LUCAS PSEUDOPRIMES OF SPECIAL TYPES

LAWRENCE SOMER

Abstract. Rotkiewicz has shown that there exist Fibonacci pseudoprimes having the forms $p(p+2)$, $p(2p-1)$, and $p(2p+3)$, where all the terms in the products are odd primes. Assuming Dickson's conjecture on prime k-tuples, we generalize this result by finding an infinite class of Lucas sequences, each having infinitely many Lucas pseudoprimes of the five types: $p(p+2)$, $p(2p-3)$, $p(2p-1)$, $p(2p+1)$, and $p(2p+3)$.

1. Introduction

It is well-known that if n is an odd prime, then

$$F_{n-(D/n)} \equiv 0 \pmod{n} \tag{1.1}$$

(see [3, p. 150]), where $D = 5$ is the discriminant of $\{F_n\}$ and (D/n) denotes the Jacobi symbol. In rare instances, there exist odd composite integers n such that n also satisfies congruence (1.1). These integers are called *Fibonacci pseudoprimes.* In [7], Rotkiewicz proved the following theorem.

Theorem 1.1. *(Rotkiewicz): Let p and q be odd primes.*

(i) *If $q = p+2$, then pq is a Fibonacci pseudoprime if and only if $p \equiv 7 \pmod{10}$.*
(ii) *If $q = 2p-1$, then pq is a Fibonacci pseudoprime if and only if $p \equiv 1 \pmod{10}$.*
(iii) *If $q = 2p+3$, then pq is a Fibonacci pseudoprime if and only if $p \equiv 3 \pmod{10}$.*

We note that the smallest Fibonacci pseudoprime is $323 = 17 \cdot 19$, which is of the form given in Theorem 1.1 (i). Dickson [2] in 1904 conjectured the following.

Conjecture 1.2. *(Prime k-tuples conjecture): If $a_1, b_1, \ldots, a_k, b_k$ are integers with each $a_i > 0$, each $\gcd(a_i, b_i) = 1$, and for each prime $p \leq k$, there is some integer n with no $a_i n + b_i$ divisible by p, then there are infinitely many positive integers n with each $a_i n + b_i$ prime.*

Assuming Conjecture 1.2, which is widely believed, for the case $k = 2$, one sees that if p and q are odd primes, then there are infinitely many Fibonacci pseudoprimes satisfying each of conditions (i), (ii), and (iii) of Theorem 1.1. We will generalize Theorem 1.1 to more general pseudoprimes called *Lucas pseudoprimes with parameters P and Q.* First we need the following definitions and results. Let $U(P,Q)$ and $V(P,Q)$ denote the Lucas sequences satisfying the second-order recursion relation

$$W_{k+2} = PW_{k+1} - QW_k, \tag{1.2}$$

where P and Q are integers, $Q \neq 0$, and $U_0 = 0,\ U_1 = 1,\ V_0 = 2,\ V_1 = P$. Associated with both $U(P,Q)$ and $V(P,Q)$ is the characteristic polynomial

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

with characteristic roots α and β. Let $D = P^2 - 4Q = (\alpha - \beta)^2$ be the discriminant of $U(P, Q)$. We assume that $D \neq 0$. By the Binet formulas,

$$U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} \tag{1.3}$$

and

$$V_k = \alpha^k + \beta^k. \tag{1.4}$$

It follows from (1.3) that if $m|n$, then $U_m|U_n$. The Lucas sequence $U(P, Q)$ is called *degenerate* if α/β is a root of unity. In particular, if $P = 0$, then $U(P, Q)$ is degenerate. It follows from the Binet formula (1.3) that U_k can equal 0 for some $k > 0$ only if $U(P, Q)$ is degenerate. The following theorem is fundamental.

Theorem 1.3. *Let $U(P, Q)$ be a Lucas sequence and let p be an odd prime such that $p \nmid PQ$. Then*

$$p|U_{p-(D/p)}. \tag{1.5}$$

Moreover,

$$p|U_{(p-(D/p))/2} \text{ if and only if } (Q/p) = 1. \tag{1.6}$$

Proof. Proofs of (1.5) are given in [6, pp. 290, 296, 297] and [1, pp. 44-45]. A proof of (1.6) is given in [5, p. 441]. □

2. The Main Theorems

We now present our main results.

Theorem 2.1. *Let $U(P, Q)$ be a Lucas sequence with discriminant D. Let p and q be distinct odd primes such that* $\gcd(pq, QD) = 1$. *Then pq is a Lucas pseudoprime with parameters P and Q in the following cases:*

(i) $q = p + 2$, $(D/p) = -1$, *and* $(D/q) = 1$. *Then $p(p + 2)$ is called a Lucas pseudoprime of type 1.*

(ii) $q = 2p - 3$, $(Q/q) = 1$, $(D/p) = 1$, *and* $(D/q) = -1$. *Then $p(2p - 3)$ is called a Lucas pseudoprime of type 2.*

(iii) $q = 2p - 1$, $(Q/q) = 1$, $(D/p) = 1$, *and* $(D/q) = 1$. *Then $p(2p - 1)$ is called a Lucas pseudoprime of type 3.*

(iv) $q = 2p + 1$, $(Q/q) = 1$, $(D/p) = -1$, *and* $(D/q) = -1$. *Then $p(2p + 1)$ is called a Lucas pseudoprime of type 4.*

(v) $q = 2p + 3$, $(Q/q) = 1$, $(D/p) = -1$, *and* $(D/q) = 1$. *Then $p(2p + 3)$ is called a Lucas pseudoprime of type 5.*

Proof.

(i) By (1.5), $p|U_{p-(D/p)} = U_{p+1}$ and $q|U_{q-(D/q)} = U_{p+1}$. Hence, $pq|U_{p+1}$. Note that

$$pq - (D/pq) = p(p + 2) + 1 = (p + 1)^2.$$

It now follows that $pq|U_{pq-(D/pq)}$, and pq is a Lucas pseudoprime with parameters P and Q.

(ii) By (1.5) and (1.6), we see that $p|U_{p-1}$ and $q|U_{(q-(D/q))/2} = U_{p-1}$. Thus, $pq|U_{p-1}$. Moreover,

$$pq - (D/pq) = p(2p - 3) + 1 = (p - 1)(2p - 1).$$

Hence, $pq|U_{pq-(D/pq)}$, implying that pq is a Lucas pseudoprime.

(iii) We observe that $p|U_{p-1}$ and $q|U_{(q-1)/2} = U_{p-1}$. Consequently, $pq|U_{p-1}$. Furthermore,

$$pq - (D/pq) = p(2p-1) - 1 = (p-1)(2p+1).$$

Thus, $pq|U_{pq-(D/pq)}$, and pq is a Lucas pseudoprime.

(iv) Notice that $p|U_{p+1}$ and $q|U_{(q-(D/q))/2} = U_{p+1}$. Therefore, $pq|U_{p+1}$. Also,

$$pq - (D/pq) = p(2p+1) - 1 = (p+1)(2p-1).$$

Hence, $pq|U_{pq-(D/pq)}$, and pq is a Lucas pseudoprime.

(v) Note that $p|U_{p+1}$ and $q|U_{(q-(D/q))/2} = U_{p+1}$. Thus, $pq|U_{p+1}$. Moreover,

$$pq - (D/pq) = p(2p+3) + 1 = (p+1)(2p+1).$$

Hence, $pq|U_{pq-(D/pq)}$, and pq is a Lucas pseudoprime.

□

Recall that p is a Sophie Germain prime of the second kind if both p and $2p-1$ are primes. Using the standard definition, we let $\omega(n)$ denote the number of distinct prime divisors of n.

Corollary 2.2. *Let $U(P,Q)$ be a Lucas sequence. Let $D = D_0^2$ and $Q = Q_0^2$ for some positive integers D_0 and Q_0. Then $p(2p-1)$ is a Lucas pseudoprime of type 3 with parameters P and Q for every odd prime p which is a Sophie Germain prime of the second kind such that* $\gcd(p(2p-1), D_0) = \gcd(2p-1, Q_0) = 1$. *Moreover, if $Q_0 > 1$ is a fixed integer, there exist $2^{\omega(Q_0)}$ distinct Lucas sequences $U(P, Q_0^2)$ such that* $\gcd(P, Q_0) = 1$ *and D is a nonzero square.*

Proof. Let p be a Sophie Germain prime of the second kind such that $\gcd(p(2p-1), D_0) = \gcd(2p-1, Q_0) = 1$. Since $(D_0^2/p) = (D_0^2/2p-1) = (Q_0^2/2p-1) = 1$, we see by Theorem 2.1 (iii) that $p(2p-1)$ is a Lucas pseudoprime of type 3 with parameters P and Q. It follows from [8] that there exist $2^{\omega(Q_0)}$ Lucas sequences $U(P, Q_0^2)$ such that $\gcd(P, Q_0) = 1$ and D is a nonzero square. □

Assuming that Conjecture 1.2 is true, we will show in Theorems 2.3 and 2.6 that for infinitely many values of D, there exist infinitely many Lucas pseudoprimes with parameters P and Q of each of the types 1 - 5 for any nondegenerate Lucas sequence $U(P,Q)$ with discriminant D.

Theorem 2.3. *Let $U(P,Q)$ be a nondegenerate Lucas sequence with discriminant $D < 0$. If Conjecture 1.2 is true, then there are infinitely many Lucas pseudoprimes pq with parameters P and Q of each of the types 1 - 5, where p and q are distinct odd primes.*

Proof. Since $D < 0$, we have $Q > P^2/4 > 0$. Let $D = -2^\gamma D_0^2 D_1$ and $Q = 2^\lambda Q_0^2 Q_1$, where $\gamma = 0$ or 1, $\lambda = 0$ or 1, and both D_1 and Q_1 are positive, odd, and square-free. Let $A = 2^\gamma D_1$ and $H = lcm(2^\gamma D_1, 2^\lambda Q_1)$. Note that $A|H$. In parts (i) - (v) of this proof, we will successively generate infinitely many Lucas pseudoprimes with parameters P and Q of each of the types 1 - 5, assuming that Conjecture 1.2 is true. We will use Conjecture 1.2 to choose $p \equiv \pm 1 \pmod{4B}$, where $B = A$ for part (i) and $B = H$ for parts (ii) - (v). If $p \equiv \pm 1 \pmod{4A}$, $q \equiv \pm 1 \pmod{4A}$, and $\gamma = 1$, then $p \equiv \pm 1 \pmod 8$ and $q \equiv \pm 1 \pmod 8$. Hence,

$$(2^\gamma/p) = (2^\gamma/q) = 1, \tag{2.1}$$

whether $\gamma = 0$ or $\gamma = 1$. Similarly, if $p = \pm 1 \pmod{4H}$ and $q = \pm 1 \pmod{4H}$, then

$$(2^\lambda/p) = (2^\lambda/q) = 1 \tag{2.2}$$

for both the cases in which $\lambda = 0$ or $\lambda = 1$. By the law of quadratic reciprocity for the Jacobi symbol, we see that

$$(D_1/p) = (D_1/q) = 1 \tag{2.3}$$

when both $p = \pm 1 \pmod{4A}$ and $q = \pm 1 \pmod{4A}$. Analogously,

$$(Q_1/q) = 1 \tag{2.4}$$

when $q = \pm 1 \pmod{4H}$. From (2.1) - (2.4), we obtain

$$(D/p) = (D_0^2/p)(-1/p)(2^\gamma/p)(D_1/p) = (1)(-1/p)(1)(1) = (-1/p) \tag{2.5}$$

when $p \equiv \pm 1 \pmod{4A}$,

$$(D/q) = (D_0^2/q)(-1/q)(2^\gamma/q)(D_1/q) = (-1/q) \tag{2.6}$$

when $q \equiv \pm 1 \pmod{4A}$, and

$$(Q/q) = (Q_0^2/q)(2^\lambda/q)(Q_1/q) = 1 \tag{2.7}$$

when $q = \pm 1 \pmod{4H}$.

(i) By Conjecture 1.2, we can choose infinitely many pairs of primes p and q such that $p \equiv -1 \pmod{4A}$ and $q = p + 2 \equiv 1 \pmod{4A}$. Then by (2.5) and (2.6),

$$(D/p) = (-1/p) = -1 \text{ and } (D/q) = (-1/q) = 1,$$

and $p(p+2)$ is a Lucas pseudoprime of type 1 with parameters P and Q by Theorem 2.1 (i).

(ii) Choose $p \equiv 1 \pmod{4H}$. Then $q = 2p - 3 \equiv -1 \pmod{4H}$. Hence, by (2.5), (2.6), and (2.7), we see that $(D/p) = (-1/p) = 1$, $(D/q) = (-1/q) = -1$, and $(Q/q) = 1$. Therefore, by Theorem 2.1 (ii), $p(2p - 3)$ is a Lucas pseudoprime of type 2.

(iii) Choose $p \equiv 1 \pmod{4H}$. Then $q = 2p - 1 \equiv 1 \pmod{4H}$. Thus, by (2.5) - (2.7), it follows that $(D/p) = (-1/p) = 1$, $(D/q) = (-1/q) = 1$, and $(Q/q) = 1$. By Theorem 2.1 (iii), we see that $p(2p - 1)$ is a Lucas pseudoprime of type 3.

(iv) Choose $p \equiv -1 \pmod{4H}$. Then $q = 2p + 1 \equiv -1 \pmod{4H}$. Therefore, $(D/p) = (-1/p) = -1$, $(D/q) = (-1/q) = -1$, and $(Q/q) = 1$. Hence, $p(2p + 1)$ is a Lucas pseudoprime of type 4 by Theorem 2.1 (iv).

(v) Choose $p \equiv -1 \pmod{4H}$. Then $q = 2p + 3 \equiv 1 \pmod{4H}$. Consequently, $(D/p) = (-1/p) = -1$, $(D/q) = (-1/q) = 1$, and $(Q/q) = 1$. Thus, $p(2p + 3)$ is a Lucas pseudoprime of type 5 by Theorem 2.1 (v).

□

Corollary 2.4. *Let $U(P, Q)$ be a nondegenerate Lucas sequence. If Conjecture 1.2 is true, there exist infinitely many Lucas pseudoprimes of type 3 with parameters P and Q.*

Proof. Let $D = (-1)^\mu D_0^2 2^\gamma D_1$ and $Q = (-1)^\nu Q_0^2 2^\lambda Q_1$, where both D_1 and Q_1 are positive, odd, and square-free, and each of $\mu, \nu, \gamma,$ and λ is equal to 0 or 1. As in the proof of Theorem 2.3, let $H = lcm(2^\gamma D_1, 2^\lambda Q_1)$. Using Conjecture 1.2, choose odd primes p and q such that $p \equiv 1 \pmod{4H}$ and $q = 2p - 1 \equiv 1 \pmod{4H}$. By the proof of Theorem 2.3, one sees that

$$(D/p) = ((-1)^\mu/p) = 1, (D/q) = ((-1)^\mu/q) = 1, \text{ and } (Q/q) = ((-1)^\nu/q) = 1.$$

By Theorem 2.3 (iii), it follows that $p(2p-1)$ is a type 3 Lucas pseudoprime with parameters P and Q. □

Example 2.5. *Consider the nondegenerate Lucas sequence $U(5,9)$ with discriminant -11. We list all Lucas pseudoprimes with parameters 5 and 9 of types 1 - 5, which are less than* 10^6.
Type 1 Pseudoprimes: $29 \cdot 31$, $101 \cdot 103$, $197 \cdot 199$, $227 \cdot 229$, $431 \cdot 433$, $461 \cdot 463$, $659 \cdot 661$, $821 \cdot 823$, $827 \cdot 829$, $857 \cdot 859$.
Type 2 Pseudoprimes: $23 \cdot 43$, $67 \cdot 131$, $71 \cdot 139$, $137 \cdot 271$, $181 \cdot 359$, $331 \cdot 659$, $577 \cdot 1151$, $617 \cdot 1231$, $643 \cdot 1283$, $661 \cdot 1319$.
Type 3 Pseudoprimes: $157 \cdot 313$, $199 \cdot 397$, $331 \cdot 661$, $379 \cdot 757$, $577 \cdot 1153$, $619 \cdot 1237$, $661 \cdot 1321$.
Type 4 Pseudoprimes: $41 \cdot 83$, $83 \cdot 167$, $131 \cdot 263$, $173 \cdot 347$, $239 \cdot 479$, $281 \cdot 563$, $593 \cdot 1187$, $659 \cdot 1319$.
Type 5 Pseudoprimes: $17 \cdot 37$, $43 \cdot 89$, $127 \cdot 257$, $193 \cdot 389$, $197 \cdot 397$, $307 \cdot 617$, $439 \cdot 881$, $523 \cdot 1049$, $659 \cdot 1321$.

Theorem 2.6. *Let $U(P,Q)$ be a nondegenerate Lucas sequence for which $D = D_0^2 D_1$ and $Q = Q_0^2 Q_1$, where D_1 is a prime greater than or equal to 7, and either $Q_1 = 1$ or $Q_1 = -D_1$. If Conjecture 1.2 is true, then there exist many Lucas pseudoprimes with parameters P and Q of each of the types 1 - 5.*

Remark 2.7. *We demonstrate that there do indeed exist infinitely many Lucas sequences $U(P,Q)$ for which D_1 and Q_1 satisfy the hypotheses of Theorem 2.6. First suppose that $D_1 \geq 7$ is a prime and $Q_1 = 1$. Let $Q = Q_0^2$. It is well-known that the Pell equation*

$$x^2 - D_1 y^2 = 4$$

has infinitely many solutions in positive integers. For a given solution (x_i, y_i), let $P = Q_0 x_i$. Then

$$D = P^2 - 4Q = Q_0^2 x_i^2 - 4Q_0^2 = Q_0^2(x_i^2 - 4) = (Q_0 y_i)^2 D_1,$$

as desired.

Now suppose that $D_1 \geq 7$ is a prime and $Q_1 = -D_1$. Let P_1 be a positive integer such that $P_1^2 < 4D_1$ and $P_1 \equiv \epsilon \pmod 2$, where $\epsilon = 1$ if $D_1 \equiv 1 \pmod 4$ and $\epsilon = 2$ if $D_1 \equiv 3 \pmod 4$. Let $Q_2 = (P_1^2 - \epsilon^2 D_1)/4$. By the Binet formulas (1.3) and (1.4),

$$V_{2n}^2(P_1, Q_2) - 4Q_2^{2n} = (P_1^2 - 4Q_2)U_{2n}^2(P_1, Q_2) = \epsilon^2 D_1 U_{2n}^2(P_1, Q_2) \tag{2.8}$$

for $n \geq 1$. Let $Q = Q_2^{2n} Q_1 = -Q_2^{2n} D_1$ and $P = \epsilon D_1 U_{2n}(P_1, Q_2)$. Then by (2.8), we see that

$$D = P^2 - 4Q = \epsilon^2 D_1^2 U_{2n}^2(P_1, Q_2) + 4Q_2^{2n} D_1 = V_{2n}^2(P_1, Q_2) D_1,$$

as desired.

Example 2.8. *Consider the nondegenerate Lucas sequence $U(7,9)$ with discriminant 13. We list all Lucas pseudoprimes with parameters 7 and 9 of types 1 - 5, which are less than* 10^6.
Type 1 Pseudoprimes: $41 \cdot 43$, $59 \cdot 61$, $137 \cdot 139$, $197 \cdot 199$, $281 \cdot 283$, $431 \cdot 433$, $821 \cdot 823$, $827 \cdot 829$.
Type 2 Pseudoprimes: $17 \cdot 31$, $43 \cdot 83$, $113 \cdot 223$, $181 \cdot 359$, $191 \cdot 379$, $233 \cdot 463$, $251 \cdot 499$, $311 \cdot 619$, $347 \cdot 691$, $373 \cdot 743$, $433 \cdot 863$, $563 \cdot 1123$, $641 \cdot 1279$.
Type 3 Pseudoprimes: $79 \cdot 157$, $139 \cdot 277$, $157 \cdot 313$, $337 \cdot 673$, $547 \cdot 1093$, $607 \cdot 1213$.
Type 4 Pseudoprimes: $41 \cdot 83$, $233 \cdot 467$, $293 \cdot 587$, $431 \cdot 863$, $509 \cdot 1019$, $683 \cdot 1367$.
Type 5 Pseudoprimes: $7 \cdot 17$, $137 \cdot 277$, $337 \cdot 677$, $397 \cdot 797$, $467 \cdot 937$.

In order to prove Theorem 2.6, we will need the following two theorems. From here on, we let $\epsilon_i = \pm 1$ for $i \geq 1$.

Theorem 2.9. *Let p be an odd prime such that either $p \equiv 3 \pmod 4$ and $p \geq 11$ or $p \equiv 1 \pmod 4$ and $p \geq 29$. Let $\delta(n) = (n/p)$, where n is an integer. If $(\epsilon_1, \epsilon_2, \epsilon_3)$ is any 3-tuple of +1's and -1's, then there exists an integer n such that $1 \leq n \leq p-3$ and $(\delta(n), \delta(n+1), \delta(n+2)) = (\epsilon_1, \epsilon_2, \epsilon_3)$.*

Proof. This is proved in [4, pp. 156-158]. □

Theorem 2.10. *Let $p \geq 7$ be a prime. Let $\delta(n)$ be defined as in Theorem 2.9. For any given ordered pair (ϵ_1, ϵ_2), there exists an integer n such that $1 \leq n \leq p-1$ and $(\delta(n), \delta(n+3)) = (\epsilon_1, \epsilon_2)$.*

Proof. Let $a_0 = 0, a_{i+1} \equiv a_i + 3 \pmod p$, and $0 \leq a_i \leq p-1$ for $0 \leq i \leq p-1$. Since $\gcd(3,p) = 1$, we have $a_i \neq a_j$ for $0 \leq i < j \leq p-1$ Thus it suffices to find an integer n such that $(\delta(a_n), \delta(a_{n+1})) = (\epsilon_1, \epsilon_2)$. First suppose that $p \equiv 1 \pmod 4$ and $p \geq 13$. Since there exist $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues, it is clear that there exists an integer m such that $1 \leq m \leq p-1$ and $(\delta(a_m), \delta(a_{m+1})) = (\epsilon_3, \epsilon_4)$, where $\epsilon_3 \neq \epsilon_4$. Then $(\delta(a_{p-m-1}), \delta(a_{p-m})) = (\epsilon_4, \epsilon_3)$. Moreover, there exists an integer i such that $1 \leq i \leq p-1, a_i = 1, a_{i+1} = 4, a_{p-i-1} = p-4$, and $a_{p-i} = p-1$. Then

$$(\delta(a_i), \delta(a_{i+1})) = (\delta(a_{p-i-1}), \delta(a_{p-i})) = (1,1).$$

Since the four integers 1, 4, p - 4, and p - 1 are all different and the number of quadratic residues equals the number of quadratic nonresidues modulo p, it is easily seen that there must exist an integer j such that $1 \leq j \leq p-1$ and $(\delta(a_j), \delta(a_{j+1})) = (-1,-1)$. The result now follows in this case.

Now suppose that $p \equiv 3 \pmod 4$. If $p = 7$ or 11, it is seen by inspection that the theorem is true. Suppose that $p \geq 19$. Then there exists an integer m such that $a_m = 1$ and $a_{m+1} = 4$, which implies that $a_{p-m-1} = p-4$ and $a_{p-m} = p-1$. Then

$$(\delta(a_m), \delta(a_{m+1})) = (1,1) \text{ and } (\delta(a_{p-m-1}), \delta(a_{p-m})) = (-1,-1).$$

We now consider the case in which $p \geq 19, p \equiv 1 \pmod 3$ and $p \equiv 3 \pmod 4$. Then $a_{(2p+1)/3} = 1$, which implies that $a_{(p-1)/3} = p-1$, Noting that $a_3 = 9$, we see that the 3-tuple

$$(\delta(a_3), \delta(a_{(p-1)/3}), \delta(a_{(2p+1)/3})) = (1,-1,1).$$

Since $3 < (p-1)/3 < (2p+1)/3$, it follows that there exist integers i and j such that $3 \leq i < (p-1)/3, (p-1)/3 \leq j < (2p+1)/3$, and both

$$(\delta(a_i), \delta(a_{i+1})) = (1,-1) \text{ and } (\delta(a_j), \delta(a_{j+1})) = (-1,1).$$

Finally, we consider the case in which $p \geq 23, p \equiv 2 \pmod 3$, and $p \equiv 3 \pmod 4$. For $1 \leq n \leq p-1$, note that $a_n \equiv 1 \pmod 3$ if and only if $(p+1)/3 \leq n \leq (2p-1)/3$, and $a_n \equiv 2 \pmod 3$ if and only if $(2p+2)/3 \leq n \leq p-1$. Note also that $a_{(p+1)/3} = 1$ and $a_{(2p-1)/3} = p-1$. Then the ordered pair

$$(\delta(a_{(p+1)/3}), \delta(a_{(2p-1)/3})) = (1,-1).$$

It thus suffices to find an integer k such that $1 \leq k \leq p-1,\ k \equiv 2 \pmod 3$, and $\delta(k) = 1$. Then $a_i = k$ for some i such that $(2p+2)/3 \leq i \leq p-1$, and it would follow that there exist integers j and m such that $(p+1)/3 \leq j \leq (2p-1)/3, (2p+2)/3 \leq m \leq p-1, (\delta(a_j), \delta(a_{j+1})) = (1,-1)$, and $(\delta(a_m - 1), \delta(a_m)) = (-1,1)$ Let $p = \lfloor\sqrt{p}\rfloor^2 + \ell$, where

$1 \leq \ell \leq 2\lfloor\sqrt{p}\rfloor$. Then the next two squares greater than p are $p + 2\lfloor\sqrt{p}\rfloor + 1 - \ell$ and $p + 4\lfloor\sqrt{p}\rfloor + 4 - \ell$. Thus, there are two consecutive squares between p and $2p$ if

$$p > 4\lfloor\sqrt{p}\rfloor + 3. \tag{2.9}$$

It is easily seen that inequality (2.9) holds if $p \geq 23$. At least one of the two consecutive squares $p + 2\lfloor\sqrt{p}\rfloor + 1 - \ell$ and $p + 4\lfloor\sqrt{p}\rfloor + 4 - \ell$ is congruent to $1 \pmod 3$. Call this square N. Then $p \leq N \leq 2p$. Hence, $1 \leq N - p \leq p - 1, \delta(N - p) = \delta(N) = 1$, and

$$N - p \equiv 1 - 2 \equiv 2 \pmod 3,$$

as desired. □

Proof of Theorem 2.6: Let $\delta(n) = (n/D_1)$. Assume that Conjecture 1.2 is true. In parts (i) - (v) of this proof, we will generate in turn infinitely many Lucas pseudoprimes with parameters P and Q of each of the types 1 - 5.

(i) By Theorem 2.1 (i) and the properties of the Legendre symbol, $p(p + 2)$ is a Lucas pseudoprime of type 1 with parameters P and Q if p and $p + 2$ are odd primes such that

$$(D/p) = (D_1/p) = -1 \text{ and } (D/p + 2) = (D_1/p + 2) = 1. \tag{2.10}$$

By the law of quadratic reciprocity, if $p \equiv 1 \pmod 4$, then (2.10) holds if and only if

$$(p/D_1) = -1 \text{ and } (p + 2/D_1) = (-1)^{(D_1-1)/2}. \tag{2.11}$$

By inspection, one sees that if $D_1 = 7, 13$, or 17, then there exists an integer n_1 such that $1 \leq n_1 \leq D_1 - 1$ and both

$$\delta(n_1) = 1 \text{ and } \delta(n_1 + 2) = (-1)^{(D_1-1)/2}. \tag{2.12}$$

By Theorem 2.9, it now follows that (2.12) holds for some integer n_1 such that $1 \leq n_1 \leq D_1 - 1$ whenever $D_1 \geq 7$. By the prime k-tuples conjecture and the Chinese Remainder Theorem, there exist infinitely many primes p such that $p \equiv 1 \pmod 4$, $p \equiv n_1 \pmod{D_1}$, and $p + 2$ is a prime. It now follows that there exist many Lucas pseudoprimes of type 1 with parameters P and Q.

(ii) By Theorem 2.1 (ii), $p(2p - 3)$ is a Lucas pseudoprime of type 2 with parameters P and Q if p and $2p - 3$ are odd primes such that

$$(D/p) = (D_1/p) = 1, \tag{2.13}$$

$$(D/2p - 3) = (D_1/2p - 3) = -1, \tag{2.14}$$

and

$$(Q/2p - 3) = 1. \tag{2.15}$$

If $Q_1 = 1$, then (2.15) clearly holds. If $Q_1 = -D_1$, then (2.14) implies that (2.15) is satisfied, since $2p - 3 \equiv 3 \pmod 4$. Suppose further that $p \equiv 1 \pmod 4$. Then by the law of quadratic reciprocity, (2.13) and (2.14) both hold if and only if

$$(p/D_1) = 1 \text{ and } (2p - 3/D_1) = (-1)^{(D_1+1)/2}. \tag{2.16}$$

We now observe that $(p/D_1) = 1$ if and only if

$$(2p/D_1) = (2/D_1). \tag{2.17}$$

By Theorem 2.10, there exists an integer n_2 such that $1 \leq n_2 \leq D_1 - 1$ and both

$$\delta(n_2) = (-1)^{(D_1+1)/2} \text{ and } \delta(n_2 + 3) = (2/D_1). \tag{2.18}$$

By Conjecture 1.2 and the Chinese Remainder Theorem, there exist infinitely many primes p such that $p \equiv 1 \pmod 4$, $p \equiv (n_2+3)(D_1+1)/2 \pmod{D_1}$, and $2p-3$ is also a prime. Note that if $p \equiv (n_2+3)(D_1+1)/2 \pmod{D_1}$, then $2p-3 \equiv n_2 \pmod{D_1}$ and $2p \equiv (n_2+3) \pmod{D_1}$. It now follows that $p(2p-3)$ is a Lucas pseudoprime of type 2 with parameters P and Q for each p satisfying the above conditions.

(iii) By Corollary 2.4, there exist infinitely many Lucas pseudoprimes $p(2p-1)$ of type 3 with parameters P and Q.

(iv) By Theorem 2.1 (iv), $p(2p+1)$ is a Lucas pseudoprime of type 4 with parameters P and Q if p and $2p+1$ are odd primes such that

$$(D/p) = (D_1/p) = -1, \tag{2.19}$$

$$(D/2p+1) = (D_1/2p+1) = -1, \tag{2.20}$$

and

$$(Q/2p+1) = 1. \tag{2.21}$$

It is evident that (2.21) is satisfied if $Q_1 = 1$, while if $Q_1 = -D_1$, then (2.20) implies that (2.21) also holds, since $2p+1 \equiv 3 \pmod 4$. Suppose additionlly that $p \equiv 1 \pmod 4$. Then by the law of quadratic reciprocity, (2.19) and (2.20) are both satisfied if and only if

$$(p/D_1) = -1 \text{ and } (2p+1/D_1) = (-1)^{(D_1+1)/2}. \tag{2.22}$$

Notice that $(p/D_1) = -1$ if and only if

$$(2p/D_1) = -(2/D_1). \tag{2.23}$$

By inspection and Theorem 2.9, if $p \geq 7$, then there exists an integer n_3 such that $1 \leq n_3 \leq D_1 - 1$ and both

$$\delta(n_3) = -(2/D_1) \text{ and } \delta(n_3+1) = (-1)^{(D_1+1)/2}. \tag{2.24}$$

By Conjecture 1.2 and the Chinese Remainder Theorem, there exist infinitely many primes p such that $p \equiv 1 \pmod 4$, $p \equiv (n_3)(D_1+1)/2 \pmod{D_1}$, and $2p+1$ is also a prime. Observe that $2p \equiv n_3 \pmod{D_1}$ and $2p+1 \equiv (n_3+1) \pmod{D_1}$. We now see that $p(2p+1)$ is a Lucas pseudoprime of type 4 with parameters P and Q.

(v) The proof that there exist infinitely many Lucas pseudoprimes $p(2p+3)$ of type 5 with parameters P and Q is similar to the proof of part (ii), upon noting that if p and $2p+3$ are both odd primes, then $2p+3 \equiv 1 \pmod 4$. □

3. Degenerate Recurrences

For completeness, we now treat the case in which the Lucas sequence $U(P,Q)$ is a degenerate recurrence.

Proposition 3.1. *The Lucas sequence $U(P,Q)$ is degenerate if and only if exactly one of the following holds:*

(i) *$\alpha/\beta = -1, P = 0, Q = N$, and $D = -4N$ for some nonzero integer N. Then $U_k = 0$ if and only if $2|k$.*

(ii) *α/β is a primitive cube root of unity. Then $P = N$, $Q = N^2$, and $D = -3N^2$ for some nonzero integer N. Moreover, $U_k = 0$ if and only if $3|k$.*

(iii) *α/β is a primitive fourth root of unity. Then $P = 2N$, $Q = 2N^2$, and $D = -4N^2$ for some nonzero integer N. Furthermore, $U_k = 0$ if and only if $4|k$.*

(iv) *α/β is a primitive sixth root of unity. Then $P = 3N$, $Q = 3N^2$, and $D = -3N^2$ for some nonzero integer N. Moreover, $U_k = 0$ if and only if $6|k$.*

Proof. This is proved in [9, p. 613]. □

Theorem 3.2. *Let $U(P,Q)$ be a degenerate Lucas sequence. Then $m > 1$ is a Lucas pseudoprime with parameters P and Q if m is any odd composite integer such that $\gcd(m, D) = 1$.*

Proof. By Proposition 3.1, if α and β are the characteristic roots of $U(P,Q)$, then α/β is a primitive kth root of unity, where $k = 2, 3, 4$, or 6. Suppose that $k = 2$. Then by Proposition 3.1, $P = 0, Q = N$, and $D = -4N$ for some nonzero integer N. Clearly, $2|m - (D/m)$, and hence $U_{m-(D/m)} \equiv 0 \pmod{m}$. Thus, m is a Lucas pseudoprime with parameters P and Q in this case.

Now suppose that $k = 4$. Then $P = 2N, Q = 2N^2$, and $D = -4N^2$ for some nonzero integer N. Note that $m \equiv 1$ or $3 \pmod{4}$. By the properties of the Jacobi symbol and law of quadratic reciprocity for the Jacobi symbol,

$$(D/m) = (-4N^2/m) = (-1/m) = (-1)^{(m-1)/2}.$$

Hence, $m - (D/m) \equiv 0 \pmod{4}$. Thus, $U_{m-(D/m)} \equiv 0 \pmod{m}$, and m is a Lucas pseudoprime.

Finally, suppose that $k = 3$ or 6. Then $D = -3N^2$ for some nonzero integer N. Observe that $m \equiv 1$ or $5 \pmod{6}$. Then

$$(D/m) = (-3/m)(N^2/m) = (-3/m).$$

Using the properties of the Jacobi symbol and law of quadratic reciprocity for the Jacobi symbol, it now follows that $(-3/m) = 1$ if $m \equiv 1 \pmod{6}$ for both the cases in which $m \equiv \pm 1 \pmod{4}$, and $(-3/m) = -1$ if $m \equiv 5 \pmod{6}$ for both the cases in which $m \equiv \pm 1 \pmod{4}$. Therefore, $m - (D/m) \equiv 0 \pmod{6}$. Consequently, $U_{m-(D/m)} \equiv 0 \pmod{m}$, and m is a Lucas pseudoprime. □

References

[1] R. D. Carmichael, *On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$*, Ann. of Math., Second Series, **15** (1913), 30–70.

[2] L. E. Dickson, *A New Extension of Dirichlet's Theorem on Prime Numbers*, Messenger Math., **33** (1904), 155–161.

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Oxford University Press, Oxford, 1960.

[4] H. Hasse, *Vorlesungen über Zahlentheorie*, Springer-Verlag, Berlin, 1950.

[5] D. H. Lehmer, *An Extended Theory of Lucas' Functions*, Ann. of Math., Second Series, **31** (1930), 419–448.

[6] E. Lucas, *Théorie des Fonctions Numériques Simplement Périodiques*, Amer. J. Math., **1** (1878), 184–240, 289–321.

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

[8] L. Somer and F. Luca, *Solution to Problem H-622*, The Fibonacci Quarterly, **44.1** (2006), 93–94.

[9] M. Ward, *Prime Divisors of Second Order Recurring Sequences*, Duke Math. J., **21** (1954), 607–614.

MSC2000: 11B39, 11A51

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