References

1. P. R. J. Asveld. "A Family of Fibonacci-Like Sequences." *Fibonacci Quarterly* *25.1* (1987):81-83.
2. J. C. Turner. "Convolution Trees and Pascal-T Triangles." *Fibonacci Quarterly* (to appear).

*****

MORE ON THE FIBONACCI PSEUDOPRIMES

Adina Di Porto and Piero Filipponi
Fondazione Ugo Bordoni, Roma, Italy
(Submitted May 1987)

1. Generalities

The idea of writing this note was triggered by the necessity that occurred in the course of our research job, of expressing the quantity $x^n + y^n$ (x and y arbitrary quantities, n a nonnegative integer) in terms of powers of xy and $x + y$. Such expressions, commonly referred to as *Waring formulae*, are given in high school books and others (e.g., see [1]) only for the first few values of n, namely

$$\begin{cases} x^0 + y^0 = 2 \\ x^1 + y^1 = x + y \\ x^2 + y^2 = (x + y)^2 - 2xy \\ x^3 + y^3 = (x + y)^3 - 3xy(x + y) \\ x^4 + y^4 = (x + y)^4 - 4xy(x + y)^2 + 2(xy)^2. \end{cases} \tag{1.1}$$

Without claiming the novelty of the result, we found (see [2]) the following general expression

$$x^n + y^n = \sum_{k=0}^{[n/2]} (-1)^k C_{n,k} (xy)^k (x + y)^{n-2k}, \tag{1.2}$$

where

$$\begin{cases} C_{0,0} = 2 \\ C_{n,k} = \dfrac{n}{n - k}\dbinom{n - k}{k} = nB_{n,k} \quad (n \ge 1) \end{cases} \tag{1.3}$$

and $[a]$ denotes the greatest integer not exceeding a.

Several interesting combinatorial and trigonometrical identities emerge (see [2]) from certain choices of x and y in (1.2). In particular, sensing Lucas numbers L_n on the left-hand side of (1.2) is quite natural for a Fibonacci fan. In fact, replacing x and y by $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$, respectively, we get

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

$$L_n = \sum_{k=0}^{[n/2]} C_{n,k} \quad (n \geq 0), \tag{1.4}$$

that is

$$L_n = 1 + nS_n \quad (n \geq 1), \tag{1.5}$$

where

$$S_n = \sum_{k=1}^{[n/2]} \frac{1}{n-k}\binom{n-k}{k} = \sum_{k=1}^{[n/2]} B_{n,k}. \tag{1.6}$$

We point out that the equality (1.5) can also be obtained using the relationships (see [3], [4])

$$L_n = F_{n-1} + F_{n+1} \tag{1.7}$$

$$F_{n+1} = \sum_{k=0}^{[n/2]} \binom{n-k}{k}, \tag{1.8}$$

where F_n stands for the n^{th} Fibonacci number.

Observing (1.5), the following question arises spontaneously:

"When is the congruence

$$L_n \equiv 1 \pmod{n} \quad (n > 1) \tag{1.9}$$

verified?"

The obvious answer is:

"The congruence (1.9) holds iff S_n is integral."

Theorem 1: If n is relatively prime to k $(1 \leq k \leq [n/2])$, then $B_{n,k}$ is a positive integer.

Proof: The statement holds clearly for $k = 1$. Consequently, let us consider the case $2 \leq k \leq [n/2]$. Letting

$$P_{n,k} = \prod_{j=1}^{k-1} (n - k - j), \tag{1.10}$$

it suffices to prove that, if n is relatively prime to k, then $P_{n,k}/k!$ is integral. It is known [5] that

$$P_{n,k} \equiv 0 \pmod{(k-1)!},$$

that is,

$$A_{n,k} = P_{n,k}/(k-1)! \tag{1.11}$$

is an integer. Again, from [5] we have

$$(n-k)P_{n,k} \equiv 0 \pmod{k!} \tag{1.12}$$

whence, dividing both the two sides and the modulus by $(k-1)!$, we can write

$$(n-k)A_{n,k} \equiv 0 \pmod{k}, \tag{1.13}$$

see [6, Ch. 3., Sec. 3(b)]. If n is relatively prime to k, from (1.13) it follows that

$$n - k \not\equiv 0 \pmod{k}, \tag{1.14}$$

$$A_{n,k} \equiv 0 \pmod{k}. \tag{1.15}$$

From (1.15) and (1.11), it appears that, if n is relatively prime to k, then

$$P_{n,k} \equiv 0 \pmod{k!}. \quad \text{Q.E.D.}$$

From Theorem 1 it follows that, if n is prime, all addends $B_{n,k}$, cf. (1.6), are integral. Therefore, S_n is integral. This is a further proof of the well-known result (see [7])

$$L_n \equiv 1 \pmod{n} \quad (\text{if } n \text{ is a prime}). \tag{1.16}$$

2. On the Fibonacci Pseudoprimes

The sum S_n can be integral also if n is not a prime. In particular, this sum can also be integral if two or more of its addends $B_{n,k}$ are not integral. The composite numbers n which satisfy this property, i.e., for which congruence (1.9) holds, are called *Fibonacci Pseudoprimes* (see [8]), which we abbreviate *F.Psps.* and denote by Q_k ($k = 1, 2, \ldots$).

Proposition 1: A composite number n is a F.Psp. iff S_n is integral.

The smallest F.Psp. is $Q_1 = 705$. It was discovered by M. Pettet in 1966 [9] who discovered also $Q_2 = 2465$ and $Q_3 = 2737$, but we cannot forget the unbelievable misfortune of D. Lind [10] who in 1967 limited his computer experiment for disproving the converse of (1.6) to $n = 700$, thus missing the mark by a hair's breadth. In the early 1970s, J. Greener (Lawrence Livermore Lab.) discovered Q_4 and Q_5 [7]. To the best of our knowledge, the F.Psps. are known up to $Q_7 = 6721$. The discovery of Q_6 and Q_7 is due to G. Logothetis [8].

Curiosity led us to discover many more F.Psps. Using the facilities of the Istituto Superiore P.T. (the Italian Telecommunication Ministry), a weighty computer experiment was carried out to find all F.Psps. within the interval $[2, 10^6]$. They are shown in Table 1 together with their canonical factorization. The computational algorithm is outlined in Section 3, where a worked example is also appended.

Inspection of Table 1 suggests some considerations on the basis of which we state several propositions and theorems. Most of them show that certain classes of integers are not F.Psps., thus extending the results established in [8, Sec. 6]. Some conjectures can also be formulated.

Consideration 1: No even F.Psps. occur in Table 1.

Proposition 2:

(i) $L_{6n} \not\equiv 1 \pmod{6n}$

(ii) $L_{6n+2} \not\equiv 1 \pmod{6n+2}$ (n odd)

(iii) $L_{6n+4} \not\equiv 1 \pmod{6n+4}$ (n even)

Proof:

(i) The congruence $L_{6n} \equiv 0 \pmod{2}$ implies that $6n \nmid L_{6n} - 1$.

(ii) Using the identities [11, formula (11)] and I_{23}, I_{22} (from [3]), it can be proved that

$$(L_{6n+2} - 1)/2 = F_{6n+2} + \sum_{k=1}^{2n-1} F_{3k}. \tag{2.1}$$

Since $F_{3k} \equiv 0 \pmod{2}$ and $F_{6n+2} \equiv 1 \pmod{2}$, the quantity on the left-hand side of (2.1) is clearly odd, that is,

$$L_{6n+2} - 1 \not\equiv 0 \pmod{4}.$$

Since, for n odd, the congruence $6n + 2 \equiv 0 \pmod 4$ holds, it follows that

$$6n + 2 \nmid L_{6n+2} - 1 \quad (n \text{ odd}).$$

(iii) The proof is similar to that of (ii) and is omitted for brevity. Q.E.D.

TABLE 1

Q_{1} =	705 = 3 · 5 · 47	Q_{44} =	252601 = 41 · 61 · 101
Q_{2} =	2465 = 5 · 17 · 29	Q_{45} =	254321 = 263 · 967
Q_{3} =	2737 = 7 · 17 · 23	Q_{46} =	257761 = 7 · 23 · 1601
Q_{4} =	3745 = 5 · 7 · 107	Q_{47} =	268801 = 13 · 23 · 29 · 31
Q_{5} =	4181 = 37 · 113	Q_{48} =	272611 = 131 · 2081
Q_{6} =	5777 = 53 · 109	Q_{49} =	283361 = 13 · 71 · 307
Q_{7} =	6721 = 11 · 13 · 47	Q_{50} =	302101 = 317 · 953
Q_{8} =	10877 = 73 · 149	Q_{51} =	303101 = 101 · 3001
Q_{9} =	13201 = 43 · 307	Q_{52} =	327313 = 7 · 19 · 23 · 107
Q_{10} =	15251 = 101 · 151	Q_{53} =	330929 = 149 · 2221
Q_{11} =	24465 = 3 · 5 · 7 · 233	Q_{54} =	399001 = 31 · 61 · 211
Q_{12} =	29281 = 7 · 47 · 89	Q_{55} =	430127 = 463 · 929
Q_{13} =	34561 = 17 · 19 · 107	Q_{56} =	433621 = 199 · 2179
Q_{14} =	35785 = 5 · 17 · 421	Q_{57} =	438751 = 541 · 811
Q_{15} =	51841 = 47 · 1103	Q_{58} =	447145 = 5 · 37 · 2417
Q_{16} =	54705 = 3 · 5 · 7 · 521	Q_{59} =	455961 = 3 · 11 · 41 · 337
Q_{17} =	64079 = 139 · 461	Q_{60} =	489601 = 7 · 23 · 3041
Q_{18} =	64681 = 71 · 911	Q_{61} =	490841 = 13 · 17 · 2221
Q_{19} =	67861 = 79 · 859	Q_{62} =	497761 = 11 · 37 · 1223
Q_{20} =	68251 = 131 · 521	Q_{63} =	512461 = 31 · 61 · 271
Q_{21} =	75077 = 193 · 389	Q_{64} =	520801 = 241 · 2161
Q_{22} =	80189 = 17 · 53 · 89	Q_{65} =	530611 = 461 · 1151
Q_{23} =	90061 = 113 · 797	Q_{66} =	556421 = 431 · 1291
Q_{24} =	96049 = 139 · 691	Q_{67} =	597793 = 7 · 23 · 47 · 79
Q_{25} =	97921 = 181 · 541	Q_{68} =	618449 = 13 · 113 · 421
Q_{26} =	100065 = 3 · 5 · 7 · 953	Q_{69} =	635627 = 563 · 1129
Q_{27} =	100127 = 223 · 449	Q_{70} =	636641 = 461 · 1381
Q_{28} =	105281 = 11 · 17 · 563	Q_{71} =	638189 = 619 · 1031
Q_{29} =	113573 = 137 · 829	Q_{72} =	639539 = 43 · 107 · 139
Q_{30} =	118441 = 83 · 1427	Q_{73} =	655201 = 23 · 61 · 467
Q_{31} =	146611 = 271 · 541	Q_{74} =	667589 = 13 · 89 · 577
Q_{32} =	161027 = 283 · 569	Q_{75} =	687169 = 7 · 89 · 1103
Q_{33} =	162133 = 73 · 2221	Q_{76} =	697137 = 3 · 7 · 89 · 373
Q_{34} =	163081 = 17 · 53 · 181	Q_{77} =	722261 = 491 · 1471
Q_{35} =	179697 = 3 · 7 · 43 · 199	Q_{78} =	741751 = 431 · 1721
Q_{36} =	186961 = 31 · 37 · 163	Q_{79} =	851927 = 881 · 967
Q_{37} =	194833 = 23 · 43 · 197	Q_{80} =	852841 = 11 · 31 · 41 · 61
Q_{38} =	197209 = 199 · 991	Q_{81} =	853469 = 239 · 3571
Q_{39} =	209665 = 5 · 19 · 2207	Q_{82} =	920577 = 3 · 7 · 59 · 743
Q_{40} =	219781 = 271 · 811	Q_{83} =	925681 = 23 · 167 · 241
Q_{41} =	228241 = 13 · 97 · 181	Q_{84} =	930097 = 7 · 23 · 53 · 109
Q_{42} =	229445 = 5 · 109 · 421	Q_{85} =	993345 = 3 · 5 · 47 · 1409
Q_{43} =	231703 = 263 · 881	Q_{86} =	999941 = 577 · 1733

It must be noted that the well-known result [7] $L_{2^k} \not\equiv 1 \pmod{2^k}$ $(k \geq 2)$ appears to be included in the incongruences (ii) and (iii).

Proposition 2 can be summarized by the following

Theorem 2: If n is even but $n \neq 2(6k \pm 1)$ $(k = 1, 2, \ldots)$, then n is not a F.Psp.

The set of integers of the form $2(6k \pm 1)$ contains all numbers that are twice a prime greater than 3.

Proposition 3: If $n = 2p$ is twice a prime and $1 \leq k \leq p - 1$, then the fractional part of $B_{n,k}$ is either 0 or 1/2.

The proof of Proposition 3 is based on the argument used in the proof of Theorem 1 and is omitted for brevity.

Since the last term of the sum S_{2p}, cf. (1.6), is $B_{2p,p} = 1/p$, from Proposition 3 it follows that the fractional part of this sum is either $1/p$ or $1/p + 1/2$. Noting that, in the particular case $p = 2$, the fractional part of S_4 is clearly 1/2, from Proposition 1 we have

Theorem 3: If n is twice a prime, then n is not a F.Psp.

On the other hand, the same result can be obtained using the congruence [7]

$$L_{kp} \equiv L_k \pmod{p} \quad (p \text{ a prime}) \tag{2.2}$$

whence we get $L_{2p} - 1 \equiv 2 \pmod{p}$, that is, $2p \nmid L_{2p} - 1$.

Now, let us consider the integers of the form $2(6k \pm 1)$ with $6k \pm 1$ composite and state the following

Theorem 4: If $n = 2(6k \pm 1)$ and $k \equiv \mp 1 \pmod 5$ (i.e., if n is even, divisible by 5 and not divisible by 3 and 4), then n is not a F.Psp.

Proof: The identity I_{17} [3] can be rewritten in the form

$$L_{2(2m\pm1)} - 1 = 5F^2_{2m\pm1} - 3$$

whence we obtain the congruence

$$L_{2(2m\pm1)} - 1 \equiv 2 \pmod 5, \tag{2.3}$$

which implies that $2(6k \pm 1) \nmid L_{2(6k\pm1)} - 1$ if $6k \pm 1 \equiv 0 \pmod 5$, that is, if $k \equiv \mp 1 \pmod 5$. Q.E.D.

Finally, we observe that there exist F.Psps. of the form $6k \pm 1$ with $k \not\equiv \mp 1 \pmod 5$ (e.g., $Q_{65} = 6 \cdot 88435 + 1$ and $Q_{66} = 6 \cdot 92737 - 1$) and state the following

Theorem 5: If $n = 2k + 1$ is a F.Psp., then $2n$ is not a F.Psp.

Proof (reductio ad absurdum): Let us suppose that

$$L_{2(2k+1)} = L_{4k+2} \equiv 1 \pmod{4k + 2}. \tag{2.4}$$

From identity I_{18} [3] and (2.4), we can write

$$L_{4k+2} - 2 \equiv -1 \equiv L^2_{2k+1} \pmod{4k + 2},$$

whence we obtain the congruence

$$L^2_{2k+1} \equiv -1 \pmod{2k + 1} \tag{2.5}$$

which contradicts the assumption. Q.E.D.

Consideration 1, together with Theorems 2, 3, 4, and 5, allows us to offer the following

Conjecture 1: F.Psps. are odd.

Consideration 2: The F.Psps. listed in Table 1 are given by the product of a certain number of distinct primes.

Using (2.2), one can readily prove the following

Theorem 6: If $p_1, p_2, \ldots, p_k$ are distinct odd primes, then $n = p_1 p_2 \ldots p_k$ is a F.Psp. iff $L_{n/p_i} \equiv 1 \pmod{p_i}$ $(i = 1, 2, \ldots, k)$.

For example, we see that

$$3 \cdot 5 \cdot 47 = Q_1 \Leftrightarrow \begin{cases} L_{15} \equiv 1 \pmod{47} \\ L_{141} \equiv 1 \pmod{5} \\ L_{235} \equiv 1 \pmod{3}. \end{cases}$$

On the basis of Theorem 6, we observe that, if p and q are distinct odd primes $(q > p)$, then

$$L_{pq} \equiv 1 \pmod{pq} \Leftrightarrow \begin{cases} L_p \equiv 1 \pmod{q} \\ L_q \equiv 1 \pmod{p} \end{cases} (q > p). \tag{2.6}$$

Now, the upper congruence on the right-hand side of (2.6) is clearly impossible for $p = 3, 5, 7, 11, 13$. It follows that $n = pq$ is not a F.Psp. for the above values of p. The smallest p such that $n = pq$ is a F.Psp. is $p = 37$.

In [8] the authors show that, for the conjecture $L_n \not\equiv 1 \pmod{n^2}$ $(n > 1)$, it follows that p^k (p a prime, $k > 1$) is not a F.Psp. We formulate the following

Conjecture 2: F.Psps. are square-free.

Consideration 3: The rightmost digits of the F.Psps. listed in Table 1 are not uniformly distributed.

The occurrence frequency $f(c)$ of the rightmost digit c of the F.Psps. within the interval $[2, 10^6]$ is shown in Table 2.

TABLE 2

c	$f(c)$
1	45
3	6
5	11
7	13
9	11

Moreover, it can be noted that, in the same interval, only 17% of the F.Psps. are of the form $4n + 3$. Hence, the F.Psps. congruent to 3 both modulo 4 and modulo 10 are supposedly *very rare*.

Consideration 4: The density of the F.Psps. less than n *shows a comparatively slow decrease as* n *increases, within the interval* $[2, 10^6]$.

Conjecture 3: There are infinitely many F.Psps.

Let $q(n)$ denote the number of F.Psps. smaller than or equal to a given positive integer n. Numerically, the F.Psp.-counting function $q(n)$ seems asymptotically related to the prime-counting function $\pi(n)$ (cf. [4, p. 204].

Conjecture 4: $q(n)$ is asymptotic to $\pi(\sqrt{n})/\alpha$.

The behaviors of $q(n)$ and $\hat{\pi}(\sqrt{n})/\alpha$ vs n are plotted in Figure 1 for $2 \le n \le 10^6$, $\hat{\pi}(x) = x/\ln x$ being the Gauss estimate of $\pi(x)$.

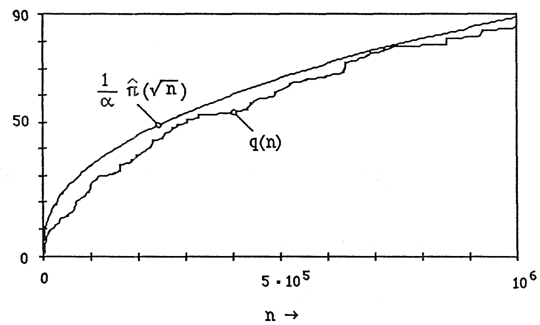

FIGURE 1

Behaviors of $q(n)$ and $\hat{\pi}(\sqrt{n})/\alpha$ vs n

We conclude this section by pointing out that, for a given odd prime p, it is possible to find out necessary (sufficient) conditions for $n = pk$ (k an integer greater than 2) to be (not to be) a F.Psp.

Hinging upon the periodicity of the Lucas sequence reduced modulo p (P being the period), we observe that

$$\begin{cases} L_n \equiv 1 \pmod 3 \text{ iff } n \equiv 1, 3, 4 \pmod 8 \\ L_n \equiv 1 \pmod 5 \text{ iff } n \equiv 1 \pmod 4 \\ L_n \equiv 1 \pmod 7 \text{ iff } n \equiv 1, 7 \pmod{16} \\ L_n \equiv 1 \pmod{11} \text{ iff } n \equiv 1 \pmod{10} \\ \vdots \\ L_n \equiv 1 \pmod p \text{ iff } n \equiv r_1, r_2, \ldots, r_s \pmod P. \end{cases} \tag{2.7}$$

It is readily seen that, if $n = pk \not\equiv r_1, r_2, \ldots, r_s \pmod P$, then $L_{pk} \not\equiv 1 \pmod p$ and *a fortiori* $L_{pk} \not\equiv 1 \pmod{pk}$, that is, $n = pk$ is not a F.Psp. As an example, solving some of the congruences (2.7) $pk \equiv r_1, r_2, \ldots, r_s \pmod P$ in k and taking into account that an even integer not of the form $2(6h \pm 1)$ (cf. Theorem 2) is not a F.Psp., lead to the statement of the following

Theorem 7: If either $n = 3k$ and $k \not\equiv 1, 3 \pmod 8$
or $n = 5k$ and $k \not\equiv 1 \pmod 4$
or $n = 7k$ and $k \not\equiv 1, 7 \pmod{16}$
or $n = 11k$ and $k \not\equiv 1 \pmod{10}$
or $n = 13k$ and $k \not\equiv 1, 13 \pmod{28}$
or $n = 17k$ and $k \not\equiv 1, 17 \pmod{36}$
or $n = 19k$ and $k \not\equiv 1 \pmod{18}$,
then n is not a F.Psp.

Denoting by $M_n = 2^n - 1$ the n^{th} *Mersenne number*, we can state the following corollary to Theorem 7.

Corollary 1: If $n = 2h$ and $h \geq 2$, then M_n is not a F.Psp.

Proof: Since $M_n = 2^{2h} - 1 \equiv 0 \pmod 3$ and $k = (2^{2h} - 1)/3 \equiv 5 \pmod 8$, the proof follows directly from the first statement of Theorem 7. Q.E.D.

Furthermore, considering the following classes of composite integers congruent to 3 modulo 10 (cf. Consideration 3 for $c = 3$):

$n_1 = 3(10k + 1) \quad (k = 1, 2, \ldots)$

$n_2 = 13(10k + 1) \quad (k = 1, 2, \ldots)$

$n_3 = 11(10k + 3) \quad (k = 0, 1, \ldots)$

$n_4 = 19(10k + 7) \quad (k = 0, 1, \ldots)$

$n_5 = 7(10k + 9) \quad (k = 0, 1, \ldots)$

$n_6 = 17(10k + 9) \quad (k = 0, 1, \ldots)$

the intersection of which is not empty, we can state the following further corollary to Theorem 7.

Corollary 2: If either $n = n_1$ and $k \not\equiv 0, 1 \pmod 4$
or $n = n_2$ and $k \not\equiv 0, 4 \pmod{14}$
or $n = n_3$
or $n = n_4$ and $k \not\equiv 3 \pmod 9$
or $n = n_5$ and $k \not\equiv 3, 4 \pmod 8$
or $n = n_6$ and $k \not\equiv 8, 10 \pmod{18}$,
then n is not a F.Psp.

3. A Computational Algorithm to Find L_n Reduced Modulo n

The algorithm described in the following finds the value of $\langle L_n \rangle_n$ (L_n reduced modulo n) after $[\log_2 n]$ recursive calculations. The values of n composite ($2 \le n \le 10^6$) for which $\langle L_n \rangle_n = 1$ correspond, obviously, to the F.Psps. Q_k shown in Table 1.

Step 1: Decompose n as a sum of powers of 2.

$$n = \sum_{i=0}^{m} a_i 2^i, \tag{3.1}$$

where $m = [\log_2 n]$ and a_i can assume either the value 0 or the value 1.

Step 2: Starting from the initial values

$$\begin{cases} L_{k_0} = L_1 = 1 \\ F_{k_0} = F_1 = 1, \end{cases} \tag{3.2}$$

calculate the pairs

$$(L_{k_i}, F_{k_i}) \quad (i = 1, 2, \ldots, m - 1) \tag{3.3}$$

where $k_0 = 1$ and

$$k_i = \begin{cases} 2k_{i-1} & \text{if } a_{m-i} = 0 \\ 2k_{i-1} + 1 & \text{if } a_{m-i} = 1. \end{cases} \tag{3.4}$$

The pairs (3.3) can be calculated, on the basis of the previously obtained values, using the identities

$$L_{2k} = L_k^2 + 2(-1)^{k-1}, \tag{3.5}$$

$$L_{2k+1} = L_k(5F_k + L_k)/2 + (-1)^{k-1}, \tag{3.6}$$

$$F_{2k} = F_k L_k, \tag{3.7}$$

and

$$F_{2k+1} = L_k(F_k + L_k)/2 + (-1)^{k-1}, \tag{3.8}$$

derived from identities I_7, I_8, I_{15}, I_{18}, and I_{32} [3].

Step 3: Calculate L_n using

$$L_n = \begin{cases} L_{2k_{m-1}} & \text{if } a_0 = 0 \\ L_{2k_{m-1}+1} & \text{if } a_0 = 1. \end{cases} \tag{3.9}$$

End.

The algorithm works modulo n throughout. We recall, cf. (3.6) and (3.8), that the multiplicative inverse of 2 modulo an odd n is $(n + 1)/2$.

As a practical example, the various steps to find $\langle L_n \rangle_n$ for $n = Q_{23} = 90061$ are shown in the following.

$$Q_{23} = 90061 = 2^{16} + 2^{14} + 2^{12} + 2^{11} + 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^3 + 2^2 + 2^0$$

$$m = 16$$

i	a_{m-i}	k_i	$\langle L_{k_i} \rangle_{Q_{23}}$	$\langle F_{k_i} \rangle_{Q_{23}}$
0	1	1	1	1
1	0	2	3	1
2	1	5	11	5
3	0	10	123	55
4	1	21	24476	10946
5	1	43	86547	30844
6	1	87	78960	73765
7	1	175	27806	89112
8	1	351	89985	90027
9	1	703	9349	4181
10	1	1407	26554	23164
11	0	2814	27349	70287
12	0	5628	11194	17179
13	1	11257	69119	26137
14	1	22515	59408	0
15	0	45030	90059	0
16	1	90061	1	-

4. Conclusions

We think that a thorough investigation of the behavior of the fractional part of the quantity $B_{n,k}$, cf. (1.6), as n and k vary could lead to the discovery of further properties of the F.Psps.

4.1. A practical application

If we could know *a priori* that an integer N is not a F.Psp., then the algorithm developed in Section 3 would ascertain the primality of N.

On the other hand, the proof of Conjecture 4 would suffice to make the above algorithm an efficient *probabilistic test* for the primality of large numbers. Besides being interesting *per se*, this algorithm could find an application in modern cryptography. Currently, probabilistic testing for the primality of large numbers (more than 100 digits) plays a relevant role in the so-called public-key cryptosystems [12]. The most widely used probabilistic test is the SS (Solovay & Strassen) test [13]. The computational complexity of a *single* step of this test is slightly greater than the complexity of our algorithm. Usually, 100 steps of the SS algorithm are required, thus assuring that N is prime with probability $p_1 = 1 - 1/2^{100} \approx 1 - 7.88 \cdot 10^{-31}$. If Conjecture 4 were proved, we could state that a sufficiently large number N satisfying the congruence $L_N \equiv 1 \pmod{N}$ is prime with probability $p_2 \approx 1 - 2/(\alpha\sqrt{N})$. It can be readily proved that, if N has more than 61 digits, $p_2 > p_1$. For example, if N is a 100-digit number, we have $p_2 \approx 1 - 3.9 \cdot 10^{-50}$.

4.2. A remark

We wish to conclude this section and the paper with a remark. It appears that $Q_5 = F_{19}$ and $Q_{17} = L_{23}$. We asked ourselves whether this fact has an intimate significance and whether there exist other F.Psps. which are either Fibonacci or Lucas numbers.

First we noted that $h = 19$ is the smallest prime such that F_h is composite: $F_{19} = 4181 = 37 \cdot 113$. Moreover, if we exclude $k = 3$ (recall that L_{3n} is even) $k = 23$ is the smallest prime such that L_k is composite: $L_{23} = 64079 = 139 \cdot 461$. The subsequent values of h and k that verify this property are $h = 31$ and $k = 29$. Using the algorithm described in Section 3, we ascertained that

$$L_{F_{31}} \equiv 1 \pmod{F_{31}} \quad (F_{31} = 1346269 = 557 \cdot 2417)$$

and

$$L_{L_{29}} \equiv 1 \pmod{L_{29}} \quad (L_{29} = 1149851 = 59 \cdot 19489).$$

The following question arises: "Are all the composite Fibonacci and Lucas numbers with prime subscript, F.Psps.?"

Furthermore, we found that

$$L_{L_{32}} \equiv 1 \pmod{L_{32}},$$

$L_{32} = 4870847 = 1087 \cdot 4481$ being the smallest composite Lucas number of which the subscript is a power of 2.

Finally, we note that $Q_6 = L_{18} - 1$. A brief search showed that the smallest F.Psp. equal to a Fibonacci number diminished by 1 is

$$F_{33} - 1 = 3524577 = 3 \cdot 7 \cdot 47 \cdot 3571.$$

References

1. *Dizionario Enciclopedico Italiano* (entry: Waring, Edward).
2. O. Brugia & P. Filipponi. "Waring Formulae and Certain Combinatorial Identities." Int. Rept. 3B5986 (1986). Fondazione Ugo Bordoni, Roma.
3. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin Co., 1969.
4. M. R. Schroeder. *Number Theory in Science and Communication*. 2nd ed. Berlin: Springer-Verlag, 1986.
5. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*. 2nd ed. Oxford: The Clarendon Press, 1945.
6. I. M. Vinogradov. *Elements of Number Theory*. New York: Dover Publ. Inc., 1954.
7. V. E. Hoggatt, Jr., & M. Bicknell. "Some Congruences of the Fibonacci Numbers Modulo a Prime P." *Mathematics Magazine* 47.5 (1974):210-214.
8. J. M. Pollin & I. J. Schoenberg. "On the Matrix Approach to Fibonacci Numbers and the Fibonacci Pseudoprimes." *Fibonacci Quarterly* 18.3 (1980): 261-268.

9. M. Pettet. Problem B-93. *Fibonacci Quarterly 4.2* (1966):191.
10. D. Lind. Solution to Problem B-93. *Fibonacci Quarterly 5.1* (1967):111-112.
11. H. T. Freitag & P. Filipponi. "On the Representation of Integral Sequences $\{F_n/d\}$ and $\{L_n/d\}$ as Sums of Fibonacci Numbers and as Sums of Lucas Numbers." *Proc. of the Second Int. Conf. on Fibonacci Numbers and Their Appl.*, San Jose, California, August 1986, pp. 97-112.
12. R. L. Rivest, A. Shamir, & L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Comm. ACM 21.2* (1978):120-126.
13. R. Solovay & V. Strassen. "A Fast Monte-Carlo Test for Primality." *SIAM J. Comput. 6.1* (1977):84-85.

*****

A REMARK ON A THEOREM OF WEINSTEIN

J. W. Sander

Institut fur Mathematik, Universitat Hannover
Welfengarten 1, 3000 Hannover 1, Fed. Rep. of Germany
(Submitted June 1987)

Let $(f_n)_{n\in\mathbb{N}_0}$ denote the Fibonacci sequence:

$$f_0 = 0,\ f_1 = 1,\ f_{n+2} = f_{n+1} + f_n \quad (n \geq 0).$$

For a positive integer m, let $\underline{m} = \{1, 2, \ldots, m\}$. In [5] L. Weinstein proves by an inductive argument the following

Theorem 1: For a positive integer m let $A \subseteq \{f_n : n \in \underline{2m}\}$ with $|A| \geq m + 1$. Then there are f_k, $f_j \in A$, $k \neq j$, such that $f_k | f_j$.

Proof: It is a well-known fact that $f_k | f_j$ for $k | j$ (see, e.g., [4]). Hence, it suffices to show that, for $B \subseteq \underline{2m}$ with $|B| = m + 1$, there are k, $j \in B$, $k \neq j$, such that $k | j$. Let $2^{e(B)}$ denote the exact power of 2 dividing the positive integer b, and define, for all $r \in \underline{2m}$, $2 \nmid r$,

$$B_r = \{b \in B : b/2^{e(B)} = r\}.$$

Obviously, $\bigcup_r B_r = B$. Since $|B| = m + 1$, the pigeon-hole principle yields a B_r containing two distinct elements $k < j$ of B. By definition of B_r, $k | j$.

Remark 1: It should be mentioned that the theorem is best possible, since for $|B| = m$ the conclusion does not hold: Choose, for example, $B = \underline{2m} \setminus \underline{m}$. It might be an interesting question to ask how many sets $B \subseteq \underline{2m}$ with $|B| = m$ have the property that any two elements k, $j \in B$, $k \neq j$, satisfy $k \nmid j$.

A problem similar to the one treated in Theorem 1 will be considered in

Theorem 2: For a positive integer m let $A \subseteq \{f : n \in \underline{2m}\}$ with $|A| \geq m + 1$. Then there are f_k, $f_j \in A$, $k \neq j$, such that $(f_k, f_j) = 1$.

Proof: Since $(f_k, f_j) = f_{(k,j)}$ (see [4]), it suffices to show that for $B \subseteq \underline{2m}$ with $|B| = m + 1$, there are k, $j \in B$, $k \neq j$, such that $(k, j) = 1$. For $r \in \underline{m}$,