=U_{2m}/P$. Then N_1 and N_2 are both positive odd integers such that $\gcd(N_1N_2,PQD)=1$. Further, if m is composite, then N_1 and N_2 are both composite. Moreover, $(D/m)=(D/N_1)=(D/N_2)$ if any of the following three conditions are satisfied:*

(i) $P\equiv 1 \pmod 2$;

(ii) $P\equiv 0 \pmod 4$ *and* $Q\equiv -1 \pmod 4$;

(iii) $P\equiv 2 \mod 4$ *and* $Q\equiv -1 \pmod 8$.

Proof. By Theorem 4.7, we can assume that $P>0$. We note that $P=U_2$ and m is odd. It now follows by Theorem 2.4 (vii) and (ix), Lemmas 2.6, 2.7, 2.9, and 4.10 that both N_1 and N_2 are positive odd integers such that $\gcd(N_1N_2,PQD)=1$. By Corollary 4.2, N_1 and N_2 are both composite if m is composite. By (2.3),

$$\begin{aligned} N_1=U_m(P,Q)&=\sum_{k=0}^{(m-1)/2}\binom{m}{2k+1}\frac{1}{2^{m-1}}P^{m-(2k+1)}D^k\\ &=m\frac{1}{2^{m-1}}P^{m-1}+\binom{m}{3}\frac{1}{2^{m-1}}P^{m-3}D+\dots\\ &\quad+\binom{m}{m-2}\frac{1}{2^{m-1}}P^2D^{(m-3)/2}+\frac{1}{2^{m-1}}D^{(m-1)/2} \end{aligned} \tag{6.1}$$

and

$$\begin{aligned} N_2=U_{2m}(P,Q)/P&=\sum_{k=0}^{m-1}\binom{2m}{2k+1}\frac{1}{2^{2m-1}}P^{2m-2k-2}D^k\\ &=m\frac{1}{2^{2m-2}}P^{2m-2}+\binom{2m}{3}\frac{1}{2^{2m-1}}P^{2m-4}D+\dots\\ &\quad+\binom{2m}{2m-3}\frac{1}{2^{2m-1}}P^2D^{m-2}+\frac{1}{2^{2m-1}}D^{m-1}. \end{aligned} \tag{6.2}$$

(i) Suppose that $P\equiv 1 \pmod 2$ and $3\nmid m$ if $Q\equiv 1 \pmod 2$. Then $D=P^2-4Q\equiv 1 \pmod 4$. Then by (6.1) and (6.2), we obtain

$$N_1=U_m\equiv m(2^{-1}P)^{m-1} \pmod D \tag{6.3}$$

and

$$N_2=U_{2m}/P\equiv m(2^{-1}P)^{2(m-1)} \pmod D. \tag{6.4}$$

It now follows from (6.3), (6.4), Lemma 4.10, and the properties of the Jacobi symbol that

$$(D/N_1)=(N_1/D)=(m/D)((2^{-1}P)^{m-1}/D)=(m/D)=(D/m)$$

and

$$(D/N_2) = (N_2/D) = (m/D)((2^{-1}P)^{2(m-1)}/D) = (m/D) = (D/m).$$

(ii) Suppose that $P \equiv 0 \pmod 4$ and $Q \equiv -1 \pmod 4$. Let $P = 4i$ and $Q = 4j - 1$. Then

$$D = P^2 - 4Q = 16i^2 - 16j + 4 \equiv 4 \pmod{16}.$$

Hence, $D = 4D_1$, where $D_1 \equiv 1 \pmod 4$. It now follows from (6.1) and (6.2) that

$$N_1 = U_m \equiv m(2^{-1}P)^{m-1} \pmod{D_1}$$

and

$$N_2 = U_{2m}/P \equiv m(2^{-1}P)^{2(m-1)} \pmod{D_1}.$$

Since N_1 and N_2 are odd, we see by Lemma 4.10, (6.1), and (6.2) that

$$\begin{aligned}(D/N_1) &= (4D_1/N_1) = (4/N_1)(D_1/N_1) = (D_1/N_1) = (N_1/D_1)\\ &= (m/D_1)((2^{-1}P)^{m-1}/D_1) = (m/D_1) = (D_1/m)\\ &= (4/m)(D_1/m) = (4D_1/m) = (D/m)\end{aligned}$$

and

$$\begin{aligned}(D/N_2) &= (4D_1/N_2) = (4/N_2)(D_1/N_2) = (D_1/N_2) = (N_2/D_1)\\ &= (m/D_1)((2^{-1}P)^{2(m-1)}/D_1) = (m/D_1)\\ &= (D_1/m) = (4D_1/m) = (D/m).\end{aligned}$$

(iii) Suppose that $P \equiv 2 \pmod 4$ and $Q \equiv -1 \pmod 8$. Let $P = 4i + 2$ and $Q = 8j - 1$. Then

$$P^2 = 16(i^2 + i) + 4 \equiv 4 \pmod{32} \tag{6.5}$$

and

$$D = P^2 - 4Q = 16(i^2 + i) - 32j + 8 \equiv 8 \pmod{32}.$$

Therefore,

$$D = 8D_2, \tag{6.6}$$

where $D_2 \equiv 1 \pmod 4$. We observe by (6.1) and (6.2) that

$$N_1 = U_m \equiv m(2^{-1}P)^{m-1} \pmod{D_2} \tag{6.7}$$

and

$$N_2 = U_{2m}/P \equiv m(2^{-1}P)^{2(m-1)} \pmod{D_2}. \tag{6.8}$$

It now follows by (6.7), (6.8), and Lemma 4.10 that

$$\begin{aligned}(D/N_1) &= (8D_2/N_1) = (2/N_1)(4/N_1)(D_2/N_1) = (2/N_1)(D_2/N_1) = (2/N_1)(N_1/D_2)\\ &= (2/N_1)(m/D_2)((2^{-1}P)^{m-1}/D_2) = (2/N_1)(m/D_2)\\ &= (2/N_1)(D_2/m) = (2/N_1)(4/m)(D_2/m) = (2/N_1)(4D_2/m)\end{aligned} \tag{6.9}$$

and

$$\begin{aligned}(D/N_2) &= (8D_2/N_2) = (2/N_2)(4/N_2)(D_2/N_2) = (2/N_2)(D_2/N_2) = (2/N_2)(N_2/D_2)\\ &= (2/N_2)(m/D_2)((2^{-1}P)^{2(m-1)}/D_2) = (2/N_2)(m/D_2)\\ &= (2/N_2)(D_2/m) = (2/N_2)(4/m)(D_2/m) = (2/N_2)(4D_2/m). \qquad (6.10)\end{aligned}$$

Inspecting $U(P,Q)$ modulo 8 and making use of the fact that $P^2 \equiv 4 \pmod 8$, we find that $\lambda(8) = 8$ and the initial terms of $U(P,Q) \pmod 8$ are

$$0, 1, P, 5, 6P, 5, 3P, 1, 4P \equiv 0, 1, P, \ldots \pmod 8. \qquad (6.11)$$

From (6.11), we see that

$$\text{if } m \equiv 1 \text{ or } 7 \pmod 8, \text{ then } N_1 = U_m(P,Q) \equiv 1 \pmod 8,$$

while

$$\text{if } m \equiv 3 \text{ or } 5 \pmod 8, \text{ then } N_1 = U_m(P,Q) \equiv 5 \pmod 8.$$

It then follows by the properties of the Jacobi symbol that

$$(2/m) = (2/N_1). \qquad (6.12)$$

We now see by (6.9), (6.12), and (6.6) that

$$(D/N_1) = (2/N_1)(4D_2/m) = (2/m)(4D_2/m) = (8D_2/m) = (D/m),$$

as desired.

We finish our proof by showing that $(D/N_2) = (D/m)$. Let

$$m = 8r + s, \text{ where } s \in \{1, 3, 5, 7\}.$$

Then

$$2m = 16r + 2s, \text{ where } 2s \in \{2, 6, 10, 14\}.$$

Since $Q \equiv -1 \pmod 8$, we have that $Q \equiv -1 \pmod{16}$ or $Q \equiv -9 \pmod{16}$. We first consider the case in which $Q \equiv -1 \pmod{16}$. Examining $U(P,Q)$ modulo 16 and making use of the fact that $P^2 \equiv 4 \pmod{16}$, we find that $\lambda(16) = 16$ and the first 19 terms of $U(P,Q) \pmod{16}$ are

$$\begin{aligned}&U_0 \equiv 0,\ U_1 \equiv 1,\ U_2 \equiv P,\ U_3 \equiv 5,\ U_4 \equiv 6P,\ U_5 \equiv 13,\ U_6 \equiv 3P,\ U_7 \equiv 9,\\ &U_8 \equiv 12P,\ U_9 \equiv 9,\ U_{10} \equiv 5P,\ U_{11} \equiv 13,\ U_{12} \equiv 2P,\ U_{13} \equiv 5,\ U_{14} \equiv 7P,\\ &U_{15} \equiv 1,\ U_{16} \equiv 8P \equiv 0,\ U_{17} \equiv 1,\ U_{18} \equiv P \pmod{16}. \qquad (6.13)\end{aligned}$$

It now follows from (6.13) that

$$\text{if } Q \equiv -1 \pmod{16}, \text{ then } U_{2m} \equiv sP \pmod{16}. \qquad (6.14)$$

Since $P \equiv 2 \pmod 4$, we obtain from (6.14) that

$$\text{if } Q \equiv -1 \pmod{16}, \text{ then } N_2 = U_{2m}/P \equiv s \equiv m \pmod 8. \tag{6.15}$$

We now treat the case in which $Q \equiv -9 \pmod{16}$. Inspecting $U(P,Q)$ modulo 16, we see that $\lambda(16) = 16$ and the first 19 terms of $U(P,Q) \pmod{16}$ are

$$\begin{aligned} &U_0 \equiv 0,\ U_1 \equiv 1,\ U_2 \equiv P,\ U_3 \equiv 13,\ U_4 \equiv 6P,\ U_5 \equiv 13,\ U_6 \equiv 3P,\ U_7 \equiv 1,\\ &U_8 \equiv 12P,\ U_9 \equiv 9,\ U_{10} \equiv 5P,\ U_{11} \equiv 5,\ U_{12} \equiv 2P,\ U_{13} \equiv 5,\ U_{14} \equiv 7P,\\ &U_{15} \equiv 9,\ U_{16} \equiv 8P \equiv 0,\ U_{17} \equiv 1, U_{18} \equiv P \pmod{16}. \end{aligned} \tag{6.16}$$

We find by (6.16) that

$$\text{if } Q \equiv -9 \pmod{16}, \text{ then } U_{2m} \equiv sP \pmod{16}. \tag{6.17}$$

It now follows from (6.17) that

$$\text{if } Q \equiv -9 \pmod{16}, \text{ then } N_2 = U_{2m}/P \equiv s \equiv m \pmod 8. \tag{6.18}$$

By (6.15) and (6.18), we obtain that

$$(2/m) = (2/N_2). \tag{6.19}$$

We now observe by (6.10), (6.19), and (6.6) that

$$(D/N_2) = (2/N_2)(4D_2/m) = (2/m)(4D_2/m) = (8D_2/m) = (D/m).$$

The proof is now complete. □

We are now ready for the proofs of Theorems 6.2 and 6.3, whose statements are given below.

Theorem 6.2. *Let $U(P,Q)$ be a nondegenerate LSFK for which $\gcd(P,Q) = 1$ and $D > 0$. Let $m \geq 5$ be an odd prime or a Lucas pseudoprime of the second kind such that $\gcd(m, PQD) = 1$ and $3 \nmid m$ if $P \equiv Q \equiv 1 \pmod 2$. Let $N_1 = U_m$. Suppose that N_1 is composite if m is an odd prime. Then N_1 is a strong Lucas pseudoprime if any of the following three conditions are satisfied:*

(i) $P \equiv 1 \pmod 2$;

(ii) $P \equiv 0 \pmod 4$ *and* $Q \equiv -1 \pmod 4$;

(iii) $P \equiv 2 \pmod 4$ *and* $Q \equiv -1 \pmod 8$.

Proof. By Lemma 6.1, N_1 is a positive odd composite integer. Since m is odd, it will then follow from Corollary 3.15 that N_1 is a strong Lucas pseudoprime if we

can show that N_1 is a Lucas pseudoprime. Noting that m is an odd prime or a Lucas pseudoprime of the second kind, we find that

$$U_m \equiv (D/m) \pmod{m}. \tag{6.20}$$

We see by (6.20) that

$$m \mid U_m - (D/m). \tag{6.21}$$

It now follows by Proposition 2.3 (iii) and (6.21) that

$$N_1 = U_m \mid U_{N_1-(D/m)}.$$

It will then follow that N_1 is a Lucas pseudoprime if we can show that

$$(D/m) = (D/N_1). \tag{6.22}$$

However, (6.22) holds by Lemma 6.1. The proof is now established. □

Theorem 6.2 was proved in [22] for the case in which $P > 0$ and P is odd.

Theorem 6.3. *Let $U(P,Q)$ be a nondegenerate LSFK for which $Q = \pm 1$. Then $D > 0$. Let $m \geq 5$ be an odd prime or a Lucas pseudoprime of the second kind such that $\gcd(m, PD) = 1$ and $3 \nmid m$ if $P \equiv 1 \pmod 2$. Let $N_1 = U_m$. Then $\gcd(N_1, PD) = 1$ and $3 \nmid N_1$ if $P \equiv 1 \pmod 2$. Suppose that N_1 is composite if m is an odd prime and $Q = -1$. Then N_1 is a strong Lucas pseudoprime and a Frobenius pseudoprime such that $\gcd(N_1, PD) = 1$ and $3 \nmid N_1$ if $P \equiv Q \equiv 1 \pmod 2$, if any of the following two conditions are satisfied:*

(i) $P \equiv 1 \pmod 2$;

(ii) $P \equiv 0 \pmod 2$ *and* $Q = -1$.

Proof. By Remark 2.2, $D > 0$. By Corollary 4.2 (i) and Theorem 5.1 (i), $N_1 = U_m$ is composite. It now follows from Theorem 6.2 that N_1 is a strong Lucas pseudoprime if (i) or (ii) holds. We see by Lemma 6.1 that $\gcd(N_1, PD) = 1$. We also see from Lemma 2.8 that $3 \nmid N_1$ if $P \equiv 1 \pmod 2$. Since $Q = \pm 1$, it now follows from Theorem 3.19 that N_1 is also a Frobenius pseudoprime if (i) or (ii) holds. □

Theorem 6.3 was proved in [22] for the case in which $P > 0$ and P is odd.

Remark 6.4. Consider the nondegenerate LSFK $U(P,Q)$, where $Q = \pm 1$. Using Theorem 6.3, we can explicitly find infinitely many Frobenius pseudoprimes that are also strong Lucas pseudoprimes with parameters P and Q. Let m be a Lucas pseudoprime of the second kind such that $\gcd(m, PD) = 1$ and $3 \nmid m$ if $P \equiv 1 \pmod 2$. Let $M_1 = U_m$ and $M_{i+1} = U_{M_i}$ for $i \geq 1$. Then by Theorem 6.3, M_i is a Frobenius pseudoprime for $i \geq 1$.

Theorem 6.5. *Let $U(P,Q)$ be a nondegenerate LSFK for which $\gcd(P,Q) = 1$ and $D > 0$. Let $m \geq 5$ be an odd prime or a Frobenius pseudoprime such that $\gcd(m, PQD) = 1$ and $3 \nmid m$ if $P \equiv Q \equiv 1 \pmod 2$. Let $N_2 = U_{2m}/P$. Then N_2 is a Lucas pseudoprime if any of the following three conditions are satisfied:*

(i) $P \equiv 1 \pmod 2$*;*

(ii) $P \equiv 0 \pmod 4$ *and* $Q \equiv -1 \pmod 4$*;*

(iii) $P \equiv 2 \pmod 4$ *and* $Q \equiv -1 \pmod 8$*.*

Proof. By Lemma 6.1, N_2 is a positive odd composite integer. Since m is odd, it follows from Proposition 2.3 (vi) that $P \mid V_m$. By Proposition 2.3 (i),

$$N_2 = U_{2m}/P = U_m V_m/P. \tag{6.23}$$

Noting that m is an odd prime or a Frobenius pseudoprime such that $\gcd(m, D) = 1$, we find that

$$U_m \equiv (D/m) \pmod m \text{ and } V_m \equiv P \pmod m. \tag{6.24}$$

Therefore, by (6.23) and (6.24),

$$U_{2m}/P = U_m(V_m/P) \equiv (D/m)PP^{-1} \equiv (D/m) \pmod m. \tag{6.25}$$

Then by (6.25),

$$m \mid U_{2m}/P - (D/m) \text{ and } 2 \mid U_{2m}/P - (D/m), \tag{6.26}$$

because U_{2m}/P is odd. Consequently, by (6.26),

$$2m \mid U_{2m}/P - (D/m). \tag{6.27}$$

Therefore, by Proposition 2.3 (iii) and (6.27),

$$N_2 = U_{2m}/P \mid U_{2m} \mid U_{N_2-(D/m)}.$$

To complete the proof, we need to show that

$$(D/m) = (D/N_2). \tag{6.28}$$

However, (6.28) holds by Lemma 6.1. Theorem 6.5 now follows. □

Theorem 6.5 was proved in [22] for the case in which $P > 0$ and P is odd.

Theorem 6.6 improves on Theorem 6.5 when $Q = \pm 1$ by showing that in this case, $U_{2m}(P,Q)/P$ is a Lucas pseudoprime when m is an odd prime or a Lucas pseudoprime rather than requiring that m be an odd prime or a Frobenius pseudoprime. As mentioned above in Remark 3.20, Theorem 6.11 below shows that there are infinitely many Lucas pseudoprimes that are not Frobenius pseudoprimes.

Theorem 6.6. *Let $U(P,Q)$ be a nondegenerate LSFK for which $Q = \pm 1$. Then $D > 0$. Let $m \geq 5$ be an odd prime or a Lucas pseudoprime such that $\gcd(m, PD) = 1$ and $3 \nmid m$ if $P \equiv 1 \pmod 2$. Let $N_2 = U_{2m}/P$. Then $\gcd(N_2, PD) = 1$ and $3 \nmid N_2$ if $P \equiv 1 \pmod 2$. Further, N_2 is a Lucas pseudoprime if either of the following two conditions is satisfied:*

(i) $P \equiv 1 \pmod 2$*;*

(ii) $P \equiv 0 \pmod 2$ *and* $Q = -1$.

Proof. By Remark 2.2, $D > 0$. By Corollary 4.2 (ii), $N_2 = U_{2m}/P$ is composite. Moreover, by Lemma 6.1, N_2 is a positive odd integer such that $\gcd(N_2, PD) = 1$. Since m is odd, it follows from Proposition 2.3 (vi) that $P \mid V_m$. By Proposition 2.3 (i),

$$U_{2m}/P = U_m(V_m/P).$$

To complete the proof, we need to show that

$$U_{N_2-(D/N_2)} \equiv 0 \pmod{N_2}. \tag{6.29}$$

Let $r = m - (D/m)$. Then r is even and by Proposition 2.3 (ii),

$$U_{r+1}^2 - U_r U_{r+2} = Q^r = 1. \tag{6.30}$$

Since m is an odd prime or a Lucas pseudoprime,

$$U_r \equiv 0 \pmod{m}. \tag{6.31}$$

Thus, by (6.30) and (6.31),

$$U_{r+1}^2 \equiv 1 \pmod{m}.$$

Let p be a prime such that $p^i \parallel m$ for some $i \geq 1$. Then

$$U_{r+1}^2 \equiv 1 \pmod{p^i}. \tag{6.32}$$

Since there exist primitive roots modulo p^i, we have that

$$U_{r+1} \equiv \varepsilon \pmod{p^i}, \tag{6.33}$$

where $\varepsilon \in (-1, 1)$. Thus, by (6.33) and Lemma 2.5,

$$V_r \equiv U_{r+1}V_0 \equiv \varepsilon V_0 \equiv 2\varepsilon \pmod{p^i}, \quad V_{r+1} \equiv U_{r+1}V_1 \equiv \varepsilon V_1 \equiv P\varepsilon \pmod{p^i}. \tag{6.34}$$

Therefore, by (6.30), (6.32), (6.33) and the recursion relation (1.1) defining both $U(P,Q)$ and $V(P,Q)$, we have that

$$-QU_{r-1} = U_{r+1} - PU_r \equiv \varepsilon - P \cdot 0 \equiv \varepsilon \pmod{p^i} \tag{6.35}$$

and

$$-QV_{r-1} = V_{r+1} - PV_r \equiv P\varepsilon - 2P\varepsilon \equiv -P\varepsilon \pmod{p^i}. \tag{6.36}$$

Since $-Q = \pm 1$, we see by (6.35) and (6.36) that

$$U_{r-1} \equiv -Q\varepsilon \pmod{p^i} \text{ and } V_{r-1} \equiv PQ\varepsilon \pmod{p^i}. \tag{6.37}$$

Now suppose that $(D/m) = 1$. Since $\gcd(P, m) = 1$, we see by (6.33), (6.34), and Proposition 2.3 (i) that

$$\begin{aligned} N_2 &= U_{2m}/P = U_m V_m/P = U_{r+1}V_{r+1}/P \equiv \varepsilon(\varepsilon P)P^{-1} \\ &\equiv \varepsilon^2 \equiv 1 \equiv (D/m) \pmod{p^i}. \end{aligned} \tag{6.38}$$

Next suppose that $(D/m) = -1$. Then by (6.37), (6.38), and Proposition 2.3 (i),

$$\begin{aligned} N_2 &= U_{2m}/P = U_m V_m/P = U_{r-1}V_{r-1}/P \equiv (-Q\varepsilon)(PQ\varepsilon)P^{-1} \\ &\equiv -Q^2\varepsilon^2 \equiv -1 \equiv (D/m) \pmod{p^i}. \end{aligned} \tag{6.39}$$

Thus, by (6.38) and (6.39),

$$N_2 - (D/m) \equiv 0 \pmod{p^i}, \tag{6.40}$$

whether $(D/m) = 1$ or $(D/m) = -1$ for an arbitrary prime p such that $p^i \parallel m$. Therefore, it follows by (6.40) that

$$N_2 - (D/m) \equiv 0 \pmod{m}. \tag{6.41}$$

Since N_2 is odd, we also see that

$$N_2 - (D/m) \equiv 0 \pmod{2}. \tag{6.42}$$

Noting that m is odd, we find by (6.41) and (6.42) that

$$N_2 - (D/m) \equiv 0 \pmod{2m}. \tag{6.43}$$

Since $2m \mid N_2 - (D/m)$ by (6.43), we see by Proposition 2.3 (iii) that

$$N_2 = U_{2m}/P \mid U_{2m} \mid U_{N_2-(D/m)}.$$

It will now follow by (6.29) that N_2 is a Lucas pseudoprime if we can show that

$$(D/m) = (D/N_2). \tag{6.44}$$

However, (6.44) holds by Lemma 6.1. □

Remark 6.7. Let $U(P,Q)$ be a nondegenerate Lucas sequence with discriminant D, where $Q = \pm 1$. Suppose further that either it is the case that $P \equiv 1 \pmod 2$ or it is the case that $P \equiv 0 \pmod 2$ and $Q = -1$. By Theorem 6.6 and by Theorem 6.11 below, there in fact exist infinitely many Lucas pseudoprimes M' with parameters P and ± 1 such that $\gcd(M', PD) = 1$, $3 \nmid M'$ if $P \equiv 1 \pmod 2$, and M' is not a Frobenius pseudoprime. Given a Lucas pseudoprime M_1' such that $\gcd(M', PD) = 1$ and $3 \nmid M_1'$ if $P \equiv 1 \pmod 2$, we can use Theorem 6.6 to explicitly find infinitely many other Lucas pseudoprimes M_i' with parameters P and $Q = \pm 1$. Let $M_{i+1}' = \frac{1}{P} U_{2M_i'}$ for $i \geq 1$. Then

$$M_2', M_3', M_4', \ldots,$$

are also Lucas pseudoprimes N with parameters P and Q.

Example 6.8. Consider the Fibonacci sequence $U(1,-1)$. We observe by Tables 1 and 5 of [16] that there are 155 Lucas pseudoprimes less than 1 000 000, of which 56 are also Frobenius pseudoprimes. The first 10 Lucas pseudoprimes less than 1 000 000 which are not Frobenius pseudoprimes are

$$323, 377, 1891, 3827, 6601, 8149, 11663, 13981, 17119, 17711.$$

Theorem 6.9. *Consider the LSFK $U(P,Q)$, where $Q = \pm 1$. Let N be a Lucas pseudoprime such that $\gcd(N, D) = 1$ and N is not a strong Lucas pseudoprime. Suppose that $2^k \parallel \rho(N)$. Then we have:*

(i) *If $Q = -1$, then N is a Frobenius pseudoprime if and only if $N \equiv (D/N) \pmod{2^{k+1}}$ and $(D/N) = 1$;*

(ii) *If $Q = 1$, then N is a Frobenius pseudoprime if and only if $N \equiv (D/N) \pmod{2^{k+1}}$.*

This is proved in Theorem 3.2 of [22].

Theorem 6.10. *Consider the nondegenerate LSFK $U(P,Q)$, where $Q = \pm 1$. Then $D > 0$. Let $m \geq 5$ be an odd prime or a Lucas pseudoprime such that $\gcd(m, PD) = 1$ and $3 \nmid m$ if P is odd. Let $N_2 = U_{2m}/P$. Suppose that either $P \equiv 1 \pmod 2$ or it is the case that $P \equiv 0 \pmod 2$ and $Q = -1$. Then N_2 is a Lucas pseudoprime. Moreover, the following hold:*

(i) *Suppose that P is odd and $Q = -1$. Then N_2 is a Frobenius pseudoprime if and only if $m \equiv (D/m) \pmod 6$ and $(D/m) = 1$.*

(ii) *Suppose that P is odd and $Q = 1$. Then N_2 is a Frobenius pseudoprime if and only if $m \equiv (D/m) \pmod 6$.*

(iii) *Suppose that $P \equiv 0 \pmod 2$ and $Q = -1$. Then N_2 is a Frobenius pseudoprime if and only if $m \equiv (D/m) \pmod 4$ and $(D/m) = 1$.*

Proof. By Remark 2.2 and Theorem 6.6, $D > 0$ and $N_2 = U_{2m}/P$ is a Lucas pseudoprime. Moreover, N_2 cannot also be a strong Lucas pseudoprime. To see this, we note that by Theorem 4.1, U_m has a primitive prime divisor p and U_{2m} has a primitive divisor q. Then $\rho(p) = m$ and $\rho(q) = 2m$. Since $P = U_2$, we see by Proposition 2.3 (iii) that $pq \mid N_2 = U_{2m}/P$. It now follows from Theorem 3.14 that N_2 is not a strong Lucas pseudoprime. Further by Lemma 6.1,

$$(D/m) = (D/N_2) \tag{6.45}$$

if any of the hypotheses of parts (i)–(iii) holds. Noting that $q \mid N_2$ and $\rho(q) = 2m$, we observe that $\rho(N_2) = 2m$. Thus,

$$2 \parallel \rho(N_2). \tag{6.46}$$

We now see by Theorem 6.9 and (6.46) that one of the following two results (a) and (b) holds depending on whether $Q = -1$ or $Q = 1$:

(a) If $Q = -1$, then N_2 is a Frobenius pseudoprime if and only if $N_2 \equiv (D/N_2) \pmod 4$ and $(D/N_2) = 1$.

(b) If $Q = 1$, then N_2 is a Frobenius pseudoprime if and only if $N_2 \equiv (D/N_2) \pmod 4$.

(i) Suppose that $P \equiv 1 \pmod 2$ and $Q = -1$. By inspection, one sees that $\lambda(4) = 6$. In particular, the initial terms of $U(P, Q)$ modulo 4 are

$$0, 1, P, 2, -P, 1, 0, 1, P, \ldots \pmod 4. \tag{6.47}$$

Since m is odd and $3 \nmid m$, we can write m as $6i + \varepsilon \pmod 6$ for some i, where $\varepsilon \in \{-1, 1\}$. Then $2m \equiv 2\varepsilon \pmod 6$. By (6.47), we see that

$$U_{2m} \equiv \varepsilon P \pmod 4.$$

Noting that P is odd, we see that

$$N_2 = U_{2m}/P \equiv \varepsilon \pmod 4. \tag{6.48}$$

It thus follows from (6.48) that if $m \equiv \varepsilon \pmod 6$, then $N_2 = U_{2m}/P \equiv \varepsilon \pmod 4$. We now see from (6.48), (6.45) and Statement (a) that

N_2 is a Frobenius pseudoprime if and only if $m \equiv (D/m) \pmod 6$ and $(D/m) = 1$,

as desired.

(ii) Suppose that that $P \equiv 1 \pmod 2$ and $Q = 1$. By examination, one sees that $\lambda(4) = 3$ or 6. In particular, the initial terms of $U(P, Q)$ modulo 4 are

$$0, 1, P, 0, -P, -1, 0, 1, P, \ldots \pmod 4.$$

As in the proof of part (i), we find that

$$N_2 = U_{2m}/P \equiv \varepsilon \pmod 4.$$

Let $m = 6i + \varepsilon \pmod 6$ for some i, where $\varepsilon \in \{-1, 1\}$. Using Statement (b) and the same arguments as those in the proof of part (i), we conclude that

N_2 is a Frobenius pseudoprime if and only if $m \equiv (D/m) \pmod 6$,

as desired.

We now separate the proofs of part (iii) into two parts, (iiia) and (iiib).

(iiia) Suppose that $Q = -1$ and $2^k \parallel P$, where $k \geq 2$. By inspection, one finds that $\lambda(2^{k+2}) = 8$. Noting that $P^2 \equiv 0 \pmod{2^{k+2}}$, we see that the initial terms of $U(P, Q)$ modulo 2^{k+2} are

$$0, 1, P, 1, 2P, 1, 3P, 1, 4P \equiv 0, 1, P, \ldots \pmod{2^{k+2}}. \tag{6.49}$$

Since m is odd, we can represent m as $m = 4i + \varepsilon$, where $\varepsilon \in \{-1, 1\}$. Then $2m = 8i + 2\varepsilon$. Since $2^k \parallel P$, we obtain from (6.49) that

$$N_2 = U_{2m}/P \equiv \varepsilon \equiv m \pmod 4. \tag{6.50}$$

It now follows from (6.45), (6.50), and Statement (a) that

N_2 is a Frobenius pseudoprime if and only if $m \equiv (D/m) \pmod 4$ and $(D/m) = 1$.

(iiib) Finally suppose that $Q = -1$ and $P \equiv 2 \pmod 4$. By inspection, we see that $\lambda(8) = 8$. Noting that $P^2 \equiv 4 \pmod{16}$ by (6.5) in the proof of Lemma 6.1, we find that the initial terms of $U(P, Q)$ modulo 8 are

$$0, 1, P, 5, 6P, 5, 3P, 1, 4P \equiv 0, 1, P, \ldots \pmod 8. \tag{6.51}$$

We can write m as $m = 4i + j$, where $j \in \{1, 3\}$. Then $2m = 8i + 2j$. Hence by (6.51),

$$U_{2m} \equiv jP \pmod 8. \tag{6.52}$$

Since $P \equiv 2 \pmod 4$, we obtain from (6.52) that

$$N_2 = U_{2m}/P \equiv j \equiv m \pmod 4. \tag{6.53}$$

Then by (6.45), (6.53), and Statement (a), we find that

N_2 is a Frobenius pseudoprime if and only if $m \equiv (D/m) \pmod 4$ and $(D/m) = 1$.

The proof is now complete. □

Theorem 6.11. *Consider the LSFK $U(P, Q)$, where $Q = \pm 1$ and P is odd if $Q = 1$. Let m be an odd prime or a Lucas pseudoprime. Then there exist infinitely many Lucas pseudoprimes with parameters P and Q of the form U_{2m}/P that are Frobenius pseudoprimes, and there also exist infinitely many Lucas pseudoprimes with parameters P and Q of the form U_{2m}/P that are not Frobenius pseudoprimes.*

Proof. This follows from Theorem 6.10, Dirichlet's theorem on the infinitude of primes in arithmetic progressions, and Theorem 4.6. □

7. Conclusion

The purpose of this paper is to generate new classes of infinitely many Lucas and Frobenius pseudoprimes with parameters P and Q for the case in which $Q = \pm 1$. Frobenius pseudoprimes are of particular interest because they are simultaneously Lucas pseudoprimes, Lucas pseudoprimes of the second kind, Dickson pseudoprimes, and Dickson pseudoprimes of the second kind. In [22], we obtained infinitely many Frobenius pseudoprimes with parameters P and $Q = \pm 1$ under the assumption that P is an odd positive integer. In this article, we extend these results by also allowing P to be negative or even. In Theorem 6.6, we further obtained infinitely many new Lucas pseudoprimes with parameters P and $Q = \pm 1$. Furthermore, in Theorem 6.5, we showed that there are infinitely many Lucas pseudoprimes with parameters P and $Q = \pm 1$ of the form U_{2m}/P that are also Frobenius pseudoprimes, and there also exist infinitely many Lucas pseudoprimes with parameters P and $Q = \pm 1$ of the form U_{2m}/P that are not Frobenius pseudoprimes, where m is an odd prime or a Lucas pseudoprime.

The reason that we concentrate on the situation in which the parameter $Q = \pm 1$ is due to Theorem 3.18 and Remark 3.8. By Theorem 3.18, N is a Frobenius pseudoprime with parameters P and Q, where $\gcd(N, PQ(P^2 - 4Q)) = 1$, if N is both an Euler–Lucas pseudoprime with parameters P and Q and an Euler pseudoprime to the base Q. If $Q = \pm 1$, then N is automatically an Euler pseudoprime to the base Q by Remark 3.8. Thus, if $Q = \pm 1$ and P is an integer such that $\gcd(N, P(P^2 - 4Q)) = 1$, then N only needs to be an Euler–Lucas pseudoprime with parameters P and Q in order to also be a Frobenius pseudoprime with parameters P and Q. Remark 3.8 and Theorems 3.18 and 3.19 in fact are our main tools to generate infinitely many Frobenius pseudoprimes. However, for a given nonzero integer $Q \neq \pm 1$, it is far more difficult to find a composite integer N and a nonzero integer P such that N is both an Euler–Lucas pseudoprime with parameters P and Q and an Euler pseudoprime to the base Q, so that we can apply Theorem 3.18. One example is given by $Q = 31$, $N = 133$, and $P = 25$ (see [2, p. 1397]), in which case 133 is a Frobenius pseudoprime with parameters 25 and 31.

Let $F(P, Q; x)$ denote the number of Frobenius pseudoprimes with parameters P and Q less than or equal to x. It follows from Theorem 3.19 of this paper, Theorem 1 of [11], and Theorem 7 of [2] that if $Q = \pm 1$, then

$$F(P, Q; x) \geq c(P, Q) \log x \quad \text{for all sufficiently large } x,$$

where $c(P, Q)$ is a constant dependent on P and Q, which yields that there are infinitely many Frobenius pseudoprimes with parameters P and Q. This leads to the following natural question for which no answer is known (see [2, p. 1411]).

We have the following open question: Given the fixed nonzero integer $Q \neq \pm 1$ and an arbitrary nonzero integer P, find a nontrivial lower bound for $F(P, Q; x)$.

In particular, are there infinitely many composite integers N such that N is a Frobenius pseudoprime with the parameters P and Q for some nonzero integer P?

The principal application of pseudoprimes is in primality testing, since the criterion for an odd composite integer N to be a particular type of pseudoprime is, by definition, satisfied by each prime number, and pseudoprimes are rare compared to primes. If a positive odd integer $N > 1$ does not satisfy the criterion for N to be a particular type of pseudoprime, then we know that N cannot be prime. Since pseudoprimes are rare compared to the primes, it is very likely that a randomly chosen composite odd integer N will not be a pseudoprime of a particular type and thus shown to not be prime. In the case of Euler pseudoprimes, we can use the Solovay–Strassen probabilistic primality test to conclude that N is very likely to be a prime if it satisfies the property of being an Euler pseudoprime for several randomly chosen bases. A more powerful probabilistic primality test is achieved by using the Miller–Rabin test for N to be a strong pseudoprime to several bases. An odd composite integer $N = d \cdot 2^s + 1$, where d is odd, is a strong pseudoprime to the base a if:

$$a^d \equiv 1 \pmod{N}$$

or

$$a^{d \cdot 2^r} \equiv -1 \pmod{N} \text{ for some } 0 \leq r < s.$$

For a discussion of various types of pseudoprimes, see [8, pp. 148–150]. Let $L(P, Q; x)$ denote the number of Lucas pseudoprimes with parameters P and Q less than or equal to x. We note in particular that by Theorem 6 and its Corollary in [2, p. 1399], there exists a positive constant c such that

$$F(P, Q; x) \leq L(P, Q; x) < x \exp(-c(\log x \log\log x)^{1/2}),$$

which implies that the sum of the reciprocals of all Lucas pseudoprimes with parameters P and Q converges. Since the sum of the reciprocals of all primes diverges, we see that Lucas pseudoprimes are indeed scarce compared to primes and can be used for primality tests.

The Baillie–PSW primality test (see [2]) and the enhanced Baillie–PSW primality test (see [1]) provide further incentive to study Lucas and Frobenius pseudoprimes with parameters P and Q, where $Q \neq \pm 1$. Both tests have never been shown to fail and are based on testing whether an odd positive integer N is both a strong pseudoprime to the base 2 and a strong Lucas pseudoprime with parameters P and $Q \neq \pm 1$ and discriminant $D = P^2 - 4Q$ satisfying $(D/N) = -1$. Strong pseudoprimes to the base 2 and strong Lucas pseudoprimes with parameters P and Q are used in the Baillie–PSW primality test, because these pseudoprimes are rarer than pseudoprimes to the base 2 and Lucas pseudoprimes with parameters P and Q, respectively. Robert Baillie observed in [2] that the property of the odd composite integer N being a pseudoprime or a strong pseudoprime to the base 2

appears to be largely independent of the property of N being a Lucas pseudoprime or a strong Lucas pseudoprime with parameters P and Q such that $(D/N) = -1$, where $Q \neq \pm 1$. Baillie based this assumption on the observation that for small moduli m, by far the largest percentage of pseudoprimes and strong pseudoprimes to the base 2 lay in residue class 1 modulo m, (see Table 4 of [11]), while the Lucas pseudoprimes and strong Lucas pseudoprimes N with parameters P and Q for which $(D/N) = -1$ tended to fall mostly in the residue class $m - 1$ modulo m (see Table 2 of [1]). These considerations led R. Baillie (see [2]) to believe that it would be extremely rare, if it happened at all, for an odd composite integer N to be both a strong pseudoprime to the base 2 and a strong Lucas pseudoprime with parameters P and Q and discriminant D satisfying $(D/N) = -1$.

In an early version of the Baillie–PSW primality test, John Selfridge used Method A given below (see [11, p. 1024]) to generate parameters P and Q and discriminant D in order to test whether a given positive integer N is a strong Lucas pseudoprime:

Method A. Let D be the first element of the sequence $5, -7, 9, -11, \ldots$ for which $(D/N) = -1$. Let $P = 1$ and $Q = (1 - D)/4$.

This algorithm never sets $Q = 1$, but for $D = 5$, it sets $Q = -1$. Method A sets $Q = -1$ fairly often, namely when $N \equiv \pm 3 \pmod{10}$ (see [1, p. 1934]). Table 4 of [2] shows that all Frobenius pseudoprimes less than 10^8 with parameters P and Q chosen by Method A above have $Q = -1$. The first few Frobenius pseudoprimes chosen by Method A are $N = 5777$, $N = 10877$, $N = 75077$, and $N = 100127$ (for these, $P = 1$, $Q = -1$). Since we want pseudoprimes to be as rare as possible for our primality test, Method A was modified to Method A* given below so that the chosen parameter Q is never equal to ± 1 (see [2, p. 1409]).

Method A*. Choose D, P, and Q as in Method A above. If $Q = -1$, change P and Q to 5.

Note that Method A* leaves $D = P^2 - 4Q$ unchanged from Method A.

The original Baillie–PSW primality test (see [2, p. 1412] and [1, p. 1936]) has these steps:

(1) If N is not a strong pseudoprime to the base 2, then N is composite, so stop.

(2) Choose the Lucas parameters P, Q, and D using Method A*. If N is not a strong Lucas pseudoprime with parameters P and Q such that $(D/N) = -1$, then N is composite. Otherwise, declare N to be (probably) prime.

In Table 1 of [1], Baillie, Fiori, and Wagstaff showed that there were 419849 strong pseudoprimes to the base 2 and 474971 strong Lucas pseudoprimes less than 10^{15} using Method A*, but only five Dickson pseudoprimes of the second kind less than 10^{15} using Method A*. This observation led the authors of [1] to propose the following enhanced Baillie–PSW primality test adding extra steps to the original Baillie–PSW primality test. These steps involve testing whether the odd positive

integer N is also a Dickson pseudoprime of the second kind with parameters P and Q and an Euler pseudoprime to the base Q. The steps for this strengthened primality test are as follows (see [1, p. 1939]):

(1) If N is not a strong pseudoprime to the base 2, then N is composite; stop.

(2) Choose the Lucas parameters P, Q, and D using Method A*. If N is not a strong Lucas pseudoprime with parameters P and Q such that $(D/N) = -1$, then N is composite; stop.

(3) If N is not a Dickson pseudoprime of the second kind with parameters P and Q, then N is composite; stop.

(4) If N is not an Euler pseudoprime to the base Q, then N is composite; stop. Otherwise, declare N to be (probably) prime.

There is no known example of a composite integer N that is declared prime by either the original Baillie–PSW primality test or the enhanced Baillie–PSW primality test. A reward of \$620 has been offered for an example of a composite integer N that passes the original Baillie–PSW primality test. No one has claimed the reward after 45 years, though this primality test has been tried on billions of large odd integers N (see [1, p. 1936]). In 2021, the authors of [1] have offered a reward of \$2000 for an instance of a composite integer N that the enhanced Baillie–PSW primality test declares to be prime (see [1, p. 1936]).

Acknowledgments. We wish to congratulate Professor Curtis Cooper upon his retirement from the editorship of The Fibonacci Quarterly. The first author of this paper had the pleasure of writing two other joint papers with Curtis Cooper on pseudoprimes related to kth-order linear recurrences. The second author was supported by the Czech Academy of Sciences (RVO 67985840).

References

[1] R. Baillie, A. Fiori, S. S. Wagstaff, Jr., Strengthening the Baillie–PSW primality test, *Math. Comp.* **90** (2021), 1931–1955.

[2] R. Baillie, S. S. Wagstaff, Jr., Lucas pseudoprimes, *Math. Comp.* **35** (1980), 1391–1417.

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

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

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

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

[7] P. Kiss, Some results on Lucas pseudoprimes, *Ann. Univ. Sci. Budapest. Eőtvős Sect. Math.* **28** (1985), 153–159.

[8] M. Křížek, L. Somer, A. Šolcová, From great discoveries in number theory to applications, Springer, Cham, 2021.

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

[10] F. Luca, L. Somer, Lucas sequences for which $4 \mid \phi(|u_n|)$ for almost all n, *Fibonacci Quart.* **44** (2006), 249–263.

[11] C. Pomerance, J. L. Selfridge, S. S. Wagstaff, Jr., The pseudoprimes to $25 \cdot 10^9$, *Math. Comp.* **35** (1980), 1003–1026.

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

[13] A. Rotkiewicz, On Lucas numbers with two intrinsic divisors, *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **10** (1962), 223–232.

[14] A. Rotkiewicz, On the pseudoprimes with respect to the Lucas sequence, *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **21** (1973), 793–797.

[15] A. Rotkiewicz, Lucas pseudoprimes, *Funct. Approx. Comment. Math.* **28** (2000), 97–104.

[16] A. Rotkiewicz, Lucas and Frobenius pseudoprimes, *Ann. Math. Sil.* **17** (2003), 17–39.

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

[18] L. Somer, Generalization of a theorem of Drobot, *Fibonacci Quart.* **40** (2002), 435–437.

[19] L. Somer, Lucas sequences U_k for which U_{2p} and U_{2p} are pseudoprimes for almost all primes p, *Fibonacci Quart.* **44** (2006), 7–12.

[20] L. Somer, M. Křížek, Prime Lehmer and Lucas numbers with composite indices, *Fibonacci Quart.* **51** (2013), 194–214.

[21] L. Somer, M.Křížek, On primes in Lucas sequences, *Fibonacci Quart.* **53** (2015), 2–23.

[22] L. Somer, M. Křížek, Frobenius, Lucas, and Dickson pseudoprimes, *Fibonacci Quart.* **60** (2022), 325–343.

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

[24] `mathworld.wolfram.com/FibonacciPrime.html`