THE FIBONACCI QUARTERLY

THE OFFICIAL JOURNAL OF
THE FIBONACCI ASSOCIATION

VOLUME 8 NUMBER 1

CONTENTS

PART I — ADVANCED

PART II — ELEMENTARY

THE FIBONACCI QUARTERLY

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

DEVOTED TO THE STUDY
OF INTEGERS WITH SPECIAL PROPERTIES

All subscription correspondence should be addressed to Bro. A. Brosseau, Mary's College, Calif. All checks ($6.00 per year) should be made out to the Fibonacci Association or the Fibonacci Quarterly. Manuscripts intended for publication in the Quarterly should be sent to Verner E. Hoggatt, Jr., Mathematics Department, San Jose State College, San Jose, Calif. All manuscripts should be typed, double-spaced. Drawings should be made the same size as they will appear in the Quarterly, and should be done in India ink on either vellum or bond paper. Authors should keep a copy of the manuscript sent to the editors.

The Quarterly is entered as third-class mail at the St. Mary's College Post Office, California, as an official publication of the Fibonacci Association.

THE LUCAS-LEHMER TEST FOR MERSENNE NUMBERS

SIDNEY KRAVITZ
Dover, New Jersey

The purpose of this note is to present certain computer calculations relating to the Lucas-Lehmer Test for the primality of Mersenne Numbers.

The Lucas-Lehmer Test states that the Mersenne number $M_p = 2^p - 1$ is prime if and only if $S_{p-1} \equiv 0 \mod M_p$ where

$$S_{i+1} = S_i^2 - 2 \tag{1}$$

and $S_1 = 4$. Lehmer further states* that this test is valid not only for $S_1 = 4$ but for S_1 equal to 2^{p-2} different numbers mod M_p. These 2^{p-2} starting values, $S_{1,i}$, $(i = 1,2,\cdots,2^{p-2})$ are determined by

$$S_{1,i+1} = 14\, S_{1,i} - S_{1,i-1} \tag{2}$$

where $S_{1,1} = S_1 = 4$ and $S_{1,2} = 52$.

Figure 1 demonstrates the Lucas-Lehmer Test for $M_7 = 2^7 - 1 = 127$. Each of the $2^{p-2} = 32$ starting values, $S_{1,i}$, as determined by Eq. (2) leads to $S_6 = 0 \mod M_7$ following Eq. (1). There are 16 different values of S_2, 8 different values of S_3, etc. Note that $S_7 = -2$ and $S_8 = 2 \mod M_7$. The result is that $2^{p-1} + 1 = 65$ different numbers mod M_p are involved in the Lucas-Lehmer test.

What happens to the other $q^{p-1} - 2 = 62$ numbers mod M_7 when we apply Eq. (1)? This is shown in Fig. 2. We see that successive terms do not lead to a zero term, but instead are repetitive in cycles whose periods are divisors of $(p - 1)$. Figure 2 shows four cycles of double sixes and two cycles of double threes.

A computer program was used to determine the structure of the Lucas-Lehmer Test for M_7, M_{13} and M_{17} with the following results.

---

*D. H. Lehmer, "An Extended Theory of Lucas' Functions," Annals of Math., (2) 31 (1930), pages 419-448.

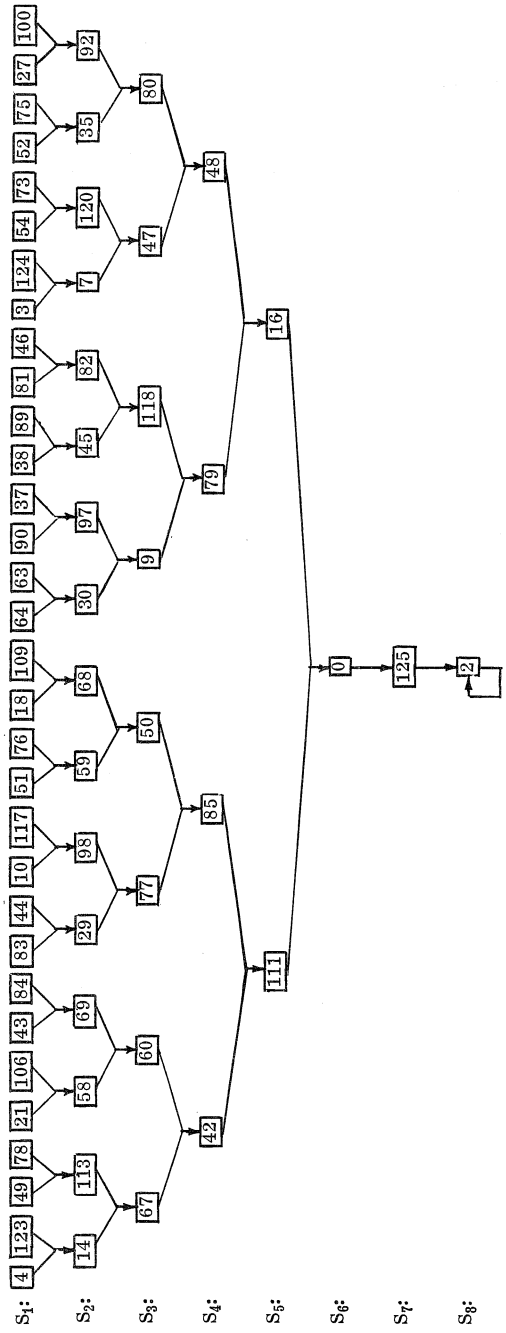


Fig. 1 The Lucas-Lehmer Test for $M_7 = 127$ Involving 65 Numbers mod 127

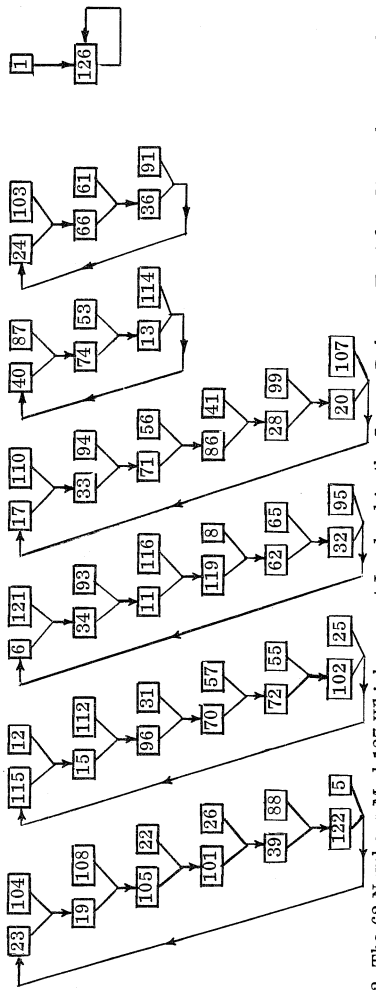


Fig. 2 The 62 Numbers Mod 127 Which are not Involved in the Lucas-Lehmer Test for M_7. There are four cycles of double sixes and two cycles of double threes.

For $M_7 = 127$

A Lucas-Lehmer pattern of $2^{p-1} + 1$ terms	making 65 terms
4 cycles of double sixes	making 48 terms
2 cycles of double threes	making 12 terms
The two terms ±1	making 2 terms
	Total 127 terms

For $M_{13} = 8191$

A Lucas-Lehmer pattern of $2^{p-1} + 1$ terms	making 4097 terms
165 cycles of double twelves	making 3960 terms
9 cycles of double sixes	making 108 terms
1 cycle of double fours	making 8 terms
2 cycles of double threes	making 12 terms
1 cycle of double twos	making 4 terms
The two terms ±1	making 2 terms
	Total 8191 terms

For $M_{17} = 131,071$

A Lucas-Lehmer pattern of $2^{p-1} + 1$ terms	making 65537 terms
2032 cycles of double sixteens	making 65024 terms
30 cycles of double eights	making 480 terms
3 cycles of double fours	making 24 terms
1 cycle of double twos	making 4 terms
The two terms ±1	making 2 terms
	Total 131071 terms

For $M_{19} = 524287$

A Lucas-Lehmer pattern of $2^{p-1} + 1$ terms	making 262145 terms
7252 cycles of double eighteens	making 261072 terms
56 cycles of double nines	making 1008 terms
4 cycles of double sixes	making 48 terms
2 cycles of double threes	making 12 terms
The two terms ±1	making 2 terms
	Total 524287 terms

* * * * *

RECURRENCE FORMULAS

JOSEPH ARKIN
Spring Valley, New York
and
RICHARD POLLACK
New York University, New York, New York

In this paper p(n) shall denote, as usual, the number of partitions of n; that is, the number of solutions of the equation:

$$x_1 + 2x_2 + 3x_3 + \cdots + nx_n = n$$

in non-negative integers. We state the following identity

$$p(n) = -\sum_{\substack{0\le i\le m \\ m<j\le n}} p(i)\, e(j-i)\, p(n-j) \quad , \tag{1}$$

where $e(k) = (-1)^k$ if $k = \frac{1}{2}(3h^2 \pm h)$, 0 otherwise, and $p(0) = 1$.

The proof of (1) will be evident as a special case of the following more general form. (See acknowledgement.) Put

$$f(x) = \sum_{n=0}^{\infty} a(n)\, x^n, \quad (f(x))^{-1} = \sum_{n=0}^{\infty} b(n) x^n \quad ,$$

where for convenience $a(0) = b(0) = 1$. Then

$$\sum_{j=0}^{n} a(j)\, b(n-j) = 0 \qquad (n > 0) \quad . \tag{2}$$

Now consider the sums

$$S = \sum_{\substack{0\le i\le m \\ m<j\le n}} n(i)\, b(j-i)\, a(n-j) \quad ,$$

$$T = \sum_{0\le i\le j\le m} a(i) b(j-i)\, a(n-j)$$

where $0 < m < n$. Then in the first place, by (2),

$$(3) \qquad T = \sum_{j=0}^{m} a(n - j) \sum_{i=0}^{j} a(i)\, b(j - i) = a(n) .$$

In the next place,

$$S + T = \sum_{0 \le i \le m} \sum_{i \le j \le n} a(i)\, b(j - i)\, a(n - j)$$

$$= \sum_{0 \le i \le m} a(i) \sum_{s=0}^{n-i} b(s)\, a(n - i - s) .$$

The inner sum on the extreme right vanishes unless $n - i = 0$; since $m < n$ this condition is satisfied for no value of i in the range $0 \le i \le m$ and therefore $S + T = 0$.

Combining this with (3), we get $S = -a(n)$, or, explicitly,

$$(4) \qquad \sum_{\substack{0 \le i \le m \\ m < j \le n}} a(i)\, b(j - i)\, a(n - j) = -a(n) \qquad (0 < m < n) .$$

The recurrence (1) clearly follows from (4).

Note. Since we may equally well have started out with $(f(x))^{-1}$ rather than $f(x)$, we have also

$$\sum_{\substack{0 \le i \le m \\ m < j \le n}} b(i)\, a(j - i)\, b(n - j) = -b(n) \qquad (0 < m < n) .$$

ACKNOWLEDGEMENT

The authors wish to thank Professor L. Carlitz of Duke University for his generous letter extending (1) into this more general form.

* * * * *

THE t-FIBONACCI NUMBERS AND POLYPHASE SORTING

W. C. LYNCH
Case Institute of Technology, Cleveland, Ohio

1. INTRODUCTION

This paper is divided into two parts that can be read almost independently. The first part defines a generalization of the Fibonacci numbers called the t-Fibonacci numbers, and investigates certain of their properties in detail and without reference to their applications. The second part describes merge sorting and particularly polyphase sorting. A new solution to the initial distribution problem is presented, which constitutes an important application of the theory developed in the first part of this paper.

The reader may start either with the Fibonacci theory in Part 1 or with the sorting application in Part 2. Results from Part 1 are used only in Section 7, the last section of Part 2. The material in Sections 2, 5, and 6 is an exposition of known results in a form designed to help introduce the new results which appear in the other sections.

PART I

2. THE t-FIBONACCI NUMBERS

Any sequence of numbers U_n which satisfies

$$U_n = U_{n-1} + \cdots + U_{n-t} \tag{1}$$

will be called a t-Fibonacci sequence. The i^{th} t-Fibonacci sequence is the special t-Fibonacci sequence with initial conditions $U_j = \delta_{ij}$ for $1 \leq j \leq t$. The Kronecker delta is represented by δ_{ij}

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

The cumulative t-Fibonacci sequence is the special t-Fibonacci sequence with the initial conditions $U_j = 1$ for $1 \leq j \leq t$. We will denote the n^{th} term of the i^{th} t-Fibonacci sequence by ${}_iU_n$ and the n^{th} term of the cumulative t-Fibonacci sequence by ${}_\Sigma U_n$. Clearly

$$\Sigma U_n = \sum_{i=1}^{t} {}_iU_n .$$

Mention of t in the notation is suppressed since t will remain fixed for any given discussion in this paper. Further, we will restrict t so that $t \geq 2$. Values of ${}_iU_n$ and ΣU_n for $t = 4$ are given in Fig. 1.

n	${}_1U_n$	${}_2U_n$	${}_3U_n$	${}_4U_n$	ΣU_n
0	-1	-1	-1	1	-2
1	1	0	0	0	1
2	0	1	0	0	1
3	0	0	1	0	1
4	0	0	0	1	1
5	1	1	1	1	4
6	1	2	2	2	7
7	2	3	4	4	13
8	4	6	7	8	25
9	8	12	14	15	49
10	15	23	27	29	94
11	29	44	52	56	181
12	56	85	100	108	349
13	108	164	193	208	673

Fig. 1 The 4-Fibonacci Numbers

Many interesting relations can be observed in Fig. 1. We may verify directly that

$$(2) \qquad {}_iU_{t+1} = 1 .$$

Another central pair of relations is

$$(3) \qquad {}_1U_n = {}_tU_{n-1}$$

$$(4) \qquad {}_iU_n = {}_{i-1}U_{n-1} + {}_tU_{n-1}, \quad \text{for} \quad 2 \leq i \leq t .$$

By (1) and the initial conditions

$$(5) \qquad {}_iU_n = \delta_{in} \qquad 1 \leq n \leq t$$

we may verify (2) and (3) directly for $2 \leq m \leq t$. Equation (1a) and the initial conditions allow us to verify (2) and (3) for $n = t + 1$. By summing each side of (2) and (3) over the previous t terms, we can, by induction on n, establish their validity for all n.

For the case $t = 2$, the sequence ${}_1U_n$ and ${}_tU_n = {}_2U_n$ are both the usual Fibonacci sequences. Further, for $t = 2$, ${}_\Sigma U_n = {}_1U_n + {}_2U_n = {}_2U_{n-1} + {}_2U_n = {}_2U_{n+1}$. Thus for $t = 2$, all the sequences are the familiar ones, differing only in the designation of the first element.

3. NUMBER REPRESENTATIONS IN THE t-FIBONACCI NUMBER SYSTEM

We will say a sequence C_j, $j > 1$, is a representation of the integer K in the t-Fibonacci number system if and only if the following conditions are met:

(a) $$C_j = 0 \quad \text{or} \quad C_j = 1 \quad ,$$

(b) $$K = \sum_{j=1}^{\infty} C_j {}_\Sigma U_j \quad ,$$

(c) $j \leq t$ and $C_j = 0$ implies that $C_i = 0$ for all $i \leq j$,

(d) for all $i \geq 0$, if $C_j = 1$ for $i < j < i + t - 1$ then $C_{i+t} = 0$.

This rather technical definition describes a binary positional notation for representing integers. The coefficient digits are restricted to zero and one. The value of the j^{th} position in the notation is ${}_\Sigma U_j$. For example, when $t = 4$ (refer to Fig. 1 again),

$$39 = 25 + 13 + 1$$

or in the positional notation

$$39 = 1100\,|\,1000 \ .$$

(It is convenient to insert a vertical line t digits from the right.)

By condition (c), $39 = 1100|0100$ would be incorrect, and by condition (d), $39 = 1011|1110$ would be incorrect.

Condition (c) says that the positions of value 1 that we use must be the left-most ones available. Condition (d) says that we may have no more than $t - 1$ ones in a row. It is not immediately clear whether or not all positive integers are representable, or whether such a representation is unique.

We now present the

COUNTING ALGORITHM:

Let C_j be a representation for K.

Step (1) Select the largest j such that $t \geq j \geq 1$ and $C_k = 0$ for all $k \leq j$. Change C_j from 0 to 1.

Step (2) If C_j through C_{j+t-1} are not all 1's then the algorithm terminates.

Step (3) If C_j through C_{j+t-1} are all 1's then change C_{j+t} from 0 to 1 (if C_{j+t} is not 0 then the original sequence has 1's in C_{j+1} through C_{j+t} and thus violated condition (d)). Increase j by t and go back to Step (2).

We observe the following about the counting algorithm when C_j is a representation of K:

1. Step (1) increases by one the value of the representation.
2. Step (3) does not change the value of the representation since U_n
3. Each application of Step (3) reduces the number of 1's in the representation so that the algorithm terminates.
4. At termination, the resulting sequence of C_j's satisfies (a) through (d) and is thus a representation of $K + 1$.
5. If C_{n-1} was the non-zero coefficient of maximum index in the original representation of K, then either

   5a. C_{n-1} is still the non-zero coefficient of maximum index in the representation of $K + 1$ or

   5b. The resulting representation of $K + 1$ contains the sole non-zero entry C_n ($K + 1 = \Sigma U_n$).

As step 3 was or was not executed with $j = n - t$, 5a or 5b applies.

Lemma 1. Each sequence C_j which satisfies (a) through (d) represents an integer K such that $K < \Sigma U_n$, where C_{n-1} is the non-zero coefficient of maximum index.

Proof: Repeatedly apply the Counting Algorithm to C_j. Since an infinite number of integers can be represented, some application of the algorithm (say, the r^{th}) must terminate with condition 5b holding. Then $K + r = {}_{\Sigma}U_n$ so that $K < {}_{\Sigma}U_n$.

We now prove

Theorem 2: (Extended Zeckendorf theorem) Each non-negative integer has a unique representation in the t-Fibonacci number system.

Proof: We will show that the theorem holds for all integers less than U_n. The proof will proceed by induction on n.

Base Step: Take $n = t + 1$. Then ${}_{\Sigma}U_n = t$. For all non-negative integers less than t, representability is assured by having enough positions (t) of value 1 available. Uniqueness follows from condition (d). Condition (d) is satisfied trivially.

Induction Step: Let ${}_{\Sigma}U_{n-1} \leq K < {}_{\Sigma}U_n$ and assume the theorem for all non-negative integers $< {}_{\Sigma}U_{n-1}$. Using (3) as a clue, we observe that

$$ {}_{\Sigma}U_n = 2{}_{\Sigma}U_{n-1} - {}_{\Sigma}U_{n-t-1} . \tag{6}$$

Since we are on an induction step, n is greater than $t + 1$ so that

$$ {}_{\Sigma}U_{n-t-1} > 0 .$$

It then follows that

$$ {}_{\Sigma}U_n - {}_{\Sigma}U_{n-1} < {}_{\Sigma}U_{n-1} , \tag{7a}$$

and certainly

$$ 0 \leq K - {}_{\Sigma}U_{n-1} < {}_{\Sigma}U_{n-1} . \tag{7b}$$

Since, by induction, we can represent $K - {}_{\Sigma}U_{n-1}$ (clearly with $C_{n-1} = 0$), we can represent K except for some uncertainty about condition (d). But the only place (d) could be violated would be for C_{n-1} down to C_{n-t} to be all 1's. If that is the case, then $K \geq {}_{\Sigma}U_{n-1} + \cdots + {}_{\Sigma}U_{n-t} = {}_{\Sigma}U_n$, contrary to assumption. Thus K is representable. By Lemma 2, every representation of K

must have $C_{n-1} = 1$. Otherwise Lemma 1 asserts that $K < {}_{\Sigma}U_{n-1}$, contrary to the induction assumption. If K has two representations, say C_j and C'_j, then $K - {}_{\Sigma}U_{n-1}$ is represented by D_j and D'_j where D_j is obtained from C_j by changing C_{n-1} from 1 to 0. Similarly, D'_j is obtained from C'_j. Both D_j and D'_j are then distinct representations for $K - {}_{\Sigma}U_{n-1}$. Since by (7b),

$$K - {}_{\Sigma}U_{n-1} < {}_{\Sigma}U_{n-1} ,$$

this is impossible by the induction hypothesis. The representation for K is thus unique. Q. E. D.

Theorem 2 for the case $t = 2$ is the familiar Zeckendorf Theorem [2].

In any representation, (d) implies that one of the t bottom positions must be zero. Select the left-most zero position from the bottom t positions and change it to a one. This increases the value of the representation by one and preserves condition (c). It may, however, cause a violation of condition (d). If this is so, the 1 we added must be the right-most in a string of t ones. Zero out that string of ones and change the next highest position (it must be zero or there would already have been a string of t ones contrary to (d)) to a one. Repeat this "carrying" step as often as necessary to assure condition (d). Figure 2 depicts counting in the 4-Fibonacci system.

4. t-FIBONACCI DISTRIBUTIONS

We define the n^{th} t-Fibonacci distribution to be the t dimensional vector $({}_1U_n, {}_2U_n, \cdots, {}_tU_n) = V_n$. Using vector addition in the usual sense (add corresponding components), it is clear that

$$V_n = V_{n-1} + V_{n-2} + \cdots + V_{n-t} . \tag{8}$$

That is, the V_n's satisfy the t-Fibonacci equation. It is clear that the sum of the components of V_n is ${}_{\Sigma}U_n$.

We will say that V is the t-distribution for the integer K if and only if

$$V = \sum_j C_j V_j ,$$

where C_j is the representation for K.

K	Representation	4-Distribution
0	000|0000	(0, 0, 0, 0)
1	000|1000	(0, 0, 0, 1)
2	000|1100	(0, 0, 1, 1)
3	000|1110	(0, 1, 1, 1)
4	001|0000 ← 000|1111	(1, 1, 1, 1)
5	001|1000	(1, 1, 1, 2)
6	001|1100	(1, 1, 2, 2)
7	010|0000 ← 001|1110	(1, 2, 2, 2)
8	010|1000	(1, 2, 2, 3)
9	010|1100	(1, 2, 3, 3)
10	010|1110	(1, 3, 3, 3)
11	011|0000 ← 010|1111	(2, 3, 3, 3)
12	011|1000	(2, 3, 3, 4)
13	100|0000 ← 011|1100	(2, 3, 4, 4)

Fig. 2 Representation and 4-Distribution of $0 \leq K \leq 13$

The Counting Algorithm makes it clear that the t-distribution for $K + 1$ is obtained from the t-distribution for K simply by adding 1 to the j^{th} component where j is the left-most zero position in the bottom t positions of the representation for K. See Fig. 2.

Corresponding to each non-negative integer K, we now have two quantities, the representation of K in the t-Fibonacci number system and the t-distribution for K. Given the (representation) (t-distribution) for K we can calculate the (representation) (t-distribution) for $K + 1$. If K is ${}_{\Sigma}U_n$ for some n then the representation for K has but one 1 bit and the t-distribution has ${}_iU_n$ for its i^{th} component (the t-distribution is a "row" in a tabulation like that in Fig. 1). Given the t-distribution for some ${}_{\Sigma}U_n$ we can easily calculate the t-distribution for ${}_{\Sigma}U_{n+1}$ by means of Eqs. (3) and (4).

We now ask what is the effect of applying Eqs. (3) and (4) to an arbitrary t-distribution. In particular, is the result a t-distribution, and, if so, for which integer? Let X be the t-distribution for K and let the i^{th} component of $f(X)$ be

$$f(X)_i = \begin{cases} X_t & \text{if } i = 1 \\ X_{i-1} + X_t & \text{if } 1 < i \leq t \end{cases}$$

(the subscripts refer to the component positions of the t-dimensional vectors). Notice that f is a linear function on the t-dimensional vector space. Now,

$$X = \sum_{j=1}^{\infty} C_j V_j ,$$

where the C_j's are the coefficients in the representation of K.

$$f(x) = f\left(\sum_{j=1}^{\infty} C_j V_j\right) = \sum_{j=1}^{\infty} C_j f(V_j) = \sum_{j=1}^{\infty} C_j V_{j+1} = \sum_{j=2}^{\infty} C_{j-1} V_j .$$

Let $D_1 = 0$ and $D_{j+1} = C_j$ so we have

$$f(X) = \sum_{j=1}^{\infty} D_j V_j .$$

Since D_j satisfies (a) through (d), f(X) is the t-distribution for the integer represented by the D_j's. In other words, applying f to the t-distribution for K yields the t-distribution for an integer whose representation in the t-Fibonacci number system is the representation of K shifted left one place. Observe, in Fig. 2, the entries for 5 and 11. Applying f to the 4-distribution of 5 yields the 4-distribution of 11. The representation of 5 shifted left one place yields the representation of 11.

Since it is a non-singular linear transformation, f is invertible. Considering g(X) where

$$g(X)_j = \begin{cases} X_1 & \text{if } i = t \\ X_{i+1} - X_1 & \text{if } 1 \leq i < t \end{cases} .$$

The inverse of f is clearly g. Applying g to the t-distribution of the t-distribution of the integer whose representation is the representation of K shifted right one place provided condition (c) is not violated by the right shift operation.

Since f is not onto, the domain of g must be restricted to coincide with the range of f. Condition (c) will not be violated under precisely this condition. Thus the composition gf is the identity function.

PART II

5. SORTING BY MERGING

In data-processing by digital computers, it very often proves to be convenient or essential to arrange large volumes of data into a linear sequence. The unit of data is called a record. Each record has associated with it a number called its key. The process of arranging the records into a sequence (or file) so that the key values are non-decreasing is called sorting.

A utility company will keep its customer file in ascending order by customer number. The incoming utility bill payments will be sorted into ascending order by customer number. The customer file (particularly the customer's balance) can now be adjusted to account for the payment. With both files in order by customer number, this can be accomplished without undue searching through either file.

The sorting of large files is not particularly simple. Usually the files are much too large to be held in the memory of the computer, and they must be recorded on some linear medium such as magnetic tape. The primary method of sorting such external files depends on the technique of merging. If we have two files already sorted into order, we can combine, or merge, these into one file. We do this as follows. Call the two files to be merged A and B and the resulting file C. File C is initially empty. We look at the first records of A and B and select the one with the smallest key. We transfer this record from the input file to C, removing it from the input file. We repeat this process until both A and B are exhausted. File C will now contain the records from A and B and will be in ascending order. See Fig. 3.

We will say that a file in ascending order by its key is a sorted file. The idea behind merge sorting is to begin with many small sorted files; perhaps

A	B	C
2	4	2
3	7	3
5	8	4
6	10	5
9		6
11		7
		8
		9
		10
		11

Fig. 3 Merger of A and B to form C

each contains but one record. By repeated mergers, the average length of the sorted files grows, and, more importantly, the number of files decreases after each merger. Since the number of files cannot increase indefinitely, the process must terminate with one file in sorted order.

We propose to look into the details of this process, particularly a merge sorting technique called polyphase sorting. Let us begin by describing a simpler technique called "balanced symmetric sorting." Suppose initially that we have twenty-seven files arranged on six magnetic tapes as follows:

tapes	1	2	3	4	5	6
files	9	9	9	0	0	0

.

That is, tapes 1, 2, and 3 contain nine files each (one after the other), while tapes 4, 5, and 6 are empty. By an obvious extension of the described merging process, we can merge together three files at once. Suppose we merge the files that appear first on tapes 1, 2, and 3. This new file is placed on tape 4 so that we have twenty-five files.

1	2	3	4	5	6
8	8	8	1	0	0

.

By their nature, tapes 1, 2, and 3 are in position to read their second files and tape 4 is positioned to write a file after the one just constructed. Tape 4 is not in a convenient position to re-read the file just written. Files from 1, 2, and 3 are merged again, and the resulting file is written on tape 5. One more merger (the result to tape 6) gives us the twenty-one files.

1	2	3	4	5	6
6	6	6	1	1	1

We make six more mergers, writing the resulting files cyclically on tapes 4, 5, and 6, yielding nine files.

1	2	3	4	5	6
0	0	0	3	3	3

Each file is three times as long as the originals. We rewind all six tapes and make three mergers yielding

1	2	3	4	5	6
1	1	1	0	0	0

We rewind again and one merger gives us

1	2	3	4	5	6
0	0	0	1	0	0

All the records appear on tape 4 as one sorted file. It should be clear that the number of passes (i.e., the number of times each record is processed) is

$$\log_{\frac{(t+1)}{2}} (f)$$

where $t + 1$ is the number of available tapes and f is the number of files. The more tapes, the faster it goes. Figure 4 tabulates a sort of forty-nine files on five tapes. Usually, the number of files and the number of tapes don't come out even as in the example above, and some "fudging" is needed. For a more complete discussion of merge sorting, see [4] and [5].

Tapes	1	2	3	4	5
	16	16	17	0	0
	0	0	0	8	9
	5	6	6	0	0
	0	0	0	3	3
	1	1	1	0	0
	0	0	0	0	1

Fig. 4 A Sort of 49 Files on Five Tapes

6. POLYPHASE SORTING

Let us try to construct a four-way merge process with just five tapes. The natural thing to do is work the problem backwards. Suppose we wish to end with just one file on tape 5.

	tapes				
pass	1	2	3	4	5
	0	0	0	0	1

We must have gotten here by merging four files, one each on tapes 1, 2, 3, and 4.

	tapes				
pass	1	2	3	4	5
5	1	1	1	1	0

one each from 1, 2, 3, and 4 to 5. How did we get here? We could get the one file on tape 4 by a four-way merger of one file each from tapes 1, 2, 3, and 5.

	tapes				
pass	1	2	3	4	5
6	2	2	2	0	1

one each from 1, 2, 3, and 5 to 4. Notice that the sorting process leaves files on tapes 1, 2, and 3 and rewinds 5. The key idea of this process, called polyphase sorting [5] is not to exhaust all of the input files available. The next few steps backward are:

pass	tapes 1	2	3	4	5	
7	4	4	0	2	3	2 each from 1, 2, 4, 5 to 3
8	8	0	4	6	7	4 each from 1, 3, 4, 5 to 2
9	0	8	12	14	15	8 each from 2, 3, 4, 5 to 1
10	15	23	27	29	0	15 each from 1, 2, 3, 4 to 5
11	44	52	56	0	29	29 each from 1, 2, 3, 5 to 4

At each step, we four-way merge as many files as are available on the tape with the smallest number of files, then rewind this tape. We leave the residue on the other tapes for subsequent passes.

To simplify the analysis of this process, we can give the tapes "logical" names. We will select the names W and L_1, L_2, L_3, L_4. The tape we will write on is designated as W. The tape with the smallest number of files is L_1 and L_2 is the tape with the next smallest number up to L_4, the tape with the largest number of files. The correspondence of logical names to tape unit numbers was as follows for the previous example.

pass	tapes 1	2	3	4	5
4	W	L_1	L_2	L_3	L_4
5	L_1	L_2	L_3	L_4	W
6	L_2	L_3	L_4	W	L_1
7	L_3	L_4	W	L_1	L_2
8	L_4	W	L_1	L_2	L_3
9	W	L_1	L_2	L_3	L_4
10	L_1	L_2	L_3	L_4	W
11	L_2	L_3	L_4	W	L_1

At the end of each pass, the logical labels shift right one with respect to the physical numbers.

It will be much more convenient to organize the tableau containing the number of files per tape per pass by logical names rather than physical tape numbers. The example is given in Fig. 5.

Usually the W column is dropped, since it is always zero. Compare Fig. 5 with Fig. 1 in Part 1.

pass	L_1	L_2	L_3	L_4	W
0	-1	-1	-1	1	0
1	1	0	0	0	0
2	0	1	0	0	0
3	0	0	1	0	0
4	0	0	0	1	0
5	1	1	1	1	0
6	1	2	2	2	0
7	2	3	4	4	0
8	4	6	7	8	0
9	8	12	14	15	0
10	15	23	27	29	0
11	29	44	52	56	0

Fig. 5 A Polyphase Sort of 181 Files

The sorting rule for each pass is clear. We four-way merge n times, where n is the number of files on L_1, n files are written on W, which becomes L_4 in the next pass. We rewind L_1 and it becomes W (since it is empty) on the next pass. Now L_1 has lost n files and becomes L_{i-1} on the next pass. Hence if $\#L_i$ is the number of files on L_i at pass n we have the sorting rule

$$\#_{n-1}L_4 = \#_nL_1$$
$$\#_{n-1}L_{i-1} = \#_nL_1 - \#_nL_1 \qquad 1 < i \leq 4 .$$

Applying these relations, we can fill in the tableau for $0 \leq n < 4$.

To construct the tableau in the opposite direction, it is clear that

$$\#_nL_1 = \#_{n-1}L_4$$
$$\#_nL_i = \#_{n-1}L_{i-1} + \#_{n-1}L_4 \qquad 1 < i \leq t$$

for

$$1 \leq n \leq t \qquad \#_nL_i = \delta_{in} .$$

7. A DISTRIBUTION AND CONTROL ALGORITHM FOR POLYPHASE SORTING

It is at once clear that $\#_n L_i$ is ${}_iU_n$ and that row n of the tableau placed in vector form is the t-distribution for ${}_\Sigma U_n$. Note that we have ${}_\Sigma U_n$ files at pass n.

We now raise two related problems. How do we adjust if the number of files to be sorted is not some ${}_\Sigma U_n$? And, in general, how do we determine the initial distribution of the files over t tapes? The answer to this second question is complicated by the fact that in general, we will not know how many files are to be sorted. The files will initially be contained on some other tape and we will read them one by one and distribute them over the input tapes. We must distribute them in such a manner that at any time we will be prepared to carry out the polyphase algorithm. This is because we won't know which file is last until we come upon it. This distribution problem is discussed in 8 .

The following algorithm is proposed for calculating the initial distribution. We will number the files in sequence and represent the number in the t-Fibonacci number system. As we distribute a file we will obtain its number by counting up by one the number representation of the previous file. This involves inserting a 1 in one of the lower t positions (say position j) of the representation of the number of the previous file and adjusting for carries. Refer back to the Counting Algorithm. The new file to be distributed is then copied to tape j. At each step, then, the distribution of files is the t-distribution for the number of files thus far distributed.

If we distribute 11 files on four tapes, Fig. 2 indicates that the distribution would be (2, 3, 3, 3). If we take one pass on the polyphase sort algorithm we obtain 5 files distributed (1, 1, 1, 2). (Two files each are merged from the four tapes, leaving three tapes with one file and creating a new tape with two files.) We can keep track of this by shifting the representation right one place. The representation for 11 is $011|0000$ and the representation for 5 is $01|1000$. Another pass of the polyphase algorithm gives us two files with the 4-distribution (0, 0, 1, 1) and the representation $0|1100$.

If we try another pass, nothing happens since L_i contains no files. Also, the shift would give the unacceptable representation $|0110$ (this violates (c)). We instead should add dummy files to tapes L_1 and L_2. Dummy files are files with no records in them. By (d), this promotes the representation to

1|0000 and the distribution to (1, 1, 1, 1). One more pass produces the representation 0|1000 and the distribution (0, 0, 0, 1), and we are done. Actually, this last merger was only two-way, but we pretended it was four-way!

The rule then is that when a shift of the representation to the right is not allowed because a zero would shift into position t, dummy files should be added to the indicated tapes. With this slight adjustment, any number of files may be sorted. Figure 6 gives a blow-by-blow account of a five-tape, four-way merger of nine files.

Operation	Representation	Distribution	Comment
distribute	000|1000	(0, 0, 0, 1)	to tape 4
distribute	000|1100	(0, 0, 1, 1)	to tape 3
"	000|1110	(0, 1, 1, 1)	to tape 2
"	001|0000	(1, 1, 1, 1)	to tape 1
"	001|1000	(1, 1, 1, 2)	to tape 4
"	001|1100	(1, 1, 2, 2)	to tape 3
"	010|0000	(1, 2, 2, 2)	to tape 2
"	010|1000	(1, 2, 2, 3)	to tape 4
"	010|1100	(1, 2, 3, 3)	to tape 3
sort	001|1000	(1, 1, 1, 2)	dummy files added to 1, 2
sort	000|1100	(0, 0, 1, 1)	
sort	000|1000	(0, 0, 0, 1)	dummy files added to 1, 2

Fig. 6

A little thought will produce a slightly more economical method of adding dummy files, but we leave this to the reader's imagination.

8. CONCLUSION

We have presented a generalization of the Fibonacci numbers and developed some of their salient properties. In particular, we proved an extension of Zeckendorf's theorem, and used this to develop the t-Fibonacci positional number system. We investigated the processes of counting and shifting in this number system.

In Part 2, we reviewed the basics of merge sorting and polyphase sorting and went on to use the theory of Part 1 to develop a new initial distribution and merge-control algorithm.

It seems clear that this sort of analysis can be carried out for many other merge sorting schemes (e.g., oscillating [7] or cascade sort [5]). With each sorting scheme, we should be able to associate a number system. This number system should be such that one pass of the merger corresponds to shifting the representation of the number of files right, one place. The initial distribution of files is controlled by the mechanics of counting and imperfect distributions are adjusted to prevent shifting digits off the right end of the count.

ACKNOWLEDGEMENT

The author is indebted to D. E. Knuth for many valuable suggestions.

REFERENCES

1. J. L. Brown, Jr., "Zeckendorf's Theorem and Some Applications," Fibonacci Quarterly, Vol. 2, No. 3, pp. 163-168.
2. W. C. Carter, "Mathematical Analysis of Merge-Sorting Techniques," Proc. IFIP Congress 62, Munich 1962.
3. D. E. Daykin, Journal London Math. Soc., 35 (1960), pp. 143-160.
4. E. H. Friend, "Sorting on Electronic Computer Systems," J. Assoc. for Computing Machinery, Vol. 3 (1956), p. 134.
5. C. C. Gotlieb, "Sorting on Computers," Comm. Association for Computing Machinery, Vol. 6, No. 5, pp. 194-201.
6. R. L. Gilstad, "Polyphase Merge Sorting — An Advanced Technique," Proc. Eastern Joint Computer Conference (1960).
7. D. E. Knuth, CACM 6 (1963), pp. 555-563.
8. W. D. Malcolm, "String Distribution for the Polyphase Sort," Comm. Association for Computing Machinery, Vol. 6, No. 5, pp. 217-220.
9. A. G. Mendoza, CACM 5 (1962), pp. 502-504.
10. E. P. Miles, Jr., American Math. Monthly, 67 (1960), pp. 745-752.
11. V. Schlegel, El Progreso Mat. 4 (1894), pp. 171-174.
12. S. Sobel, "Oscillating Sort-A New Merge Sorting Technique," J. Assoc. for Computing Machinery, Vol. 9, No. 3, pp. 371-374.

★ ★ ★ ★ ★

FACTORIZATION OF FIBONACCI NUMBERS

D. E. DAYKIN
University of Malaya, Kuala Lampur
and
L. A. G. DRESEL
University of Reading, England

1. INTRODUCTION AND SUMMARY

The Fibonacci numbers F_n may be defined by the recurrence relation $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$ with $F_0 = 0$ and $F_1 = 1$. The factors of the first 60 Fibonacci numbers were published by Lucas (with only two errors) in 1877 [1], and recently a table of factors of F_n for $n \leq 100$ has been published by the Fibonacci Association in [2].

If F_z is the smallest Fibonacci number divisible by the prime p, then $z = z(p)$ is defined as the entry point (or rank) or p in the Fibonacci sequence; furthermore p divides F_n if and only if n is divisible by $z(p)$, and there are rules for determining what power of p will divide such an F_n ([3], p. 396).

To find the entry point $z(p)$ for a given p, we can generate the Fibonacci sequence modulo p until we obtain an element $F_z \equiv 0$; on a computer this process involves only additions and subtractions, and we work throughout with numbers less than $2p$. Tables of entry points have been published by Brother U. Alfred [4], and have also been inverted to give p as a function of z. We extended the inverted table up to $p = 660{,}000$ by restricting our search to the first 256 Fibonacci numbers, i.e., to $z \leq 256$, and by this means we were able to give complete factorizations of 36 numbers F_n with $n > 100$ in [5].

In the present paper we shall adopt the alternative approach of fixing z and searching for primes for which this z is the entry point. In Sections 3 and 4 we shall prove the following theorems:

Theorem 1. If z is the entry point of a prime $p > 5$ then

(i) if z is odd, we have either

(a) $p = 4rz + 1$ and $p \equiv 1, 29, 41, 49 \pmod{60}$,

or (b) $p = (4r+2)z - 1$ and $p \equiv 13, 17, 37, 53 \pmod{60}$;

(ii) if $z \equiv 2 \pmod 4$, we have

$$p = rz + 1 \quad \text{and} \quad p = 1, 11, 19, 29 \pmod{30};$$

(iii) if $z \equiv 0 \pmod 4$, we have either

(a) $p = 2rz + 1$ and $p = 1, 29, 41, 49 \pmod{60}$,

or (b) $p = (2r + 1)z - 1$ and $p = 7, 23, 43, 47 \pmod{60}$,

where in all cases r is an integer.

Theorem 2. $2z(p)$ divides $p \pm 1$ if and only if $p \equiv 1 \pmod 4$.

In Section 5 we describe how we have used Theorem 1 as the basis of a computer program for factorizing Fibonacci numbers, and in Section 6 we give some numerical results obtained in this way.

2. SOME PRELIMINARY RESULTS

The Lucas numbers L_n are defined by the same recurrence relation as the Fibonacci numbers F_n, namely $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$, but with $L_0 = 2$ and $L_1 = 1$. We shall require the following well known identities:

$$F_{2n} = F_n L_n \tag{1}$$

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

$$L_n^2 - L_{n-1}L_{n+1} = (-1)^n 5 \ . \tag{3}$$

When p is an odd prime and m is an integer prime to p, the Legendre symbol (m/p) is defined to be $+1$ if m is a quadratic residue of p, i.e., if the equation

$$x^2 \equiv m \pmod p$$

has a solution in integers; whereas if there is no such solution, (m/p) is defined to be -1. It can be shown (ref. 6, Chap. 6) that, for $p > 5$,

$$(-1/p) = 1 \quad \text{if and only if} \quad p \equiv 1 \pmod 4 \tag{4}$$

(5a) $(5/p) = 1$ if and only if $p \equiv 1$ or $9 \pmod{10}$

(5b) $(5/p) = -1$ if and only if $p \equiv 3$ or $7 \pmod{10}$

(6) $(-5/p) = 1$ if and only if $p \equiv 1, 3, 7,$ or $9 \pmod{20}$.

It can also be shown (e.g., using Theorem 180, ref. 6), that if z is the Fibonacci entry point of p, then (for $p > 5$)

(7) $$p - (5/p) \equiv 0 \pmod{z} .$$

This leads to

Lemma 1

(8a) $p = qz + 1$ if $p \equiv 1$ or $9 \pmod{10}$,

(8b) $p = qz - 1$ if $p \equiv 3$ or $7 \pmod{10}$,

where z is the entry point of p and q is an integer.

We shall further use the fact that if p is a prime greater than 5, then

(9) $p \equiv 1, 7, 11, 13, 17, 19, 23,$ or $29 \pmod{30}$,

since otherwise p would be divisible by 2, 3, or 5.

If we reduce the Fibonacci sequence (for which $F_0 = 0$, $F_1 = 1$) modulo p, we obtain a periodic sequence. The period $k = k(p)$ is the smallest integer k for which

$$F_k \equiv 0 \pmod{p} \quad \text{and} \quad F_{k+1} \equiv 1 \pmod{p} .$$

It is clear that the entry point $z(p)$ will divide the period $k(p)$, and the following results have been proved by Oswald Wyler [7]:

(10a) $k(p) = z(p)$ if $z(p) \equiv 2 \pmod{4}$,

(10b) $k(p) = 2z(p)$ if $z(p) \equiv 0 \pmod{4}$,

(10c) $k(p) = 4z(p)$ if $z(p)$ is odd.

We shall also use a result proved by D. D. Wall (ref. 8, Theorems 6 and 7), namely

(11a) $k(p)$ divides $p - 1$ if $p \equiv 1$ or $9 \pmod{10}$,

(11b) $k(p)$ divides $2(p + 1)$, but not $p + 1$, if $p = 3$ or $7 \pmod{10}$.

3. PROOF OF THEOREM 1

To prove Theorem 1 we have to consider separately the three cases of z odd, z twice an odd integer, and z divisible by 4, where $z = z(p)$ is the entry point of a prime $p > 5$.

(i) We first consider the case of z odd and prove

Lemma 2. If z is odd, then $p \equiv 1 \pmod{4}$.

To prove this, take $n - 1 = z$ in the identity (2); then $n - 1$ is odd, and (by definition of z) p divides F_{n-1}, so that we have $(F_n)^2 \equiv -1 \pmod{p}$ it follows, as stated in (4), that $p \equiv 1 \pmod{4}$.

Combining this result with that of Lemma 1 we see that when z is odd we have either

(a) $p = 4rz + 1$ and $p \equiv 1$ or $9 \pmod{10}$,

or

(b) $p = (4r + 2)z - 1$ and $p \equiv 3$ or $7 \pmod{10}$.

Part (i) of Theorem 1, as stated in the introduction, then follows by using the result (9) and selecting those residues modulo 60 which satisfy $p \equiv 1 \pmod{4}$.

(ii) Next, we consider the case where $z = 2s$ and s is an odd integer. In this case p divides F_{2s} but not F_s, so that it follows from the identity (1) that p divides L_s. Taking $n - 1 = s$ in the identity (3) we have $L_n^2 \equiv 5 \pmod{p}$, and it follows, as stated in (5a), that $p \equiv 1$ or $9 \pmod{10}$. Using this result together with Lemma 1 we obtain

Lemma 3. If z is twice an odd integer, then

$$p = qz + 1 \quad \text{and} \quad p \equiv 1 \text{ or } 9 \pmod{10}.$$

Part (ii) of Theorem 1 now follows by using the result (9). Moreover, Lemma 3 establishes the following result which was conjectured by A. C. Aitken (private communication to R. Rado in 1961):

Theorem 3. If p is a prime then $d \equiv 1 \pmod{p}$ for any divisor d of L_p.

(iii) Finally we consider the case where $z = 2s$ and s is an even integer. As before, it follows from (1) that p divides L_s, but taking $n - 1 = s$ in (3) we now obtain $L_n^2 \equiv -5 \pmod{p}$ since n is odd. Using the result (6) we deduce that $p \equiv 1, 3, 7,$ or $9 \pmod{20}$, and combining this with Lemma with the result (9) we have that when $z \equiv 0 \pmod{4}$ either

$$\text{(a)} \quad p = qz + 1 \quad \text{and} \quad p \equiv 1, 29, 41, 49 \pmod{60},$$

or

$$\text{(b)} \quad p = qz - 1 \quad \text{and} \quad p \equiv 7, 23, 43, 47 \pmod{60}.$$

Since the result (10b) applies to these cases, the period k is now given by $k = 2z$. Applying (11a), we see that in case (a), q must be an even integer, say $q = 2r$. Similarly, applying (11b) we see that in case (b) q must be an odd integer, say $2r + 1$. This establishes part (ii) of Theorem 1.

In proving Theorem 1 we have used only the identities (1), (2) and (3). It is interesting to note that, although we applied similar techniques to many other identities, these did not lead to any further significant results.

4. PROOF OF THEOREM 2

To prove that for $p > 5$, $2z(p)$ divides $p - (5/p)$ if and only if $p \equiv 1 \pmod{4}$, we have to consider the three cases as before.

(i) When z is odd, we have by Lemma 2 that $p \equiv 1 \pmod{4}$; we also know from (7) that z divides $p - (5/p)$, which is an even number, and hence when z is odd $2z$ divides $p - (5/p)$.

(ii) When z is twice an odd integer, we have by Lemma 3 that

$$p = qz + 1 \quad \text{and} \quad p \equiv 1 \text{ or } 9 \pmod{10}.$$

It follows that $2z$ divides $p - 1$ if and only if q is even, and this condition is equivalent to $p \equiv 1 \pmod{4}$ in this case.

(iii) When $z \equiv 0 \pmod{4}$, we have already proved (at the end of Section 3) that either

(a) $p = qz + 1$ with q an even integer,

or

(b) $p = qz - 1$ with q an odd integer.

In case (a) we have $p \equiv 1 \pmod 4$ and $2z$ divides $p - 1$, whereas in case (b) we have $p \equiv 3 \pmod 4$ and $2z$ does not divide $p + 1$.

This completes the proof of Theorem 2.

A restricted form of this theorem, namely $2z(p)$ divides $p \pm 1$ if $p \equiv 1 \pmod 4$, has recently been proved by R. P. Backstrom ([9], lemmas 4 and 6).

5. APPLICATION TO THE FACTORIZATION OF FIBONACCI NUMBERS

Consider now the problem of finding the prime factors of F_n for a given n. If n is not prime, then F_n will have some improper factors p whose entry points $z(p)$ divide n. Given n in the range $100 < n \leq 200$, it is a simple matter to consider all the divisors d of n and use the known factorizations of F_d for $d \leq 100$ (as given in [2]) to list all the improper factors of F_n. The remaining factors p will then be proper factors such that $z(p) = n$, and these must satisfy the conditions of Theorem 1 with $z = n$.

Consider first the case of n odd. Our computer program calculates F_n and then divides it in turn by all the improper factors of F_n (with suitable multiplicaties) which are supplied as data. We are then left with a quotient Q_n whose factors p must have $z(p) = n$. To determine these factors, we let the computer generate numbers N (not necessarily prime) satisfying the conditions for p in Theorem 1(i) with $z = n$. These numbers N in general fall into 8 residue classes modulo $60n$, but it was found that when n is divisible by 3, 5, or 15 the number of residue classes goes up to 12, 10, or 15, respectively. For each n these residue classes were determined by the computer in accordance with Theorem 1 and the numbers N were then generated systematically from the lowest upward. For each N the program tests whether Q_n is divisible by N, and if it is it prints N as a factor and replaces Q_n by Q_n/N. Any factor N found in this way will be a prime, for if not, N would be the product of factors which should have been divided out from F_n or Q_n at an earlier stage of the progress. Finally, when N becomes sufficiently large for N^2 to exceed the current value of Q_n, we can

stop the process and conclude that Q_n is prime; for if not, we would have $Q_n = N_1N_2 < N^2$ which implies that Q_n has a factor smaller than N, and any such factor would have been divided out at an earlier stage.

In the case of n even, say $n = 2m$, we can proceed slightly differently on account of the identity

$$F_{2m} = F_mL_m .$$

The computer program now generates L_m and our object is to factorize this. We need only supply as data those improper factors of F_n which do not also divide F_m, and dividing L_m by these factors we obtain the quotient Q_n. According as $\frac{1}{2}n = m$ is odd or even we use Theorem 1 (ii) or 1 (iii) to generate numbers N satisfying the conditions for p when $z = n = 2m$. It was found that these numbers N in general fall into 8, 10, or 12 residue classes modulo 30n, though in some cases 20 and even 30 residue classes occurred.

6. NUMERICAL RESULTS

A program on the lines described above was run on the Elliott 803 computer at Reading University, using multi-length integer arithmetic. In addition to the factorizations listed by us in [5], the following further factorizations were obtained (the factors before the asterisk being improper factors):

F103 = 519121 x 5644193 x 512119709
F115 = 5 x 28657 * 1381 x 2441738887963981
F133 = 13 x 37 x 113 * 3457 x 42293 x 351301301942501
F135 = 2 x 5 x 17 x 53 x 109 x 61 x 109441 * 1114769954367361
F141 = 2 x 2971215073 * 108289 x 1435097 x 142017737
F149 = 110557 x 162709 x 4000949 x 85607646594577

We also factorized a further 17 numbers F_n with n even, and because of the identity $F_{2m} = F_mL_m$ it will be sufficient to list the prime factors of the corresponding Lucas numbers L_m (those factors that are improper factors of F_{2m} are placed before the asterisk):

L61 = 5600748293801 (prime)
L62 = 3 * 3020733700601
L68 = 7 * 23230657239121
L71 = 688846502588399 (prime)
L73 = 151549 x 11899937029
L76 = 7 * 1091346396980401
L77 = 29 x 199 * 229769 x 9321929
L80 = 2207 * 23725145626561
L82 = 3 * 163 x 800483 x 350207569
L85 = 11 x 3571 * 1158551 x 12760031
L91 = 29 x 521 * 689667151970161
L92 = 7 * 253367 x 9506372193863
L93 = 2^2 x 3010349 * 63799 x 35510749
L94 = 3 * 563 x 5641 x 4632894751907
L96 = 2 x 1087 x 4481 * 11862575248703
L98 = 3 x 281 * 5881 x 61025309469041
L100 = 7 x 2161 * 9125201 x 5738108801

In each case the process was taken sufficiently far to ensure that the final quotient is a prime, as explained in the previous section. In the case of F115 this involved testing trial factors N almost up to 5×10^7.

REFERENCES

1. Edouard Lucas, Bull. di Bibl. e di St. d. Sc. Mat. e Fis., Vol. 10 (March 1877), pp. 129-170.
2. Brother U. Alfred, An Introduction to Fibonacci Discovery, The Fibonacci Association, 1965.
3. L. E. Dickson, History of the Theory of Numbers, Carnegie Institution, Vol. 1, 1919.
4. Brother U. Alfred, Tables of Fibonacci Entry Points, The Fibonacci Association, 1965.
5. L. A. G. Dresel and D. E. Daykin, "Factorization of 36 Fibonacci Numbers F_n with $n > 100$," Fibonacci Quarterly, Vol. 3, pp. 232-233, October, 1965.

[Continued on page 82.]

GENERALIZED FIBONACCI K-SEQUENCES

HYMAN GABAI
York College (CUNY) and University of Illinois (UICSM)

1. INTRODUCTION

For $k \geq 2$, the Fibonacci k-sequence $F(k)$ may be defined recursively by

$$f_n = 0 \quad (n \leq 0), \quad f_1 = 1, \quad f_n = \sum_{i=n-k}^{n-1} f_i \quad (n > 1).$$

A generalized Fibonacci k-sequence $A(k)$ may be constructed by arbitrarily choosing $a_1, a_0, a_{-1}, \cdots, a_{2-k}$, and defining

$$a_n = 0 \quad (n < 2 - k), \quad a_n = \sum_{i=n-k}^{n-1} a_i \quad (n > 1).$$

In this paper, some well-known properties of $F(2)$ (see [1] and [8]) are generalized to the sequences $A(k)$. For some properties of $F(k)$, see [4], [6], and [7]. The sequences $A(3)$ are investigated in [9].

The pedagogical values of introducing Fibonacci sequences in the classroom are well known. (See, for example [3], pp. 336-367.) It seems possible that the generalizations described in this paper may suggest some areas of investigation suitable for high school and college students. (See, for example [5].) For once a theorem concerning $F(2)$ has been discovered, one may search for corresponding theorems concerning $A(2)$, $F(3)$, $A(3)$, $\cdots$ and finally $F(k)$ and $A(k)$. (See [2].)

2. THEOREMS

The first theorem is a "shift formula" needed in the proof of Theorem 6.

Theorem 1. For $n \geq 2$, $a_{n+1} = 2a_n - a_{n-k}$.

Theorem 2 is a generalization of the theorem that any two consecutive terms of $F(2)$ are relatively prime.

Theorem 2. For $n \geq 2$, every common divisor of

$$a_n, \quad a_{n+1}, \quad a_{n+2}, \quad \cdots, \quad a_{n+k-1}$$

is a divisor of $a_2, a_3, \cdots, a_{n-1}$.

Some summation theorems are given in Theorems 3, 4, and 5.

Theorem 3. (a) For $n \geq 1$ and $m \geq 1$,

$$\sum_{i=0}^{n} a_{ki+m+1} = \sum_{i=m+1-k}^{kn+m} a_i .$$

(b) For $n \geq 1$,

$$\sum_{i=1}^{n} a_{ki} = \sum_{i=0}^{kn-1} a_i .$$

(c) For $n \geq 1$,

$$a_{kn} - a_0 = \sum_{\substack{1<i<kn-1 \\ i \not\equiv 0 \pmod{k}}} a_i$$

Theorem 4. For $n \geq 2 - k$,

$$\sum_{i=2-k}^{n} a_i = \frac{1}{k-1}\left(a_{n+k} - a_1 + \sum_{i=1}^{k-2} i a_{-i} - \sum_{i=1}^{k-2} (k - i - 1)a_{n+i}\right) .$$

Theorem 5. For $n \geq 1$,

$$\sum_{i=1}^{n} a_i^2 = a_n a_{n+1} - a_1 a_0 - \sum_{j=2}^{k-1} \sum_{i=1}^{n} a_i a_{i-j} .$$

Theorems 6, 7, and 8 show relations between F(k) and A(k).

Theorem 6. For $n \geq 1$ and $m \geq 1$,

$$a_{n+m} = \sum_{j=1}^{k} \left(a_{n-k+j} \sum_{i=1}^{j} f_{m-j+1} \right) .$$

Theorem 7. Let d_m be the greatest common divisor of

$$f_m, \ f_{m-1}, \ \cdots, \ f_{m-k+2} .$$

If $m \geq 1$, m divides n, and d_m divides a_m, then d_m divides a_n.

Theorem 8. Let r be the largest root of the polynomial equation

$$x^k - \sum_{i=0}^{k-1} x^i = 0 .$$

Then

(a) $$\lim_{n \to \infty} \left(\frac{a_n}{f_n} \right) = \frac{1}{r^k} \sum_{j=2}^{k+1} \left(a_{j-k} \sum_{i=1}^{j-1} r^{k-i} \right) ,$$

and

(b) $$\lim_{n \to \infty} \left(\frac{a_{n+1}}{a_n} \right) = r .$$

3. PROOFS OF THEOREMS

Theorem 1 follows directly from the definition of A(k). For, if $n \geq 2$, then

$$a_{n+1} = \sum_{i=n-k+1}^{n} a_i = \sum_{i=n-k}^{n-1} a_i + a_n - a_{n-k} = 2a_n - a_{n-k} .$$

To prove Theorem 2, suppose that d is a common divisor of a_n, a_{n+1}, $\cdots$, a_{n+k-1}. Since

$$a_{n+k-1} = \sum_{i=n-1}^{n+k-2} a_i = a_{n-1} + \sum_{i=n}^{n+k-2} a_i ,$$

it follows that d also divides a_{n-1}. It follows, by induction, that d divides a_{n-2}, $\cdots$, a_2.

For the proof of Theorem 3(a), choose any integer $m \geq 1$. Now Theorem 3(a) holds for $n = 1$ because

$$\sum_{i=0}^{1} a_{ki+m+1} = a_{m+1} + a_{k+m+1}$$

$$= \sum_{i=m+1-k}^{m} a_i + \sum_{i=m+1}^{k+m} a_i = \sum_{i=m+1-k}^{k+m} a_i .$$

Furthermore, if Theorem 3(a) holds for $n = p$, then it holds for $n = p + 1$ because we then have

$$\sum_{i=0}^{p+1} a_{ki+m+1} = a_{k(p+1)+m+1} + \sum_{i=0}^{p} a_{ki+m+1}$$

$$= \sum_{i=kp+m+1}^{k(p+1)+m} a_i + \sum_{i=m+1-k}^{kp+m} a_i$$

$$= \sum_{i=m+1-k}^{k(p+1)+m} a_i .$$

Hence Theorem 3(a) holds for $n \geq 1$, $m \geq 1$.

In the proof of Theorem 3(b), we apply Theorem 3(a), choosing $m = k - 1$:

$$\sum_{i=0}^{n} a_{ki+k} = \sum_{i=0}^{kn+k-1} a_i \ .$$

Theorem 3(b) follows since the left side of this equation is equal to

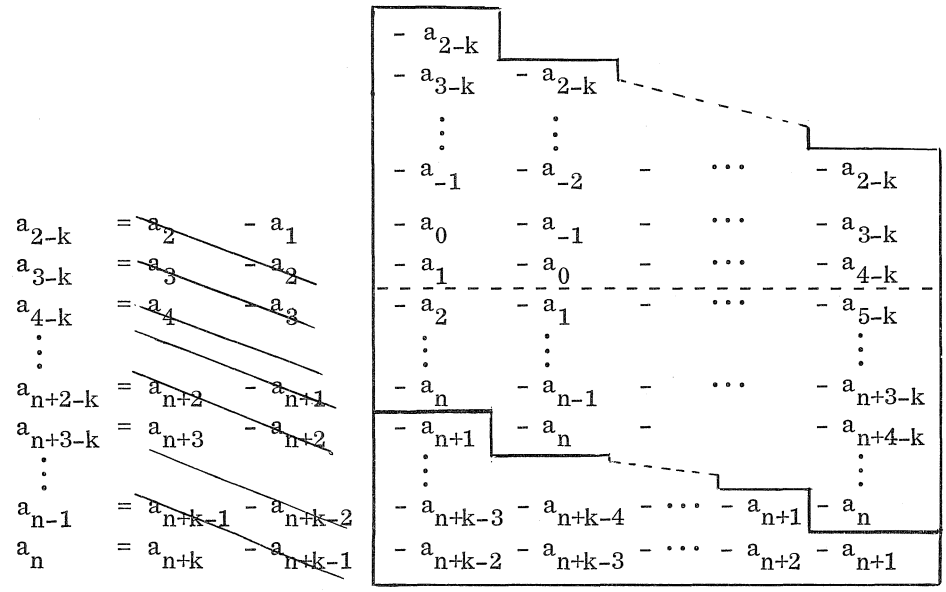
$$a_{kn+k} + \sum_{i=1}^{n} a_{ki} \ ,$$

and the right side is equal to

$$\sum_{i=0}^{kn-1} a_i + \sum_{i=kn}^{kn+k-1} a_i = \sum_{i=0}^{kn-1} a_i + a_{kn+k} \ .$$

Theorem (3c) is an immediate consequence of Theorem 3(b).

Inductive proofs of Theorems 4 and 5 are omitted. One may, however, verify (or discover!) Theorem 4 by considering the following diagram:



It follows from this diagram that

$$\sum_{i=2-k}^{n} a_i = a_{n+k} - a_1 - (k-2)\sum_{i=2-k}^{n} a_i + \sum_{i=1}^{k-2} i a_{-i} - \sum_{i=1}^{k-2} (k-i-1)a_{n+i} .$$

For the proof of Theorem 6, let n be any integer such that $n \geq 1$. Theorem 6 holds for $m = 1$ because

$$\sum_{j=1}^{k} a_{n-k+j} \sum_{i=1}^{j} f_{1-j+i} = \sum_{j=1}^{k} (a_{n-k+j} f_1) = a_{n+1} .$$

If Theorem 6 holds for $m = p$, then it holds for $m = p+1$ because we then have

$$\begin{aligned}
a_{n+(p+1)} = a_{(n+1)+p} &= \sum_{j=1}^{k} \left(a_{n+1-k+j} \sum_{i=1}^{j} f_{p-j+i} \right) \\
&= \sum_{j=2}^{k+1} \left(a_{n-k+j} \left\{ \sum_{i=1}^{j} f_{p+1-j+i} - f_{p+1} \right\} \right) \\
&= \sum_{j=1}^{k} \left(a_{n-k+j} \sum_{i=1}^{j} f_{p+1-j+i} \right) - a_{n-k+1} f_{p+1} \\
&\quad + a_{n+1} \sum_{i=1}^{k+1} f_{p-k+i} - \left(\sum_{j=2}^{k+1} a_{n-k+j} \right) f_{p+1} \\
&= \sum_{j=1}^{k} \left(a_{n-k+j} \sum_{i=1}^{j} f_{p+1-j+i} \right) \\
&\quad + f_{p+1}(-a_{n-k+1} + 2a_{n+1} - a_{n+2}) \\
&= \sum_{j=1}^{k} \left(a_{n-k+j} \sum_{i=1}^{j} f_{p+1-j+i} \right) .
\end{aligned}$$

The last equality is obtained by applying Theorem 1. Hence Theorem 6 holds for $n \geq 1$ and $m \geq 1$.

Theorem 7 obviously holds for $n = m$. We shall prove that if Theorem 7 holds for $n = mp$, then it holds for $n = m(p + 1)$.

Suppose, therefore, that d_m divides a_{mp}. By Theorem 6,

$$a_{m(p+1)} = a_{mp+m} = \sum_{j=1}^{k-1} \left(a_{mp-k+j} \sum_{i=1}^{j} f_{m-j+i} \right) + a_{mp} f_{m+1} .$$

Since d_m divides each term of the sum

$$\sum_{i=1}^{j} f_{m-j+i} ,$$

where $1 \leq j \leq k - 1$, and d_m divides a_{mp}, it follows that d_m divides $a_{m(p+1)}$.

For the proof of Theorem 8(a), we once again apply Theorem 6. We choose $n = 1$ and divide by f_{1+m}:

$$\frac{a_{1+m}}{f_{1+m}} = \sum_{j=1}^{k} \left(a_{1-k+j} \sum_{i=1}^{j} \frac{f_{m-j+i}}{f_{1+m}} \right) .$$

In [6] it is shown that, for any integer q,

$$\lim_{m \to \infty} \left(\frac{f_{m+q}}{f_m} \right) = r^q .$$

It follows, therefore, that

$$\lim_{n \to \infty} \left(\frac{a_n}{f_n} \right) = \sum_{j=1}^{k} \left(a_{1-k+j} \sum_{i=1}^{j} r^{i-j-1} \right)$$

$$= \frac{1}{r^k} \sum_{j=1}^{k} \left(a_{1-k+j} \sum_{i=1}^{j} r^{i-j-1+k} \right)$$

$$= \frac{1}{r^k} \sum_{j=2}^{k+1} \left(a_{j-k} \sum_{i=1}^{j-1} r^{k-i} \right) .$$

Theorem 8(b) holds since

$$\lim_{n\to\infty}\left(\frac{a_{n+1}}{a_n}\right) = \lim_{n\to\infty}\left(\frac{a_{n+1}}{f_{n+1}}\cdot\frac{f_n}{a_n}\cdot\frac{f_{n+1}}{f_n}\right)$$

$$= \left(\lim_{n\to\infty}\frac{a_n}{f_n}\right)\left(\lim_{n\to\infty}\frac{a_n}{f_n}\right)^{-1}\left(\lim_{n\to\infty}\frac{f_{n+1}}{f_n}\right) = r\ .$$

REFERENCES

1. Brother U. Alfred, "An Introduction to Fibonacci Discovery," The Fibonacci Association, 1965.
2. Brother U. Alfred, "Exploring Recurrent Sequences," Fibonacci Quarterly, Vol. 1, No. 2, 1963, pp. 81-83.
3. M. Beberman and H. Vaughan, High School Mathematics, Course 3, D. C. Heath, 1966.
4. D. E. Ferguson, "An Expression for Generalized Fibonacci Numbers," Fibonacci Quarterly, Vol. 4, No. 3, 1966, pp. 270-272.
5. M. Feinberg, "Fibonacci-Tribonacci," Fibonacci Quarterly, Vol. 1, No. 3, 1963, pp. 71-74.
6. I. Flores, "Direct Calculation of K-Generalized Fibonacci Numbers," Fibonacci Quarterly, Vol. 5, No. 3, 1967, pp. 259-266.
7. E. P. Miles, "Generalized Fibonacci Numbers and Associated Matrices," American Mathematical Monthly, Vol. 67, No. 8, 1960, pp. 745-752.
8. N. N. Vorobyov, The Fibonacci Numbers, D. C. Heath, 1963.
9. M. E. Waddill and L. Sacks, "Another Generalized Fibonacci Sequence," Fibonacci Quarterly, Vol. 5, No. 3, 1967, pp. 209-222.

★ ★ ★ ★ ★

DON'T FORGET!

It's TIME to renew your subscription to the Fibonacci Quarterly!

ON SOLVING $C_{n+2}=C_{n+1}+C_n+n^m$ BY EXPANSIONS AND OPERATORS

R. J. WEINSHENK
Lockheed Missiles & Space Company, Sunnyvale, California
and
V. E. HOGGATT, JR.
San Jose State College, San Jose, California

1. INTRODUCTION

It was the purpose of this paper to derive the general solution of the non-homogeneous difference equation

$$C_{n+2} = C_{n+1} + C_n + n^m$$

In so doing, two distinct approaches were employed to derive the particular solution associated with this equation, 1) a polynomial expansion method and 2) an operator method. The latter approach is believed to be a unique combined application of E, Δ, and the Fibonacci generating function.

The general solution of the non-homogeneous difference equation

$$C_{n+2} = C_{n+1} + C_n + n^m \tag{1}$$

is composed of the solution to the homogeneous equation

$$C_{n+2} = C_{n+1} + C_n \tag{2}$$

and a solution of the particular equation. See [4,5]. Since the polynomial term, n^m, is of degree m, a particular solution to (1) can be expected to be of the form

$$(C_n)_p = \sum_{i=0}^{m} a_{im} n^{m-i} , \tag{3}$$

from considerations produced in Section 4. A related problem appears in [8].

If

$$P_m(n) = (C_n)_p \quad , \tag{4}$$

the general solution of Eq. (1) can be expressed as

$$C_n = A_m F_{n+1} + B_m F_n - P_m(n) \tag{5}$$

where $F_{n+1} = F_n + F_{n-1}$ and $F_0 = 0$, $F_1 = 1$, since F_{n+1} and F_n are linearly independent (Fibonacci numbers), and therefore span the space of solutions of the homogeneous part (e).

2. THE PARTICULAR SOLUTION

Since the particular solution of Eq. (1) is of the form

$$(C_n)_p = \sum_{i=0}^{m} a_{im} n^{m-i} \quad , \tag{6}$$

substitution of (6) into Eq. (1) yields

$$\sum_{i=0}^{m} a_{im}(n+2)^{m-i} = \sum_{i=0}^{m} a_{im}(n+1)^{m-i} + \sum_{i=0}^{m} a_{im} n^{m-i} + n^m \quad . \tag{7}$$

By transposing and expanding these terms and then equating coefficients of, say, the n^{m-j} terms for $j \neq 0$, the general term of (7) becomes

$$\begin{aligned} &\left(a_{jm} n^{m-j} + \frac{2(m-j+1)n^{m-j}}{1!} a_{(j-1)m} + \cdots + \frac{2^j m(m-1)\cdots(m-j+1)n^{m-j}}{j!} a_{0m}\right) \\ &-\left(n^{m-j} a_{jm} + \frac{(m-j+1)n^{m-j}}{1!} a_{(j-1)m} + \cdots + \frac{m(m-1)\cdots(m-j+1)n^{m-j}}{j!} a_{0m}\right) \\ &- a_{jm} n^{m-j} = 0 \end{aligned} \tag{8}$$

$j \neq 0$ and all non-negative integers, n.

Since this equation is satisfied for all non-negative integer values of n, it is, in particular, satisfied for $n \neq 0$. Therefore, combining like subscripted a_{im} terms, this equation becomes

$$(9)\qquad -a_{jm} + \frac{(2^1 - 1)(m - j + 1)}{1!}\, a_{(j-1)m} + \cdots + \frac{(2^j - 1)m(m - 1)(m - 2)\cdots(m - j + 1)}{j!}\, a_{0m} = 0 .$$

Solving (9) for a_{jm} immediately yields

$$(10)\qquad a_{jm} = \sum_{i=0}^{j-1} a_{im} \frac{(2^{j-i} - 1)(m - i)!}{(j - i)!\,(m - j)!} = \sum_{i=0}^{j-1} a_{im} (2^{j-i} - 1)\binom{m - i}{j - i}.$$

Consequently, from Eq. (10), an expression for each a_{im} of Eq. (6) has been obtained in terms of the previous a_{im}.

For the particular case in which $j = 1$, Eq. (10) reduces to

$$(11)\qquad a_{1m} = a_{0m}\, m .$$

But Eq. (8) and those terms of the type $a_{0m} n^m$ yield the expression

$$(12)\qquad -a_{0m} n^m = n^m ,$$

which is valid for all non-negative integers n. Consequently, this equation immediately yields the result

$$(13)\qquad a_{0m} = -1$$

for all non-negative integers m. From Eq. (11), therefore, it is evident that

$$(14)\qquad a_{1m} = -m$$

for all non-negative integers m.

Using the previously derived expressions, it is now possible to generate all of the coefficients, a_{im}, of Eq. (6). In fact, the following theorem provides an expression for the a_{im} which is independent of any summation.

Theorem:

$$a_{jm} = a_{jj}\binom{m}{j} \quad \text{for all} \quad j < m . \tag{15}$$

Proof by mathematical induction:

From Eq. (10), it is evident that

$$a_{(j+1)(j+1)} = \sum_{i=0}^{j} a_{i(j+1)}(2^{j+1-i} - 1) \tag{16}$$

By the use of mathematical induction it can be easily verified that for $j = 0$ and $j = 1$,

$$a_{jm} = a_{jj}\binom{m}{j} \quad \text{for} \quad 0 < m < j . \tag{17}$$

Therefore, assume

$$a_{jm} = a_{jj}\binom{m}{j} \quad \text{for some particular } j . \tag{18}$$

It must be shown that

$$a_{(j+1)m} = a_{(j+1)(j+1)}\binom{m}{j+1} . \tag{19}$$

From Eq. (18) it is immediate that

$$a_{i(j+1)} = a_{ii}\binom{j+1}{i} \quad \text{for} \quad i \leq j . \tag{20}$$

Substituting expression (20) into (16) yields

$$a_{(j+1)(j+1)} = \sum_{i=0}^{j} a_{ii}(2^{j+1-i} - 1)\binom{j+1}{i} . \tag{21}$$

Multiplying both sides of (21) by

$$\binom{m}{j+1} \tag{22}$$

transforms the above equation into

$$a_{(j+1)(j+1)}\binom{m}{j+1} = \sum_{i=0}^{j} a_{ii}(2^{j+1-i} - 1)\frac{m!}{1!(m-j-1)!} \cdot \frac{1}{(j+1+i)!} . \tag{23}$$

But from Eq. (10),

$$a_{(j+1)m} = \sum_{i=0}^{j} a_{im}(2^{j+1-i} - 1)\binom{m-i}{j+1-i} . \tag{24}$$

By substituting (18) into (24), one obtains the equation

$$a_{(j+1)m} = \sum_{i=0}^{j} a_{ii}(2^{j+1-i} - 1)\frac{m!}{1!(m-j-1)!(j+1-i)} . \tag{25}$$

Consequently, equating expressions (23) and (25) yields the desired result that

$$a_{(j+1)(j+1)}\binom{m}{j+1} = a_{(j+1)m} . \qquad \text{Q. E. D.} \tag{26}$$

From this theorem and Eqs. (4) and (6), the particular solution of expression (1) can now be written in the final form

$$P_m(n) = \sum_{i=0}^{m} a_{ii}\binom{m}{i} n^{m-i} , \tag{27}$$

where, from (10) and (26), it is seen that

$$a_{kk} = \sum_{p=0}^{k-1} (2^{k-p} - 1)a_{pk} = \sum_{p=0}^{k-1} (2^{k-p} - 1)\binom{k}{k-p} a_{pp} \tag{28}$$

where $a_{0k} = -1$ and $a_{1k} = -k$.

3. THE GENERAL SOLUTION

Using the expressions for the particular solution of (5) which were derived in the previous section, the general solution of Eq. (1) can now be found. Assuming the general solution is of the form

$$C_n = A_m F_{n+1} + B_m F_n - P_m(n) , \tag{29}$$

an expression for A_m and B_m will now be derived.

From Eq. (29), it is clear that

$$C_0 = A_m - P_m(0) . \tag{30}$$

But from Eq. (27), it is immediately evident that

$$P_m(0) = a_{mm} , \tag{31}$$

and, consequently, Eq. (30) becomes

$$A_m = C_0 + a_{mm} . \tag{32}$$

Substituting this expression into Eq. (29) and solving for B_m by setting $n = 1$ yields

$$B_m = C_1 - C_0 - a_{mm} + P_m(1) \quad (33)$$

But since from Eq. (3)

$$P_m(1) = \sum_{i=0}^{m} a_{im} \quad (34)$$

Equation (33) now becomes

$$B_m = C_1 - C_0 + \sum_{i=0}^{m-1} a_{im} \quad (35)$$

The final expression for the general solution, Eq. (29), can be written

$$C_n = (C_0 + a_{mm})F_{n+1} + (C_1 - C_0 + \sum_{i=0}^{m-1} a_{im}\ F_n - P_m(n) \quad (36)$$

4. THE USE OF OPERATORS TO FIND THE PARTICULAR SOLUTION, $P_m(n)$

An interesting method for finding the particular solution of Eq. (1) without the necessity of solving a large system of linear equations will now be investigated. The material in this section is experimental and unrigorous. For the difference operator, Δ, the method is valid for polynomials but for the forward shifting operator, E, the limitations are less clear. This method uses the two operators E and Δ which are defined in the following manner:

$$E[f(n)] = f(n + 1) \quad (37)$$

and

$$\Delta f(n) = f(n + 1) - f(n) \quad (38)$$

Consequently,

(39) $$E = \Delta + 1 .$$

From Eq. (37), it is possible to write (1) as

(40) $$(E^2 - E - 1)C_n = n^m .$$

Therefore, the particular solution of this expression is the function generated by using the inverse operator $(E^2 - E - 1)^{-1}$, on n^m. That is,

(41) $$P_m(n) = (E^2 - E - 1)^{-1} n^m .$$

But from Eq. (39), it is immediate that

(42) $$\frac{1}{(E^2 - E - 1)} = \frac{1}{(\Delta^2 + \Delta - 1)}$$

From the definition of the Fibonacci generating function [1],

(43) $$\frac{1}{1 - x - x^2} = \sum_{i=0}^{\infty} F_{i+1} x^i ,$$

it is seen that

(44) $$\frac{-1}{(1 - \Delta - \Delta^2)} = -\sum_{i=0}^{\infty} F_{i+1} \Delta^i .$$

Therefore, from Eqs. (41), (42), and (44),

(45) $$P_m(n) = -\sum_{i=0}^{\infty} F_{i+1} \Delta^i (n^m) .$$

But from Eq. (38), it is clear that

(46) $$\Delta^{i}(n^{m}) = 0 \quad \text{for all } i > m.$$

Consequently, the final form of the particular solution can be written as

(47) $$P_m(n) = -\sum_{i=0}^{m} F_{i+1}\Delta^{i}(n^{m}) .$$

As an example, suppose $m = 2$. Then (47) reduces to

(48) $$P_2(n) = -(F_1 n^2 + F_2[(n+1)^2 - n^2] + F_3[(n+2)^2 - 2(n+1)^2 + n^2]) .$$

Combining terms reduces this equation to

(49) $$P_2(n) = -(n^2 + 2n + 5) .$$

Another expression for $P_m(n)$ can be derived solely in terms of E. Clearly,

(50) $$\frac{1}{(E^2 - E - 1)} = \frac{1}{E^2}\left(\frac{1}{1 - \frac{1}{E} - \frac{1}{E^2}}\right) .$$

But, once again, the right side of this expression can be written as

(51) $$\frac{1}{E^2}\sum_{i=0}^{\infty} F_{i+1}E^{-i} .$$

Consequently, the final expression for the particular solution can be written as

$$P_m(n) = \sum_{i=0}^{\infty} F_{i+1} E^{-(i+2)}(n^m) \tag{52}$$

where

$$E(n^m) = (n + 1)^m \tag{53}$$

and

$$E^{-1}(n^m) = (n - 1)^m \ . \tag{54}$$

Here we stop when n is reduced to zero. These solutions are of a different form than those using Δ and include the homogeneous part, too. We note the equivalence in a paper by Ledin [6]. See Brother Alfred [9] and Zeitlin [10].

5. CONCLUSION

As far as the authors know, the conditions under which the methods in Section 4 remain valid is an open and interesting question. Douglas Lind has pointed out that if $C_{n+1} = C_n + n$ were to be solved by the method $(E - 1)C_n = n$, then

$$C_n = \frac{-1}{1 - E}(n) = -\left(\sum_{k=0}^{\infty} E^k\right)(n)$$

diverges unless some stopping rule is invoked.

REFERENCES

1. V. E. Hoggatt, Jr., and S. L. Basin, "A Primer on the Fibonacci Sequence, Part II," Fibonacci Quarterly, Vol. 1, Number 2, April 1963, p. 61.
2. V. E. Hoggatt, Jr., and S. L. Basin, "A Primer on the Fibonacci Sequence, Part I," Fibonacci Quarterly, Vol. 1, No. 1, Feb., 1963, p. 65.

[Continued on page 60.]

ON PRIMES AND PSUEDO-PRIMES RELATED TO THE FIBONACCI SEQUENCE

EDWARD A. PARBERRY
Pennsylvania State University, State College, Pennsylvania

The two sequences $\{U_n\}$ and $\{V_n\}$ which satisfy the recurrence relation $f(n+1) = f(n) + f(n-1)$, and the initial conditions: $J_1 = U_2 = 1$; $V_1 = 1$, $V_2 = 3$; are called the Fibonacci and Lucas sequences, respectively. These sequences have some interesting divisibility properties which are related to the study of prime numbers. For instance, it is well known that every prime number divides infinitely many of the Fibonacci numbers [1, Th. 180, p. 150]; but, although for any particular prime we can give any number of the terms which it divides, we cannot in general give a general rule for finding the least such number. This is the so-called "rank of apparition" problem, where the rank of apparition of a number n, designated by ω_n, is the subscript of the least Fibonacci number which n divides. Wall [2] has shown that a number m divides U_n if and only if ω_m divides N. This property is used frequently in the text without further reference.

The particular divisibility properties with which this paper is concerned are the two "Lucas" equations which hold for all prime $m > 5$ [1, p. 150]:

$$U_{(m-\epsilon_m)} \equiv 0 \pmod{m} \tag{1}$$

$$U_m \equiv \epsilon_m \pmod{m} \quad , \tag{2}$$

where

$$\epsilon_m = \begin{bmatrix} 1 & \text{if } m \equiv \pm 1 \pmod 5 \\ -1 & \text{if } m \equiv \pm 2 \pmod 5 \end{bmatrix}.$$

Clearly it would be nice if (1) and (2) were to hold only for prime m, but this is not the case.

In [3], Emma Lehmer shows that there are infinitely many composite numbers, m, for which (1) is satisfied. She calls these numbers Fibonacci pseudo-primes. Her result is proved here as a special case of Theorem 3, and is extended in Theorem 4 to show that an infinite proper subset of her

pseudo-primes also satisfy (2). For the purpose a composite number, m, which satisfies both (1) and (2), and which is relatively prime to 30, a strong pseudo-prime.

The main results in the text are as follows:

Theorem 1. Let n be either a prime >5 or a strong pseudo-prime, then:

$$U_{\frac{1}{2}(n-\epsilon_n)} \equiv 0 \pmod{n}, \text{ iff } n \equiv 1 \pmod{4}, \tag{3}$$

$$V_{\frac{1}{2}(n-\epsilon_n)} \equiv 0 \pmod{n}; \text{ iff } n \equiv 3 \pmod{4}. \tag{4}$$

Theorem 2. Let $(n,30) = 1$, and let $m = U_n$, then the following are all equivalent:

$$U_n \equiv \epsilon_n \pmod{n}; \tag{5}$$

$$U_{(m-\epsilon_m)} \equiv 0 \pmod{m}; \tag{6}$$

$$U_{\frac{1}{2}(m-\epsilon_m)} \equiv 0 \pmod{m}; \tag{7}$$

$$U_m \equiv \epsilon_m \pmod{m}. \tag{8}$$

Theorem 3. Let n be a prime >5, or a strong pseudo-prime, then for $m = U_{2n}$,

$$U_{(m-\epsilon_m)} \equiv 0 \pmod{m}; \text{ and } m \text{ is composite.} \tag{9}$$

Remark: Theorem 3 is precisely Emma Lehmer's observation in [3] for n actually prime. However, it was not clear in her proof that the relation depends only on n satisfying (1) and (2), and $(n,30) = 1$. Theorem 4 now determines those n for which $m = U_{2n}$ satisfies relation (2) as well.

Theorem 4. If $m = U_{2n}$ as in Theorem 3, then m is a strong pseudo-prime if and only if $n \equiv 1,4 \pmod{15}$.

Theorem 1 establishes an identity similar to (1) which gives a further necessary condition for primality (and strong pseudo-primality). This result does not go very far in establishing a set of sufficient conditions, but it has the saving features of determining the parity of the rank of apparition of many primes (Corollaries 1 and 2), and of resolving the conjecture by D. Thoro [4] that no prime of the form $4n + 3$ divides any Fibonacci number with an odd subscript (Corollary 3).

Theorem 5 is the famous Lucas theorem on the primality of Mersenne numbers (numbers of the form $2^p - 1$ where p is a prime $\equiv 3 \pmod 4$). It is included here because Theorem 1 allows a new and elementary proof.

It is obvious [1, p. 150] that U_n is prime only if $n = 4$, or n is prime. Clearly if $m = U_p$ is prime, it must satisfy (1), (2), and (3) when taken as a subscript. However if U_p is not prime, it need not a-priori satisfy any of them. Theorem 2 shows that indeed U_p satisfies all three tests, and in fact that U_p, if not prime, generates an infinite set of strong pseudo-primes recursively.

The following identities are used in the text and may all be found in [2, pp. 148-150].

$$U_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}, \quad \text{where} \quad \alpha = -\beta^{-1} = \frac{1 + \sqrt{5}}{2} ; \tag{10}$$

$$V_n = \alpha^n + \beta^n ; \tag{11}$$

$$U_n = (-1)^{n-1} U_{-n}, \quad V_n = (-1)^n V_{-n} ; \tag{12}$$

$$2^{n-1} U_n = \sum_{k=0}^{\left[\frac{1}{2}(n-1)\right]} \binom{n}{2k+1} 5^k ; \tag{13 (a)}$$

$$2^{n-1} V_n = \sum_{k=0}^{\left[\frac{1}{2}(n-1)\right]} \binom{n}{2k} 5^k ; \tag{13 (b)}$$

(14) $$(U_n, U_{n+1}) = 1, \quad (V_n, V_{n+1}) = 1 ;$$

(15) $$(U_n, V_n) \leq 2, \text{ and equality holds iff } n \equiv 0 \pmod 3;$$

(16) $$U_n^2 - U_{n-1}U_{n+1} = (-1)^{n-1} ;$$

(17) $$V_n = U_{n+1} + U_{n-1} ;$$

Also, in the proof of Theorem 5, we use the following theorem by Lucas [5, p. 302]:

(18) If $\omega_N = N - 1$, or $N + 1$, then N is prime.

Lemma 1. $$U_{a+b} = U_a V_b + (-1)^a U_{b-a}$$

Proof.
$$U_a V_b = \left(\frac{\alpha^a - \beta^a}{\sqrt{5}}\right)(\alpha^b + \beta^b)$$
$$= \frac{\alpha^{a+b} - \beta^{a+b} + \alpha^a\beta^b - \alpha^b\beta^a}{\sqrt{5}}$$
$$= \frac{\alpha^{a+b} - \beta^{a+b}}{\sqrt{5}} - (\alpha\beta)^a \frac{\alpha^{b-a} - \beta^{b-a}}{\sqrt{5}}$$
$$= U_{a+b} - (-1)^a U_{b-a}$$

Lemma 2. (i) $$mV_m \equiv U_m \pmod 5 ;$$

(ii) $U_m \equiv m \pmod 5$, if $m \equiv 1 \pmod 4$;

(iii) $U_m \equiv -m \pmod 5$, if $m \equiv 3 \pmod 4$;

(iv) $U_m \equiv -\frac{1}{2}m \pmod 5$, if $m \equiv 0 \pmod 4$;

(v) $U_m \equiv \frac{1}{2}m \pmod 5$, if $m \equiv 2 \pmod 4$.

Proof. From (13),

$$2^{n-1}U_n = \sum_{k=0}^{\left[\frac{1}{2}(n-1)\right]} \binom{n}{2k+1} 5^k \equiv n \pmod 5 \tag{19}$$

and

$$2^{n-1}V_n = \sum_{k=0}^{\left[\frac{1}{2}(n-1)\right]} \binom{n}{2k} 5^k \equiv 1 \pmod 5 \tag{20}$$

Multiplying (19) and (20), and dividing out 2^{n-1}, we get (i). From Fermat's theorem, $2^{4n} \equiv 1 \pmod 5$, $2^{4n+1} \equiv 2 \pmod 5$, etc., and the other relations follow since $(2,5) = 1$.

Theorem 1. Let n be either a prime >5 or a strong pseudo-prime. then

$$U_{\frac{1}{2}(n-\epsilon_n)} \equiv 0 \pmod n \quad \text{iff} \quad n \equiv 1 \pmod 4 \tag{3}$$

$$V_{\frac{1}{2}(n-\epsilon_n)} \equiv 0 \pmod n \quad \text{iff} \quad n \equiv 3 \pmod 4 \tag{4}$$

Proof. In Lemma 1, let

$$a = \tfrac{1}{2}(n - \epsilon_n), \quad b = \tfrac{1}{2}(n + \epsilon_n),$$

then by Eq. (2),

$$U_n = U_{\frac{1}{2}(n-\epsilon_n)} V_{\frac{1}{2}(n+\epsilon_n)} + (-1)^{\frac{1}{2}(n-\epsilon_n)} U_{\epsilon_n} \equiv \epsilon_n \pmod n \tag{21}$$

now

$$U_1 = U_{-1} = 1, \quad \text{and} \quad (-1)^{\frac{1}{2}(n-\epsilon_n)} \equiv \epsilon_n \pmod n \quad \text{iff} \quad n \equiv 1 \pmod 4.$$

Hence

$$U_{\frac{1}{2}(n-\epsilon_n)}\, V_{\frac{1}{2}(n+\epsilon_n)} \equiv 0 \pmod{n} \quad \text{iff} \quad n \equiv 1 \pmod{4} \,. \tag{22}$$

Also, from (1),

$$U_{(n-\epsilon_n)} = U_{\frac{1}{2}(n+\epsilon_n)}\, V_{\frac{1}{2}(n-\epsilon_n)} \equiv 0 \pmod{n} \,. \tag{23}$$

Now suppose $n \equiv 1 \pmod 4$, and the $p^e \mid n$, while $p^e \nmid U_{\frac{1}{2}(n-\epsilon_n)}$ then from (22),

$$p \mid V_{\frac{1}{2}(n+\epsilon_n)}$$

and from (23),

$$p \mid V_{\frac{1}{2}(n-\epsilon_n)}$$

which is impossible since by (14),

$$\left(V_{\frac{1}{2}(n+\epsilon_n)},\ V_{\frac{1}{2}(n-\epsilon_n)}\right) = 1 \,.$$

Hence

$$n \mid U_{\frac{1}{2}(n-\epsilon_n)} \quad \text{iff} \quad n \equiv 1 \pmod{4} \,,$$

which proves (3).

If, on the other hand, $n \equiv 3 \pmod 4$; then (21) shows that $p \mid n$ implies

$$U_{\frac{1}{2}(n-\epsilon_n)}\, V_{\frac{1}{2}(n+\epsilon_n)} \equiv \pm 2 \pmod{p} \,.$$

Therefore

$$\left(U_{\frac{1}{2}(n-\epsilon_n)},\ n\right) = 1 \,;$$

hence from (23),

$$n \Big| V_{\frac{1}{2}(n-\epsilon_n)} .$$

And finally if $n \equiv 1 \pmod 4$, then $n \Big| U_{\frac{1}{2}(n-\epsilon_n)}$; and since

$$\left(U_{\frac{1}{2}(n-\epsilon_n)}, V_{\frac{1}{2}(n-\epsilon_n)} \right) \leq 2, \quad n \nmid V_{\frac{1}{2}(n-\epsilon_n)} ,$$

Corollary 1. If $p \equiv 3 \pmod 4$, then ω_p is even.

Proof. This follows from (1) and Theorem 1, since $\omega_p \Big| p - \epsilon_p$ which is even, but $\omega_p \nmid \frac{1}{2}(p - \epsilon_p)$.

Corollary 2. If $p \equiv 13, 17 \pmod{20}$, then ω_p is odd.

Proof. Here $\epsilon_p = -1$, $p \equiv 1 \pmod 4$, hence $\frac{1}{2}(p - \epsilon_p)$ is odd. Therefore, since

$$p \Big| U_{\frac{1}{2}(p-\epsilon_p)} \quad \text{implies} \quad \omega_p \Big| \tfrac{1}{2}(p - \epsilon_p) ,$$

ω_p is odd.

Corollary 3. (Thoro [3]) If $p \mid U_{(2n+1)}$, then $p \not\equiv 3 \pmod 4$.

Proof. $p \mid U_{2n+1}$ implies $\omega_p \mid 2n + 1$ which in turn implies $p = 2$, or $p \equiv 1 \pmod 4$ by Corollary 1.

Theorem 2. Let $(n, 30) = 1$, and let $m = U_n$. Then the following are all equivalent:

(5) (a) $$U_n \equiv \epsilon_n \pmod n ;$$

(6) (b) $$U_{(m-\epsilon_m)} \equiv 0 \pmod m ;$$

(7) (c) $$U_{\frac{1}{2}(m-\epsilon_m)} \equiv 0 \pmod m ;$$

(8) (d) $$U_m \equiv \epsilon_m \pmod m .$$

Proof. (a)$\Leftrightarrow$(b).

From Lemma 2, we see that $U_n = m \equiv \pm n \pmod 5$, since n is odd. Therefore $\epsilon_m = \epsilon_n$, and replacing ϵ_n in (a), we have

$$n \mid U_n - \epsilon_m \Leftrightarrow U_n \mid U_{u_n - \epsilon_m} = U_{m-\epsilon_m} .$$

(b) $\Leftrightarrow$ (c)

Since n is odd, and U_n is odd (since $3 \nmid n$) we have:

$$U_n = m \mid U_{m-\epsilon_m} \Leftrightarrow n \mid m - \epsilon_m \Leftrightarrow n \mid \tfrac{1}{2}(m - \epsilon_m) \Leftrightarrow U_n = m \mid U_{\frac{1}{2}(m-\epsilon_m)} .$$

(c) $\Rightarrow$ (d)

Using Lemma 1, we have

$$(24) \quad U_m = U_{\frac{1}{2}(m-\epsilon_m)} V_{\frac{1}{2}(m+\epsilon_m)} + (-1)^{\frac{1}{2}(m-\epsilon_m)} \equiv (-1)^{\frac{1}{2}(m-\epsilon_m)} \pmod{m} .$$

Now since n is odd, we see by Corollary 3, that

$$U_n = m \equiv 1 \pmod{4} .$$

Hence

$$(-1)^{\frac{1}{2}(m-\epsilon_m)} = \epsilon_m .$$

(d) $\Rightarrow$ (c)

Comparing (d) with (24), we see that

$$(25) \quad U_{\frac{1}{2}(m-\epsilon_m)} V_{\frac{1}{2}(m+\epsilon_m)} \equiv 0 \pmod{m} ,$$

and from (16), we see that

$$U_m^2 - U_{m-\epsilon_m} U_{m+\epsilon_m} = (-1)^{m-1} \equiv 1 \pmod{m} ,$$

hence

$$(26) \quad U_{m-\epsilon_m} U_{m+\epsilon_m} \equiv 0 \pmod{m} .$$

Now suppose $p^e \mid m$, and $p^e \nmid U_{\frac{1}{2}(m-\epsilon_m)}$, then $p \mid V_{\frac{1}{2}(m+\epsilon_m)}$ by (25). Also $\omega_p \mid n$ and is therefore odd, hence

$$\omega_p \mid \tfrac{1}{2}(m - \epsilon_m) \Rightarrow \omega_p \mid m - \epsilon_m \Rightarrow p^e \nmid U_{m-\epsilon_m} .$$

Therefore, Eq. (26) implies that $p \mid U_{m+\epsilon_n}$. But ω_p is also odd, hence

$$\omega_p \mid m + \epsilon_m \Rightarrow \omega_p \mid \tfrac{1}{2}(m + \epsilon_m) \Rightarrow p \mid U_{\frac{1}{2}(m+\epsilon_m)} ,$$

which is a contradiction since

$$\left(U_{\frac{1}{2}(m+\epsilon_m)} , V_{\frac{1}{2}(m+\epsilon_m)} \right) \leq 2 .$$

Hence

$$p^e \mid m \Rightarrow p^e \mid U_{\frac{1}{2}(m-\epsilon_m)} ,$$

which means that

$$m \mid U_{\frac{1}{2}(m-\epsilon_m)} . \quad \text{Q.E.D.}$$

Theorem 3. Let n be a prime > 5, or a strong pseudo-prime, then for $m = U_{2n}$,

$$U_{(m-\epsilon_m)} \equiv 0 \pmod{m} ;$$

and m is composite.

Proof. We note that $U_{2n} = U_n V_n$ by Lemma 1, and is therefore composite for $n \geq 2$.

Now, using (2) and (17):

$$U_{2n} \equiv U_n V_n \equiv \epsilon_n V_n \equiv \epsilon_n (U_{n+\epsilon_n} + U_{n-\epsilon_n}) \pmod{n} ,$$

and using (1), and Lemma 1:

$$U_{2n} \equiv \epsilon_n\left(U_{(n+\epsilon_n)}\right) \equiv \epsilon_n\left(U_n V_{\epsilon_n} + (-1)^n U_{-(n-\epsilon_n)}\right)$$

$$\equiv \epsilon_n^2 V_{\epsilon_n} \equiv V_{\epsilon_n} \equiv \epsilon_n \pmod{n} \quad .$$

Hence, $n \mid m - \epsilon_n$; which, since n and m are odd, implies:

$$2n \mid m - \epsilon_n \Rightarrow U_{2n} = m \mid U_{(m-\epsilon_n)} \quad . \tag{27}$$

To complete the proof, we note that by Lemma 2,

$$U_{2n} = m \equiv \pm n \pmod{5}, \text{ hence } \epsilon_m = \epsilon_n \quad .$$

Theorem 4. If $m = U_{2n}$ as in Theorem 3, then m is a strong pseudo-prime if and only if $n \equiv 1,4 \pmod{15}$.

Proof. From Theorem 3, and Lemma 1,

$$U_m = U_{\frac{1}{2}(m-\epsilon_m)} V_{\frac{1}{2}(m+\epsilon_m)} + (-1)^{\frac{1}{2}(m-\epsilon_m)} U_{\epsilon_m} \quad .$$

Now if $m \equiv \epsilon_m \pmod 4$, then $2n \mid \frac{1}{2}(m - \epsilon_m)$ by (27); hence:

$$U_m \equiv (-1)^{\frac{1}{2}(m-\epsilon_m)} U_{\epsilon_m} \equiv 1 \pmod{m} \quad .$$

On the other hand, if $m \equiv -\epsilon_m \pmod 4$, then a new application of Lemma 1 gives:

$$U_m = U_{\frac{1}{2}(m-2n-\epsilon_m)} V_{\frac{1}{2}(m+2n+\epsilon_m)} + (-1)^{\frac{1}{2}(m-2n-\epsilon_m)} U_{2n+\epsilon_m} \quad ;$$

which shows, since now $2n \mid \frac{1}{2}(m - 2n - \epsilon_m)$, that

$$U_m \equiv U_{2n+\epsilon_m} \equiv U_{2n-\epsilon_m} \not\equiv \pm 1 \pmod{m} \quad ,$$

hence $U_m \equiv \epsilon_m \pmod{m}$ iff $\epsilon_m = 1$ and $m \equiv 1 \pmod 4$. This corresponds to $n \equiv \pm 1 \pmod 5$, and $n \equiv 1 \pmod 3$ (i.e., $n \equiv 1, 4 \pmod{15}$). Q.E.D.

Theorem 5. (Lucas [5, p. 310]) Let $p \equiv 3 \pmod 4$ be a prime, then $N = 2^p - 1$ is a prime if and only if $V_{2(p-1)} \equiv 0 \pmod N$.

Remark. This is the simplest test of primality known; since

$$V_{2^n} = V^2_{2(n-1)} - 2 ,$$

and hence can be calculated in only n steps.

Proof. Sufficiency:

Let

$$V_{2(p-1)} \equiv 0 \pmod N ,$$

then by Lemma 1,

$$U_{2^p} = U_{2(p-1)}V_{2(p-1)} \equiv 0 \pmod N = \omega_N \Big| 2^p .$$

and since

$$\left(U_{2(p-1)}, V_{2(p-1)}\right) = 1, \ \omega_N = 2^p ;$$

which by (18) gives that N is prime.

Necessity:

Let N be prime, and then since $N \equiv 3 \pmod 4$, we have by Theorem 1,

$$N \Big| V_{\frac{1}{2}(N-\epsilon_N)} ,$$

and since

$$2^p - 1 \equiv 2^3 - 1 \equiv 2 \pmod 5 ,$$

$\epsilon_N = -1$. Therefore, $N \Big| V_{2(p-1)}$. Q.E.D.

REFERENCES

1. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, 4th Ed., 1960.
2. D. D. Wall, "Fibonacci Series Modulo m," Amer. Math. Monthly, 67 (1960).
3. E. Lehmer, "On the Infinitude of Fibonacci Pseudo-Primes," Fibonacci Quarterly, October, 1964, p. 229.
4. D. Thoro, "Two Fibonacci Conjectures," Fibonacci Quarterly, October, 1965, p. 186.
5. E. Lucas, "Theorie der Fonctions Numeriques Simplement Periodiques," Amer. J. of Math., Vol. 1, Baltimore, 1878.

* * * * *

[Continued from page 48.]

3. F. B. Hildebrand, Methods of Applied Mathematics, Englewood Cliffs, Prentice-Hall, Inc., 1961, pp. 227-249.
4. James A. Jeske, "Linear Recurrence Relations, Part I," Fibonacci Quarterly, Vol. 1, No. 2, April 1965, p. 69.
5. Kenneth S. Miller, An Introduction to the Calculus of Finite Differences and Difference Equations, New York, Henry Holt and Co., 1960, pp. 126-157.
6. George Ledin, Jr., "On a Certain Kind of Fibonacci Sums," Fibonacci Quarterly, Vol. 5, No. 1, Feb., 1967, pp. 45-58.
7. R. J. Weinshenk, "Convolutions and Difference Equations Associated with the N-Reflections of Light in two Glass Plates," San Jose State College Masters Thesis, June, 1965.
8. J. A. H. Hunter, Problem H-48 with solution in Vol. 3, No. 4, p. 303, Fibonacci Quarterly.
9. Brother U. Alfred, "Summation of $\sum_{k=1}^{n} k^m F_{k+r}$ Finite Difference Approach," Fibonacci Quarterly, Vol. 5 (19672, pp. 91-98.
10. David Zeitlin, "On Summation Formulas and Identities for Fibonacci Numbers," Fibonacci Quarterly, Vol. 5 (1967), pp. 1-43.

* * * * *

SOME FIBONACCI AND LUCAS IDENTITIES

L. CARLITZ
Duke University, Durham, North Carolina
and
H. H. FERNS
Victoria, B. C., Canada

1. In the usual notation, put

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad L_n = \alpha^n + \beta^n \tag{1.1}$$

where

$$\alpha = \tfrac{1}{2}(1 + \sqrt{5}), \quad \beta = \tfrac{1}{2}(1 - \sqrt{5}),$$
$$\alpha^2 = \alpha + 1, \quad \beta^2 = \beta + 1, \quad \alpha\beta = -1 . \tag{1.2}$$

It is rather obvious that polynomial identities can be used in conjunction with (1.1) and (1.2) to produce Fibonacci and Lucas identities. For example, by the binomial theorem,

$$\alpha^{2n} = (\alpha + 1)^n = \sum_{s=0}^{n} \binom{n}{s} \alpha^s$$

which gives

$$F_{2n} = \sum_{s=0}^{n} \binom{n}{s} F_s, \qquad L_{2n} = \sum_{s=0}^{n} \binom{n}{s} L_s \tag{1.3}$$

and indeed

Supported in part by NSF Grant GP 5174.

$$(1.4) \qquad F_{2n+k} = \sum_{s=0}^{n} \binom{n}{s} F_{s+k}, \qquad L_{2n+k} = \sum_{s=0}^{n} \binom{n}{s} L_{s+k},$$

where k is an arbitrary integer.

Again, since

$$\alpha^3 = \alpha(\alpha + 1) = 2\alpha + 1,$$

we get in the same way

$$(1.5) \qquad F_{3n+k} = \sum_{s=0}^{n} \binom{n}{s} 2^s F_{s+k}, \qquad L_{3n+k} = \sum_{s=0}^{n} \binom{n}{s} 2^s L_{s+k}.$$

More generally, since

$$\alpha^r = F_r \alpha + F_{r-1},$$

it follows that

$$(1.6) \qquad F_{rn+k} = \sum_{s=0}^{n} \binom{n}{s} F_r^s F_{r-1}^{n-s} F_{s+k}, \qquad L_{rn+k} = \sum_{s=0}^{n} \binom{n}{s} F_r^s F_{r-1}^{n-s} L_{s+k}.$$

This can be carried further. For example, since

$$(1.7) \qquad \alpha^{2m} = L_m \alpha^m - (-1)^m,$$

we get

$$(1.8) \qquad \begin{aligned} F_{2mn+k} &= \sum_{s=0}^{n} (-1)^{(n-s)(m+1)} \binom{n}{s} L_m^s F_{ms+k}, \\ L_{2mn+k} &= \sum_{s=0}^{n} (-1)^{(n-s)(m+1)} \binom{n}{s} L_m^s L_{ms+k}. \end{aligned}$$

The identity (1.7) generalizes to

$$\alpha^{rm} = \frac{F_{rm}}{F_m}\alpha^m - (-1)^m \frac{F_{(r-1)m}}{F_m} \quad . \tag{1.9}$$

Indeed (1.9) is equivalent to

$$\alpha^{rm}(\alpha^m - \beta^m) = (\alpha^{rm} - \beta^{rm})\alpha^m - \alpha^m\beta^m(\alpha^{(r-1)m} - \beta^{(r-1)m}) \ ,$$

which is obviously true. From (1.9), we obtain

$$\begin{aligned} F_m^n F_{rmn+k} &= \sum_{s=0}^{n} (-1)^{(n-s)(m+1)} F_{(r-1)m}^{n-s} F_{rm}^s F_{ms+k} \ , \\ F_m^n L_{rmn+k} &= \sum_{s=0}^{n} (-1)^{(n-s)(m+1)} F_{(r-1)m}^{n-s} F_{rm}^s L_{ms+k} \ . \end{aligned} \tag{1.10}$$

With each of the above identities is associated a number of related identities. For example, we may rewrite

$$\alpha^r = F_r\alpha + F_{r-1}$$

as either

$$\alpha^r - F_r\alpha = F_{r-1} \quad \text{or} \quad \alpha^r - F_{r-1} = F_r\alpha \ .$$

Hence we obtain

$$\begin{aligned} \sum_{s=0}^{n} (-1)^s \binom{n}{s} F_r^s F_{r(n-s)+s+k} &= F_{r-1}^n F_k \ , \\ \sum_{s=0}^{n} (-1)^s \binom{n}{s} F_r^s L_{r(n-s)+s+k} &= F_{r-1}^n L_k \ , \end{aligned} \tag{1.11}$$

and

$$\sum_{s=0}^{n} (-1)^{n-s} \binom{n}{s} F_{r-1}^{n-s} F_{rs+k} = F_r^n F_{n+k} ,$$

$$\sum_{s=0}^{n} (-1)^{n-s} \binom{n}{s} F_{r-1}^{n-s} L_{rs+k} = F_r^n L_{n+k} . \tag{1.12}$$

We remark that (1.9) can be generalized even further, namely to

$$F_{rm} \alpha^{sm} - F_{sm} \alpha^{rm} = (-1)^{sm} F_{(r-s)m} , \tag{1.13}$$

and (1.10) can now be extended in an obvious way.

2. Additional identities are obtained by making use of formulas such as

$$\alpha^2 + 1 = \alpha\sqrt{5} . \tag{2.1}$$

Note that

$$\beta^2 + 1 = -\beta\sqrt{5} . \tag{2.2}$$

Thus we get

$$\sum_{s=0}^{n} \binom{n}{s} \alpha^{2s} = 5^{n/2} \alpha^n , \quad \sum_{s=0}^{n} \binom{n}{s} \beta^{2s} = (-1)^n 5^{n/2} \beta^n ,$$

so that

$$\sum_{s=0}^{n} \binom{n}{s} F_{2s+k} = 5^{n/2} \frac{\alpha^{m+k} - (-1)^n \beta^{n+k}}{\alpha - \beta} .$$

It follows that

$$\sum_{s=0}^{n} \binom{n}{s} F_{2s+k} = \begin{cases} 5^{n/2} F_{n+k} & (n \text{ even}) \\ 5^{(n-1)/2} L_{n+k} & (n \text{ odd}) \end{cases} . \tag{2.3}$$

Similarly

$$\sum_{s=0}^{n} \binom{n}{s} L_{2s+k} = \begin{cases} 5^{n/2} L_{n+k} & (n \text{ even}) \\ 5^{(n+1)/2} F_{n+k} & (n \text{ odd}) \end{cases} . \tag{2.4}$$

We omit the variants of (2.3) and (2.4).

We can generalize (2.1) as follows:

$$\begin{cases} \alpha^{2m} = F_{2m}\alpha\sqrt{5} - L_{2m-1} \\ \alpha^{2m+1} = L_{2m+1}\alpha - L_{2m}\sqrt{5} \end{cases} . \tag{2.5}$$

The corresponding formulas for β^m are

$$\begin{cases} \beta^{2m} = -F_{2m}\beta\sqrt{5} - L_{2m-1} \\ \beta^{2m+1} = L_{2m+1}\beta + F_{2m}\sqrt{5} \end{cases} . \tag{2.6}$$

We therefore get the following generalizations of (2.3) and (2.4):

$$\sum_{s=0}^{n} \binom{n}{s} L_{2m-1}^{n-s} F_{2ms+k} = \begin{cases} 5^{n/2} F_{2m}^{n} F_{n+k} & (n \text{ even}) \\ 5^{(n-1)/2} F_{2m}^{n} L_{n+k} & (n \text{ odd}) \end{cases} , \tag{2.8}$$

$$\sum_{s=0}^{n} \binom{n}{s} L_{2m-1}^{n-s} L_{2ms+k} = \begin{cases} 5^{n/2} F_{2m}^{n} L_{n+k} & (n \text{ even}) \\ 5^{(m+1)/2} F_{2m}^{n} F_{n+k} & (n \text{ odd}) \end{cases} , \tag{2.9}$$

$$\sum_{s=0}^{n} (-1)^{n-s} \binom{n}{s} L_{2m+1}^{s} F_{2m(n-s)+n+k} = \begin{cases} 0 & (n \text{ even}) \\ 2 \cdot 5^{(n-1)/2} F_{2m}^{n} & (n \text{ odd}), \end{cases} \tag{2.10}$$

$$(2.11)\quad \sum_{s=0}^{n} (-1)^{n-s}\binom{n}{s} L_{2m+1}^{s} L_{2m(n-s)+n+k} = \begin{cases} 2\cdot 5^{n/2} F_{2m}^{2} & (n \text{ even}) \\ 0 & (n \text{ odd}) . \end{cases}$$

We omit the variants of (2.8), $\cdots$, (2.11).

3. In the next place,

$$(1+\alpha x)^n(1+x)^n = \sum_{r=0}^{n}\binom{n}{r}\alpha^r x^r \sum_{s=0}^{n}\binom{n}{s}x^s$$

$$= \sum_{k=0}^{2n} x^k \sum_{r=0}^{k}\binom{n}{r}\binom{n}{k-r}\alpha^r .$$

On the other hand,

$$(1+\alpha x)^n(1+x)^n = (1+\alpha^2 x+\alpha x^2)^n$$

$$= \sum_{r=0}^{n}\binom{n}{r}\alpha^r x^r (\alpha+x)^r$$

$$= \sum_{r=0}^{n}\binom{n}{r}\alpha^r x^r \sum_{s=0}^{r}\binom{r}{s}\alpha^{r-s} x^s$$

$$= \sum_{k=0}^{2n} x^k \sum_{3s\le 2k}\binom{n}{k-s}\binom{k-s}{s}\alpha^{2k-3s} .$$

Comparing coefficients of x^k we get

$$(3.1)\quad \sum_{r=0}^{k}\binom{n}{r}\binom{n}{k-r}\alpha^r = \sum_{3s-2k}\binom{n}{k-s}\binom{k-s}{s}\alpha^{2k-3s} .$$

It therefore follows that

$$(3.2)\qquad \sum_{r=0}^{k}\binom{n}{r}\binom{n}{k-r}F_{r+j} = \sum_{3s\le 2k}\binom{n}{k-s}\binom{k-s}{s}F_{2k-3s+j}$$

and

$$(3.3)\qquad \sum_{r=0}^{k}\binom{n}{r}\binom{n}{k-r}L_{r+j} = \sum_{3s\le 2k}\binom{n}{k-s}\binom{k-s}{s}L_{2k-3s+j}$$

for all j. In particular, for $k = n$, these formulas reduce to

$$(3.4)\qquad \sum_{r=0}^{n}\binom{n}{r}^2F_{r+j} = \sum_{3s\le 2n}\binom{n}{2s}\binom{2s}{s}F_{2n-3s+j}$$

and

$$(3.5)\qquad \sum_{r=0}^{n}\binom{n}{r}^2L_{r+j} = \sum_{3s\le 2n}\binom{n}{2s}\binom{2s}{s}L_{2n-3s+j}\ ,$$

respectively.

We have similarly

$$(1+\alpha^2x)^n(1-x)^n = \sum_{r=0}^{n}\binom{n}{r}\alpha^{2r}x^r\sum_{s=0}^{n}(-1)^s\binom{n}{s}x^s$$

$$= \sum_{k=0}^{2n}x^k\sum_{r=0}^{k}(-1)^{k-r}\binom{n}{r}\binom{n}{k-r}\alpha^{2r}\ ;$$

$$(1 + \alpha^2 x)^n (1 - x)^n = (1 + \alpha x - \alpha^2 x^2)^n$$

$$= \sum_{r=0}^{n} \binom{n}{r} \alpha^r x^r (1 - \alpha x)^r$$

$$= \sum_{r=0}^{n} \binom{n}{r} \alpha^r x^r \sum_{s=0}^{r} (-1)^s \binom{r}{s} \alpha^s x^s$$

$$= \sum_{k=0}^{2n} \alpha^k x^k \sum_{2s \le k} (-1)^s \binom{n}{k-s} \binom{k-s}{s} .$$

Comparing coefficients of x^k we get

$$(3.6) \qquad \sum_{r=0}^{k} (-1)^{k-r} \binom{n}{r} \binom{n}{k-r} \alpha^{2r} = \alpha^k \sum_{2s \le k} (-1)^s \binom{n}{k-s} \binom{k-s}{s} .$$

It follows that

$$(3.7) \qquad \sum_{r=0}^{k} (-1)^{k-r} \binom{n}{r} \binom{n}{k-r} F_{2r+j} = F_{k+j} \sum_{2s \le k} (-1)^s \binom{n}{k-s} \binom{k-s}{s} ,$$

$$(3.8) \qquad \sum_{r=0}^{k} (-1)^{k-r} \binom{n}{r} \binom{n}{k-r} L_{2r+j} = L_{k+j} \sum_{2s \le k} (-1)^s \binom{n}{k-s} \binom{k-s}{s} .$$

In particular, for $k = n$, we get

$$(3.9) \qquad \sum_{r=0}^{n} (-1)^{n-r} \binom{n}{r}^2 F_{2r+j} = F_{n+j} \sum_{2s \le n} (-1)^s \binom{n}{2s} \binom{2s}{s} ,$$

$$(3.10) \qquad \sum_{r=0}^{n} (-1)^{n-r} \binom{n}{r}^2 L_{2r+j} = L_{n+j} \sum_{2s \le n} (-1)^s \binom{n}{2s} \binom{2s}{s} .$$

More general results can be obtained by using (1.7). For brevity, we shall omit the statement of the formulas in question.

4. The formulas

$$\sum_{k=0}^{n}\binom{n}{k}^2 F_k = -\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\binom{n+k}{k}F_{n-k}\ , \tag{4.1}$$

$$\sum_{k=0}^{n}\binom{n}{k}^2 L_k = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\binom{n+k}{k}L_{n-k} \tag{4.2}$$

were proposed as a problem in this Quarterly (Vol. 4 (1966), p. 332, H-97). The formulas

$$\sum_{k=0}^{n}\binom{n}{k}^2 F_{2k} = \sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k}F_{n-k}\ , \tag{4.3}$$

$$\sum_{k=0}^{n}\binom{n}{k}^2 L_{2k} = \sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k}L_{n-k} \tag{4.4}$$

were also proposed as a problem (Vol. 5 (1967), p. 70, H-106). They can be proved rapidly by making use of known formulas for the Legendre polynomial.

We recall that [1, 162, 166]

$$P_n(x) = \sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k}\left(\frac{x-1}{2}\right)^k$$

$$= \sum_{k=0}^{n}\binom{n}{k}^2\left(\frac{x-1}{2}\right)^k\left(\frac{x+1}{2}\right)^{n-k} = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\binom{n+k}{k}\left(\frac{x+1}{2}\right)^k. \tag{4.5}$$

If we take $u = (x + 1)/(x - 1)$, we get

$$\sum_{k=0}^{n} \binom{n}{k}^2 u^k = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k}(u-1)^{n-k} , \tag{4.6}$$

$$\sum_{k=0}^{n} \binom{n}{k}^2 u^k = \sum_{k=0}^{n} (-1)^{n-k}\binom{n}{k}\binom{n+k}{k}u^k(u-1)^{n-k} . \tag{4.7}$$

Multiplying both sides of (4.6) by u^j and then take $u = \alpha, \beta$. Since $\alpha - 1 = \alpha^{-1}$, we get

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

$$\sum_{k=0}^{n} \binom{n}{k}^2 \beta^{k+j} = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k}\beta^{j+k-n} .$$

It follows that

$$\sum_{k=0}^{n} \binom{n}{k}^2 F_{k+j} = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k}F_{j+k-n} , \tag{4.8}$$

$$\sum_{k=0}^{n} \binom{n}{k}^2 L_{k+j} = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k}L_{j+k-n} . \tag{4.9}$$

For $j = 0$, (4.8) and (4.9) reduce to (4.1) and (4.2), respectively.

If in the next place we replace $u = \alpha^2, \beta^2$ in (4.6), we get

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

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

so that

$$\sum_{k=0}^{n} \binom{n}{k}^2 F_{2k+j} = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k} F_{n-k+j} , \tag{4.10}$$

$$\sum_{k=0}^{n} \binom{n}{k}^2 L_{2k+j} = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k} L_{n-k+j} . \tag{4.11}$$

These formulas evidently include (4.3) and (4.4).

In exactly the same way (4.7) yields

$$\sum_{k=0}^{n} \binom{n}{k}^2 F_{k+j} = \sum_{k=0}^{n} (-1)^{n-k}\binom{n}{k}\binom{n+k}{k} F_{2k+j-n} , \tag{4.12}$$

$$\sum_{k=0}^{n} \binom{n}{k}^2 L_{k+j} = \sum_{k=0}^{n} (-1)^{n-k}\binom{n}{k}\binom{n+k}{k} L_{2k+j-n} , \tag{4.13}$$

and

$$\sum_{k=0}^{n} \binom{n}{k}^2 F_{2k+j} = \sum_{k=0}^{n} (-1)^{n-k}\binom{n}{k}\binom{n+k}{k} F_{k+j+n} , \tag{4.14}$$

$$\sum_{k=0}^{n} \binom{n}{k}^2 L_{2k+j} = \sum_{k=0}^{n} (-1)^{n-k}\binom{n}{k}\binom{n+k}{k} L_{k+j+n} . \tag{4.15}$$

The identities (4.8), $\cdots$, (4.15) can be generalized further by employing, in place of (4.5), the following formulas for Jacobi polynomials 1, 255 :

$$P_n^{(\lambda,\mu)}(x) = \sum_{k=0}^{n} \binom{n+\lambda}{n-k}\binom{n+\mu}{k}\left(\frac{x-1}{2}\right)^k\left(\frac{x+1}{2}\right)^{n-k}$$

$$= \binom{\lambda+n}{n}\sum_{k=0}^{n}\binom{n}{k}\frac{(n+\lambda+\mu+1)_k}{(\lambda+1)_k}\left(\frac{x-1}{2}\right)^k$$

$$= \binom{\mu+n}{n}\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\frac{(n+\lambda+\mu+1)_k}{(\mu+1)_k}\left(\frac{x+1}{2}\right)^k ,$$

where

$$(\lambda+1)_n = (\lambda+1)(\lambda+2)\cdots(\lambda+n), \qquad (\lambda+1)_0 = 1 .$$

The final results are

$$(4.16)\qquad \sum_{k=0}^{n}\binom{n+\lambda}{k}\binom{n+\mu}{n-k}F_{k+j} = \binom{\lambda+n}{n}\sum_{k=0}^{n}\binom{n}{k}\frac{(n+\lambda+\mu+1)_k}{(\lambda+1)_k}F_{j+k-n},$$

$$(4.17)\qquad \sum_{k=0}^{n}\binom{n+\lambda}{k}\binom{n+\mu}{n-k}L_{k+j} = \binom{\lambda+n}{n}\sum_{k=0}^{n}\binom{n}{k}\frac{(n+\lambda+\mu+1)_k}{(\lambda+1)_k}L_{j+k-n},$$

$$(4.18)\qquad \sum_{k=0}^{n}\binom{n+\lambda}{k}\binom{n+\mu}{n-k}F_{2k+j} = \binom{\lambda+n}{n}\sum_{k=0}^{n}\binom{n}{k}\frac{(n+\lambda+\mu+1)_k}{(\lambda+1)_k}F_{n-k+j},$$

$$(4.19)\qquad \sum_{k=0}^{n}\binom{n+\lambda}{k}\binom{n+\mu}{n-k}L_{2k+j} = \binom{\lambda+n}{n}\sum_{k=0}^{n}\binom{n}{k}\frac{(n+\lambda+\mu+1)_k}{(\lambda+1)_k}L_{n-k+j},$$

$$(4.20)\qquad \sum_{k=0}^{n}\binom{n+\lambda}{k}\binom{n+\mu}{n-k}F_{k+j} = \binom{\mu+n}{n}\sum_{k=0}^{n}\binom{n}{k}\frac{(n+\lambda+\mu+1)_k}{(\lambda+1)_k}F_{j+2k-n},$$

$$(4.21)\qquad \sum_{k=0}^{n}\binom{n+\lambda}{k}\binom{n+\mu}{n-k}L_{k+j} = \binom{\mu+n}{n}\sum_{k=0}^{n}\binom{n}{k}\frac{(n+\lambda+\mu+1)_k}{(\lambda+1)_k}L_{j+2k-n},$$

$$(4.22)\qquad \sum_{k=0}^{n}\binom{n+\lambda}{k}\binom{n+\mu}{n-k}F_{2k+j} = \binom{\mu+n}{n}\sum_{k=0}^{n}\binom{n}{k}\frac{(n+\lambda+\mu+1)_k}{(\lambda+1)_k}F_{j+k+n},$$

$$(4.23)\qquad \sum_{k=0}^{n}\binom{n+\lambda}{k}\binom{n+\mu}{n-k}L_{2k+j} = \binom{\mu+n}{n}\sum_{k=0}^{n}\binom{n}{k}\frac{(n+\lambda+\mu+1)_k}{(\lambda+1)_k}L_{j+k+n}.$$

We remark that taking $u = -\alpha$ in (4.6) leads to

$$(4.24)\qquad \sum_{k=0}^{n}(-1)^k\binom{n}{k}^2F_{k+j} = \sum_{n=0}^{n}(-1)^{n-k}\binom{n}{k}\binom{n+k}{k}F_{2n-2k+j},$$

$$(4.25)\qquad \sum_{k=0}^{n}(-1)^k\binom{n}{k}^2L_{n+j} = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\binom{n+k}{k}L_{2n-2k+j},$$

and so on.

Some of the formulas in the earlier part of the paper are certainly not new. However, we have not attempted the rather hopeless task of finding where they first occurred. In any event, it may be of interest to derive them by the methods of the present paper. It would, of course, be possible to find many additional identities.

REFERENCE

1. E. D. Rainville, Special Functions, Macmillan, New York, 1960.

* * * * *

ADVANCED PROBLEMS AND SOLUTIONS

Edited by
RAYMOND E. WHITNEY
Lock Haven State College, Lock Haven, Pennsylvania

Send all communications concerning Advanced Problems and Solutions to Raymond E. Whitney, Mathematics Department, Lock Haven State College, Lock Haven, Pennsylvania 17745. This department especially welcomes problems believed to be new or extending old results. Proposers should submit solutions or other information that will assist the editor. To facilitate their consideration, solutions should be submitted on separate signed sheets within two months after publication of the problems.

H-166 Proposed by H. H. Ferns, Victoria, B. C., Canada.

Prove the identity

$$F_{2mn} = \begin{cases} \sum_{i=1}^{n} \binom{n}{i} L_m^i F_{mi} & \text{if } m \text{ is odd} \\ \sum_{i=1}^{n} (-1)^{n+i} L_m^i F_{mi} & \text{if } m \text{ is even} \end{cases},$$

where F_n and L_n are the n^{th} Fibonacci and n^{th} Lucas numbers, respectively.

H-167 Proposed by L. Carlitz, Duke University, Durham, North Carolina.

Put

$$S_k = \sum_{n=1}^{\infty} \frac{1}{F_n F_{n+k}} .$$

Show that, for $k \geq 0$,

$$\text{(A)} \qquad F_{2k+2} S_{2k+2} = k + 1 - \sum_{n=1}^{2k} \frac{k - \left[\frac{1}{2}(n-1)\right]}{F_n F_{n+2}} ,$$

(B) $$F_{2k+1}S_{2k+1} = S_1 - k + \sum_{n=0}^{2k-1} \frac{k - \left[\frac{n}{2}\right]}{F_n F_{n+2}},$$

where $[a]$ denotes the greatest integer function.

Special cases of (A) and (B) have been proved by Brother Alfred Brousseau, "Summation of Infinite Fibonacci Series," Fibonacci Quarterly, Vol. 7, No. 2, April, 1969, pp. 143-168.

H-168 Proposed by David A. Klarner, University of Alberta, Edmonton, Alberta, Canada.

If

$$a_{ij} = \binom{i + j - 2}{i - 1}$$

for $i, j = 1,2,\cdots,n$, show that $\det\{a_{ij}\} = 1$.

SOLUTIONS

GENERALIZE

H-137 Proposed by J. L. Brown, Jr., Ordnance Research Laboratory, State College, Pennsylvania.

GENERALIZED FORM OF H-70: Consider the set S consisting of the first N positive integers and choose a fixed integer k satisfying $0 < k \leq N$. How many different subsets A of S (including the empty subset) can be formed with the property that $a' - a'' \neq k$ for any two elements a', a'' of A: that is, the integers i and k + k do not both appear in A for any $i = 1,2, \cdots, N - k$.

Solution by the Proposer.

Let $N = r \pmod k$ so that $N = tk + r$ with t a positive integer and $0 \leq r \leq k - 1$.

Each subset A of S can be made to correspond to a binary sequence $(\alpha_1,\alpha_2,\alpha_3,\cdots,\alpha_N)$ of N terms by the rule that $\alpha_i = 1$ if $i \in A$ and $\alpha_i = 0$ if $i \notin A$. For a given subset A and its corresponding binary sequence $(\alpha_1, \alpha_2, \cdots, \alpha_N)$, define k binary sequences as follows:

$$\begin{aligned}
A_1 &= (\alpha_1, \alpha_{1+k}, \alpha_{1+2k}, \cdots, \alpha_{1+tk}) \\
A_2 &= (\alpha_2, \alpha_{2+k}, \alpha_{2+2k}, \cdots, \alpha_{2+tk}) \\
&\vdots \\
A_r &= (\alpha_r, \alpha_{r+k}, \alpha_{r+2k}, \cdots, \alpha_{r+tk}) \\
A_{r+1} &= (\alpha_{r+1}, \alpha_{r+1+k}, \alpha_{r+1+2k}, \cdots, \alpha_{r+1+(t-1)k}) \\
&\vdots \\
A_k &= (\alpha_k, \alpha_{2k}, \alpha_{3k}, \cdots, \alpha_{tk}) \quad .
\end{aligned}$$

Then the subset A corresponding to $(\alpha_1, \alpha_2, \cdots, \alpha_N)$ satisfies the given constraint if and only if each A_m independently for $m = 1,2,\cdots,k$ is a binary sequence without consecutive 1's. But it is well known that the total number of binary sequences of length n without consecutive 1^s is F_{n+2}. Since each of the r sequences $A_1,\cdots,A_r$ has length $t+1$ and each of the remaining $k-r$ sequences $A_{r+1},\cdots,A_k$ has length t, it follows that the total number of subsets with the required property is $F_{r+3}^{r} F_{t-2}^{k-r}$.

Also solved by M. Yoder.

FIBONOMIALS

H-138 Proposed by George E. Andrews, Pennsylvania State University, University Park, Pennsylvania.

If F_n denotes the sequence of polynomials $F_1 = F_2 = 1$, $F_n = F_{n-1} + x^{n-2}F_{n-2}$, prove that $1 + x + x^2 + \cdots + x^{p-1}$ divides F_{p+1} for any prime $p = \pm 2 \pmod 5$.

Solution by L. Carlitz, Duke University, Durham, North Carolina.

Let $\Phi_n(x)$ denote the cyclotomic polynomial:

$$\Phi_n(x) = \prod_{rs=n} (x^r - 1)^{\mu(s)} \quad ,$$

where $\mu(s)$ is the Mobius function. We shall prove that F_{n+1} is divisible by $\Phi_n(x)$ if and only if $n \equiv \pm 2 \pmod 5$, where n is an arbitrary positive integer

(not necessarily prime). Indeed, we obtain the residue of $F_{n+1} \pmod{\Phi_n(x)}$ for all n. In particular, we find that

$$F_{n+1} \equiv 1 \pmod{\Phi_n(x)},$$

when $n \equiv \pm 1 \pmod{10}$.

I. Schur (Berliner Sitzungsberichte (1917), pp. 302-321) has proved that if

$$F_1 = F_2 = 1, \quad F_{n+2} = F_{n+1} + x^n F_n \qquad (n \geq 1),$$

then

$$F_{n+1} = \sum_{k=-r}^{r} (-1)^k x^{\frac{1}{2}k(5k-1)} \begin{bmatrix} n \\ e(k) \end{bmatrix} , \tag{1}$$

where

$$e(k) = \left[\tfrac{1}{2}(n + 5k)\right], \qquad r = \left[\tfrac{1}{5}(n + 2)\right]$$

and

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{cases} \dfrac{(1 - x^n)(1 - x^{n-1}) \cdots (1 - x^{n-k+1})}{(1 - x)(1 - x^2) \cdots (1 - x^k)} & (0 \leq k \leq n), \\ 0 & (\text{otherwise}). \end{cases}$$

$\begin{bmatrix} n \\ k \end{bmatrix}$ is a polynomial in x with positive integral coefficients: also it is evident from the definition that for $1 \leq k \leq n$, $\begin{bmatrix} n \\ k \end{bmatrix}$ is divisible by the cyclotomic polynomial $\Phi_n(x)$.

Thus (1) implies

$$F_{n+1} \equiv (-1)^r x^{\frac{1}{2}r(5r-1)} \begin{bmatrix} n \\ e(r) \end{bmatrix} + (-1)^r x^{\frac{1}{2}r(5r+1)} \begin{bmatrix} n \\ e(-r) \end{bmatrix} \pmod{\Phi_n(x)}. \tag{2}$$

The following table is easily verified.

n	r	e(r)	e(-r)
10 m	2 m	10 m	0
10 m + 1	2 m	10 m	0
10 m + 2	2 m	10 m + 1	1
10 m + 3	2 m + 1	10 m + 4	-1
10 m + 4	2 m + 1	10 m + 4	-1
10 m + 5	2 m + 1	10 m + 5	0
10 m + 6	2 m + 1	10 m + 5	0
10 m + 7	2 m + 1	10 m + 6	1
10 m + 8	2 m + 2	10 m + 9	-1
10 m + 9	2 m + 2	10 m + 9	-1

Therefore, making use of (2), we get the following values for the residue of $F_{n+1} \pmod{\Phi_n(x)}$:

n	residue of $F_{n+1} \pmod{\Phi_n(x)}$
10 m	$x^{m(10m-1)} + x^{m(10m+1)} \equiv x^{9m} + x^{m}$
10 m + 1	$x^{m(10m+1)} \equiv 1$
10 m + 2	0
10 m + 3	0
10 m + 4	$-x^{(2m+1)(5m+2)} \equiv -x^{5m+2}$
10 m + 5	$-x^{(2m+1)(5m+2)} - x^{(2m+1)(5m+3)} \equiv -x^{4m+2} - x^{6m+3}$
10 m + 6	$-x^{(2m+1)(5m+3)} \equiv -x^{5m+3}$
10 m + 7	0
10 m + 8	0
10 m + 9	$x^{(m+1)(10m+9)} \equiv 1$

As a check, we compute F_{n+1}, $2 \leq n \leq 10$, and the corresponding residues,

n	F_{n+1}	residue $(\mathrm{mod}\ \Phi_n)$
2	$1 + x$	0
3	$1 + x + x^2$	0
4	$1 + x + x^2 + x^3 + x^4$	$1 \equiv -x^2$
5	$1 + x + x^2 + x^3 + 2x^4 + x^5 + x^6$	$-x^2 - x^3$
6	$1 + x + x^2 + x^3 + 2x^4 + 2x^5 + 2x^6 + x^7 + x^8 + x^9$	$1 \equiv -x^3$
7	$1 + x + x^2 + x^3 + 2x^4 + 2x^5 + 3x^6 + 2x^7 + 2x^8 + 2x^9 + 2x^{10} + x^{11} + x^{12}$	0
8	$1 + x + x^2 + x^3 + 2x^4 + 2x^5 + 3x^6 + 3x^7 + 3x^8 + 3x^9 + 3x^{10} + 3x^{11} + 3x^{12} + 2x^{13} + x^{14} + x^{15} + x^{16}$	0
9	$1 + x + x^2 + x^3 + 2x^4 + 2x^5 + 3x^6 + 3x^7 + 4x^8 + 4x^9 + 4x^{10} + 4x^{11} + 5x^{12} + 4x^{14} + 3x^{15} + 3x^{16} + 2x^{17} + 2x^{18} + x^{19} + x^{20}$	1

Remarks. 1. If we use the fuller notation $F_n(x)$ in place of F_n and ϵ denotes a primitive n^{th} root of unity, then the statement $F_{n+1}(x)$ is divisible by $\Phi_n(x)$ is equivalent to $F_{n+1}(\epsilon) = 0$. Using the recurrence for F_n, it is not difficult to show that, for n odd,

$$F_{n+1}(\epsilon) = \left| F_{\frac{1}{2}(n+3)}(\epsilon) \right|^2 - \left| F_{\frac{1}{2}(n-1)}(\epsilon) \right|^2 ,$$

while for n even,

$$F_{n+1}(\epsilon) = \left| F_{k+1}(\epsilon) \right|^2 + \epsilon^{-k} \left| F_k(\epsilon) \right|^2 \qquad (n = 2k) .$$

2. In the next place, it follows from the recurrence that

$$\sum_{n=0}^{\infty} F_{n+1} a^n = \sum_{k=0}^{\infty} \frac{a^{2k} x^{k^2}}{(a)_k} , \tag{3}$$

where

$$(a)_k = (1 - a)(1 - ax) \cdots (1 - ax^k) .$$

Since

$$\frac{1}{(a)_k} = \sum_{r=0}^{\infty} \begin{bmatrix} k+r \\ r \end{bmatrix} a^r ,$$

we get

$$F_{n+1} = \sum_{2k \le n} \begin{bmatrix} n-k \\ k \end{bmatrix} x^{k^2} .$$

If we take $a = x$ in (3), we get

$$1 + \sum_{n=1}^{\infty} F_n x^n = \sum_{k=0}^{\infty} \frac{x^{k^2}}{(x)_k} = \prod_{n=0}^{\infty} (1 - x^{5n+1})^{-1} (1 - x^{5n+4})^{-1} ,$$

by the first Roger-Ramanujan identity (see, for example, Hardy and Wright, Introduction to the Theory of Numbers, Oxford, 1954, p. 290).

Incidentally, if

$$G_1 = G_2 = 1, \quad G_{n+1} = G_n + x^n G_{n-1} \qquad (n > 1) ,$$

then we have

$$\sum_{n=0}^{\infty} G_{n+1} a^n = \sum_{k=0}^{\infty} \frac{a^{2k} x^{k^2+k}}{(a)_k} , \tag{4}$$

and

$$G_{n+1} = \sum_{2k \le n} \begin{bmatrix} n-k \\ k \end{bmatrix} x^{k^2+k} .$$

If we take $a = x$ in (4), we get

$$1 + G_n x^n = \sum_{k=0}^{\infty} \frac{x^{k^2+k}}{(x)_k} = \prod_{n=0}^{\infty} (1 - x^{5n+2})^{-1} (1 - x^{5n+3})^{-1}$$

by the second Rogers-Ramanujan identity.

INTEGRITY

H-140 Proposed by Douglas Lind, University of Virginia, Charlottesville, Virginia.

For a positive integer m, let $\alpha = \alpha(m)$ be the least positive integer such that $F_\alpha \equiv 0 \pmod m$. Show that the highest power of a prime p dividing $F_1F_2 \cdots F_n$ is

$$\sum_{k=1}^{\infty} \left[\frac{n}{\alpha(p^k)} \right]$$

where $[x]$ denotes the greatest integer contained in x. Using this, show that the Fibonacci binomial coefficients

$$\begin{bmatrix} m \\ r \end{bmatrix} = \frac{F_m F_{m-1} \cdots F_{m-r+1}}{F_1 F_2 \cdots F_r} \qquad (r > 0)$$

are integers.

Solution by the Proposer.

It is known [D. D. Wall, "Fibonacci Series Modulo m," Amer. Math. Monthly, 67 (1960), 525-532] that $F_r \equiv 0 \pmod m$ if and only if $r \equiv 0 \pmod{\alpha(m)}$. Then the number of F_r with $r \leq n$ which are exactly divisible by p^k is $[n/\alpha(p^k)]$, establishing the first part. Note that $\alpha(p^k) \to \infty$ as $k \to \infty$, so for fixed p this is actually a finite sum.

Now let $(m) = F_1F_2 \cdots F_m$. Then

$$\begin{bmatrix} m \\ r \end{bmatrix} = \frac{(m)!}{(r)!(m-r)!} .$$

It suffices to show that for any prime p, the highest power of p dividing the numerator is not less than that dividing the denominator. By the first part, this is equivalent to

$$(\star) \qquad \sum_{k=1}^{\infty}\left[\frac{m}{\alpha(p^k)}\right] \geq \sum_{k=1}^{\infty}\left[\frac{r}{\alpha(p^k)}\right] + \sum_{k=1}^{\infty}\left[\frac{m-r}{\alpha(p^k)}\right] .$$

But the elementary inequality $[x + y] \geq [x] + [y]$ shows that

$$\left[\frac{m}{\alpha}\right] \geq \left[\frac{r}{\alpha}\right] + \left[\frac{m - r}{\alpha}\right] ,$$

implying (⋆) and the result.

Also solved by M. Yoder.

★ ★ ★ ★ ★

[Continued from page 30.]

6. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford, 1930, fourth ed., 1960.
7. O. Wyler, "On Second-Order Recurrences," Amer. Math. Monthly, 72, pp. 500-506, May, 1965,
8. D. D. Wall, "Fibonacci Series Modulo m," Amer. Math. Monthly, 67, pp. 525-532 (June 1960).
9. R. P. Backstrom, "On the Determination of the Zeros of the Fibonacci Sequence," Fibonacci Quarterly, Vol. 5, pp. 313-322, December, 1966.

★ ★ ★ ★ ★

JUST OUT
by Joseph and Frances Gies

A new book---Leonardo of Pisa and the new mathematics of the Middle Ages---concerning our Fibonacci. Thomas Y. Crowell Company, New York, 1970, pp. 127 --$3.95.

ARITHMETIC OF PENTAGONAL NUMBERS

RODNEY T. HANSEN
Montana State University, Bozeman, Montana

The pentagonal numbers are the integers

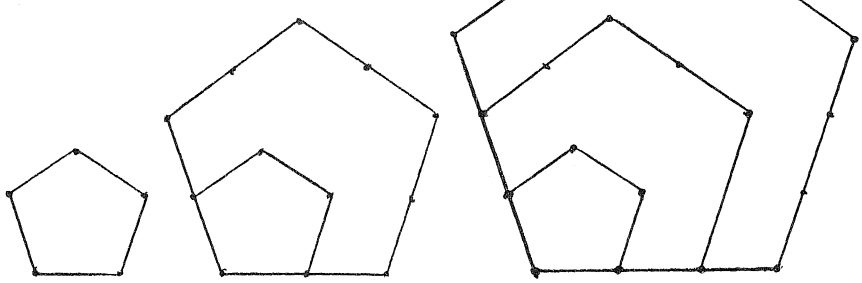
$$p_n = \frac{n}{2}(3n - 1), \qquad n = 1,2,\cdots .$$

Each number p_n can also be derived by summing the first n terms of the arithmetic progression

$$1, 4, 7, 10, 13, \cdots, 3m - 2 .$$

Geometrically, considering regular pentagons homothetic with respect to one of the vertices and containing 2, 3, 4, $\cdots$, n points at equal distances along each side, the sum of all points for a given n yields p_n. Pictorially we have the following: [1, p. 10]

n: 1 2 3 4



p_n: .

In this paper we shall give several algebraic identities involving pentagonal numbers of different orders. The principal result is that an infinite number of pentagonal numbers exist which are, at the same time, the sum and difference of distinct pentagonal numbers. A similar result for triangular numbers has been found by W. Sierpinski [2, pp. 31-32].

A table of p_n's will first be constructed.

p_n	0	1	2	3	4	5	6	7	8	9
0		1	5	12	22	35	51	70	92	117
1	145	176	210	247	287	330	376	425	477	532
2	590	651	715	782	852	925	1,001	1,080	1,162	1,247
3	1,335	1,426	1,520	1,617	1,717	1,820	1,926	2,035	2,147	2,262
4	2,380	2,501	2,625	2,752	2,882	3,015	3,115	3,290	3,432	3,577
5	3,725	3,876	4,030	4,187	4,347	4,510	4,676	4,845	5,017	5,192
6	5,370	5,551	5,735	5,922	6,112	6,305	6,501	6,700	6,902	7,107
7	7,315	7,526	7,740	7,957	8,177	8,400	8,626	8,855	9,087	9,322
8	9,560	9,801	10,045	10,292	10,542	10,795	11,051	11,310	11,572	11,837
9	12,105	12,376	12,650	12,927	13,207	13,490	13,776	14,065	14,357	14,652

We note from the above-given arithmetic progression that

$$p_n - p_{n-1} = 3n - 2, \qquad \text{for} \quad n = 2, 3, \cdots,$$

and from the above table that

$$p_8 = p_4 + p_7, \quad p_{24} = p_7 + p_{23}, \quad p_{49} = p_{10} + p_{48}, \quad \text{and} \quad p_{33} = p_{13} + p_{32}.$$

Noting that the first term on the right of each of the above equalities is of the form $3n + 1$, we find that

$$p_{3n+1} = \frac{(3n + 1)}{2} [3(n + 1) - 1] = \frac{1}{2}(27n^2 + 15n + 2).$$

Setting

$$p_m - p_{m-1} = 3m - 2 = \frac{1}{2}(27n^2 + 15n + 2)$$

we have

$$m = \frac{1}{2}(9n^2 + 5n + 2),$$

an integer. The first theorem follows.

Theorem 1. For any integer $n \geq 1$,

$$p_{\frac{1}{2}(9n^2+5n+2)} = p_{(3n+1)} + p_{\frac{n}{2}(9n+5)} .$$

A subset of the above defined pentagonal numbers yields our main result.

Theorem 2. For any positive integer n,

$$p_{\frac{1}{2}[9(3n)^2+5(3n)+2]} = p_{[3(3n)+1]} + p_{\frac{3n}{2}[9(3n)+5]}$$

$$= p_{\frac{1}{8}(6561n^4+2430n^3+495n^2+50n+8)} - p_{\frac{n}{8}(6561n^3+2430n^2+495n+50)}$$

Proof. First it is necessary to express

$$p_{\frac{1}{2}(81n^2+15n+2)}$$

in terms of n.

$$p_{\frac{1}{2}(81n^2+15n+2)} = \frac{\frac{1}{2}(81n^2 + 15n + 2)}{2} \left\{ 3\left[\frac{1}{2}(81n^2 + 15n + 2)\right] - 1 \right\}$$

$$= \frac{1}{8}(19,683n^4 + 7290n^3 + 1485n^2 + 150n + 8) .$$

Equating $p_s - p_{s-1}$ to

$$p_{\frac{1}{2}(81n^2+15n+2)}$$

yields

$$s = \frac{1}{8}(6561n^4 + 2430n^3 + 495n^2 + 50n + 8) .$$

By mathematical induction on n we have that s is an integer; completing the proof.

For $n = 1$ and 2 we have, for example,

$$p_{49} = p_{10} + p_{48} = p_{1193} - p_{1192}$$

or

$$3577 = 145 + 3432 = 2,134,277 - 2,130,700$$

and

$$p_{178} = p_{19} + p_{177} = p_{15,813} - p_{15,812}$$

or

$$47,437 = 532 + 46,905 = 375,068,547 - 375,021,110 .$$

A rather curious relationship exists between n and p_{sn}; namely, that each positive integer can be expressed in an infinite number of ways as a quadratic expression involving a pentagonal number.

Theorem 3. Any positive integer n can be expressed as

$$n = \frac{1 + \sqrt{1 + 24p_{s \cdot n}}}{6 \cdot s}$$

for any positive integer s.

Proof. From the definition of a pentagonal number we have

$$p_{sn} = \frac{sn}{2}(3 \cdot sn - 1) = \frac{3(sn)^2 - sn}{2}$$

$$0 = 3s^2n^2 - sn - 2p_{sn}$$

$$n = \frac{+s \pm \sqrt{(-s)^2 - 4(3s^2)(-2p_{sn})}}{2 \cdot 3s^2} = \frac{1 \pm \sqrt{1 + 24p_{sn}}}{6s} .$$

Taking the positive root, the desired result is obtained.

The pentagonal numbers are not closed with respect to the operation of multiplication. However, the following three cases are quickly verified:

$$p_{87} = p_2 p_{39}, \quad p_{187} = p_4 p_{40}, \quad \text{and} \quad p_{392} = p_7 p_{47} .$$

It is not known if an infinite number of such pairs exist.

REFERENCES

1. J. V. Uspensky and M. A. Heaslet, Elementary Number Theory, McGraw-Hill, New York, 1939.
2. W. Sierpiński, "Un théorème sur les nombres triangulaires," Elemente Der Mathematik, Bank 23, Nr 2 (März, 1968), pp. 31-32.

* * * * *

CORRECTIONS

Please make the following changes in "Associated Additive Decimal Digital Bracelets," appearing in the Fibonacci Quarterly in October, 1969:

On page 288, line 25, change "terms" to "forms."

On page 289, line 2, change "8" to read "B."

On page 290, line 11, change "7842" to "6842."

On page 290, line 13, change "and" to read "And."

On page 294, line 20, change "19672" to read "1967)."

On page 294, line 26, change "1969" to read "1959."

Please change the formulas given in "Diagonal Sums of Generalized Pascal Triangles," page 353, Volume 7, No. 5, December, 1969, lines 11 and 12, to read

$$p_1(q) = \sum_{k=0}^{[q/3]} \sum_{m=0}^{\left[\frac{q-3k}{2}\right]} \frac{q(q - m - 2k - 1)!}{(q - 2m - 3k)!m!k!} \cdot \left(\frac{x}{1 - x}\right)^{q-m-2k}$$

$$p_2(q) = \sum_{k=0}^{[q/3]} \sum_{m=0}^{\left[\frac{q-3k}{2}\right]} \frac{q(q - m - 2k - 1)!}{(q - 2m - 3k)!m!k!} \cdot \left(\frac{x}{1 - x}\right)^{q-k} (-1)^{q-m-3k}$$

LETTERS TO THE EDITOR

Dear Editor:

It may be of interest to your readers to note that there is a simple elementary proof of Theorem 7, page 91, Vol. 6, No. 3, June 1968, by D. A. Lind, which uses the method of descent.

To restate the Theorem,

Theorem

(1) $$5x^2 \pm 4 = y^2 ,$$

if and only if x is a Fibonacci number and y is the corresponding Lucas number.

Proof. It is a simple identity to show that a Fibonacci and Lucas number satisfy (1) using the identities $u_n = u_{n+1} - u_{n-1}$, $v_n = u_{n+1} + u_{n-1}$, and $u_{n+1}u_{n-1} - u_n^2 = (-1)^n$.

To show the converse, suppose x is the smallest positive integer which is not a Fibonacci number which satisfies (1). Then $x \geq 4$ so that clearly $2x < y < 3x$ and y is the same parity as x. Hence, let $y = x + 2t$ with $t < x$. By substitution,

$$4x^2 - 4tx - 4t^2 \pm 4 = 0$$

solving for $2x$,

$$2x = t \pm \sqrt{5t^2 \pm 4}$$

so that

$$5t^2 \pm 4 = s^2$$

where t and s are integers. Therefore t is a smaller solution to (1) than x so t must be a Fibonacci number and s is the corresponding Lucas number. But then

$$2x = u_n \pm v_n$$

and since $v_n > u_n$, $n > 1$

$$2x = u_n + v_n = 2u_{n+1}$$

so that x is a Fibonacci number if t is, QED.

I have continued to enjoy the Fibonacci Quarterly since its inception. Keep up the good work.

David E. Ferguson
Programmatics, Inc.,
Los Angeles, California

Dear Editor:

I cheerfully donate these formulas to you. I think they have a place in the Quarterly. If you agree and feel you would like to develop a note on the basis of these formulas, I would be happy indeed.

$$\begin{aligned}
L_n &= L_n \\
L_n^2 &= L_{2n} + 2(-1)^n \\
L_n^3 &= L_{3n} + 3L_n(-1)^n \\
L_n^4 &= L_{4n} + 4L_n^2 + 2(-1)^{n+1}(-1)^n \\
L_n^5 &= L_{5n} + 5L_n^3 + 5L_n(-1)^{n+1}(-1)^n \\
L_n^6 &= L_{6n} + 6L_n^4 + 9L_n^2(-1)^{n+1} + 2(-1)^n \\
L_n^7 &= L_{7n} + 7L_n^5 + 14L_n^3(-1)^{n+1} + 7L_n(-1)^n \\
L_n^8 &= L_{8n} + 8L_n^6 + 20L_n^4(-1)^{n+1} + 16L_n^2 + 2(-1)^{n+1}(-1)^n \\
L_n^9 &= L_{9n} + 9L_n^7 + 27L_n^5(-1)^{n+1} + 30L_n^3 + 9L_n(-1)^{n+1}(-1)^n \\
L_n^{10} &= L_{10n} + 10L_n^8 + 35L_n^6(-1)^{n+1} + 50L_n^4 + 25L_n^2(-1)^{n+1} + 2(-1)^n \\
&\quad . \quad .
\end{aligned}$$

Harlan L. Umansky
Emerson High School
Union City, New Jersey

★ ★ ★ ★ ★

SPIRALS, CHECKERBOARDS, POLYOMINOES, AND THE FIBONACCI SEQUENCE

JEAN H. ANDERSON
2400 Ione Street, St. Paul, Minnesota 55113

Any number N may be written as the sum of powers of two; that is,

$$N = a_{n-1} \cdot 2^{n-1} + a_{n-2} \cdot 2^{n-2} + \cdots + a_1 \cdot 2^1 + a_0 \cdot 2^0 ,$$

where the coefficients are each either 1 or 0. Thus, for example,

$$\begin{aligned} 37 &= 32 + 4 + 1 \\ &= 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\ &= 100101 \text{ in binary notation.} \end{aligned}$$

Suppose that, beginning at the right-hand side, the whole expression for N is coiled up and fitted onto a checkerboard with $a_0 \cdot 2^0$ at the lower-left (red) of the four central cells and the other terms proceeding in a counterclockwise manner. Then the upper left (black) cell of the board coincides with $a_{63} \cdot 2^{63}$. We can say that a vacant cell represents a 0 coefficient and a cell containing a pawn represents a 1 coefficient. Thus any number N (smaller than 2^{64}) may be indicated by a unique arrangement of pawns on the checkerboard; conversely, any particular arrangement of pawns corresponds to a unique number N.

The following observations may be made:

1. Since the spiral can be continued indefinitely or terminated at any integer, checkerboards of any size may be so covered.

2. Cells can be labeled with the corresponding exponent of two. Pawns placed on 0, 4, 16, and 36, for example — along the upper left diagonal — correspond to the binary number 1000000000000000000010000000000010001, or 68,719,542,289 in the customary base ten notation.

3. A k-by-k board can be used to represent any number K less than $2^{(k)^2}$.

4. Any cell has a numerical value greater than the sum of all lesser cells.

5. With the usual placement of the checkerboard having the lower left corner colored red, all red cells are labeled with even numbers — including 0 — and all black cells are labeled with odd numbers.

6. The "parity" of a number N is defined as the absolute value of the difference between the number of pawns on black cells and the number of pawns on red cells in its checkerboard representation. With an even number of pawns the parity is always even, while an odd number of pawns has an odd parity.

7. Any cell n lies rookwise adjacent to at most four cells, with no cell greater than $(k)^2$, the size of the board. These cells are:

(1) If n is a square, the adjacent cells are $n + 1$, $n - 1$, $n + 4\sqrt{n} + 3$, and $n + 4\sqrt{n} + 5$. These values of n lie at the corners of the spiral which fall along the diagonal going upward to the left and passing through cells 0 and 1. If $n - 1$ is negative (for the 0 cell only), replace $n - 1$ by 7.

(2) For cells lying along the diagonal upward to the right, that is, if n is of the form $a \cdot (a + 1)$, then the adjacent cells are $n + 1$, $n - 1$, $n + 4[\sqrt{n}] + 5$, and $n + 4[\sqrt{n}] + 7$, where the brackets [ ] indicate $n - 1$ is negative (for the 0 cell only), replace $n - 1$ by 3.

(3) For all other cells, the adjacent cells are $n + 1$, $n - 1$, $n + 4[\sqrt{n}] + 6 + j$, and $n - 4[\sqrt{n}] + 2 - j$, where $j = +1$ if $n > [\sqrt{n}] \cdot [\sqrt{n} + 1]$, and $j = -1$ if $n < [\sqrt{n}] \cdot [\sqrt{n} + 1]$. If $n = [\sqrt{n}] \cdot [\sqrt{n} + 1]$, the formulae in (2) should be used; if $\sqrt{n} = [\sqrt{n}]$, the formulae in (1) should be used.

The above rules enable us to travel from any cell to any other cell on any size checkerboard, without even seeing the board, simply by repeated applications of algebraic formulae. The only limitation is that the board be either square — $(k)^2$ — or square plus one extra row — $(k) \cdot (k + 1)$ — for any k.

NUMBERS REPRESENTED BY p PAWNS

One can easily (in theory, anyhow) make a list N(p) of all numbers which can be expressed by exactly p pawns. For $p = 5$, for example, the list begins with $N(5)_{min} = 2^5 - 1 = 31$, and continues 47, 55, 59, 61, 62, 79, 87, 91, 94, 103, 107, 109, 110, 115, 117, 118, 121, $\cdots$.

The number of integers less than 2^z which can be represented by one pawn is obviously z; it is the number of ways of selecting one object from z identical objects. The number of integers less than z which can be represented by p pawns is

$$\binom{z}{p} = \frac{z!}{p!(z-p)!} ,$$

or, for 5 pawns and a regulation checkerboard,

$$\binom{64}{5} = \frac{64 \cdot 63 \cdot 62 \cdot 61 \cdot 60}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 7{,}624{,}512 ,$$

a not inconsequential number. For $z = 16$ the number of integers represented by 5 pawns drops to 4368.

Question: What is the largest integer (decimal notation) that can be represented by 5 pawns on a 4-by-4 checkerboard? (See Fig. 1.)

Answer: The board has $(4)^2 = 16$ cells. The cells giving the largest number using five pawns are cells 15, 14, 13, 12, and 11, corresponding to the number $2^{15} + 2^{14} + 2^{13} + 2^{12} + 2^{11}$, or $32768 + 16384 + 8192 + 4096 + 2048 = 63, 448$.

THE FIBONACCI SEQUENCE

Some interesting patterns on the checkerboard are obtained by plotting the Fibonacci sequence: $F_1 = 1$, $F_2 = 1$, $F_3 = 2, \cdots, F_{k+2} = F_k + F_{k+1}$. (At each step simply add together the binary representations of the last two numbers. $F_1 = F_2$, F_3, F_4, F_7, F_{10}, F_{13}, F_{16}, and F_{22}, alone of **all** Fibonacci numbers less than F_{60} (= 1548008755920), possess the property that each pawn lies rookwise adjacent to at least one other pawn. This happens to be the property defining the polyominoes. Specifically, F_{10} (= 55) is the U-pentomino and F_{13} (= 233) is the P-pentomino. (See Solomon W. Golomb, Polyominoes, for an extensive discussion of polyomino properties and problems.)

The Lucas sequence ($L_1 = 1$, $L_2 = 2$, $L_{k+2} = L_k + L_{k+1}$) similarly produces several polyominoes at the beginning of the run, notably the pentominoes P (= 47) and W (= 199). Other sequences do the same. (See V. E. Hoggatt, Jr., Fibonacci and Lucas Numbers.)

Question: Given a large enough checkerboard, can any polyomino be so positioned as to result in a Fibonacci (or Lucas) number?

Answer: Unsolved.

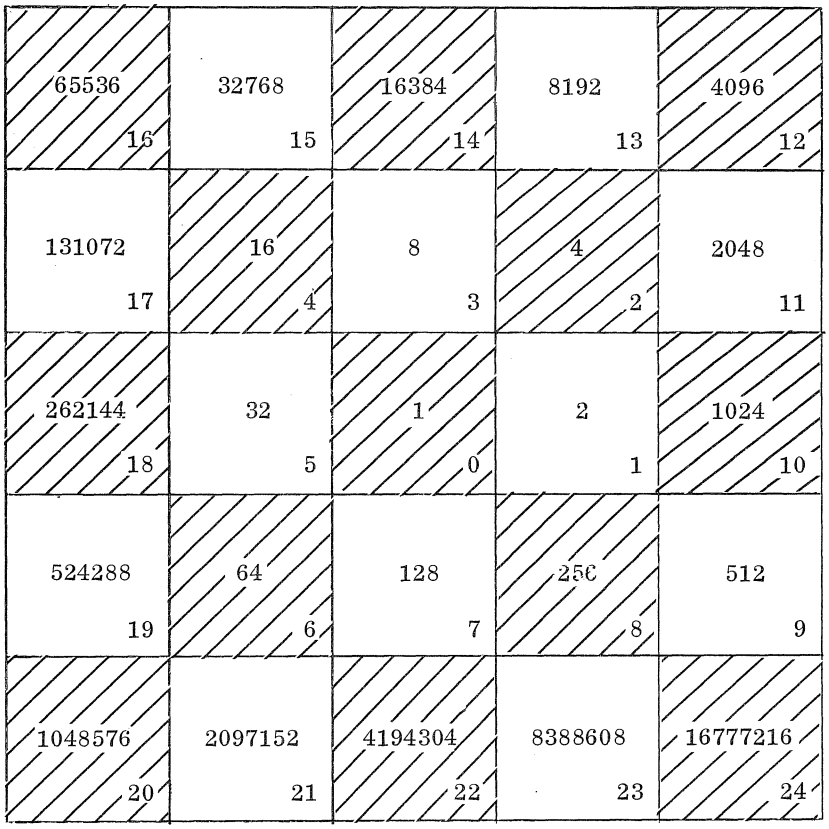


Fig. 1

(The numbers in the center of the squares represent blue. The numbers in the corners represent red. The red cells of the checkerboard are the screened ones.)

POLYOMINOES

Finally we arrive at the focal point of this paper. We have shown that any set of pawns uniquely represents a particular number N. A particular configuration of pawns may be shifted up or down or sideways, or even rotated or reflected, thus generating an entire sequence of numbers describing the relative positions of the pawns within the set and differing only in the placement of the set on the board. For example, the X-pentomino can be described by 171, 1287, 10254, 163896. We can specify that a configuration of pawns is best described by the least number N.

Our purpose is to find the number P(p) of p-ominoes.

We observe first that, since all p-ominoes can be placed on a checkerboard having no more than p x p cells, there are at the very most

$$\binom{p^2}{p} = \frac{(p^2)!}{p!\,(p^2 - p)!}$$

different p-ominoes. Thus for $p = 5$, $P(5) \leq 53{,}130$. This is the number of ways of choosing any five cells of the 25, without specifying that they be rook-wise connected.

But only the straight p-omino needs such a large board; in fact, it requires only one cell more than a $(p - 1) \times (p - 1)$ board. All other p-ominoes can be fitted onto a $(p - 1) \times (p - 1)$ board and in fact require only one cell more than a $(p - 2) \times (p - 2)$ board. For $p = 5$, $P(5)$ thus becomes no more than 1 plus

$$\binom{(p - 2)^2 + 1}{p}$$

or $P(5) \leq 1 + 252$. Actually, only t_1 pieces require such a large board; all the rest can be fitted onto a $(p - 3) \times (p - 3)$ board plus one cell. For $p = 5$, then, $P(5) \leq 1 + t_1 + 1$. The argument can be generalized for any p.

A candidate for t_1 has at least one pawn which lies in the strip $(p - 2)^2 = (p - 3)^2$; that is, the decimal representation of a t_1 polyomino lies in the range $2^{(p-2)^2+1}$ down to $2^{(p-3)^2+1}$. For pentominoes this range is 1024 to 32.

Going back to the list N(5) of numbers having five pawns in their plots, we can see that for connected cells the parity of N(5) is no more than $(p + 2)/4$, that is, either 3 or 1 for $p = 5$. This reduces the number of candidates for polyominoes; specifically, a parity of 5 means that all pawns lie on cells of the same color. A 4x4 board with one additional cell has 9 red cells and 8 black cells, producing

$$\binom{9}{5} + \binom{8}{5} = 126 + 56 = 182$$

numbers of parity 5. A 3x3 board with one extra cell has 5 red cells and 5 black sells, together yielding two numbers of parity 5.

Now at last we start counting polyominoes. We count one straight p-omino first. Then we examine each number in the range $2^{(p-2)^2+1}$ down to 2^p (1024 to 32 for the pentominoes), and finally count one for the p-omino formed by the first p cells of the spiral. Certain restrictions in the range can often be developed. Within the range, an acceptable number must have exactly p one's

in its binary representation, and must have a parity of no more than $(p + 2)/4$. Then we look at the p exponents $n_1, n_2, \cdots, n_p$ associated with 1 coefficients (in other words, the labels on the cells occupied by pawns). We calculate the rookwise adjacent cells associated with n_1 (from paragraph 7) and see if at least one of these is included in the set of p exponents, say n_3. If so, we calculate the neighbors of n_3 and see if at least one of these is included in the set of exponents. If any one of the exponents cannot be reached by a series of steps from n_1, the number being tested does not represent a polyomino.

Finally having excluded all numbers which do not correspond to polyominoes, we are of necessity left with the list of numbers which do. We do not yet, however, have $P(p)$, the total number of p-ominoes, for we have not yet excluded rotations, reflections, and translations. Methods of algebraically excluding these duplications can obviously easily be developed.

The general expression for $N(p)_{max}$, corresponding to the straight p-omino, is $2^{(p-1)(p-2)} \cdot (2^p - 1)$, and for $N(p)_{min}$ it is $2^p - 1$, corresponding to an occupation of the first p cells of the spiral.

Question: What are the "best" decimal and binary representations and parities of the twelve pentominoes?

Answer:

	Binary	Decimal	Parity
I	11 11100 00000 00000	126976	1
L	11111 00000	992	1
Y	11110 00001	963	1
N	11001 00011	803	1
X	101 01011	171	3
V	11 11100	124	1
T	11 10011	115	1
W	11 01101	109	1
F	11 01011	107	1
Z	11 00111	103	1
U	1 01111	55	1
P	11111	31	1

Bonus Question: The reader who determines the parity of 16760865 deserves an "E" for effort, with a "well done!" for replotting it into its "best" configuration and decimal representation.

Answer: Parity 1, 13 pawns forming a W, 991177.

* * * * *

LINEAR RECURSION RELATIONS — LESSON SEVEN
ANALYZING LINEAR RECURSION SEQUENCES

BROTHER ALFRED BROUSSEAU
St. Mary's College, California

Frequently one encounters problems such as the following: Find the next three terms in the following sequences:

$$1,\ 3,\ 5,\ 7,\ 9,\ 11,\ \cdots$$
$$3,\ 4,\ 7,\ 11,\ 18,\ 29,\ \cdots$$
$$3,\ 6,\ 12,\ 24,\ 48,\ 96,\ \cdots$$

As has been pointed out many times, the solution to such problems is highly indeterminate. It is "obvious" that the general term of the first sequence is

$$T_n = 2n - 1$$

But

$$T_n = 2n - 1 + (n - 1)(n - 2)(n - 3)(n - 4)(n - 5)(n - 6)V_n$$

where V_n is the n^{th} term of any sequence of finite quantities would do just as well. Similarly for the other cases.

Or looking at the matter from the standpoint of linear recursion relations, the six numbers in each case might be the first six terms of a linear recursion relation of the sixth order. Hence any infinite number of possibilities arises.

How can the problem be made more specific? Possibly, one might say: Find the expression for the n^{th} term of a linear recursion relation of minimum order. Whether this is sufficient to handle all instances of this type is an open question, but it would seem to take care of the present cases.

The solutions in the three instances listed above are:

$$T_{n+1} = 2T_n - T_{n-1}$$
$$T_{n+1} = T_n + T_{n-1}$$
$$T_{n+1} = 2T_n$$

If a sequence has terms which were derived from a polynomial expression in n, this expression can be found by the method of differences. As was pointed out in the first lesson, if the terms derive from a polynomial of degree k, the k^{th} differences are constant and the $(k+1)^{st}$ difference is zero. A simple method of reconstituting the polynomial is to use Newton's Interpolation Formula:

$$f(n) = \frac{\Delta^k f(0)}{k!} n^{(k)} + \frac{\Delta^{k-1} f(0) n^{(k-1)}}{(k-1)!} + \cdots + \frac{\Delta f(0) n^{(1)}}{1!} + f(0) \tag{1}$$

where $\Delta^k f(0)$ is the k^{th} difference taken at the zero value and $n^{(k)}$ is the factorial $n(n-1)(n-2)\cdots(n-k+1)$ of k terms.

Example. Determine the polynomial of lowest degree which fits the following set of values.

n	f(n)	$\Delta f(n)$	$\Delta^2 f(n)$	$\Delta^3 f(n)$
0	6			
		5		
1	11		32	
		37		18
2	48		50	
		87		18
3	135		68	
		155		18
4	290		86	
		241		18
5	531		104	
		345		18
6	876		122	
		467		18
7	1343		140	
		607		
8	1950			

Using Newton's Interpolation Formula,

$$f(n) = \frac{18}{3!} n(n-1)(n-2) + \frac{32}{2!} n(n-1) + 5n + 6$$

$$f(n) = 3n^3 + 7n^2 - 5n + 6.$$

Suppose that we have a sequence whose terms are the sum of the terms of two sequences: (1) A sequence whose values derive from a polynomial: (2) A sequence whose terms form a geometric progression. Is it possible to determine the components of this sequence?

Imagine that the terms of the sequence have been separated into their two component parts. Then on taking differences, the effect of the polynomial will eventually become nil. How does a geometric progression function under differencing? This can be seen from the table below.

a			
ar	$a(r-1)$	$a(r-1)^2$	
ar^2	$ar(r-1)$	$ar(r-1)^2$	$a(r-1)^3$
ar^3	$ar^2(r-1)$	$ar^2(r-1)^2$	$ar(r-1)^3$
ar^4	$ar^3(r-1)$	$ar^3(r-1)^2$	$ar^2(r-1)^3$

Clearly, differencing a geometric progression produces a geometric progression with the same ratio. By examining the form of the leading term, one can readily deduce the value of a, the initial term of the geometric progression as well.

Example.

POLYNOMIAL AND GEOMETRIC PROGRESSION COMBINED

n	T_n				
1	4				
		12			
2	16		42		
		54		58	
3	70		100		80
		154		138	
4	224		238		240
		392		378	
5	616		616		720
		1008		1098	
6	1624		1714		2160
		2722		3258	
7	4346		4972		6480
		7644		9738	
8	12040		14710		
		22404			
9	34444				

In the last column, one has a geometric progression with ratio 3, but not in the previous column. Hence the polynomial that was combined with the geometric

progression was of degree 3. For the geometric progression, $r = 3$ and

$$a \times 2^4 = 80, \text{ so that } a = 5 .$$

Eliminating the effect of the geometric progression from the leading terms gives:

$$\begin{aligned} 58 - 2^3 \times 5 &= 18 \\ 42 - 2^2 \times 5 &= 22 \\ 12 - 2 \times 5 &= 2 \\ 4 - 5 &= -1 \end{aligned}$$

To apply Newton's Formula, we have to go back to the zero elements by extrapolation.

$$\Delta^3 f(0) = 18, \quad \Delta^2 f(0) = 22 - 18 = 4, \quad \Delta f(0) = 2 - 4 = -2$$
$$f(0) = -1 - (-2) = 1 .$$

Hence

$$f(n) = \frac{18}{3!} n(n-1)(n-2) + \frac{4}{2!} n(n-1) - 2n + 1$$
$$f(n) = 3n^3 - 7n^2 + 2n + 1 .$$

Hence the term of the sequence has the form:

$$T_n = 3n^3 - 7n^2 + 2n + 1 + 5 \times 3^{n-1} .$$

The recursion relation for this term can be readily found by the methods of the previous lesson.

POLYNOMIAL AND FIBONACCI SEQUENCE

If we know that the terms of a sequence are formed by combining the elements of a polynomial sequence and a Fibonacci sequence, we have a situation similar to the previous case. For whereas the polynomial element vanishes

on taking a sufficient number of differences, the Fibonacci element persists. This can be seen from the following table.

n	T_n	ΔT_n	$\Delta^2 T_n$	$\Delta^3 T_n$
1	T_1	T_0		
2	T_2	T_1		
3	T_3	T_2	T_{-1}	T_{-2}
4	T_4	T_3	T_0	T_{-1}
5	T_5	T_4	T_2	T_0
6	T_6	T_5	T_3	T_1
7	T_7	T_6	T_4	T_2
8	T_8			

Example.

n	T_n				
1	2				
		6			
2	8		21		
		27		23	
3	35		44		-6
		71		17	
4	106		61		5
		132		22	
5	238		83		-1
		215		21	
6	453		104		4
		319		25	
7	772		129		3
		448		28	
8	1220		157		
		605			
9	1825				

The last column has a Fibonacci property, but the previous column does not. Hence the polynomial must have been of degree three. We identify the first terms of the Fibonacci sequence as being 3, the zero term as 4, the term with -1 subscript as -1, etc. The effect of these terms can be eliminated from the leading edge of the table to give: 23 - 5 = 18; 21 - (-1) = 22; 6 - 4 = 2; 2 - 3 = -1. Calculating the zero differences as before, the final form of the term to be found is:

$$T_n = 3n^3 - 7n^2 + 2n + 1 + V_n$$

where

$$V_1 = 3, \quad V_2 = 7, \quad \text{and} \quad V_{n+1} = V_n + V_{n-1} .$$

PROBLEMS

1. Determine the polynomial for which f(1) = -4; f(2) = 22; f(3) = 100; f(4) = 200; f(5) = 532; f(6) = 946; f(7) = 1532; f(8) = 2320.

2. The following sequence of values correspond to terms T_1, T_2, etc. of a sequence which is the sum of a polynomial and a Fibonacci sequence: 0, 4, 12, 29, 53, 87, 132, 192, 272, 381. Determine the polynomial and the Fibonacci sequence components.

3. The values: 13, 72, 227, 526, 1023, 1784, 2899, 4506, 6839 include a polynomial component and a geometric progression component. Determine the general form of the term of the sequence.

4. The sequence values: 4, 14, 12, 22, 20, 30, 28, 38, 36, $\cdots$ combine a polynomial and a geometric progression. Determine the general form of the term of the sequence.

5. The sequence values: 7, 19, 45, 109, 219, 395, 653, 1017, 1515 have a polynomial and a Fibonacci component. Determine the general form of the polynomial and find the Fibonacci sequence.

(Solutions to these problems can be found on page 112.)

* * * * *

CORRECTION

Please make the following changes to "Remark on a Theorem by Waksman," appearing in the Fibonacci Quarterly, October, 1969, p. 230.

On line 1, change "$Q = Q^* \cup \{1\}$" to "$Q^* = Q \cup \{1\}$"

On line 9, change "[2, p. 62]" to "[2, § 62]"

On line 18, change "$\notin V \cap Q$" to "$\in V \cap U$"

On line 20, change "a prime" to "an integer $p \in Q^*$."

AN ALGORITHM FOR FINDING THE GREATEST COMMON DIVISOR

V. C. HARRIS
San Diego State College, San Diego, California

Our problem is to find the greatest common divisor (m,n) of two positive integers m and n. If $m = 2^a M$ and $n = 2^b N$ where M and N are odd and a and b are nonnegative integers, then $(m,n) = (2^a, 2^b)(M,N)$. Since $(2^a, 2^b)$ is obtained by inspection, we are mainly concerned with finding (M,N). Alternatively, we assume m and n are odd.

Suppose m and n odd with $n < m$. Then

$$(1) \qquad m = q_1 n + R_1, \qquad 0 \leq R_1 < n \ ,$$

and

$$(2) \qquad m = (q_1 + 1)n + (R_1 - n), \quad 0 \leq R_1 < n, \quad -n \leq R_1 - n < 0 \ .$$

Select (1) or (2) according as R_1 or $R_1 - n$ is even (since n is odd, one of R_1 and $R_1 - n$ is even, the other odd) and call the remainder s_1 so that $s_1 = 2^c r_1$ where r_1 is odd and c is positive. Then $(m,n) = (n, r_1)$ and the next division is with n and r_1. At each step, the even remainder is chosen, and the even part divided out, before the next division is performed. The last nonzero remainder is (m,n).

As an example, we find $(28567, 3829)$. The divisions are

$$28567 = 7 \cdot 3829 + 4 \cdot 441$$

$$3829 = 9 \cdot 441 - 4 \cdot 35$$

$$441 = 11 \cdot 35 + 8 \cdot 7$$

$$35 = 5 \cdot 7$$

Hence $(28567, 3829) = 7$. Four divisions are required. One notes that Euclid's method requires 6 divisions and the least absolute value algorithm requires 5 divisions in finding this g. c. d.

We have the theorem:

If $\eta(a,b)$ is the number of divisions required to find (a,b) by the given algorithm, then the pair (a,b) with the smallest sum such that $\eta(a,b) = k$ is the pair $(2^{k+1} - 3,\ 2^k - 1)$ whose sum is $3 \cdot 2^k - 4$.

Working backward, we see that the divisions involving the smallest dividend and divisor at each step for various values of η are:

η	Divisions
1	$1 = 1 \cdot 1$
2	$5 = 1 \cdot 3 + 2 \cdot 1$ $\quad 3 = 3 \cdot 1$
3	$13 = 1 \cdot 7 + 2 \cdot 3$ $\quad 7 = 3 \cdot 3 - 2 \cdot 1$ $\quad 3 = 3 \cdot 1$
4	$29 = 1 \cdot 15 + 2 \cdot 7$ $\quad 15 = 3 \cdot 7 - 2 \cdot 3$ $\quad 7 = 3 \cdot 3 - 2 \cdot 1$ $\quad 3 = 3 \cdot 1$
5	$61 = 1 \cdot 31 + 2 \cdot 15$ $\quad 31 = 3 \cdot 15 - 2 \cdot 7$ $\quad \cdots$
...	...
n	$2^{n+1} - 3 = 1 \cdot (2^n - 1) + 2 \cdot (2^{n-1} - 1), \quad n \geq 1$

As a consequence, if $a < 2^k - 1$, then $\eta(a,b) < k$. The results are tabulated:

No. of digits in a	1	2	3	4	5	6	7	8	9	10
$\eta(a,b)$ <	4	7	10	14	17	20	24	27	30	34

It may be remarked that primes 3, or 5, and so on, may be removed from m and n, so that all factors of 3, 5 and so on, may be dropped from the subsequent divisors. Of course, for other than small primes, this would not reduce the work involved. Also, if base 2 is used, dropping factors of 2 from the divisors is trivial.

NOTE ON THE NUMBER OF DIVISIONS REQUIRED IN FINDING THE GREATEST COMMON DIVISOR

V. C. HARRIS
San Diego State College, San Diego, California

Lamé [1] has shown that in applying Euclid's algorithm to two positive integers a and b, the number of divisions required is not greater than five times the number of digits in the smaller of a and b. (Only base ten is considered in this note.) In the proof given by Uspensky and Heaslet [2] an upper limit for the number $n \leq 1$ of divisions required is shown to be $p/\log_{10}\xi + 1$ where p is the number of digits in the smaller of a and b and

$$\xi = (1 + \sqrt{5})/2 \ .$$

We have $\xi = 1.61803^{+}$ so that $\log_{10}\xi > 0.208978$ and $1/\log_{10}\xi < 4.7852$. Hence the number N of divisions required is

$$N = n + 1 < p(4.7852) + 1 \ .$$

Hence

$$N < 5p - 0.2148p + 1$$

and so

$$N \leq 5p + 1 + [-0.2148p] \ .$$

One could use the simpler but less accurate $N \leq 5p - [p/5]$. Using this, the improvement over Lame's statement would be 1 for $5 \leq p \leq 9$, 2 for $10 \leq p \leq 14$, etc.

REFERENCES

1. G. Lamé, "Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers," C. R. Acad. Sci., Paris, 19, 1844, pp. 867-870.
2. Uspensky and Heaslet, Elementary Number Theory, McGraw-Hill, New York, 1939, Ch. III.

ELEMENTARY PROBLEMS AND SOLUTIONS

Edited by
A. P. HILLMAN
University of New Mexico, Albuquerque, New Mexico

Send all communications regarding Elementary Problems and Solutions to Professor A. P. Hillman, Department of Mathematics and Statistics, University of New Mexico, Albuquerque, New Mexico, 87106. Each problem or solution should be submitted in legible form, preferably typed in double spacing, on a separate sheet or sheets, in the format used below. Solutions should be received within three months of the publication date.

Contributors (in the United States) who desire acknowledgement of receipt of their contributions are asked to enclose self-addressed stamped postcards.

B-178 Proposed by James E. Desmond, Florida State University, Tallahassee, Florida.

For all positive integers n show that

$$F_{2n+2} = \sum_{i=1}^{n} 2^{n-i} F_{2i-1} + 2^n$$

and

$$F_{2n+3} = \sum_{i=1}^{n} 2^{n-i} F_{2i} + 2^{n+1} \quad .$$

Generalize.

B-179 Based on Douglas Lind's Problem B-165.

Let Z^+ consist of the positive integers and let the function b from Z^+ to Z^+ be defined by $b(1) = b(2) = 1$, $b(2k) = b(k)$, and $b(2k + 1) = b(k + 1) + b(k)$ for $k = 1,2,\cdots$. Show that every positive integer m is a value of $b(n)$ and that $b(n + 1) \geq b(n)$ for all positive integers n.

B-180 Proposed by Reuben C. Drake, North Carolina A T University, Greensboro, North Carolina.

Enumerate the paths in the Cartesian plane from $(0,0)$ to $(n,0)$ that consist of directed line segments of the four following types:

Type	I	II	III	IV
Initial Point	$(k,0)$	$(k,0)$	$(k,1)$	$(k,1)$
Terminal Point	$(k,1)$	$(k+1,0)$	$(k+1,1)$	$(k+1,0)$

B-181 Proposed by J. B. Roberts, Reed College, Portland, Oregon.

Let m be a fixed integer and let $G_{-1} = 0$, $G_0 = 1$, $G_n = G_{n-1} + G_{n-2}$ for $n \geq 1$. Show that $G_0, G_m, G_{2m}, G_{3m}, \cdots$ is the sequence of upper left principal minors of the infinite matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & \cdots \\ G_{m-2} & G_{m-2} + G_m & 1 & 0 & \cdots \\ 0 & (-1)^m & G_{m-2} + G_m & 1 & \cdots \\ 0 & 0 & (-1)^m & G_{m-2} + G_m & \cdots \\ 0 & 0 & 0 & (-1)^m & \cdots \\ \vdots & & & & \end{pmatrix}$$

B-182 Proposed by James E. Desmond, Florida State University, Tallahassee, Florida.

Show that for any prime p and any integer n,

$$F_{np} \equiv F_n F_p \pmod{p} \quad \text{and} \quad L_{np} \equiv L_n L_p \equiv L_n \pmod{p}.$$

B-183 Proposed by Gustavus J. Simmons, Sandia Corporation, Albuquerque, New Mexico.

A positive integer is a palindrome if its digits read the same forward or backward. The least positive integer n such that n^2 is a palindrome but n is not is 26. Let S be the set of n such that n^2 is a palindrome but n is not. Is S empty, finite, or infinite?

SOLUTIONS

FIBONACCI PYTHAGOREAN TRIPLES

B-160 Proposed by Robert H. Anglin, Dan River Mills, Danville, Virginia.

Show that if $x = F_nF_{n+3}$, $y = 2F_{n+1}F_{n+2}$, and $z = F_{2n+3}$, then

$$x^2 + y^2 = z^2 .$$

Solution by Michael Yoder, Student, Albuquerque Academy, Albuquerque, New Mexico.

Let $u = F_{n+2}$ and $v = F_{n+1}$. Then

$$u^2 - v^2 = (u + v)(u - v) = F_{n+3}F_n = x, \quad 2uv = y, \quad u^2 + v^2 = z,$$

and hence $x^2 + y^2 = z^2$.

Also solved by Herta T. Freitag, Bruce W. King, Douglas Lind, John W. Milsom, A. G. Shannon (Boroko, T. P. N. G.), Gregory Wulcyzn, and the Proposer.

PELL NUMBER IDENTITIES

B-161 Proposed by John Ivie, Student, University of California, Berkeley, California.

Given the Pell numbers defined by $P_{n+2} = 2P_{n+1} + P_n$, $P_0 = 0$, $P_1 = 1$, show that for $k > 0$:

(i) $$P_k = \sum_{r=0}^{\lceil (k-1)/2 \rceil} \binom{k}{2r+1} 2^r .$$

(ii) $$P_{2k} = \sum_{r=1}^{k} \binom{k}{r} 2^r P_r .$$

Solution by Douglas Lind, Cambridge University, Cambridge, England.

Let

$$a = 1 + \sqrt{2}, \quad b = 1 - \sqrt{2}$$

be the roots of the characteristic polynomial $x^2 - 2x - 1$. It follows from the theory of difference equations that there are constants A and B such that

$$P_n = Aa^n + Bb^n .$$

Solving the system of simultaneous equations resulting by setting $n = 0, 1$, we find

$$A = 1/2\sqrt{2}, \qquad B = -1/2\sqrt{2} .$$

Hence

$$P_k = \frac{1}{2\sqrt{2}}(a^k - b^k) = \frac{1}{2\sqrt{2}} \sum_{j=0}^{k} \binom{k}{j} \left[2^{j/2} - (-1)^j 2^{j/2}\right]$$

$$= \frac{1}{2\sqrt{2}} \sum_{r=0}^{[\frac{1}{2}(k-1)]} \binom{k}{2r+1} \left[2 \cdot 2^{\frac{1}{2}(2r+1)}\right] = \sum_{r=0}^{[\frac{1}{2}(k-1)]} \binom{k}{2r+1} 2^r .$$

Also, since a and b satisfy $x^2 = 2x + 1$, we have

$$P_{2k} = \frac{1}{2\sqrt{2}}(a^{2k} - b^{2k}) = \frac{1}{2\sqrt{2}}\left((2a+1)^k - (2b+1)^k\right)$$

$$= \sum_{r=0}^{k} \binom{k}{r} 2^r \left(\frac{a^r - b^r}{2\sqrt{2}}\right) = \sum_{r=0}^{k} \binom{k}{r} 2^r P_r .$$

Also solved by Herta T. Freitag, Bruce W. King, Gregory Wulcyzn, Michael Yoder, and the Proposer.

A REPRESENTATION THEOREM

B-162 Proposed by V. E. Hoggatt, Jr., San Jose State College, San Jose, California.

Let r be a fixed positive integer and let the sequence $u_1, u_2, \cdots$ satisfy $u_n = u_{n-1} + u_{n-2} + \cdots + u_{n-r}$ for $n > r$ and have initial conditions $u_j = 2^{j-1}$ for $j = 1, 2, \cdots, r$. Show that every representation of U_n as a sum of distinct u_j must be of the form u_n itself or contain explicitly the terms u_{n-1}, u_{n-2}, u_{n-r+1} and some representation of u_{n-r}.

Solution by Michael Yoder, Student, Albuquerque Academy, Albuquerque, New Mexico.

For $r = 1$, the theorem is trivial; we therefore assume $r \geq 2$. First we show by induction that

$$\sum_{i=1}^{n} u_i < u_{n+2} .$$

For $n = 1,2,\cdots,r$ this is obvious; and if

$$\sum_{i=1}^{n} u_i < u_{n+2}, \quad \text{where} \quad n < r ,$$

$$\sum_{i=1}^{n+1} u_i < u_{n+2} + u_{n+1} \leq u_{n+3} .$$

Now let

$$u_n = \sum_{k<n} c(k)u_k ,$$

$c(k) = 0$ or 1 for all k, be a representation of u_n and assume $c(j) = 0$ for some j with $n - r + 1 \leq j \leq n - 1$. Then

$$\sum_{k<n} c(k)u_k < \sum_{k=1}^{n-1} u_k - u_j$$

$$\leq \left(\sum_{k=1}^{n-r-1} u_k + \sum_{k=n-r}^{n-1} u_k \right) - u_{n-r+1}$$

$$= \left(\sum_{k=1}^{n-r-1} u_k - u_{n-r+1} \right) + u_n < u_n ,$$

which is a contradiction. Thus we must have

$$u_n = u_{n-1} + \cdots + u_{n-r+1} + S ,$$

where S is some representation of u_{n-r}.

See "Generalized Fibonacci Numbers and the Polygonal Numbers," Journal of Recreational Mathematics, July, 1968, pp. 144-150.

Also solved by the Proposer.

A VARIANT OF THE EULER-BINET FORMULA

B-163 Proposed by Phil Mana, University of New Mexico, Albuquerque, New Mexico.

Let n be a positive integer. Clearly

$$(1 + \sqrt{5})^n = a_n + b_n\sqrt{5}$$

with a_n and b_n integers. Show that 2^{n-1} is a divisor of a_n and of b_n.

Solution by David Zeitlin, Minneapolis, Minnesota.

Let

$$\alpha = (1 + \sqrt{5})/2 \quad \text{and} \quad \beta = (1 - \sqrt{5})/2 .$$

Elimination of β^n from $L_n = \alpha^n + \beta^n$ and $\sqrt{5}F_n = \alpha^n - \beta^n$ gives

$$2\alpha^n = L_n + \sqrt{5}F_n .$$

Thus,

$$(1 + \sqrt{5})^n = 2^{n-1}L_n + \sqrt{5}(2^{n-1}F_n),$$

where $\alpha_n = 2^{n-1}L_n$ and $b_n = 2^{n-1}F_n$.

Also solved by Juliette Davenport, Herta T. Freitag, John E. Homer, Jr., John Ivie, Bruce W. King, Douglas Lind, Peter A. Lindstrom, A. G. Shannon (Boroko, T. P. N. G.), Michael Yoder, and the proposer.

A GENERALIZED SEQUENCE WITH CHARACTERISTIC 11,111

B-164 Proposed by J. A. H. Hunter, Toronto, Canada.

A Fibonacci-type sequence is defined by:

$$G_{n+2} = G_{n+1} + G_n,$$

with $G_1 = a$ and $G_2 = b$. Find the minimum positive values of integers a and b, subject to a being odd, to satisfy:

$$G_{n-1}G_{n+1} - G_n^2 = -11111(-1)^n \quad \text{for} \quad n > 1.$$

Solution by Michael Yoder, Student, Albuquerque Academy, Albuquerque, New Mexico.

If the given equation is true for any one value of n, it is true for all values of n; hence taking $n = 2$, we get

$$\begin{aligned} a(a + b) - b^2 &= -11111 , \\ 4a^2 + 4ab - 4b^2 &= -44444, \\ (2a + b)^2 &= 5b^2 - 44444 . \end{aligned}$$

Now $5b^2 - 44444 > b^2$ leads to $b > 105$; trying $b = 106, 107, \cdots$ in succession, one finds the smallest value of b to make $5b^2 - 44444$ a square $b = 111$. However, this gives $2a + b = 131$, $a = 10$, and a is supposed to be odd. Continuing with $b = 112, 113, \cdots$, we find

$$166^2 = 5(120)^2 - 44444 ,$$

which gives $a = 23$, $b = 120$ as the smallest solution.

Also solved by Christine Anderson, Herta T. Freitag, John E. Homer, Jr., Gregory Wulczyn, and the Proposer.

A MONOTONIC SURJECTION FROM Z^+ TO Z^+

B-165 Proposed by Douglas Lind, University of Virginia, Charlottesville, Virginia.

Define the sequence $\{b(n)\}$ by $b(1) = b(2) = 1$, $b(2k) = b(k)$, and

$$b(2k + 1) = b(k + 1) + b(k) \quad \text{for} \quad k \geq 1 .$$

For $n \geq 1$, show the following:

(a) $$b([2^{n+1} + (-1)^n]/3) = F_{n+1} .$$

(b) $$b([7 \cdot 2^{n-1} + (-1)^n]/3) = L_n .$$

Solution by Michael Yoder, Student, Albuquerque Academy, Albuquerque, New Mexico.

(a) For $n = 0,1$ the formula is easily verified. Assume it is true for $n - 2$ and $n - 1$ with $n \geq 2$; then if n is even,

$$\begin{aligned} b[(2^{n+1} + 1)/3] &= b[(2^n - 1)/3 + b(2^n + 2)/3] \\ &= F_n + b[(2^{n-1} + 1)/3] \\ &= F_n + F_{n-1} = F_{n+1} . \end{aligned}$$

Similarly, if n is odd,

$$b[(2^{n+1} - 1/3] = F_{n+1} .$$

(b) For $n = 1,2$ the theorem is true; and by exactly the same argument as in (a), it follows by induction for all positive integers n.

Also solved by Herta T. Freitag and the Proposer.

* * * * *

(Continued from page 101.)

SOLUTIONS TO PROBLEMS

1. $5n^3 - 4n^2 + 3n - 8$.
2. $3n^2 - 8n + 4$ and the Fibonacci sequence: $1,4,5,9,14,\cdots$.
3. $7n^3 + 3n^2 - 5n + 2 + 3x2^n$.
4. $4n + 3 + 3(-1)^n$.
5. $2n^3 - 3n^2 - n + 5$ and the Fibonacci sequence $4L_n$.

* * * * *

SUSTAINING MEMBERS

*H. L. Alder
V. V. Alderman
G. L. Alexanderson
R. H. Anglin
*Joseph Arkin
Larry Badii
Col. R. S. Beard
Leon Bernstein
*Marjorie Bicknell
John W. Biggs
Frank Boehm
J. L. Bohnert
M. B. Boisen, Jr.
L. H. Brackenberry
*Terry Brennan
C. A. Bridger
Leonard Bristow
Maxey Brooke
*Bro. A. Brousseau
*J. L. Brown, Jr.
C. R. Burton
*Paul F. Byrd
N. S. Cameron
L. Carlitz
L. C. Carpenter
P. V. Charland
P. J. Cocussa
D. B. Cooper
J. R. Crenshaw
D. E. Daykin
J. W. DeCelis
F. DeKoven
J. E. Desmond
A. W. Dickinson
N. A. Draim
D. C. Duncan
M. H. Eastman
C. F. Ellis
H. S. Ellsworth
Merritt Elmore
*Charter Members

R. S. Erlein
H. W. Eves
R. A. Fairbairn
A. J. Faulconbridge
*H. H. Ferns
D. C. Fielder
E. T. Frankel
H. M. Gehman
G. R. Glabe
E. L. Godfrey
Ruth Goodman
*H. W. Gould
Nicholas Grant
G. B. Greene
B. H. Gundlach
*J. H. Halton
W. R. Harris, Jr.
V. C. Harris
L. B. Hedge
Cletus Hemsteger
*A. P. Hillman
Bruce H. Hoelter
*V. E. Hoggatt, Jr.
*A. F. Horadam
D. F. Howells
J. A. H. Hunter
*Dov Jarden
*S. K. Jerbic
J. H. Jordan
D. A. Klarner
Kenneth Kloss
D. E. Knuth
Eugene Kohlbecker
Sidney Kravitz
George Ledin, Jr.
Hal Leonard
Eugene Levine
J. B. Lewis
*D. A. Lind
*C. T. Long
A. F. Lopez

F. W. Ludecke
J. S. Madachy
*J. A. Maxwell
*Sister M. DeSales McNabb
John Mellish, Jr.
C. T. Merriman
Mrs. Lucile Morton
Mel Most
Stephen Nytch
Roger O'Connell
P. B. Onderdonk
F. J. Ossiander
L. A. Pape
R. J. Pegis
M. M. Risueno
*D. W. Robinson
*Azriel Rosenfeld
T. J. Ross
F. G. Rothwell
I. D. Ruggles
H. J. Schafer
J. A. Schumaker
H. D. Seielstad
B. B. Sharpe
L. R. Shenton
G. Singh
David Singmaster
A. N. Spitz
M. N. S. Swamy
A. Sylvester
*D. E. Thoro
H. L. Umansky
M. E. Waddill
*C. R. Wall
*L. A. Walker
R. J. Weinshenk
R. A. White
V. White
H. E. Whitney
P. A. Willis
Charles Ziegenfus

ACADEMIC OR INSTITUTIONAL MEMBERS

SAN JOSE STATE COLLEGE
San Jose, California

ST. MARY'S COLLEGE
St. Mary's College, California

DUKE UNIVERSITY
Durham, No. Carolina

VALLEJO UNIFIED SCHOOL DISTRICT
Vallejo, California

NORWICH UNIVERSITY
NORTHFIELD, VT.

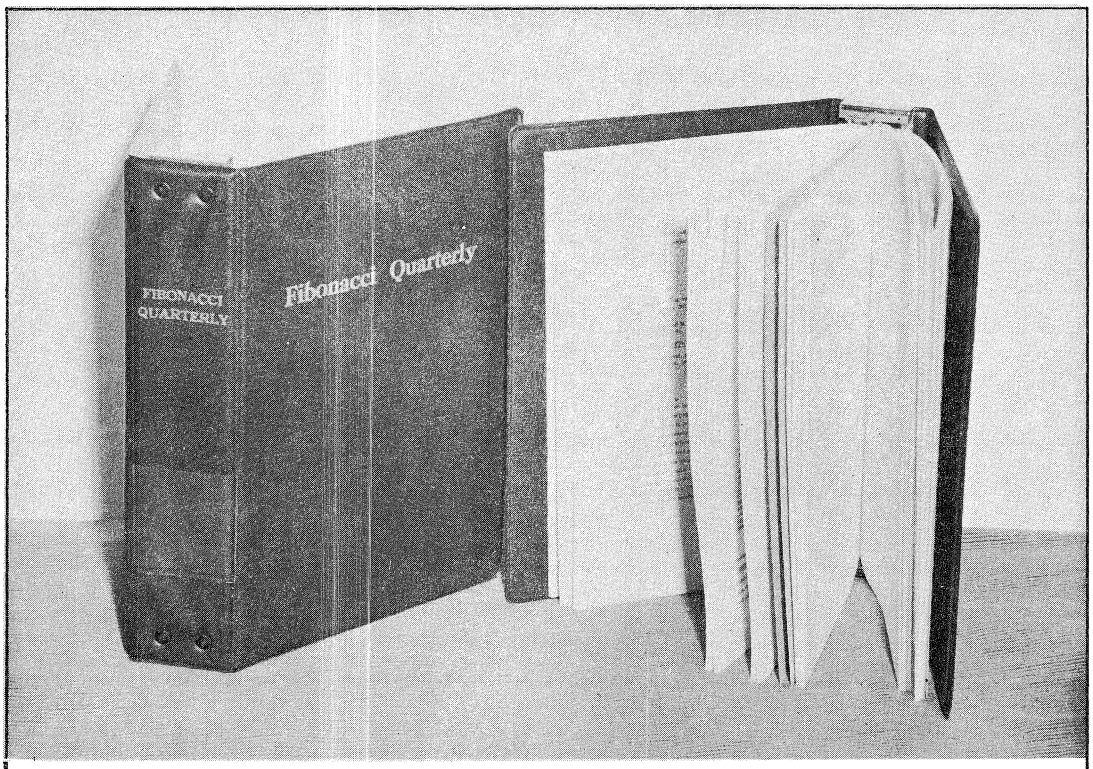
WASHINGTON STATE UNIVERSITY
Pullman, Washington

SACRAMENTO STATE COLLEGE
Sacramento, California

UNIVERSITY OF SANTA CLARA
Santa Clara, California

THE CALIFORNIA
MATHEMATICS COUNCIL

WAKE FOREST UNIVERSITY
WINSTON-SALEM, N. C.



BINDERS NOW AVAILABLE

The Fibonacci Association is making available a binder which can be used to take care of one volume of the publication at a time. This binder is described as follows by the company producing it:

> "....The binder is made of heavy weight virgin vinyl, electronically sealed over rigid board equipped with a clear label holder extending 2 -3/4" high from the bottom of the backbone, round cornered, fitted with a 1 1/2 " multiple mechanism and 4 heavy wires."

The name, FIBONACCI QUARTERLY, is printed in gold on the front of the binder and the spine. The color of the binder is dark green. There is a small pocket on the spine for holding a tab giving year and volume. These latter will be supplied with each order if the volume or volumes to be bound are indicated.

The price per binder is $3.50 which includes postage (ranging from 50¢ to 80¢ for one binder). The tabs will be sent with the receipt or invoice.

All orders should be sent to: Brother Alfred Brousseau, Managing Editor, St. Mary's College, Calif. 94575