FROBENIUS, LUCAS, AND DICKSON PSEUDOPRIMES

LAWRENCE SOMER AND MICHAL KŘÍŽEK

Abstract. We prove results about various types of pseudoprimes with respect to Lucas sequences. In particular, we investigate Frobenius pseudoprimes that satisfy properties of several different types of pseudoprimes. We also find Frobenius pseudoprimes with many divisors for which each of its composite divisors is also a Frobenius pseudoprime.

1. Introduction

Let $U(P,Q)$ and $V(P,Q)$ be the Lucas sequences satisfying the second-order recursion relation

$$W_{n+2}(P,Q) = PW_{n+1}(P,Q) - QW_n(P,Q), \tag{1.1}$$

with discriminant $D = D(P,Q) = P^2 - 4Q$, where P and Q are integers, and the initial terms are $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = P$, respectively. We suppress the parameters P and Q when they are understood. We will investigate various pseudoprimes connected with the Lucas sequences $U(P,Q)$ and $V(P,Q)$. Associated with $U(P,Q)$ and $V(P,Q)$ is the characteristic polynomial

$$f(x) = x^2 - Px + Q \tag{1.2}$$

with characteristic roots α and β. We observe that $D = D(P,Q) = (\alpha - \beta)^2$. We note that

$$\alpha = \frac{P + \sqrt{D}}{2}, \quad \beta = \frac{P - \sqrt{D}}{2}. \tag{1.3}$$

By the Binet formulas,

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad V_n = \alpha^n + \beta^n. \tag{1.4}$$

Proposition 1.1 below follows from the Binet formulas (1.4).

Proposition 1.1. *For the Lucas sequences $U(P,Q)$ and $V(P,Q)$ we have:*

(i) $U_{2n}(P,Q) = U_n(P,Q)V_n(P,Q)$.

(ii) $V_n^2(P,Q) - DU_n^2(P,Q) = 4Q^n$.

(iii) *If $m \mid n$, then $U_m \mid U_n$.*

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

It is known that if N is an odd prime such that $\gcd(N, PQD) = 1$, then the following four congruences are all satisfied for given Lucas sequences $U(P,Q)$ and $V(P,Q)$, with discriminant

D, where (D/N) denotes the Jacobi symbol (see [1, pp. 1391–1396] and Theorem 2.11 (ii)):

$$U_{N-(D/N)} \equiv 0 \pmod{N}, \tag{1.5}$$

$$U_N \equiv (D/N) \pmod{N}, \tag{1.6}$$

$$V_N \equiv P \pmod{N}, \tag{1.7}$$

$$V_{N-(D/N)} \equiv 2Q^{(1-(D/N))/2} \pmod{N}. \tag{1.8}$$

It also occurs rarely that at least one of the congruences (1.5)–(1.8) holds if N is a positive odd composite integer. We note that by [1, 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 that are given in [16].

Definition 1.2. The positive odd composite integer N is called a *Lucas pseudoprime with respect to the Lucas sequence* $U(P,Q)$ if $\gcd(N,QD)=1$ and congruence (1.5) holds. (We will denote N as a Lucas pseudoprime if the Lucas sequence $U(P,Q)$ is understood.)

Definition 1.3. The positive odd composite integer N is called a *Lucas pseudoprime of the second kind with respect to the Lucas sequence* $U(P,Q)$ if $\gcd(N,QD)=1$ and congruence (1.6) holds.

Definition 1.4. The positive odd composite integer N is called a *Dickson pseudoprime with respect to the Lucas sequence* $V(P,Q)$ if congruence (1.7) holds.

Definition 1.5. The positive odd composite integer N is called a *Dickson pseudoprime of the second kind with respect to the Lucas sequence* $V(P,Q)$ if $\gcd(N,QD)=1$ and congruence (1.8) holds.

For particular Lucas sequences $U(P,Q)$ and $V(P,Q)$, it is known that there exist infinitely many odd composite integers N that satisfy each of the congruences (1.5)–(1.8) (see Theorem 2.24). This gives rise to the following definition appearing in [16].

Definition 1.6. The positive odd composite integer N is called a *Frobenius pseudoprime with respect to the Lucas sequences* $U(P,Q)$ and $V(P,Q)$ if $\gcd(N,PQD)=1$ and congruences (1.5)–(1.8) all hold.

In this paper, we will find Lucas pseudoprimes, Dickson pseudoprimes of the second kind, and Frobenius pseudoprimes with respect to the given Lucas sequences $U(P,Q)$ and $V(P,Q)$. In many cases, we will choose Q to be ± 1.

We also define the following four types of pseudoprimes, which satisfy the same properties as odd primes (see [1]). These definitions appear in [1].

Definition 1.7. Consider the Lucas sequences $U(P,Q)$ and $V(P,Q)$. The positive odd composite integer N is called an *Euler-Lucas pseudoprime* if $\gcd(N,QD)=1$ and

$$U_{(N-(D/N))/2} \equiv 0 \pmod{N} \quad \text{if } (Q/N)=1, \tag{1.9}$$

or

$$V_{(N-(D/N))/2} \equiv 0 \pmod{N} \quad \text{if } (Q/N)=-1. \tag{1.10}$$

Definition 1.8. Consider the Lucas sequences $U(P,Q)$ and $V(P,Q)$. 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* if either

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

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

It follows from Proposition 1.1 (i) and (iii) that Euler-Lucas pseudoprimes and strong Lucas pseudoprimes are both Lucas pseudoprimes.

Definition 1.9. Let N be a positive odd composite integer, and let a be a positive integer such that $\gcd(a, N)) = 1$. Then, N is a *pseudoprime to the base* a if

$$a^{N-1} \equiv 1 \pmod{N}. \tag{1.11}$$

Definition 1.10. *Let N be a positive odd composite integer, and let a be a positive integer such that* $\gcd(a, N) = 1$. *Then, N is an Euler pseudoprime to the base a if*

$$a^{(N-1)/2} \equiv 1 \pmod{N} \quad \text{if } (a/N) = 1, \tag{1.12}$$

or

$$a^{(N-1)/2} \equiv -1 \pmod{N} \quad \text{if } (a/N) = -1. \tag{1.13}$$

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

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 (1.4) 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. Because the characteristic polynomial f 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 $n = 1, 2, 3, 4$, or 6. The following theorem determines all degenerate Lucas sequences $U(P, Q)$ and $V(P, Q)$.

Theorem 1.11. *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 [19, p. 613].

From here on, we will let p denote an odd prime and we will always assume that the Lucas sequences $U(P, Q)$ and $V(P, Q)$ are nondegenerate. We will frequently assume that $Q = \pm 1$. In this case, it follows from Theorem 1.11 that $D = P^2 - 4Q > 0$.

2. Preliminaries and Known Results

We will need the following results and definitions for our main results of this paper.

Theorem 2.1. *Consider the Lucas sequence $U(P, Q)$. Let N be a composite odd integer 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 [1].

Theorem 2.2. *Consider the Lucas sequence $U(P, Q)$. Suppose that N is an Euler-Lucas pseudoprime and N is an Euler pseudoprime to the base Q, where* $\gcd(N, PQD) = 1$. *Then, N is a Frobenius pseudoprime.*

Remark 2.3. Let m be a positive odd integer, and let $Q = \pm 1$. Then, by the properties of the Jacobi symbol,

$$Q^{(m-1)/2} = (Q/m), \tag{2.1}$$

and m is always an Euler pseudoprime to the bases 1 and -1.

Corollary 2.4. *Consider the Lucas sequence $U(P,Q)$, where $Q = \pm 1$. If N is a strong Lucas pseudoprime, then N is a Frobenius pseudoprime.*

Proof. By Theorem 2.1, N is also an Euler-Lucas pseudoprime. The result now follows from Theorem 2.2 and Remark 2.3. □

Theorem 2.5. *Consider the Lucas sequence $U(P,Q)$. Suppose that N is an Euler-Lucas pseudoprime and N is a Frobenius pseudoprime, where $\gcd(N, PQD) = 1$. Then, N is an Euler pseudoprime to the base Q.*

Theorem 2.6. *Consider the Lucas sequence $U(P,Q)$. Suppose that N is a Frobenius pseudoprime and N is an Euler pseudoprime to the base Q, where $\gcd(N, 2PQD) = 1$. Then, N is an Euler-Lucas pseudoprime.*

Theorem 2.7. *Consider the Lucas sequence $U(P,Q)$. Suppose that N is a square free Dickson pseudoprime of the second kind and N is an Euler pseudoprime to the base Q, where $\gcd(N, QD) = 1$. Then, N is an Euler-Lucas pseudoprime.*

Theorems 2.2, 2.5, and 2.7 are proved in [15], and Theorem 2.6 is proved in Theorem 5 of [1].

Theorem 2.8. *Consider the Lucas sequence $U(P,Q)$, where $Q = \pm 1$. Let $N > 1$ be an odd integer such that $\gcd(N, PD) = 1$. If N is a square free Dickson pseudoprime of the second kind, then N is a Frobenius pseudoprime.*

Proof. By Theorem 2.7 and Remark 2.3, N is an Euler-Lucas pseudoprime. It now follows by Theorem 2.2 that N is a Frobenius pseudoprime. □

Rotkiewicz [16] proved Theorem 2.8 for the case in which $U(P,Q)$ is the Fibonacci sequence. His proof is essentially the same as that given for the proof of Theorem 2.8.

Given the Lucas sequence $U(P,Q)$ and a positive integer m, we define the rank of appearance $\rho(m)$ to be the least positive integer k such that $m \mid U_k$. We say that the prime p is a *primitive prime divisor* of U_n if $\rho(p) = n$. We have the following two theorems on primitive prime divisors.

Theorem 2.9. (Carmichael) *Consider the Lucas sequence $U(P,Q)$, where $\gcd(P,Q) = 1$ and $D > 0$. Then, U_n has a primitive prime divisor if $n \neq 1, 2, 3, 6,$ or 12.*

This is proved in Theorem XXIII of [3].

Theorem 2.10. (Bilu, Hanrot, and Voutier) *Consider the Lucas sequence $U(P,Q)$, where $\gcd(P,Q) = 1$. Then, U_n has a primitive prime divisor if $n > 30$.*

This is proved in [2].

The following theorem presents well-known properties of the Lucas sequences $U(P,Q)$ and $V(P,Q)$.

Theorem 2.11. *Consider the Lucas sequences $U(P,Q)$ and $V(P,Q)$ with discriminant D. Let m and n be positive integers.*

(i) *If $\gcd(m,Q) = 1$, then $m \mid U_n$ if and only if $\rho(m) \mid n$.*

(ii) *If p is an odd prime and $p \nmid QD$, then $p \mid U_{p-(D/p)}$.*
(iii) *If $p \mid D$ and $p \nmid Q$, then $\rho(p) = p$.*
(iv) *If $p \nmid QD$, then $p \mid U_{(p-(D/p))/2}$ if and only if $(Q/p) = 1$.*
(v) *If $p \nmid QD$, then $p \mid V_{(p-(D/p))/2}$ if and only if $(Q/p) = -1$.*
(vi) *If $\gcd(mn, Q) = 1$ and $m \mid n$, then $\rho(m) \mid \rho(n)$.*
(vii) *If $p \nmid Q$, $\rho(p^k) = \rho(p)$, and $\rho(p^{k+1}) \neq \rho(p^k)$, then $\rho(p^j) = p^{\max(j-k,0)}\rho(p)$ for $j \geq 1$.*
(viii) *If $\gcd(m, n) = \gcd(mn, Q) = 1$, then $\rho(mn) = \operatorname{lcm}(\rho(m), \rho(n))$.*
(ix) *If $p \nmid QD$ and $\rho(p) = m$, then $p \equiv (D/p) \pmod{m}$.*

This follows from the results in [13, pp. 53–74], [3] and [8].

Lemma 2.12. *Let U(P, Q) and V(P, Q) be Lucas sequences for which $2 \nmid \gcd(P, Q)$.*

(i) *Suppose P is odd and Q is even. Then, $2 \nmid U_n$ and $2 \nmid V_n$ for $n \geq 1$.*
(ii) *Suppose P is even and Q is odd. Then, $2 \mid U_n$ if and only if $2 \mid n$, and $2 \mid V_n$ for all $n \geq 0$.*
(iii) *Suppose P and Q are odd. Then, $2 \mid U_n$ if and only if $3 \mid n$, and $2 \mid V_n$ if and only if $3 \mid n$.*
(iv) *If $\rho(2)$ exists, then $\rho(2) \leq 3$.*

This is proved in Lemma 2.10 of [9].

Theorem 2.13. (McDaniel) *Consider the Lucas sequences $U(P, Q)$ and $V(P, Q)$, where $\gcd(P, Q) = 1$. Let $m = 2^a m'$ and $n = 2^b n'$ be positive integers, where m' and n' are odd and $a, b \geq 0$. Let $d = \gcd(m, n)$. Then,*

(i)
$$\gcd(U_m, U_n) = |U_d|,$$

(ii)
$$\gcd(V_m, V_n) = \begin{cases} |V_d|, & \text{if } a = b, \\ 1 \text{ or } 2, & \text{if } a \neq b, \end{cases}$$

(iii)
$$\gcd(U_m, V_n) = \begin{cases} |V_d|, & \text{if } a > b, \\ 1 \text{ or } 2, & \text{if } a \leq b. \end{cases}$$

This is proved in [10].

Given the positive integer m, the 2-adic valuation of m, denoted by $\nu_2(m)$, is defined to be the largest nonnegative integer i such that $2^i \mid m$.

Corollary 2.14. *Consider the Lucas sequences $U(P, Q)$ and $V(P, Q)$, where $\gcd(P, Q) = 1$. Let p and q be distinct odd primes.*

(i) *If $\rho(p)$ is odd, then $p \nmid V_n$ for any $n \geq 0$.*
(ii) *If $\nu_2(p) \neq \nu_2(q)$, then $pq \nmid V_n$ for any $n \geq 0$.*

Proof. Part (i) follows from Theorem 2.13 (iii), while part (ii) follows from Theorem 2.13 (ii). □

Lemma 2.15. *Let $U(P, Q)$ and $V(P, Q)$ be Lucas sequences such that $D > 0$. Then, $|U_n|$ is strictly increasing for $n \geq 2$ and $|V_n|$ is strictly 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 [5] and Lemma 2.8 of [9].

Theorem 2.16. *Let $U(P_1, Q_1)$ and $V(P_1, Q_1)$ be nondegenerate Lucas sequences for which $\gcd(P_1, Q_1) = 1$. Let $k \geq 2$ and let $P = V_k(P_1, Q_1)$ and $Q = Q_1^k$. Let $D_1 = D(P_1, Q_1)$ and $D = D(P, Q)$ be the discriminants of $U(P_1, Q_1)$ and $U(P, Q)$, respectively. Then, $U(P, Q)$ is also a nondegenerate Lucas sequence for which*

$$U_n(P, Q) = \frac{U_{kn}(P_1, Q_1)}{U_k(P_1, Q_1)},$$

$\gcd(P, Q) = 1$, and $D = D_1 U_k^2(P_1, Q_1)$.

This follows from the proof of Lemma 2.20 in [9].

Proposition 2.17. *Consider the Lucas sequence $U(P, Q)$. Let N be a Lucas pseudoprime such that $\gcd(N, QD) = 1$. Let p be a prime such that $p \mid N$. Suppose that $\rho(p^k) = \rho(p)$ and $\rho(p^{k+1}) \neq \rho(p)$. If $p^i \mid N$, then $1 \leq i \leq k$.*

Proof. Suppose that $i > k$ and $p^i \mid N$. Then, $\rho(p^i) \mid \rho(N)$ by Theorem 2.11 (vi). It follows by Theorem 2.11 (vii) that $p \mid \rho(p^i)$. Because $N \mid U_{N-(D/N)}$, we see that $\rho(N) \mid N - (D/N)$ by Theorem 2.11 (i). Thus, $\gcd(N, \rho(N)) = 1$, which contradicts $p \mid \rho(N)$. □

Proposition 2.18. *Consider the Lucas sequence $U(P, Q)$. Let*

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

be an odd composite integer such that $\gcd(N, QD) = 1$. Suppose that N is a Lucas pseudoprime. Then, $\rho(p_i^{k_i}) = \rho(p_i)$ 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 $1 \leq i < j \leq s$.

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.

Proof. This follows from Proposition 2.17, the definition of a strong Lucas pseudoprime, and the discussion on page 1397 of [1]. □

Corollary 2.19. *Consider the Lucas sequence $U(P, Q)$. Let N be a Lucas pseudoprime for which $\gcd(N, DQ) = 1$. Then, N is a strong Lucas pseudoprime if $\rho(N)$ is odd.*

Proof. By Theorem 2.11 (vi), if $p \mid N$, then $\rho(p) \mid \rho(N)$. The result now follows from Proposition 2.18. □

Definition 2.20. Consider the Lucas sequence $U(P, Q)$. Let N be a positive composite odd integer such that $\gcd(N, QD) = 1$. Then, N is called a *super Lucas pseudoprime* if each divisor of N greater than 1 is a prime or a Lucas pseudoprime.

Remark 2.21. It is immediately seen that each composite divisor of a super Lucas pseudoprime is also a super Lucas pseudoprime. If N is a Lucas pseudoprime that is a product of exactly two distinct odd primes, then N is a super Lucas pseudoprime, because its only proper divisors greater than 1 are primes. Such super Lucas pseudoprimes are not that interesting. Phong [12] proved that there exist infinitely many super Lucas pseudoprimes with respect to an arbitrary Lucas sequence $U(P, Q)$ having exactly three distinct prime divisors. Somer and Křížek [18] generalized this result by finding infinitely many super Lucas pseudoprimes with respect to particular Lucas sequences $U(P, Q)$ that have exactly four distinct prime divisors. We similarly define a super Frobenius pseudoprime as a positive composite odd integer N for which each divisor of N greater than 1 is a prime or a Frobenius pseudoprime, etc.

Theorem 2.22. *Consider the Lucas sequence $U(P,Q)$. Let p_1, p_2, …, 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 a 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 $i = 1,\ldots,s$,

$$p_i \equiv (D/p_i) \pmod{h}. \tag{2.2}$$

Proof. It follows by Theorem 2.11 (viii) that $\rho(N) = h$. By Proposition 2.17, a necessary condition for N to be a super Lucas pseudoprime is that $\rho(p_i^{k_i}) = \rho(p_i)$ for $i = 1,\ldots,s$. Suppose that (2.2) holds for $i \in \{1,\ldots,s\}$. Let $d = p_1^{g_1} p_2^{g_2} \cdots p_s^{g_s}$ be a composite divisor of N, where $0 \leq g_i \leq k_i$ for $i = 1,\ldots,s$. To show that d is a Lucas pseudoprime and thus N is a super Lucas pseudoprime, it suffices, by Theorem 2.11 (i), to establish that

$$\rho(d) \mid d - (D/d). \tag{2.3}$$

Because $p_i \equiv (D/p_i) \pmod{h}$ for $i = 1,\ldots,s$, we see by the properties of the Jacobi symbol that

$$d \equiv \prod_{i=1}^{s} (D/p_i)^{g_i} \equiv \prod_{i=1}^{s} (D/p_i^{g_i}) \equiv (D/d) \pmod{h}, \tag{2.4}$$

or equivalently,

$$d - (D/d) \equiv 0 \pmod{h}. \tag{2.5}$$

Let $\rho_i = \rho\big(p_i^{g_i}\big)$. We observe that if $g_i \geq 1$, then $\rho\big(p_i^{g_i}\big) = \rho(p_i)$, otherwise $\rho(p_i^{g_i}) = 1$. It now follows from Theorem 2.11 (viii) that

$$\rho(d) = \operatorname{lcm}(\rho(p_1), \rho(p_2), \ldots, \rho(p_s)) \mid h. \tag{2.6}$$

It now follows from (2.5) and (2.6) that (2.3) holds. The remainder of the proof of Theorem 2.22 follows from the proof of Theorem 12.25 on pp. 141–142 of [7] and the proof of Lemma 2 of [12]. □

Proposition 2.23. *Consider the Lucas sequence $U(P,Q)$, where $Q = \pm 1$. Let*

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

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

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

(Note that we allow the possibility that i can equal j.) Then, N is a super strong Lucas pseudoprime and a super Frobenius Lucas pseudoprime.

Proof. Let d be a positive composite divisor of N. It follows from Theorem 2.11 (ix) and Theorem 2.22 and its proof that d is a super Lucas pseudoprime. We now see by Proposition 2.18 that d is also a strong Lucas pseudoprime. The result now follows by Corollary 2.4. □

Theorem 2.24. (Rotkiewicz) *Consider the Lucas sequence $U(P,Q)$, 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.*

This is proved in Theorem 1 of [14].

We observe that if $N=p_1p_2$ is a strong Lucas pseudoprime and a Frobenius pseudoprime, then it is trivially a super strong Lucas pseudoprime and a super Frobenius pseudoprime by Remark 2.21. In Theorem 2.26 below, given an arbitrary integer $C\geq 3$, we will find particular Lucas sequences $U(P,Q)$ for which there are infinitely many odd integers with exactly C distinct odd prime divisors that are super strong Lucas pseudoprimes and super Frobenius pseudoprimes.

Theorem 2.25. *Consider the Lucas sequence $U(P,Q)$, 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 2.26. *Let $U(P,Q)$ be a Lucas sequence for which $P>0$, P or Q is odd, $\gcd(P,Q)=1$, and $D>0$. Let $D=D_0^2D_1$, where D_1 is square free, and suppose that P is odd or P is even and $D_1\equiv 1 \pmod 4$. Let m be an odd prime or a Lucas pseudoprime of the second kind such that $\gcd(m,PQD)=1$, $m\neq 3$, and $3\nmid m$ if $P\equiv Q\equiv 1 \pmod 2$. Let $N=U_m$. Then, N is odd. If N is composite, then N is a strong Lucas pseudoprime. In particular, N is composite if Q is a perfect square or m is a Lucas pseudoprime of the second kind. If N is composite and m is an odd prime, then N is a super strong Lucas pseudoprime. Furthermore, if $Q=1$ or $Q=-1$ and N is composite, then N is a Frobenius pseudoprime. Moreover, if m is prime and $Q=1$ or $Q=-1$ and N is composite, then N is a Frobenius pseudoprime.*

This follows from the proofs of Theorems 2 and 3 of [17], Lemma 2.12, Theorem 2.22, and Corollary 2.19.

Theorem 2.27. *Consider the Lucas sequence $U(P,Q)$, where $\gcd(P,Q)=1$. Suppose that $p\geq 7$ and $\gcd(p,PQD)=1$. Then, $|U_{2p}/P|$ is a super Lucas pseudoprime if it is not the case that $p=13$, $P=\pm 1$, and $Q=2$.*

Proof. Note that $P=U_2$. Thus, by Theorem 2.13 (i), $P\mid U_{2p}$. By Theorem 2 of [6], $|U_{2p}/P|$ is a super Lucas pseudoprime if it is composite. By Theorem 2.10 and the proof of Theorem 3.1 of [9], $|U_{2p}/P|$ is composite if $p\geq 7$ and it is not the case that $p=13$, $P=\pm 1$, and $Q=2$. We observe that $|U_{26}(\pm 1,2)|=181$, which is prime. □

3. Main Results

We now present our main results.

Theorem 3.1. *Let $U(P,Q)$ be a Lucas sequence for which $P>0$, P is odd, $\gcd(P,Q)=1$, and $D>0$. Let m be an odd prime or a Frobenius pseudoprime such that $\gcd(m,PQD)=1$, $m\neq 3$, and $3\nmid m$ if Q is odd. Let $N=U_{2m}/P$. Then, N is a Lucas pseudoprime.*

Proof. We note that m is odd and $m\geq 5$. By Lemma (i), $U_{2m}/P=U_mV_m/P$. Because $V_1=P$, we see by Theorem 2.13 (ii) and Lemma 2.15 that $P\mid V_m$, $U_m>0$, and $V_m>0$. By Theorem 2.9, U_m and U_{2m} both have a primitive prime divisor. Thus, N is composite. By Lemma 2.12, U_m and V_m are odd. Because $\gcd(P,Q)=1$, P is odd, and $D=P^2-4Q$, it follows that $\gcd(2P,D)=1$.

Noting that m is an odd prime or a Frobenius pseudoprime, we find that

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

Thus,

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

Then,

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

because U_{2m}/P is odd. Consequently,

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

Therefore, by Proposition 1.1 (iii),

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

To complete the proof, we need to show that $(D/m) = (D/N)$. We note that $D = P^2 - 4Q \equiv 1 \pmod{4}$. Using the binomial theorem to expand the expression for U_{2m} given by the Binet formula in (1.4), we obtain

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

Hence,

$$N = U_{2m}/P \equiv m(2^{-1}P)^{2(m-1)} \pmod{D}. \tag{3.1}$$

It now follows from (3.1) and the properties of the Jacobi symbol that

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

The result now follows. □

Theorem 3.1 was proved in Theorem 3 of [11] for the case in which $U(P,Q)$ is the Fibonacci sequence and in Theorem 1 of [17] for the case in which $P = 1$.

Theorem 3.2. *Consider the Lucas sequences $U(P,Q)$ and $V(P,Q)$, 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 $2^k \parallel \rho(N)$, where $2^k \parallel m$ means that $2^k \mid m$ but $2^{k+1} \nmid m$.*

(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 $N \equiv (D/N) \pmod{2^{k+1}}$.*

Proof. We will treat cases (i) and (ii) together. By Theorems 2.2 and 2.6 and Remark 2.3, N is a Frobenius pseudoprime if and only if N is an Euler-Lucas pseudoprime. Because N is a Lucas pseudoprime that is not a strong Lucas pseudoprime, it follows from Corollary 2.19 that $k \geq 1$. Moreover, by Proposition 2.18 and Corollary 2.14 (ii), $N \nmid V_n$ for any $n \geq 0$. Thus, N is an Euler-Lucas pseudoprime if and only if

$$(Q/N) = 1 \quad \text{and} \quad N \mid U_{(N-(D/N))/2}. \tag{3.2}$$

By Theorem 2.11 (i), (3.2) can occur if and only if $(Q/N) = 1$ and

$$\rho(N) \mid (N - (D/N))/2. \tag{3.3}$$

Because N is a Lucas pseudoprime, we observe that

$$N \mid U_{N-(D/N)}. \tag{3.4}$$

Because $2^k \parallel \rho(N)$ and $\rho(N) \mid N - (D/N)$ by (3.4) and Theorem 2.11 (i), it follows from (3.3) that N will be an Euler-Lucas pseudoprime if and only if

$$N \equiv (D/N) \pmod{2^{k+1}}, \tag{3.5}$$

which implies that

$$N \equiv (D/N) \pmod{4}. \tag{3.6}$$

We note by the properties of the Jacobi symbol that if $Q = -1$, then $(Q/N) = 1$ if and only if $N \equiv 1 \pmod 4$. Because $(1/N) = 1$, we now see by (3.2), (3.5), and (3.6) that N is an Euler-Lucas pseudoprime if and only if $(Q/N) = 1$. By Theorem 2.22, we see that N is a super Lucas pseudoprime and

$$N \equiv (D/N) \pmod{2^{k+1}},$$

and $N \equiv 1 \pmod{2^{k+1}}$ when $Q = -1$. The result now follows. □

Theorem 3.3. *Consider the Lucas sequence $U(P,Q)$, where $P > 0$, P is odd, and $Q = \pm 1$. Suppose that m is an odd prime or a Frobenius pseudoprime such that $\gcd(m, 6PD) = 1$. Let $N = U_{2m}/P$. Then, N is a Lucas pseudoprime. Moreover, the following hold:*

(i) *If $Q = -1$, then N is a Frobenius pseudoprime if and only if $m \equiv (D/m) \pmod 6$ and $(D/m) = 1$.*
(ii) *If $Q = 1$, then N is a Frobenius pseudoprime if and only if $m \equiv (D/m) \pmod 6$.*

Proof. We will prove parts (i) and (ii) together. Let $N = U_{2m}/P$. By the proof of Theorem 3.1, N is an integer, $N > 0$, $(D/N) = (D/m)$, and N is a Lucas pseudoprime. By Theorem 2.9, U_m has an odd primitive prime divisor p and U_{2m} has an odd primitive prime divisor q. So, $\rho(U_{2m}) \le 2m$. Noting that $U_2 = P$ and $\gcd(P, m) = 1$, we see that $pq \mid N$, which implies by Proposition 2.18 that $\rho(N) = 2m$ and N is not a strong Lucas pseudoprime. Thus, $2^1 \parallel \rho(N)$.

We now show that if $m \equiv \delta(D/m) \pmod 6$, where $\delta \in \{-1, 1\}$, then $N \equiv \delta(D/m) \pmod 4$. Because $(D/N) = (D/m)$, the result will now follow from Theorem 3.2. By inspection, one finds that $U(P,Q)$ is purely periodic modulo 4 with its least period equal to 3 or 6. In particular, the initial terms of $U(P,1)$ modulo 4 are

$$0,\ 1,\ P,\ 0,\ -P,\ 3,\ 0,\ 1,\ P, \ldots, \tag{3.7}$$

while the initial terms of $U(P,-1)$ modulo 4 are

$$0,\ 1,\ P,\ 2,\ -P,\ 1,\ 0,\ 1,\ P, \ldots. \tag{3.8}$$

Thus by (3.7) and (3.8), if $m \equiv \delta(D/m) \pmod 6$, where $\delta \in \{-1, 1\}$, then

$$U_{2m}(P,Q)/P \equiv \delta(D/m)PP^{-1} \equiv \delta(D/m) \pmod 4$$

and the theorem follows. □

Theorem 3.3 was proved in Theorem 4 of [11] for the case in which $U(P,Q)$ is the Fibonacci sequence and in Theorem 8 of [16] for the case in which $U(P,Q)$ is the Fibonacci sequence and m is an odd prime.

By Theorem 2.24, there exist infinitely many Frobenius pseudoprimes with respect to a given Lucas sequence $U(P,Q)$, where $Q = \pm 1$. As a counterpoint, we have the following theorem, which follows from Theorems 3.1, 3.3, and 2.25, and from Dirichlet's theorem on primes in arithmetic progressions.

Theorem 3.4. *Consider the Lucas sequence $U(P,Q)$, where $P > 0$, P is odd, and $Q = \pm 1$. Then, there exist infinitely many Lucas pseudoprimes of the form U_{2p}/P that are not Frobenius pseudoprimes, and there exist infinitely many Lucas pseudoprimes of the form U_{2m}/P, where m is a Frobenius pseudoprime, which are not Frobenius pseudoprimes.*

Theorem 3.4 was proved by Rotkiewicz in Theorem 8 of [16] for the case in which $U(P,Q)$ is the Fibonacci sequence.

We have the following examples for Theorem 3.3.

Example 3.5. Consider the Lucas sequence $U(3,-1)$ with discriminant 13. By Theorem 3.3 (i) and inspection, there are 36 odd primes $p < 1000$ for which $\frac{1}{3}U_{2p}$ is a Frobenius pseudoprime, namely,

$$\begin{aligned} p = {} & 43, 61, 79, 103, 127, 139, 157, 181, 199, 211, 277, 283, 313, 337, 367, 373, 433, 439, \\ & 523, 547, 571, 601, 607, 673, 727, 751, 757, 823, 829, 859, 883, 907, 919, 937, 991, 997. \end{aligned}$$

Example 3.6. Consider the Lucas sequence $U(7,1)$ with discriminant $45 = 3^2 \cdot 5$. By Theorem 3.3 (ii) and inspection, there are 79 odd primes $p < 1000$ for which $\frac{1}{7}U_{2p}$ is a Frobenius pseudoprime, namely,

$$\begin{aligned} p = {} & 17, 19, 23, 31, 47, 53, 61, 79, 83, 107, 109, 113, 137, 139, 151, 167, 173, 181, 197, 199, \\ & 211, 227, 229, 233, 241, 257, 263, 271, 293, 317, 331, 347, 349, 353, 379, 383, 409, 421, 439, \\ & 443, 467, 499, 503, 541, 557, 563, 571, 587, 593, 601, 617, 619, 631, 647, 653, 661, 677, 683, 691, \\ & 709, 739, 743, 751, 769, 773, 797, 811, 827, 829, 857, 859, 863, 887, 919, 947, 953, 977, 983, 991. \end{aligned}$$

Example 3.7. Consider the Fibonacci sequence $U(1,-1)$ with discriminant 5. By Theorem 3.3 and Table 5 of [16], there are 31 Frobenius pseudoprimes $m < 10^6$ for which U_{2m} is a Frobenius pseudoprime. These are:

$$\begin{aligned} m = {} & 6721, 13201, 34561, 51841, 64681, 67861, 90061, 96049, 97921, \\ & 118441, 146611, 163081, 186961, 197209, 219781, 252601, 257761, \\ & 268801, 272611, 302101, 399001, 433621, 438751, 489601, 512461, \\ & 520801, 530611, 655201, 741751, 852841, 925681. \end{aligned}$$

Theorem 3.8. *Consider the Lucas sequence $U(P,Q)$, where $Q = \pm 1$. Let N be an odd prime or a Lucas pseudoprime such that $\gcd(N,D) = 1$. Then, N^2 is a Dickson pseudoprime of the second kind.*

Proof. Because N is odd, $N^2 \equiv 1 \pmod 4$. Note that $(D/N^2) = 1$. By the Binet formulas (1.4),

$$V_{N^2-(D/N^2)} - 2Q^{(N^2-(D/N^2))/2} = V_{N^2-1} - 2 = V_{2(N-1)(N+1)/2} - 2 = D(U_{(N-1)(N+1)/2})^2. \quad (3.9)$$

Because N is a Lucas pseudoprime,

$$N \mid U_{N-(D/N)} \mid U_{(N-1)(N+1)/2},$$

which implies that

$$N^2 \mid (U_{(N-1)(N+1)/2})^2. \quad (3.10)$$

It now follows from (3.9) and (3.10) that N^2 is a Dickson pseudoprime of the second kind. □

We note that Theorem 3.8 was proved by Rotkiewicz in the case of the Fibonacci sequence in Theorem 4 of [16].

In Theorems 3.9 and the examples, we show how to generate many Frobenius pseudoprimes and Dickson pseudoprimes of the second kind from a given positive integer that is a super Lucas pseudoprime and a strong Lucas pseudoprime.

Theorem 3.9. *Consider the Lucas sequence $U(P,Q)$, where $Q = \pm 1$. Let*

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

be an odd prime or an integer that is a super Lucas pseudoprime and a strong Lucas pseudoprime, where $\gcd(N, PD) = 1$ and $\rho(p_i^{k_i}) = \rho(p_i) < \rho(p_i^{k_i+1})$ for $i \in \{1, 2, \ldots, s\}$. Then, the following hold:

(i) *Each positive composite divisor of N is a super Frobenius pseudoprime that is also a super strong Lucas pseudoprime. The number of such divisors is equal to*

$$\prod_{i=1}^{s}(k_i + 1) - (s + 1). \tag{3.11}$$

(ii) *Each positive divisor of N^2, which is not a divisor of N, is a super Dickson pseudoprime of the second kind, but not a Frobenius pseudoprime. The number of such divisors of N^2 is equal to*

$$\prod_{i=1}^{s}(2k_i + 1) - \prod_{i=1}^{s}(k_i + 1). \tag{3.12}$$

Proof. (i) If N is a strong Lucas pseudoprime, then by Theorem 2.1, N is an Euler-Lucas pseudoprime, and hence by Theorem 2.2 and Remark 2.3, N is also a Frobenius pseudoprime. Let d be any positive composite divisor of N. Then, d is also a super Lucas pseudoprime. It now follows from Proposition 2.18 and our argument above that d is also a strong Lucas pseudoprime and a Frobenius pseudoprime. The rest of assertion (i) follows by a simple counting argument.

(ii) Suppose that $d \mid N^2$, but $d \nmid N$. Then by Theorem 2.11 (vii), d is composite and $\rho(p^m) \neq \rho(p)$ for some prime p such that $p^m \parallel d$, where $m \geq 2$. Then, $p \mid \rho(p^m)$ by Theorem 2.11 (vii), which implies by Proposition 2.17 that d is not a Lucas pseudoprime, and consequently not a Frobenius pseudoprime.

We show that d is a Dickson pseudoprime of the second kind. Let q be a prime that divides d. Because N is a super Lucas pseudoprime, we see by Theorem 2.22 that

$$q \equiv (D/q) \pmod{\rho(N)}. \tag{3.13}$$

Let $d = q_1 q_2 \cdots q_t$, where the q_is are primes, possibly repeated. Then,

$$\begin{aligned} d - (D/d) &= q_1 \cdots q_t - (D/d) \equiv (D/q_1) \cdots (D/q_t) - (D/d) \\ &\equiv (D/d) - (D/d) \equiv 0 \pmod{\rho(N)}. \end{aligned} \tag{3.14}$$

Thus, $N \mid U_{d-(D/d)}$ by Theorem 2.11 (i). Let

$$\nu_2(\rho(N)) = k. \tag{3.15}$$

Then, $2^k \mid d - (D/d)$ by (3.14).

By the Binet formulas (1.4) and because N is an Euler pseudoprime to the base Q, it follows that

$$\begin{aligned} V_{d-(D/d)} - 2Q^{(d-(D/d))/2} &= DU^2_{(d-(D/d))/2} = V_{d-(D/d)} - 2Q^{(d-1)/2}Q^{(1-(D/d))/2} \\ &\equiv V_{d-(D/d)} - 2(Q/d)Q^{(1-(D/d))/2} \pmod{d} \end{aligned} \tag{3.16}$$

and

$$\begin{aligned} V_{d-(D/d)} + 2Q^{(d-(D/d))/2} &= V^2_{(d-(D/d))/2} = V_{d-(D/d)} + 2Q^{(d-1)/2}Q^{(1-(D/d))/2} \\ &\equiv V_{d-(D/d)} + 2(Q/d)Q^{(1-(D/d))/2} \pmod{d}. \end{aligned} \tag{3.17}$$

We will show that if $(Q/d) = 1$, then $N \mid U_{d-(D/d))/2}$, whereas if $(Q/d) = -1$, then $N \mid V_{d-(D/d))/2}$. Recall that $d \mid N^2$ and $\gcd(N, D) = 1$. Applying (3.16) when $(Q/d) = 1$ and applying (3.17) when $(Q/d) = -1$, it will then follow that d is a Dickson pseudoprime of the second kind. Suppose that p and q are primes such that $p^a \parallel N$ and $q^b \parallel N$. Because N is a strong Lucas pseudoprime, it follows from Proposition 2.18 and Theorem 2.11 (viii) that

$$\nu_2(\rho(p^a)) = \nu_2(\rho(q^b)) = \nu_2(\rho(N)) = k. \tag{3.18}$$

By Proposition 1.1 (i),

$$U_{d-(D/d)} = U_{(d-(D/d))/2}V_{(d-(D/d))/2}.$$

Because $N \mid U_{d-(D/d)}$ and $\nu_2(\rho(p^a) = \nu_2(\rho(q^b) = k$, we see by Theorem 2.11 (i) that $p^aq^b \mid U_{d-(D/d))/2}$ if $\nu_2(d - (D/d)) > k$, whereas $p^aq^b \mid V_{d-(D/d))/2}$ if $\nu_2(d - (D/d)) = k$.

Let $d_1 = \gcd(U_{d-(D/d))/2}, V_{d-(D/d))/2})$. Because $\gcd(N, 2QD) = 1$, we observe by Theorem 2.13 (iii) that $\gcd(d_1, N) = 1$. It now follows that

$$N \mid U_{(d-(D/d))/2} \quad \text{if and only if} \quad 2^{k+1} \mid d - (D/d) \tag{3.19}$$

and

$$N \mid V_{(d-(D/d))/2} \quad \text{if and only if} \quad 2^k \parallel d - (D/d). \tag{3.20}$$

By (3.13) and (3.15), we can order the primes $q_1, \ldots, q_t$, not necessarily distinct, dividing d so that

$$q_i \equiv (D/q_i) + 2^k \pmod{2^{k+1}}$$

for $i = 1, 2, \ldots, \ell$ and

$$q_i \equiv (D/q_i) \pmod{2^{k+1}}$$

$i = \ell + 1, \ldots, t$. Set $\ell = 0$ if $q_i \equiv (D/q_i) \pmod{2^{k+1}}$ for $i = 1, \ldots, t$. Then,

$$\begin{aligned} d - (D/d) &\equiv \prod_{i=1}^{\ell}((D/q_i) + 2^k) \cdot \prod_{i=\ell+1}^{t} (D/q_i) - (D/d) \\ &\equiv (D/d)(1 + \sum_{i=1}^{\ell} 2^k) - (D/d) \equiv \sum_{i=1}^{\ell} 2^k \pmod{2^{k+1}}. \end{aligned} \tag{3.21}$$

Empty products in (3.21) are interpreted as being equal to 1 and empty sums in (3.21) are considered to be equal to 0. Thus, $2k \parallel d - (D/d)$ if and only if ℓ is odd. It now follows from (3.19) and (3.20) that

$$N \mid U_{(d-(D/d))/2} \quad \text{if and only if} \quad \ell \text{ is even}, \tag{3.22}$$

whereas

$$N \mid V_{(d-(D/d))/2} \quad \text{if and only if} \quad \ell \text{ is odd}. \tag{3.23}$$

Noting that if N is an odd prime, then N satisfies congruence (1.9) or congruence (1.10), it follows that for $i = 1, \ldots, t$ we have

$$(Q/q_i) = 1 \quad \text{if and only if} \quad U_{(d-(D/d))/2} \equiv 0 \pmod{q_i}, \tag{3.24}$$

whereas

$$(Q/q_i) = -1 \quad \text{if and only if} \quad V_{(d-(D/d))/2} \equiv 0 \pmod{q_i}. \tag{3.25}$$

Notice that (3.19) and (3.20) both hold if $d > 1$ is any prime divisor of N^2, not just a divisor of N^2 not dividing N. It now follows from (3.19), (3.20), (3.24), and (3.25) that

$$(Q/q_i) = 1 \quad \text{if and only if} \quad 2^{k+1} \mid d - (D/d), \tag{3.26}$$

whereas

$$(Q/q_i) = -1 \quad \text{if and only if} \quad 2^k \parallel d - (D/d) \tag{3.27}$$

for $i = 1, \ldots, t$. Then,

$$(Q/d) = \prod_{i=1}^{t} (Q/q_i) = \prod_{i=1}^{\ell} (-1) \cdot \prod_{i=\ell+1}^{t} 1 = (-1)^{\ell}. \tag{3.28}$$

It now follows from (3.28), (3.22), and (3.23) that

$$(Q/d) = 1 \quad \text{if and only if} \quad N \mid U_{(d-(D/d))/2}, \tag{3.29}$$

whereas

$$(Q/d) = -1 \quad \text{if and only if} \quad N \mid V_{(d-(D/d))/2} \tag{3.30}$$

for $i = 1, \ldots, t$, as desired. The remainder of part (ii) now follows from a straightforward counting argument. □

Theorem 3.10. *Consider the Lucas sequence $U(P, Q)$, where $Q = \pm 1$. Then, there are infinitely many Dickson pseudoprimes of the second kind that are not Frobenius pseudoprimes.*

Proof. Let p be any prime such that $p \nmid QD$. Suppose that $\rho(p^k) = \rho(p)$, but $\rho(p^{k+1}) \neq \rho(p)$. Then by Theorem 3.9 (ii) and Proposition 2.17, p^i is a Dickson pseudoprime of the second kind for $k + 1 \leq i \leq 2k$, but p^i is not a Lucas pseudoprime. The result now follows. □

Theorem 3.10 was proved by Rotkiewicz in Theorem 9 of [16] for the case in which $U(P, Q)$ is the Fibonacci sequence.

In the examples below, we illustrate Theorems 3.9 and 3.10 by finding integers N that are super Frobenius pseudoprimes and super strong Lucas pseudoprimes with a large number of composite divisors. In Example 3.11, for any two prime divisors p and q of N, $\rho(p) = \rho(q)$, whereas in Example 3.12, there exist prime divisors p and q of N for which $\rho(p) \neq \rho(q)$. In these examples, we make use of factorizations of large Fibonacci numbers given in the website `mersennus.net/fibonacci/f1000.txt`.

Example 3.11. Consider the Fibonacci sequence $U(1, -1)$. Let $N = p_1 \cdots p_8$, where the primes p_i are given by

$$p_1 = 13421,\ p_2 = 93941,\ p_3 = 197273,\ p_4 = 575717,\ p_5 = 844117,\ p_6 = 12239041,$$
$$p_7 = 172189606346553144129857452596316985 69,$$
$$p_8 = 133966687249177599369698223968340643079471970600954572 57.$$

Then, $\rho(p_i) = 671$ for $i = 1, \ldots, 8$, and by Proposition 2.18 and Theorem 3.9 (i), each of the $2^8 - 9 = 247$ composite divisors of N is a super Frobenius pseudoprime and super strong Lucas pseudoprime. Moreover, by Theorem 3.9 (ii), each of the $3^8 - 2^8 = 6305$ divisors of N^2 that are not divisors of N is a super Dickson pseudoprime of the second kind.

Example 3.12. Consider the Fibonacci sequence $U(1,-1)$. Let $N = p_1 \cdots p_7$, where the primes p_i are given by

$$p_1 = 3821263937,\ p_2 = 2089,\ p_3 = 20357,\ p_4 = 36017,\ p_5 = 40193,$$
$$p_6 = 322073,\ p_7 = 6857029027549.$$

Then, $\rho(p_1) = 87$ and $\rho(p_i) = 261 = 3 \cdot 87$ for $i = 2, 3, \ldots, 7$. Thus, $\rho(N) = 261$ by Theorem 2.11 (viii). Furthermore,

$$p_i \equiv (D/p_i) \equiv (5/p_i) \equiv (p_i/5) \equiv 1 \pmod{261} \quad \text{for } i = 1, \ldots, 7.$$

Therefore, N is a super Lucas pseudoprime by Theorem 2.22. Because N is a Lucas pseudoprime, it follows by Proposition 2.18 that N is a strong Lucas pseudoprime. It now follows from Theorem 3.9 (i) that each of the $2^7 - 8 = 120$ composite divisors of N is a super Frobenius pseudoprime and super strong Lucas pseudoprime. Moreover, by Theorem 3.9 (ii), each of the $3^7 - 2^7 = 2059$ divisors of N^2 that are not divisors of N is also a super Dickson pseudoprime of the second kind.

Example 3.13. Let $U(P,Q)$ be a Lucas sequence, where $Q = \pm 1$. Let p be any prime such that $\gcd(p, PD) = 1$ and $\rho(p^2) \neq \rho(p)$. Then by Theorem 3.9 (ii) and the proof of Theorem 3.10, p^2 is a super Dickson pseudoprime of the second kind but not a Frobenius pseudoprime. It is known that for the Fibonacci sequence $U(1,-1)$, there are no primes p such that $\rho(p^2) = \rho(p)$ for $p < 9.7 \cdot 10^{14}$ (see [4]).

Now, consider the Lucas sequence $U(5639,-1)$. By inspection, one sees that $\rho(19^4) = \rho(19) = 6$, while $\rho(19^5) = 6 \cdot 19 = 114 \neq \rho(19)$. Then by Corollary 2.4, Proposition 2.18, Theorem 3.9, and the proof of Theorem 3.10, 19^i is a super strong Lucas pseudoprime and a super Frobenius pseudoprime for $i = 2, 3, 4$, whereas 19^i is a super Dickson pseudoprime of the second kind but not a Frobenius pseudoprime for $i = 5, 6, 7, 8$.

Let $U(P,Q)$ be a given Lucas sequence, where $Q = \pm 1$. Theorem 3.9 states that if N is a super Lucas pseudoprime and a strong Lucas pseudoprime, then N is a super Frobenius pseudoprime and N^2 is a Dickson pseudoprime of the second kind. By way of contrast, Example 3.14 gives instances in which N is a Frobenius pseudoprime or N^2 is a Dickson pseudoprime of the second kind, but it is not the case that N is both a super Lucas pseudoprime and a strong Lucas pseudoprime.

Example 3.14. Consider the Fibonacci sequence $U(1,-1)$.

(i) By Table 5 of [16], $6721 = 11 \cdot 13 \cdot 47$ is a Frobenius pseudoprime. We observe that $\rho(11) = 10$, $\rho(13) = 7$, and $\rho(47) = 16$. It follows however from Theorem 2.22 and Proposition 2.18 that 6721 is not a super Lucas pseudoprime and N is not a strong Lucas pseudoprime.

(ii) By Table 5 of [16], $925681 = 23 \cdot 167 \cdot 241$ is a Frobenius pseudoprime. By inspection, $\rho(23) = 24$, $\rho(167) = 168$, and $\rho(241) = 120$. It now follows that 925681 is not a super Lucas pseudoprime, but N is a strong Lucas pseudoprime.

(iii) Let $N = 377 = 13 \cdot 29$. By Table 1 of [16] and by Theorem 3.8, N is a Lucas pseudoprime and N^2 is a Dickson pseudoprime of the second kind. By Table 4 of [16], $4901 = 13^2 \cdot 29$ is also a Dickson pseudoprime of the second kind, but $10933 = 13 \cdot 29^2$ is not a Dickson pseudoprime of the second kind. Thus, N^2 is not a super Dickson pseudoprime of the second kind.

(iv) Let $N = p_1 \cdots p_6$, where the primes p_i are given by

$$p_1 = 541,\ p_2 = 1114769954367361,\ p_3 = 271,\ p_4 = 811,\ p_5 = 42391,\ p_6 = 119611.$$

Then, $\rho(p_1) = 90$, $\rho(p_2) = 135$, and $\rho(p_i) = 270$ for $i = 3, 4, 5, 6$. Thus, by Theorem 2.11 (viii), $\rho(N) = 270$. By inspection, one sees that

$$(D/p_i) = (5/p_i) = (p_i/5) = (1/5) = 1$$

and

$$p_i \equiv (D/p_i) \equiv 1 \pmod{270}$$

for $i = 1, \ldots, 6$. Thus, N is a super Lucas pseudoprime by Theorem 2.22. Further, by Proposition 2.18, N is not a strong Lucas pseudoprime. Moreover, we see that $(D/N) = (5/N) = 1$ and $N \equiv (D/N) \equiv 1 \pmod 4$. Noting that $2 \parallel \rho(N) = 270$, it now follows from Theorem 3.2 that N is a Frobenius pseudoprime.

By inspection, one sees that 41 of the composite divisors of N are Frobenius pseudoprimes, whereas the remaining 16 composite divisors of N are not Frobenius pseudoprimes.

In Theorem 3.9, it was shown that the integer N being a super Lucas pseudoprime and a strong Lucas pseudoprime guarantees that N is also a super Frobenius pseudoprime and N^2 is a super Dickson pseudoprime of the second kind. A necessary condition for N to be a super Frobenius pseudoprime is for N to be a super Lucas pseudoprime. The following theorem shows that it is possible for N to be a super Frobenius pseudoprime and N^2 to be a super Dickson pseudoprime of the second kind if N is a super Lucas pseudoprime but not a strong Lucas pseudoprime.

Theorem 3.15. *Consider the Lucas sequence $U(P, Q)$, where $Q = \pm 1$. Let*

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

be a super Lucas pseudoprime that is not a strong Lucas pseudoprime, where $\gcd(N, PD) = 1$. Suppose that $\rho(p_i^{k_i}) = \rho(p_i) < \rho(p_i^{k_i+1})$ for $i \in \{1, 2, \ldots, s\}$. Suppose further that $p_i \equiv (D/p_i) \pmod{2\rho(N)}$ for $i \in \{1, 2, \ldots, s\}$. Then, $(Q/p_i) = 1$. Moreover, if $Q = -1$, then $p_i \equiv 1 \pmod 4$ and $(D/p_i) = 1$ for $i \in \{1, \ldots, s\}$. Further, the following hold:

(i) *Each positive composite divisor of N is a super Frobenius pseudoprime. The number of such divisors is equal to*

$$\prod_{i=1}^{s}(k_i + 1) - (s + 1). \tag{3.31}$$

(ii) *Each positive divisor of N^2, which is not a divisor of N, is a super Dickson pseudoprime of the second kind, but not a Frobenius pseudoprime. The number of such divisors of N^2 is equal to*

$$\prod_{i=1}^{s}(2k_i + 1) - \prod_{i=1}^{s}(k_i + 1). \tag{3.32}$$

Proof. Because N is a Lucas pseudoprime that is not a strong Lucas pseudoprime, it follows by Corollary 2.19 that $2 \mid \rho(N)$. Suppose that $p \mid N$. Then,

$$p \equiv (D/p) \pmod{2\rho(N)} \tag{3.33}$$

by hypothesis. Hence,

$$(p - (D/p))/2 \equiv 0 \pmod{\rho(N)}. \tag{3.34}$$

Because $\rho(p) \mid \rho(N)$ by Theorem 2.11 (vi), we see from (3.34) that

$$(p - (D/p))/2 \equiv 0 \pmod{\rho(p)}. \tag{3.35}$$

It now follows from Theorem 2.11 (i) that

$$p \mid U_{(p-(D/p))/2},$$

which implies by Theorem 2.11 (iv) that $(Q/p) = 1$. If $Q = -1$, we now see by Euler's criterion that $p \equiv 1 \pmod 4$. Because $4 \mid 2\rho(N)$, we find by (3.33) that $(D/p) = 1$ when $Q = -1$. Let $d > 1$ be an integer such that if $p \mid d$, then $p \mid N$. Let $d = q_1 q_2 \cdots q_t$, where the q_is are primes, possibly repeated. In the proof of part (i), we will let d be a composite divisor of N. In the proof of part (ii), we will let d be a divisor of N^2, which is not a divisor of N. By (3.33), our earlier discussion, and the properties of the Jacobi symbol, we see that

$$(Q/d) = (Q/q_1 \cdots q_t) = (Q/q_1) \cdots (Q/q_t) = 1^t = 1 \tag{3.36}$$

and

$$\begin{aligned} d - (D/d) &= q_1 \cdots q_t - (D/d) \equiv (D/q_1) \cdots (D/q_t) - (D/d) \equiv (D/q_1 \cdots q_t) - (D/d) \\ &\equiv (D/d) - (D/d) \equiv 0 \pmod{2\rho(N)}. \end{aligned} \tag{3.37}$$

Thus,

$$\rho(N) \mid (d - (D/d))/2, \tag{3.38}$$

which implies by Theorem 2.11 (i) that

$$N \mid U_{(d-(D/d))/2}. \tag{3.39}$$

We also note that if $Q = -1$, it follows by a similar argument as that used for the evaluation of (Q/d) in (3.36) that $(D/d) = 1$.

(i) Let d be a composite divisor of N. Because $d \mid N$, we see by (3.36) and (3.39) that d is an Euler-Lucas pseudoprime. Hence, by Theorem 2.2 and Remark 2.3, d is a Frobenius pseudoprime, which yields that N is a super Frobenius pseudoprime. The remainder of part (i) now follows by a simple counting argument.

(ii) Let d be a divisor of N^2, which is not a divisor of N. By the proof of part (ii) of Theorem 3.9, d is not a Frobenius pseudoprime. By (3.16) in the proof of Theorem 3.9 (ii) and Remark 2.3, we see that

$$\begin{aligned} V_{d-(D/d)} - 2Q^{(d-(D/d))/2} &= DU^2_{(d-(D/d))/2} = V_{d-(D/d)} - 2Q^{(d-1)/2}Q^{(1-(D/d))/2} \\ &= V_{d-(D/d)} - 2(Q/d)Q^{(1-(D/d))/2} \end{aligned} \tag{3.40}$$

By (3.39), $N^2 \mid U^2_{(d-(D/d))/2}$. Because $d \mid N^2$ and $(Q/d) = 1$ by (3.36), it follows from (3.40) that d is a super Dickson pseudoprime of the second kind. The rest of part (ii) follows by a straightforward counting argument.

□

Example 3.16. Consider the Fibonacci sequence $U(1, -1)$. Let $N = p_1 \cdots p_4$, where the primes p_i are given by

$$p_1 = 3001,\ p_2 = 570601,\ p_3 = 601,\ p_4 = 87129547172401.$$

Then $\rho(p_1) = 25$, $\rho(p_2) = 100$, and $\rho(p_i) = 300$ for $i = 3, 4$. Thus, $\rho(N) = 300$ by Theorem 2.11 (viii). Moreover,

$$p_i \equiv (D/p_i) \equiv (5/p_i) \equiv (p_i/5) \equiv 1 \pmod{600} \quad \text{for } i = 1, \ldots, 4.$$

Therefore, N is a super Lucas pseudoprime by Theorem 2.22. We observe by Proposition 2.18 that N is not a strong Lucas pseudoprime. It now follows from Theorem 3.15 (i) that each of the $2^4 - 5 = 11$ composite divisors of N is also a Frobenius pseudoprime. Moreover, by

Theorem 3.15 (ii), each of the $3^4 - 2^4 = 65$ divisors of N^2 that are not divisors of N is also a Dickson pseudoprime of the second kind.

The following theorem shows that for special values of P and Q, there exist infinitely many odd positive odd integers N, each having any prescribed number of distinct prime divisors, such that for the Lucas sequence $U(P,Q)$, we have that N is a super Frobenius pseudoprime and a super strong pseudoprime and that N^2 is a super Dickson pseudoprime of the second kind. We let $\tau(n)$ denote the number of distinct positive divisors of the positive integer n. Note that if A is any positive integer greater than 1, then $\tau(p^{A-1}) = A$ when p is a prime. Because τ is a multiplicative function, it follows that if m is any positive integer, then there exists a positive integer n such that $\tau(n) = m$. Moreover, it is easily seen that if M is any positive integer, we can choose this positive integer n so that $\gcd(n, M) = 1$.

Theorem 3.17. *Let $C > 1$ be a fixed integer. Let $U(P_1, Q_1)$ be a nondegenerate Lucas sequence for which $Q_1 = \pm 1$. Let D_1 be the discriminant of $U(P_1, Q_1)$. Let k be a positive integer such that $\tau(k) = C$ and $\gcd(k, D_1) = 1$. Let $P = V_k(P_1, Q_1)$ and $Q = Q_1^k$. Then, $U(P,Q) = U(P, \pm 1)$ is also a nondegenerate Lucas sequence with discriminant*

$$D = D_1 U_k^2(P_1, Q_1). \tag{3.41}$$

Let $p > 3$ be any prime such that $p \nmid kD_1$. Let d_i, $i = 1, 2, \ldots, C$, be the distinct positive divisors of k. Then, $U_{pd_i}(P_1, Q_1)$ has an odd primitive prime divisor p_i that is also a primitive prime divisor of $U_p(P,Q)$ and which is relatively prime to D. Let $N = p_1 p_2 \cdots p_C$. Then, $\gcd(N, D) = 1$ and N is a super Frobenius pseudoprime and a super strong Lucas pseudoprime with respect to $U(P,Q)$. Further, N^2 is a super Dickson pseudoprime of the second kind with respect to $U(P,Q)$.

Proof. By Theorem 2.16, $U(P,Q) = U(P, \pm 1)$ is a nondegenerate Lucas sequence with discriminant $D = D_1 U_k^2(P_1, Q_1)$. By Theorem 2.9, $U_{pd_i}(P_1, Q_1)$ has an odd primitive prime divisor p_i for $i = 1, 2, \ldots, C$. Because $p \nmid k$, we have that $pd_i \nmid k$. It now follows from Theorem 2.11 (i) that $p_i \nmid U_k(P_1, Q_1)$. Hence,

$$\gcd(N, U_k(P_1, Q_1)) = 1. \tag{3.42}$$

We further note that if $i \in \{1, \ldots, C\}$, then by Proposition 1.1 (iii), $p_i \mid U_{pk}(P_1, Q_1)$, because $pd_i \mid pk$. Thus,

$$N \mid U_{pk}(P_1, Q_1). \tag{3.43}$$

It follows from Theorem 2.11 (i), (iii), and (viii) that if $n \geq 1$, then $\gcd(D_1, U_n(P_1, Q_1)) > 1$ only if $\gcd(D_1, n) > 1$. We note by hypothesis that $\gcd(D_1, pk) = 1$. Therefore,

$$\gcd(D_1, U_{pk}(P_1, Q_1)) = 1.$$

It now follows from (3.43) that $\gcd(N, D_1) = 1$. Because $D = D_1 U_k^2(P_1, Q_1)$, it then follows from (3.42) that $\gcd(N, D) = 1$.

We observe by Proposition 1.1 (iii) that

$$U_{pd_i}(P_1, Q_1) \mid U_{pk}(P_1, Q_1)$$

for $i = 1, \ldots, C$. Notice by Theorem 2.16 that

$$U_p(P,Q) = \frac{U_{pk}(P_1, Q_1)}{U_k(P_1, Q_1)}. \tag{3.44}$$

Because $U_1 = 1$ and $pd_i \nmid k$ for $1 \leq i \leq C$, it follows from (3.44) and Theorem 2.11 (i) that p_i is a primitive prime divisor of $U_p(P,Q)$ for $i = 1, \ldots, C$. Thus, by Corollary 2.4 and Proposition 2.18, N is a super Frobenius pseudoprime and a super strong Lucas pseudoprime with respect

to $U(P,Q)$. Moreover, by Theorem 3.9 (ii), N^2 is a super Dickson pseudoprime of the second kind with respect to $U(P,Q)$. □

Acknowledgment

We express our appreciation to the anonymous referee for the careful reading of the paper and improvements to our paper. This paper was supported by RVO 67985840 of the Czech Republic.

References

[1] R. Baillie and S. S. Wagstaff, Jr., *Lucas pseudoprimes*, Math. Comp., **35** (1980), 1391–1417.
[2] Y. Bilu, G. Hanrot, and P. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine. Angew., **539** (2001), 75–122.
[3] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math., **15** (1913), 30–70.
[4] F. G. Dorais and D. Klyve, *A Wieferich prime search up to* 6.7×10^{15}, J. Integer Seq., **14** (2011), Article 11.9.2, 1–14.
[5] P. Hilton, J. Pedersen, and L. Somer, *On Lucasian numbers*, The Fibonacci Quarterly, **35.1** (1997), 43–47.
[6] P. Kiss, *Some results on Lucas pseudoprimes*, Ann. Univ. Eőtvős Sect. Math., **28** (1985), 153–159.
[7] M. Křížek, F. Luca, and L. Somer, *17 Lectures on Fermat Numbers*, Springer-Verlag, New York, 2001.
[8] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math., **31** (1930), 419–448.
[9] 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.
[10] W. McDaniel, *The G. C. D. in Lucas sequences and Lehmer number sequences*, The Fibonacci Quarterly, **29.1** (1991), 24–29.
[11] E. A. Parberry, *On primes and pseudo-primes related to the Fibonacci sequence*, The Fibonacci Quarterly, **8.1** (1970), 49–60.
[12] B. M. Phong, *On super Lucas and super Lehmer pseudoprimes*, Studia Sci. Math. Hungar., **23** (1988) 435–442.
[13] P. Ribenboim, *The New Book of Prime Number Records*, Springer, New York, 1996.
[14] A. Rotkiewicz, *On the pseudoprimes with respect to the Lucas sequence*, Bull. Acad. Polon. Sci. Sér. 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] L. Somer, *Lucas sequences* $\{U_k\}$ *for which* U_{2p} *and* U_p *are pseudoprimes for almost all primes* p, The Fibonacci Quarterly, **44.1** (2006), 7–12.
[18] L. Somer and M. Křížek, *On Lehmer superpseudoprimes*, The Fibonacci Quarterly, **53.3** (2015), 206–212.
[19] M. Ward, *Prime divisors of second order recurring sequences*, Duke Math. J., **21** (1954), 607–614.

MSC2020: 11B39, 11A51

Department of Mathematics, Catholic University of America, Washington, D.C. 20064, U.S.A.
Email address: somer@cua.edu

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