GENERATING M-STRONG FIBONACCI PSEUDOPRIMES

Adina Di Porto and Piero Filipponi
Fondazione Ugo Bordoni, Via B. Castiglione, 59, I-00142 Roma, Italy
(Submitted January 1991)

1. Introduction and Generalities

One of the most important problems to be faced when using public-key cryptosystems (see [7] for background material) is to generate a large number of large ($\geq 10^{100}$) prime numbers. This hard to handle problem has been elegantly by-passed by submitting randomly generated odd integers n (which are, of course, of unknown nature) to one or more *probabilistic primality tests*. If n fails a test, then it is *surely* composite, whereas, if n passes the tests, then it is said to be a *probable prime* and is accepted as a prime. More precisely, the term "probable prime" stands for prime number candidates until their primality (or compositeness) has been established [6, p. 92].

In [2] we proposed a simple method for finding large probable primes. To make this paper self-contained, we recall briefly both this method and the definitions given in [2] and [3] of which this paper is an extension.

Let the generalized Lucas numbers $V_n(m)$ (or simply V_n) be defined as

$$(1.1) \qquad V_n = \alpha^n + \beta^n,$$

where

$$(1.2) \qquad \begin{cases} \alpha = -1/\beta = (m + \Delta)/2 \\ \Delta = (m^2 + 4)^{1/2}. \end{cases}$$

It is known (e.g., see [2]) that the congruence

$$(1.3) \qquad V_n \equiv m \pmod{n}$$

holds if n is prime. In [2] we analyzed some properties of the *m-Fibonacci Pseudoprimes* (m-F.Psps.), defined as the *odd* composites satisfying (1.3) for a given value of m, and proposed to accept an integer n of unknown nature as a prime if (1.3) is fulfilled for $m = 1, 2, \ldots, M$, where M is an integer somehow depending on the order of magnitude of n.

The above mentioned method is rather efficient from the point of view of the amount of calculations involved but traps are laid for it by the existence of *M-strong Fibonacci Pseudoprimes* (M-sF.Psps.) defined in [3] as the odd composites n which satisfy (1.3) for $1 \leq m \leq M$.

A correct use of this method for cryptographic purposes would imply the knowledge of the largest M for which at least one M-sF.Psp. exists below a given limit (say, 10^{100}). An attempt in this direction is made by the authors in this paper (see also [3]) by finding formulas for generating M-sF.Psps. for arbitrarily large M (section 3). In section 4 some numerical results are presented from which we could get the hang of the order of magnitude of such largest value of M.

2. Preliminaries

Let us rewrite the quantity Δ [cf. (1.2)] as

$$(2.1) \qquad \Delta = \Big(\prod_j 2^d p_j^{a_j}\Big)^{1/2} = \prod_j 2^s p_j^{b_j} \Big(\prod_j 2^r p_j^{c_j}\Big)^{1/2} \; (d \in \{0, 2, 3\};\ r,\ c_j \in \{0, 1\}),$$

where p_j are distinct odd primes. Both the power to which they are raised in the canonical decomposition of Δ^2 and the value of d depend, obviously, on m.

First, we state the following lemmas.

Lemma 1: p_j is of the form $4k + 1$ ($k \in \mathbb{N} = \{1, 2, \ldots\}$) for any j (and m).

Proof (reductio ad absurdum): Let us assume that the congruence

(2.2) $\quad \Delta^2 = m^2 + 4 \equiv 0 \pmod{4k + 3}$,

where $4k + 3$ is a prime, holds. The congruence (2.2) implies that $m^2 \equiv -4 \pmod{4k + 3}$, that is, it implies that -4 is a quadratic residue modulo $4k + 3$. Now, by using the properties of the Legendre symbol, we have

$$\left(\frac{-4}{4k + 3}\right) = \left(\frac{(-1)4}{4k + 3}\right) = \left(\frac{-1}{4k + 3}\right)\left(\frac{2^2}{4k + 3}\right) = (-1)^{(4k+2)/2} \cdot 1 = -1,$$

which contradicts the assumption. Q.E.D.

Lemma 2: p_j is a quadratic residue modulo any prime of the form $kp_j + 1$.

Proof: From Lemma 1 and [4, Th. 99, p. 76], we can write

$$\left(\frac{p_j}{kp_j + 1}\right) = \left(\frac{kp_j + 1}{p_j}\right) = \left(\frac{1}{p_j}\right) = 1. \quad \text{Q.E.D.}$$

Then, let us state the following

Theorem 1: Let q_i be odd rational primes such that [cf. (2.1)]

(2.3) $\quad q_i \equiv 1 \left(\bmod\ 8^r \prod_j p_j^{c_j}\right)$

and let

(2.4) $\quad n = \prod_i q_i^a \quad (a \in \{0, 1\})$

be an odd (square-free) composite. Moreover, define $\Lambda(n)$ as

(2.5) $\quad \Lambda(n) = \operatorname{lcm}(q_i - 1)_i$.

If $n - 1 \equiv 0 \pmod{\Lambda(n)}$, then $V_n \equiv m \pmod{n}$, that is n is an m-F.Psp.

Proof: By considering congruences defined over quadratic fields [4, Ch. XII], from the definition of α and (2.1) we have

$$2\alpha = m + \prod_j 2^s p_j^{b_j}\left(\prod_j 2^r p_j^{c_j}\right)^{1/2}$$

whence, due to the primality of q_i, the congruence

(2.6) $\quad (2\alpha)^{q_i} = 2^{q_i}\alpha^{q_i} \equiv m^{q_i} + \left(\prod_j 2^s p_j^{b_j}\right)^{q_i}\left(\prod_j 2^r p_j^{c_j}\right)^{q_i/2} \pmod{q_i}$

can be written. By using Fermat's little theorem, (2.6) becomes

(2.7) $\quad 2\alpha^{q_i} \equiv m + \prod_j 2^s p_j^{b_j}\left(\prod_j 2^r p_j^{c_j}\right)^{(q_i-1)/2}\left(\prod_j 2^r p_j^{c_j}\right)^{1/2} \pmod{q_i}$.

From (2.3), Lemma 2, and [4, Th. 95, p. 75], (2.7) can be rewritten as

$$2\alpha^{q_i} \equiv m + \prod_j 2^s p_j^{b_j}\left(\prod_j 2^r p_j^{c_j}\right)^{1/2} = 2\alpha \pmod{q_i},$$

whence, we have

(2.8) $\quad \alpha^{q_i} \equiv \alpha \pmod{q_i}, \qquad \alpha^{q_i - 1} \equiv 1 \pmod{q_i}$.

By hypothesis [i.e., $n - 1 \equiv 0 \pmod{q_i - 1}$] and (2.8), we have

$$\alpha^{n-1} \equiv 1 \pmod{q_i}$$

and, consequently,

$$\alpha^{n-1} \equiv 1 \left(\bmod \prod_i q_i\right) \quad (\text{i.e., mod } n),$$

whence

(2.9) $\alpha^n \equiv \alpha \pmod{n}$.

Analogously, it can be proved that

(2.10) $\beta^n \equiv \beta \pmod{n}$.

Finally, from (2.9) and (2.10) we have

$$V_n(m) = \alpha^n + \beta^n \equiv \alpha + \beta = m \pmod{n}. \quad \text{Q.E.D.}$$

3. Generating M-sF.Psps.

In this section a simple method for generating M-sF.Psps., which are also Carmichael numbers, is discussed.

Let us consider any expression [5, p. 99] of the form

$$(3.1) \quad n(T) = \prod_{i=1}^{h}(k_i T + 1) = \prod_{i=1}^{h} P_i \quad (h \geq 3;\ k_i,\ T \in \mathbb{N})$$

which gives Carmichael numbers $n(T)$ for all values of T such that P_i ($i = 1, 2, \ldots, h$) is prime.

For $n(T)$ to be an m-F.Psp. by Theorem 1, we must impose that

$$(3.2) \quad P_i \equiv 1 \left(\bmod\ 8^r \prod_j p_j(m)\right) \quad (i = 1, 2, \ldots, h),$$

where [cf. (2.1)] the primes $p_j(m)$ (with $c_j = 1$) are all distinct *odd* primes which appear in the canonical decomposition of $m^2 + 4$ raised to an *odd power* and $r = 1$ (0) if $d = 3$ ($\neq 3$), that is, if $m - 2$ is (is not) divisible by 4.

Due to the particular structure of the factors P_i, (3.2) can be fulfilled by simply imposing that

$$(3.3) \quad T = 8^r \prod_j p_j(m) t \quad (t \in \mathbb{N})$$

so that

$$(3.4) \quad n(t) = \prod_{i=1}^{h} P_i = \prod_{i=1}^{h}\left(k_i 8^r \prod_j p_j(m) t + 1\right).$$

Recalling that the congruence $n(t) - 1 \equiv 0 \pmod{\mathrm{lcm}(P_i - 1)_i}$ holds by construction, Theorem 1 ensures that $n(t)$ is an m-F.Psp. (and a Carmichael number) for all values of t such that P_i is prime ($i = 1, 2, \ldots, h$).

Now, it is clear that if we wish to construct an M-sF.Psp. ($M \geq 2$), we must simply multiply $8k_i$ by the least common multiple of all distinct primes $p_j(m)$ ($m = 1, 2, \ldots, M$).

$$(3.6) \quad C_M = \mathrm{lcm}(p_j(m))_{j,\ 1 \leq m \leq M}$$

thus, getting the number

$$(3.7) \quad n_M(t) = \prod_{i=1}^{h}(8C_M k_i t + 1)$$

which is an M-sF.Psp. (and a Carmichael number) for all values of t such that all the h factors in the product (3.7) are prime.

An Important Remark: An M-sF.Psp. constructed by using the above method may be an $(M + a)$-sF.Psp. ($a \geq 1$) as well. For this to happen (see also [2, Th. 6]) it suffices that either

$$(3.8) \quad C_{M+a} = C_M$$

or

$$(3.9) \quad t_0 \equiv 0 \pmod{\mathrm{lcm}(p_j(m))_{j,\ M+1 \leq m \leq M+a}},$$

where t_0 is any value of t such that [cf. (3.7)] $8C_M k_i t + 1$ is prime ($i = 1, 2, \ldots, h$).

It should be noted that a so-obtained M-sF.Psp. may be an $(M + a)$-sF.Psp. even though (3.8) and/or (3.9) are not satisfied. This fact will be investigated in a further work. Some numerical examples of the said occurrences will be shown in section 4.

4. Numerical Results

Some simple expressions of the form (3.1) are

(4.1) $\quad n(T) = (6T + 1)(12T + 1)(18T + 1),$

(4.2) $\quad n'(T) = n(T)(36T + 1),$

(4.3) $\quad n''(T) = (12T + 1)(24T + 1)(36T + 1)(72T + 1)(144T + 1).$

A computer experiment to find M-sF.Psps. was carried out on the basis of the simplest among them [namely, (4.1)] which was discovered by Chernick [6] in 1939.

According to the procedure discussed in section 3 [cf. (3.7)], we see that, since for $m = 1$ we have $\Delta = \sqrt{5}$, the numbers

(4.4) $$n_2(t) = (5 \cdot 8 \cdot 6t + 1)(5 \cdot 8 \cdot 12t + 1)(5 \cdot 8 \cdot 18t + 1)$$
$$= (240t + 1)(480t + 1)(720t + 1)$$

are 2-sF.Psps. (and Carmichael numbers) for all values of t such that all three factors on the right-hand side of (4.4) are prime. The smallest among them is $n_2(20) = 663{,}805{,}468{,}801$.

Following this procedure, we sought numbers $n_M(t)$ ($M = 3, 4, \ldots$) which are M-sF.Psps. not exceeding 10^{100}.

The number of digits (#d) of the smallest M-F.Psps. found in this way is shown against M in Table 1.

Table 1

M	#d	M	#d	M	#d
		10	29	29	76
1	8	11	29	21	61
2	12	12	36	22	61
3	16	13	45	23	61
4	16	14	45	24	61
5	18	15	51	25	61
6	18	16	51	26	61
7	29	17	51	27	95
8	29	18	65	28	98
9	29	19	71	29	98

By means of our experiment we could not find any 30-sF.Psp. below 10^{100}.

Just as an illustration, and for the delight of lovers of large numbers, we show the smallest (98 digits) 29-sF.Psp. found by us:

41,703,652,779,296,795,260,673,920,462,490,602,986,625,330,278,308,
957,565,652,181,464,065,185,928,126,878,406,976,583,823,233,761.

This remarkable number is, as previously mentioned, also a Carmichael number. Its canonical factorization (three 33-digit prime factors) is available upon request. This number [namely, $n_{28}(23)$] has been constructed to be a 28-sF.Psp. [see An Important Remark above and paragraph (vi) of the Remark below). The authors would be deeply grateful to anyone bringing to their knowledge a 29-sF.Psp. smaller than $n_{23}(23)$ and/or a 30-sF.Psp. < 10^{100}.

Remark: It must be noted that (cf. Table 1), due to the fulfillment of (3.8),

(i) the numbers $n_3(t)$ [cf. (3.7)] which are 3-sF.Psps. are 4-sF.Psps. as well,

(ii) the numbers $n_5(t)$ which are 5-sF.Psps. are 6-sF.Psps. as well,

(iii) the numbers $n_8(t)$ which are 8-sF.Psps. are 11-sF.Psps. as well,

(iv) the numbers $n_{15}(t)$ which are 15-sF.Psps. are 16-sF.Psps. as well,

(v) the numbers $n_{22}(t)$ which are 22-sF.Psps. are 26-sF.Psps. as well,

(vi) the numbers $n_{28}(t)$ which are 28-sF.Psps. are 29-sF.Psps. as well.

Moreover, due to the fulfillment of (3.9), the smallest $n_{21}(t)$ which is a 21-sF.Psp. [namely, $n_{21}(488)$] is a 22-sF.Psp. Therefore, by (v), it is a 26-sF.Psp. as well.

Finally, the smallest $n_{15}(t)$ which is a 15-sF.Psp. [and, by (iv), a 16-sF.-Psp.] is, rather surprisingly, a 17-sF.Psp. This number [namely, $n_{15}(378)$] has 51 digits and is the smallest 17-sF.Psp. with which we are acquainted.

Acknowledgment

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

Addendum

Professor W. Müller (Universität Klagenfurt, Austria) communicated to us that on March 30, 1992, Dr. R. Pinch (University of Cambridge, UK) proved the existence of the ∞-sF.Psps. These *exceptional* numbers satisfy the congruence (1.3) for *all* values of the parameter m. The smallest among them is

$$443372888629441 = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331.$$

References

1. J. Chernick. "On Fermat's Simple Theorem." *Bull. Amer. Math. Soc.* 45 (1939): 269-74.
2. A. Di Porto & P. Filipponi. "A Probabilistic Primality Test Based on the Properties of Certain Generalized Lucas Numbers." *Lecture Notes on Computer Science 330*, pp. 211-23. Berlin: Springer-Verlag, 1988.
3. A. Di Porto, P. Filipponi, & E. Montolivo. "On the Generalized Fibonacci Pseudoprimes." *Fibonacci Quarterly 28.4* (1990):347-54.
4. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers.* 2nd ed. Oxford: Clarendon Press, 1945.
5. P. Ribenboim. *The Book of Prime Number Records.* New York: Springer-Verlag, 1988.
6. H. Riesel. *Prime Numbers and Computer Methods for Factorization.* Boston: Birkäuser, 1985.
7. R. L. Rivest, A. Shamir, & L. Adleman. "A Method for Obtaining Digital Signature and Public-Key Cryptosystems." *Comm. ACM 21.2* (1978):120-26.

AMS Classification numbers: 11A51, 11A07. 11B39

*****