ON THE INFINITUDE OF LUCAS PSEUDOPRIMES

Paul S. Bruckman
615 Warren Street, Everett, WA 98201
(Submitted July 1992)

The following properties of certain positive integers n are set forth:

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

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

It is well-known that properties (1) and (2) are satisfied if n is prime. If (1) is satisfied for some composite n, then n is called a *Fibonacci pseudoprime* (or FPP). If (2) is satisfied for some composite n, then n is called a *Lucas pseudoprime* (or LPP). Let U and V denote the sets of FPP's and LPP's, respectively.

It must be remarked that the above terminology is different from that used by many other authors; frequently, the term "Fibonacci pseudoprime" is used to describe numbers that satisfy (2), and/or "Lucas pseudoprime" sometimes is used to describe numbers that satisfy (1). There are, no doubt, some very good reasons for describing such numbers by one term versus another. In most papers that this author has seen, the subject matter is only *one* of the types of numbers here described, which tends to minimize confusion. When both types of numbers are being discussed, as is the case in this paper, it seems preferable to adopt the terminology defined above. Readers of this journal may tend to be more sympathetic to this usage, for obvious reasons. Apologies are made here and now to those readers who may take exception to the nomenclature adopted here.

In a 1964 paper [2], E. Lehmer showed that U is an infinite set, specifically by proving that $n = F_{2p}$ satisfies (1) for any prime $p > 5$. In a 1970 paper [3], E. A. Parberry proved some interesting results related to those of Lehmer, indirectly commenting on the infinitude of U, by a different approach. It is informative to paraphrase that portion of Parberry's results that touches on the subject of this paper; we state this as a theorem.

Theorem 1: (*) If $\gcd(n, 30) = 1$ and n is a FPP, then F_{2n} has these same properties.

Note that if $\gcd(n, 30) = 1$, then it is also true that $\gcd(F_{2n}, 30) = 1$. Theorem 1 implies that, beginning with any FPP n with $\gcd(n, 30) = 1$ (e.g., $n = 323 = 17 \cdot 19$, which is the smallest element of U), we may form the infinite sequence:

$$n,\ F_{2n},\ F_{2F_{2n}},\ F_{2F_{2F_{2n}}},\ \text{etc., each element of which is a FPP.} \tag{3}$$

We have, therefore, another demonstration (distinct from Lehmer's) that U is an infinite set.

In a 1986 paper [1], P. Kiss, B. M. Phong, & E. Lieuwens showed, along with other important results, that there exist infinitely many numbers n that are simultaneously FPP's and LPP's (i.e., the set $U \cap V$ is infinite). Actually, this is a corollary of their more general results. By the way, we remark that the smallest element of $U \cap V$ is $4181 = 37 \cdot 113 = F_{19}$.

In light of these results, it may seem redundant to prove once again that V is infinite, as the title of this paper implies. Nevertheless, the approach used below differs from that of Kiss,

Phong, & Lieuwens, and is worthy of mention. Moreover, it displays a kind of symmetry in relation to Theorem 1, providing as it does the "Lucas" counterpart of that theorem. This is stated as follows.

Theorem 2: (**) If $\gcd(n, 6) = 1$ and n is a LPP, then L_n has these same properties.

Proof: Let $u = L_n$, $v = \frac{1}{2}(u-1)$. Note that u must be odd, since $\gcd(n, 3) = 1$, hence v is an integer. We consider three possibilities:

(a) $n \equiv 1 \pmod{12}$: then $u \equiv 1 \pmod 8$, hence $v \equiv 0 \pmod 4$. Let $v = 2^r w$, where $r \geq 2$ and w is odd. Since $L_n \equiv 1 \pmod n$, thus $n|2v$. However, n is odd, so $n|w$. Then $L_n | L_w$. Now $F_v = F_w L_w L_{2w} L_{4w} \ldots L_{2^{r-1}w}$, which shows that $u|F_v$. Also, since v is even, the following identity is satisfied: $L_u - 1 = 5F_v F_{v+1}$. Therefore, $L_u \equiv 1 \pmod u$.

(b) $n \equiv 7 \pmod{12}$: then $u \equiv 5 \pmod 8$, hence $v \equiv 2 \pmod 4$. In this case, $v = 2w$, where w is odd. As in (a), $u|F_v$ and $L_u - 1 = 5F_v F_{v+1}$, so $L_u \equiv 1 \pmod u$.

(c) $n \equiv 5$ or $11 \pmod{12}$: then $u \equiv 3$ or $7 \pmod 8$, hence v is odd. As above, we have $n|2v \Rightarrow n|v \Rightarrow u|L_v$. Now, however, $L_u - 1 = L_v L_{v+1}$. Thus, $L_u \equiv 1 \pmod u$.

In all cases, $L_u \equiv 1 \pmod u$. It only remains to show that $u = L_n$ is composite; however, this follows immediately from the fact that n is odd and composite, since $L_p | u$ for any prime divisor p of n. Thus, L_n is a LPP and $\gcd(L_n, 6) = 1$, proving the theorem.

The smallest LPP not divisible by 2 or 3 is $m = 2465 = 5 \cdot 17 \cdot 29$ (in fact, *no* LPP is even, as Di Porto and this author have independently shown). Beginning with m, for example (or any other LPP not divisible by 3), we may form the infinite sequence:

$$m,\ L_m,\ L_{L_m},\ L_{L_{L_m}},\ \text{etc., each element of which is a LPP.} \tag{4}$$

Therefore, V is infinite.

Clearly, the sequences indicated in (3) and (4) increase extremely rapidly, an observation that may have some applications in primality testing. This aspect is left for other researchers. Also, the focus of this paper has been on the so-called "Fibonacci pseudoprimes" and "Lucas pseudoprimes," rather than on any of the many generalizations of these numbers studied by other writers. No doubt, such generalizations may be readily found; however, this was not explored here, and is left for future research.

REFERENCES

1. 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.
2. E. Lehmer. "On the Infinitude of Fibonacci Pseudo-Primes." *The Fibonacci Quarterly* **2.3** (1964):229-30.
3. E. A. Parberry. "On Primes and Pseudo-Primes Related to the Fibonacci Sequence." *The Fibonacci Quarterly* **8.1** (1970):49-60.

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

❖❖❖