We may note in passing that the row sum in Figure 1b is given by

$$\sum_{r=0}^{n} 2^{n-r}\binom{n}{n-r} = 3^n. \tag{3}$$

Also, the right-rising diagonal generates the series 1, 2, 5, 12, 29, 70, ... given by $R_n = 2R_{n-1} + R_{n-2}$, and the left-rising diagonal yields 1, 1, 3, 5, 11, 21, ... given by $L_n = L_{n-1} + 2L_{n-2}$. Other properties of the array may be found by the reader.

REFERENCES

1. Various references to this formula are given in: L. E. Dickson. *History of the Theory of Numbers.* Vol. I, p. 402. 1971 reprint, Chelsea, N.Y.
2. G. Wulczyn. Problem B-339. *The Fibonacci Quarterly* 14, No. 3 (1976): 286.

*****

ON THE MATRIX APPROACH TO FIBONACCI NUMBERS AND THE FIBONACCI PSEUDOPRIMES

JACK M. POLLIN
United States Military Academy, West Point, NY
AND
I. J. SCHOENBERG
Mathematics Research Center, University of Wisconsin-Madison, WI 53706

INTRODUCTION

We consider sequences (x_n) of integers satisfying for all n the recurrence relation

$$x_{n+1} = x_n + x_{n-1}. \tag{1}$$

The x_n are uniquely defined if we prescribe the elements of the "initial vector" (x_0, x_1). On choosing $(x_0, x_1) = (0, 1)$, we obtain the *Fibonacci numbers* $x_n = F_n$, while the choise $(x_0, x_1) = (2, 1)$ gives the *Lucas numbers* $x_n = L_n$.

In [3], V. E. Hoggatt, Jr., and Marjorie Bicknell discuss the following conjecture of K. W. Leonard (unpublished).

Conjecture 1: *We have the congruence*

$$L_n \equiv 1 \pmod{n}, \quad (n > 1) \tag{2}$$

if and only if n is a prime number.

Among the many interesting results of [3], we single out the following:

Theorem 1: *The "if" part of Conjecture 1 is correct; i.e.,*

$$L_p \equiv 1 \pmod{p}, \text{ where } p \text{ is a prime.} \tag{3}$$

Theorem 2: *The "only if" part of Conjecture 1 is wrong, as shown by the congruence*

$$L_{705} \equiv 1 \pmod{705}, \tag{4}$$

while $705 = 3 \cdot 5 \cdot 47$ *is composite.*

Sponsored by the United States Army under Contract No. DAAG29-75-C-0024.

We are grateful to D. H. Lehmer for an informative letter [4] in which he expresses familiarity with these results; also, that composite numbers that satisfy (2) are called *Fibonacci pseudoprimes*, which we abbreviate F. Psps. In [3], the authors report, on the basis of computer results, that beyond 705 the next F. Psps are

$$2465,\ 2737,\ 3745,\ 4181. \tag{5}$$

Conjecture 1 was communicated to one of us several years ago by Richard S. Field, of Los Angeles. We became aware of the paper [3] only recently. Before this, in November 1976, George Logothetis, a graduate student in Computer Science in Madison, using Professor George Collins' SAC 2 program, found for us not only the five F. Psps already mentioned, but also two new ones:

$$5777,\ 6721, \tag{6}$$

He also found that these seven numbers are the only F. Psps that are ≤ 9161.

In the present paper we do the following:

1. Present a proof of Theorem 1 that uses from elementary number theory only Euclid's lemma.
2. Give a second proof of Theorem 2, and establish

Theorem 3: $L_{2465} \equiv 1 \pmod{2465}$.

These numerical results are here derived by the matrix approach as described in [2, Ch. 11]. In [3, p. 211], Theorem 2 is proved in a few lines by showing that the sequence L_n mod 705 has the period 704. Since $L_1 = 1$, the relation (4) follows. In §3 we describe this method of periods and show that while it proved Theorem 2, it did not work to establish Theorem 3. In [4], D. H. Lehmer stated that

$$2737 = 7 \cdot 17 \cdot 23 \textit{ is a Fibonacci pseudoprime}, \tag{7}$$

and that the method of periods will apply. This we verify.

3. Show, in §5, that the matrix approach allows us to develop *ab initio* some of the basic properties of Fibonacci numbers as presented in [1, §10.14]. As we assume no previous knowledge of Fibonacci numbers, this paper may serve as an introduction to these numbers.
4. The failure of the "only if" part of Conjecture 1 suggests a search for classes of composite numbers n which are *not* Fibonacci pseudoprimes. In §6 we state some modest results in this direction which suggested the following:

Conjecture 2: *If* $n > 1$, *then*

$$L_n \not\equiv 1 \pmod{n^2}. \tag{8}$$

Again George Logothetis showed (8) to hold for $n \leq 7611$. Some further striking results obtained in the course of this computation are described at the end of the paper.

1. A PROOF OF THEOREM 1

Observe that the Lucas numbers L_n are explicitly given by

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n \text{ for all } n, \tag{1.1}$$

because $(1 \pm \sqrt{5})/2$ are the roots of the characteristic equation $x^2 - x - 1 = 0$ of (1); hence, the right side of (1.1) satisfies (1), while it assumes the

same initial values as L_n for $n = 0$ and $n = 1$. Now let $n = p$ be a prime > 2. Expanding the binomials and cancelling the irrational terms, we find that

$$L_p - 1 = \frac{1}{2^{p-1}}\left\{1 + \binom{p}{2}5 + \binom{p}{4}5^2 + \cdots + \binom{p}{p-1}5^{\frac{p-1}{2}}\right\} - 1$$

$$= \frac{1}{2^{p-1}}\left\{\binom{p}{2}5 + \cdots + \binom{p}{p-1}5^{\frac{p-1}{2}}\right\} - \frac{2^p - 2}{2^p}$$

Applying the binomial expansion of $(1+1)^p$ in the numerator of the last term, we obtain

$$L_p - 1 = \frac{1}{2^{p-1}}\left\{\binom{p}{2}5 + \cdots + \binom{p}{p-1}5^{\frac{p-1}{2}}\right\} - \frac{1}{2^p}\left\{\binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-1}\right\}.$$

The left side is an integer, while the right side is of the form pa/b, where p does not divide b, and therefore, $(p, b) = 1$. By Euclid's lemma, we conclude that b divides a, which proves (3).

2. THE MATRIX APPROACH AND A PROOF OF THEOREM 2

We replace the relation (1) by the *vector recurrence relation*

$$\begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} x_{n-1} \\ x_n \end{pmatrix} \tag{2.1}$$

to which is it visibly equivalent. Writing

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \tag{2.2}$$

and iterating (2.1), we obtain

$$\begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix} = A^n\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}. \tag{2.3}$$

This brings to bear on our problem the powerful tool of matrix multiplication. To prove Theorem 2, it suffices to work modulo 705. We observe that (2.3) implies

$$\begin{pmatrix} L_{704} \\ L_{705} \end{pmatrix} \equiv A^{704}\begin{pmatrix} 2 \\ 1 \end{pmatrix} \pmod{705}, \tag{2.4}$$

and that we are to determine the matrix $A^{704} \pmod{705}$. This is readily done with a hand calculator if we use the binary representation of 704:

$$704 = 64 + 128 + 512 = 2^6 + 2^7 + 2^9. \tag{2.5}$$

By successively squaring matrices, and working mod 705 throughout, we find $A^{2^k} \pmod{705}$ for $k = 1, 2, \ldots, 9$, and, in particular,

$$A^{2^6} \equiv \begin{pmatrix} 142 & 423 \\ 423 & 565 \end{pmatrix},\ A^{2^7} \equiv \begin{pmatrix} 283 & 141 \\ 141 & 424 \end{pmatrix},\ A^{2^9} \equiv \begin{pmatrix} 424 & 564 \\ 564 & 283 \end{pmatrix} \pmod{705}.$$

Multiplying these matrices together, mod 705, we find, by (2.5), that

$$A^{704} \equiv \begin{pmatrix} 142 & 423 \\ 423 & 565 \end{pmatrix} \pmod{705}.$$

Now (2.4) shows that

$$\begin{pmatrix} L_{704} \\ L_{705} \end{pmatrix} \equiv \begin{pmatrix} 142 & 423 \\ 423 & 565 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 707 \\ 1411 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 1 \end{pmatrix} \pmod{705}. \tag{2.7}$$

Therefore, $L_{705} \equiv 1 \pmod{705}$, and Theorem 2 is established.

A few remarks on these matrix operations are in order. Observe that A is a symmetric matrix, i.e., $A^T = A$. We also know that the product BC of two symmetric matrices that commute ($BC = CB$), is also symmetric. Since any two powers A^m and A^n clearly commute, it follows that all powers A^m are symmetric. This means that in multiplying two powers of A, we need to compute only one of the two elements off the main diagonal.

The matrix multiplications performed above require the following important check against errors. Passing to determinants, from $|A| = -1$, we conclude that $|A^m| = (-1)$. Since all the above exponents m are even, we see that $|A^m| = 1$, and, of course, $|A^m| \equiv 1 \pmod{705}$. The check is to verify that *after each matrix multiplication*, the resulting product M satisfies

$$|M| \equiv 1 \pmod{705}.$$

3. ON THE HOGGATT-BICKNELL PROOF OF THEOREM 2

In order to make this paper self-sufficient, we establish the known lemmas below. Let k be given, $k > 1$, and let us denote by $(L_n, \text{ mod } k)$ the sequence (L_n) of Lucas numbers reduced mod k.

Lemma 1: *The sequence* $(L_n, \text{ mod } k)$ *is periodic.*

Proof: Clearly, $(L_n, \text{ mod } k)$ is periodic if and only if for some r and s we have

$$(x_r, x_{r+1}) \equiv (x_s, x_{s+1}) \pmod{k}, \quad r < s.$$

It follows that there is no periodicity if and only if

$$\text{for every pair } (r, s), \text{ such that } r < s \text{ we have } (x_r, x_{r+1}) \not\equiv (x_s, x_{s+1}) \pmod{k}.$$

But this is obviously impossible, as there are only k^2 distinct pairs $(u, v) \pmod{k}$ available.

The Hoggatt-Bicknell proof of Theorem 2 is based on the following sufficient conditions for $(L_n, \text{ mod } k)$ to have the period m.

Lemma 2: *If the following conditions are satisfied,*

$$k = \prod_{i=1}^{t} a_i, \ (a_i, a_j) = 1 \text{ if } i \neq j, \tag{3.1}$$

$$A_i \text{ is a period of } (L_n, \text{ mod } a_i), \tag{3.2}$$

$$A_i \mid m \text{ for all } i, \tag{3.3}$$

then

$$m \text{ is a period of } (L_n, \text{ mod } k). \tag{3.4}$$

Proof: By (3.2), $L_{n+A_i} \equiv L_n \pmod{a_i}$ for all n. By (3.3), if follows that

$$L_{n+m} \equiv L_n \pmod{a_i} \text{ for all } n, \text{ and all } i, \tag{3.5}$$

because a multiple of a period is also a period. Now (3.1) and (3.5) imply that $L_{n+m} \equiv L_n \pmod{k}$ for all n, which proves (3.4).

Lemma 2 applied nicely to the case of $k = 705 = 3 \cdot 5 \cdot 47$, for (3.1) holds with $t = 3$, $a_1 = 3$, $a_2 = 5$, $a_3 = 47$. Simple direct calculations with L_n show that (3.2) is satisfied with $A_1 = 8$, $A_2 = 4$, $A_3 = 32$. Also (3.3) holds for $m = 704$, because 8, 4, and 32 are all divisors of 704. By Lemma 2, we conclude that $L_{n+704} \equiv L_n \pmod{705}$ for all n. In particular for $n = 1$ we obtain $L_{705} \equiv 1 \pmod{705}$, which proves Theorem 2. For $n = 0$ we also obtain that $L_{704} \equiv L_0 = 2 \pmod{705}$, which we already know from (2.7).

This method will not allow us to prove Theorem 3. Indeed, the relation (4.3) below shows that $m = 2464$ is *not* a period of $(L_n, \text{mod } 2465)$.

4. A PROOF OF THEOREM 3

By (2.3) we are to determine

$$A^{2464} \pmod{2465}. \tag{4.1}$$

From $2464 = 32 + 128 + 256 + 2048 = 2^5 + 2^7 + 2^8 + 2^{11}$, we obtain

$$A^{2464} = A^{2^5} \cdot A^{2^7} \cdot A^{2^8} \cdot A^{2^{11}}. \tag{4.2}$$

By successive squaring of matrices mod 2465, we find that

$$A^{2^5} \equiv \begin{pmatrix} 379 & 1714 \\ 1714 & 2093 \end{pmatrix}, \quad A^{2^7} \equiv \begin{pmatrix} 1393 & 1886 \\ 1886 & 814 \end{pmatrix},$$

$$A^{2^8} \equiv \begin{pmatrix} 495 & 1482 \\ 1482 & 1977 \end{pmatrix}, \quad A^{2^{11}} \equiv \begin{pmatrix} 1858 & 1221 \\ 1221 & 614 \end{pmatrix}, \pmod{2465}.$$

Multiplying these together, we find by (4.2) that

$$A^{2464} \equiv \begin{pmatrix} 117 & 783 \\ 783 & 900 \end{pmatrix},$$

and finally, by (2.3)

$$\begin{pmatrix} L_{2464} \\ L_{2465} \end{pmatrix} \equiv \begin{pmatrix} 117 & 783 \\ 783 & 900 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1017 \\ 2466 \end{pmatrix} \equiv \begin{pmatrix} 1017 \\ 1 \end{pmatrix} \pmod{2465}. \tag{4.3}$$

Thus, $L_{2465} \equiv 1 \pmod{2465}$, which proves Theorem 3.

The information that $L_{2464} \equiv 1017 \pmod{2465}$ shows that $m = 2464$ *is not a period of* $(L_k, \text{mod } 2465)$, and this is the reason why the method of §3 would not work.

Similarly, we can work out on a hand-calculator, such as SR-51A, the matrix $A^{n-1} \pmod{n}$ for any $n < 10^5$. Indeed, all matrix multiplications, mod n, are feasible, because all numbers that we encounter are $< 10^{10}$, the capacity of the calculator.

In [4], D. H. Lehmer pointed out that the second number of (5), namely $2737 = 7.17.23$ is a Fibonacci pseudoprime, and that Lemma 2 applies to show it. This is easily verified: Lemma 2 applies to $k = 2737$ with

$$t = 3,\ a_1 = 7,\ a_2 = 17,\ a_3 = 23,\ A_1 = 16,\ A_2 = 36,\ A_3 = 48, \text{ and } m = 2736.$$

Therefore, 2737 is a period of $(L_n, \text{mod } 2737)$ and it follows that $L_{2736} \equiv 2$, $L_{2737} \equiv 1 \pmod{2737}$. Therefore, (7) is established.

5. FURTHER APPLICATIONS OF THE MATRIX APPROACH

Out applications in §2 and §4 were mainly computational. We now wish to show how the matrix A allows us to develop *ab initio* some of the best known properties of the Fibonacci numbers.

Let us make the relation (2.3) or

$$\begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix} = A^n \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \tag{5.1}$$

more explicit by writing

$$A^n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \tag{5.2}$$

where it becomes

$$\begin{aligned} x_n &= a_n x_0 + b_n x_1 \\ x_{n+1} &= c_n x_0 + d_n x_1. \end{aligned} \tag{5.3}$$

This easily generalizes to

$$\begin{aligned} x_{n+k} &= a_n x_k + b_n x_{k+1}, \\ x_{n+k+1} &= c_n x_k + d_n x_{k+1}. \end{aligned} \tag{5.4}$$

Indeed, by (5.1),

$$\begin{pmatrix} x_{n+k} \\ x_{n+k+1} \end{pmatrix} = A^{n+k}\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = A^n \cdot A^k \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = A^n \begin{pmatrix} x_k \\ x_{k+1} \end{pmatrix},$$

again by (5.1). This and (5.2) show that (5.4) holds. We obtain $x_n = F_n$ if we choose $x_0 = F_0 = 0$ and $x_1 = F_1 = 1$, and (5.3) shows that

$$\begin{aligned} F_n &= b_n, \\ F_{n+1} &= d_n. \end{aligned} \tag{5.5}$$

Applying (5.4) to $x_n = F_n$ and $k = 1$, and observing that $F_1 = 1$, $F_2 = 1$, we obtain

$$\begin{aligned} F_{n+1} &= a_n + b_n \\ F_{n+2} &= c_n + d_n. \end{aligned}$$

These relations and (5.5) show that

$$\begin{aligned} a_n &= F_{n+1} - F_n = F_{n-1}, \\ c_n &= F_{n+2} - F_{n+1} = F_n. \end{aligned}$$

We have thus shown that

$$A^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}. \tag{5.6}$$

See also [2, Theorem II].

Our previous remark that $|A^n| = (-1)^n$ shows that

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n, \tag{5.7}$$

which is a known relation derived in the same way in [2, Theorem III]. From (5.6), we also see that the elements of all the matrices of §2 and §4 are appropriate Fibonacci numbers reduced by the moduli 705 and 2465, respectively.

Let us derive the known property that

$$F_n \text{ divides } F_{nr} \text{ if } r > 0. \tag{5.8}$$

From (5.4) and (5.6), we obtain for $x_n = F_n$ the relation

$$\begin{pmatrix} F_{n+k} \\ F_{n+k+1} \end{pmatrix} = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}\begin{pmatrix} F_k \\ F_{k+1} \end{pmatrix}. \tag{5.9}$$

Replacing n and k by nr and n, respectively, we obtain

$$\begin{pmatrix} F_{n(r+1)} \\ F_{n(r+1)+1} \end{pmatrix} = \begin{pmatrix} F_{nr-1} & F_{nr} \\ F_{nr} & F_{nr+1} \end{pmatrix}\begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix},$$

whence

$$F_{n(r+1)} = F_{nr-1}F_n + F_{nr}F_{n+1}.$$

This shows that if F_n divides F_{nr}, then F_n also divides $F_{n(r+1)}$, which proves (5.8) by induction, since (5.8) is obvious if $r = 1$.

As a further example, let us establish the known property:

$$\text{If } (m, n) = d, \text{ then } (F_m, F_n) = F_d. \tag{5.10}$$

Since d divides m and also n, it follows from (5.8) that

$$F_d \text{ divides } F_m \text{ and also } F_n. \tag{5.11}$$

It remains to show that F_d is the *greatest* common divi r of F_m and F_n. Let r and s be such that $d = mr + ns$. From (5.9), on replacing n and k by mr and ns, respectively, we obtain

$$\begin{pmatrix} F_{mr+ns} \\ F_{mr+ns+1} \end{pmatrix} = \begin{pmatrix} F_{mr-1} & F_{mr} \\ F_{mr} & F_{mr+1} \end{pmatrix} \begin{pmatrix} F_{ns} \\ F_{ns+1} \end{pmatrix}.$$

This shows in particular that $F_d = F_{mr+ns}$ can be written as

$$F_d = F_{mr-1}F_{ns} + F_{mr}F_{ns+1}. \tag{5.12}$$

By (5.8), any divisor δ of F_m and of F_n also divides F_{mr} and F_{ns}, and by (5.12) that δ also divides F_d. Therefore, F_d is the greatest common divisor of F_m, F_n, and (5.10) is established.

A last example concerns the Lucas numbers. *Let us show that*

$$L_{n+1}L_{n-1} - L_n^2 = (-1)^{n+1} \cdot 5. \tag{5.13}$$

From (5.1) and (5.6), we have

$$\begin{pmatrix} L_n \\ L_{n+1} \end{pmatrix} = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

Again for $x_n = L_n$, but from (5.4) with $k = -1$, we get that

$$\begin{pmatrix} L_{n-1} \\ L_n \end{pmatrix} = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} \begin{pmatrix} -1 \\ 2 \end{pmatrix}$$

because $L_{-1} = -1$, $L_0 = 2$. The last two relations combined give

$$\begin{pmatrix} L_{n-1} & L_n \\ L_n & L_{n+1} \end{pmatrix} = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Passing to determinants and using (5.7), we obtain (5.13).

6. SOME COMPOSITE NUMBERS THAT ARE NOT FIBONACCI PSEUDOPRIMES

We have defined a number n as a *Fibonacci pseudoprime* (F. Psps) if it is composite and satisfies $L_n \equiv 1 \pmod{n}$. F. Psps are rare: We have seen that there are only seven F. Psps ≤ 9161. It would seem of interest to exhibit some composite n which are not F. Psps. A modest beginning in this direction are the following results.

Theorem 4: *The numbers*

$$2^k, \ (k > 1) \tag{6.1}$$

are not Fibonacci pseudoprimes. Actually

$$L_{2^k} \equiv 2^k - 1 \pmod{2^k}. \tag{6.2}$$

Theorem 5: *If p is an odd prime such that*

$$L_p \not\equiv 1 \pmod{p^2}, \tag{6.3}$$

then

$$L_{p^k} \not\equiv 1 \pmod{p^k} \text{ for } k > 1, \tag{6.4}$$

hence p^k is not a Fibonacci pseudoprime.

For brevity, we omit proofs which might be given elsewhere. We rather discuss the assumption (6.3).

Computer computations made by George Logothetis (Nov. 1976) show that

$$L_n \not\equiv 1 \pmod{n^2} \text{ if } 2 \leq n \leq 7611, \tag{6.5}$$

whether n is prime or composite. He computed the remainder r_n, hence

$$L_n \equiv r_n \pmod{n^2},\ 0 \leq r_n < n^2, \tag{6.6}$$

for all n such that $2 \leq n \leq 7611$, with the following results.

1. *The remainders* $r_n = 0$ *and* $r_n = 1$ *were never found.* This result led us to formulate Conjecture 2 of our Introduction.

2. *The value* $r_n = 2$ *appeared only if* $n \equiv 0 \pmod{24}$.

For $n = 24k$, *he found that* $r_n = 2$ *precisely for the following* 100 *values of* k:

$k =$										
	1	2	3	4	5	6	8	9	10	12
	14	15	16	18	20	24	25	27	28	30
	32	36	40	42	45	46	48	50	51	54
	55	56	57	60	64	70	72	75	80	81
	84	90	92	96	98	100	102	108	110	112
	114	120	125	126	128	135	138	140	144	150
	153	155	160	162	165	168	171	180	182	184
	188	192	195	200	204	205	210	215	220	224
	225	228	230	240	243	250	252	255	256	270
	275	276	280	285	288	294	300	305	306	310

This is remarkable numerical evidence. From generally large values, the remainder r_n in (6.6) drops down to $r_n = 2$ for $n = 24k$ and values of k as listed. We also mention that the last Lucas number, L_{7611}, has 1591 digits.

From the identity $L_{4n} - 2 = 5(F_{2n})^2$ [2, Identity I_{16}, p. 59], it follows that $L_{24k} - 2 = 5(F_{12k})^2$. Therefore, $L_{24k} - 2 \equiv 0 \pmod{(24k)^2}$ if and only if

$$F_{12k} \equiv 0 \pmod{24k}. \tag{6.7}$$

From the computer results above, we see that (6.7) holds for the 100 values of k listed above, and does not hold for the other values of

$$k \leq [7611/24] = 317.$$

REFERENCES

1. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers.* 3rd ed. Oxford: Oxford University Press, 1954.
2. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers.* Boston: Houghton Mifflin Co., 1969.
3. V. E. Hoggatt, Jr., & Marjorie Bicknell. "Some Congruences of the Fibonacci Numbers Modulo a Prime p." *Math. Magazine* 47 (1974):210-214.
4. D. H. Lehmer. Personal letter to the authors, November 28, 1976.

*****

FREE GROUP AND FIBONACCI SEQUENCE

G. WALTHER
Institut für Didaktik der Mathematik, Postfach 380, W. Germany

Let X be a nonempty set $X = \{x_i | i \in I\}$ where I is a suitable index set and X^{-1} another set in one-to-one correspondence with X. A word of length n in the elements of $X \cup X^{-1}$ is an ordered set of n elements ($n \geq 0$) each of $X \cup X^{-1}$.

A word of length n will be written as $x_{i_1}^{s_1} \ldots x_{i_n}^{s_n}$ where each sign s_i is i or -1. With "1" we denote the unique word of length 0. The product of two words is defined as follows. Let a be an arbitrary word $1a = a1 : a$.