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

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, $L_{24k} - 2 \equiv 0\ [\bmod\ (24k)^2]$ 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

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

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 $X = \{x_i \mid i \in I\}$ 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 ($n \geqq 0$) 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 $1a = a1 : a$.

Let a and b be words of positive lengths m and n; i.e.,

$$a = x_{i_1}^{s_1} \ldots x_{i_m}^{s_m} \quad \text{and} \quad b = x_{j_1}^{t_1} \ldots x_{j_n}^{t_n},$$

then

$$ab := x_{i_1}^{s_1} \ldots x_{i_m}^{s_m} x_{j_1}^{t_1} \ldots x_{j_n}^{t_n}$$

and the length of the product is $m + n$.

If we define the relation "adjacent" between words, which turns out to be an equivalence relation, and the product $[a][b] := [ab]$ of equivalence classes $[a]$ and $[b]$ of words a and b, we get the free group $F(X)$ over the generating set X.

A word in $X \cup X^{-1}$ is reduced if it has the form

$$x_{i_1}^{s_1} \ldots x_{i_m}^{s_m} \quad \text{and} \quad x_{i_{k+1}}^{s_{k+1}} \neq x_{i_k}^{-s_k} \text{ for } k = 1, 2, \ldots, m - 1.$$

Two elements, $x_i^{s_i}$ and $x_j^{s_j} \in X \cup X^{-1}$, will be called an inverse couple of elements if

$$x_i^{s_i} x_j^{s_j} = 1 \quad \text{or} \quad x_j^{s_j} x_i^{s_i} = 1.$$

Now we are in the position to formulate our problem.

Let $a = a_1 \ldots a_n$ be a word of length n with $a_i \in X \cup X^{-1}$ for $1 \leq i \leq n$. What is the maximum number of ways in which it could be reduced

a. to different words of length g $(n \geq g)$?
b. to different words?
c. to words of length g?

<u>*Theorem*</u>: Let A_{gn}, B_n, and C_{gn} be the numbers mentioned above. Then we get

α) $$A_{gn} = \begin{cases} \dbinom{\frac{g+n}{2}}{g} & \text{if } g \text{ and } n \text{ have the same parity and } g \leq n \\ 0 & \text{otherwise} \end{cases}$$

β) $$B_n = B_{n-1} + B_{n-2}, \; B_0 = B_1 = 1$$

γ) $$C_{gn} = \begin{cases} \dbinom{n-1}{t} - \dbinom{n-1}{t-2} & \text{for } g = n - 2t \text{ and } 0 \leq t < \frac{n}{2} \\ 1 & \text{for } g = n \\ 0 & \text{otherwise} \end{cases}$$

<u>*Corollary*</u>: Expression of B_n as a sum of binomial coefficients.

With the convention $\binom{n}{0} = 1$, $\binom{n}{m} = 0$, for $n < m$,

we get the well-known relation

$$B_n = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots.$$

To prove the theorem, we use a known procedure to construct the reduced word for $a = a_1 \ldots a_n$.

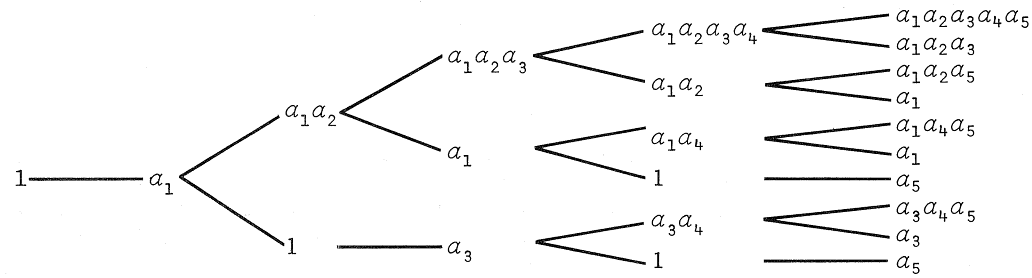
Let $w_0 := 1$ and $w_1 := a_1$, and let w_i be found for $1 \leq i < n$.

i) If w_i does not end in a_{i+1}^{-1}, then $w_{i+1} := w_i a_i$.

ii) If w_i does end in a_{i+1}^{-1}, then $w_{i+1} := z$, where $w_i = z a_{i+1}^{-1}$.

In a somehow "inverse" sense, we can get a survey over the reduction process by means of a tree.

Take the word $a = a_1 a_2 a_3 a_4 a_5$ for example:



It is evident, from the cancellation process, that $A_{gn} = C_{gn} = 0$ iff g and n have different parity.

Proof:

α) As cancellation diminishes the length of a word by 2, it is clear, from rules (i) and (ii) that

$$A_{gn} = A_{g,n-2} + A_{g-1,n-1} \text{ for } n \geq 2,$$

with the additional conditions $A_{gn} = 0$ iff g and n have different parity, $A_{0n} = 1$, $A_{gg} = 1$ for $0 \leq g \leq n$, $A_{gn} = 0$ for $g > n$.

The transformation $D_{ik} := A_{k,2i-k}$ for $0 \leq k \leq i$, $D_{ii} = 1$ for $i \geq 0$,

$$D_{i0} = \begin{cases} 1 & \text{if } i \text{ is even} \\ 0 & \text{if } i \text{ is odd,} \end{cases}$$

and $D_{ik} = 0$ for $k > i$, together with its inverse transformation,

$$A_{pq} = D_{\frac{p+q}{2},p},$$

yields the fundamental binomial relation

$$D_{ik} = D_{i-k,k} + D_{i-1,k-1} \text{ for } i, k \geq 1,$$

with solution $D_{ik} = \binom{i}{k}$. Translating this result, we get $A_{gn} = \binom{\frac{g+n}{2}}{g}$.

β) For $n = 0, 1, 2$, the proposition is true. Let $a = a_1 \ldots a_{n-2}a_{n-1}a_n$ be a word of length $n - 2$. Then we distinguish two cases:

1. $a_i a_n \neq 1$ for $i < n$ (i.e., a_i is the last "letter" of a word of maximum length $n - 1$). By the induction hypothesis, the maximum number of different words to which a word of length $n - 1$ can be reduced is B_{n-1}. The B_{n-1} different words $w_1, \ldots, w_{B_{n-1}}$ consequently lead to B_{n-1} different words $w_1a_n, \ldots, w_{B_{n-1}}a_n$.

2. $a_ia_n = 1$. I.e., a_i, a_n is an inverse couple for $i < n$; therefore, the length of words under consideration is reduced by 2. Consequently, we have a contribution of B_{n-2} to the amount of B_n.

γ) For illustration consider the word $w = a_1a_2a_3a_4a_5$ which could be reduced to a_1, for example, in exactly two ways:

a_2, a_3 and a_2, a_5 are two inverse couples;
a_2, a_3 and a_4, a_5 are two inverse couples (cf. the tree above).

The cancellation process yields the following special relations:

$$C_{mn} = 0 \text{ for } m > n;\ C_{mm} = 1;\ C_{mn} = 0 \text{ for } m, n, \text{ with different parity;}$$

$$C_{0n} = C_{1,n-1} \text{ for } n \geq 1.$$

A simple induction argument shows that $C_{n-2,n} = n - 1$ for $n \geq 2$.

We get all possible reduced words w' from $w = a \ldots a_{n-1}a_{n-2}a_n$ of length $n - 2$ *either* extending all $n - 2$ words

$$w'' = x_{i_1} \ldots x_{i_{n-2}}$$

$$(i_1 < i_2 < \cdots < i_{n-2} \text{ and } x_{i_j} \in \{a_1, \ldots, a_{n-2}\})$$

with a_n, i.e., $w' = w''a_n$ *or* from the single word $a_1 \ldots a_{n-2}$. In the latter case, a_{n-1}, a_n is the only inverse couple of w.

Besides the special relations for C_{mn}, we have the general relation

$$(*) \qquad C_{mn} = C_{m+1,n-1} + C_{m-1,n-1} \text{ for } m, n \geq 1.$$

Let $E_{ik} := C_{k,i+k}$ for $i, k \geq 0$, respectively, $C_{mn} = E_{n-m,m}$ for $n \geq m$ and $n, m \geq 0$. From $C_{0n} = C_{1,n-1}$ follows $E_{i0} = E_{i-2,1}$ for $i \geq 2$.

From (*), we get

$$(**) \qquad E_{ik} = E_{i,k-1} + E_{i-2,k+1} \text{ for } i \geq 2, k \geq 1.$$

Considering $C_{n-2,n} = n - 1$ for $n \geq 2$, we have $E_{2k} = 1 + k$.

Next we express E_{ik} by $E_{i-2,k}$ for $i \geq 2$; (**) yields

$$E_{ik} = \sum_{p=1}^{k+1} E_{i-2,p}.$$

An iteration procedure and $E_{2k} = 1 + k$ leads to the following "monstrous" expression:

$$E_{2t,k_{t-1}} = \sum_{k_{t-2}=1}^{k_{t-1}+1} \cdots \sum_{k_1=1}^{k_2+1} \sum_{r=1}^{k_1+1} (r + 1) \text{ for } t \geq 2, k_i \geq 0.$$

Remark: Since $C_{mn} = 0$ for m, n with different parity, we have $E_{ik} = 0$ for i an odd number.

We prove by induction that

$$E_{2t,k_{t-1}} = \binom{k_{t-1} + 2t - 1}{t} - \binom{k_{t-1} + 2t - 1}{t - 2}, \quad t \geq 2.$$

For $t = 2$, we have

$$E_{2,k_1} = \sum_{r=1}^{k_1+1} (r + 1) = \frac{(k_1 + 4)(k_1 + 1)}{2} = \frac{(k_1 + 3)(k_1 + 2)}{2} - 1$$

$$= \binom{k_1 + 3}{2} - \binom{k_1 + 3}{0}.$$

To show

$$\sum_{k_{t-1}=1}^{k_t+1} \left[\binom{k_{t-1} + 2t - 1}{t} - \binom{k_{t-1} + 2t - 1}{t - 2}\right] = \binom{k_t + 2t + 1}{t + 1} - \binom{k_t + 2t + 1}{t - 1}$$

$$= E_{2(t+1),k_t},$$

we need the following

Lemma: $$\sum_{k=1}^{n+1} \binom{c + k}{j} = \binom{c + n + 2}{j + 1} - \binom{c + 1}{j + 1}.$$

Proof of the Lemma: On the one hand

$$\sum_{k=1}^{n} \prod_{i=0}^{j} (k + i) = (j + 1)! \sum_{k=1}^{n} \binom{k + j}{j + 1};$$

on the other hand

$$\sum_{k=1}^{n} \prod_{i=0}^{j} (k + i) = \frac{1}{j + 2} \sum_{i=0}^{j+1} (n + i).$$

Combining these two identities yields

$$\text{(***)} \qquad \sum_{k=1}^{n} \binom{k + j}{j + 1} = \binom{n + j + 1}{j + 2}.$$

From

$$\sum_{k=1}^{n+1} \binom{c + k}{j} = \sum_{k=0}^{c+n-j+2} \binom{k + j - 1}{j} - \sum_{k=0}^{c-j+1} \binom{k + j - 1}{j},$$

follows, with (***), the assertion.

Now we continue the proof of the theorem. With the aid of the lemma,

$$\sum_{k_{t-1}=1}^{k_t+1} \left[\binom{k_{t-1} + 2t - 1}{t} - \binom{k_{t-1} + 2t - 1}{t - 2} \right]$$

$$= \binom{k_t + 2t + 1}{t + 1} - \binom{2t}{t + 1} - \binom{k_t + 2t + 1}{t - 1} + \binom{2t}{t - 1}$$

$$= \binom{k_t + 2t + 1}{t + 1} - \binom{k_t + 2t + 1}{t - 1} = E_{2(t+1),\, k_t}.$$

To prove the corollary, we use

$$B_n = \sum_{g \le n} A_{gn} = \sum_{g \le n} \binom{\frac{g + n}{2}}{g} = \binom{n}{n} + \binom{n - 1}{n - 2} + \cdots$$

$$= \binom{n}{0} + \binom{n - 1}{1} + \cdots .$$

$\binom{\frac{g + n}{2}}{g}$ is defined, because g and n have the same parity.

*****