LUCAS SEQUENCES $\{U_k\}$ FOR WHICH U_{2p} AND U_p ARE PSEUDOPRIMES FOR ALMOST ALL PRIMES p

Lawrence Somer

Department of Mathematics, Catholic University of America, Washington, DC 20064

(Submitted May 2003 - Final Revision December 2003)

ABSTRACT

It was proven by Emma Lehmer that for almost all odd primes p, F_{2p} is a Fibonacci pseudoprime. In this paper, we generalize this result to Lucas sequences $\{U_k\}$. In particular, we find Lucas sequences $\{U_k\}$ for which either U_{2p} is a Lucas pseudoprime for almost all odd primes p or U_p is a Lucas pseudoprime for almost all odd primes p.

1. INTRODUCTION

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

$$F_{n-(D/n)} \equiv 0 \pmod{p} \tag{1}$$

(see [7, p.150]), where $D = 5$ is the discriminant of $\{F_k\}$ and (D/n) denotes the Jacobi symbol. In rare instances, there exist odd composite integers n such that n also satisfies congruence (1). These integers are called Fibonacci pseudoprimes. The smallest Fibonacci pseudoprime is $323 = 17 \cdot 19$. It was proved independently by Duparc [3] and E. Lehmer [9] that F_{2p} is a Fibonacci pseudoprime for all primes $p > 5$. It was further shown by Parberry [10] that F_p is a Fibonacci pseudoprime whenever p is an odd prime and F_p is composite. Unfortunately, it is not known whether there are infinitely many primes for which F_p is composite. In this note we will generalize the results above by finding infinite classes of Lucas sequences $\{U_k\}$ for which U_{2p} or U_p are Lucas pseudoprimes for all but finitely many primes p. Before proceeding further, we will need the following results and definitions.

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

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

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

$$f(x) = x^2 - Px + Q \tag{3}$$

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

$$U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta},\ V_k = \alpha^k + \beta^k. \tag{4}$$

Let $U(P,Q)$ and $V(P,Q)$ be Lucas sequences. If n is an odd prime such that $(n, QD) = 1$, then the following four congruences all hold (see [1, pp. 1391-1392]):

$$U_{n-(D/n)} \equiv 0 \pmod{n}. \tag{5}$$

$$U_n \equiv (D/n) \pmod{n}. \tag{6}$$

$$V_n \equiv P \pmod{n}. \tag{7}$$

$$V_{n-(D/n)} \equiv 2Q^{(1-(D/n))/2} \pmod{n}. \tag{8}$$

Occasionally, positive odd composite integers satisfy at least one of the congruences (5) - (8). This leads to the following definitions:

Definition 1: A positive odd composite integer n for which (5) holds is called a *Lucas pseudoprime* with parameters P and Q.

Definition 2: A positive odd composite integer n for which (6) holds is called a *Lucas pseudoprime of the second kind* with parameters P and Q.

Definition 3: A positive odd composite integer n for which (7) holds is called a *Dickson pseudoprime* with parameters P and Q.

Definition 4: A positive odd composite integer n for which (8) holds is called a *Dickson pseudoprime of the second kind* with parameters P and Q.

In Definitions 1 - 4, we will suppress the parameters P and Q if it is clear which Lucas sequences are associated with the respective pseudoprimes. By [1, pp. 1391-1392], if n is a positive integer such that $(n, 2PQD) = 1$, then any two of congruences (5) - (8) imply the other two.

Analogously to the definition of Frobenius pseudoprime presented in [6] and [2, pp 133-134], we make the following definition:

Definition 5: A positive odd composite integer n is called a *Frobenius pseudoprime* with parameters P and Q if $(n, PQD) = 1$ and n satisfies all four of the congruences (5) - (8).

Before presenting our main results, we will need to define additional types of pseudoprimes.

Definition 6: A positive odd composite integer n is called a *Fermat pseudoprime* to the base a if $(a, n) = 1$ and

$$a^{n-1} \equiv 1 \pmod{n}. \tag{9}$$

Definition 7: A positive odd composite integer n is called an *Euler pseudoprime* to the base a if $(a, n) = 1$ and

$$a^{(n-1)/2} \equiv (a/n) \quad \pmod{n}. \tag{10}$$

Remark 1: It is clear that an Euler pseudoprime to the base a is a Fermat pseudoprime to the base a. We further note that every positive odd composite integer is an Euler pseudoprime to both the bases 1 and -1.

Definition 8: Let $U(P,Q)$ and $V(P,Q)$ be Lucas sequences. A positive odd composite integer n is called an *Euler-Lucas pseudoprime* with parameters P and Q if

$$U_{(n-(D/n))/2} \equiv 0 \pmod{n} \text{ if } (Q/n) = 1 \tag{11}$$

or

$$V_{(n-(D/n))/2} \equiv 0 \pmod{n} \text{ if } (Q/n) = -1. \tag{12}$$

Definition 9: Let $U(P,Q)$ and $V(P,Q)$ be Lucas sequences. A positive odd composite integer n such that $(n,\ QD)=1$ is called a *strong Lucas pseudoprime* with parameters P and Q if $n-(D/n)=2^s r,\ r$ odd, and

$$\begin{aligned}&\text{either } U_r \equiv 0 \pmod{n} \text{ or}\\ &V_{2^t r} \equiv 0 \pmod{n} \text{ for some } t,\ 0 \le t < s.\end{aligned} \tag{13}$$

Remark 2: It is evident that both Euler-Lucas pseudoprimes and strong Lucas pseudoprimes with parameters P and Q are Lucas pseudoprimes with parameters P and Q. It was proved in [1, p. 1397] that every strong Lucas pseudoprime with parameters P and Q is an Euler-Lucas pseudoprime with parameters P and Q. It was further proved in [1, p. 1397] that if n is an Euler-Lucas pseudoprime with parameters P and Q such that either $(Q/n)=-1$ **or** $n-(D/n)\equiv\ 2 \pmod 4$, then n is a strong Lucas pseudoprime with parameters P and Q. We further note that all of the congruences (9) - (13) are satisfied for odd primes n (see [1, p. 1396]).

In Theorems 1 and 2 below, we find Lucas sequences $U(P,Q)$ for which U_{2p} and U_p are Lucas pseudoprimes for all but finitely many primes p. In Theorem 3, we further find Lucas sequences $U(P,Q)$ for which U_p is both a strong Lucas pseudoprime and a Frobenius pseudoprime for all but finitely many primes p. In the hypotheses of these theorems we want to ensure that $U_k>0$ for $k\ge 1$. It was shown in the proof of Lemma 3 of [8] that if $P=U_2=V_1>0$ and $D>0$, then $\{U_k\}$ and $\{V_k\}$ are strictly increasing for $k\ge 2$ and $U_k>0$ and $V_k>0$ for $k\ge 1$. If $P<0$, then $U_2<0$ and $V_1<0$, while if $D<0$, then U_k and V_k can be less than 0 – for example, if $P=1,\ Q=2,$ and $D=-7$, then $U_3=-1$ and $V_2=-3$. We further note that if $P=0$, then $U_{2k}=0$ for all $k\ge 1$, and all composite odd integers are Lucas pseudoprimes in this case. From this point on, we exclude the trivial case in which $P=0$. Accordingly, we will assume from here on that $P>0$ and $D>0$.

Theorem 1: *Let $U(1,Q)$ be a Lucas sequence such that $Q\le -1$. Let n be an odd prime or a Frobenius pseudoprime such that $(n,QD)=1$. Further, suppose that $3\not| n$ if Q is odd. Then U_{2n} is a Lucas pseudoprime.*

Proof: We first note that $D=1^2-4Q>0$. Let $m=U_{2n}=U_nV_n$. Then m is composite since $U_n>1$ and $V_n>1$. Moreover, if Q is odd, then U_k is even if and only if $3\mid k$, while U_k is odd for $k\ge 1$ if Q is even. Thus, it follows from the hypotheses that both U_n and U_{2n} are odd.

By (6),

$$U_n \equiv (D/n) \pmod{n}.$$

By (7),

$$V_n \equiv P \equiv 1 \pmod{n}.$$

Thus,

$$U_{2n} \equiv (D/n) \pmod{n}.$$

Then

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

and

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

Consequently,

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

Therefore,

$$m = U_{2n} \mid U_{m-(D/n)}. \tag{14}$$

To complete the proof, we need to show that $(D/n) = (D/m)$. Note that $D = 1^2 - 4Q \equiv 1 \pmod 4$. By expanding the first expression in (4) by use of the binomial theorem (see also [13, pp. 467-468]), we obtain

$$U_{2n} \equiv 2n(1/2)^{2n-1} \equiv n(2^{-1})^{2(n-1)} \pmod D. \tag{15}$$

It now follows from (15) and the properties of the Jacobi symbol that

$$(D/m) = (D/U_{2n}) = (U_{2n}/D) = (n/D)((2^{-1})^{2(n-1)}/D) = (n/D) = (D/n).$$

The result now follows. □

Remark 3: Parberry [10] proved that for the Fibonacci sequence $U(1,-1)$, if $n > 5$ is either a prime or a Frobenius pseudoprime, then U_{2n} is both an Euler-Lucas pseudoprime and a Frobenius pseudoprime if and only if $n \equiv 1$ or $19 \pmod{30}$. Thus, by virtue of Dirichlet's theorem on the infinitude of primes in arithmetic progressions, there are infinitely many terms U_{2n} which are both Euler-Lucas pseudoprimes and Frobenius pseudoprimes for the Fibonacci sequence. On page 134 of [2] and page 22 of [5] and page 885 of [6] it is written that the first Frobenius-Fibonacci pseudoprime is $5777 = 53 \cdot 109$. It is not true, because the first Frobenius-Fibonacci pseudoprime is $n = 4181 = 37 \cdot 113$ (see A. Rotkiewicz's paper [15]).

Theorem 2: *Let $U(P,Q)$ be a Lucas sequence for which $P > 0$, $Q \neq 0$, P or Q is odd, and $D > 0$. Let $D = D_0^2 D_1$, where D_1 is square free, and suppose that either P is odd or P is even and $D_1 \equiv 1 \pmod 4$. Suppose further that $d = (P,Q) = 1$ and Q is a perfect square. Let n be an odd prime or a Lucas pseudoprime of the second kind such that $(n,QD) = 1$, $n \neq 3$, and $3 \nmid n$ if $P \equiv Q \equiv 1 \pmod 2$. Then U_n is a strong Lucas pseudoprime.*

Proof: We first claim that U_n is odd. Note that n is odd. If P is even and Q is odd, then U_k is odd if and only if k is odd. If P is odd and Q is even, then U_k is odd for all $k \geq 1$. If P and Q are both odd, then U_k is even if and only if $3 \mid k$. Therefore, U_n is odd by hypothesis.

We now show that U_n is composite. Note that $d = 1$ and Q is a square. It was shown by Rotkiewicz [11] that if $k > 3$ is odd then U_k has two primitive prime divisors, where the prime p is a primitive prime divisor of U_k if $p | U_k$ but $p \nmid U_l$ for $1 \leq l < k$. (Due to a slightly different definition of primitive prime divisor, Rotkiewicz excluded the case $U_5(3,1)$, but $U_5(3,1) = 55 = 5 \cdot 11$ has two primitive prime divisors according to our definition.) Thus U_n is composite.

Let $m = U_n$, $m - (D/m) = 2^s r$, and $m - (D/n) = 2^h g$, where r and g are odd. To show that m is a strong Lucas pseudoprime, it suffices to demonstrate that $U_r \equiv 0 \pmod m$. We note that if P is odd, then $D \equiv 1 \pmod 4$, and hence $D_1 \equiv 1 \pmod 4$. Then by (6),

$$n \mid U_n - (D/n).$$

Since n is odd,

$$n \mid (U_n - (D/n))/2^h.$$

Thus,

$$m = U_n \mid U_{(m-(D/n))/2^h}.$$

To prove that $U_r \equiv 0 \pmod{m}$, it remains to show that $(D/n) = (D/m)$, since this would also imply that $s = h$. By Lemma 1 of [13],

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

Noting that both n and U_n are odd and using the properties of the Jacobi symbol, we see that

$$\begin{aligned}(D/m) &= (D/U_n) = (D_0^2/U_n)(D_1/U_n)\\ &= (D_1/U_n) = (U_n/D_1)\\ &= (n/D_1)((P/2)^{n-1}/D_1) = (n/D_1)\\ &= (D_1/n) = (D_0^2 D_1/n) = (D/n).\end{aligned}$$

The result now follows. □

If we restrict the hypotheses of Theorem 2, we obtain the following stronger result.

Theorem 3: *Let $U(P,1)$ be a Lucas sequence for which $P \geq 3$. Let $D = D_0^2 D_1$, where D_1 is square free and suppose that either P is odd or P is even and $D_1 \equiv 1 \pmod 4$. Let $n > 3$ be a prime or a Lucas pseudoprime of the second kind such that $(n, PD) = 1$ and $3 \not| n$ if P is odd. Then U_n is both a strong Lucas pseudoprime and a Frobenius pseudoprime.*

Proof: Note that $D > 0$, since $P \geq 3$. It now follows from Theorem 2 that U_n is a strong Lucas pseudoprime, and hence an Euler-Lucas pseudoprime. It was shown in Theorem 1 of [14] that if m is an Euler-Lucas pseudoprime with parameters P and Q and m is an Euler pseudoprime to the base Q, then m is a Frobenius pseudoprime with parameters P and Q. Since $Q = 1$, U_n is clearly an Euler pseudoprime to the base Q. Thus, U_n is also a Frobenius pseudoprime with parameters P and 1. □

For the Fibonacci sequence we know that there are infinitely many Frobenius pseudoprimes n with $\left(\frac{5}{n}\right) = 1$ (see Parberry [10] and Rotkiewicz [15]).

C. Pomerance put forward (in a letter to A. Rotkiewicz) the following problem: Given integers P, Q with $D = P^2 - 4Q$ not a square, do there exist infinitely many, or at least one, Lucas Pseudoprimes n with parameters P and Q satisfying $\left(\frac{D}{n}\right) = -1$? (see also [4] p. 316).

An affirmative answer to this question in the strong sense (infinitely many) is contained in the following theorem of A. Rotkiewicz and A. Schinzel [16].

Given integer P, Q with $D = P^2 - 4Q \neq 0, -Q, -2Q, -3Q$, and $\epsilon = \pm 1$, every arithmetic progression $ax + b$, where $(a, b) = 1$, which contains an odd integer n_0 with $\left(\frac{D}{n_0}\right) = \epsilon$ contains infinitely many strong Lucas pseudoprimes n with parameters P and Q such that $\left(\frac{D}{n}\right) = \epsilon$. The number $N(X)$ of such strong pseudoprimes not exceeding X satisfies

$$N(X) > c(P, Q, a, b, \epsilon)\frac{\log X}{\log\log X}$$

where $c(P, Q, a, b, \epsilon)$ is a positive constant depending on P, Q, a, b, ϵ.

ACKNOWLEDGMENT

I would like to thank the referee for careful reading of the paper and suggestions which improved the presentation of the paper.

REFERENCES

[1] R. Baillie & S. Wagstaff, Jr. "Lucas Pseudoprimes." *Math. Comp.* **35** (1980): 1391-1417.
[2] R. E. Crandall & C. Pomerance. *Prime Numbers.* New York: Springer, 2001.
[3] H. J. A. Duparc. "On Almost Primes of the Second Order." *Math. Centrum Amsterdam*, Rap. **ZW** 1955-013 (1955): 1-13.
[4] P. Erdös, P. Kiss and A. Sárközy. "Lower Bound for the Counting Function of Lucas Pseudoprimes." *Math. Comp.* **51** (1988): 315-323.
[5] J. F. Grantham. "Frobenius Pseudoprimes." A dissertation submitted to the Graduate Faculty of the University of Georgia, Athens, GA, 1997.
[6] J. Grantham. "Frobenius Pseudoprimes." *Math. Comp.* **70** (2001): 873-891.
[7] G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers.* 5th ed. Oxford: Clarenddon Press, 1979.
[8] P. Hilton, J. Pedersen, & L. Somer. "On Lucasian Numbers." *The Fibonacci Quarterly* **35.1** (1997): 43-47.
[9] E. Lehmer. "On the Infinitude of Fibonacci Pseudoprimes." *The Fibonacci Quarterly* **2.3** (1964): 229-230.
[10] E. A. Parberry. "On Primes and Pseudoprimes Related to the Fibonacci Sequence." *The Fibonacci Quarterly* **8.1** (1970): 49-69.
[11] A. Rotkiewicz. "On Lucas Numbers with Two Intrinsic Prime Divisors." *Bull. Acad. Polon. Sci. Sér. Math. Astronom. Phys.* **10** (1962): 229-232.
[12] A. Rotkiewicz. "On the Pseudoprimes with Respect to the Lucas Sequences." *Bull. Acad. Polon. Sci. Sér. Math. Astronom. Phys.* **21** (1973): 793-797.
[13] A. Rotkiewicz. "Arithmetical Progressions Formed by Lucas Pseudoprimes." *Number Theory.* Diophantine, Computational and Algebraic Aspects, 465-472. Ed. K. Györy, A. Pethö, and V. T. Sos. Berlin: Walter de Gruyter, 1998.
[14] A. Rotkiewicz. "Lucas Pseudoprimes." *Funct. Approximatio Comment. Math.* **28** (2000): 97-104.
[15] A. Rotkiewicz. "Lucas and Frobenius Pseudoprimes." *Annales Mathematicae Silesiane* **17** (2003): 17-39.
[16] A. Rotkiewicz and A. Schinzel. "On Lucas Pseudoprimes with a Prescribed Value of the Jacobi Symbol." *Bull. Polish Acad. Sci. Math.* **48.1** (2000): 77-80.

AMS Classification Numbers: 11B39, 11A51

✠ ✠ ✠