LUCAS PSEUDOPRIMES ARE ODD

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

(*Submitted July 1992*)

It is well known that the congruence

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

is satisfied by all prime n. However, there are also many composite n satisfying (1), the smallest example being $n = 705 = 3 \cdot 5 \cdot 47$ (indeed, there are infinitely many such n). The term "Lucas pseudoprime" (or LPP) appears to be appropriate to describe such composite n. It must be mentioned, however, that there is little uniformity in the literature regarding this subject. An alternative term which is frequently used is "Fibonacci pseudoprime"; however, since this term has occasionally been used to describe those composite n which satisfy the following congruence:

$$F_{n-(5/n)} \equiv 0 \pmod{n}, \text{ where } \gcd(n, 10) = 1 \text{ and } (5/n) \text{ is a Jacobi symbol,} \tag{2}$$

it was felt advisable to avoid the latter term in this article. Accordingly, we adopt the term "Lucas pseudoprimes" (or LPP's) to describe those composite n satisfying (1). Incidentally, if U and V represent the sets of composite integers satisfying (2) and (1), respectively, it is known that U, V, and $U \cap V$ are infinite sets.

Di Porto & Filipponi [3] indicated the values of all LPP's < 10^6 (a total of 86 values). Also, in private correspondence [4], Filipponi provided the author with a table of 852 LPP's, which are all the LPP's < 10^8. On the basis of the values obtained, Di Porto & Filipponi proposed several conjectures. We are concerned here only with proving one of these conjectures, namely, that all LPP's are odd.

As it turns out, Di Porto (one of the proposers of this conjecture) has recently proven her own conjecture independently (see [5]); moreover, it came to the author's attention that a much earlier proof of this result had been given by White, Hunt, & Dresel [7] no later than 1977. The author was made aware of these revelations only after this paper was originally submitted for publication. The author publicly acknowledges the priority of these earlier efforts, and also gives Di Porto credit for her independently derived proof, which predates this paper. Developments such as these give an indication of the rapid rate of growth of knowledge in this fascinating field.

In spite of the earlier proofs, it does not seem amiss to present another proof of the statement that all LPP's are odd; this is particularly true since the proof given here differs from the earlier proofs in several particulars.

Our proof depends, in part, on some results obtained in [3], namely, that the existence of any even LPP, which we denote by n, implies that $n \equiv \pm 2$ (mod 12), and that $n \neq 2p$, where p is prime. We also require a result which we state as a lemma, without proof; the reader is referred to [1] for a proof.

Lemma 1:

$$L_{5^r} \equiv L_{5^{r-1}} \pmod{5^r}, \; r = 1, 2, \ldots . \tag{3}$$

In addition, we will need some basic results concerning the Fibonacci rank of appearance, or entry-point. We recall that, for a given $n \geq 1$, the *rank of appearance* (or *entry-point*) of n, which we denote as $Z(n)$, is defined to be the smallest positive integer t such that $n|F_t$. Various other terms and/or notation have been used by other authors, again pointing to a dearth of uniformity in the literature. One frequently used term, namely, "rank of apparition," is particularly odious to this writer, and shall be avoided steadfastly. As has been pointed out by Ribenboim [6], the latter term stems from a bad translation of the French *loi d'apparition*, which means "law of appearance," *not* "law of apparition"; in all English dictionaries, "apparition" means "ghost."

The following properties are well known and stated without further comment:

$$\begin{aligned}
&\text{(i)} && Z(n) \text{ exists for all } n \geq 1; \\
&\text{(ii)} && Z(m)|n \text{ iff } m|F_n; \\
&\text{(iii)} && Z(m)|Z(n) \text{ iff } m|n \text{ iff } F_m|F_n; \\
&\text{(iv)} && \text{If } n = \prod_{i=1}^{\omega} p_i^{e_i}, \text{ then } Z(n) = \operatorname{lcm}\left[Z(p_1^{e_1}), Z(p_2^{e_2}), \ldots, Z(p_\omega^{e_\omega})\right]; \\
&\text{(v)} && Z(p^e) = p^f Z(p), \text{ where } 0 \leq f < e.
\end{aligned} \tag{4}$$

Finally, we require another result, also stated without proof as a lemma; refer to [2] for a proof.

Lemma 2:

$$n = Z(n) \text{ iff } n = 5^u \text{ or } n = 12 \cdot 5^u, \ u \geq 0. \tag{5}$$

With these tools, the proof of the oddness of LPP's is surprisingly elementary. Now for our proof!

Suppose, to the contrary that $2n$ is a LPP. Thus, we assume that

$$L_{2n} \equiv 1 \pmod{2n}, \tag{6}$$

where n is composite and $\gcd(n, 6) = 1$, using Di Porto & Filipponi's results in [3]. The following simple identities are readily verifiable: $L_{2n} - 1 = F_{3n} / F_n$ and $L_n^2 = 5F_n^2 - 4 = L_{2n} - 2$. Along with (6), these imply the congruences:

$$\begin{aligned}
&\text{(i)} && L_n^2 \equiv -1 \pmod{2n}; \\
&\text{(ii)} && 5F_n^2 \equiv 3 \pmod{2n}; \\
&\text{(iii)} && F_{3n} \equiv 0 \pmod{2n}.
\end{aligned} \tag{7}$$

From (7)(i) and (ii), we see that $L_n \not\equiv 0, F_n \not\equiv 0 \pmod{2n}$. Thus, $F_m \not\equiv 0 \pmod{2n}$ for all m dividing n, since $F_m|F_n$. From (7)(iii), it follows that

$$Z(2n) = 3n. \tag{8}$$

Now n, and thus $Z(2n)$, are odd. Also, $Z(2n) = \operatorname{lcm}[Z(2), Z(n)]$, or

$$Z(2n) = 3n = \operatorname{lcm}[3, Z(n)]. \tag{9}$$

Since $\gcd(3, n) = 1$, we see from (9) that $3^e \| Z(n) \Rightarrow e = 0$ or 1. We consider these two possibilities as separate cases.

Case I. $\gcd(3, Z(n)) = 1$

By (9), $Z(2n) = 3Z(n) = 3n$, so $n = Z(n)$. Using Lemma 2 and the fact that $\gcd(6, n) = 1$ and n is composite, we see that $n = 5^u, u \geq 2$. Let $n = 5m$, where $m = 5^{u-1}$. Now (7)(i) implies that $L_n^2 \equiv -1 \pmod{n}$, and $L_n \equiv L_m \pmod{n}$, by Lemma 1; hence, $L_m^2 \equiv -1 \pmod{n} \Rightarrow L_{2m} \equiv 1 \pmod{n}$ $\Rightarrow L_{2m} \equiv 1 \pmod{m}$. Also, since $\gcd(3, 2m) = 1$, L_{2m} is odd (another well-known fact). Therefore, $L_{2m} \equiv 1 \pmod{2m}$. This is equivalent to the statement that $2m$ is a LPP, *provided m* is composite. By an easy inductive process, we see that $2n$, $2n/5$, $2n/5^2, \ldots, 2 \cdot 5^2 = 2n/5^{u-2}$ are all LPP's. However, as we may readily verify from a table of Lucas numbers, $L_{50} \equiv 23 \not\equiv 1 \pmod{50}$, so 50 is *not* a LPP. The contradiction eliminates this possibility.

Case II. $3^1 \| Z(n)$

By (9), $Z(2n) = Z(n) = 3n$. Also, $Z(12n) = \operatorname{lcm}[Z(12), Z(n)] = \operatorname{lcm}[12, 3n] = 12n$. Again using Lemma 2 and the fact that $\gcd(6, n) = 1$, we reach a contradiction, as in Case I.

We conclude that our original assumption is faulty and, therefore, that all LPP's are odd.

REFERENCES

1. P. S. Bruckman. Solution to Problem B-734. *The Fibonacci Quarterly*, this issue, pages 183-84.
2. P. S. Bruckman. Solution to Problem H-472. *The Fibonacci Quarterly*, this issue, pages 190-91.
3. A. Di Porto & P. Filipponi. "More on the Fibonacci Pseudoprimes." *The Fibonacci Quarterly*. **27.3** (1989):232-42.
4. P. Filipponi. Private correspondence with the author (November 1992).
5. A. Di Porto. "Nonexistence of Even Fibonacci Pseudoprimes of the 1st Kind." *The Fibonacci Quarterly* **31.2** (1993):173-77.
6. P. Ribenboim. *The Little Book of Big Primes*. Berlin: Heidelberg; New York: Springer-Verlag, 1991.
7. D. J. White, J. N. Hunt, & L. A. G. Dresel. "Uniform Huffman Sequences Do Not Exist." *Bull. London Math. Soc.* **9** (1977):193-98.

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