SOME INTERESTING SUBSEQUENCES OF THE FIBONACCI AND LUCAS PSEUDOPRIMES

Paul S. Bruckman
13 Webster Ave., Highwood, IL 60040

(*Submitted December 1994*)

1. INTRODUCTION

In this paper, certain interesting sequences of positive integers are investigated. As will be demonstrated, these are subsequences of the Fibonacci and Lucas pseudoprimes, as they have been defined in the author's previous papers ([2], [3], [4], [9]). Indeed, it will be shown that the elements of two of these subsequences are strong Lucas pseudoprimes and Euler-Lucas pseudoprimes.

The secondary aim of this paper is to partially unify some of the more significant results previously obtained by other authors regarding such pseudoprimes.

Throughout this paper, lower-case letters represent integers, usually positive (unless otherwise indicated); the letters p, q, q_1, and r represent primes.

In Section 2, the definitions and properties required to prove our main results are given. These are readily accessible in the standard literature and are presented with minimal commentary.

A brief historical summary of some of the more relevant findings of previous researchers is presented in Section 3.

Section 4 sets forth the main results, including proofs, and Section 5 consists of concluding remarks.

2. DEFINITIONS AND PROPERTIES

The *Jacobi symbol* is defined in any elementary number theory text, where it is customarily expressed as a product of *Legendre symbols* in its definition. As a consequence of such definition, the Jacobi symbol assumes certain values (either +1 or −1) dependent on the residue class of its arguments. We take a slightly different approach and simply *define* the Jacobi symbol in terms of this residue class. The arguments are restricted to the values that are relevant to the topic of this paper.

Definition 2.1 The *Jacobi symbol* $(\frac{u}{n})$ is defined as follows for $u = -1, -3$, or 5, and for the indicated values of n:

(a) $$\left(\frac{-1}{n}\right) = (-1)^{\frac{1}{2}(n-1)} = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4}, \\ -1 & \text{if } n \equiv -1 \pmod{4}; \end{cases}$$

(b) $$\left(\frac{-3}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{6}, \\ -1 & \text{if } n \equiv -1 \pmod{6}; \end{cases}$$

(c) $$\left(\frac{5}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{10}, \\ -1 & \text{if } n \equiv \pm 3 \pmod{10}. \end{cases}$$

For brevity, we also write ε_n for $\left(\frac{5}{n}\right)$. Note that if $n = p$, an odd prime, the Jacobi symbol coincides with the Legendre symbol. The symbol $\left(\frac{u}{n}\right)$ is undefined for values of n not indicated above.

Definition 2.2: Given any integer u, the *Fibonacci entry-point of u*, denoted by $Z(u)$, is the smallest positive integer z such that $u \mid F_z$. If $Z(p) = m$, we say that p is a *primitive prime divisor* (p.p.d.) of F_m.

Note: A classical result of Carmichael states that F_u has a p.p.d. for all $u \neq 1, 2, 6$, or 12.

Definition 2.3:

(a) Given any integer u, the *Fibonacci period (mod u)*, denoted by $k(u)$, is the smallest positive integer k such that $F_{n+k} \equiv F_n \pmod{u}$ for all integers n.

(b) The *Lucas period (mod u)*, denoted by $\bar{k}(u)$, is the smallest positive integer $\bar{k}$ such that $L_{n+\bar{k}} \equiv L_n \pmod{u}$ for all integers n.

Definition 2.4: The *strong Lucas pseudoprimes* (denoted SLPP's) are those composite u with $\gcd(u, 10) = 1$, $u - \varepsilon_u = d \cdot 2^s$, $s \geq 1$, d being odd, such that either:

(a) $u \mid F_d$, or

(b) $u \mid L_{d \cdot 2^t}$ for some t with $0 \leq t < s$.

Let U denote the set of SLPP's.

Definition 2.5: The *Euler-Lucas pseudoprimes* (denoted ELPP's) are those composite u with $\gcd(u, 10) = 1$ such that either

(a) $u \mid F_{\frac{1}{2}(u-\varepsilon_u)}$ when $\left(\frac{-1}{u}\right) = 1$, or

(b) $u \mid L_{\frac{1}{2}(u-\varepsilon_u)}$ when $\left(\frac{-1}{u}\right) = -1$.

Let V denote the set of ELPP's.

Definition 2.6: The *Fibonacci pseudoprimes* (denoted FPP's) are those composite u with $\gcd(u, 10) = 1$ such that $u \mid F_{u-\varepsilon_u}$. Let X denote the set of FPP's.

Definition 2.7: The *Lucas pseudoprimes* (denoted LPP's) are those composite u such that $L_u \equiv 1 \pmod{u}$. Let Y denote the set of LPP's.

Definition 2.8: The *Fibonacci-Lucas pseudoprimes* (denoted FLPP's) are those u that are both FPP's and LPP's. Let $W = X \cap Y$ denote the set of FLPP's.

Comment: As we will later indicate, the sets V and W are identical. For the time being, however, we will maintain the distinction between these two sets.

In addition to the pseudoprimes defined above, there are other related pseudoprimes that have been studied by previous authors. Since these are only of peripheral interest to the topic of this paper, we merely mention these in passing. For example, Rotkiewicz [16], [17] and Baillie &

Wagstaff [1] discuss sequences of psuedoprimes u that (for the Fibonacci and Lucas sequences in particular) satisfy either of the following relations, given that $\gcd(u, 10) = 1$:

$$F_u \equiv \varepsilon_u \pmod{u}; \tag{2.1}$$

$$L_{u-\varepsilon_u} \equiv 2\varepsilon_u \pmod{u}. \tag{2.2}$$

It may be shown that if u satisfies any *two* of the relations given in Definitions 2.6, 2.7, or in (2.1) and (2.2), the other two relations are implied.

We next introduce the special sequences that are of interest to the topic of this paper.

Definition 2.9: Define the following ratios for any arbitrary prime p (except as indicated), and for $e = 0, 1, 2, \ldots$:

(a) $A_e(p) = F_{p^{e+1}} / F_{p^e}$, $p \neq 5$; $A_e(5) = F_{5^{e+1}} / 5F_{5^e}$;

(b) $B_e(p) = L_{p^{e+1}} / L_{p^e}$, $p \neq 2$;

(c) $C_e(p) = F_{2\cdot p^{e+1}} / F_{2\cdot p^e}$, $p \neq 2, 5$; $C_e(5) = F_{2\cdot 5^{e+1}} / 5F_{2\cdot 5^e}$.

Note that $C_e(p) = A_e(p) \cdot B_e(p)$ for all odd p. Where no confusion is likely to arise, we omit the argument p and/or the subscript e. Clearly, A, B, and C are positive integers in all cases.

Next, we indicate some relevant properties.

Properties 2.1:

(a) $Z(u) \mid v$ iff $u \mid F_v$;

(b) $Z(p) \mid (p - \varepsilon_p)$;

(c) $Z(u) = \underset{p^e \| u}{\mathrm{LCM}}\{Z(p^e)\}$;

(d) $Z(p^e) = p^f Z(p)$ for some f with $0 \leq f < e$;

(e) for all odd p, $Z(p)$ is even iff $p \mid L_u$ for some u.

Properties 2.2:

(a) $k(u) = \begin{cases} \bar{k}(u) & \text{if } 5 \nmid u, \\ 5\bar{k}(u) & \text{if } 5 \mid u; \end{cases}$

(b) $\bar{k}(u) = \underset{p^e \| u}{\mathrm{LCM}}\{\bar{k}(p^e)\}$;

(c) $\bar{k}(p^e) = p^f \bar{k}(p)$ for some f with $0 \leq f < e$ (for odd primes p, f is the same as in Property 2.1(d);

(d) if $p \neq 2, 5$, $\bar{k}(p) = \begin{cases} Z(p) & \text{if } Z(p) \equiv 2 \pmod{4}, \\ 2Z(p) & \text{if } 4 \mid Z(p), \\ 4Z(p) & \text{if } Z(p) \text{ is odd.} \end{cases}$

Note: Properties 2.2(b)-(d) for the Lucas period also apply to the Fibonacci period $k(u)$; however, scant use of this fact will be made here.

Properties 2.3: We assume $p \neq 2, 5$ and write $p' = \frac{1}{2}(p-1)$, $m = p^e$, $\varepsilon = \varepsilon_p$. In (e) and (f) below, we assume $\gcd(n, 10) = 1$ and write $t = \frac{1}{2}(n - \varepsilon_n)$.

(a) $A = (-1)^{p'}\left(1 + \sum_{j=1}^{p'} (-1)^j L_{2mj}\right);$

(b) $B = 1 + \sum_{j=1}^{p'} L_{2mj};$

(c) $C = 1 + \sum_{j=1}^{p'} L_{4mj};$

(d) $L_{2mp+\varepsilon} = -\varepsilon + 5F_{mp+\varepsilon}F_{mp} = \varepsilon + L_{mp+\varepsilon}L_{mp};$

(e) $L_t^2 - 5L_tF_{t+\varepsilon_n} + 5F_{t+\varepsilon_n}^2 = (-1)^t + \varepsilon_n;$

(f) $L_{t+\varepsilon_n}^2 - 5L_{t+\varepsilon_n}F_t + 5F_t^2 = (-1)^t.$

The derivations of Properties 2.3 involve elementary identities and are omitted. We will return to these definitions and properties in Section 4. First, however, we give a brief overview of some of the more significant results.

3. HISTORICAL SUMMARY

The use of the term "pseudoprime" in the preceding section stems from the fact that the defining relations are satisfied when $u = p$ (with $p \neq 2, 5$ in all but Definition 2.7). The author's papers [2], [3], [4] may be referred to for comments regarding the merit of adopting the nomenclature employed in Definitions 2.6-2.8, since other nomenclature is used by other authors. Some of the prior findings of other authors have been mentioned in the author's papers (op.cit.); for the sake of continuity, we reiterate these findings below.

In a 1955 paper by Duparc [12], apparently the first proof that *X*, *Y*, and *W* are infinite sets is given. In particular, Duparc showed that $F_{2p} \in X$ for all $p > 5$. This result was independently rediscovered by E. Lehmer in a 1964 paper [14]. Using a different method, Parberry [15] showed that X is infinite; specifically, Parberry showed that if $\gcd(n, 30) = 1$ and $n \in X$, then $F_n \in X$ [from which it follows necessarily that $\gcd(F_n, 30) = 1$]. In a 1986 paper [13], Kiss, Phong, and Lieuwens showed that *W* is infinite; of course, this implies that *X* and *Y* are infinite. In a recent paper [2], the author proved that the "LPP" counterpart of Parberry's result holds, namely that if $n \in Y$ and $\gcd(n, 6) = 1$, then $L_n \in Y$ [from which it follows necessarily that $\gcd(L_n, 6) = 1$]. This is an independent proof that *Y* is infinite.

It is also known that all LPP's are odd. Apparently the first proof of this result was given by White, Hunt, and Dresel in 1977 paper [18]. Other independent proofs of this result were subsequently given by Di Porto [10] and by the author [3].

Many other interesting properties (or apparent properties) may be given, but we will restrict our discussion to those properties that are more or less relevant to the topic of this paper and, in particular, to the ratios introduced in Definition 2.9.

Di Porto and Filipponi observed, and later proved in a 1988 paper [11], that if L_{2^e} is composite, it is a LPP. In a recently submitted problem for this journal [6], the author proves a generalization of such a result; this is indicated below in (3.1).

Other observations made recently by the author have been submitted to this journal as proposed problems (viz. [7]. [8]) and are indicated below:

$$\text{If } A_e(2) \text{ is composite, then } A_e(2) \in W; \tag{3.1}$$

$$\text{If } e \geq 1 \text{ and } A_e(3)\,[B_e(3)] \text{ is composite, then } A_e(3)\,[(B_e(3)] \in W; \tag{3.2}$$

$$C_e(3) \in (X - Y); \tag{3.3}$$

$$\text{If } A_e(5)\,[B_e(5)] \text{ is composite, then } A_e(5)\,[B_e(5)] \in W; \tag{3.4}$$

$$C_e(5) \in (X - Y). \tag{3.5}$$

In fact, even stronger results are true, although we will not prove these here; namely, $A_e(p) \in U$, if $p = 2, 3, 5$, and $B_e(p) \in U$, if $p = 3, 5$.

The results indicated in (3.1)-(3.5) were obtained initially, suggesting the generalizations that are indicated in Section 4 (for $p > 5$).

Note that there is no definition of $B_e(2)$ in Definition 2.9(b), since $L_{2^e} \nmid L_{2^{e+1}}$. Also, there is no definition of $C_e(2)$, since this would be essentially the same as for $A_e(2)$ (by virtue of the identity $F_{2n} = F_n L_n$).

The result of (3.2) excludes the case $e = 0$, since $L_3 = 4$ is composite but is neither a FPP nor a LPP. Also, note the extra factor of 5 in the denominator of the definitions of $A_e(5)$ and $C_e(5)$; this is a consequence of the special role played by the number 5 in the Fibonacci and Lucas sequences.

Therefore, for one reason or another, the primes 2, 3, and 5 require special treatment. This is not the case for $p > 5$; in the remainder of this paper we will assume $p > 5$.

It is worthwhile to reiterate the notation introduced in the prologue to Properties 2.3, since we will use this frequently:

$$\varepsilon = \varepsilon_p, \quad m = p^e, \quad e = 0, 1, \ldots. \tag{3.6}$$

We will also write mp for p^{e+1}, for brevity. Note also that $\gcd(A, B) = 1$, $AB = C$, and that A, B, and C are all relatively prime to 30.

4. MAIN RESULTS

We will make frequent use of the definitions and properties introduced in Section 2, often without specific reference thereto. Our main results are Theorems 4.1 and 4.2 (with their corollaries).

Theorem 4.1:

(a) If A is composite, then $A \in U$;

(b) If B is composite, then $B \in U$.

Corollary 4.1:

(a) If A is composite, then $A \in W$;

(b) If B is composite, then $B \in W$.

Corollary 4.2:

(a) If F_p is composite, then $F_p \in W$;

(b) If L_p is composite, then $L_p \in W$.

Our proof of the theorems requires several preliminary results, indicated in this section as lemmas.

Lemma 4.1: $Z(A) = mp$; $Z(B) = Z(C) = 2mp$.

Proof: From Definition 2.9 and from Carmichael's result (see Note after Definition 2.2), it follows that $Z(q) = mp$ for some q with $q \mid F_{mp}$. Also, $q \nmid F_m$, since $Z(q) \nmid m$. Then $q \mid A$. Indeed, $Z(r) = mp$ for **all** prime r with $r \mid F_{mp}, r \nmid F_m$. Then $Z(A) = mp$.

Using Property 2.1(e), we argue similarly that $Z(B) = 2mp$. Then, since $C = AB$, $Z(C) =$ LCM$(mp, 2mp) = 2mp$.

Lemma 4.2: $A \equiv \varepsilon_p$, $B \equiv 1$, $C \equiv \varepsilon_p \pmod{mp}$.

Proof: This follows directly from Theorem 1 of a recent paper by Young [19], along with the observation that $C = AB$.

Lemma 4.3: $A \equiv \varepsilon_A$, $B \equiv \varepsilon_B$, $C \equiv \varepsilon_C \pmod{mp}$.

Proof: Since $Z(q) = mp$ for all $q \mid A$, we have $mp \mid (q - \varepsilon_q)$ or $q \equiv \varepsilon_q \pmod{mp}$. If $A = \prod q^f$, then $A \equiv \prod (\varepsilon_q)^f \equiv \prod \varepsilon_{q^f} \equiv \varepsilon_A \pmod{mp}$. Likewise, $B = \varepsilon_B \pmod{mp}$. Also, $C = AB \equiv \varepsilon_A \varepsilon_B \equiv \varepsilon_C \pmod{mp}$.

Combining the results of Lemmas 4.2 and 4.3, we obtain

Lemma 4.4: $\varepsilon_A = \varepsilon_C = \varepsilon_p$; $\varepsilon_B = 1$.

Henceforth, we use the symbol ε interchangeably to denote $\varepsilon_A, \varepsilon_C$, or ε_p; however, $\varepsilon_B = 1$ in all cases.

Lemma 4.5: $\bar{k}(A) = \bar{k}(C) = 4mp$; $\bar{k}(B) = 2mp$.

Proof: Let q be the same as in the proof of Lemma 4.1. Then, since $Z(q) = mp$ is odd, it follows from Property 2.2(d) that $\bar{k}(q) = 4mp$ for all $q \mid A$; thus, $\bar{k}(A) = 4mp$. But, $\bar{k}(q_1) = 2mp = Z(q_1)$ for all $q_1 \mid B$, since $2mp \equiv 2 \pmod 4$. Then $\bar{k}(B) = 2mp$ and $\bar{k}(C) =$ LCM$(4mp, 2mp) = 4mp$.

Proof of Theorem 4.1: Since $\gcd(A, 10) = 1$, Lemma 4.3 implies that $A - \varepsilon = 2^s \cdot d$ for some $s \geq 1$ and odd d, such that $Z(A) = mp \mid d$. Then $A \mid F_d$, which shows that $A \in U$ if A is composite [using Definition 2.4(a)].

Similarly, $B - 1 = 2^{s_1} \cdot d_1$ for some $s_1 \geq 1$, odd d_1, such that $Z(B) = 2mp \mid 2d_1$. Since $mp \mid d_1$ and d_1 is odd, we have $L_{mp} \mid L_{d_1}$. Also, $B \mid L_{mp}$, and so $B \mid L_{d_1}$. By Definition 2.4(b), $B \in U$, provided B is composite. The proof is complete.

To prove Corollary 4.1, we invoke Theorem 3 of a 1980 paper by Baillie and Wagstaff [1], which implies that all SLPP's are ELPP's, i.e., that $U \subseteq V$. Also, certain results due to Rotkiewicz (see [16], [17]) imply that all ELPP's are FLPP's, i.e., that $V \subseteq W$. Then $U \subseteq W$, which together with Theorem 4.1 implies Corollary 4.1. Corollary 4.2 is a special case of this (with $e = 0$); this result was obtained by the author in a recent paper [4].

As mentioned after Definition 2.8, the author shows (in a problem [5] submitted to this journal) that the sets V and W are actually identical. In light of this, no further explicit mention of the set of ELPP's (V) will be made.

The corresponding theorem dealing with the ratio C is somewhat more involved. As was the case for A and B, we require some preliminary results. We introduce the following notation:

$$\theta = \begin{cases} 1 & \text{if } e \text{ is even,} \\ 0 & \text{if } e \text{ is odd.} \end{cases} \tag{4.1}$$

Lemma 4.6: $m \equiv p^{\theta} \pmod{12}$.

Proof: Since $p \equiv \pm 1 \pmod 6$, then $m \equiv 1$ if e is even, $m \equiv p$ if e is odd (mod 12).

Note that $\bar{k}(20) = \text{LCM}(\bar{k}(4), \bar{k}(5)) = \text{LCM}(6, 4) = 12$ and $k(20) = 5 \cdot 12 = 60$. To characterize B (mod 20), it suffices to consider all residues p (mod 12), since B involves Lucas numbers. However, to characterize A and C (mod 20), we must consider all residues p (mod 60), since A and C involve Fibonacci numbers. From Lemma 4.6, it follows that $L_{2mj} \equiv L_{2jp}\theta$ (mod 20), for all j. Then Properties 2.3(a)-(c) imply the following

Lemma 4.7: $A_e \equiv A_{\theta}$, $B_e \equiv B_{\theta}$, $C_e \equiv C_{\theta}$ (mod 20).

Using any standard table of F_u and L_u for $1 \le u \le 60$, along with quadratic reciprocity, we next form Table 1 below.

TABLE 1

p (mod 60)	$\left(\frac{5}{p}\right)$	$\left(\frac{-3}{p}\right)$	p^2 (mod 60)	F_{p^2} (mod 20)	L_{p^2} (mod 20)	$A_0 \equiv A_1$ $\equiv F_p$ (mod 20)	$B_0 \equiv B_1$ $\equiv L_p$ (mod 20)	$C_0 \equiv C_1$ $\equiv F_{2p}$ (mod 20)
1	1	1	1	1	1	1	1	1
7	−1	1	−11	9	1	−7	9	−3
11	1	−1	1	1	1	9	−1	−9
13	−1	1	−11	9	1	−7	1	−7
17	−1	−1	−11	9	1	−3	−9	7
19	1	1	1	1	1	1	9	9
23	−1	−1	−11	9	1	−3	−1	3
29	1	−1	1	1	1	9	−9	−1
−29	1	1	1	1	1	9	9	1
−23	−1	1	−11	9	1	−3	1	−3
−19	1	−1	1	1	1	1	−9	−9
−17	−1	1	−11	9	1	−3	9	−7
−13	−1	−1	−11	9	1	−7	−1	7
−11	1	1	1	1	1	9	1	9
−7	−1	−1	−11	9	1	−7	−9	3
−1	1	−1	1	1	1	1	−1	−1

As we may readily verify, using Table 1, $A_0 \equiv A_1 \equiv F_p$, $B_0 \equiv B_1 \equiv L_p$, $C_0 \equiv C_1 \equiv F_{2p}$ (mod 20). Then $(F_p)^2 \equiv F_{p^2}$, $(L_p)^2 \equiv L_{p^2}$, and $(F_{2p})^2 \equiv F_{2p^2}$ (mod 20), from which we obtain

Lemma 4.8: $A_e \equiv A_0$, $B_e \equiv B_0$, $C_e \equiv C_0$ (mod 20).

From Lemma 4.8, and by inspection of the entries in Table 1, we obtain the following lemma.

Lemma 4.9: $C \equiv \left(\frac{-3}{p}\right)$ (mod 4).

We are now ready to state the main theorem regarding C.

Theorem 4.2: $C \in (X-Y)$, unless $p \equiv 1$ or 19 (mod 30), in which case $C \in W$.

Proof: We may suppose that A and B are composite. The following proof needs some modification if either A or B is prime. Since $A \in X$ and $B \in X$, we see that $Z(A) = mp|(A-\varepsilon)$, $Z(B) = 2mp|(B-1)$. Since $C - \varepsilon = AB - \varepsilon = (A-\varepsilon)(B-1) + (A-\varepsilon) + \varepsilon(B-1)$, then $mp|(C-\varepsilon)$. Since mp is odd and $C-\varepsilon$ is even, we have $Z(C) = 2mp|(C-\varepsilon)$. $C = AB$ is necessarily composite, so $C \in X$.

From Lemmas 4.3, 4.4, and 4.9, we see that

$$C \equiv \begin{cases} \varepsilon & (\text{mod } 4mp) \quad \text{if } \varepsilon = \left(\frac{-3}{p}\right), \\ \varepsilon + 2mp & (\text{mod } 4mp) \quad \text{if } \varepsilon = -\left(\frac{-3}{p}\right). \end{cases} \tag{$*$}$$

Then, from Lemma 4.5, we obtain

$$L_C \equiv \begin{cases} L_\varepsilon \equiv \varepsilon \quad (\text{mod } C), & \text{if } \varepsilon = \left(\frac{-3}{p}\right), \\ L_{2mp+\varepsilon} \quad (\text{mod } C), & \text{if } \varepsilon = -\left(\frac{-3}{p}\right). \end{cases} \tag{$**$}$$

Now $A|F_{mp}$ and $B|L_{mp}$, clearly. Property 2.3(d) implies that $L_{2mp+\varepsilon} \equiv -\varepsilon$ (mod A), while $L_{2mp+\varepsilon} \equiv \varepsilon$ (mod B). Since $C = AB$, we see that $L_{2mp+\varepsilon} \not\equiv 1$ (mod C). Then ($**$) implies that $L_C \equiv 1$ (mod C) iff $\varepsilon = (-3/p) = 1$. By reference to Table 1, this occurs precisely when $p \equiv 1$, 19, -29, or -11 (mod 60), i.e., when $p \equiv 1$ or 19 (mod 30). Thus, $C \in Y$ iff $p \equiv 1$ or 19 (mod 30), which completes the proof.

For the special case in which $e = 0$, we obtain the following corollary.

Corollary 4.3: $F_{2p} \in (X-Y)$, unless $p \equiv 1$ or 19 (mod 30), in which case $F_{2p} \in W$.

This result extends that of Duparc [12] (and of Lehmer [14]) mentioned in Section 3.

Theorem 4.2 cannot be improved, in the sense that $C \notin U$ when $p \equiv 1$ or 19 (mod 30). To see this, first suppose $p \equiv 1$ or 19 (mod 30), so that $\varepsilon = 1$. Since $C \in X$, by Theorem 4.2, we see that $Z(C) = 2mp|(C-1)$. Letting $C - 1 = 2^s d$, where $s \geq 1$ and d is odd, then $2mp|2d$. Thus, $C|F_{2mp}|F_{2d}$. In order for $C \in U$, it is necessary that either $C|F_d$ or $C|L_d$. However, $A|F_d$ and $B|L_d$. Since $\gcd(A, B) = 1$, it is impossible for either $C|F_d$ or $C|L_d$. Therefore, $C \notin U$, as claimed.

5. CONCLUSION

No attempt has been made to generalize the results of this paper so as to apply to more general second-order sequences. The author is content to confine his investigation to the Fibonacci and Lucas sequences and to leave such generalizations to others. It is apparent, however, that any such generalizations are easily suggested by the results of this paper.

Many other areas of research are suggested for the various pseudoprimes discussed in Section 2, in some cases leading to fascinating, difficult, and as yet unanswered questions. In recent years, due to the application of LPP's to the area of primality testing and public key crytography, there has been a tendency to shift the focus of investigation on LPP's. As this brief overview has attempted to indicate, however, there are areas of theoretical interest encompassing *all* of the pseudoprimes defined here.

ACKNOWLEDGMENT

The author gratefully acknowledges the helpful suggestions of the anonymous referee, who provided some references that were previously unknown to the author, strengthened the results so as to involve SLPP's and ELPP's, and provided proofs of some of these results.

REFERENCES

1. R. Baillie & S. Wagstaff, Jr. "Lucas Pseudoprimes." *Math. of Comp.* **35.152** (1980):1391-1417.
2. P. S. Bruckman. "On the Infinitude of Lucas Pseudoprimes." *The Fibonacci Quarterly* **32.2** (1994):153-54.
3. P. S. Bruckman. "Lucas Pseudoprimes are Odd." *The Fibonacci Quarterly* **32.2** (1994): 155-57.
4. P. S. Bruckman. "On a Conjecture of Di Porto and Filipponi." *The Fibonacci Quarterly* **32.2** (1994):158-59.
5. P. S. Bruckman. Problem H-496. *The Fibonacci Quarterly* **33.2** (1995):187.
6. P. S. Bruckman. Problem H-498. *The Fibonacci Quarterly* **33.2** (1995):187.
7. P. S. Bruckman. Problem H-499. *The Fibonacci Quarterly*.**33.4** (1995):378.
8. P. S. Bruckman. Problem H-501. *The Fibonacci Quarterly*.**33.4** (1995):379.
9. P. S. Bruckman. "A Characterization of Quadratfrei Lucas Pseudoprimes." *Pi Mu Epsilon Journal* **10.3** (1994-1999):207-11.
10. A. Di Porto. "Nonexistence of Even Fibonacci Pseudoprimes of the 1st Kind." *The Fibonacci Quarterly* **31.2** (1993):173-77.
11. A. Di Porto & P. Filipponi. "A Probabilistic Primality Test Based on the Properties of Certain Generalized Lucas Numbers." In *Lecture Notes in Computer Science* **330:**211-13. Ed. C. G. Günther. Berlin: Springer-Verlag, 1988.
12. H. J. A. Duparc. "On Almost Primes of the Second Order." Rapport ZW, 1955-013, pp. 1-13. Math. Center, Amsterdam, 1955.
13. P. Kiss, B. M. Phong, & E. Lieuwens. "On Lucas Pseudoprimes Which Are Products of s Primes." In *Fibonacci Numbers and Their Applications* **1:**131-39. Ed. A. N. Philippou, G. E. Bergum, & A. F. Horadam. Dordrecht: Reidel, 1986.
14. E. Lehmer. "On the Infinitude of Fibonacci Pseudoprimes." *The Fibonacci Quarterly* **2.3** (1964):229-30.

15. E. A. Parberry. "On Primes and Pseudo-Primes Related to the Fibonacci Sequence." *The Fibonacci Quarterly* **8.1** (1970):49-60.

16. A. Rotkiewicz. "On the Pseudoprimes with Respect to the Lucas Sequences." *Bull. Acad. Polon. Sci. Ser. Math. Astr. Phys.* **21.9** (1973):793-97.

17. A. Rotkiewicz. "Problems on Fibonacci Numbers and Their Generalizations." In *Fibonacci Numbers and Their Applications* **1**:241-55. Ed. A. N. Philippou, G. E. Bergum, & A. F. Horadam. Dordrecht: Reidel, 1986.

18. D. J. White, J. N. Hunt, & L. A. G. Dresel. "Uniform Huffman Sequences Do Not Exist." *Bull. London Math. Soc.* **9** (1977):193-98.

19. P. T. Young. "*p*-Adic Congruences for Generalized Fibonacci Sequences." *The Fibonacci Quarterly* **32.1** (1994):2-10.

AMS Classification Numbers: 11A07, 11B39, 11B50