ON THE EXISTENCE OF EVEN FIBONACCI PSEUDOPRIMES WITH PARAMETERS P AND Q

Richard André-Jeannin
IUT GEA, Route de Romain, 54400 Longwy, France

(*Submitted June 1994*)

1. INTRODUCTION

Let us consider the generalized Lucas sequence $\{V_n\}$ defined by the recurrence relation

$$V_n = PV_{n-1} - QV_{n-2};\ V_0 = 2,\ V_1 = P,$$

where P is a positive integer and $Q = \pm 1$. A Fibonacci pseudoprime with parameters P and Q [(P, Q)-FPSP] is a composite number n such that

$$V_n \equiv P \pmod{n}.$$

Recently (see [1], [2], and [5]), the following theorem was proved.

Theorem 1: There do not exist even Fibonacci pseudoprimes with parameters $P = 1$ and $Q = -1$.

In this paper, our aim is to investigate the existence of the even (P, Q)-FPSP. We shall prove the following result.

Theorem 2: If $(P, Q) \neq (1, -1)$ and $(P, Q) \neq (1, 1)$, then there exists at least one even Fibonacci pseudoprime with parameters P and Q.

Theorem 2 is a consequence of Theorem 1 and of the following propositions.

Proposition 1: There do not exist even Fibonacci pseudoprimes with parameters $P = Q = 1$.

Proposition 2: $n = 2^k, k \geq 2$. is a (P, Q)-FPSP, $Q = \pm 1$, if and only if $P \equiv 2 \pmod{2^k}$ or $P \equiv -1 \pmod{2^k}$.

Proposition 3: If $P \equiv 0 \pmod 4$ or $P \equiv 1 \pmod 4$ (with $P \neq 1$) and if $(P, Q) \neq (5, 1)$, then there exists an odd prime number p such that $n = 2p$ is an even (P, Q)-FPSP.

Proposition 4: There exist odd prime numbers p and q, with $p \neq q$, such that $n = 2pq$ is an even $(5, 1)$-FPSP.

2. PRELIMINARIES

In this section, we shall gather some lemmas which will be needed in the sequel.

Lemma 1: If $P \equiv 0 \pmod 4$ and $Q = \pm 1$, then the number $A = P^2 - P - 2Q$ admits an odd prime divisor.

Proof: We have $A \equiv 2 \pmod 4$ since $P \equiv 0 \pmod 4$, whence A admits an odd prime divisor, unless $A = \pm 2$, which is clearly impossible.

Lemma 2: If $P \equiv 1 \pmod 4$ and $Q = \pm 1$, then the number $A = P^2 - P - 2Q$ admits an odd prime divisor $p \neq 3$, unless $(P, Q) = (1, -1)$, $(P, Q) = (1, 1)$, or $(P, Q) = (5, 1)$.

Proof: We have $A \equiv 2 \pmod 4$ since $P \equiv 1 \pmod 4$, whence A admits an odd prime divisor, unless $A = \pm 2$. We consider two possibilities:

(a) Assuming first that $Q = -1$, we see that $A = P^2 - P + 2 = \pm 2$ if and only if $P = 1$. Moreover, $A \equiv \pm 1 \pmod 3$. Thus, A admits an odd prime divisor $p \neq 3$ when $P \neq 1$.

(b) Supposing now that $Q = 1$, we see that $A = P^2 - P - 2 = \pm 2$ if and only if $P = 1$. Moreover, $A \equiv 0 \pmod 3$ only if $P \equiv 2 \pmod 3$. Thus, A admits an odd prime divisor $p \neq 3$, except possibly when $P \equiv 1 \pmod 4$ and $P \equiv 2 \pmod 3$; in other words, when $P \equiv 5 \pmod{12}$. If $P = 5$, then $A = 18 = 2 \cdot 3^2$. If $P > 5$, we put $P = 12k + 5\,(k \geq 1)$ and we get that $A = 18(2k+1)(4k+1)$ and at least one of the factors $(2k+1)$ or $(4k+1)$ contains an odd prime divisor $p \neq 3$, since g.c.d.$(2k+1, 4k+1) = 1$. This completes the proof.

Lemma 3: Let $\{a_k\}$ be a sequence of integers defined by the recurrence relation

$$a_{k+1} = a_k^2 - 2, \quad k \geq 1. \tag{2.1}$$

If a_1 is even, then $a_k \equiv 2 \pmod{2^k}$, $k \geq 1$, and if a_1 is odd, then $a_k \equiv -1 \pmod{2^k}$, $k \geq 1$.

Proof: The statements clearly hold for $k = 1$. Let us suppose that $a_k \equiv \alpha \pmod{2^k}$, where $k \geq 1$ and $\alpha = -1$ or $\alpha = 2$ (notice that $\alpha^2 - 2 = \alpha$). Thus, we have

$$a_k = \alpha + \lambda 2^k, \text{ where } \lambda \text{ is an integer}$$

and

$$\begin{aligned} a_{k+1} &= a_k^2 - 2 = \alpha^2 - 2 + 2^{k+1}(\alpha\lambda + \lambda^2 2^{k-1}) \\ &\equiv \alpha^2 - 2 = \alpha \pmod{2^{k+1}}. \end{aligned}$$

This completes the proof.

3. PROOFS

Proof of Proposition 1: Let us consider the sequence

$$V_n = V_{n-1} - V_{n-2},\ V_0 = 2,\ V_1 = 1.$$

It is clear that the sequence $\{V_n\}$ is periodic, with period 6 and that

$$V_{6k} = 2,\ k \geq 0, \quad \text{and} \quad V_{6k \pm 2} = -1,\ k \geq 0,$$

which implies that there does not exist an even (1, 1)-FPSP.

Proof of Proposition 2: It is well known and readily proven [4] that, for every $n \geq 0$, $V_{2n} = V_n^2 - 2Q^n$, and thus that

$$V_{2^{k+1}} = V_{2^k}^2 - 2(\pm 1)^{2^k} = V_{2^k}^2 - 2, \text{ for } k \geq 1.$$

Hence, the sequence $a_k = V_{2^k}$ satisfies the recurrence relation (2.1). Noticing that $a_1 = V_2 = P^2 - 2Q \equiv P^2 \equiv P \pmod 2$, we see by Lemma 3 that $V_{2^k} \equiv 2 \pmod{2^k}$ if $k \geq 1$ and P is even, and that

$V_{2^k} \equiv -1 \pmod{2^k}$ if $k \geq 1$ and P is odd. Hence 2^k $(k > 1)$ is a (P, Q)-FPSP if and only if $P \equiv 2$ (mod 2^k) or $P \equiv -1 \pmod{2^k}$.

Remark: The proof for P odd positive and $Q = -1$ can be found on page 175 in [2].

Corollary: $n = 4$ is a (P, Q)-FPSP if and only if $P \equiv 2 \pmod 4$ or $P \equiv -1 \pmod 4$.

Proof of Proposition 3: We first recall some well-known properties:

(i) If P is even, then $V_n \equiv 0 \pmod 2$ for every $n \geq 0$.
(ii) If P is odd, then $V_n \equiv 0 \pmod 2$ if and only if $n \equiv 0 \pmod 3$.
(iii) If p is a prime number, then $V_{np} \equiv V_n \pmod p$ for every $n \geq 0$.

For a proof of (iii), the reader may wish to consult [3] or [4]. Let us now suppose that $P \equiv 0$ (mod 4) or $P \equiv 1 \pmod 4$ and that p is an odd prime number. The congruence $V_{2p} \equiv P \pmod{2p}$ is equivalent to the system

$$V_{2p} \equiv P \pmod 2 \tag{3.1}$$

and

$$V_{2p} \equiv P \pmod p. \tag{3.2}$$

By (i) and (ii), the congruence (3.1) holds for every odd prime number p if $P \equiv 0 \pmod 4$ and for every prime number $p > 3$ if $P \equiv 1 \pmod 4$. By (iii), we see that (3.2) is equivalent to $V_2 \equiv P$ $(\bmod p)$ which can also be written

$$P^2 - P - 2Q \equiv 0 \pmod p. \tag{3.3}$$

If $P \equiv 0 \pmod 4$, we see by Lemma 1 that there exists an odd prime number p such that (3.3) and, thus, (3.2) hold. If $P \equiv 1 \pmod p$ and $P > 5$, we see by Lemma 2 that the same result holds (with $p > 3$), so the proof is complete.

Remark: If $(P, Q) = (5, 1)$, we see by Lemma 2 that there does not exist an odd prime number p such that $n = 2p$ is a $(5, 1)$-FPSP. Actually, we see by (3.3) that $p = 3$ and by (ii) we have $V_{2p} = V_6 \equiv 0 \not\equiv 5 \pmod 2$.

Proof of Proposition 4: Let us suppose that $(P, Q) = (5, 1)$. We shall prove that $n = 6554 = 2 \cdot 29 \cdot 113$ is an even $(5, 1)$-FPSP. Let $N(p)$ be the period of the sequence $\{V_n\}$ modulo p. By direct computation, one can see that $N(2) = 3$, $N(29) = 5$, and $N(113) = 57$. We also see that $6554 \equiv -1$ [mod $N(p)$], where $p = 2$, $p = 29$, or $p = 113$. Hence,

$$V_{6554} = V_{kN(p)-1} \equiv V_{N(p)-1} = 5V_{N(p)} - V_{N(p)+1} = 5 \pmod p,$$

and therefore,

$$V_{6554} \equiv 5 \pmod{6554}.$$

This completes the proof.

Remark: One can also verify that the numbers $11026 = 2\cdot 37\cdot 149$, $26506 = 2\cdot 29\cdot 457$, and $119074 = 2\cdot 29\cdot 2053$ are even $(5, 1)$-FPSP. This can be easily checked, noticing that $N(37) = 9$, $N(149) = 75$, and $N(457) = N(2053) = 57$.

ACKNOWLEDGMENT

I am grateful to the referee for pointing out a generalization of an earlier version of Proposition 2.

REFERENCES

1. P. S. Bruckman. "Lucas Pseudoprimes Are Odd." *The Fibonacci Quarterly* **32.2** (1994): 155-57.
2. A. Di Porto. "Nonexistence of Even Fibonacci Pseudoprimes of the 1st Kind." *The Fibonacci Quarterly* **31.2** (1993):173-77.
3. V. E. Hoggatt, Jr., & M. Bicknell. "Some Congruences of the Fibonacci Numbers Modulo a Prime *P*." *Mathematics Magazine* **47.5** (1974):210-14.
4. E. Lucas. "Théorie des fonctions numériques simplement périodiques." *Amer. J. Math.* **1** (1878):184-220, 289-321.
5. 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: 11B39, 11B50, 11A07

❖❖❖