ON A CONJECTURE OF DI PORTO AND FILIPPONI

Paul S. Bruckman
615 Warren Street, Everett, QA 98201

(*Submitted July 1992*)

We begin by describing the following two properties of certain natural numbers n:

$$F_{n-(5/n)} \equiv 0 \pmod{n}, \text{ where } \gcd(n, 10) = 1, \text{ and } (5/n) \text{ is a Jacobi symbol;} \tag{1}$$

$$L_n \equiv 1 \pmod{n}. \tag{2}$$

As is well known, properties (1) and (2) are satisfied if n is prime. More interestingly, there are infinitely many composite numbers n which satisfy (1) and/or (2). We call these n "Fibonacci pseudoprimes" (or FPP's) if they satisfy (1), and "Lucas pseudoprimes" (or LPP's) if they satisfy (2). As has been remarked elsewhere [1], this nomenclature is not standard, but should be acceptable to most readers of this quarterly.

These numbers, and their generalizations, have been extensively studied by other writers. It is not our aim here to outline all the various results currently available, or in progress; suffice it to say that interest in these numbers is relatively recent, and known results are correspondingly scarce. Much of the interest in these numbers, in recent years, centers around their application in primality testing and public-key cryptography; however, it is beyond the scope of this paper to delve into this fascinating topic.

We also mention the work of Kiss, Phong, & Lieuwens [4] which showed, among other things, that there exist infinitely many numbers n that are simultaneously FPP's and LPP's. For the sake of our discussion, we shall term such numbers "Fibonacci-Lucas pseudoprimes" (or FLPP's).

In a 1989 paper [3], Di Porto & Filipponi asked the following question (which we paraphrase here, to conform with our nomenclature): "Are all the composite Fibonacci and Lucas numbers with prime subscript LPP's?"

As we shall show, the answer to this question is affirmative, if we exclude the subscript 3 (a minor oversight which Di Porto & Filipponi undoubtedly intended to account for). However, more is true: we shall, in fact, prove the following symmetric results.

Theorem 1: Given $n = F_p$, where p is a prime > 5, then n is a FLPP if and only if n is composite.

Theorem 2: Given $n = L_p$, where p is a prime > 5, then n is a FLPP if and only if n is composite.

Proof of Theorem 1: Note that $\gcd(n, 30) = 1$. Let $m = \frac{1}{2}(n-1)$. We consider two possibilities:

(a) $p \equiv \pm 1$ or $\pm 11 \pmod{30}$: then $n \equiv 1$ or $9 \pmod{20}$, $(5/p) = (5/n) = 1$, and m is even. Also, $F_p \equiv (5/p) \equiv 1 \pmod{p}$, so $p|2m$. Since p is odd, thus $p|m$, which implies $n|F_m$. As we may readily verify, $F_n - 1 = F_m L_{m+1}$; hence, $F_n \equiv 1 \pmod{n}$. Also, $F_{n-1} = F_{2m} = F_m L_m \equiv 0 \pmod{n}$; therefore, n satisfies property (1), and must either be prime or a FPP. Also, $L_n = F_{n-1} + F_{n+1} = 2F_{n-1} + F_n \equiv 1 \pmod{n}$, which shows that n satisfies (2) as well. Thus, n is either prime or a LPP. The conclusion of the theorem follows.

(b) $p \equiv \pm 7$ or $\pm 13 \pmod{30}$: then $n \equiv 13$ or $17 \pmod{20}$, $(5/p) = (5/n) = -1$, and m is even. Also, $F_p \equiv (5/p) \equiv -1 \pmod{p}$, so $p|(2m+2)$. Since p is odd, thus $p|(m+1)$, which implies

$n|F_{m+1}$. As we may readily verify, $F_n+1=F_{m+1}L_m$; hence, $F_n \equiv -1 \pmod{n}$. Also, $F_{n+1} = F_{2m+2} = F_{m+1}L_{m+1} \equiv 0 \pmod{n}$; therefore, n satisfies property (1), and must either be prime or a FPP. Also, $L_n = F_{n+1}+F_{n-1} = 2F_{n+1}-F_n \equiv 1 \pmod{n}$, which shows that n satisfies (2) as well. Thus, n is either prime or a LPP. The conclusion of the theorem follows.

We may remark that $p=19$ is the smallest prime for which F_p is composite; thus, $F_{19}=4181=37\cdot 113$ is the smallest FLPP provided by the theorem.

Proof of Theorem 2: Note that $n \equiv \pm 1 \pmod{10}$, so $(5/n)=1$. Let $m=\frac{1}{2}(n-1)$. Also, note that $L_p \equiv 1 \pmod{p}$; hence, $p|2m$. Since p is odd, thus $p|m$. We consider two possibilities:

(a) $n \equiv 1 \pmod{4}$: then m is even. Suppose $m=2^r d$, where $r \geq 1$ and d is odd. Since p is odd and $p|m$, thus $p|d$, which implies that $n|L_d$. Now $F_{2m}=F_dL_dL_{2d}L_{4d}\ldots L_{2^r d}$; hence, $n|F_{2m}$, i.e., $n|F_{n-1}$. Thus, n satisfies (1). Also $L_n = 1+5F_mF_{m+1}$, as readily verified. Since $n|L_d$, it follows (as above) that $n|F_m$. Thus, n satisfies (2) as well.

(b) $n \equiv 3 \pmod{4}$: then m is odd. Thus, $L_p|L_m$, i.e., $n|L_m$. Then $n|F_{2m}=F_mL_m$, or $n|F_{n-1}$. Hence, n satisfies (1). Also, $L_n = 1+L_mL_{m+1}$, as is readily verified. Thus, $n|L_m$ implies (2).

In either case, n satisfies both (1) and (2). The conclusion of the theorem now follows.

We may remark that $p = 23$ is the smallest prime for which L_p is composite; therefore, $L_{23}=64079=139\cdot 461$ is the smallest FLPP provided by the theorem.

It was brought to the author's attention by the referee that the question proposed by Di Porto & Filipponi [3] (mentioned earlier) was answered affirmatively by the proposers in a paper [2] which, as fortune would have it, was presented at Eurocrypt '88 and was published *before* [3]. In [2], Di Porto & Filipponi also generalized their results to more general types of sequences, but only dealt with LPP's (or their generalizations) and not with FPP's. One of their more interesting corollaries ([2], Corollary 3) is that L_{2^n} is a LPP, if composite (paraphrasing to employ the nomenclature introduced here); the smallest such composite L_m is $L_{32}=4870847=1087\cdot 4481$.

We close by remarking that the results derived in this paper may be generalized in various ways to yield comparable results for more general second-order sequences (as Di Porto and Filipponi, among others, have done); the Fibonacci and Lucas sequences are special cases of these more general types of sequences. No attempt at such generalization was made here, although it is likely that this would not present major difficulties.

REFERENCES

1. P. S. Bruckman. "On the Infinitude of Lucas Pseudoprimes." *The Fibonacci Quarterly* **32.2** (1994):153-54.
2. 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.
3. A. Di Porto & P. Filipponi. "More on Fibonacci Pseudoprimes." *The Fibonacci Quarterly* **27.3** (1989):232-42.
4. P. Kiss, B. M. Phong, & E. Lieuwens. "On Lucas Pseudoprimes Which Are Products of s Primes." In *Fibonacci Numbers and Their Applications*, **I**:131-39. Ed. A. N. Philippou, G. E. Bergum, & A. F. Horadam. Dordrecht: Reidel, 1986.

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

❖❖❖