NONEXISTENCE OF EVEN FIBONACCI PSEUDOPRIMES OF THE 1ST KIND*

Adina Di Porto
Fondazione Ugo Bordoni, Rome, Italy
(Submitted August 1991)

1. INTRODUCTION AND PRELIMINARIES

Fibonacci pseudoprimes of the 1^{st} *kind* (1-F.Psps.) have been defined [6] as composite integers n for which the Lucas congruence $L_n \equiv 1 \pmod{n}$ is satisfied.

The aim of this paper is to establish the following

Theorem: There do not exist *even Fibonacci pseudoprimes of the* 1^{st} *kind.*

With regard to this problem, Di Porto and Filipponi, in [4], conjectured that there are no even-Fibonacci pseudoprimes of the 1^{st} kind, providing some constraints are placed on their existence, and Somer, in [12], extends these constraints by stating some very interesting theorems. Moreover, in [1], a solution has been found for a similar problem, that is, for the sequence $\{V_n(2,1)\}$, defined by $V_0(2,1)=2$, $V_1(2,1)=3$, $V_n(2,1)=3V_{n-1}(2,1)-2V_{n-2}(2,1)=2^n+1$. Actu-ally Beeger, in [1], shows the existence of infinitely many even pseudoprimes n, that is, even n such that $2^n \equiv 2 \pmod{n} \Leftrightarrow V_n(2,1) \equiv 2+1 = V_1(2,1) \pmod{n}$.

After defining (in this section) the *generalized Lucas numbers*, $V_n(m)$, governed by the positive integral parameter m, and after giving some properties of the period of the sequences $\{V_n(m)\}$ reduced modulo a positive integer t, we define in section 2 the *Fibonacci pseudoprimes of the* m^{th} *kind* (m-F.Psps.) and we give some propositions. Finally, in section 3, we demonstrate the above theorem.

Throughout this paper, p will denote an odd prime and $V_n(m)$ will denote the *generalized Lucas numbers* (see [2], [7]), defined by the second-order linear recurrence relation

$$V_n(m) = mV_{n-1}(m) + V_{n-2}(m);\; V_0(m)=2,\; V_1(m)=m, \tag{1.1}$$

m being an arbitrary natural number. It can be noted that, letting $m=1$ in (1.1), the usual Lucas numbers L_n are obtained.

The period of the sequence $\{V_n(m)\}$ reduced modulo an integer $t>1$ will be denoted by $\mathrm{P}_{(t)}\{V_n(m)\}$. For the period of the sequence $\{V_n(m)\}$ reduced modulo p, it has been established (see [8], [13]) that

$$\text{if } J(m^2+4,p)=1, \text{ then } \mathrm{P}_{(p)}\{V_n(m)\} \mid (p-1), \tag{1.2}$$

$$\text{if } J(m^2+4,p)=-1, \text{ then } \mathrm{P}_{(p)}\{V_n(m)\} \mid 2(p+1), \tag{1.3}$$

where $J(a,n)$ is the Jacobi symbol (see [3], [10], [14]) of a with respect to n, and $x|y$ indicates that x divides y.

*This work was carried out in the framework of an agreement between the Italian PT Administration and the Fondazione Ugo Bordoni.

Moreover, it can be immediately seen that

(1.4) $$\text{if } \gcd(m^2+4, p) = p, \text{ [i.e., } m^2 \equiv -4 \pmod{p}\text{], then } \mathrm{P}_{(p)}\{V_n(m)\} = 4,$$

and, if m is an odd positive integer,

(1.5) $$\mathrm{P}_{(2)}\{V_n(m)\} = 3;\ V_n(m) \equiv 0 \pmod 2 \text{ iff } n \equiv 0 \pmod 3.$$

Note that, according to (1.2), (1.3), and (1.4), the period of any generalized Lucas sequence reduced modulo a prime p is a divisor of $\Lambda(p) = \mathrm{lcm}(p-1, 2(p+1))$, that is,

(1.6) $$\mathrm{P}_{(p)}\{V_n(m)\} \mid \Lambda(p).$$

Finally, observe that, if m is a positive integer such that $m^2 \equiv -1 \pmod{t}$, then t is of the form

(1.7) $$t = 2^k \prod_j p_j^{k_j},$$

where p_j are odd rational primes of the form (see [8], [14])

$$p_j = 4h_j + 1,\ k \in \{0, 1\} \text{ and } k_j \geq 0.$$

In this case, it follows that

(1.8) $$\mathrm{P}_{(t)}\{V_n(m)\} = 12 \text{ and } V_1(m) \equiv V_5(m) \equiv m \pmod{t}.$$

2. THE FIBONACCI PSEUDOPRIMES: DEFINITION AND SOME PROPOSITIONS

The following *fundamental property* of the numbers $V_n(m)$ has been established [11]: If n is prime, then, for all m,

(2.1) $$V_n(m) \equiv m \pmod{n}.$$

The composite numbers n for which the congruence (2.1) holds are called *Fibonacci pseudoprimes of the* m^{th} *kind* (m-F.Psps.) [6].

First, let us give some well-known results (see [5], [9]) that will be needed for our further work. Let d be an odd positive integer.

(2.2) $$V_{2d}(m) = [V_d(m)]^2 + 2,$$

(2.3) $$V_{2^k d}(m) = \left[V_{2^{k-1} d}(m)\right]^2 - 2;\ k > 1,$$

(2.4) $$V_{hd}(m) = V_h(V_d(m));\ h \geq 1.$$

To establish the theorem enounced in section 1, we state the following propositions.

Proposition 1: Let $m = 2r+1$ be an odd positive integer.

If $n = 2^k(2s+1)$, $(k \geq 1, s \geq 1)$, is an even composite integer such that $n \equiv 0 \pmod 3$, then n is not an m-F.Psp., that is,

(2.5) $$\text{If } n \equiv 0 \pmod 6, \text{ then } V_n(m) \not\equiv m \pmod{n}.$$

Proposition 2: Let $m = 2r+1$ be an odd positive integer.

(2.6) $$\text{If } n = 2^k,\ k \ge 1, \text{ then } V_{2^k}(m) \equiv -1 \pmod{2^k}.$$

From this proposition, it follows that

(2.7) $$\text{If } k > 1, \text{ then } 2^k \text{ is a } (2^k - 1)\text{-F.Psp.}$$

Proposition 3: Let $m = 2r+1$ be an odd positive integer.

(2.8) $$\text{If } n = 2^k(2s+1) \not\equiv 0 \pmod 3,\ k \ge 1,\ s \ge 2, \text{ then } V_n(m) \equiv -1 \pmod{2^k}.$$

Proof of Proposition 1: If $n \equiv 0 \pmod 6$, from (1.5) we have

(2.9) $$V_n(m) \equiv 0 \pmod 2,$$

whence we obtain

(2.10) $$V_n(m) \equiv 0 \not\equiv m = 2r+1 \pmod 2,$$

which implies that

(2.11) $$V_n(m) \not\equiv m \pmod{2^k} \Rightarrow V_n(m) \not\equiv m \pmod n. \text{ Q.E.D.}$$

Proof of Proposition 2 (by induction on k): The statement is clearly true for $k = 1$. Let us suppose that the congruence

(2.12) $$V_{2^{k-1}}(m) \equiv -1 \pmod{2^{k-1}},\ k > 1$$

holds. Observing that (2.12) implies $[V_{2^{k-1}}(m)]^2 \equiv 1 \pmod{2^k}$ and, according to (2.3), we can write

(2.13) $$V_{2^k}(m) = [V_{2^{k-1}}(m)]^2 - 2 \equiv -1 \pmod{2^k}. \text{ Q.E.D.}$$

Notice that, with the same argument, it is also possible to state that

(2.14) $$\text{If } m = (2r+1), \text{ then } V_{2^k}(m) \equiv -1 \pmod{2^{k+1}} \text{ and } V_{2^k}(m) \not\equiv -1 \pmod{2^{k+2}}.$$

Proof of Proposition 3: If $n = 2^k(2s+1)$, from (2.4) we can write

(2.15) $$V_n(m) = V_{2^k}(V_{2s+1}(m));$$

moreover, if $n \not\equiv 0 \pmod 3$, we have [see (1.5)]

(2.16) $$V_{2s+1}(m) \equiv 1 \pmod 2 \Rightarrow V_{2s+1}(m) = 2h+1,\ h \ge 0,$$

whence, according to Proposition 2, we obtain

(2.17) $$V_{2^k}(V_{2s+1}(m)) = V_{2^k}(2h+1) \equiv -1 \pmod{2^k}. \text{ Q.E.D.}$$

3. THE MAIN THEOREM

Let n be an even composite number. First, observe that $1 \not\equiv -1 \pmod{2^k}$ for all $k > 1$. Propositions 1, 2, and 3 and the above obvious remark allow us to assert:

(a) If $n \equiv 0 \pmod 3$, then n is not an 1-F.Psp., according to Proposition 1;

(b) $n = 2^k$, $(k > 1)$, is not an 1-F.Psp., according to Proposition 2;

(c) $n = 2^k(2s+1) \not\equiv 0 \pmod 3$, $(k > 1, s \geq 2)$, is not an 1-F.Psp., according to Proposition 3.

Therefore, in order to demonstrate the Theorem, "There do not exist even 1-F.Psps.," it remains to prove the following

Proposition 4: Let

(3.1) $$d \not\equiv 0 \pmod 3, d > 1$$

be an odd integer, $d > 1$. If $n = 2d$ is an even composite integer, then $L_n \not\equiv 1 \pmod n$, that is, $n = 2d$ is not an 1-F.Psp.

Proof (ab absurdo): Let us suppose that

(3.2) $$L_n = L_{2d} \equiv 1 \pmod{2d} \Rightarrow L_{2d} \equiv 1 \pmod d;$$

by (2.2) we obtain

(3.3) $$[L_d]^2 = L_{2d} - 2 \equiv 1 - 2 \equiv -1 \pmod d$$

which implies [see (1.7), sec. 1]

(3.4) $$d = \prod_j p_j^{k_j}, \ p_j = 4h_j + 1, \ k_j \geq 0.$$

Notice that (3.4) makes the $d \not\equiv 0 \pmod 3$ hypothesis unnecessary.

Under the conditions (3.1) and (3.4), we have

(3.5) $$d \equiv 1 \pmod{12} \text{ or } d \equiv 5 \pmod{12},$$

and we can find a positive integer m such that

(3.6) $$m^2 \equiv -1 \pmod d;$$

then, from (1.8) and (3.5), we can write the congruence

(3.7) $$V_d(m) \equiv m \pmod d,$$

which implies

(3.8) $$[V_d(m)]^2 \equiv m^2 \equiv -1 \pmod d.$$

Therefore, by (3.3) and (3.8), we obtain the congruence

(3.9) $$[L_d]^2 \equiv [V_d(m)]^2 \pmod d,$$

and, in particular, if p is the smallest prime factor of d, we can write

(3.10) $$[L_d]^2 \equiv [V_d(m)]^2 \pmod p \Rightarrow L_d \equiv \pm V_d(m) \pmod p.$$

First, observe that $\gcd(d, \Lambda(p)) = 1$, then we can find an odd positive integer d' such that

(3.11) $$d \cdot d' \equiv 1 \pmod{\Lambda(p)};$$

taking into account the equality (2.4), from (1.6), (3.10), and (3.11), we obtain

$$V_{d'}(L_d) = L_{d'd} \equiv 1 \equiv V_{d'}(\pm V_d(m)) = \pm V_{d'd}(m) \equiv \pm m \pmod{p}, \tag{3.12}$$

whence we obtain the congruence

$$m \equiv \pm 1 \pmod{p}$$

which contradicts the assumption

$$m^2 \equiv -1 \pmod{d} \Rightarrow m^2 \equiv -1 \pmod{p}. \text{ Q.E.D.}$$

ADDENDUM

About six months after this paper had been accepted for publication, I became aware of the fact that an alternative proof of the nonexistence of even 1-F.Psps. has been given by D. J. White, J. N. Hunt, and L. A. G. Dresel in their paper "Uniform Huffman Sequences Do Not Exist," published in *Bull. London Math. Soc.* **9** (1977):193-98.

REFERENCES

1. N. G. W. H. Beeger. "On Even Numbers n Dividing $2^n - 2$." *Amer. Math. Monthly* (1951): 553-55.
2. M. Bicknell. "A Primer on the Pell Sequence and Related Sequences." *Fibonacci Quarterly* **13.4** (1975):345-49.
3. H. Cohn. *A Second Course in Number Theory.* New York : Wiley & Sons, 1962.
4. A. Di Porto & P. Filipponi. "More on the Fibonacci Pseudoprimes." *Fibonacci Quarterly* **27.3** (1989):232-42.
5. A. Di Porto & P. Filipponi. "A Probabilistic Primality Test Based on the Properties of Certain Generalized Lucas Numbers." *Lecture Notes in Computer Science* **330** (Berlin: Springer, 1988):211-23.
6. A. Di Porto, P. Filipponi, & E. Montolivo. "On the Generalized Fibonacci Pseudoprimes." *Fibonacci Quarterly* **28.4** (1990):347-54.
7. P. Filipponi & A. F. Horadam. "A Matrix Approach to Certain Identities." *Fibonacci Quarterly* **26.2** (1988):115-26.
8. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers.* 2nd ed. Oxford: Clarendon Press, 1945.
9. D. Jarden. *Recurring Sequences.* 3rd ed. Jerusalem: Riveon Lematematika, 1973.
10. D. E. Knuth. *The Art of Computer Programming.* New York: Addison Wesley, 1981.
11. O. Ore. *Number Theory and Its History.* 2nd ed. New York: McGraw-Hill, 1956.
12. L. Somer. "On Even Fibonacci Pseudoprimes." *Applications of Fibonacci Numbers*, vol. 4. Dordrecht: Kluwer, 1991.
13. J. Sommer. *Introduction à la théorie des nombres algébriques.* Paris: Hermann et Fils, 1911.
14. I. M. Vinogradov. *Elements of Number Theory.* New York: Dover, 1945.

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