A PROBABILISTIC PRIMALITY TEST BASED ON THE PROPERTIES OF CERTAIN GENERALIZED LUCAS NUMBERS

Adina Di Porto and Piero Filipponi
Fondazione Ugo Bordoni
I–00142 Roma, Italy

Abstract

After defining a class of generalized Fibonacci numbers and Lucas numbers, we characterize the *Fibonacci pseudoprimes of the* m^{th} *kind.*

In virtue of the apparent paucity of the composite numbers which are Fibonacci pseudoprimes of the m^{th} kind for distinct values of the integral parameter m, a method, which we believe to be new, for finding large probable primes is proposed. An efficient computational algorithm is outlined.

1. Introduction and generalities

In this paper, after defining the *generalized Fibonacci numbers* U_n and the *generalized Lucas numbers* V_n (Sec.1), the *Fibonacci Pseudoprimes of the* m^{th} *kind* are characterized (Sec.2).

In virtue of the scarceness of the pseudoprimes which are simultaneously of the m^{th} kind for distinct values of m, a method for finding *probable primes* is proposed in Sec.3 (for a definition of probable primes see [1]).

In Sec.4 some theoretical aspects concerning the above said pseudoprimes are considered.

Let m be an arbitrary natural number. The generalized Fibonacci numbers $U_n(m)$ (or simply U_n, if there is no fear of confusion) and the generalized Lucas numbers $V_n(m)$ (or simply V_n) are defined (e.g., see [2]) by the second order recurrence relations

Work carried out in the framework of the Agreement between the Italian PT Administration and the Fondazione "Ugo Bordoni".

C.G. Guenther (Ed.): Advances in Cryptology - EUROCRYPT '88, LNCS 330, pp. 211-223, 1988.

$$U_{n+2} = mU_{n+1} + U_n \quad ; \quad U_0 = 0, U_1 = 1 \tag{1.1}$$

and

$$V_{n+2} = mV_{n+1} + V_n \quad ; \quad V_0 = 2, V_1 = m, \tag{1.2}$$

respectively. These numbers can also be expressed [2] by means of the closed forms (Binet forms)

$$U_n = (\alpha^n - \beta^n)/\Delta, \tag{1.3}$$

$$V_n = U_{n-1} + U_{n+1} = \alpha^n + \beta^n, \tag{1.4}$$

where

$$\begin{cases} \Delta = (m^2+4)^{1/2} \\ \alpha = (m+\Delta)/2 \\ \beta = (m-\Delta)/2. \end{cases} \tag{1.5}$$

The notations α_m, β_m and Δ_m will be employed whenever the meaning of α, β and Δ can be misunderstood (e.g., see Lemma 2). By (1.5) it can be seen that $\alpha\beta = -1$ and $\alpha + \beta = m$. Moreover, it can be noted that, letting $m = 1$ in (1.1) and (1.2), the usual Fibonacci numbers F_n and Lucas numbers L_n turn out, respectively.

A further interesting expression for V_n is [3]

$$V_n = \sum_{i=0}^{[n/2]} C_{n,i}\, m^{n-2i} \tag{1.6}$$

where

$$\begin{cases} C_{0,0} = 2 \\ C_{n,i} = \dfrac{n}{n-i}\binom{n-i}{i}. \end{cases} \tag{1.7}$$

Rewriting (1.6) as

$$V_n = m^n + n \sum_{i=1}^{[n/2]} \frac{C_{n,i}}{n}\, m^{n-2i}, \quad (n \geq 1) \tag{1.8}$$

noting that, if n is a prime then $C_{n,i}/n$ is an integer and using Fermat's little theorem, the following *fundamental property* of the numbers V_n is established

$$V_n(m) \equiv m \pmod{n} \quad \forall\ m \quad (\text{if } n \text{ is a prime}). \tag{1.9}$$

2. The Fibonacci pseudoprimes of the m^{th} kind : definition and numerical aspects

Observing (1.9), the following question arises spontaneously: "Do odd composites exist which satisfy this congruence?" The answer is affirmative.

We define as *Fibonacci Pseudoprimes of the* m^{th} *kind* (m-F.Psps.) all *odd* composite integers n for which $V_n(m) \equiv m \pmod{n}$ and denote them by $s_k(m)$ ($k = 1, 2, \ldots$). The corresponding sets will be denoted by S_m, while the sets of all m-F.Psps. not exceeding a given n will be denoted by $S_{m,n}$. For example, we found that $s_1(1) = 705 = 3 \cdot 5 \cdot 47$, $s_1(2) = 169 = 13^2$ and $s_1(3) = 33 = 3 \cdot 11$.

The numbers $s_k(1)$ have been analyzed in previous papers [4], [5]. In particular, we found that all composite integers belonging to $S_{1,n}$ (for $n = 10^8$) are square-free and most of them are congruent to 1 both modulo 4 (82.3 %) and modulo 10 (63.2 %). Moreover, we noted that this behavior seems to become more marked as n increases, but we were not able to find any justification of these facts.

Now, another question arises:"Do odd composite integers exist which are m-F.Psps. for distinct values of m ?" Once again, the answer is affirmative. For example, the number $34{,}561 = 17 \cdot 19 \cdot 107$ is the smallest number belonging to both S_1 and S_2.

A computer experiment was carried out essentially to determine the cardinality of the intersections

$$G_{n,M} = \bigcap_{m=1}^{M} S_{m,n} \quad \left(\begin{array}{l} n = 10^8 \\ M = 1, 2, \ldots, \mu \ (\mu : G_{n,\mu} = \varnothing,\ G_{n,\mu-1} \neq \varnothing) \end{array} \right). \qquad (2.1)$$

Namely, we found that, for $n = 10^8$,

$$|G_{n,1}| = |S_{1,n}| = 852\ ,\ |G_{n,2}| = 48\ ,\ |G_{n,3}| = |G_{n,4}| = 5\ ,$$

$$|G_{n,5}| = |G_{n,6}| = |G_{n,7}| = 1\ ,\ |G_{n,8}| = 0\ .$$

The fact that $G_{n,3}$ and $G_{n,4}$ have the same cardinality will be justified by Theor.6 (Sec.4). The numbers (below 10^8) belonging to these two sets are

$s_{89}(1) = 1{,}034{,}881 = 41 \cdot 43 \cdot 587$
$s_{137}(1) = 2{,}184{,}533 = 13 \cdot 197 \cdot 853$
$s_{364}(1) = 15{,}485{,}185 = 5 \cdot 79 \cdot 197 \cdot 199$
$s_{561}(1) = 39{,}002{,}041 = 13 \cdot 19 \cdot 269 \cdot 587$
$s_{802}(1) = 87{,}318{,}001 = 17 \cdot 71 \cdot 73 \cdot 991$

of which the latter belongs also to $G_{n,7}$, besides being a *Carmichael number* [1].

Let $\sigma_m(n) = |S_{m,n}|$ be the m-F.Psp.-counting function. The behavior of $\sigma_1(n)$ vs. n is shown in fig.1, while the behavior of $|G_{n,2}|$ is shown in table 1.

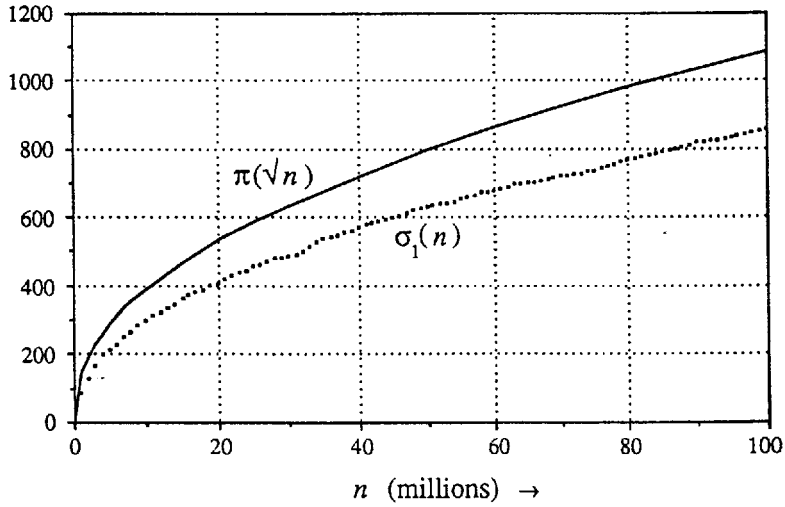

Fig.1- Behavior of $\sigma_1(n)$ vs n.

Table 1

n	$\lvert G_{n,2}\rvert$	n	$\lvert G_{n,2}\rvert$
10^7	18	$6\cdot10^7$	39
$2\cdot10^7$	27	$7\cdot10^7$	41
$3\cdot10^7$	30	$8\cdot10^7$	44
$4\cdot10^7$	36	$9\cdot10^7$	45
$5\cdot10^7$	38	10^8	48

Numerically, $\sigma_1(n)$ seems asymptotically related to the prime-counting function $\pi(n)$. The inspection of fig.1 suggests the following

CONJECTURE 1 : "There exists a positive constant c not exceeding 1 such that $\sigma_1(n)$ is asymptotic to $c\,\pi(\sqrt{n})$."

3. A possible probabilistic primality test

The numerical evidence that turns out from the experimental results suggests a method for obtaining *probable primes* .

Let $< a >_b$ denote the remainder of a divided by b. For given integers n (odd) and M ($n > M$), let us calculate

$$r_m = < V_n(m) >_n \qquad \text{for } m = 1, 2, \ldots, M \ . \tag{3.1}$$

If $r_m \neq m$ for some value of m, then n is composite. If n passes M consecutive tests, that is if $r_m = m$ for all values of m $(1 \leq m \leq M)$, then n is a probable prime (with probability P_M). A thorough investigation of the properties of the m-F.Psps. could suggest a suitable value for M depending on the order of magnitude of n. This will be the aim of a future work.

It must be noted that, if Conj.1 were proved, a sufficiently large n which passes the first test ($m = 1$) would be prime with probability

$$P_1 \approx 1 - 2c / \sqrt{n} \ . \tag{3.2}$$

Due to the apparent extreme scarceness of the composites $n \in S_m$ ($m = 1, 2, \ldots, M$), the probability P_M seems to rapidly increase as M increases. The choice of the most suitable set of tests to which submit n is still an open problem.

By suitably modifying the algorithm for obtaining $r_1 = < L_n >_n$ [4], an efficient calculation of V_n reduced modulo n can be performed. The so-obtained algorithm finds r_m after $[\log_2 n]$ recursive calculations. For example, ascertaining that the 81-digit composite

110,221,474,294,665,636,794,016,854,991,608,758,669,691,745,119,
008,792,721,304,656,075,481,680,733,031,679

belongs to S_1 required a calculation time of about 25 seconds on a VAX 11 / 750 computer.

4. Some properties of the m-F.Psps.

In this section several properties of the m-F.Psps. are demonstrated . We hope that they can lead to the discovery of further properties of these numbers. In particular , a formula which gives the minimum value of M (or an upper bound for this value) for which $|G_{n,M}| = 0$, once n is given, would be greatly appreciated.

First, let us state some theorems concerning the case $m = 1$.

THEOREM 1 : If n is an odd integer not divisible by 3 and $L_n \equiv 1 \pmod{n}$, then

$$L_{L_n} \equiv 1 \pmod{L_n} \ .$$

Proof: Since it is known [6] that L_n is odd, we can write

$L_n = 4h \pm 1 \equiv 1 \pmod{n}$ $\quad (h \in N = \{0, 1, 2, \ldots\})$.

Case 1 : $L_n = 4h + 1 \equiv 1 \pmod{n}$

We have $2h \equiv 0 \pmod{n}$, whence [7]

$$F_{2h} \equiv 0 \pmod{L_n}. \tag{4.1}$$

From the identities available in [8, p.95], we can write

$$L_{L_n} - 1 = L_{4h+1} - 1 = 5F_{2h}F_{2h+1}, \tag{4.2}$$

whence, by (4.1),

$$L_{L_n} - 1 \equiv 5 \cdot 0 \cdot F_{2h+1} \equiv 0 \pmod{L_n}.$$

Case 2 : $L_n = 4h - 1 \equiv 1 \pmod{n}$

We have $2h - 1 \equiv 0 \pmod{n}$, whence [7]

$$L_{2h-1} \equiv 0 \pmod{L_n}. \tag{4.3}$$

Again from [8, p.95], we can write

$$L_{L_n} - 1 = L_{4h-1} - 1 = L_{2h}L_{2h-1}, \tag{4.4}$$

whence, by (4.3),

$$L_{L_n} - 1 \equiv L_{2h} \cdot 0 \equiv 0 \pmod{L_n}. \qquad \text{Q.E.D.}$$

From Theor.1 we can derive the following corollaries.

COROLLARY 1 : If $p \geq 5$ is a prime and L_p is composite, then $L_p \in S_1$.

COROLLARY 2 : If n is not divisible by 3 and belongs to S_1, then $L_n \in S_1$.

Proof :

(*i*) From Theor.1 we have $L_{L_n} \equiv 1 \pmod{L_n}$.

(*ii*) By hypothesis $n = st$, with s and t odd integers not divisible by 3. Hence L_n is odd and composite [7]. This completes the proof. It can be noted that also L_n is not divisible by 3, as n is odd [6]. Q.E.D.

If n is not divisible by 3 and belongs to S_1, then the number L_n fulfils the same conditions. Therefore, we can claim that

$$L_{L_n} \in S_1 ,$$

and such a statement can be iterated *ad infinitum* , so that

$$L_{L_{\iddots_{L_n}}} \in S_1 .$$

Consequently, since there exists at least a number $s_k(1)$ not divisible by 3 (the smallest among them is $s_2(1) = 2{,}465$) the following proposition can be stated

PROPOSITION 1 (Conj. 3 in [4]) : There exist infinitely many 1-F.Psps.

THEOREM 2 : For $k \in N$,

$$L_{L_{2^k}} \equiv 1 \pmod{L_{2^k}} .$$

Proof : The statement holds clearly for $k = 0,1$. In fact, we have $L_1 \equiv 1 \pmod 1$ and $L_3 \equiv 1 \pmod 3$. Hence, let us consider $k \geq 2$. It is known [9] that

$$L_{2^k} + 1 \equiv 0 \pmod{2^k}, \tag{4.5}$$

so, L_{2^k} can be rewritten as

$$L_{2^k} = h2^k - 1 \qquad (h \in N). \tag{4.6}$$

From (4.6) and [8, p.95] we can write

$$L_{L_{2^k}} - 1 = L_{h2^k - 1} - 1 = L_{4h2^{k-2} - 1} - 1 = L_{h2^{k-1}} L_{h2^{k-1} - 1} . \tag{4.7}$$

In order to satisfy the congruence

$$L_{L_{2^k}} - 1 \equiv 0 \pmod{L_{2^k}} \tag{4.8}$$

it suffices that the left factor on the right-hand side of (4.7) is divisible by L_{2^k}, that is, it

suffices [7] that $h2^{k-1}$ is an odd multiple of 2^k. Equivalently, we can say that the fulfilment of the equality $h = 2(2t+1)$ $(t \in N)$, that is of the equality (see (4.6))

$$L_{2^k} + 1 = (2t+1)2^{k+1} \qquad (t \in N), \tag{4.9}$$

is a sufficient condition for the congruence (4.8) to be satisfied.

To establish the general validity of (4.9) we shall use induction on k and the identity I_{15} [10] which allows us to write

$$L_{2^{k+1}} = L_{2^k}^2 - 2. \tag{4.10}$$

The equality (4.9) holds for $k = 2$. In fact, we have $L_4 + 1 = 8 = (2 \cdot 0 + 1)2^3$. Let us suppose that (4.9) holds up to a certain $k > 2$. For the inductive step $k \to k+1$, from (4.10) and (4.9) we can write

$$L_{2^{k+1}} + 1 = L_{2^k}^2 - 1 = [(2t+1)2^{k+1} - 1]^2 - 1 = (2t_1 + 1)2^{k+2} \qquad (t_1 \in N).$$

Q.E.D.

COROLLARY 3 : If L_{2^k} is composite, then $L_{2^k} \in S_1$.

To prove the next theorem we need the following

LEMMA 1: If $L_n \equiv 0 \pmod{n}$, then $L_n \equiv 0 \pmod{3n}$.

Proof: The congruence $L_n \equiv 0 \pmod{n}$ implies [8, Theor. F, p.72] that

$$n = 6(2k+1) = 2 \cdot 3^{r+1}(6h \pm 1) \qquad (k, r, h \in N). \tag{4.11}$$

Therefore, it suffices to prove that

$$L_n = L_{2 \cdot 3^{r+1}(6h \pm 1)} \equiv 0 \pmod{3^{r+2}}. \tag{4.12}$$

Let us invoke induction on r. The congruence (4.12) holds for $r = 0$. In fact, considering the sequence $\{ L_n \}$ reduced modulo 9 [6], it is readily seen that $L_{6(6h \pm 1)} \equiv 0 \pmod{9}$. Let us suppose that (4.12) holds up to a certain $r > 0$. For the inductive step $r \to r+1$, using the identity $L_{s+t} = L_s L_t - L_{s-t}$ (t even) [10], we write

$$L_{2 \cdot 3^{r+2}(6h \pm 1)} = L_{(2+1) \cdot 2 \cdot 3^{r+1}(6h \pm 1)} = L_{2 \cdot 3^{r+1}(6h \pm 1)} (L_{4 \cdot 3^{r+1}(6h \pm 1)} - 1). \tag{4.13}$$

It is known [6] that $L_{4\cdot 3^{r+1}(6h\pm 1)} \equiv 1 \pmod 3$. Then, by (4.13) and hypothesis we obtain the congruence $L_{2\cdot 3^{r+2}(6h\pm 1)} \equiv 0 \pmod{3^{r+3}}$. Q.E.D.

THEOREM 3 : If $L_n \equiv 0 \pmod n$, then

$$L_{L_n-1} \equiv 1 \pmod{L_n - 1}.$$

Proof: Since we have necessarily (see (4.11)) $n = 6(2h+1)$ and, therefore [6] $L_n = 4k+2$ ($k \in N$), from Lemma 1 we have $L_n = 4k+2 \equiv 0 \pmod{18(2h+1)}$ ($h \in N$), that is

$$2k+1 \equiv 0 \pmod{9(2h+1)}. \tag{4.14}$$

From [8, p.95] we can write

$$L_n - 1 = L_{4(3h+1)+2} - 1 = F_{3[2(3h+1)+1]} / F_{2(3h+1)+1} \tag{4.15}$$

whence

$$F_{3[2(3h+1)+1]} = F_{9(2h+1)} \equiv 0 \pmod{L_n - 1}. \tag{4.16}$$

Again, from [8, p.95], we have

$$L_{L_n-1} - 1 = L_{4k+1} - 1 = 5F_{2k}F_{2k+1}. \tag{4.17}$$

Since, by (4.16) and (4.14), we see that $L_n - 1 \mid F_{9(2h+1)}$ and [7] $F_{9(2h+1)} \mid F_{2k+1}$, from (4.17) we obtain

$$L_{L_n-1} - 1 \equiv 5F_{2k} \cdot 0 \equiv 0 \pmod{L_n - 1}. \quad \text{Q.E.D.}$$

COROLLARY 4 : If $L_n \equiv 0 \pmod n$ and $L_n - 1$ (necessarily odd) is composite, then $L_n - 1 \in S_1$.

COROLLARY 5 (see [11]): If $L_{2\cdot 3^k} - 1$ ($k \geq 1$) is composite, then $L_{2\cdot 3^k} - 1 \in S_1$.

THEOREM 4 : If $n = p_1 p_2 \cdots p_k$, with $p_i = 5h_i \pm 1$ ($1 \leq i \leq k$) is a Carmichael number, then $n \in S_1$.

Proof: Let P_i be a repetition period (not necessarily the shortest period) of the Lucas sequence reduced modulo the prime p_i and let $\Lambda = \text{l.c.m.}.(P_1, P_2, \ldots, P_k)$.

A sufficient condition for n to belong to S_1 is that

$$h\Lambda + 1 = n \qquad (h \in N). \tag{4.18}$$

In fact, the fulfilment of this condition implies that $L_{h\Lambda+1} \equiv L_1 \equiv 1 \pmod{p_1 p_2 \ldots p_k}$. On the other hand, it is known [6] that if $p_i = 5h_i \pm 1$, then $P_i = p_i - 1$. Therefore, it is immediately seen that Λ equals the Carmichael λ function [1]. Since , by hypothesis, $\Lambda \mid n-1$, from (4.18) the theorem is proved. Q.E.D.

The smallest Carmichael number of the above type which is also a 1-F.Psp. is $s_{44}(1) = 252{,}601 = 41 \cdot 61 \cdot 101$, while the absolutely smallest Carmichael number which is also a 1-F.Psp. is $s_2(1) = 2{,}465 = 5 \cdot 17 \cdot 29$.

Now, let us state some theorems concerning the case $m \geq 1$.

THEOREM 5: If $p \geq 5$ is a prime such that Δ^2 is not divisible by p, then

$$V_{U_p} \equiv m \pmod{U_p}.$$

Proof: On the basis of the periodicity of the sequence $\{ U_n \}$ reduced modulo 4 [6], it can be readily proved that, if $p \geq 5$, then U_p has the form $4h+1$ ($h \in N$). Since we have [12] $U_p \equiv \pm 1 \pmod{p}$ (except for the case $\Delta^2 \equiv 0 \pmod{p}$ which implies $U_p \equiv 0 \pmod{p}$), we can write $U_p = 4h + 1 \equiv \pm 1 \pmod{p}$.

Case 1: $U_p = 4h + 1 \equiv 1 \pmod{p}$

We have $2h \equiv 0 \pmod{p}$ and, since [12] $U_n \mid U_{kn}$,

$$U_{2h} \equiv 0 \pmod{U_p}. \tag{4.19}$$

By using the identity

$$V_{4h+1} - m = \Delta^2 U_{2h} U_{2h+1} \tag{4.20}$$

easily obtainable with the aid of (1.3) and (1.4), we have

$$V_{U_p} - m = V_{4h+1} - m = \Delta^2 U_{2h} U_{2h+1} \tag{4.21}$$

whence, by (4.19)

$$V_{U_p} - m \equiv \Delta^2 \cdot 0 \cdot U_{2h+1} \equiv 0 \pmod{U_p}.$$

Case 2: $U_p = 4h + 1 \equiv -1 \pmod{p}$

The proof is analogous to that of Case 1 and is omitted for brevity. Q.E.D.

It must be noted that, for $m = 1$ and $p = 5$, the statement of Theor.5 is true even though $\Delta^2 = 5 \equiv 0 \pmod 5$. In fact, we have

$$L_{F_5} = L_5 = 11 \equiv 1 \pmod{F_5}.$$

COROLLARY 6: If $p \geq 5$ is a prime, Δ^2 is not divisible by p and U_p (necessarily odd) is composite, then $U_p \in S_m$.

COROLLARY 7: If p is a prime and F_p is composite, then $F_p \in S_1$.

In order to prove the last theorem, we need to prove the following two lemmata.

LEMMA 2: $V_n(V_{2k+1}(m)) = V_{n(2k+1)}(m)$.

Proof: By (1.5) we have

$$\alpha_{V_{2k+1}(m)} = \{V_{2k+1}(m) + (V^2_{2k+1}(m) + 4)^{1/2}\} / 2. \tag{4.22}$$

Using (1.4), (4.22) becomes

$$\alpha_{V_{2k+1}(m)} = \{\alpha_m^{2k+1} + \beta_m^{2k+1} + (\alpha_m^{4k+2} + \beta_m^{4k+2} + 2)^{1/2}\} / 2$$

$$= \{\alpha_m^{2k+1} + \beta_m^{2k+1} + (\alpha_m^{2k+1} - \beta_m^{2k+1})\} / 2 = \alpha_m^{2k+1}. \tag{4.23}$$

Analogously, it is seen that

$$\beta_{V_{2k+1}(m)} = \beta_m^{2k+1}. \tag{4.24}$$

The statement of the lemma follows directly from (4.23), (4.24) and (1.4). Q.E.D.

LEMMA 3: If $h \in N$ and $n \in S_m$, then $V_{hn}(m) \equiv V_h(m) \pmod{n}$.

Proof: Let us rewrite the result established in [13, Cor. 7] as

$$V_{hn}(m) = \sum_{i=0}^{[h/2]} C_{h,i} V_n^{h-2i}(m) \qquad (n \text{ odd}). \tag{4.25}$$

By hypothesis, (4.25) and (1.6), we can write

$$V_{hn}(m) = \sum_{i=0}^{[h/2]} C_{h,i} V_n^{h-2i}(m) \equiv \sum_{i=0}^{[h/2]} C_{h,i} m^{h-2i} = V_h(m) \pmod{n}. \qquad \text{Q.E.D.}$$

THEOREM 6: If an odd composite n passes the m^{th} test, then it passes also the $V_{2k+1}(m)^{\text{th}}$ tests ($k = 1, 2, \ldots$).

Proof: From Lemma 2, Lemma 3 can read : If $V_n(m) \equiv m \pmod{n}$, then $V_n(V_{2k+1}(m)) = V_{n(2k+1)}(m) \equiv V_{2k+1}(m) \pmod{n}$. Q.E.D.

As particular cases, we see that

- if n passes the 1st test ($m = 1$), then it passes also the tests for $m = 4, 11, 29, 76, 199, 521, 1364, \ldots$
- if n passes the 2nd test ($m = 2$), then it passes also for $m = 14, 82, 478, 2786, \ldots$
- if n passes the 3rd test ($m = 3$), then it passes also for $m = 36, 393, 4287, 46764, \ldots$
- if n passes the 4th test ($m = 4$), then it passes also for $m = 76, 1364, \ldots$ (cf. the tests passed for $m = 1$) .

5. Conclusion

Public-key cryptosystems make use of primes having approximately 100 digits, so we wish to conclude this paper with two questions.

Pessimist's question : "Do odd composites $n \leq 10^{100}$ exist which are m-F.Psps. for all values of $m \leq n - 1$?"

If such numbers exist, they will never reveal their compositeness under our test.

Optimist's question : "Let M^* be the maximum number of consecutive tests ($m = 1, 2, \ldots, M^*$) passed by any odd composite $n \leq 10^{100}$. Is M^* comparatively small (say $M^* \leq 50$)?

If the answer is in affirmative, then the method proposed in Sec.3 can readily find primes for cryptographic purposes. The calculation time is slightly less than that

required by the method proposed by Solovay & Strassen [14] for finding numbers that are prime with probability greater than or equal to $1 - 1/2^{M^*}$.

The authors offer a prize of 50,000 Italian Lire to the first person who communicates to them an odd composite (below 10^{100}) which is an m-F.Psp. for m = 1, 2, ... , 8. Of course, at least one of its factors is also requested. A decuple prize is offered to the first person who sends to them a proof that no such number exists.

A table of 1-F.Psps to 10^8 was compiled by the authors. It will be sent, free of charges, upon request.

References

[1] H.Riesel, *Prime Numbers and Computer Methods for Factorization* . Boston: Birkhäuser Inc., 1985.

[2] M.Bicknell, "A Primer on the Pell Sequence and Related Sequences", *The Fibonacci Quarterly* , vol.13, pp. 345-349, no.4, 1975.

[3] O.Brugia, P.Filipponi, "Waring Formulae and Certain Combinatorial Identities", Fondaz. Ugo Bordoni Techn. Rep. 3B5986, Oct. 1986.

[4] A.Di Porto, P.Filipponi, "More on the Fibonacci Pseudoprimes", Fondaz.Ugo Bordoni Techn. Rep. 3t0687, May 1987. *The Fibonacci Quarterly* (to appear).

[5] A.Di Porto, P.Filipponi, "Un Metodo di Prova di Primalità Basato sulle Proprietà dei Numeri di Lucas Generalizzati", Proc. of the Primo Simposio Nazionale su: *Stato e Prospettive della Ricerca Crittografica in Italia* , Roma, Oct. 1987, pp. 141-146.

[6] Bro. A.Brousseau, *An Introduction to Fibonacci Discovery* . Santa Clara (Cal.): The Fibonacci Association, 1965.

[7] L.Carlitz, "A Note on Fibonacci Numbers", *The Fibonacci Quarterly*, vol. 2, pp. 15-28, no.1, 1964.

[8] D.Jarden, *Recurring Sequences*, 3rd ed., Jerusalem : Riveon Lematematika, 1973.

[9] V.E.Hoggatt, Jr., M.Bicknell, "Some Congruences of the Fibonacci Numbers Modulo a Prime P ", *Math. Magazine* , vol. 47, pp. 210-214, no.3, 1974.

[10] V.E.Hoggatt, Jr., *Fibonacci and Lucas Numbers*, Boston: Houghton Mifflin Co., 1969.

[11] V.E.Hoggatt, Jr., G.E.Bergum, "Divisibility and Congruence Relations", *The Fibonacci Quarterly* , vol. 12, pp. 189-195, no. 2, 1974.

[12] P.Filipponi:"On the Divisibility of Certain Generalized Fibonacci Numbers by Their Subscripts", Proc. *XIII Congresso Unione Matematica Italiana*, Torino, Sept. 1987, Sezione VII-18.

[13] Jin-Zai Lee, Jia-Sheng Lee, "Some Properties of the Sequence $\{W_n(a, b ; p, q)\}$", *The Fibonacci Quarterly* , vol. 25, pp. 268-278, 283, no. 3, 1987.

[14] R.Solovay, V.Strassen, "A Fast Monte-Carlo Test for Primality", *SIAM Journal on Comput.*, vol. 6, pp. 84-85, no.1, 1977.