

VOLUME 12

THE FIBONACCI QUARTERLY

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

SERIALS DE



NUMBER 1

CONTENTS

| Fibonacci Notes — 1. Zero-One Sequences | |
|--|-----|
| and Fibonacci Numbers of Higher Order | 1 |
| Linearly Recursive Sequences of Integers Brother L. Raphael | 11 |
| The Golden Ellipse | 38 |
| On a Problem of M. Ward | 41 |
| Generalized Hidden Hexagon Squares | 45 |
| Letter to the Editor | 46 |
| Diagonal Sums of the Trinomial Triangle V. E. Hoggatt, Jr., and Marjorie Bicknell | 47 |
| Fibonacci Sequences Modulo m | 51 |
| Phi: Another Hiding Place | 65 |
| Some Geometrical Properties of the Generalized Fibonacci Sequence | 67 |
| Sets of Binomial Coefficients with Equal Products Calvin T. Long and V. E. Hoggatt, Jr. | 71 |
| On Daykin's Algorithm for Finding the G.C.D. | 80 |
| Stufe of a Finite Field | 81 |
| Iteration Algorithms for Certain Sums of Squares | 83 |
| Certain Congruence Properties (Modulo 100) of Fibonacci Numbers | 87 |
| Fibonaccian Pathological Curves | 92 |
| Irreducibility of Lucas and Generalized Lucas Polynomials G. E. BERCUM and V. E. Hoggatt, Jr. | 95 |
| Elementary Problems and Solutions | 101 |
| Advanced Problems and Solutions | 107 |

THE FIBONACCI QUARTERLY

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

DEVOTED TO THE STUDY OF INTEGERS WITH SPECIAL PROPERTIES

CO-EDITORS

V. E. Hoggatt, Jr.

Marjorie Bicknell

EDITORIAL BOARD

H. L. Alder
John L. Brown, Jr.
Brother A. Brousseau
Paul F. Byrd
L. Carlitz
H. W. Eves
H. W. Gould

A. P. Hillman
David A. Klarner
C. T. Long
M. N S. Swamy
D. E. Thoro

WITH THE COOPERATION OF

Terry Brennan Maxey Brooke Calvin D. Crabill T. A. Davis John H. Halton A. F. Horadam Dov Jarden Stephen Jerbic L. H. Lange

D. A. Lind James Maxwell Sister M. DeSales McNabb Gerald Preston D. W. Robinson Azriel Rosenfeld Lloyd Walker Charles H. Wall

The California Mathematics Council

All subscription correspondence should be addressed to Brother Alfred Brousseau, St. Mary's College, California 94575. All checks (\$8.00 per year) should be made out to the Fibonacci Association or the Fibonacci Quarterly. Two copies of manuscripts intended for publication in the Quarterly should be sent to Verner E. Hoggatt, Jr., Mathematics Department, San Jose State University, San Jose, California 95192. 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, Calif., as an official publication of the Fibonacci Association.

The Quarterly is published in February, April, October, and December, each year.

FIBONACCI NOTES 1. ZERO - ONE SEQUENCES AND FIBONACCI NUMBERS OF HIGHER ORDER

L. CARLITZ Duke University, Durham, North Carolina 27706

1. INTRODUCTION

It is well known (see, for example [1, p. 14]) that the number of sequences of zeros and ones of length n with two consecutive ones forbidden is equal to F_{n+2} . For example for n = 3, the allowable sequences are

(000), (100), (010), (001), (101).

As a first extension of this result, let f(n,k) denote the number of sequences of length

n.

(1.1) (a_1, a_2, \dots, a_n) $(a_i = 0 \text{ or } 1)$ such that (1.2) $a_i a_{i+1} \cdots a_{i+k} = 0$ $(i = 1, 2, \dots, n-k);$

that is, a string of k + 1 consecutive ones is forbidden. Also, let f(n,k,r) denote the number of such sequences with exactly r ones and let $f_j(n,k,r)$ denote the number of such sequences with r ones and beginning with j ones, $0 \le j \le r$.

It suffices to evaluate $f_0(n,k,r)$. We shall show that

(1.3)
$$f_0(n,k,r) = c_k(n-r,r)$$
,

where $c_k(n,r)$ is defined by

(1.4)
$$(1 + x + \cdots + x^k)^n = \sum_{r=0}^{kn} c_k(n, r) x^r.$$

Also if

$$f_0(n,k) = \sum_{r} f_0(n,k,r)$$

is the number of allowable sequences beginning with at least one zero, we have

^{*}Supported in part by NSF Grant GP-17031.

(1.5)

 $\mathbf{2}$

$$\sum_{n=0}^{\infty} f_0(n,k) x^n = \frac{1}{1 - x - x^2 - \dots - x^{k+1}}$$

In the next place let r, s be fixed positive integers and let f(m,n; r,s) denote the number of sequences of length m + n

$$(a_1, a_2, \dots, a_{m+n})$$
 $(a_i = 0 \text{ or } 1)$

with exactly m zeros and n ones, at most r consecutive zeros and at most s consecutive ones. Also, let $f_j(m,n; r,s)$ denote the number of such sequences beginning with exactly j zeros, $0 \le j \le r$; let $\overline{f}_k(m,n; r,s)$ denote the number of such sequences beginning with exactly k ones, $0 \le k \le s$.

As in the previous problem, it suffices to evaluate $f_0(m,n; j,k)$ and $\overline{f}_0(m,n; j,k)$. We shall show that

(1.6)
$$f_{0}(m,n; r,s) = \sum_{k} c_{r-1}(k, m-k)c_{s-1}(k, n-k) + \sum_{k} c_{r-1}(k+1, m-k-1)c_{s-1}(k, n-k) ,$$

(1.7)
$$\overline{f}_{0}(m,n; r,s) = \sum_{k} c_{r-1}(k, m-1)c_{s-1}(k, n-k) + \sum_{k} c_{r-1}(k, m-k)c_{s-1}(k+1, n-k-1),$$

(1.8)
$$f(m,n; r,s) = \sum_{k} \{c_{r-1}(k, m-k)c_{s-1}(k, n-k) + c_{r-1}(k+1, m-k-1)c_{s-1}(k, n-k) + c_{r-1}(k, m-k)c_{s-1}(k+1, n-k-1)\}$$

As a further extension one can consider sequences of 0's, 1's, and 2's, say with restrictions on the number of allowable consecutive elements of each kind. However, we leave this for another occasion.

2. FIRST PROBLEM

We now consider the first problem as defined above. It is clear from the definition that

(2.1)
$$f(n,k,r) = \sum_{j=0}^{k} f_{j}(n,k,r)$$

Also

1974]

(2.2)
$$f_0(n,k,r) = \sum_{j=0}^{k} f_j(n-1,k,r) = f(n-1,k,r)$$

.

and

(2.3)
$$f_j(n,k,r) = f_0(n-j,k,r-j)$$
 $(0 \le j \le k)$.

Hence $\,f_0\left(n,k,r\right)\,$ satisfies the mixed recurrence

(2.4)
$$f_0(n,k,r) = \sum_{j=0}^{k} f_0(n-j-1,k,r-j)$$
 $(n > k+1)$.

Now, for $r \leq k$,

$$f_{0}(1, k, r) = \delta_{0, r},$$

$$f_{0}(2, k, r) = \begin{cases} 1 & (r = 0, 1) \\ 0 & (r > 1) \end{cases},$$

$$f_{0}(3, k, r) = \begin{cases} 1 & (r = 0) \\ 2 & (r = 1) \\ 1 & (r = 2) \\ 0 & (r > 2) \end{cases}.$$

Generally, for $1 \le m \le k+1$, we have

(2.5)
$$f_0(m,k,r) = \begin{cases} \binom{m-1}{r} & (0 \le r \le m) \\ 0 & (r \ge m) \end{cases}$$

If we take n = k + 1, $r \leq k$ in (2.4) we get

$$f_0(k + 1, k, r) = \sum_{j=0}^k f_0(k - j, k, r - j)$$
.

.

By (2.5) this reduces to

$$\begin{pmatrix} k \\ r \end{pmatrix} = \sum_{j=0}^{k-1} \begin{pmatrix} k & -j & -1 \\ r & -j \end{pmatrix} + f_0 (0, k, r - k) .$$

Sinc e

4

$$\sum_{j=0}^{k-1} \binom{k-j-1}{r-j} = \sum_{j=0}^{k-1} \binom{k-j-1}{k-r-1} = \sum_{j=0}^{k-1} \binom{j}{k-r-1} = \binom{k}{k-r} \binom{k}{k-r}$$

it follows that (2.4) holds for $n \ge k + 1 \ge r$ provided we define

$$f_0(0,k,t) = 0$$
 $(t \le 0)$.

Moreover (2.4) holds for r > k, n = k + 1, since both sides vanish. Now put

(2.6)

$$F(x, y) = \sum_{n, r=0}^{\infty} f_0(n, k, r) x^n y^r$$

Then, by (2.4) and (2.5),

$$\begin{split} F(x,y) &= \sum_{n=0}^{k} \sum_{r=0}^{\infty} f_{0}(n,k,r) x^{n} y^{r} + \sum_{n=k+1}^{\infty} \sum_{r=0}^{\infty} f_{0}(n,k,r) x^{n} y^{r} \\ &= 1 + \sum_{n=1}^{\infty} \sum_{r=0}^{\infty} {n - 1 \choose r} x^{n} y^{r} \\ &+ \sum_{n=k+1}^{\infty} \sum_{r=0}^{\infty} \sum_{j=0}^{k} f_{0}(n - j - 1, k, r - j) x^{n} y^{r} \\ &= 1 + \sum_{n=1}^{k} \sum_{r=0}^{\infty} {n - 1 \choose r} x^{n} y^{r} \\ &+ \sum_{j=0}^{k} x^{j+1} y^{j} \sum_{n=k+1}^{\infty} \sum_{r=0}^{\infty} f_{0}(n - j - 1, k, r - j) x^{n-j-1} y^{r-j} \\ &= 1 + \sum_{n=1}^{k} \sum_{r=0}^{\infty} {n - 1 \choose r} x^{n} y^{r} \\ &+ \sum_{j=0}^{k} x^{j+1} y^{j} \left\{ F(x, y) = \sum_{n=0}^{k-j-1} \sum_{r=0}^{\infty} f(n, k, r) x^{n} y^{r} \right\} \end{split}$$

[Feb.

Since

$$\begin{split} \sum_{j=0}^{k} x^{j+1} y^{j} \sum_{n=0}^{k-j-1} \sum_{r=0}^{\infty} f(n,k,r) x^{n} y^{r} &= \sum_{j=0}^{k} x^{j+1} y^{j} \sum_{n=0}^{k-j-1} \sum_{r=0}^{\infty} {\binom{n-1}{r}} x^{n} y^{r} y^{r} \\ &= \sum_{n=1}^{k} \sum_{r} x^{n} y^{r} \sum_{j} {\binom{n-j-2}{r-j}} \\ &= \sum_{n=1}^{k} \sum_{r} {\binom{n-1}{r}} x^{n} y^{r} , \end{split}$$

it follows that

$$F(x,y) = 1 + \sum_{j=0}^{k} x^{j+1} y^{j} \cdot F(x,y)$$
.

Therefore

(2.7) $F(x, y) = \frac{1}{1 - x \sum_{j=0}^{k} x^{j} y^{j}} .$

If we define the coefficient $c_k(n,r)$ by means of

(2.8)
$$(1 + x + \cdots + x^k)^n = \sum_{r=0}^{kn} c_k(n,k) x^r$$
,

it is clear that

$$\frac{1}{1 - x \sum_{j=0}^{k} x^{y} y^{j}} = \sum_{s=0}^{\infty} x^{s} \left(\sum_{j=0}^{k} x^{j} y^{j} \right)^{s} .$$
$$= \sum_{s=0}^{\infty} x^{s} \sum_{r=0}^{ks} c_{k}(s, r) x^{r} y^{r}$$
$$= \sum_{n=0}^{\infty} \sum_{r=0}^{n} c_{k}(n - r, r) x^{n} y^{r} .$$

Therefore by (2.6) and (2.7) we have

1974]

(2.9)

6

$$f_0(n,k,r) = c_k(n - r, r)$$

and, in view of (2.2), (2.10)

$$f(n,k,r) = c_k(n - r + 1, r)$$
.

Moreover if we put

$$f_0(n,k) = \sum_r f_0(n,k,r)$$
,

it follows that

(2.11)
$$\sum_{n=0}^{\infty} f_0(n,k) x^n = \frac{1}{1 - \sum_{j=1}^{k+1} x^j}$$

In particular, for k = 1, it is clear from (2.11) that

(2.12)
$$f_0(n,1) = F_{n+1}$$
.

3. SECOND PROBLEM

We turn now to the second problem defined in the Introduction. It is convenient to define

(3.1)
$$\begin{cases} f_0(0,0; r,s) = \overline{f}(0,0; r,s) = 1 \\ f_j(0,0; r,s) = \overline{f}_k(0,0; r,s) = 0 \quad (j > 0, k > 0) . \end{cases}$$

The following relations follow from the definition.

(3.2)
$$\begin{cases} f_0(m,n; r,s) = \sum_{k=1}^{s} \overline{f}_k(m,n; r,s) \\ \overline{f}_0(m,n; r,s) = \sum_{j=1}^{r} f_j(m,n; r,s) \end{cases}$$

$$\begin{cases} f_j(m,n; r,s) = \sum_{k=1}^{s} \overline{f}_k(m - j, n; r,s) & (j \ge 0) \\ \\ \overline{f}_k(m,n; r,s) = \sum_{k=1}^{r} f_j(m, n - k; r,s) & (k \ge 0) \end{cases}$$

j=1

,

(3.3)

where it is understood that

$$f_0(m,n; r, s) = \overline{f}_0(m,n; r, s) = 0$$

if either $m \ or \ n$ is negative.

We have also

(3.4)
$$\begin{cases} f_{j}(m,n; r,s) = f_{0}(m - j, n; r,s) & (j > 0) \\ \overline{f}_{k}(m,n; r,s) = \overline{f}_{0}(m,n - k; r,s) & (k > 0) \end{cases}$$

In particular

(3.5)
$$\begin{cases} f_{j}(j, n; r, s) = f_{0}(0, n; r, s) = 1 & (0 \le n \le s) \\ \overline{f}_{k}(m, k; r, s) = \overline{f}_{0}(m, 0; r, s) = 1 & (0 \le m \le r) \end{cases}$$

It follows from (3.2) and (3.4) that

(3.6)
$$\begin{cases} f_0(m,n; r,s) = \sum_{k=1}^{s} \overline{f}_0(m, n - k; r, s) \\ \\ \overline{f}_0(m,n; r,s) = \sum_{j=1}^{r} f_0(m - j, n; r, s) \end{cases}$$

and therefore

(3.7)
$$\begin{cases} f_0(m,n; r,s) = \sum_{j=1}^r \sum_{k=1}^s f_0(m - j, n - k; r, s) \\ \\ \overline{f}_0(m,n; r,s) = \sum_{j=1}^r \sum_{k=1}^s \overline{f}_0(m - j, n - k; r, s) \end{cases}$$

Now put

$$F_0 = F_0(x, y) = \sum_{m, n=0}^{\infty} f_0(m, n; r, s) x^m y^n$$

•

•

$$\overline{F}_0 = \overline{F}_0(x, y) = \sum_{m, n=0}^{\infty} \overline{f}_0(m, n; r, s) x^m y^n$$

Then by (3.5) and (3.7),

$$\begin{split} F_{0} &= \sum_{k=0}^{s} y^{k} + \sum_{m,n=1}^{\infty} f_{0}(m,n; r,s) x^{m} y^{n} \\ &= \sum_{k=0}^{s} y^{k} + \sum_{m,n=1}^{\infty} \sum_{j=1}^{r} \sum_{k=1}^{s} f_{0}(m - j, n - k; r, s) x^{m} y^{n} \\ &= \sum_{k=0}^{s} y^{k} + \sum_{j=1}^{r} \sum_{k=1}^{s} x^{j} y^{k} \sum_{m,n=0}^{\infty} f_{0}(m,n; r,s) x^{m} y^{n} \\ &= \sum_{k=0}^{s} y^{k} + \sum_{j=1}^{r} \sum_{k=1}^{s} x^{j} y^{k} \cdot F_{0} , \end{split}$$

so that

(3.8)

8

$$F_0 = \frac{\sum_{k=0}^{s} y^k}{1 - \sum_{j=1}^{r} \sum_{k=1}^{s} x^j y^k} .$$

Similarly

(3.9)

$$\overline{F}_0 = \frac{\sum_{j=0}^r y^j}{1 - \sum_{j=1}^r \sum_{k=1}^s x^j y^k}$$

•

.

,

Clearly

$$f(m,n; r,s) = f_0(m,n; r,s) + \overline{f_0}(m,n; r,s)$$
 (m + n > 0)

so that

$$F(x,y) = \sum_{m,n=0}^{\infty} f(m,n; r,s) x^{m} y^{n} = -1 + F_{0}(x,y) + \overline{F}_{0}(x,y) .$$

Hence

(3.10)

$$F(x, y) = \frac{\sum_{j=0}^{r} x^{j} + \sum_{k=0}^{s} y^{k}}{1 - \sum_{j=1}^{r} \sum_{k=1}^{s} x^{j} y^{k}}$$

To get explicit formulas we take

$$\begin{pmatrix} 1 - \sum_{j=1}^{r} \sum_{k=1}^{s} x^{j} y^{k} \end{pmatrix}^{-1} = \sum_{k=0}^{\infty} x^{k} y^{k} (1 + \dots + x^{r-1})^{k} (1 + \dots + y^{s-1})^{k}$$
$$= \sum_{k=0}^{\infty} x^{k} y^{k} \sum_{i=0}^{\infty} c_{r-1}(k, i) x^{i} \sum_{j=0}^{\infty} c_{s-1}(k, j) x^{j}$$
$$= \sum_{m,n=0}^{\infty} x^{m} y^{n} \sum_{k} c_{r-1}(k, m-k) c_{s-1}(k, n-k) .$$

Then

$$\frac{\sum_{j=1}^{r} x^{j}}{1 - \sum_{j=1}^{r} \sum_{k=1}^{s} x^{j} y^{k}} = \sum_{k=0}^{\infty} x^{k+1} y^{k} (1 + \dots + x^{r-1})^{k+1} (1 + \dots + y^{s-1})^{k}$$
$$= \sum_{k=0}^{\infty} x^{k+1} y^{k} \sum_{i,j} c_{r-1} (k + 1, i) c_{s-1} (k, j) x^{i} y^{j}$$
$$= \sum_{m,n=0}^{\infty} x^{m} y^{n} \sum_{k} c_{r-1} (k + 1, m - k - 1) c_{s-1} (k, n - k) ,$$
$$\frac{\sum_{j=1}^{s} y^{k}}{1 - \sum_{j=1}^{r} \sum_{k=1}^{s} x^{j} y^{k}} = \sum_{m,n=0}^{\infty} x^{m} y^{n} \sum_{k} c_{r-1} (k, m - k) c_{s-1} (k + 1, n - k - 1) .$$

It follows that

(3.11)
$$\begin{cases} f_0(m,n; r,s) = \sum_{k} \{c_{r-1}(k, m-k)c_{s-1}(k, n-k) + c_{r-1}(k+1, m-k-1)c_{s-1}(k, n-k)\} \}, \end{cases}$$

(3.12)
$$\begin{cases} \overline{f}_{0}(m,n; r,s) = \sum_{k} \{c_{r-1}(k, m-k)c_{s-1}(k, n-k) + c_{r-1}(k, m-k)c_{s-1}(k+1, n-k+1)\} \} \end{cases}$$

1974]

and the second second

$$f(\mathbf{m}, \mathbf{n}; \mathbf{r}, \mathbf{s}) = \sum_{k} \left\{ c_{r-1}(k, m - k) c_{s-1}(k, n - k) + c_{r-1}(k + 1, m - k - 1) c_{s-1}(k, n - k) + c_{r-1}(k, m - k) c_{s-1}(k + 1, n - k - 1) \right\}.$$

When $r \rightarrow \infty$ the restrictions in the definition of f, f_j reduce to the single restriction that the number of consecutive ones is at most s. The generating functions (3.8), (3.9), (3.10) reduce to

,

,

(3.8')
$$F_0 = \frac{(1 - x) \sum_{k=0}^{s} y^k}{1 - x \sum_{k=0}^{s} y^k}$$

(3.9')
$$F_0 = \frac{1}{1 - x \sum_{k=0}^{s} y^k}$$

(3.10')
$$F = \frac{\sum_{k=0}^{S} y^{k}}{1 - x \sum_{k=0}^{S} y^{k}}$$

It can be verified that these results are in agreement with the results of Sec. 2 above.

REFERENCE

~*

1. J. Riordan, An Introduction to Combinatorial Analysis, Wiley New York, 1958.

(3.13)

LINEARLY RECURSIVE SEQUENCES OF INTEGERS

BROTHER L. RAPHAEL, FSC St. Mary's College, Moraga, California 94575

PART 1. INTRODUCTION

As harmless as it may appear, the Fibonacci sequence has provoked a remarkable amount of research. It seems that there is no end to the results that may be derived from the basic definition

$$F_{n+2} = F_{n+1} + F_n$$
 and $F_0 = 0$ and $F_1 = 1$,

which Leonardo of Pisa found lurking in the simple rabbit problem. For example, an extension of the definition yields the so-called Lucas numbers:

$$L_{n+2} = L_{n+1} + L_n$$
 and $L_0 = 2$ and $L_1 = 1$.

Evidently, any two integers may be used "to start" the sequence. However, it is well known that there is an extraordinary relationship between the Fibonacci and Lucas sequences. In particular:

$$F_{2n} = F_n L_n$$
 and $F_{n+1} + F_{n-1} = L_n$.

Precisely where does this peculiarity arise?

Then, again, many remarkable summation formulae are available. In particular, the n^{th} partial sum of the Fibonacci sequence is expressed by $F_{n+2} - 1$. The method used generally for proving such formulae is induction on the index. This involves

- 1. a guess provoked by the investigation of individual cases,
- 2. an efficient formulation of the guess, and
- 3. a proof by finite induction.

The drawbacks to this method are obvious. First, it depends very heavily on insight and cleverness, which qualities, while being desirable in any mathematician, do not lead to results very quickly. Second, this method is entirely inadequate for cases involving bulky formulations, and, of course, many times a result suggested by individual observation does not immediately come in convenient form. Finally, such a method is unable to relate and generalize results. Mathematics is incomplete until the specific, and perhaps surprising, facts are brought back to a generalization from which they maybe <u>deduced</u>. Not only does this give a foundation to the conclusions themselves, but it enables one to draw further, unsuspected conclusions, which are beyond inductive methods. Furthermore, as a result of a generalized deduction, the formulation will be more elegant and notationally consistent.

What is required then, is a generalization of the Fibonacci sequence, discarding the incidental. At points this project will appear to be unnecessarily removed from the simplicities of the original sequence, but attempts will be made to show the connections between the more general case and the more familiar results.

DE FINITIONS

The Fibonacci sequence is based on an additive relationship between any term and the two preceding terms. In our generalization, it is necessary to exploit two aspects of this relationship: we shall make it a linear dependence, and it will involve the preceding p terms. Here, and throughout, f will note the general additive sequence:

(1)
$$f_{n+p} = a_1 f_{n+p-1} + a_2 f_{n+p-2} + \cdots + a_p f_n$$
 (n = 0, 1, 2, ...).

It seems essential to the spirit of these sequences that they be integral. To insure this, we must demand that the set

$${a_i}^p_1$$

be integers. This set will be called the spectrum. But, returning to (1) and letting n = 0:

(2)

 \mathbf{or}

$$f_{p} = \sum_{k=1}^{p} a_{k} f_{p-k}$$
 ,

reveals that we must specify the first p terms of the sequence in order that the others may be obtained. The set of integers

 $\{\mathbf{f}_i\}_{0}^{p-1}$

so specified will be called the initial set, or the initials.

It might be mentioned here that the Fibonacci sequence is obtained by letting p = 2 and taking the spectrum $\{1,1\}$ and the initials $\{0,1\}$. And the Lucas sequence has p = 2, spectrum $\{1,1\}$ and initials $\{2,1\}$.

We wish now to extend the definition (1) so that negative values for the index are allowed. Using the "back-up" approach, we obtain

$$f_{p-1} = a_1 f_{p-2} + \dots + a_{p-1} f_0 + a_p f_{-1} ,$$

$$f_{-1} = \frac{1}{a_p} \left(f_{p-1} - \sum_{k=1}^{p-1} a_k f_{p-1-k} \right)$$

12

Continuing, it can be seen that, for any $n = 0, 1, 2, \cdots$,

(3)
$$f_{-n} = \frac{1}{a_p} \left(f_{p-n} - \sum_{k=1}^{p-1} a_k f_{p-n-k} \right) .$$

Clearly, in order to maintain an integral sequence for <u>all</u> values of the index, positive and negative, it is necessary to take $a_p = \pm 1$. In any case, we have that $a_p^2 = 1$.

UNARY SEQUENCES (p = 1)

The number p of necessary initial values classifies the sequence as unary, binary, tertiary, and so on. The analysis of the unary sequences is rather trivial. The spectrum is $\{a_1\}$ and the initial set $\{f_0\}$. But since p = 1, we must have $a_1 = \pm 1$, so that (1) comes down to:

or, immediately:

$$f_{n+1} = (\pm 1)^{n+1} f_0$$
.

= + f

f

In addition, it would seem altogether desirable to eliminate those sequences which can be "reduced" by dividing each term by a constant. That would leave only the <u>primitive</u> sequences for which if d divides f_k for each value of k, then d = 1. In addition, we eliminate those trivial sequences with each term zero. These conditions are met by demanding that neither the spectrum nor the initial set be all zero, and that no constant be divisible into all the spec-trum or initial set. With these restrictions, we see that the unary sequences become:

$$f_k = 1$$
, for all k, or
 $f_k = (-1)^k$.

This simply ends all discussion of unary sequences.

ALGEBRAIC GENERATORS

One of the most common manifestations of additive recursive sequences is the power series expansion of certain functions. For example, a short calculation leads one to conclude that:

$$\frac{x}{1 - x - x^2} = \sum_{k=0}^{\infty} F_k x^k .$$

The actual derivation of this result stems directly from the definition of the Fibonacci sequence. In what follows, we will use the same derivation in a generalized form. What we

1974]

LINEARLY RECURSIVE SEQUENCES OF INTEGERS

want to discover is an expression for:

$$\sum_{k=0}^{\infty} f_k x^k = \Phi(x),$$

where, by (1):

$$f_{n+p} = \sum_{k=1}^{p} a_k f_{n+p-k}$$

Now, we multiply (1) by x^{n+p} , and sum over the index n, so that:

$$\sum_{n=0}^{\infty} f_{n+p} x^{n+p} = \sum_{k=1}^{p} a_k x^k \sum_{n=0}^{\infty} f_{n+p-k} x^{n+p-k}$$

But, taking into account (4), we may rearrange this expression, and:

$$\Phi(\mathbf{x})\left(1 - \sum_{k=1}^{p} \mathbf{a}_{k} \mathbf{x}^{k}\right) = \mathbf{f}_{0} + \sum_{k=1}^{p-1} \mathbf{x}^{k}\left(\mathbf{f}_{k} - \sum_{j=1}^{k} \mathbf{a}_{j} \mathbf{f}_{k-j}\right).$$

This singularly awkward expression can be made manageable by making the somewhat arbitrary definition of $a_0 = -1$. The introduction of a_0 greatly simplifies the formulation of the required function:

(5)

(6)

$$\Phi(x) = \frac{\sum_{k=0}^{p-1} x^k \sum_{j=0}^{k} a_j f_{k-j}}{\sum_{k=0}^{p} a_k x^k}$$

We need hardly say that this is the required expression, which reduces to the familiar Fibonacci power series when p = 2, $a_1 = a_2 = 1$, and $f_0 = 0$, $f_1 = 1$. But, further investigation of (5) leads to considerations which will be of crucial importance later. First, we remark that the denominator is a p^{th} -degree polynomial:

$$-a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^p$$
, $(a_0 = -1)$,

which will be called the spectral polynomial.

Then, with regard to the numerator, the following definition will be made:

$$h_{m,k} = -\sum_{j=0}^{k} a_j f_{m+k-j}$$
 for $0 \le k \le p$.

14

(4)

[Feb.

In other words, $h_{m,k}$ is a partial sum of terms. For example:

$$h_{m,0} = -a_0 f_m = f_m$$

$$h_{m,p} = 0 cf (1).$$

$$h_{m,p-1} = a_p f_{m-1} ,$$

and, for convenience:

(7)
$$h_k = h_{0,k} = f_k - a_1 f_{k-1} - \cdots - a_k f_0$$
.

The introduction of (7) into (5) yields the remarkably concise:

(5')
$$\Phi(x) = \sum_{k=0}^{\infty} f_k x^k = \frac{-\sum_{k=0}^{p-1} h_k x^k}{\sum_{k=0}^{p} a_k x^k}$$

THE Q-SEQUENCE

In any f-sequence, it is possible to choose the initial set as any set of p consecutive terms, so that two "different" sequences may actually differ only in their indices. It seems then necessary to consider some sort of fundamental sequence. This fundamental sequence has the simplest non-trivial initial set; namely $\{0, 0, \dots, 0, 1\}$. The Fibonacci sequence is a binary case. These sequences exist for all values of p, and they will be called <u>Q</u>-sequences. Referring to (6), we will rename the partial sums $h_{m,k}$:

(8)
$$H_{m,k} = -\sum_{j=0}^{k} a_{j} Q_{m+k-j}$$
 for $0 \le k \le p$,

and, from (7):

$$H_k = H_{0,k} = -\sum_{j=0}^k a_j Q_{k-j}$$
,

but, from the definition of Q-sequences, $Q_k = 0$ for $0 \le k \le p-2$, and $Q_{p-1} = 1$:

$$H_k = 0$$
, for $0 \le k \le p - 2$, or $k = p$,
 $H_{p-1} = 1$.

Using these results in (5'), we have:

 $\sum_{k=0}^{\infty} Q_k x^k = \frac{-\sum_{k=0}^{p-1} H_k x^k}{\sum_{k=0}^{p} a_k x^k} = \frac{x^{p-1}}{-\sum_{k=0}^{p} a_k x^k}$

The right-hand member of (9) may be treated as a geometric series:

$$\frac{x^{p-1}}{1 - \sum_{k=1}^{p} a_k x^k} = x^{p-1} \left(\sum_{k_1=0}^{\infty} \sum_{k=0}^{p} \left(a_k x^k \right)^{k_1} \right) ,$$

and successive binomial expansions of the polynomial in parenthesis gives:

$$x^{p-1}\left(\sum_{k_1=0}^{\infty} \sum_{k=0}^{p} \left(a_k x^k\right)^{k_1}\right) = x^{p-1}\left(\sum_{k_1=0}^{\infty} \sum_{k_2=0}^{k_1} \left(k_1 \atop k_2\right) (a_1 x)^{k_1-k_2} \sum_{k=2}^{p} \left(a_k x^k\right)^{k_2}\right)$$

and so on. After p steps, we may collect coefficients of x^{m+p-1} in (9) and equate them, obtaining:

(10)
$$Q_{m+p-1} = \sum {\binom{k_1}{k_2}} {\binom{k_2}{k_3}} {\binom{k_3}{k_4}} \cdots {\binom{k_{p-1}}{k_p}} a_1^{k_1-k_2} a_2^{k_2-k_3} \cdots a_{p-1}^{k_{p-1}-k_p} a_p^{k_p}$$

where the sum is taken over all $\{k_i\}$ such that

$$\sum_{i=1}^{p} k_i = m ,$$

and $m + p - 1 \ge 0$. Looking at the binary case (p = 2), we discover that

$${\rm Q}_{n+1} \ = \ \sum_{i=0}^{\infty} {\binom{n \ - \ i}{i}} a_1^{n-2i} \, a_2^i \quad \text{,}$$

where

(9)

[Feb.

so that, for $a_1 = a_2 = 1$:

1974]

$$F_{n+1} = \sum_{i=0}^{\infty} \binom{n - i}{i}$$

which, of course, is the well-known "rising diagonal" result for Fibonacci numbers, derived from Pascal's triangle. And, for comparison, here is the ternary case:

(12)
$$Q_{n+2} = \sum_{i,j} {\binom{n-i-j}{i}} {\binom{i}{j}} a_1^{n-2i-j} a_2^{i-j} a_3^{j} .$$

<u>Remark</u>. In this section, and throughout the rest, we choose to make the agreement that $\binom{n}{k} = 0$ for all 0 < n < k. This appears a bit arbitrary, but it is used since it simplifies the summation notation. Notice that the upper index on the summation may be taken as infinity, since by our agreement the binomial coefficients vanish for large enough k. It might be pointed out that the real upper index, for example, in (11) is [n/2], that is, the greatest integer in n/2. The bulky notation required for (10) in particular in this form warrants using our more simplified method.

THE Q-SEQUENCE AS BASIS

The fundamental nature of the Q-sequence is clearly shown in the following argument. We return to (5'), and rearrange slightly:

$$\sum_{k=0}^{\infty} f_k x^k = \frac{-\sum_{k=0}^{p-1} h_k x^k}{\sum_{k=0}^{p} a_k x^k} = \sum_{k=0}^{p-1} h_k x^{k-p+1} \left(\frac{x^{p-1}}{\sum_{k=0}^{p} a_k x^k} \right)$$

then, taking into account (9), we have:

$$\sum_{k=0}^\infty \mathbf{f}_k \mathbf{x}^k = \sum_{k=0}^{p-1} \mathbf{h}_k \mathbf{x}^{k-p+1} \left(\sum_{i=0}^\infty \mathbf{Q}_i \mathbf{x}^i\right) \quad .$$

Comparing the coefficients of x^{m-p+1} in this expression, we find that:

(13)
$$f_{m-p+1} = \sum_{k=0}^{p-1} h_k Q_{m-k}$$

,

17

This clearly shows the basic nature of the Q-sequence — it forms a basis set for any other sequence having the same spectrum. But a more useful formulation may be derived by considering (7), and substituting into (13):

(14)
$$f_{m-p+1} = -\sum_{k=0}^{p-1} \sum_{j=0}^{k} a_j f_{k-j} Q_{m-k} ,$$

and then, using (8):

$$-\sum_{j=0}^{k} a_{j} Q_{m-p+1+k-j} = H_{m-p+1,k}$$
,

we have, from (14):

(15)
$$f_{m-p+1} = \sum_{k=0}^{p-1} H_{m-p+1, k} f_{p-k-1}$$
,

and finally, an obvious adjustment of index leaves us with:

(16)
$$f_m = \sum_{k=0}^{p-1} H_{m,k} f_{p-1-k}$$
 where $H_{m,k}$ is given by (8).

Remark. For certain values of k, an alternative form of (8) is desirable:

$$H_{m,k} = Q_{m+k} - \sum_{j=1}^{k} a_{j} Q_{m+k-j} = \sum_{j=1}^{p} a_{j} Q_{m+k-j} - \sum_{j=1}^{k} a_{j} Q_{m+k-j}$$

 \mathbf{or}

(17)

$$H_{m,k} = \sum_{j=1}^{p-k} a_{k+j} Q_{m-j}$$

THE H-SEQUENCE

What appeared in (8) to be merely notational convenience can now show more positive results. For example, a linear combination of p consecutive $H_{m,k}$ over the m index (in the spirit of (1)):

$$\sum_{j=1}^{p} a_{j} H_{m-j,k} = -\sum_{j=1}^{p} a_{j} \sum_{i=0}^{k} a_{i} Q_{m-j+k-i}$$
$$= -\sum_{i=0}^{k} a_{i} \sum_{j=1}^{p} a_{j} Q_{m+k-i-j}$$

$$= -\sum_{i=0}^{k} a_i Q_{m+k-i} = H_{m,k}$$

shows that $H_{m,k}$ is itself an f-sequence for any choice of k. In fact, for k = 0, the Hsequence reduces to the Q-sequence due to:

$$H_{m,0} = -\sum_{j=0}^{0} a_j Q_{m-j} = -a_0 Q_m = Q_m$$
.

But, for any choice of k, we must have in general, that H-sequences satisfy (16), since they are f-sequences:

(19)
$$H_{m,k} = \sum_{j=0}^{p-1} H_{m,j} H_{p-1-j,k}$$

which is a remarkable formula suggestive of a whole series of important results.

PART 2. MATRIX REPRESENTATIONS

A great many of the familiar Lucas and Fibonacci identities have been shown to be related to the properties of matrices. The attempt to generalize these results for higher orders of sequence directly leads to various sorts of results depending largely on the aspect taken for generalization. But our previous work has led up to the following formulae:

(8)
$$H_{m,k} = -\sum_{j=0}^{k} a_j Q_{m+k-j} \quad \text{for } 0 \le k \le p$$

and

(19)
$$H_{m,k} = \sum_{j=0}^{p-1} H_{m,j} H_{p-1-j,k}$$

(16)
$$f_m = \sum_{k=0}^{p-1} H_{m,k} f_{p-1-k}$$

These three equations are strongly suggestive of matrix multiplication, particularly the last (16). In fact, if the following definitions are made, a singularly simple formulation may be given:

(18)

LINEARLY RECURSIVE SEQUENCES OF INTEGERS

(20)

 $\underline{\mathbf{H}}^{\mathbf{m}} = \begin{pmatrix} \mathbf{H}_{\mathbf{m}+\mathbf{p}-1, 0} \cdots \mathbf{H}_{\mathbf{m}+\mathbf{p}-1, \mathbf{p}-1} \\ \vdots & \vdots \\ \mathbf{H}_{\mathbf{m}, 0} \cdots \mathbf{H}_{\mathbf{m}, \mathbf{p}-1} \end{pmatrix},$

Then:

and

(24)

$$\underline{H}^{0} = \begin{pmatrix} H_{p-1,0} \cdots H_{p-1,p-1} \\ \vdots & \vdots \\ H_{0,0} \cdots H_{0,p-1} \end{pmatrix} = I_{p}, \text{ the identity,}$$

$$\underline{\mathbf{H}}^{1} = \underline{\mathbf{H}} = \begin{pmatrix} \mathbf{a}_{1} & \mathbf{a}_{2} & \cdots & \mathbf{a}_{p-1} & \mathbf{a}_{p} \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

A glance at (19) shows that the matrix <u>H</u> is really multiplicative; that is:

$$\underline{\mathbf{H}}^{\mathbf{m}}\underline{\mathbf{H}}^{\mathbf{n}} = \underline{\mathbf{H}}^{\mathbf{m}+\mathbf{n}}$$

since (19) is merely a statement of such a multiplication, row by column. Here again, what began in (8) as mere convenience, is seen to have something of a fundamental character with regard to the recursive sequences. Now, in addition, let us define:

(21)
$$\underbrace{\overset{\bullet}{\mathbf{F}}}_{\mathbf{m}} = \begin{pmatrix} \mathbf{f}_{\mathbf{m}+\mathbf{p}-1} \\ \mathbf{f}_{\mathbf{m}+\mathbf{p}-2} \\ \vdots \\ \mathbf{f}_{\mathbf{m}+1} \\ \mathbf{f}_{\mathbf{m}} \end{pmatrix}$$

Finally, then, it is evident that (16) may be written in the matrix form:

(22)
$$\underline{\mathbf{F}}_{\mathbf{m}} = \underline{\mathbf{H}}^{\mathbf{m}} \underline{\underline{\mathbf{F}}}_{\mathbf{0}}$$

A particularly useful remark may be inserted here:

(23)
$$\det \underline{H}^{m} = (\det \underline{H})^{m} = (a_{p}(-1)^{p+1})^{m}$$

This can be seen by considering definitions (20). However, in order to maintain a sequence which has integers for all values of the index we need $a_p = \pm 1$, as was seen in (3). Hence, for any value of m, det $\underline{H}^{m} = \pm 1$. Also, the harmless observation that $\underline{H}^{m}\underline{H}^{n} = \underline{H}^{m+n}$, when compared entry for entry

leads to the remarkable:

$$\sum_{k=1}^{p} H_{m+p-k, j-1} H_{n+p-i, k-1} = H_{m+n+p-i, j-1}$$

 $\mathbf{20}$

[Feb.

which is actually a generalization of (19).

In particular, by taking i = p and j = 1 in (24), and recalling that $H_{m,0} = Q_m$ in (8), and then rearranging index in (24):

(25)
$$\sum_{k=0}^{p-1} H_{n,k} Q_{m+p-k-1} = Q_{m+n}$$

GENERAL REDUCTIONS

Rather than considering column matrices of f_k , we now extend the treatment to the square matrix, having columns given by (21):

(26)
$$\underline{F}_{m} = \begin{pmatrix} f_{m+2p-1} \cdots f_{m+p-1} \\ f_{m+2p-2} \cdots f_{m+p-2} \\ \vdots & \vdots \\ f_{m+p-1} \cdots f_{m} \end{pmatrix} \cdot$$

Then (22) becomes an expression involving $p \times p$ matrices:

where:

$$\underline{\mathbf{F}}_{0} = \begin{pmatrix} \mathbf{f}_{2p-1} \cdots \mathbf{f}_{p-1} \\ \vdots & \vdots \\ \mathbf{f}_{p-1} \cdots & \mathbf{f}_{0} \end{pmatrix} ,$$

 $\underline{\mathbf{H}}^{\mathbf{m}}\underline{\mathbf{F}}_{\mathbf{0}} = \underline{\mathbf{F}}_{\mathbf{m}}$

Taking determinants, and simplifying, using (23):

(27)
$$\det \underline{F}_{m} = \det \underline{H}^{m} \det \underline{F}_{0}$$
$$= (a_{p}(-1)^{p-1})^{m} \det \underline{F}_{0}$$

or:

$$\left| \det \underline{F}_{m} \right| = \left| \det \underline{F}_{0} \right|$$
 for any m.

Clearly, the number det \underline{F}_0 is an extraordinary constant for any sequence which depends on the initial set $\{f_i\}_0^{p-1}$, and which will be called the <u>characteristic</u>.

The characteristic of the Fibonacci sequence is

$$\begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} = 1 ,$$

while that of the Lucas sequence is

. ••

$$\begin{vmatrix} 3 & 1 \\ 1 & 2 \end{vmatrix} = 5 ,$$

as is well known.

Again, the simple remark that:

$$\underline{\mathbf{F}}_{\mathbf{m}+\mathbf{n}} = \underline{\mathbf{H}}^{\mathbf{m}+\mathbf{n}} \underline{\mathbf{F}}_{\mathbf{0}} = \underline{\mathbf{H}}^{\mathbf{m}} \underline{\mathbf{F}}_{\mathbf{n}}$$

plus, a comparison of entries, gives:

(28)
$$f_{m+n} = \sum_{k=0}^{p-1} H_{m,k} f_{n+p-1-k}$$

which is the general reduction. It is a generalization of (16).

EXAMPLES

The binary case, of course, yields the most familiar results:

(29)
$$\underline{H}^{m} = \begin{pmatrix} Q_{m+1} & a_2 Q_m \\ Q_m & a_2 Q_{m-1} \end{pmatrix}$$
so that:

$$\underline{\mathbf{H}} = \begin{pmatrix} \mathbf{a}_1 & \mathbf{a}_2 \\ \mathbf{1} & \mathbf{0} \end{pmatrix} \quad \text{and} \quad \det \underline{\mathbf{H}} = -\mathbf{a}_2 \ .$$

From (27) in the binary case:

(30)
$$f_{m+2}f_m - f_{m+1}^2 = (-a_2)^m (f_2 f_0 - f_1^2)$$

so that, for the Q-sequence:

 \mathbf{or}

$$Q_{m+2} Q_m - Q_{m+1}^2 = (-a_2)^m (-1)$$

(31)
$$Q_m^2 - Q_{m+1}Q_{m-1} = (-a_2)^{m-1}$$

and the binary reduction becomes, referring to (28):

(32)
$$Q_m f_{n+1} + a_2 Q_{m-1} f_n = f_{m+n}$$

The correspondence with the usual Fibonacci results may be worked out in detail directly from these identities.

Now, turning our attention to the ternary case (p = 3), we discover several important points. First, the elegant formulations of the binary case do not hold up for p = 3, or for higher cases. Also, symmetry of expression begins to fade with the higher sequences.

Clearly, most of the interesting properties of the Fibonacci sequence stem from its being a binary sequence, while a few come from its being a sequence in general. We will here give the ternary results:

(33)
$$\underline{H}^{m} = \begin{pmatrix} Q_{m+2} & a_{2}Q_{m+1} + a_{3}Q_{m} & a_{3}Q_{m+1} \\ Q_{m+1} & a_{2}Q_{m} + a_{3}Q_{m-1} & a_{3}Q_{m-1} \\ Q_{m} & a_{2}Q_{m-1} + a_{3}Q_{m-2} & a_{3}Q_{m-2} \end{pmatrix}$$

and

1974]

$$\underline{\mathbf{H}} = \begin{pmatrix} \mathbf{a}_1 & \mathbf{a}_2 & \mathbf{a}_3 \\ \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \end{pmatrix}$$

so that: det $\underline{H} = a_3$ hence:

(34)
$$\begin{vmatrix} f_{m+4} & f_{m+3} & f_{m+2} \\ f_{m+3} & f_{m+2} & f_{m+1} \\ f_{m+2} & f_{m+1} & f_{m} \end{vmatrix} = (a_3)^m \begin{vmatrix} f_4 & f_3 & f_2 \\ f_3 & f_2 & f_1 \\ f_2 & f_1 & f_0 \end{vmatrix}$$

For Q-sequences in the ternary case:

(35)
$$\begin{vmatrix} Q_{m+4} & Q_{m+3} & Q_{m+2} \\ Q_{m+3} & Q_{m+2} & Q_{m+1} \\ Q_{m+2} & Q_{m+1} & Q_{m} \end{vmatrix} = -(a_3)^m$$

And the ternary reduction:

(36)
$$Q_m f_{n+2} + (Q_{m+1} - a_1 Q_m) f_{n+1} + a_3 Q_{m-1} f_n = f_{m+n}$$
.

NEGATIVE INDEX

Already, we have investigated the nature of the general sequence for negative values of the index. A necessary and sufficient condition that a sequence be primitive and integral is that $a_p^2 = 1$. Now, using more recent results, it is possible to look into the matter a bit more deeply, and obtain expressions relating terms of negative index with those of positive index.

Were the matrix equation $\underline{H}^{m} \underline{F}_{0} = \underline{F}_{m}$ to hold for negative value of the index:

| | $\underline{\mathbf{F}}_{-\mathbf{m}} = \underline{\mathbf{H}}^{-\mathbf{m}} \underline{\mathbf{F}}_{0} = (\underline{\mathbf{H}}^{\mathbf{m}})^{-1} \underline{\mathbf{F}}_{0} ,$ |
|--------------------|--|
| or, in particular: | 1 |
| (37) | $\underline{\mathrm{H}}^{-\mathrm{m}} = (\underline{\mathrm{H}}^{\mathrm{m}})^{-1},$ |

so that, after the indicated inversion, we may equate the entries in (37):

(38)

 $\mathbf{24}$

$$H_{-m+p-i, j-1} = \frac{1}{\det \underline{H}^{m}} \quad \text{minor } H_{m+p-j, i-1}$$

Then, letting j = 1, and recalling (8):

$$H_{-m+p-i,0} = Q_{-m+p-i} = \frac{1}{\det \underline{H}^{m}} \quad \text{minor } H_{m+p-1,i-1}$$

-

and, then, letting i = p, we have, after reference to (23):

(39)
$$Q_{-m} = (a_p(-1)^{p+1})^{-m} \text{ minor } H_{m+p-1,p-1}$$

Then, for the general case, we need only note that from (16):

(16')
$$f_{-m} = \sum_{k=0}^{p-1} H_{-m,k} f_{p-1-k},$$

where:

(8')
$$H_{-m,k} = \sum_{j=0}^{k} a_j Q_{-m+k-j} .$$

As a footnote, we add two identities coming from the equation $\underline{H}^{m}\underline{H}^{-m} = I_{p}$, where entries are compared, after completing the multiplication on the left member:

(40)
$$\sum_{k=1}^{p} H_{m+p-k, j-1} H_{-m+p-i, k-1} = H_{p-i, j-1} = \delta_{ij}$$

for $0 \le 1 \le p$, $0 \le j \le p$ and $0 \le k \le p$, and where δ_{ij} is Kronecker's delta. If i = p and j = 1 in (40):

$$\sum_{k=1}^{p} H_{m+p-k,0} H_{-m,k-1} = H_{0,0} ,$$

which may be rewritten:

$$\sum_{k=0}^{p-1} Q_{m+p-k-1} H_{-m,k} = 0 .$$

(41)

Applying (39) to the binary case yields the intriguing result:

(42)
$$Q_{-m} = -(-a_2)^{-m}Q_{m}$$
 or that: $|Q_{-m}| = |Q_{m}|$, for $p = 2$,

while in the ternary case:

1974]

(43)
$$Q_{-m} = (a_3)^{-m}(Q_{m+1}^2 - Q_m Q_{m+2})$$
, for $p = 3$.

Clearly, the beauty of the expression for p = 2 does not carry over to the situations for greater values of p.

MATRIX SEQUENCES

An obvious, but interesting result of (26) is the matrix expression (using entrywise addition):

(44)
$$\sum_{k=1}^{p} a_k \underline{F}_{m-k} = \underline{F}_m \quad .$$

From (1), it is evident that the matrices $\{\underline{F}_k\}$ form an f-sequence with spectrum $\{a_k\}_{i}^{p}$. Furthermore, (44) may be written, using the definition of \underline{F}_{m} :

$$\sum_{k=1}^{p} \mathbf{a}_{k} \underline{\mathbf{F}}_{m-k} \ = \ \sum_{k=1}^{p} \mathbf{a}_{k} \underline{\mathbf{H}}^{m-k} \underline{\mathbf{F}}_{0} \ = \ \underline{\mathbf{H}}^{m} \underline{\mathbf{F}}_{0} \ ;$$

however, $\underline{F}_0 \neq 0$, so that, dividing it out:

(45)
$$\sum_{k=0}^{p} a_k \underline{H}^{m-k} = 0 ,$$

in which case the powers of the matrix H form an f-sequence. In fact, (45) is really a result of the Cayley-Hamilton Theorem.

ROOTS OF THE SPECTRAL POLYNOMIAL

Returning to the earlier question of explicit determination of $\,f_{}_{}_{}$ and $\,Q_{}_{}_{}_{}$, we recall that (10) was obtained, which expressed $Q_{\rm m}$ in terms of a sum of binomial coefficients. A different approach now will yield the so-called Binet form, which may then be compared with (10) for a series of remarkable relationships. But first we return to (5'):



recalling that the spectral polynomial appears in the denominator. Now consider that this polynomial has been factored in the complex field:

(46)
$$-\sum_{k=0}^{p} a_{k} x^{k} = \prod_{i=1}^{p} (1 - r_{i} x) ,$$

where the roots are $\{1/r_i\}_{i}^{p}$, a set of complex numbers, none of which are zero. Now, let us make the very strong assumption that the roots are <u>distinct</u>, so that:

(47)
$$\sum_{k=0}^{\infty} f_k x^k = \frac{\sum_{k=0}^{p-1} h_k x^k}{\prod_{i=1}^{p} (1 - r_i x)} = \sum_{i=1}^{p} \frac{A_i}{1 - r_i x} ,$$

where the right-hand member is a sum of partial fractions. What is needed is an expression for each A_i . Using a geometric series and (47):

$$\sum_{k=0}^\infty \mathbf{f}_k \mathbf{x}^k \ = \sum_{i=1}^p \mathbf{A}_i \sum_{j=0}^\infty \mathbf{r}_i^j \mathbf{x}^j \quad \text{,}$$

and, equating coefficients of x^k :

$$\mathbf{f}_{k} = \sum_{j=1}^{p} \mathbf{A}_{j} \mathbf{r}_{j}^{k}$$

Then, from (5') and (46):

(48)

$$\sum_{k=0}^{\infty} f_k x^k \left(\prod_{i=1}^{p} (1 - r_i x) \right) = \sum_{k=0}^{p-1} h_k x^k$$

[Feb.

and so, cancelling the term $(1 - r_k x)$, after introducing (47):

$$\sum_{k=1}^{p} A_k \prod_{i \neq k} (1 - r_i x) = \sum_{k=0}^{p-1} h_k x^k$$

Now, we substitute r_n (n = 1, 2, ..., p) for 1/x, and recall that the $\{r_i\}$ are distinct:

$$A_{n}\left(\prod_{i \neq n} \left(1 - \frac{r_{i}}{r_{n}}\right)\right) = \sum_{k=0}^{p-1} h_{k} (1/r_{n})^{k}$$

so that, finally:

$$A_{n} = \frac{\sum_{k=0}^{p-1} h_{k} r_{n}^{p-1-k}}{\prod_{i \neq n} (r_{n} - r_{i})}$$

which is exactly the expression for the A_n demanded for (47), and (48). In fact, now we may introduce into (48) the value for A_i derived from (49):

$$f_{m} = \sum_{j=1}^{p} \sum_{k=0}^{p-1} h_{k} \cdot \frac{r_{j}^{m+p-1-k}}{\prod_{i \neq j} (r_{j} - r_{i})}$$

(50) $f_{m} = \sum_{k=0}^{p-1} h_{k} \left(\sum_{j=1}^{p} \frac{r_{j}^{m+p-1-k}}{\prod_{i \neq i} (r_{j} - r_{i})} \right)$

However, comparing (50) with (13) and rearranging index shows that:

(51)
$$Q_{m} = \sum_{j=1}^{p} \frac{r_{j}^{m}}{\prod_{i \neq j} (r_{j} - r_{i})}$$

where, of course, the r_i are assumed to be distinct. This expression (51) is the general <u>Binet-form</u> for the Q-sequences.

,

or:

(49)

<u>Remark</u>. We note that, at the opposite extreme, the assumption might have been made that $r_i = r$ for all i, so that all the spectral polynomial roots are equal:

(52)
$$-\sum_{k=0}^{p} a_{k} x^{k} = (1 - rx)^{p},$$

in which case (5') becomes:

(53)
$$\sum_{k=0}^{\infty} f_k x^k = \frac{\sum_{k=0}^{p-1} h_k x^k}{(1 - rx)^p}$$

and a geometric expansion, and comparison of coefficients of x^m gives:

(54)
$$f_{m} = \sum_{j=0}^{p-1} {m + p - 1 - j \choose p - 1} h_{j} r^{m-j}$$

and, again, comparing this expression with (13) gives that:

(55)
$$Q_{m} = {m \choose p-1} r^{m-p+1}$$

EXAMPLES

In the binary case, many of the above results produce elegant formulae. Hence, if in (51) the roots are $1/r_1 \neq 1/r_2$ and $1 - a_1x - a_2x^2 = (1 - r_1x)(1 - r_2x)$, then:

(56)
$$Q_{m} = \frac{r_{1}^{m}}{r_{1} - r_{2}} + \frac{r_{2}^{m}}{r_{2} - r_{1}} = \frac{r_{1}^{m} - r_{2}^{m}}{r_{1} - r_{2}}$$

where $r_1 + r_2 = a_1$ and $r_1r_2 = -a_2$.

In the case that $r_1 = r_2 = r$, we have $2r = a_1$ and $r^2 = -a_2$, so that there are two cases: 1) r = +1, $a_1 = 2$ and $a_2 = -1$, and 2) r = -1, $a_1 = -2$ and $a_2 = 1$. And, in either case:

(57) $Q_m = \binom{m}{1}r^{m-1} = mr^{m-1},$ where:

$$Q_{m+2} = 2rQ_{m+1} - Q_m$$

Evidently, by factoring and dividing in (56), and then allowing r_1 to approach r_2 :

 $\mathbf{28}$

LINEARLY RECURSIVE SEQUENCES OF INTEGERS

$$Q_m = \sum_{k=0}^{m-1} r_1^{m-1-k} r_2^k = mr^{m-1}$$
 if $r_1 = r_2$,

hence, all three cases may be said to be derived from (56).

Now, foregoing the tedious calculation, we give the ternary results (p = 3):

(58)
$$Q_{m} = \frac{r_{1}^{m}}{(r_{1} - r_{2})(r_{1} - r_{3})} + \frac{r_{2}^{m}}{(r_{2} - r_{3})(r_{2} - r_{1})} + \frac{r_{3}^{m}}{(r_{3} - r_{1})(r_{3} - r_{2})} ,$$
where

w

$$1 - a_1 x - a_2 x^2 - a_3 x^3 = (1 - r_1 x)(1 - r_2 x)(1 - r_3 x)$$

If two roots are equal, then $r_2 = r_3$ say, and:

(59)
$$Q_{m} = \frac{r_{1}^{m} - r_{2}^{m}}{(r_{1} - r_{2})^{2}} - \frac{mr_{2}^{m-1}}{r_{1} - r_{2}}$$

where

$$1 - a_1 x - a_2 x^2 - a_3 x^3 = (1 - r_1 x)(1 - r_2 x)^2$$

,

And, if $\mathbf{r}_1 = \mathbf{r}_2 = \mathbf{r}_3 = \mathbf{r}$, then:

(60)
$$Q_{m} = \frac{1}{2}m(m-1)r^{m-2}$$

where

$$Q_{m+3} = 3rQ_{m+2} - 3Q_{m+1} + rQ_m$$
 and $r = +1 \text{ or } -1$

Once again, although now there are an infinite number of cases depending on the nature of the roots, it can be seen that (59) and (60) can be derived from (58) directly, using in part the identity:

$$\frac{\mathbf{r}_1^m - \mathbf{r}_2^m}{(\mathbf{r}_1 - \mathbf{r}_2)^2} = \sum_{k=2}^m \mathbf{r}_1^{m-k} \mathbf{r}_2^{k-2} (k - 1) + \frac{m\mathbf{r}_2^{m-1}}{\mathbf{r}_1 - \mathbf{r}_2} .$$

In summary, then, we can, with minor adjustments in view of multiple roots of the spectral polynomial, consider that the form (51) actually is the expression for $\,\,{\rm Q}_{m}^{}\,\,$ in terms of the roots of the spectral polynomial. On the other hand, (10) expresses Q_m in terms of the coefficients of the spectral polynomial. That this is a source of a multitude of fascinating problems is left to the imagination of the reader, as well as to his leisure.

1974]

LINEARLY RECURSIVE SEQUENCES OF INTEGERS

PART 3. SYMMETRIC FUNCTIONS

By attacking the entire problem from another point of view, it will be possible to derive a generalization of the Lucas sequence, and thence derive a set of remarkable identities involved with this generalization similar to the usual Fibonacci-Lucas result that $F_n L_n = F_{2n}$. Consider, first, a set of complex numbers $\{r_i\}_{i}^{k}$, and a defining relation:

(61)
$$\prod_{j=1}^{k} (x - r_j) = \sum_{k=0}^{k} (-1)^{i} S_{i} x^{k-i} .$$

The coefficients S_i are clearly the elementary symmetric functions of $\{r_i\}$. In particular:

$$\begin{split} S_0 &= 1, & \text{in any case,} \\ S_1 &= r_1 + r_2 + r_3 + \cdots + r_k \\ S_2 &= r_1 r_2 + r_1 r_3 + \cdots , \\ S_k &= r_1 r_2 r_3 \cdots r_k, & \text{and} \\ S_n &= 0, & \text{for } n > k . \end{split}$$

(62)

By substituting r_m into (61):

$$\mathbf{r}_{m}^{k} = \sum_{i=1}^{k} (-1)^{i-1} \mathbf{s}_{i} \mathbf{r}_{m}^{k-i}$$

or, after multiplying by r_m^{n-k} :

(63)
$$r_m^n = \sum_{i=1}^k (-1)^{i-1} S_i r_m^{n-i}$$

Suppose that t_n is any linear combination of the $\{r_j^n\}$, so that from (63), it is clear that:

$$t_n = \sum_{i=1}^k (-1)^{i-1} S_i t_{n-i}$$

In which case, if we further define $a_i = (-1)^{i-1} S_i$, we have (letting k = p):

(64)
$$t_n = \sum_{i=1}^p a_i t_{n-i}$$

Hence, from (1), a sequence of linear combinations of n^{th} powers of r_j is actually an f-sequence. Further, the Q-sequence defined by (51) is a specific case of linear combination.

It seems reasonable to investigate the properties of the simplest t-sequence, namely, the simplest linear combination of n^{th} powers of r_i , which will be called a T-sequence:

(65)
$$T_n = \sum_{j=1}^p r_j^n$$

in which case:

$$T_0 = p$$
$$T_1 = a_1$$
$$T_2 = a_1^2 + 2a_2$$

and, in general,

(66)
$$T_k = a_1 T_{k-1} + a_2 T_{k-2} + \dots + a_{k-1} T_1 + k a_k$$
 for $k \le p$

<u>Remark</u>. Since $a_i = (-1)^{i-1}S_i$, then, in particular, $a_0 = -1$, as was defined earlier. In addition, it must be remarked that the a_i defined just before (64) must be integers, in keeping with the definitions made in the first part of this paper guaranteeing that the f-sequences be sequences of integers.

From (7) and (66), it can be seen that $h_{0,k} = -a_k(p-k)$ for $k \le p$ for any T-sequence. Immediately, (5') becomes

(67)
$$\sum_{k=0}^{\infty} T_k x^k = \frac{\sum_{k=0}^{p-1} a_k (p - k) x^k}{\sum_{k=0}^{p} a_k x^k}$$

and, if s(x) denotes the spectral polynomial

$$-\sum_{k=0}^{p}a_{k}x^{k}:$$

$$\sum_{k=0}^{\infty} T_k x^k = p - x \cdot s'(x)/s(x)$$

(68)

Already, from (9):

$$\sum_{k=0}^{\infty} Q_k x^k = x^{p-1}/s(x)$$

so that clearly, we have:

(69)
$$\mathbf{s}(\mathbf{x}) \quad \frac{\mathrm{d}}{\mathrm{dx}} \left(\mathbf{x} \sum_{k=0}^{\infty} \mathbf{Q}_k \mathbf{x}^k \right) = \mathbf{x}^{p-1} \sum_{k=0}^{\infty} \mathbf{T}_k \mathbf{x}^k$$

In the derivation of which, a bit of the tedious rearrangement has been passed over. In addition, noting again that $h_{0,k} = h_k = -a_k(p - k)$ and substituting into (13):

$$T_{m-p+1} = -\sum_{k=0}^{p-1} a_k (p - k) Q_{m-k}$$
$$= -p \sum_{k=0}^{p} a_k Q_{m-k} + \sum_{k=0}^{p} a_k k Q_{m-k}$$

but the first term on the right is exactly zero by (1); so:

$$T_{m-p+1} = \sum_{k=0}^{p} k a_k Q_{m-k}$$

or:

(70)

$$T_{m} = \sum_{k=1}^{p} k a_{k} Q_{m+p-1-k}$$

Inspecting (70) and looking at various cases leads to the remark that, in fact, (70) is exactly the generalization of $L_m = F_{m+1} + F_{m-1} = F_m + 2F_{m-1}$, which is a familiar Fibonacci-Lucas identity.

EXAMPLES

What follows now is a rather long discussion of the binary case for T-sequences. The most fascinating results occur when p = 2, so that a presentation of this situation is reward-ing. First, in the binary case:

$$T_n = r_1^n + r_2^n$$
, where $r_i^2 - a_1 r_1 - a_2 = 0$, $i = 1, 2$;

32

 $T_n = 2r^n$.

or, if r₁ = r₂ = r: (71)

In either case:

$$Q_{n}T_{n} = \left(\frac{r_{1}^{n} - r_{2}^{n}}{r_{1} - r_{2}}\right)(r_{1}^{n} + r_{2}^{n})$$
$$= \frac{r_{1}^{2n} - r_{2}^{2n}}{r_{1} - r_{2}}$$

so that:

(72)
$$Q_n T_n = Q_{2n}$$
.
Then, from (70):
 $T_n = a_1 Q_m + 2a_2 Q_{m-1}$
or:
(73) $T_n = Q_{m+1} + a_2 Q_{m-1}$

The symmetry of (72) and (73) reveals the underlying charm of the Lucas sequence, which, of course, carries over to any binary T-sequence. Continuing, using (73) and (42):

$$T_{-m} = Q_{-m+1} + a_2 Q_{-m-1}$$

= $-(-a_2)^{-m+1} Q_{m-1} - a_2 (-a_2)^{-m-1} Q_{m+1}$
= $(-a_2)^{-m} (a_2 Q_{m-1} + Q_{m+1})$
= $(-a_2)^{-m} T_m$

 $|T_{-m}| = |T_{m}|$.

or, as in (42):

(74)

Applying (73), we have:

(75)
$$T_{m+1} + a_2 T_{m-1} = Q_m (a_1^2 + 4a_2)$$

while the characteristic expression (27) is:

(76)
$$T_{m+2}T_m - T_{m+1}^2 = (-a_2)^m (a_1^2 + 4a_2)$$

But the general reduction (28) provides the most elegant formulae, both for Q- and T-sequences:

(77)
$$Q_{m}T_{n+1} + a_{2}Q_{m-1}T_{n} = T_{m+n}$$
$$Q_{m}Q_{n+1} + a_{2}Q_{m-1}Q_{n} = Q_{m+n} ,$$

and, taking (74) into account:

(78)
$$T_{m-n} = (-a_2)^{-n} (Q_{m+1} T_n - Q_m T_{n+1}) Q_{m-n} = (-a_2)^{-n} (Q_{m+1} Q_n - Q_m Q_{n+1})$$

T_nT_m

so that, adding (77) and (78):

$$T_{m+n} + (-a_2)^n T_{m-n} = T_n T_m$$

 $Q_{m+n} + (-a_2)^n Q_{m-n} = T_n Q_m$

or, subtracting:

(80)
$$T_{m+n} - (-a_2)^n T_{m-n} = Q_n Q_m (a_1^2 + 4a_2) \quad cf. \quad (75)$$
$$Q_{m+n} - (-a_2)^n Q_{m-n} = Q_n T_m$$

and rearranging index in (79) and (80):

(81)

$$Q_{n+k}Q_{n-k} = (T_{2n} - (-a_2)^{n-k}T_{2k}) / (a_1^2 + 4a_2)$$

$$Q_{n+k}T_{n-k} = Q_{2n} + (-a_2)^{n-k}Q_{2k}$$

$$T_{n+k}Q_{n-k} = Q_{2n} - (-a_2)^{n-k}Q_{2k}$$

$$T_{n+k}T_{n-k} = T_{2n} + (-a_2)^{n-k}T_{2k}$$

and, finally:

(82)
$$Q_{2n}Q_{2k} = Q_{n+k}^2 - Q_{n-k}^2 = \frac{T_{n+k}^2 - T_{n-k}^2}{(a_1^2 + 4a_2)}$$

Remark. The ternary and higher cases yield no such results; that is, the symmetry and conciseness do not carry over for $p \ge 2$. Then, it is clear, the Lucas-Fibonacci relationship is based almost entirely on the character of the two sequences as binary sequences.

PART 4. FINITE SUMS

A number of Fibonacci identities are concerned with the formulation in terms of the Fibonacci sequence of the sum of a certain series of terms of the sequence. For example, the simplest case:

$$\sum_{k=0}^{n} F_{k} = F_{n+2} - 1 \ .$$

We now seek to generalize this result. Recalling earlier definitions and theorems:

$$f_{m+p} = \sum_{k=1}^{p} a_k f_{m+p-k}$$

$$\mathbf{h}_{\mathbf{m},k} = -\sum_{j=0}^{k} \mathbf{a}_{j} \mathbf{f}_{\mathbf{m}+k-j}$$

(6)

(1)

 $\mathbf{34}$

(79)
and we define: $a_0 = -1$ and $h_{0,k} = h_k$, so that:

(5')
$$\sum_{k=0}^{\infty} f_k x^k = \frac{-\sum_{k=0}^{p-1} h_k x^k}{\sum_{k=0}^{p} a_k x^k}$$

But the initial set $\{f_i\}_{0}^{p-1}$ may be chosen arbitrarily, so it is possible to choose for initials the set $\{f_{m+i}\}$ where $i = 0, 1, 2, \cdots, p = 1$. In that case, (5') becomes:

¢

(83)
$$\sum_{k=0}^{\infty} f_{m+k} x^{k} = -\frac{-\sum_{k=0}^{p-1} h_{m,k} x^{k}}{\sum_{k=0}^{p} a_{k} x^{k}}$$

and rearranging the left member:

$$\sum_{k=m}^{\infty} f_k x^{k-m} = \frac{-\sum_{k=0}^{p-1} h_{m,k} x^k}{\sum_{k=0}^{p} a_k x^k}$$

or, multiplying by x^{m} :

$$\sum_{k=m}^{\infty} f_k x^k = \frac{-\sum_{k=0}^{p-1} h_{m,k} x^{m+k}}{\sum_{k=0}^{p} a_k x^k}$$

(84)

Then, by a simple substitution:

$$\sum_{k=n}^{\infty} f_k x^k = \frac{-\sum_{k=0}^{p-1} h_{n,k} x^{n+k}}{\sum_{k=0}^{p} a_k x^k}$$

and, subtracting these two expressions:

1974]

$$\sum_{k=m}^{n-1} f_k x^k = \frac{\sum_{k=0}^{p-1} (h_{n,k} x^n - h_{m,k} x^m) x^k}{\sum_{k=0}^{p} a_k x^k}$$

Letting x = 1, and assuming that $\sum a_k \neq 0$:

$$\sum_{k=m}^{n-1} f_k = \frac{\sum_{k=0}^{p-1} (h_{n,k} - h_{m,k})}{\sum_{k=0}^{p} a_k}$$

Remark. Evidently, the sum in the left member of (86) is finite, so that in the case that $\sum a_k = 0$, the numerator on the right must be divisible by the denominator.

In the event that p = 2, we have the simpler expression:

(87)
$$\sum_{k=n}^{n-1} f_k = \frac{(f_n - f_m) + a_2(f_{n-1} - f_{m-1})}{-1 + a_1 + a_2}$$

and

(88)
$$\sum_{k=1}^{n-1} Q_k = \frac{Q_n + a_2 Q_{n-1} - 1}{a_1 + a_2 - 1}$$

which reduces to the Fibonacci expression when $a_1 = a_2 = 1$.

SUMMARY

At the outset, it was proposed to find a generalization from which all the familiar results for Fibonacci-Lucas sequences might be deduced, in addition to which a consistent notation might be developed, and finally, that the sources of the peculiarity of the Fibonacci-Lucas sequences might be found. It is hoped that such proposals are worked out in the course of the paper. All that remains to be said concerns the sources of peculiarity which is the bulk of the charm surrounding the Fibonacci-Lucas sequences. Of course, some of these properties stem from the very nature of a recursive sequence of integers (such as (5) and (27)); while other properties stem from the Q-sequence in particular (for example, (10) and (51)); while others still come from those formulae which assume different forms when $a_1 =$ $a_2 = 1$. Actually, it is quite extraordinary how many of the properties of the Fibonacci-Lucas

(85)

(86)

[Feb.

sequences are shared by a larger class of sequences.

REFERENCES

- 1. James A. Jeske, "Linear Recurrence Relations, Part I," Fibonacci Quarterly, Vol. 1, No. 2 (April 1963), pp. 69-74; Part II, Vol. 1, No. 4 (Dec. 1963), pp. 35-40; Part III, Vol. 2, No. 3 (Oct. 1964), pp. 197-202.
- 2. Ken Siler, "Fibonacci Summations," Fibonacci Quarterly, Vol. 1, No. 3 (Oct. 1963), pp. 67-70.
- 3. E. P. Miles, Jr., "Generalized Fibonacci Numbers and Associated Matrices," Amer. Math. Monthly, 67 (1960), p. 745.
- 4. R. A. Rosenbaum, "An Application of Matrices to Linear Recursion Relations," Amer. Math. Monthly, 66 (1959), p. 792 (note).
- 5. David Zeitlin, "On Summation Formulae for Fibonacci and Lucas Numbers," Fibonacci Quarterly, Vol. 2, No. 2 (Apr. 1964), pp. 105-107.
- 6. David Zeitlin, "Power Identities for Sequences defined by $W_{n+2} = dW_{n+1} cW_n$," <u>Fib-</u> onacci Quarterly, Vol. 3, No. 4 (Dec. 1965), pp. 241-256.
- 7. V. C. Harris and Carolyn C. Styles, "A Generalization of Fibonacci Numbers," Fibonacci Quarterly, Vol. 2, No. 4 (Dec. 1964), pp. 277-289.
- 8. I. I. Kolodner, "On a Generating Function Associated with Generalized Fibonacci Sequences," Fibonacci Quarterly, Vol. 3, No. 4 (Dec. 1965), pp. 272-278.
- 9. M. E. Waddill and Louis Sacks, "Another Generalized Fibonacci Sequence," Fibonacci Quarterly, Vol. 5, No. 3 (Oct. 1967), pp. 209-222.
- 10. C. H. King, "Conjugate Generalized Fibonacci Sequences," Fibonacci Quarterly, Vol. 6, No. 1 (Feb. 1968), pp. 46-49.
- 11. T. W. Cusick, "On a Certain IntegerAssociated with a Generalized Fibonacci Sequence," Fibonacci Quarterly, Vol. 6, No. 2 (Apr. 1968), pp. 117-126.
- 12. Leon Bernstein and Helmut Hasse, "Explicit Determination of the Perron Matrices in Periodic Algorithms of the Perron-Jacobi Type with Applications to Generalized Fibonacci Numbers with Time Impulse," Fibonacci Quarterly, Vol. 7, No. 4 (Nov. 1969), pp. 394-436.
- 13. Hyman Gabai, "Generalized Fibonacci k-Sequences," Fibonacci Quarterly, Vol. 8, No. 1 (Feb. 1970), pp. 31-38.
- 14. V. E. Hoggatt, Jr., Fibonacci and Lucas Numbers, Houghton Mifflin, 1969.

THE GOLDEN ELLIPSE

H. E. HUNTLEY

Nethercombe Cottage, Canada Combe, Hutton, Weston - Super - Mare, England

The ellipse in which the ratio of the major to the minor axis (a/b) is the golden ratio φ — the "divine proportion" of Renaissance mathematicians [1]—has interesting properties. In the figure, let OA = a = φ units, OB = b = 1 unit. Clearly, if a rectangle be circumscribed about the ellipse, having its sides parallel to the axes, it will be what has been called the golden rectangle, frequently realized in ancient Greek architecture.



The Golden Ellipse $a/b = \varphi$

The modern symbol for "golden section," as it was called in the nineteenth century, is the Greek letter phi: φ , and φ and φ' are the solutions of the equation $x^2 - x - 1 = 0$.

 φ = $(1 + \sqrt{5})/2$ = -1.6180 · · · ,

Feb. 1974

$$\varphi' = (1 - \sqrt{5})/2 = -0.6180 \cdots,$$

so that $\varphi + \varphi' = 1$ and $\varphi \varphi' = -1$.

Now, the eccentricity e of an ellipse is given by

$$b^2 = a^2(1 - e^2)$$

so that the eccentricity of the golden ellipse is

(1)
$$\mathbf{e} = 1/\sqrt{\varphi} = \sqrt{-\varphi'} \quad .$$

Using the familiar notation of the figure (e.g., S and S" are the foci), from the known properties of the ellipse, we may write the following equations:

(2) OS = ae =
$$\sqrt{\varphi}$$

(3)
$$BS = \sqrt{(b^2 + a^2 e^2)} = a = \varphi$$

If $\angle OBS = \theta$,
(4) $\sec \theta = a/b = \varphi$.

If ON is perpendicular to the directrix ND ,

(5)
$$ON = a/e = \varphi^{3/2}$$

(6) SN = ON - OS =
$$a/e$$
 - ae = $1/\sqrt{\varphi}$

A property of any ellipse may be stated thus: the minor axis is the geometric mean of the major axis and the latus rectum; that is, if L is the length of the semi-latus rectum, $aL - b^2$. Hence, for the golden ellipse,

.

(7)
$$L = b^2/a = 1/\varphi = -\varphi'$$
.

Thus

$$a:b:c = \varphi:1:-\varphi' = \varphi^2:\varphi:1$$
 .

From Eqs. (2), (5), and (6),

$$ON/OS = 1/e^2 = \varphi$$
 and $OS/SN = ae/(a/e - ae) = 1/\varphi = -\varphi'$.

Hence, the focus S divides ON in the Golden Ratio.

Again, if PP' is the latus rectum,

(8)
$$OP^2 = OS^2 + SP^2 = a^2e^2 + b^4/a^4 = \varphi + \varphi^{12} = 2$$
.

THE GOLDEN ELLIPSE

Using the cosine rule for $\triangle POP'$, it may be deduced from this that the latus rectum subtends at the center O an angle α given by $\cos \alpha = 1/\varphi$, so that, from (4),

$$(9) \qquad \qquad \alpha = \theta \ .$$

Another property of the ellipse has it that a tangent at P passes through N and that $\cot \angle SPN = e$. Since $\cot \theta = b/ae$, it follows in the case of the golden ellipse that

 $\cot \angle SPN = 1/\sqrt{\varphi}$ and $\cot \theta = 1/\sqrt{\varphi}$,

so that / SPN = θ . Thus, MPSB is a parallelogram, and

(10)
$$MP = BS = a = \varphi .$$

Moreover, since MP/PN and OS/SN = φ ,

(11)
$$PN = 1$$
 and $MN = \varphi + 1 = \varphi^2$,

and P divides MN in the Golden Ratio.

It is easily shown that $OM = \varphi$ so that M lies on the auxiliary circle of the ellipse and $\triangle POM$ is isosceles. Moreover, if OP produced intersects the directrix in D, ND = $b^2/ae^2 = 1$, BDNO is a rectangle, and P divides OD in the Golden Ratio.

The interested reader may, by searching, discover for himself many other hiding places where the Golden Ratio is lurking in this ellipse. For example, superimpose on this ellipse a second, similar ellipse, with center O but rotated through a right angle. Draw a common tangent cutting OY, OX in R, S respectively, to touch the ellipse in T_1 and T_2 . Examine the ratios of the several segments of RS.

Reference

1. H. E. Huntley, "The Golden Cuboid," <u>Fibonacci Quarterly</u>, Vol. 2, No. 3 (Oct. 1964), p. 184.

 \sim

ON A PROBLEM OF M. WARD

R. R. LAXTON University of Nottingham, Nottingham, England

1. INTRODUCTION

In [3] M. Ward showed that a general non-degenerate integral linear recurrence of order two has infinitely many distinct prime divisors. He conjectured that the result was true for linear recurrences of higher order (again excluding certain degenerate ones) and, indeed, confirmed this in [4] for the case of cubic recurrences. Here we prove Ward's conjecture; the method is straightforward and uses the most elementary form of p-adic analysis. We end by discussing the limitations of the method together with the problems it raises and posing further questions concerning divisors of recurrences (especially in connection with the work of K. Mahler).

2. STATEMENT OF THE PROBLEM

2.1. Let the polynomial $f(x) = x^m - a_{m-1}x^{m-1} - \cdots - a_1x - a_0 \in \mathbb{Z}[x]$, $m \ge 1$, have no root nor ratio of distinct roots a root of unity. Say

$$f(x) = \prod_{i=1}^{m} (x - \theta_i),$$

where the θ_i are algebraic integers. Put $\mathbb{K} = \mathbb{Q}(\theta_1, \dots, \theta_m)$; it is a normal extension of the rational field \mathbb{Q} .

 $W = \{w_0, w_1, \cdots, w_n, \cdots\}$ is a (integral) linear recurrence with companion polynomial f(x) if given $w_0, w_1, \cdots, w_{m-1} \in \mathbf{Z}$, not all zero, we have

$$w_{n+m} = a_{m-1}w_{n+m-1} + \cdots + a_1w_{n+1} + a_0w_n$$
,

for all non-negative integers n. Thus all the terms of W are rational integers.

2.2. We can assume that $a_0 \neq 0$ since otherwise we would have a linear recurrence of degree less than m.

All the roots $\theta_1, \dots, \theta_m$ are distinct, so we may write

(2.1)
$$Dw_n = A_1 \theta_1^n + \dots + A_m \theta_m^n$$

for all n, where the A_i are algebraic integers in K and the rational integer D is the discriminant of f(x).

and this we exclude. Hence we may assume that $A_1A_2 \cdots A_m \neq 0$ and $m \geq 2$ since otherwise we would use (2.1) but with the zero A_i 's deleted.

To make the exposition clear, we shall assume that f(x) splits in $\mathbf{Z}[x]$, i.e., that $\theta_1, \dots, \theta_m$ are rational integers. The following proof remains valid in general (with prime ideals replacing rational primes, etc.) apart from one step and this we shall deal with at the end of the present proof.

2.3. An integer n is a <u>divisor</u> of W if n divides some term w_m of W. We shall be concerned with prime divisors of W. If a prime p divides all the roots $\theta_1, \dots, \theta_m$ then p divides all the terms w_t of W with $t \ge m$; these divisors (which are called <u>null-divisors</u>) are of no interest to us and we eliminate them. Let $u = g. c. d. (\theta_1, \dots, \theta_m)$ and rewrite (2.1) as

$$D_{W_{n}} = u^{n} \left(A_{1} \left(\frac{\theta_{1}}{u} \right)^{n} + \cdots + A_{m} \left(\frac{\theta_{m}}{u} \right)^{n} \right)$$
$$= u^{n} \left(A_{1} \delta_{1}^{n} + \cdots + A_{m} \delta_{m}^{n} \right) ,$$

with $\delta_i = \theta_i / u$ for all $i = 1, \dots, m$. It follows that given any prime p, there is at least one δ_i which is not divisible by p. This fact we will need in the subsequent proof.

2.4. From now on we will assume that the recurrence W given by (2.1) has only a finite number of prime divisors. It follows from (2.2) that there are only a finite number of primes, say p_1, \dots, p_t , which are prime divisors of the integers $U_n = A_i \delta_1^n + \ldots + A_m \delta_m^n$ for all $n = 0, 1, 2, \dots$. Essentially we prove that this assumption implies that the terms U_n assume the <u>same</u> integer value for infinitely many distinct values of n.

3. THE ANALYSIS

3.1. Let $p = p_i$ be one of the primes p_1, \dots, p_t which divide some U_n . From the construction in 2.3, we know that some δ_i is not divisible by $p - say \ \delta_1, \dots, \delta_d$ (d = d(i) ≥ 1) are p-adic units and $\delta_{d+1}, \dots, \delta_m$ are divisible by p.

For the moment, we will assume that

(3.1)
$$A_1 \delta_1^n + \cdots + A_d \delta_d^n = 0$$

for only finitely many $n \in \mathbb{Z}$, $n \ge 0$

Let k = k(i) be such that $A_1\delta_1^k + \cdots + A_d\delta_d^k \neq 0$. Say $A_1\delta_1^k + \cdots + A_d\delta_d^k \equiv 0 \pmod{p^s}$ but $A_1\delta_1^k + \cdots + A_d\delta_d^k \neq 0 \pmod{p^{s+1}}$ for some integer $s = s(i) \geq 0$. For each $j = 1, \cdots, d$, there exists a positive integer b_j such that

$$\delta_j^{b_j} \equiv 1 \pmod{p^{s+1}}$$

Now put b = b(i) = $b_1b_2\cdots b_d.$ Then for each $r\in {\bf Z}$ such that v = k+rb > s, the rational integer

(2.2)

ON A PROBLEM OF M. WARD

$$U_{v} = A_{1}\delta_{1}^{v} + \dots + A_{m}\delta_{m}^{v} \equiv A_{1}\delta_{1}^{v} + \dots + A_{d}\delta_{d}^{v}$$
$$\equiv A_{1}\delta_{1}^{k} + \dots + A_{d}\delta_{d}^{k} \pmod{p^{s+1}}.$$

Thus for all v = k + rb > s, the terms U_v are exactly divisible by p^S.

3.2. Now repeat the argument of 3.1 for each of the primes p_1, \dots, p_t . It is clear that provided the assumption (3.1) holds for each of these primes, the value selected for k = k(i) can be chosen to be the same for all p_1, \dots, p_t . Assuming then that (3.1) holds for each p_i , $i = 1, \dots, t$, we have constructed a subsequence $U_{v(i)}$ of $\{U_n, n = 0, 1, \dots\}$ for all $r \in \mathbf{Z}$ with v(i) = k + rb(i) > s(i), all of whose terms are exactly divisible by $p^{s(i)}$.

Therefore for all $r \in \mathbf{Z}$ such that $v = k + rb(1)b(2) \cdots b(t) > max(s(1), \cdots, s(t))$, the infinite subsequence $\{U_v\}$ of $\{U_n\}$ takes on the form $\pm N$ for some fixed integer N (since the primes p_1, \cdots, p_t are the only prime divisors of terms of this sequence $\{U_n\}$ of rational integers).

3.3. Now both the derivation in 3.2 and the <u>denial</u> of assumption (3.1) for some prime among p_1, \dots, p_t give rise to statements of the form: $"A_1\delta_1^n + \dots + A_f\delta_f^n$ takes the same value for infinitely many $n \in \mathbb{Z}$, $n \ge 0$." Here A_i and δ_i are non-zero algebraic integers (actually we have assumed they are rational; see 2.2) and $f \ge 2$ ($f = m \ge 2$ for the derivation in 3.2 and for (3.1) to be false we must have $f = d(i) \ge 2$).

By p-adic methods (see for example K. Mahler's article [1]) we can conclude from this that some ratio δ_i / δ_j , $i \neq j$, is a root of unity and hence $\theta_i / \theta_j = u \delta_i / u \delta_j$ is a root of unity. This contradicts our initial hypothesis and so the assumption that the recurrence W has only finitely many prime divisors is false.

4. REMARK ON THE GENERALIZATION OF THE PROOF

We need consider the case when f(x) does not split in $\mathbb{Z}[x]$ and so $\theta_1, \dots, \theta_m$ are not rational integers but only algebraic integers. As we remarked in 2.2, we use prime ideals <u>p</u> of the normal extension **K** instead of rational primes p and <u>p</u>-adic analysis instead of p-adic analysis. This part of the generalization causes us no trouble but there is a slight difficulty in getting rid of the null-divisors of W in 2.3 and forming Eq. (2.2). There we put u = g. c. d. ($\theta_1, \dots, \theta_m$) and subsequently considered the sequence $U_n = A_1 \delta_1^n + \cdots + A_m \delta_m^n$ of rational integers — and the fact that the U_n are rational integers is important in Sec. 3.2 where we used the fact that the only units in the rationals are ±1 (and thereby deducing that we obtained an infinite subsequence $\{U_v\}$ of $\{U_n\}$ taking the values N for some fixed $N \in \mathbb{Z}$). To overcome this we let q_1, \dots, q_s be the set (possibly empty) of all rational primes dividing g. c. d. (a_0, \dots, a_{m-1}), the coefficients of f(x). In the normal extension $\mathbf{K} = \mathbf{Q}(\theta_1, \dots, \theta_m)$ let the ideal (q_i) have prime ideal decomposition

$$(\mathbf{q}_i) = (\underline{\mathbf{q}}_{i(1)} \cdots \underline{\mathbf{q}}_{i(r)})^{\alpha_i}, \quad \alpha_i \in \mathbf{Z}, \quad \alpha_i > 0$$

Now each prime ideal $\underline{q}_{i(k)}$ contains all $\theta_1, \dots, \theta_m$; let $\beta_{i(k)} > 1$ be the highest power of $\underline{q}_{i(k)}$ dividing all $\theta_1, \dots, \theta_m$. Since **K** is normal we have

1974]

Feb. 1974

$$\beta_{i(1)} = \beta_{i(2)} = \cdots = \beta_{i(r)} = \beta_{i}$$
,

say. We do this for all $i = 1, \dots, s$. Put $\alpha = \alpha_1 \alpha_2 \dots \alpha_s$ and then

$$\prod_{i,k} {\beta_i \choose \underline{q}_{i(k)}}^{\alpha} = (u) ,$$

where u is a rational integer.

Now instead of considering all terms w_n of W we consider only the subsequence $\{w_{_{OP}}\}$ and (2.2) then becomes

$$Dw_{\alpha n} = A_1 \theta_1^{\alpha n} + \cdots + A_m \theta_m^{\alpha n} = u^n (A_1 \delta_1^n + \cdots + A_m \delta_m^n)$$
,

with $\delta_i = \theta_i^{\alpha} / u$ for all $i = 1, \dots, m$. Here $\{A_1 \delta_1^n + \dots + A_m \delta_m^n\}$ is a sequence of rational integer terms and for any prime <u>p</u> at least one δ_i is a <u>p</u>-adic integer. The analysis can now proceed as previously.

5. PROBLEMS CONCERNING FURTHER GENERALIZATIONS

5.1. One would suppose that the result established here can be generalized to arbitrary linear recurrences, not just those W all of whose terms are integers. However, our method of proof breaks down in this general situation since in Sec. 3.2, we needed the fact that there are only a finite number of units in \mathbf{Z}

5.2. In [2], K. Mahler has shown (using the p-adic generalization of Roth's Theorem) that in a non-degenerate linear recurrence of order two (with c. p. $x^2 - Px + Q$, $4p > Q^2$ and $Q \ge 2$) every infinite <u>subsequence</u> has an infinite number of prime divisors. Again one would suppose that this is true for linear recurrences of higher order.

5.3. Let $f(x) = x^2 - Px + Q \in \mathbb{Z}[x]$, $Q \neq 0$, and $W = \{\dots, w_0, w_1, \dots, w_n, \dots\}$ $w_0, w_1 \in \mathbb{Z}$ be a linear recurrence satisfying $w_{n+2} = Pw_{n+1} - Qw_n$, for all $n \in \mathbb{Z}$ (we are allowing the recurrence to go in both directions so that now not all terms are integers). Then one can establish that if every prime is a divisor of W and $Q = \pm 1$, then some term of W is 0 and so it is essentially the Lucas sequence \dots , 0, 1, P, \dots associated with f(x). Is this result true for arbitrary Q?

REFERENCES

- 1. K. Mahler, "Eine arithmetische Eigenshaft der Taylor koeffizienten rationaler Funktionen," Proc. Amsterdam Acad., 38 (1935), pp. 50-60.
- 2. K. Mahler, "A Remark on Recursive Sequences," J. Indian Math. Soc. (Dehli) 1.
- M. Ward, "Prime Divisors of Second-Order Recurring Sequences," <u>Duke Math. J.</u>, 21 (1954), pp. 607-614.
- 4. M. Ward, "The Laws of Apparition and Repetition of Primes in a Cubic Recurrence," Trans. Amer. Math. Soc., 79 (1955), pp. 72-90.

◇◆◇◆

GENERALIZED HIDDEN HEXAGON SQUARES

A. K. GUPTA The University of Michigan, Ann Arbor, Michigan 48104

The triangular array of binomial coefficients is well known. Recently, Hoggatt and Hansel [2] have obtained a very surprising result involving these numbers. Stanton and Cowan [3] and Gupta [1] have generalized this triangular array to a tableau. In this paper, we generalize the results due to Hoggatt and Hansel.

Let, for any positive integer m and any integer n, $\binom{m}{n} = 0$ if either $n \ge m$ or n < 0. Then we prove the following theorem.

<u>Theorem</u>. The product of the six binomial coefficients spaced around $\binom{m}{n}$, viz.,

$$\binom{m - r_1}{n - r_2}\binom{m - r_1}{n}\binom{m}{n - r_2}\binom{m + r_2}{n + r_1}\binom{m + r_2}{n}\binom{m + r_1}{n}\binom{m}{n + r_1},$$

where r_1 and r_2 are positive integers, is a perfect integer square.

Proof. The product of the six binomial coefficients is

$$\frac{(m - r_1)!}{(n - r_2)!(m - r_1 - n + r_2)!} \cdot \frac{(m - r_1)!}{(n)!(m - r_1 - n)!} \cdot \frac{(m)!}{(m - r_2)!(m - n + r_2)!} \cdots \\ = \left[\frac{(m - r_1)!(m)!(m + r_2)!}{(n - r_2)!(m - r_1 - n + r_2)!(n)!(m - r_1 - n)!(m - n + r_2)!(n + r_1)!} \right]^2 .$$

Now, the product of binomial coefficients is an integer, since each binomial coefficient is an integer. And the square of a rational number is an integer if and only if the rational number is an integer. Hence the product is an integer square.

It is interesting to note that

$$\binom{m}{n-r_2}\binom{m-r_1}{n}\binom{m+r_2}{n+r_1} = \binom{m-r_1}{n-r_2}\binom{m+r_2}{n}\binom{m}{n+r_1},$$

which is what really happens to make the product of six numbers a perfect square.

<u>Corollary 1</u>. If $r_1 = r_2$, we get the product of six binomial coefficients which are

equally spaced around $\begin{pmatrix} m \\ n \end{pmatrix}$. <u>Corollary 2</u>. If $r_1 = r_2 = 1$, we get the product of six binomial coefficients that surround $\begin{pmatrix} m \\ n \end{pmatrix}$. This is the result of Hoggatt and Hansel [2]. Hence their result is a very special case of our general theorem.

By taking different values for r_1 and r_2 , we can obtain several configurations which yield products of binomial coefficients which are squares. In fact, one can build up a long serpentine configuration, or snowflake curves, as noted by Hoggatt and Hansel.

Note that the theorem holds for generalized binomial coefficients (and hence for q-binomials), and in particular for the Fibonomial coefficients.

REFERENCES

- 1. A. K. Gupta, "On a 'Square' Functional Equation," unpublished.
- V. E. Hoggatt, Jr., and Walter Hansel, "The Hidden Hexagon Squares," <u>Fibonacci Quar-terly</u>, Vol. 9, No. 2 (April, 1971), pp. 120 and 133.
- R. G. Stanton and D. D. Cowan, "Note on a 'Square' Functional Equation," <u>Siam Review</u>, Vol. 12 (1970), pp. 277-279.

LETTER TO THE EDITOR

Dear Editor:

Here are two related problems for the <u>Fibonacci Quarterly</u>, based on some remarkable things discovered last week by Ellen Crawford (a student of mine).

<u>Problem 1.</u> Prove that if m and n are any positive integers, there exists a solution x to the congruence

$$F_{v} \equiv m \pmod{3^{n}}$$
.

Solution. Let m be fixed: we shall show that it is possible to solve the simultaneous congruences

$$F_{x} \equiv m \pmod{3^{n}}$$
$$F_{x} + F_{x+1} \neq 0 \pmod{3}$$

(*)

This is clearly true for n = 1. It is also easy to prove by induction, using

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$$
,

(Continued on page 79.)

DIAGONAL SUMS OF THE TRINOMIAL TRIANGLE

V. E. HOGGATT, JR., and MARJORIE BICKNELL San Jose State University, San Jose, California 95192

In an earlier paper [1], a method was given for finding the sum of terms along any rising diagonals in any polynomial coefficient array, given by

$$(1 + x + x^{2} + \cdots + x^{r-1})^{n}$$
, $n = 0, 1, 2, \cdots, r \ge 2$,

which sums generalized the numbers u(n; p,q) of Harris and Styles [2], [3]. In this paper, an explicit solution of the general case for the trinomial triangle is derived.

If we write only the coefficients appearing in the expansions of the trinomial $(1 + x + x^2)^n$, we have

| 1 | | | | | | | | | | |
|---|----------|----|----------|----|----|----|----|----|---|---|
| 1 | 1 | 1 | | | | | | | | |
| 1 | 2 | 3 | 2 | 1 | | | | | | |
| 1 | 3 | 6 | 7 | 6 | 3 | 1 | | | | |
| 1 | 4 | 10 | 16 | 19 | 16 | 10 | 4 | 1 | | |
| 1 | 5 | 15 | 30 | 45 | 51 | 45 | 30 | 15 | 5 | 1 |
| | | | | | | | | | | |

Call the top row the zeroth row and the left-most column the zeroth column. Then, the column generating functions are

(1)
$$G_0 = \frac{1}{1-x}, \quad G_1 = \frac{x}{(1-x)^2}, \quad G_2 = \frac{x}{(1-x)^3}$$
$$G_{n+2} = \frac{x}{1-x} (G_{n+1} + G_n), \quad n \ge 0.$$

We desire to find the sums u(n; p,q) which are the sums of those elements found by beginning in the zeroth column and the nth row and taking steps p units up and q units right throughout the left-justified trinomial triangle. Let

(2)
$$G = \sum_{n=0}^{\infty} x^{np} G_{nq} = \sum_{n=0}^{\infty} u(n; p, q) x^{n}$$

Our first problem is to find a recurrence for every $q^{\mbox{th}}$ column generator. We need two sequences,

(3)
$$P_n(x) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad Q_n(x) = \alpha^n + \beta^n$$

Both $P_n(x)$ and $Q_n(x)$ obey

$$u_{n+2}(x) = \frac{x}{1-x} (u_{n+1}(x) + u_n(x))$$
.

So let

$$A = \frac{x}{1 - x};$$

then

(4)

$$P_{n+2}(x) = A(P_{n+1}(x) + P_n(x))$$

$$Q_{n+2}(x) = A(Q_{n+1}(x) + Q_n(x))$$

$$\alpha^{n+2} = A(\alpha^{n+1} + \alpha^n)$$

$$\beta^{n+2} = A(\beta^{n+1} + \beta^n)$$

Next, we list the first few members of $P_n(x)$ and $Q_n(x)$.

| n | $P_n(x)$ | Q _n (x) |
|----------|---------------------|------------------------------------|
| 0 | 0 | 2 |
| 1 | 1 | А |
| 2 | А | $A^2 + 2A$ |
| 3 | $A^2 + A$ | $A^3 + 3A^2$ |
| 4 | $A^{3} + 2A^{2}$ | $A^4 + 4A^3 + 2A^2$ |
| 5 | $A^4 + 3A^3 + A^2$ | $A^5 + 5A^4 + 5A^3$ |
| 6 | $A^5 + 4A^4 + 3A^3$ | $A^{6} + 6A^{5} + 9A^{4} + 2A^{3}$ |
| | ••• | |

Note that the coefficients of $Q_n(x)$ are simply the terms appearing on rising diagonals of the Lucas triangle [4]. The coefficients of $P_n(x)$ and $Q_n(x)$ are the same as those of the Fibonacci and Lucas polynomials, and $P_n(1) = F_n$, $Q_n(1) = L_n$, the nth Fibonacci and Lucas number, respectively.

By mathematical induction, it is easy to show that

(5)
$$Q_n(x) = P_{n+1}(x) + AP_{n-1}(x)$$

Then, the general recurrence for the k^{th} terms is

1974] DIAGONAL SUMS OF THE TRINOMIAL TRIANGLE

(6)
$$u_{k(n+2)}(x) = Q_{k}(x) u_{k(n+1)}(x) + (-1)^{k+1} A^{k} u_{kn}(x)$$

Then, a recurrence relation for every $\,q^{{\rm th}}\,$ column generator is

(7)
$$G_{q(n+2)}(x) = Q_{q}(x)G_{q(n+1)}(x) + (-1)^{q+1}A^{q}G_{qn}(x)$$

In summing elements to find u(n; p,q) from the column generators, we need to multiply the column generators by powers of x so that the coefficients summed lie along the chosen diagonals of the trinomial array. Then

(8)
$$G_{q(n+2)}^{*}(x) = x^{p}Q_{q}(x)G_{q(n+1)}^{*}(x) + x^{2p}(-1)^{q+1}A^{q}G_{qn}^{*}(x) + G_{q}^{*}(x) = \frac{1}{1 - x}, \qquad G_{q}^{*}(x) = x^{p}G_{q}(x)$$

Let

$$\mathbf{G}_{n} = \sum_{i=0}^{n} \mathbf{G}_{iq}^{*}$$

and

$$\lim_{n \to \infty} G_n = G$$
,

the generating function for the numbers u(n; p,q). We next sum Eq. (8),

$$\sum_{i=0}^{n} G_{q(i+2)}^{*}(x) = \sum_{i=0}^{n} x^{p} Q_{q}(x) G_{q(i+1)}^{*}(x) + \sum_{i=0}^{n} x^{2p} (-1)^{q+1} A^{q} G_{qi}^{*}(x) ,$$

which becomes, upon expansion,

$$\begin{split} & \operatorname{G}_n \ - \ \operatorname{G}_q^*(x) \ - \ \operatorname{G}_0^*(x) \ + \ \operatorname{G}_{(n+1)q}^*(x) \ + \ \operatorname{G}_{(n+2)q}^*(x) \\ & = \ x^p \operatorname{Q}_q(x) \operatorname{G}_{(n+1)q}^*(x) \ + \ x^p \operatorname{Q}_q(x) \operatorname{G}_n \ - \ x^p \operatorname{Q}_q(x) \operatorname{G}_0^*(x) \\ & \quad + \ x^{2p} (-1)^{q+1} \operatorname{A}^q \operatorname{G}_n \ . \end{split}$$

Collecting terms, our sum simplifies to

$$G_{n}(1 - x^{p}Q_{q}(x) - x^{2p}(-1)^{q+1}A^{q}) = G_{0}^{*}(x)(1 - x^{p}Q_{q}(x)) + G_{q}^{*}(x) + R_{n},$$

where R_n involves only terms involving $G^*_{(n+1)q}(x)$ and $G^*_{(n+2)q}(x)$. It can be shown that

$$\lim_{n \to \infty} G_n^*(x) = 0$$

49

for |x| < 1/r, r > 2, so that $\lim_{n \to \infty} R_n = 0$. Then, taking the limit as $n \to \infty$ of our sum and simplifying,

$$G = \frac{G_0^*(x)(1 - x^p Q_q(x)) + G_q^*(x)}{1 - x^p Q_q(x) + x^{2p} (-A)^q}$$

which becomes Eq. (9) from the identity given in Eq. (8):

(9)
$$G = \frac{G_0(x)(1 - x^p Q_q(x)) + x^p G_q(x)}{1 - x^p Q_q(x) + x^{2p}(-A)^q} = \sum_{n=0}^{\infty} u(n; p, q) x^n ,$$

where $G_n(x)$ is defined by Eq. (1), $A = \frac{x}{1-x}$, and

(10)
$$Q_{k}(x) = \sum_{i=0}^{\left[\binom{k+1}{2}\right]} \left[\binom{k-i}{i} + \binom{k-i-1}{i-1}\right] A^{k-i} .$$

REFERENCES

- 1. V. E Hoggatt, Jr., and Marjorie Bicknell, "Diagonal Sums of Generalized Pascal Triangles," Fibonacci Quarterly, Vol. 7, No. 4, Nov. 1969, pp. 341-358.
- V. C. Harris and Carolyn C. Styles, "A Generalization of Fibonacci Numbers," <u>Fibonacci</u> <u>Quarterly</u>, Vol. 2, No. 4, Dec. 1964, pp. 277-289.
- V. C. Harris and Carolyn C. Styles, "Generalized Fibonacci Sequences Associated with a Generalized Pascal Triangle," <u>Fibonacci Quarterly</u>, Vol. 4, No. 3, Oct. 1966, pp. 241-248.
- Verner E. Hoggatt, Jr., "An Application of the Lucas Triangle," <u>Fibonacci Quarterly</u>, Vol. 8, No. 4, Oct. 1970, pp. 360-364.

FIBONACCI SEQUENCES MODULO M

AGNES ANDREASSIAN American University of Bierut, Bierut, Lebanon

Most of the questions concerning the length of the period of the recurring sequence obtained by reducing a general Fibonacci sequence by a modulus m have been answered by D. D. Wall [1]. The problem discussed in this paper is to determine the number of ordered pairs (a, b) with $0 \le a \le m$ and $0 \le b \le m$ that produce these various possible lengths.

The results that have been used in this study are summarized below. The proofs of these theorems are omitted here except for "Theorem 12" whose proof in [1] is incorrect. The outline of a correct proof of "Theorem 12" was proposed by D. D. Wall in answer to a letter sent to him asking for clarification.

SUMMARY OF KNOWN RESULTS

Using the notation in [1], let f_n denote the n^{th} term of the Fibonacci sequence where $f_0 = a$, $f_1 = b$, and $f_{n+1} = f_n + f_{n-1}$. Let h = h(a, b, m) denote the length of the period of this sequence when it is reduced modulo m, taking least non-negative residues. When h does not depend on a and b we may write h = h(m) instead. The special Fibonacci sequence which starts with the pair (0, 1) will be denoted by $\{u_n\}$ and its period when reduced modulo m by k(m). The sequence which starts with (2, 1) will be denoted by $\{v_n\}$. The letter p will be used to denote a prime and e a positive integer. In studying the possible values of h(a, b, m) we may assume, without any loss of generality, that (a, b, m) = 1.

1. If

$$m = \Pi^{e_{i}}_{p_{i}}$$
 and $h\left(a, b, p_{i}^{e_{i}}\right) = h_{i}$,

then $h(a, b, m) = LCM[h_i]$ [1, Theorem 2].

2. If t is the largest integer such that $k(p^t) = k(p)$ then $k(p^e) = p^{e-t}k(p)$ for $e \ge t$ [1, Theorem 5].

<u>Remark.</u> The proof of this theorem as given in [1] is rather incomplete. It is possible to give a complete proof by using induction on e as suggested, but a much neater proof for the case when p is an odd prime is given by Robinson [2], by the use of matrix algebra.

For p = 2, Robinson's proof that $k(p^{e+1})$ is either $k(p^e)$ or $pk(p^e)$ still holds, and the proof that shows that if $k(p^{e+1}) = pk(p^e)$, then $k(p^{e+2}) = pk(p^{e+1})$ is still applicable for e > 1. The case p = 2 and e = 1 is verified by direct computations since we have k(2) = 3, $k(2^2) = 6$, and $k(2^3) = 12$.

In particular, if $k(p^2) \neq k(p)$, we obtain $k(p^e) = p^{e-1}k(p)$. In [3] Mamangakis has shown that (1) if c and p are relatively prime and cp occurs in $\{u_n\}$, then $k(p^2) \neq k(p)$,

and (2) if c and p are relatively prime, $e \leq d$, and $u_j = cp^d$ is the first multiple of p to occur in $\{u_n\}$, then $k(p^e) = k(p)$ if and only if u_{j-1} has the same order mod p and mod p^e . For all p up to 10,000 it has been shown that $k(p^2) \neq k(p)$. However, it has not yet been proved that $k(p^2) = k(p)$ is impossible.

3. If m > 2, then k(m) is even [1, Theorem 4].

4. If $(b^2 - ab - a^2, p^e) = 1$, then $h(p^e) = k(p^e)$ [1, Corollary to Theorem 8].

5. If $p \equiv \pm 3 \pmod{10}$, then $h(p^e) = k(p^e)$ [1, Theorem 8].

6. $h(2^e) = k(2^e)$ [1, Theorem 9].

7. If $b^2 - ab - a^2 \neq 0 \pmod{5}$, then $h(5^e) = k(5^e)$; and if $b^2 - ab - a^2 \equiv 0 \pmod{5}$, then $h(5^e) = (1/5)k(5^e) [1, \text{ Theorem 9}].$

8. If $m = p^e$, p > 2, and if there is a pair (a,b) which gives $h(a,b,p^e) = 2t + 1$, then $k(p^e) = 4t + 2$ [1, Theorem 10].

9. If $m = p^e$, $p \ge 2$, and if $k(p^e) = 4t + 2$ then $h(a,b,p^e) = 2t + 1$ for some pair (a,b) [1, Theorem 11].

10. If $m = p^e$, $p \ge 2$, $p \ne 5$, and h is even, then $h(p^e) = k(p^e)$ [1, Theorem 12]. <u>Proof.</u> Since $f_h = u_{h-1}a + u_hb$, we have

(1)
$$f_h - a = bu_h + a(u_{h-1} - 1) \equiv 0 \pmod{p^e}$$
;
(2) $f_{h+1} - b = b(u_{h+1} - 1) + au_h \equiv 0 \pmod{p^e}$.

Since we are assuming that $(a,b,p^e) = 1$, considering a and b as the unknowns, the determinant must be zero. Hence $u_h^2 - (u_{h+1} - 1)(u_{h-1} - 1) \equiv 0 \pmod{p^e}$. But it is known that $u_h^2 - u_{h+1}u_{h-1} = (-1)^{h-1}$, and so $u_{h+1} + u_{h-1} \equiv 1 + (-1)^h \pmod{p^e}$. Since h is even and $u_{h+1} = u_h + u_{h-1}$, this gives $2u_{h-1} + u_h \equiv 2 \pmod{p^e}$, or $u_h \equiv 2(1 - u_{h-1}) \pmod{p^e}$. It has been shown that if $b^2 - ab - a^2 \not\equiv 0 \pmod{p}$ we obtain the unique solution $u_h \equiv 0$ and $u_{h-1} \equiv 1 \pmod{p^e}$, and so $h(p^e) = k(p^e)$. Next consider the cases for which $b^2 - ab - a^2 \equiv 0 \pmod{p}$. Since $u_h \equiv 2(1 - u_{h-1}) \pmod{p^e}$, substituting in (1) we obtain

$$2b(1 - u_{h-1}) + a(u_{h-1} - 1) \equiv 0 \pmod{p^e}$$
, or $(2b - a)(1 - u_{h-1}) \equiv 0 \pmod{p^e}$.

We will show that $(2b - a, p^e) = 1$. The condition $b^2 - ab - a^2 \equiv 0 \pmod{p}$ can be written in the equivalent form $(2b - a)^2 \equiv 5a^2 \pmod{p}$. Now if $p \mid (2b - a)$, then $p \mid 5a^2$; but $p \neq 5$, hence $p \mid a$. Therefore $p \mid 2b$, and since $p \geq 2$, $p \mid b$. Thus $(a, b, p^e) \neq 1$ contrary to assumption. Hence $p \nmid (2b - a)$, and so we may cancel 2b - a from the above congruence obtaining $1 - u_{h-1} \equiv 0 \pmod{p^e}$, or $u_{h-1} \equiv 1 \pmod{p^e}$. Since $u_h \equiv 2(1 - u_{h-1}) \pmod{p^e}$, this implies that $u_h \equiv 0 \pmod{p^e}$, and so again $h(p^e) = k(p^e)$.

11. If h(a, b, p) = k(p), then $h(a, b, p^{e}) = k(p^{e})$ [1, Corollary 2 to Theorem 12].

12. Let f(m) denote the smallest positive integer, n, for which $u_n \equiv 0 \pmod{m}$, and let p be an odd prime. If 2/f(p), then $k(p^e) = 4f(p^e)$ [4].

FIBONACCI SEQUENCES MODULO M

THE PROBLEM

For any given modulus m, there are m^2 possible ordered pairs in sequence. Of these m^2 ordered pairs we would like to determine the number of pairs corresponding to each of the various possible lengths for that modulus. For example, if m = 7 we obtain

| . (| 0, | 0, | ••• | • | | | | | | | | | | | | | | | | length | 1 | (1 pair) |
|-----|----|----|-----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|-----|--------|----|------------|
| (| 0, | 1, | 1, | 2, | 3, | 5, | 1, | 6, | 0, | 6, | 6, | 5, | 4, | 2, | 6, | 1, | 0, | • | • • | length | 16 | (16 pairs) |
| (| 0, | 2, | 2, | 4, | 6, | 3, | 2, | 5, | 0, | 5, | 5, | 3, | 1, | 4, | 5, | 2, | 0, | • | •• | length | 16 | (16 pairs) |
| (| 0, | 3, | 3, | 6, | 2, | 1, | 3, | 4, | 0, | 4, | 4, | 1, | 5, | 6, | 4, | з, | 0, | • | •• | length | 16 | (16 pairs) |

Hence 1 pair produces a sequence of length 1 and 48 pairs produce sequences of length 16. Viewing these as infinite sequences extending to the right as well as to the left, some of these sequences become indistinguishable. Thus instead of number of pairs it is convenient to talk about number of distinct sequences of a given length. In the above example, there is 1 distinct sequence of length 1 and there are 3 distinct sequences of length 16.

Let n(h,m) denote the number of distinct sequences of length h when the sequence is reduced mod m. This will be abbreviated to n(h) when it is clear what modulus is used. Thus the problem is to determine the values of n(h) corresponding to the various possible values of h for any given modulus m.

Since the results summarized from [1] hold when $(a,b,p^e) = 1$, we must consider what happens when $(a,b,p^e) \neq 1$. When m = p, there is only one pair, namely (0,0), with $(a,b,p) \neq 1$ and it produces a sequence of length 1. When $m = p^2$, then sequences for which $(a,b,p^e) = 1$ are all the sequences for mod p multiplied throughout by p. When $m = p^3$, the sequences for which $(a,b,p^3) \neq 1$ are all the sequences for mod p^2 multiplied throughout by p. Thus, in general when $m = p^e$ we can trace back all the sequences except the one arising from (0,0) to pairs for mod p^e , p^{e-1} , p^{e-2} , ..., p where the condition of being relatively prime holds. The pair (0,0) will always have length 1 no matter what the modulus is.

We shall henceforth abbreviate k(p) as k.

<u>Theorem 1.</u> Let $m = p^e$ where p = 2 or $p \equiv \pm 3 \pmod{10}$. If $k(p^2) \neq k(p)$ then n(1) = 1 and

$$n(p^{i}k) = \frac{p^{i}(p^{2} - 1)}{k}$$

for $i = 0, 1, \dots, e - 1$.

<u>Proof.</u> By 5 and 6, if p = 2 or $p \equiv \pm 3 \pmod{10}$ and if $(a, b, p^e) = 1$, then $h(a, b, p^e) = k(p^e)$. If $(a, b, p^e) \neq 1$, then we still have $h(a, b, p^e) | k(p^e)$. Since $k(p^e) = p^{e-1}k$, the possible values of $h(a, b, p^e)$ are 1, k, pk, p^{2k} , \cdots , $p^{e-1}k$. We know that there is always

1974]

one sequence of length 1, namely when a = 0 and b = 0. Thus n(1) = 1. We will show that all of the $n(p^{e-1}k)$ sequences come from cases where $(a,b,p^e) = 1$. We know that the sequences for which $(a,b,p^e) \neq 1$ are the same sequences as for mod p^{e-1} multiplied throughout by p, and these sequences have the same lengths as the corresponding sequences for mod p^{e-1} . Since none of the sequences for mod p^{e-1} has a length greater than $k(p^{e-1})$ $= p^{e-2}k$, no sequence for which $(a, b, p^e) \neq 1$ can have a length of $p^{e-1}k$. Moreover, all the sequences for which $(a, b, p^e) = 1$ have lengths of $p^{e-1}k$ and so are included in $n(p^{e-1}k)$.

Since $\sum n(h_i) \cdot h_i = m^2$ where h_i are the different possible lengths, we must have

$$1 + \sum_{i=0}^{e-1} n(p^{i}k) \cdot p^{i}k = p^{2e}$$

and

$$1 + \sum_{i=0}^{e-2} n(p^i k) \cdot p^i k = p^{2e-2} .$$

Subtracting we obtain

$$n(p^{e-1}k) \cdot p^{e-1}k = p^{2e-2}(p^2 - 1)$$

and so

$$n(p^{e-1}k) = \frac{p^{e-1}(p^2 - 1)}{k}$$

Now since $n(p^{e-2}k)$, $n(p^{e-3}k)$, \cdots , $n(p^0k)$ represent the numbers of the sequences for which (a, b, p^e) $\neq 1$, they correspond to the sequences for mod p^{e-1} . But for mod p^{e-1} , the sequences that have lengths of $p^{e-2}k$ are those for which (a', b', p^{e-1}) = 1 where a = pa' and b = pb'. The number of these sequences gives $n(p^{e-2}k)$. Hence we may use the formula derived above and obtain

$$n(p^{e-2}k) = \frac{p^{e-2}(p^2 - 1)}{k}$$

Thus in general for mod p^e we have

$$n(p^{i}k) = \frac{p^{i}(p^{2} - 1)}{k}$$

for $i = 0, 1, \dots, e - 1$.

Since k(2) = 3 and $k(2^2) \neq k(2)$ we have:

Corollary. For mod 2^e , n(1) = 1 and $n(3 \cdot 2^i) = 2^i$ for $i = 0, 1, \dots, e-1$.

<u>Theorem 1'</u>. Let $m = p^e$ where $p \equiv \pm 3 \pmod{10}$. If t is the largest integer such that $k(p^t) = k(p)$ with $t \ge 1$, then (1) for $e \le t$, n(1) = 1 and

$$n(k) = \frac{p^{2e} - 1}{k}$$

,

and (2) for e > t, n(1) = 1,

$$n(k) = \frac{p^{2t} - 1}{k}$$
, and $n(p^{i-t+1}k) = \frac{p^{i+t-1}(p^2 - 1)}{k}$

for $i = t, \cdots, e - 1$.

Proof.

(1) For $e \le t$, $k(p^e) = k(p)$ and so all the sequences except the (0,0) sequence have length k. Since $\sum h_i n(h_i) = p^{2e}$ this means

$$n(k) = \frac{p^{2e} - 1}{k}$$
.

(2) For e > t, the possible lengths are 1, k, pk, \cdots , $p^{e-t}k$. Since all the lengths of the sequences for mod p^e can be identified as the lengths for mod p^e , p^{e-1} , \cdots , p, p^0 where (a, b, m) = 1, we have:

For mod p^0 , n(1) = 1. For mod p, n(1) = 1 and $n(k) = (p^2 - 1)/k$. For mod p^t , n(1) = 1 and $n(k) = (p^{2t} - 1)/k$. For mod p^{t+1} , n(1) = 1, $n(k) = (p^{2t} - 1)/k$, and $n(pk) = (p^{2t+2} - p^{2t})/pk = (p^{2t-1}(p^2 - 1))/k$. For mod p^{t+2} , n(1) = 1, $n(k) = (p^{2t} - 1)/k$,

$$n(pk) = \frac{p^{2t-1}(p^2 - 1)}{k}$$
 and $n(p^2k) = \frac{p^{2t+4} - p^{2t+2}}{p^2k} = \frac{p^{2t}(p^2 - 1)}{k}$.

. . .

Therefore, for mod p^e , n(1) = 1, $n(k) = (p^{2t} - 1)/k$, and

1974]

<u>Theorem 2.</u> If $m = 5^{e}$, then n(1) = 1, n(4) = 1, $n(4 \cdot 5^{i}) = 6 \cdot 5^{i-1}$ for $i = 1, \dots, e - 1$, and $n(4 \cdot 5^{e}) = 5^{e-1}$.

<u>Proof.</u> We always have n(1) = 1. With the assumption that $(a, b, 5^e) = 1$ we know by 7 that if $(b^2 - ab - a^2, 5) = 1$ then $h(5^e) = k(5^e)$, and if $(b^2 - ab - a^2, 5) \neq 5$ then $h(5^e) = (1/5)k(5^e)$.

It can be shown that the assumption $(a, b, 5^e) = 1$ is superfluous in the first case because if $(a, b, 5^e) \neq 1$, then 5|a and 5|b; hence $5|(b^2 - ab - a^2)$ contradicting $(b^2 - ab - a^2, 5) = 1$. Thus, if $(b^2 - ab - a^2, 5) = 1$, then $(a, b, 5^e) = 1$.

In general, we know that there are $p^{2e} - p^{2e-2}$ pairs (a,b) with $(a,b,p^e) = 1$. We wish to determine how many of these $5^{2e} - 5^{2e-2}$ pairs give $(b^2 - ab - a^2, 5) = 5$. This is equivalent to $b^2 - ab - a^2 \equiv 0 \pmod{5}$, or $(2a + b)^2 \equiv 5b^2 \pmod{5}$, or $(2a + b) \equiv 0 \pmod{5}$. Hence $b \equiv -2a \pmod{5}$, or $b \equiv 3a \pmod{5}$. Thus if $(a, b, 5^e) = 1$ and

$$(b^2 - ab - a^2, 5) = 5,$$

a can take $5^{e} - 5^{e-1}$ different values and corresponding to each value of a, b can have 5^{e-1} values. Therefore, there will be $5^{e-1}(5^{e} - 5^{e-1}) = 4 \cdot 5^{2e-2}$ such pairs (a,b). Since the total number of pairs (a,b) for which $(a,b,5^{e}) = 1$ is $5^{2e} - 5^{2e-2}$ and all the cases for which $(b^{2} - ab - a^{2}, 5) = 1$ arise from these, the number of pairs (a,b) such that $(b^{2} - ab - a^{2}, 5) = 1$ is given by $5^{2e} - 5^{2e-2} - 4 \cdot 5^{2e-1} = 4 \cdot 5^{2e-1}$. This is the number of pairs that produce sequences of length $k(5^{e})$. Since k = k(5) = 20, $k(5^{e}) = 5^{e-1}k = 4 \cdot 5^{e}$ and so

$$n(4.5^{e}) = \frac{4.5^{2e-1}}{4.5^{e}} = 5^{e-1}$$
.

We have $4 \cdot 5^{2e-2}$ pairs with (a, b, 5^e) = 1 producing sequences of length $\frac{1}{5}k(5^e) = 4 \cdot 5^{e-1}$. There are also the cases for which (a, b, 5^e) $\neq 1$. But there are the sequences for mod 5^{e-1} multiplied throughout by 5. Since $k(5^{e-1}) = 4 \cdot 5^{e-1}$ the number of pairs that produce sequences of length $4 \cdot 5^{e-1}$ is given by $4 \cdot 5^{2e-2} + 4 \cdot 5^{2(e-1)-1}$ and so

$$n(4 \cdot 5^{e-1}) = \frac{4 \cdot 5^{2e-2} + 4 \cdot 5^{2e-3}}{4 \cdot 5^{e-1}} = 6 \cdot 5^{e-2}$$

We have $\frac{1}{5}k(5^{i+1}) = k(5^i) = 4 \cdot 5^i$ for $i = 1, 2, \dots, e-1$ and so

$$n(4\cdot5^{i}) = \frac{4\cdot5^{2(i+1)-2} + 4\cdot5^{2(i+1)-3}}{4\cdot5^{i}} = 6\cdot5^{i-1}$$

[Feb.

57

for $i = 1, 2, \dots, e - 1$. In addition to these there are the pairs that produce sequences of length $\frac{1}{5}k(5) = 4$. The number of such pairs is $4 \cdot 5^{2e-2}$, where e = 1. Hence,

$$n(4) = (4.5^{\circ})/4 = 1$$
.

Theorem 3. Let $m = p^e$ where $p \equiv \pm 1 \pmod{10}$. If $k(p^2) \neq k(p)$ then (1) If 4|k, n(1) = 1 and

$$n(p^{i}k) = \frac{p^{i}(p^{2} - 1)}{k}$$

for $i = 0, 1, \dots, e - 1$ and (2) if 4/k, n(1) = 1,

$$n(p^{i}k/2) = \frac{2(p-1)}{k}$$

and

$$n(p^{i}k) = \frac{(p-1)(p^{i+1}+p^{i}-1)}{k}$$

for $i = 0, 1, \dots, e - 1$.

<u>Proof.</u> By 3, $k(p^e)$ is even, and so it is either of the form 4t or of the form 4t + 2. (1) If $k(p^e) = 4t$, by 8, $h(p^e)$ cannot be odd; and if h is even then by 10, $h(p^e) = k(p^e)$. Thus on condition (a, b, p^e) = 1, $h(p^e) = k(p^e) = p^{e-1}k$, and so the proof of Theorem 1 is applicable here. We also note that the condition $4|k(p^e)|$ is equivalent to that of 4|k| since $k(p^e) = p^{e-1}k$ and $2/p^{e-1}$.

(2) If $k(p^{e}) = 4t + 2$, by 9 $h(p^{e}) = 2t + 1$ for some (a,b). By 4 if $(b^{2} - ab - a^{2}, p^{e}) = 1$, then $h(p^{e}) = k(p^{e})$. Now consider $(b^{2} - ab - a^{2}, p^{e}) \neq 1$; if $h(a, b, p^{e})$ is even, by 10 $h(a, b, p^{e}) = k(p^{e})$; and if $h(a, b, p^{e})$ is odd, by 8, $h(a, b, p^{e}) = \frac{1}{2}k(p^{e})$.

Let us first consider the case for mod p. To determine the number of pairs (a,b) for which $(b^2 - ab - a^2, p) \neq 1$, consider $b^2 - ab - a^2 \equiv 0 \pmod{p}$, or $(2b - a)^2 \equiv 5a^2 \pmod{p}$. Since 5 is a quadratic residue of primes of this form, $x^2 \equiv 5 \pmod{p}$ has two solutions ±c. Thus the above condition is equivalent to $2b - a \equiv \pm ca \pmod{p}$, or

$$b \equiv \left(\frac{1 \pm c}{2}\right) a \pmod{p}$$
,

or $b_1 \equiv ra$ and $b_2 \equiv sa \pmod{p}$, where $r \equiv (1+c)/2$ and $s \equiv (1-c)/2 \pmod{p}$. Note that $r \neq s \pmod{p}$ for this would imply $c \equiv 0$ and hence $c^2 \equiv 0 \pmod{p}$.

To have (a, b, p) = 1, we must have (a, p) = 1 because if $(a,p) \neq 1$, then p|a; but

$$b \equiv \left(\frac{1 \pm c}{2}\right) a \pmod{p}$$
,

and so $b \equiv 0 \pmod{p}$ and $p \mid b$; hence $(a, b, p) \neq 1$. Therefore for mod p there are p - 1 possible values of a that will give (a, b, p) = 1 and $(b^2 - ab - a^2, p) \neq 1$; and

FIBONACCI SEQUENCES MODULO M

[Feb.

corresponding to each value of a, there are two values of b. Hence, there are 2(p - 1) pairs (a,b) with (a,b,p) = 1 and (b² - ab - a², p) \neq 1. We obtain:

If $a \equiv 1$, $b_1 \equiv r$ and $b_2 \equiv s \pmod{p}$;

If $a \equiv 2$, $b_1 \equiv 2r$ and $b_2 \equiv 2s \pmod{p}$;

•••

If $a \equiv p-1$, $b_1 \equiv (p-1)r$ and $b_2 \equiv (p-1)s \pmod{p}$.

It is clear that no matter what a is, for mod p, the pairs (a, ar) will all produce sequences of the same length as the pair (1,r), and similarly the pairs (a, as) will all produce sequences of the same length as the pair (1,s).

Now, we know that since k(p) = 4t + 2 there exist (a, b) such that $h(a, b, p) = \frac{1}{2}k(p) = 2t + 1$. But if there is one pair (a, b) satisfying this, there are at least p - 1 pairs (a, b) with h(a, b, p) = 2t + 1. We will show that there are only p - 1 such pairs.

Without any loss of generality we may assume a to be 1. We will show that either (1,r) or (1,s) but not both, will produce a sequence of length 2t + 1 when reduced mod p. Now suppose that both (1,r) and (1,s) produce sequences of length 2t + 1. We have

1, r, 1 + r, 1 + 2r, 2 + 3r,
$$\cdots$$
, $u_{n-1} + u_n r$, \cdots (mod p);
1, s, 1 + s, 1 + 2s, 2 + 3s, \cdots , $u_{n-1} + u_n s$, \cdots (mod p).

Therefore, we must have $u_{2t} + u_{2t+1}r \equiv 1$ and $u_{2t} + u_{2t+1}s \equiv 1 \pmod{p}$. Hence $u_{2t+1}(r-s) \equiv 0 \pmod{p}$. By 12, f(p) must be even for if f(p) is odd, then $4 |k(p^e)$. This gives $u_{2t+1} \neq 0 \pmod{p}$ for otherwise f(p) | (2t + 1) which is impossible. Hence we have $r \equiv s \pmod{p}$, and we have shown that this is impossible. Thus, the pairs (1, r) and (1, s) cannot both produce sequences of length 2t + 1.

An alternative proof is the following. Since $b^2 - ab - a^2 \equiv 0 \pmod{p}$ we must have $r^2 - r - 1 \equiv 0 \pmod{p}$, or $1 + r \equiv r^2 \pmod{p}$. Using the recurrence relation $f_n = f_{n-1} + f_{n-2}$ we may obtain $r + r^2 = r(1 + r) \equiv r^3 \pmod{p}$, $r^2 + r^3 = r(r + r^2) \equiv r^4 \pmod{p}$, etc. Thus the sequence

1, r,
$$1 + r$$
, $1 + 2r$, $2 + 3r$, ... (mod p)

may be written as 1, r, r^2 , r^3 , r^4 , \cdots (mod p). Similarly, the sequence 1, s, 1 + s, 1 + 2s, 2 + 3s, \cdots (mod p) may be written as 1, s, s^2 , s^3 , s^4 , \cdots (mod p).

Therefore, the assumption that these two sequences have periods of length 2t + 1 when reduced mod p, implies that $r^{2t+1} \equiv 1$ and $s^{2t+1} \equiv 1 \pmod{p}$. Multiplying these two congruences we obtain $(rs)^{2t+1} \equiv 1 \pmod{p}$. But

$$rs \equiv \frac{1 - c^2}{4} \equiv -1 \pmod{p}$$

because $c^2 \equiv 5 \pmod{p}$, and so $(-1)^{2t+1} \equiv 1 \pmod{p}$ which is impossible. Hence (1,r) and (1,s) cannot both produce sequences of length $\frac{1}{2}k(p) = 2t + 1$.

58

and

 $ab = a^2$ b) $\neq 1$ and (a b r

Therefore of the 2(p - 1) pairs (a,b) for which $(b^2 - ab - a^2, p) \neq 1$ and (a,b,p) = 1, p - 1 pairs produce sequences of length $\frac{1}{2}k$ and the other p - 1 pairs produce sequences of length k.

Since the total number of pairs (a,b) with (a,b,p) = 1 is given by $p^2 - 1$, we can now find the number of pairs (a,b) for which (a,b,p) = 1 and $(b^2 - ab - a^2, p) = 1$. We obtain $(p^2 - 1) - 2(p - 1) = (p - 1)^2$. All of these produce sequences of length k. Therefore for mod p we have

$$n(1) = 1, n\left(\frac{k}{2}\right) = \frac{2(p-1)}{k}$$

$$n(k) = \frac{(p - 1) + (p - 1)^2}{k} = \frac{p(p - 1)}{k}$$

We shall next consider the case for mod p^e . The condition $(b^2 - ab - a^2, p^e) \neq 1$ is equivalent to $(b^2 - ab - a^2, p) \neq 1$. Therefore we must again have

$$\mathbf{b} \equiv \left(\frac{1 \pm \mathbf{c}}{2}\right) \mathbf{a} \pmod{\mathbf{p}}$$

We know that (a, b, p^e) = 1 if and only if (a, p^e) = 1. Hence there are $p^e - p^{e-1}$ possible values of a, and corresponding to each value of a there are $2p^{e-1}$ values of b. Thus there are $2p^{e-1}(p^e - p^{e-1})$ pairs (a,b) with $(a,b,p^e) = 1$ and $(b^2 - ab - a^2, p^e) \neq 1$. If $a \equiv 1$, $b_1 \equiv r + jp$ and $b_2 \equiv s + jp \pmod{p^e}$ where $j = 0, 1, 2, \cdots, p^{e-1} - 1$. If $a \equiv 2$, $b_1 \equiv 2r + jp$ and $b_2 \equiv 2s + jp \pmod{p^e}$, where $j = 0, 1, 2, \cdots, p^{e-1} - 1$. These are equivalent to $b_1 \equiv 2(r + jp)$ and $b_2 \equiv 2(s + jp) \pmod{p^e}$, where $j = 0, 1, 2, \cdots, p^{e-1} - 1$.

Since for any a, the sequences (a, a(r + jp)) and (a, a(s + jp)) will all have the same length as (1, r + jp) and (1, s + jp), respectively, for $j = 0, 1, \dots, p^{e-1} - 1$, it is sufficient to consider the sequences (1, r + jp) and (1, s + jp) for $j = 0, 1, \dots, p^{e-1} - 1$.

Since $k(p^e) = 4t + 2$, we know that for at least one value of j, at least one of (1, r + jp) and (1, s + jp) produces a sequence of length 2t + 1. Suppose for some value of j, $h = h(1, r + jp, p^e) = 2t + 1$. We will show that then for any i where i is one of 0, 1, 2, \dots , $p^{e-1} - 1$, $h(1, s + ip, p^e) \neq 2t + 1$. Suppose for some i,

$$h = h(1, r + jp, p^{e}) = h(1, s + ip, p^{e}) = \frac{1}{2}k = 2t + 1.$$

We have

1,
$$r + jp$$
, ..., $u_{n-1} + u_n(r + jp)$, ... (mod p^e);
1, $s + ip$, ..., $u_{n-1} + u_n(s + ip)$, ... (mod p^e);

and so

$$u_{h-1} + u_h(r + jp) \equiv 1 \equiv u_{h-1} + u_h(s + ip) \pmod{p^e}$$
,

or $u_h(r+jp) \equiv u_h(s+ip) \pmod{p^e}$. Since by 12 $u_h \neq 0 \pmod{p}$, we may cancel u_h and obtain $r+jp \equiv s+ip \pmod{p^e}$, or $r \equiv s \pmod{p}$ which is impossible.

Hence if for some value of j, $h(1 + r + jp, p^e) = 2t + 1$ then for no value of i can $h(1, s + ip, p^e)$ be equal to 2t + 1. Similarly, if for some value of j,

$$h(1, s + jp, p^{e}) = 2t + 1,$$

then for no value of i can $h(1, r + ip, p^e)$ be equal to 2t + 1.

Next, we will show that only one value of j gives a length of 2t + 1. Suppose both (1, r + jp) and (1, r + ip) produce sequences of length h = 2t + 1, where i and j are two different numbers from $0, 1, \dots, p^{e-1} - 1$. Therefore

$$\begin{split} u_{h-1} + u_h(r + jp) &\equiv 1 \equiv u_{h-1} + u_h(r + ip) \pmod{p^e}, \\ u_h(r + jp) &\equiv u_h(r + ip) \pmod{p^e}. \end{split}$$

Since by 12, $u_h \neq 0 \pmod{p}$, we have $r + jp \equiv r + ip \pmod{p^e}$, or $jp \equiv ip \pmod{p^e}$, or $j \equiv i \pmod{p^{e-1}}$ which is impossible. Therefore of the $2p^{e-1}$ values corresponding to each value of a, only one can produce a sequence of length 2t + 1. But there are $p^e - p^{e-1}$ possible values of a. Hence there are $p^e - p^{e-1}$ or $p^{e-1}(p-1)$ pairs (a,b) that produce sequences of length $\frac{1}{2}k(p^e)$. The remaining $2p^{e-1}(p^e - p^{e-1}) - (p^e - p^{e-1})$ or $p^{e-1}(p-1)(2p^{e-1}-1)$ pairs (a,b) that have (a, b, $p^e) = 1$ and $(b^2 - ab - a^2, p^e) \neq 1$ produce sequences of length $k(p^e)$. Also since there are $p^{2e} - p^{2e-2}$ pairs (a,b) for which (a, b, $p^e) = 1$, we have

$$(p^{2e} - p^{2e-2}) - 2p^{e-1}(p^{e} - p^{e-1})$$

or $p^{2e-2}(p-1)^2$ pairs with $(b^2 - ab - a^2, p^e) = 1$. All of these produce sequences of length $k(p^e)$. In addition to these, there are the sequences for which $(a, b, p^e) \neq 1$. Thus for mod p^e we have n(1) = 1,

$$n(p^{i}k/2) = \frac{p^{i}(p-1)}{p^{i}k/2} = \frac{2(p-1)}{k}$$

and

$$n(p^{i}k) = \frac{p^{i}(p-1)(2p^{i}-1) + p^{2i}(p-1)^{2}}{p^{i}k} = \frac{(p-1)(p^{i+1}+p^{i}-1)}{k} \quad (i = 0, 1, \dots, e-1).$$

<u>Theorem 3'</u>. Let $m = p^e$ where $p \equiv \pm 1 \pmod{10}$ and let t be the largest integer such that $k(p^t) = k(p)$ with t > 1.

 \mathbf{or}

FIBONACCI SEQUENCES MODULO M

(1) if 4|k, then (a) for $e \leq t$, n(1) = 1 and

$$n(k) = \frac{p^{2e} - 1}{k}$$
,

and (b) for e > t, n(1) = 1,

$$m(k) = \frac{p^{2t} - 1}{k} ,$$

and

$$n(p^{i-t+1}k) = \frac{p^{i+t-1}(p^2 - 1)}{k}$$
 for $i = t, \dots, e - 1$.

(2) if 4/k, then (a) for $e \leq t$, n(1) = 1,

$$n\left(\frac{k}{2}\right) = \frac{2(p^{e} - 1)}{k}$$

and

$$n(k) = \frac{p^{e}(p^{e} - 1)}{k}$$

and (b) for e > t, n(1) = 1,

$$n\left(\frac{k}{2}\right) = \frac{2(p^{t} - 1)}{k} ,$$
$$n(k) = \frac{p^{t}(p^{t} - 1)}{k} ,$$

$$n(p^{i-t+1}k/2) = \frac{2p^{t-1}(p-1)}{k}$$
,

and

$$n(p^{i-t+1}k) = \frac{p^{t-1}(p-1)(p^{i+1}+p^i-1)}{k}$$

for $i = t, \dots, m - 1$.

Proof. (1) Same as the proof for Theorem 1'.

(2) We have shown in Theorem 3 that if (a, b, p^e) = 1, for mod p^e , $p^{e-1}(p-1)$ pairs (a, b) produce sequences of length $\frac{1}{2}k(p^e)$ and

$$p^{e-1}(p - 1)(2p^{e-1} - 1) + p^{2e-2}(p - 1)^2$$

 \mathbf{or}

$$p^{e-1}(p - 1)(p^e + p^{e-1} - 1)$$

1974]

61

For mod p^0 , n(1) = 1. For mod p, n(1) = 1,

$$n\left(\frac{k}{2}\right) = \frac{2(p-1)}{k},$$

and

$$n(k) = \frac{p(p-1)}{k}$$

For mod
$$p^2$$
, $n(1) = 1$,

$$n\left(\frac{k}{2}\right) = \frac{2(p-1)}{k} + \frac{2p(p-1)}{k} = \frac{2(p^2-1)}{k} ,$$

$$n(k) = \frac{p(p-1)}{k} + \frac{p(p-1)(p^2+p-1)}{k} = \frac{p^2(p^2-1)}{k} ,$$

and

For mod p^t , n(1) = 1,

$$n\left(\frac{k}{2}\right) = \sum_{i=0}^{t-1} \frac{2p^{i}(p-1)}{k} = \frac{2(p^{t}-1)}{k}$$

,

and

$$n(k) = \sum_{i=0}^{t-1} \frac{p^{i}(p-1)(p^{i+1}+p^{i}-1)}{k} = \frac{p^{t}(p^{t}-1)}{k}$$

For mod
$$p^{t+1}$$
, $n(1) = 1$,

$$n\left(\frac{k}{2}\right) = \frac{2(p^{t} - 1)}{k} ,$$
$$n(k) = \frac{p^{t}(p^{t} - 1)}{k} ,$$
$$n(pk/2) = \frac{2p^{t-1}(p - 1)}{k}$$

and

$$n(pk) = \frac{p^{t-1}(p-1)p^{t+1} + p^{t} - 1}{k}$$

FIBONACCI SEQUENCES MODULO M

For mod p^{t+2} , n(1) = 1,

$$n\left(\frac{k}{2}\right) = \frac{2(p^{t} - 1)}{k}, \quad n(k) = \frac{p^{t}(p^{t} - 1)}{k}, \quad n(pk/2) = \frac{2p^{t-1}(p - 1)}{k},$$
$$n(pk) = \frac{p^{t-1}(p - 1)(p^{t+1} + p^{t} - 1)}{k}, \quad n(p^{2}k/2) = \frac{2p^{t-1}(p - 1)}{k},$$
$$n(p^{2}k) = \frac{p^{t-1}(p - 1)(p^{t+2} + p^{t+1} - 1)}{k}.$$

• • •

Thus for $e \leq t$, we have n(1) = 1,

$$n\left(\frac{k}{2}\right) = \sum_{i=0}^{e-1} \frac{2p^{i}(p-1)}{k} = \frac{2(p^{e}-1)}{k}$$

and

$$n(k) = \sum_{i=0}^{e-1} \frac{p^{i}(p-1)(p^{i+1}+p^{i}-1)}{k} = \frac{p^{e}(p^{e}-1)}{k} ;$$

and for e > t we have n(1) = 1,

$$n\left(\frac{k}{2}\right) = \frac{2(p^{t}-1)}{k}$$
, $n(k) = \frac{p^{t}(p^{t}-1)}{k}$, $n(p^{i-t+1}k/2) = \frac{2p^{t-1}(p-1)}{k}$,

and

$$n(p^{i-t+1}k) = \frac{p^{t-1}(p-1)(p^{i+1}+p^{i}-1)}{k}$$
 for $i = t, \dots, e-1$.

Theorem 4. Let $N(h,m) = h \cdot n(h,m)$. If

$$m = \prod_{i=1}^{n} p_{i}^{e_{i}},$$

then

$$n(h,m) = \sum_{\text{LCM}[h_i]=h} \frac{\prod_{i=1}^{n} N(h_i, p_i^{e_i})}{h}$$

,

where $h_i = h(a, b, p_i^{e_i})$.

1974]

and

n

<u>Proof.</u> Consider the equivalent problem for which the modulus is of the form $\prod_{i=1}^{n} \prod_{i=1}^{n} \prod_{i=1}^{n$

Let $[h_1, h_2]$ denote the least common multiple of h_1 and h_2 . We have seen that each pair of pairs (a,b) (mod m_1) and (c,d) (mod m_2) gives a unique pair (e,f) (mod m_1m_2), of length $h = [h_1, h_2]$. Therefore there are $N(h_1, m_1) \cdot N(h_2, m_2)$ such pairs (e,f) with length h_1 (mod m_1) and length h_2 (mod m_2). Now any pair (e,f) (mod m_1m_2) with length h when reduced mod m_1 produces a sequence of length h_1 and when reduced mod m_2 produces a sequence of length h_2 such that $[h_1, h_2] = h$. Hence

$$N(h, m_1m_2) = \sum_{[h_1, h_2]=h} N(h_1, m_1) \cdot N(h_2, m_2), \text{ and so } n(h, m_1m_2) = \sum_{[h_1, h_2]=h} \frac{N(h_1, m_1) \cdot N(h_2, m_2)}{h}.$$

By induction, this result is now easily extended to the case $m = \prod_{i=1}^{n} m_i$, where $n \ge 2$, and all the m_i are pairwise relatively prime. Thus we obtain

$$n(h,m) = \sum_{LCM[h_i]=h} \frac{\prod_{i=1}^{m} N(h_i,m_i)}{h} .$$

In particular, if $m_i = p_i^{e_i}$ for $i = 1, \dots, n$, we have

$$n(h,m) = \sum_{LCM[h_i]=h} \frac{\prod_{i=1}^{n} N(h_i, p_i^i)}{h}$$

These four theorems cover all possible values of m. Thus if $k(p^e)$ is known, the values of h(a, b, m) as well as n(h,m) can be determined.

I would like to acknowledge the assistance Prof. D. Singmaster gave me with his criticisms and suggestions in putting this paper in its final form.

REFERENCES

- 1. D. D. Wall, "Fibonacci Series Modulo m," Amer. Math. Monthly, 67 (1960), 525-532.
- D. W. Robinson, "The Fibonacci Matrix Modulo m," <u>Fibonacci Quarterly</u>, 1 (1963), pp. 29-35.
- 3. S. E. Mamangakis, "Remarks on the Fibonacci Series Modulo m," Amer. Math. Monthly, 68 (1961), pp. 648-649.
- 4. J. Vinson, "The Relation of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence," Fibonacci Quarterly, 1 (1963), pp. 37-45.

PHI: ANOTHER HIDING PLACE

H. E. HUNTLEY Nethercombe Cottage, Canada Combe, Hutton, Weston - Super - Mare, England

From an area A of any outline, regular or irregular, there is cut an area B, having the same outline as that of A under the following conditions: (i) The peripheries of A and B have one point O in common; (ii) B is oriented so that O and the centroids C_a and C_b of A and B are colinear. It follows that C, the centroid of the remnant (A - B) also lies in the straight line OC_aC_b produced.





Let the ratio of the linear dimensions of A and B be a:b, their respective areas being λa^2 , λb^2 ; OC_a/OC_b = a/b.

Taking moments about O,

$$\lambda b^2 \cdot OC_b + \lambda (a^2 - b^2) \cdot OC = \lambda a^2 \cdot OC_a$$
,

whence, multiplying by $1/\lambda b^2 \cdot OC_{\rm h}$,

$$1 + \left(\frac{a^2}{b^2} - 1\right) \cdot \frac{OC}{OC_b} = \frac{a^3}{b^3}$$

Since $(a/b) - 1 \neq 0$,

$$\left(\, \frac{a}{b} \, + \, 1 \right) \cdot \, \frac{\mathrm{OC}}{\mathrm{OC}_b} \ = \ \frac{a^2}{b^2} \, + \, \frac{a}{b} \, + \, 1 \quad . \label{eq:eq:optimal_states}$$

Phi, the Golden Section, is now uncovered by writing OC/OC_b = 2, giving

$$\frac{a^2}{b^2} - \frac{a}{b} - 1 = 0 ,$$

whence $a/b = \phi$ or $a/b = 1/\phi$.

The result is, of course, applicable to regular plane figures. In the case of the circle the centroid C of the remnant lune falls on the endpoint of the diameter of B through O.





Any chord of circle A through O is cut by the circumference of B in the Golden Section: $PO/QO = \phi = (1 + \sqrt{5})/2$.

THE FIBONACCI ASSOCIATION PROGRAM OF SATURDAY, OCTOBER 20, 1973 St. Mary's College

SOME PROPERTIES OF TRIANGULAR NUMBERS Marjorie Bicknell, A. C. Wilcox High School, Santa Clara, California

THE GOLDEN SECTION REVISITED Edmundo Alvillar, San Francisco, California

OPERATORS ASSOCIATED WITH STIRLING NUMBERS Elaine E. Alexander, California Polytechnic State University

ALGORITHMS FOR THIRD-ORDER RECURSION SEQUENCES Brother Alfred Brousseau, St. Mary's College, California

ON THE DIOPHANTINE EQUATION $1 + x + \cdots + x^{a} = y^{b}$ Hugh Edgar, San Jose State University, San Jose, California

PASCAL, CATALAN, AND LAGRANGE WITH CONVOLUTIONS Verner E. Hoggatt, Jr., San Jose State University, San Jose, California.

SOME GEOMETRICAL PROPERTIES OF THE GENERALIZED FIBONACCI SEQUENCE

D. V. JAISWAL Holkar Science College, Indore, India

1. INTRODUCTION

In this paper, some geometrical properties of the generalized Fibonacci sequence $\{T_n\}$ have been discussed. The sequence $\{T_n\}$ being defined by

$$T_{n+1} = T_n + T_{n-1}$$
,
 $T_1 = a$, $T_2 = b$.

On taking a = b = 1, the Fibonacci sequence $\{F_n\}$ is obtained. We shall make use of the following identities [1]

(1.1)
$$T_{m+n} = T_m F_{n+1} + T_{m-1} F_n.$$

(1.2)
$$F_n F_{n+m} - F_{n-s} F_{n+m+s} = (-1)^{n-s} F_s F_{s+m}$$

(1.3)
$$T_m T_{n+k} - T_{m+k} T_n = (-1)^m F_k F_{n-m} D$$

where D is the characteristic number of the sequence and is given by

$$T_n^2 - T_{n-1}T_{n+1} = (-1)^n D;$$
 2a < b.
2. THEOREM 1

Area of the triangle having vertices at the points designated by the rectangular cartesian coordinates (T_n, T_{n+r}) , (T_{n+p}, T_{n+p+r}) , (T_{n+q}, T_{n+q+r}) is independent of n. <u>Proof</u>. Twice the area of the specified triangle is equal to the absolute value of the

<u>**Proof.**</u> Twice the area of the specified triangle is equal to the absolute value of the determinant

 $\begin{vmatrix} \mathbf{T}_{\mathbf{n}} & \mathbf{T}_{\mathbf{n}+\mathbf{r}} & \mathbf{1} \\ \mathbf{T}_{\mathbf{n}+\mathbf{p}} & \mathbf{T}_{\mathbf{n}+\mathbf{p}+\mathbf{r}} & \mathbf{1} \\ \mathbf{T}_{\mathbf{n}+\mathbf{q}} & \mathbf{T}_{\mathbf{n}+\mathbf{q}+\mathbf{r}} & \mathbf{1} \end{vmatrix}$

Using (1.1) for the second column the determinant can be written as

$$F_{r+1} \begin{vmatrix} T_{n} & T_{n} & 1 \\ T_{n+p} & T_{n+p} & 1 \\ T_{n+q} & T_{n+q} & 1 \end{vmatrix} + F_{r} \begin{vmatrix} T_{n} & T_{n-1} & 1 \\ T_{n+p} & T_{n+p-1} & 1 \\ T_{n+q} & T_{n+q-1} & 1 \end{vmatrix}$$

The first determinant is obviously zero; in the second on alternately subtracting the second and first column from each other, the suffixes can be reduced and finally we get

$${}^{\pm F}{}_{r} \left| \begin{array}{ccc} {}^{T}{}_{1} & {}^{T}{}_{2} & 1 \\ {}^{T}{}_{p+1} & {}^{T}{}_{p+2} & 1 \\ {}^{T}{}_{q+1} & {}^{T}{}_{q+2} & 1 \end{array} \right|$$

according as n is odd or even.

On expanding the determinant along the third column, we obtain

$${}^{\pm}\mathbf{F}_{\mathbf{r}} [(\mathbf{T}_{p+1}\mathbf{T}_{q+2} - \mathbf{T}_{p+2}\mathbf{T}_{q+1}) - (\mathbf{T}_{1}\mathbf{T}_{q+2} - \mathbf{T}_{2}\mathbf{T}_{q+1}) \\ + (\mathbf{T}_{1}\mathbf{T}_{p+2} - \mathbf{T}_{2}\mathbf{T}_{p+1})] ,$$

which on using (1.3) reduces to

$$\pm F_{r}[F_{q} - F_{p} - (-1)^{p}F_{q-p}]D$$
.

Thus the area of the specified triangle is independent of n.

Particular Case. On taking r = h, p = 2h, q = 4h, a = b = 1, we find that the area of the triangle whose vertices are (F_n, F_{n+h}) , (F_{n+2h}, F_{n+3h}) , (F_{n+4h}, F_{n+5h}) is equal to the value of (2.1)

$$\frac{1}{2}F_{h}(F_{4h} - 2F_{2h})$$

Duncan [2] has proved that the area of this triangle is

$$\frac{1}{2} [\, {}^{\mathbf{F}}_{\mathbf{h}} \, ({}^{\mathbf{F}}_{4\mathbf{h}} \, - \, {}^{\mathbf{F}}_{2\mathbf{h}} \,) \, - \, ({}^{\mathbf{F}}_{3\mathbf{h}} \, {}^{\mathbf{F}}_{4\mathbf{h}} \, - \, {}^{\mathbf{F}}_{2\mathbf{h}} \, {}^{\mathbf{F}}_{5\mathbf{h}} \,) \,] \, ,$$

which on using (1.2) simplifies to the value given in (2.1).

3. THEOREM 2

Lines drawn through the origin with the direction ratios T_n, T_{n+p}, T_{n+q} , where p and q are arbitrary constants are always coplanar for every value of n.

<u>Proof.</u> Direction ratios of any three such lines are T_i , T_{i+p} , T_{i+q} ; T_j , T_{j+p} , T_{j+q} ; T_k , T_{k+p} , T_{k+q} . These will be coplanar if

(3.1)
$$\begin{vmatrix} T_{i} & T_{i+p} & T_{i+q} \\ T_{j} & T_{j+p} & T_{j+q} \\ T_{k} & T_{k+p} & T_{k+q} \end{vmatrix} = 0$$

On using the relation (1.1), the left-hand side of (3.1) can be written as the sum of four determinants, each of which is zero. Hence proved.

4. THEOREM 3

Set of points designated by the cartesian coordinates (T_n, T_{n+p}, T_{n+q}) where p and

q are arbitrary constants and $n = 1, 2, 3, \cdots$, are always coplanar. This plane passes through the origin, and its equation is independent of n.

,

Proof. Equation to the plane passing through any three points of the set is

(4.1)
$$\begin{vmatrix} x & y & z & 1 \\ T_{i} & T_{i+p} & T_{i+q} & 1 \\ T_{j} & T_{j+p} & T_{j+q} & 1 \\ T_{k} & T_{k+p} & T_{k+q} & 1 \end{vmatrix} = 0$$

where i, j and k are particular values of n. Here the coefficient of x is

$$= [(T_{j+p}T_{k+q} - T_{j+q}T_{k+p}) - (T_{i+p}T_{k+q} - T_{i+q}T_{k+p}) + (T_{i+p}T_{j+q} - T_{i+q}T_{j+p})] = (-1)^{p} F_{q-p} \{ (-1)^{j} F_{k-j} - (-1)^{i} F_{k-i} + (-1)^{i} F_{j-i} \} D.$$

The coefficient of y is obtained on putting p = 0 in the coefficient of x; the coefficient of z is obtained from the coefficient of y on replacing q by p; the constant term is zero as is already proved in (3.1).

Thus the equation to the plane simplifies to

(4.2)
$$(-1)^{p} F_{q-p} x - F_{q} y + F_{p} z = 0 .$$

This equation is independent of n. Also it does not depend on the initial values a and b. Q.E.D.

<u>Particular Case.</u> On taking a = 1, b = 3 we obtain the Lucas sequence $\{L_n\}$. The points (F_i, F_{i+2}, F_{i+5}) , $i = 1, 2, 3, \cdots$; (L_j, L_{j+2}, L_{j+5}) , $j = 1, 2, 3, \cdots$; (T_k, T_{k+2}, T_{k+5}) , $k = 1, 2, 3, \cdots$; all lie on the plane 2x - 5y + z = 0.

5. THEOREM 4

The set of planes

$$T_n x + T_{n+p} y + T_{n+q} z + T_{n+r} = 0$$
,

where p, q, r are arbitrary constants, and $n = 1, 2, 3, \dots$; all intersect in a given line whose equation is independent of n.

Proof. Let two such planes be

(5.1)
$$\begin{array}{rcl} T_{i}x + T_{i+p}y + T_{i+q}z + T_{i+r} &= 0\\ T_{j}x + T_{j+p}y + T_{j+q}z + T_{j+r} &= 0 \end{array}$$

The equation to the line of intersection of the parallel planes through the origin is

$$\frac{x}{T_{i+p}T_{j+q} - T_{i+q}T_{j+p}} = \frac{y}{T_iT_{j+q} - T_{i+q}T_j} = \frac{z}{T_iT_{j+p} - T_{i+p}T_j}$$

SOME GEOMETRICAL PROPERTIES OF THE GENERALIZED FIBONACCI SEQUENCE

On using (1.3) and proceeding as in (4.2) this simplifies to

$$\frac{\mathbf{x}}{\left(-1\right)^{p}\mathbf{F}_{q-p}} = \frac{-\mathbf{y}}{\mathbf{F}_{q}} = \frac{\mathbf{z}}{\mathbf{F}_{p}}$$

Similarly the line of intersection of the planes given by (5.1) meets the plane z = 0, at the point given by

$$\frac{x}{(-1)^{p}F_{r-p}} = \frac{-y}{F_{r}} = \frac{1}{F_{p}} .$$

Thus the equation to the line of intersection of the planes given by (5.1) becomes

(5.2)
$$\frac{(-1)^{p} F_{p} x - F_{r-p}}{F_{q-p}} = \frac{F_{p} y + F_{r}}{-F_{q}} = \frac{z}{F_{p}}$$

Hence proved.

Particular Case. The set of planes whose equations are

$$\begin{aligned} & F_{i}x + F_{i+1}y + F_{i+3}z + F_{i+4} = 0, & i = 1, 2, 3, \cdots; \\ & L_{j}x + L_{j+1}y + L_{j+3}z + L_{j+4} = 0, & j = 1, 2, 3, \cdots; \\ & T_{k}x + T_{k+1}y + T_{k+3}z + T_{k+4} = 0, & k = 1, 2, 3, \cdots; \end{aligned}$$

all intersect along the line

$$\frac{x+2}{1} = \frac{y+3}{2} = \frac{z}{-1} \; .$$

I am grateful to Dr. V. M. Bhise, G. S. Tech. Institute, Indore, for his help and guidance in the preparation of this paper.

REFERENCES

- 1. Brother Alfred Brousseau, <u>An Introduction to Fibonacci Discovery</u>, The Fibonacci Association, San Jose, California (1965).
- Dewey C. Duncan, "Chains of Equivalent Fibonacci-wise Triangles," <u>Fibonacci Quarter-</u> terly, Vol. 5, No. 1 (February 1967), pp. 87-88.

~~~~
SETS OF BINOMIAL COEFFICIENTS WITH EQUAL PRODUCTS

CALVIN T. LONG Washington State University, Pullman, Washington 99163 and University of British Columbia, Vancouver, B.C., Canada and VERNER E. HOGGATT, JR. San Jose State University, San Jose, California 95192

1. INTRODUCTION

In [2], Hoggatt and Hansell show that the product of the six binomial coefficients surrounding any particular entry in Pascal's triangle is an integral square. They also observe that the two products of the alternate triads of these six numbers are equal. Quite remarkably, Gould conjectured and Hillman and Hoggatt [1] have now proved that the two greatest common divisors of the numbers in the above-mentioned triads are also equal though their least common multiples are, in general, not equal. Hillman and Hoggatt also generalize the greatest common divisor property to more general arrays.

The integral square property was further investigated by Moore [4], who showed that the result is true for any regular hexagon of binomial coefficients if the number of entries per side is even, and by the present author [3], who generalized the earlier results to nonregular hexagons, octagons, and other arrays of binomial coefficients whose products are squares.

In the present paper, we generalize the equal product property of Hoggatt and Hansell along the lines of [3] and also make some observations and conjectures regarding a generalized greatest common divisor property.

It will suit our purpose to represent Pascal's triangle (or, more precisely, a portion of it) by a lattice of dots as in Fig. 1. We will have occasion to refer to various polygonal figures and when we do, unless expressly stated to the contrary, we shall always mean a simple closed polygonal curve whose vertices are lattice points. Occasionally, it will be convenient to represent a small portion of Pascal's triangle by letter arranged in the proper position.



2. SETS OF BINOMIAL COEFFICIENTS WITH EQUAL PRODUCTS

As in [3], we begin by deriving a fundamental lemma which is basic to all of the other results of this section.

Lemma 1. Consider two parallelograms of binomial coefficients oriented as in Fig. 2 and with corner coefficients a, b, c, d and e, f, g, h as indicated. Then the products acfh and bdeg are equal.

<u>Proof</u>. For suitable integers m, n, r, s, and t, the binomial coefficients in question may be represented in the form

$$a = \begin{pmatrix} m+s \\ n \end{pmatrix}, \quad b = \begin{pmatrix} m \\ n \end{pmatrix}, \quad c = \begin{pmatrix} m+r \\ n+r \end{pmatrix}, \quad d = \begin{pmatrix} m+s+r \\ n+r \end{pmatrix},$$
$$c = \begin{pmatrix} m+r \\ n+r+t \end{pmatrix}, \quad f = \begin{pmatrix} m \\ n+r+t \end{pmatrix}, \quad g = \begin{pmatrix} m+s \\ n+s+r+t \end{pmatrix}, \quad h = \begin{pmatrix} m+s+r \\ n+s+r+t \end{pmatrix}.$$

Thus, the desired products are

$$acfh = \frac{(m + s)!}{n! (m - n + s)!} \cdot \frac{(m + r)!}{(n + r)! (m - n)!}$$
$$\cdot \frac{m!}{(n + r + t)! (m - n - r - t)!} \cdot \frac{(m + s + r)!}{(n + s + r + t)! (m - n - t)!}$$

and

bdeg =
$$\frac{m!}{n! (m - n)!} \cdot \frac{(m + s + r)!}{(n + r)(m - n + s)!}$$

 $\cdot \frac{(m + r)}{(n + r + t)! (m - n - t)!} \cdot \frac{(m + s)!}{(n + r + s + t)! (m - n - r - t)!}$

and these are clearly equal as claimed.

As a first consequence of Lemma 1, we obtain the equal product result of Hoggatt and Hansell.

Theorem 2. Let a, b, c, d, e, f, and g denote binomial coefficients as in the array

Then aec = fbd.

<u>Proof.</u> The parallelograms a, f, e, g and b, g, d, c are oriented as in Lemma 1. Therefore, fgbd = aegc and this implies the desired result.

By essentially the same argument, we obtain the following more general statement about products of coefficients at the vertices of hexagons in Pascal's triangle.

<u>Theorem 3.</u> Let $m \ge 1$ and $n \ge 1$ be integers and let H be a convex hexagon whose sides lie on the horizontal rows and main diagonals of Pascal's triangle. Let the number of

coefficients on the respective sides of H be m, n, m, n, m, and n in that order, and let a, b, c, d, e, and f be the coefficients in cyclic order at the vertices of H. Then ace = bdf.

<u>Proof.</u> Without loss in generality, we may take m to be the number of coefficients along the bottom side of H. If we consider two m-by-n parallelograms with a common vertex and with corner coefficients a, b, c, d, e, f, and g as in Fig. 3, then, again by Lemma 1, fgbd = aegc and this implies the equality claimed.



Fig. 3

Now, as in [3], let us call the hexagons of Hoggatt and Hansell fundamental hexagons and say that a polygonal figure P on Pascal's triangle is <u>tiled</u> with fundamental hexagons if P is "covered" by a set F of fundamental hexagons F in such a way that

- i. The vertices of each F in F are coefficients in P or in the interior of P.
- ii. Each boundary coefficient of P is a vertex of precisely one F in F, and
- iii. Each interior coefficient of P is interior to some F in F or is a vertex shaped by precisely two elements of F.

We can then prove the following result.

<u>Theorem 4.</u> Let P_n be a polygonal figure on Pascal's triangle with boundary coefficients a_1, a_2, \dots, a_n in order around P_n . If P_n can be tiled by fundamental hexagons, then n = 2s for some $s \ge 3$ and

$$\underset{i=1}{\overset{s}{\underset{i=1}{\prod}}} a_{2i-1} = \underset{i=1}{\overset{s}{\underset{i=1}{\prod}}} a_{2i} \ .$$

<u>Proof.</u> Suppose that P_n can be tiled with r fundamental hexagons. The proof proceeds by induction on r. Clearly the least value of r is 1 which occurs only in the case of the fundamental hexagon itself. In this case, n = 6 and the result is true by Theorem 2. Now suppose that the result is true for any polygon that can be tiled with fewer than k fundamental hexagons where $k \ge 1$ is fixed and let P_n be a polygon that can be tiled with k fundamental hexagons. Let H be one of the hexagons which tiles P_n and contains at least one boundary point of P_n . We distinguish five cases.

<u>Case 1</u>. H contains just one boundary point of P_n . Without loss in generality, we may let a_n be the boundary point of P_n which is in H. Let a'_n , a'_{n+1} , a'_{n+2} , a'_{n+3} , and a'_{n+4} denote the other five boundary points of H in order around H. Let P_m be the polygon obtained from P_n by deleting H. Then the boundary points of P_m are a_1, a_2, \cdots , a_{n-1} , a'_n , a'_{n+1} , a'_{n+2} , a'_{n+3} , and a'_{n+4} . Thus, m = n+4. Also, since P_m can be tiled by k - 1 fundamental hexagons, n+4 = m = 2t for some t and

$$a_1 a_3 \cdots a_{n-1} a'_{n+1} a'_{n+3} = a_2 a_4 \cdots a_{n-2} a'_n a'_{n+2} a'_{n+4}$$

But, since H is a fundamental hexagon, it follows that

$$a_{n}a'_{n+1}a'_{n+3} = a'_{n}a'_{n+2}a'_{n+4}$$

and this clearly implies that

$$\underset{i=1}{\overset{s}{\prod}} a_{2i-1} = \underset{i=1}{\overset{s}{\prod}} a_{2i}$$

since n = 2t - 4 = 2s. This completes the proof for Case 1.

<u>Cases 2-4</u>. In these cases, respectively, H contains 2, 3, 4, or 5 boundary points of P_n . We omit the proofs of these cases since they essentially duplicate the proof of Case 1. This completes the proof.

With Theorem 4 and Lemma 1 as our principal tools we are now able to give several quick results.

<u>Theorem 5.</u> Let H_n be a convex hexagon with an even number of coefficients per side, with sides oriented along the horizontal rows and main diagonals of Pascal's triangle, and with boundary coefficients a_1, a_2, \dots, a_n in order around H_n . Then n = 2s for some $s \ge 3$ and

$$\prod_{i=1}^{s} a_{2i-1} = \prod_{i=1}^{s} a_{2i} .$$

<u>Proof.</u> This is an immediate consequence of Theorem 4 since H_n can be tiled by fundamental hexagons as shown in Theorem 5 of [3].

<u>Theorem 6.</u> Let K_n be any convex octagon with sides oriented along the horizontal and vertical rows and main diagonals of Pascal's triangle and with boundary coefficients a_1, a_2, \dots, a_n in order around K_n . Let the number of coefficients on the various sides of K_n be 2r, 2s, t, 2u, 2v, t, and 2s as indicated in Fig. 4. Then n = 2h for some $h \ge 4$ and



Proof. The proof is the same as for Theorem 5 and will be omitted.

We observe that the convexity conditions in both Theorems 3 and 5 are necessary since neither result is true for the hexagon of Fig. 5. Also, it is easy to find examples of convex hexagons where the results of Theorems 3 and 5 do not hold if the conditions on the number of elements per side are not met. In fact, we conjecture that the conditions in these theorems are both necessary and sufficient. On the other hand, the convexity condition of Theorem 6 is <u>not</u> necessary since the result holds for the octagon of Fig. 6 which is clearly not convex. We make no conjecture regarding necessary and sufficient conditions for the result of Theorem 6 to hold for octagons in general, or indeed, for hexagons whose sides may not lie along the horizontal rows and main diagonals of Pascal's triangle. We note that the octagon of Fig. 6 cannot be tiled by fundamental hexagons but can be tiled by pairs of properly oriented "fundamental parallelograms" as indicated by the shading in the figure. Thus, the most general theorem for these and other polygons will most likely have to be couched in terms of tilings by sets of pairs of fundamental parallelograms.





1974]

3. ADDITIONAL COMMENTS ON EQUAL PRODUCTS

Theorem 3 gives an equal product result for the corner coefficients of hexagons and it is natural to seek similar results for octagons. It is easy to find octagons like those in Figs. 4 and 6 for which the equal product property on vertices does not hold. Nevertheless, it is possible to find classes of octagons for which the equal product property does hold for the products of alternate corner coefficients.

<u>Theorem 7.</u> Let K be a convex octagon formed as in Fig. 7 by adjoining parallelograms with r and s and r and t elements on a side to a parallelogram with r elements on each side. If the corner coefficients are a_1, a_2, \dots, a_8 as shown, then

$$a_1 a_3 a_5 a_7 = a_2 a_4 a_6 a_8$$
.

<u>Proof.</u> We have only to observe that a_1 , a_4 , a_5 , a_8 and a_2 , a_3 , a_6 , a_7 are vertices of pairs of parallelograms oriented as in Lemma 1. The result is then immediate.

Again it is clear that the convexity condition of Theorem 7 is not necessary. The proof, after all, rests on the presence of the properly oriented pairs of parallelograms. In precisely the same way we show that $a_1a_3a_5a_7 = a_2a_4a_6a_8$ for each of the three octagons of Fig. 8. Note that for K_2 the two products are <u>not</u> products of alternate vertices around the octagon.

Clearly the preceding methods can be used to obtain a wide variety of configurations of binomial coefficients which divide into sets with equal products. As illustrations we give several examples of polygons (sometimes not closed, simple, or connected) with this property.



Fig. 8

4. THE GREATEST COMMON DIVISOR PROPERTY

As mentioned in Section 1, if the array



represents coefficients from Pascal's triangle, then afe = cbg and Hillman and Hoggatt





Fig. 9

[Feb.

Unfortunately, it is easy to find examples of regular hexagons with sides oriented along the main diagonals and horizontal rows of Pascal's triangle where the two alternate triads of corner coefficients have different greatest common divisors in spite of the fact that they have equal products by Theorem 3. We have such examples for hexagons with 3, 4, 5 and 6 coefficients per side and conjecture that the property only holds in general for the fundamental hexagons of Hoggatt and Hansell. Also, we observe that, for the parallelograms of Fig. 2, the products acfh and bdeg are equal but that (a, c, f, h) is not necessarily equal to (b, d, e, g). At the same time, we have been unable to find examples of hexagons of the type of Theorem 5 where the greatest common divisor of the two sets of alternate boundary coefficients are not equal. Of course, these greatest common divisors are usually equal to one, but the three regular hexagons with four elements per side whose upper left-hand coefficients are, respectively.

 $\begin{pmatrix} 13\\6 \end{pmatrix}$, $\begin{pmatrix} 14\\6 \end{pmatrix}$, and $\begin{pmatrix} 17\\6 \end{pmatrix}$

have pairs of greatest common divisors equal to 13, 13, and 34, respectively. We conjecture that the greatest common divisors of the two sets of alternate boundary coefficients for the hexagons of Theorem 5 are equal.

This is not true, however, of the octagons of Theorem 6, since, in particular,

$$\begin{pmatrix} \begin{pmatrix} 5\\1 \end{pmatrix}, & \begin{pmatrix} 8\\2 \end{pmatrix}, & \begin{pmatrix} 9\\4 \end{pmatrix}, & \begin{pmatrix} 6\\3 \end{pmatrix} \end{pmatrix} = 1, \\ \begin{pmatrix} \begin{pmatrix} 6\\1 \end{pmatrix}, & \begin{pmatrix} 9\\3 \end{pmatrix}, & \begin{pmatrix} 8\\4 \end{pmatrix}, & \begin{pmatrix} 5\\2 \end{pmatrix} \end{pmatrix} = 2,$$

and these are alternate boundary coefficients of such an octagon. Of course, this makes it clear that not all polygons that can be tiled with fundamental hexagons have the equal greatest common divisor property. At the same time, some figures that cannot be tiled with fundamental hexagons appear to have the equal greatest common divisor property. For example, this appears to be true of the octagon of Fig. 11 in [3] though we have no proof of this fact. This leaves the question of the characterization of figures having the equal greatest common divisor property quite open.

5. GENERALIZATIONS AND EXTENSIONS

There are an infinitude of other Pascal-like arrays in which the Hexagon Squares property holds. For example, the Fibonomial triangle and the generalized Fibonomial triangle. If, indeed we replace F_n by $f_n(x)$, the property holds and thus for each x integral yields an infinitude of such arrays. For example, if x = 2, we get the Pell numbers, or every k^{th} Pell Number Sequence works.

REFERENCES

- A. P. Hillman and V. E. Hoggatt, Jr., "On Gould's Hexagon Conjecture, <u>Fibonacci Quar-terly</u>, Vol. 10, No. 6 (Dec. 1972), pp. 561-564.
- V. E. Hoggatt, Jr., and W. Hansell, "The Hidden Hexagon Squares," <u>Fibonacci Quarter-</u> <u>ly</u>, Vol. 9, No. 2 (Apr. 1971), pp. 120, 133.
- 3. Calvin T. Long, "Arrays of Binomial Coefficients whose Products are Squares," <u>Fibon-acci Quarterly</u>, Vol. 11, No. 5 (Dec. 1973), pp. 449-456.
- Carl L. Moore, "More Hidden Hexagon Squares," <u>Fibonacci Quarterly</u>, Vol. 11, No. 5 (Dec. 1973), p. 525.

~~~

(Continued from page 46.)

that

$$F_{8\cdot 3^{n-1}} \equiv 3^{n} \pmod{3^{n+1}}$$
  
$$F_{8\cdot 3^{n-1}-1} \equiv 1 + 3^{n} \pmod{3^{n+1}}$$

Therefore

$$F_{8:3^{n-1}+x} \equiv F_x + 3^n (F_x + F_{x+1}) \pmod{3^{n+1}}.$$

If x satisfies (\*), then either x or  $8 \cdot 3^{n-1} + x$  or  $16 \cdot 3^{n-1} + x$  will be congruent to m modulo  $3^{n+1}$ . Therefore (\*) has solutions for arbitrarily large n.

<u>Problem 2</u>. The number N is said to have complete Fibonacci residues if there exists a solution to the congruence

$$F_x \equiv m \pmod{N}$$

for all integers m. A computer search shows that the only values of  $N \leq 500$  having complete Fibonacci residues are the divisors of

$$3^5$$
,  $2^2 \cdot 5^3$ ,  $2 \cdot 3 \cdot 5^3$ ,  $5 \cdot 3^4$ , or  $7 \cdot 5^3$ .

Determine all N which have complete Fibonacci residues.

Problem 3 is submitted by the undersigned and Leonard Carlitz, Duke University, Durham, North Carolina.

<u>Problem 3.</u> Show that if  $= e^{\pi i/n}$ , then

(Continued on page 82.)

# ON DAYKIN'S ALGORITHM FOR FINDING THE G.C.D.

V. C. HARRIS San Diego State College, San Diego, California 92115

In a recent issue of the Fibonacci Quarterly, Daykin [1] has given an algorithm for finding the greatest common divisor of two positive integers. The process can be obtained by changing the signs in Euclid's algorithm (using subtraction in Euclid's algorithm instead of addition, as possibly Euclid may have done [2]) and taking numbers modulo  $10^{k}$ , where k is the number of digits in the larger of the two numbers whose g. c. d. is being obtained. It appears, then, that the number of additions required is the sum of the quotients in Euclid's method; also, that any modulus (larger than the numbers whose g. c. d. is being obtained) may be used in place of  $10^{k}$ .

To illustrate this, we have Daykin's example and, on the right, the modification of Euclid's as suggested above. To find (2847, 1168):

| 2847 | (+88 <b>32</b> ) | -2847 | (+1168) |
|------|------------------|-------|---------|
| 1679 | (+8832)          | -1679 | (+1168) |
| 511  |                  | -511  |         |
| 8832 | (+511)           | -1168 | (+511)  |
| 9343 | (+511)           | -657  | (+511)  |
| 9854 |                  | -146  |         |
| 511  | (+9854)          | -511  | (+146)  |
| 365  | (+9854)          | -365  | (+146)  |
| 219  | (+9854)          | -219  | (+146)  |
| 73   |                  | -73   |         |
| 9854 | (+73)            | -146  | (+73)   |
| 9927 | (+73)            | -73   | (+73)   |
| 0    |                  | 0     |         |

Hence (2847, 1168) = 73.

#### REFERENCES

- 1. D. E. Daykin, "An Addition Algorithm for Greatest Common Divisor," <u>Fibonacci Quar</u>terly, Vol. 8, No. 3 (Oct., 1970), pp. 347-349.
- Donald E. Knuth, <u>The Art of Computer Programming</u>, Addison-Wesley Pub. Co., Vol. 2, pp. 293-337.

►

## STUFE OF A FINITE FIELD

#### SAHIB SINGH Clarion State College, Clarion, Pennsylvania 16214

## INTRODUCTION

Stufe of a field is connected with the property of integer -1 in that field. It is defined to be the least integer s such that  $-1 = \alpha_1^2 + \alpha_2^2 + \cdots + \alpha_3^2$ , where each  $\alpha_1$  belongs to the field. In [2] Chowla and Chowla have determined the stufe of a cyclotomic field. Pfister has shown in [3] that the stufe of a finite field is  $\leq 2$ . Our aim is to elaborate this result further. We do this in the following theorem.

<u>Theorem</u>. Stufe of  $GF(p^n)$ , where p is prime and  $n \ge 1$ , is always one except for the case when n is odd and  $p \equiv 3 \pmod{4}$ , in which case its value is two.

<u>Proof.</u> We know that the non-zero elements of  $GF(p^n)$ , denoted by  $GF^*(p^n)$ , form a cyclic multiplicative group. Also, it is well known that if G is a cyclic group of order k and m divides k, then there exists a unique subgroup of order m in G. Since (p - 1) divides  $(p^n - 1)$  for all n, therefore it follows that the members of  $GF^*(p)$  constitute the unique subgroup of order (p - 1) in  $GF^*(p^n)$ . Now we develop the proof by considering different cases.

<u>Case 1</u>. Let p = 2. If  $\lambda$  is a generator of  $GF^*(2^n)$ , then  $\lambda^{(2^n-1)} = 1$ , which means that  $\lambda^{2^n} = \lambda$  implying that  $\lambda$  is a square which enables us to conclude that each element of  $GF^*(2^n)$  is a square and thus -1 is a square. In the subsequent cases, p is understood to be an odd prime.

<u>Case 2</u>. Let n be even. From the above analysis it is clear that if  $\lambda$  is a generator of  $GF^*(p^n)$ , then

$$\lambda \left( \frac{p^n - 1}{p - 1} \right)$$

is a primitive root mod p. In view of the values of p and n we conclude that

$$\left(\frac{p^n-1}{p-1}\right)$$

is even, which again means that this primitive root mod p is a square implying that -1 is a square.

Case 3. Let n be odd. In this case,

$$\frac{p^n - 1}{p - 1}$$

## STUFE OF A FINITE FIELD

is odd. Thus half the members of  $GF^*(p)$  which are quadratic residues mod p would be squares and the remaining half are not. If  $p \equiv 1 \pmod{4}$ , it is well known that (-1) is a quadratic residue mod p and hence is a square. If  $p \equiv 3 \pmod{4}$ , then (-1) is a quadratic non-residue mod p and therefore is not a square. In this case -1 is the sum of two squares, which easily follows from (3) or (4).

#### REFERENCES

- 1. G H. Hardy and E. M. Wright, <u>An Introduction to the Theory of Numbers</u>, Oxford University Press, London, 1965.
- 2. P. Chowla and S. Chowla, "Determination of the Stufe of Certain Cyclotomic Fields," Journal of Number Theory, Vol. 2 (1970), pp. 271-272.
- Albert Pfister, "Zur Darstellung Von I Als Summe Von Quadraten in einem Körper," Journal of London Math. Society, Vol. 40 (1965), pp. 159-165.
- 4. Sahib Singh, "Decomposition of Each Integer as Sum of Two Squares in a Finite Integral Domain," to appear in the Indian Journal of Pure and Applied Mathematics.

5. B. L. Van Der Waerden, Algebra, Vol. 1, Frederick Ungar Pub. Co., N. Y., 1970.

(Continued from page 79.)

$$L_{n} = \prod_{k=1}^{\lfloor n/2 \rfloor} (\omega^{2k-1} + 3 + \omega^{-2k+1})$$

(ii)

(i)

$$F_{n} = \prod_{k=1}^{\lfloor n/2 \rfloor} (\omega^{2k} + 3 + \omega^{-2k}) .$$

Donald E. Knuth Professor Stanford University Stanford, California 94305

#### FIBONACCI CURIOSITY

#### The THIRTEENTH PERFECT NUMBER is built on the prime $p = 521 = L_{13}$

## $2^{520}(2^{521} - 1)$ .

<u>~`~</u>~~~

Brother Alfred Brousseau

# **ITERATION ALGORITHMS FOR CERTAIN SUMS OF SQUARES**

#### EDGAR KARST University of Arizona, Tuscon, Arizona 85721

The following three-step iteration algorithm to generate x simultaneously in  $2x + 1 = a^2$  and  $3x + 1 = b^2$  was mentioned, but not proved, in [4, p. 211]:

| 1.10 - 1      | = | 9     | $9^2$              | = | 81         | (81 - 1)/2         | = | $40 = x_1$         |
|---------------|---|-------|--------------------|---|------------|--------------------|---|--------------------|
| 9.10 - 1      | = | 89    | 89 <sup>2</sup>    | = | 7921       | (7921 - 1)/2       | = | $3960 = x_2$       |
| 89.10 - 9     | = | 881   | $881^{2}$          | = | 776161     | (776161 - 1)/2     | = | $388080 = x_3$     |
| 881.10 - 89   | = | 8721  | $8721^{2}$         | = | 76055841   | (76055841 - 1)/2   | = | $38027920 = x_4$   |
| 8721.10 - 881 | = | 86329 | 86329 <sup>2</sup> | = | 7452696241 | (7452696241 - 1)/2 | = | $3726348120 = x_5$ |

<u>Proof.</u> From  $2x + 1 = a^2$  and  $3x + 1 = b^2$  comes  $3a^2 - 2b^2 = 1$ . If  $a_n$ ,  $b_n$  is any solution of this generalized Pell equation, then  $a_{n+1} = 5a_n + 4b_n$ ,  $b_{n+1} = 6a_n + 5b_n$  is the next larger one. From these, we obtain immediately  $a_{n+1} + a_{n-1} = 10a_n$ ,  $b_{n+1} + b_{n-1} = 10b_n$ , which is equivalent to the algorithm.

For the n<sup>th</sup> term formula we use the usual approach by linear substitutions (for example, [1, p. 181]) and obtain

$$x_{n} = \left[ (\sqrt{6} + 2)(5 + 2\sqrt{6})^{n} + (\sqrt{6} - 2)(5 - 2\sqrt{6})^{n} \right]^{2} / 48 - 1/2 .$$

This formula has three shortcomings: (1) it uses fractions, (2) it employs roots, and (3) it has n in the exponent. The algorithm above has none of them.

Similar arguments are valid for a four-step iteration algorithm [3] to generate  $\,x\,$  in  $\,x^2$  +  $(x\,+\,1)^2\,=\,y^2$  .

Sometimes, the n<sup>th</sup> term formula may be simple, as for  $a^2 + b^2 + (ab)^2 = c^2$ , a and b consecutive positive integers [2]. Here we have

$$(n - 1)^2 + n^2 + [(n - 1)n]^2 = (n^2 - n + 1)^2$$
,

and hence we need no algorithm. But for a = 1 an algorithm would be helpful. Let us first find some clues to such an algorithm. We have by hand and by a table of squares:

 The alternating +1 and -1 in the last column, which shows a constant pattern, suggests the possibility of an algorithm. If we can find all b, say, from  $b_3 = 12$  on, we will also have all c. After some trials and errors, we obtain

Iteration Algorithm 1  $6 \cdot 2 - 0 = 12$   $6 \cdot 12 - 2 = 70$   $6 \cdot 70 - 12 = 408$   $6 \cdot 408 - 70 = 2378$   $6 \cdot 2378 - 408 = 13860$  $6 \cdot 13860 - 2378 = 80782$ 

which yields easily the next four results:

Similarly, we approach the case a = 2. We have by hand and a table of squares:

 $2^{2} + 1^{2} + 2^{2} = 3^{2} = (1^{2} + 2)^{2}$   $2^{2} + 3^{2} + 6^{2} = 7^{2} = (3^{2} - 2)^{2}$   $2^{2} + 8^{2} + 16^{2} = 18^{2} = (4^{2} + 2)^{2}$   $2^{2} + 21^{2} + 42^{2} = 47^{2} = (7^{2} - 2)^{2}$ 

The alternating +2 and -2 in the last column, which shows a constant pattern, suggests the possibility of an algorithm. If we can find all b, say, from  $b_3 = 8$  on, we will also have all c. After some trials and errors we obtain:

Iteration Algorithm 2

 $3 \cdot 3 - 1 = 8$   $3 \cdot 8 - 3 = 21$   $3 \cdot 21 - 8 = 55$   $3 \cdot 55 - 21 = 144$   $3 \cdot 144 - 55 = 377$  $3 \cdot 377 - 144 = 987$ 

which yields easily the next four results:

Slightly different behaves the case a = 3. We have by hand and a table of squares:

 $3^{2} + 0^{2} + 0^{2} = 3^{2} = (0^{2} + 3)^{2}$   $3^{2} + 2^{2} + 6^{2} = 7^{2} = (2^{2} + 3)^{2}$   $3^{2} + 4^{2} + 12^{2} = 13^{2} = (4^{2} - 3)^{2}$   $3^{2} + 18^{2} + 54^{2} = 57^{2}$   $3^{2} + 80^{2} + 240^{2} = 253^{2} = (16^{2} - 3)^{2}$   $3^{2} + 154^{2} + 462^{2} = 487^{2} = (22^{2} + 3)^{2}$   $3^{2} + 684^{2} + 2052^{2} = 2163^{2}$ 

Here the doubly alternating +3 and -3 in the last column would show a constant pattern, if the exceptional values  $57^2$  and  $2163^2$  could be eliminated. This suggests the possibility of two algorithms. To obtain further results, we write an Integer-FORTRAN program for the IBM 1130 which yields

> $3^2 +$  $3038^2 +$  $9114^2 =$  $9607^2 = (98^2 + 3)^2$  $3^2$  +  $5848^2$  +  $17544^2$  =  $18493^2$  =  $(136^2 - 3)^2$  $3^2$  + 25974<sup>2</sup> +  $77922^2 =$  $82137^{2}$  $3^2$  + 115364<sup>2</sup> +  $346092^2 =$  $364813^2 =$  $(604^2 - 3)^2$  $3^2 + 222070^2 +$  $666210^2 =$  $702247^2 = (838^2 + 3)^2$  $3^2$  +  $986328^2$  +  $2958984^2$  =  $3119043^{2}$  $3^2 + 4380794^2 + 13142382^2 = 13853287^2 = (3722^2 + 3)^2$ .

Now we want to find an algorithm which should generate the sequence 80, 154, 3038, 5848, 115364, 222070, 4380794,  $\cdots$ . Let the terms  $b_1 = 0$ ,  $b_2 = 2$ , and  $b_3 = 4$  be given; then  $b_0 = -4$  is the left neighbor of  $b_1 = 0$ , since  $3^2 + (-4)^2 + (-12)^2 = 13^2 = (4^2 - 3)^2$  is the logical extension to the left. With this trick and some trials and errors, we obtain

Iteration Algorithm 3

 $38 \cdot 2 - (-4) = 80$   $2 \cdot 80 - 2 \cdot 4 + 2 = 154$   $38 \cdot 80 - 2 = 3038$   $2 \cdot 3038 - 2 \cdot 154 + 80 = 5848$   $38 \cdot 3038 - 80 = 115364$   $2 \cdot 115364 - 2 \cdot 5848 + 3038 = 222070$   $38 \cdot 115364 - 3038 = 4380794$ 

Now there remains only to find an algorithm which should generate 25974, 986328,  $\cdots$ . Here we have not far to go, since such an algorithm is already contained in the former one, and we obtain easily

Iteration Algorithm 4 38.684 - 18 = 25974 38.25974 - 684 = 986328

Finally, one could ask: Does there exist a general formula for solving  $x^2 + y^2 + z^2 = w^2$ ? The answer is yes. Let  $x = p^2 + q^2 - r^2$ , y = 2pr, z = 2qr, and  $w = p^2 + q^2 + r^2$ ; then  $x^2 + y^2 + z^2 = w^2$  becomes 0 = 0. But this formula has two shortcomings: (1) it uses fractions, and (2) it employs roots, since, for example, the solution of  $3^2 + 2^2 + 6^2 = 7^2$  requires  $p = \sqrt{2}/2$ ,  $q = 3\sqrt{2}/2$ , and  $r = \sqrt{2}$ .

#### REFERENCES

- Irving Adler, "Three Diophantine Equations," <u>Fibonacci Quarterly</u>, Vol. 6, No. 3 (1968), pp. 360-369; Vol. 7, No. 2 (1969), pp. 181-193.
- 2. E. P. Starke, Elem. Prob. E2151, Amer. Math. Monthly, 76 (1969), p. 187.
- 3. Edgar Karst, "A Four-Step Iteration Algorithm to Generate x in  $x^2 + (x + 1)^2 = y^2$ ," Fibonacci Quarterly, Vol. 7, No. 2 (1969), p. 180.

4. Zentralblatt für Mathematik, 151 (1968), pp. 211-212.

# CERTAIN CONGRUENCE PROPERTIES (MODULO 100) OF FIBONACCI NUMBERS

#### MICHAEL R. TURNER Regis College, Denver, Colorado 80221

<u>Remark</u>. It was originally observed by the author that if p is a prime  $\geq 5$ , then  $\mathbb{F}_{p^2} \equiv p^2 \pmod{100}$ . Further study led to this theorem which characterizes those Fibonacci numbers which terminate in the same last two digits as their indices. The original observation is proved as a corollary to the theorem.

<u>Theorem</u>.  $F_n \equiv n \pmod{100}$  if and only if

 $n \equiv 1, 5, 25, 29, 41$ , or 49 (mod 60) or  $n \equiv 0 \pmod{300}$ .

Proof. From [1], we have the well known formula

(1) 
$$F_n = 2^{1-n} \left[ \binom{n}{1} + 5\binom{n}{3} + 5^2\binom{n}{5} + \dots + 5^{\frac{m-1}{2}}\binom{n}{m} \right] ,$$

where m = n if n is odd, and m = n - 1 if n is even.

<u>Lemma 1</u>.  $F_{60k} \equiv 20k \pmod{100}$ . Proof. Observe that (1) implies

(2) 
$$2^{n-1}F_n \equiv n+5 \frac{n(n-1)(n-2)}{6} \pmod{25}$$
.

From [1], we have for n,  $m \ge 2$ , (n,m) = d implies that  $(F_n, F_m) = F_d$ . Now (2) implies  $2^{60k-1}F_{60k} \equiv 60k + 50k (60k - 1)(60k - 2) \pmod{25}$ , which reduces to  $2^{60k-1}F_{60k} \equiv 10k \pmod{25}$ . Since  $2^{20} \equiv 1 \pmod{25}$ , we get  $F_{60k} \equiv 20k \pmod{25}$ . Since 6 divides 60k, it follows that  $F_6$  divides  $F_{60k}$ . Now  $F_6 = 8$ , so  $F_{60k} \equiv 0 \pmod{4}$ . Combining this with  $F_{60k} \equiv 20k \pmod{25}$ , we get  $F_{60k} \equiv 20k \pmod{4}$ . Combining 1.

We now prove one of the congruences in the theorem.

(3) 
$$n \equiv 1 \pmod{60}$$
 implies  $F_n \equiv n \pmod{100}$ 

<u>Proof.</u> Clearly  $n \equiv 1$  implies  $F_n \equiv n \pmod{100}$ . Assume that for all  $k \leq N$ ,  $n \equiv 60k + 1$  implies  $F_n \equiv n \pmod{100}$ . Now if  $n \equiv 60N + 1$  for <u>even</u> N, then  $n \equiv 120k + 1$  for  $k \equiv N/2 \leq N$ .

From [2], we have the following identity, which will prove extremely useful in what follows.

(4)  $F_{n+m+1} = F_n F_m + F_{n+1} F_{m+1}$ .

In particular,

88

$$F_{120k+1} = F_{60k}^2 + F_{60k+1}^2$$

Using Lemma 1 and induction hypotheses, we get

$$F_n = F_{60k+1}^2 + F_{60k}^2 \equiv (60k + 1)^2 + (20k)^2 \equiv 120k + 1 = n \pmod{100}$$
.

If n = 60N + 1 for <u>odd</u> N, then n = 120k + 60 + 1 for k = (N - 1)/2. Then  $F_n = F_{120k}F_{60} + F_{120k+1}F_{61}$ . Inspection of any large table such as [3] verifies that  $F_{61} =$ 61 (mod 100). Thus, by Lemma 1 and induction hypothesis, we have

$$F_n \equiv 40k \cdot 20 + (120k + 1) \cdot 61 \equiv 120k + 60 + 1 \equiv n \pmod{100}$$
.

This proves the congruence.

into five cases.

Case 1.  $n \equiv 1 \pmod{5}$ .

Assume  $F_n \equiv n \pmod{100}$ . Then  $F_n \equiv n \pmod{4}$  and  $F_n \equiv n \pmod{25}$ . Now (2) implies  $2^{n-1}F_n \equiv n \pmod{25}$ , since

$$5 \frac{n(n - 1)(n - 2)}{6} \equiv 0 \pmod{25}.$$

Also, (5,n) = 1 and  $F_n \equiv n \pmod{100}$ , so we may cancel the n and  $F_n$  to get  $2^{n-1} \equiv 1$ (mod 25). Since 2 belongs to the exponent 20 (mod 25), it follows that  $n \equiv 1 \pmod{20}$ . Thus  $n \equiv 1 \pmod{4}$ . But  $F_n \equiv n \equiv 1 \pmod{4}$ , so  $F_n$  must be odd. But  $F_n$  is even if and only if  $n \equiv 0 \pmod{3}$ , so  $n \equiv 1 \text{ or } 2 \pmod{3}$ . Combining results,

$$\begin{array}{c} n \equiv 1 \pmod{3} \\ n \equiv 1 \pmod{20} \end{array} \right\} n \equiv 1 \pmod{60} \quad \text{or} \quad \begin{array}{c} n \equiv 2 \pmod{3} \\ n \equiv 1 \pmod{20} \end{array} \right\} n \equiv 1 \pmod{60} \quad \text{or} \quad \begin{array}{c} n \equiv 2 \pmod{3} \\ n \equiv 1 \pmod{20} \end{array} \right\} n \equiv 41 \pmod{60} \ .$$

Now suppose that  $n \equiv 41 \pmod{60}$ . Let n = 60k + 41. By Lemma 2,

$$F_n \equiv 20k \cdot F_{40} + (60k + 1)F_{41} \pmod{100}$$
.

By inspection of tables, we have  $F_{40} \equiv 55 \pmod{100}$  and  $F_{41} \equiv 41 \pmod{100}$ . Therefore, we have

$$F_n \equiv (60k + 41) + 20k \cdot 55 \equiv 60k + 41 \equiv n \pmod{100}$$
.

This result, along with (3), completes the proof of Case 1.

Case 2.  $n \equiv 2 \pmod{5}$ .

This case is impossible, for as in Case 1, it follows that  $n \equiv 1 \pmod{20}$ , a contradiction.

Case 3.  $n \equiv 3 \pmod{5}$ . Let n = 3 + 5k. Then from (2),

$$2^{2+5k} F_n \equiv n + n \cdot \frac{5(2 + 5k)(1 + 5k)}{6} \pmod{25}.$$

Assuming  $F_n \equiv n \pmod{100}$ , we may cancel the  $F_n$  and n's, since (n, 25) = 1, obtaining  $3 \cdot 2^{3+5k} \equiv 6 + 5 \cdot 2 \cdot 1 \pmod{25}$ . Thus  $2^{5k+6} \equiv 1 \pmod{25}$ . But this congruence implies  $5k + 6 \equiv 0 \pmod{20}$ , or  $5k \equiv 14 \pmod{20}$ . This congruence is not possible, so case 3 is impossible.

Case 4.  $n \equiv 4 \pmod{5}$ .

Assume  $F_n \equiv n \pmod{100}$ . Let n = 4 + 5k. Then  $3 \cdot 2^{4+5k} \equiv 6 + 5 \cdot 3 \cdot 2 \pmod{25}$ , so  $2^{5k-5} \equiv 1 \pmod{25}$ , and  $5k \equiv 5 \pmod{20}$ . Thus  $n = 5k + 4 \equiv 9 \pmod{20}$ .  $F_n$  and n are therefore odd, so  $n \equiv 1$  or 2 (mod 3). Combining results,

Now suppose that  $n \equiv 29 \pmod{60}$ . Let n = 29 + 60k. By Lemma 2,

$$F_n \equiv F_{60k}F_{28} + F_{60k+1}F_{29} \pmod{100}$$
.

By inspection of tables,  $F_{28} \equiv 11 \pmod{100}$ , and  $F_{29} \equiv 29 \pmod{100}$ . Thus by Lemma 1, we have

 $F_n \equiv 20k \cdot 11 + (60k + 1) \cdot 29 \equiv 60k + 29 \equiv n \pmod{100}$ .

Suppose  $n \equiv 49 \pmod{60}$ . Let n = 49 + 60k. By similar reasoning,

 $F_n \equiv 20k \cdot F_{48} + (60k + 1)F_{49} \equiv 20k \cdot 76 + (60k + 1) \cdot 49 \equiv 60k + 49 \equiv n \pmod{100}$ .

This result completes the proof of Case 4.

Case 5.  $n \equiv 0 \pmod{5}$ .

Let  $n = 5^{S} \cdot k$ , where  $s \ge 1$ , and (5,k) = 1. We shall consider in order the possibilities  $n \equiv 0, 1, 2, and 3 \pmod{4}$ . Assume  $F_n \equiv n \pmod{100}$ . If  $n \equiv 0 \pmod{4}$ , and s = 1, then n = 5k, where (5,k) = 1. Thus we get  $2^{n-1}F_n \equiv n \pmod{25}$  from (2). Now  $F_n \equiv n \equiv 5k \pmod{25}$  implies  $2^{n-1} \cdot 5 \equiv 5 \pmod{25}$ , so  $n \equiv 1 \pmod{4}$ . But in this case, the last result is impossible, so it follows that  $s \ge 2$ . Also, since  $F_n$  must be even, we have  $n \equiv 0 \pmod{3}$ . Finally,  $n \equiv 0 \pmod{5^S}$  implies  $n \equiv 0 \pmod{25}$ . Combining, we have

1974]

 $\left.\begin{array}{cccc} n \equiv 0 \pmod{3} \\ n \equiv 0 \pmod{4} \\ n \equiv 0 \pmod{25} \end{array}\right\} n \equiv 0 \pmod{300} .$ 

Let us suppose that  $n \equiv 0 \pmod{4}$ ; we have  $F_n$  odd, so there are two combinations:

If  $n \equiv 2 \pmod{4}$ , we have

 $\begin{array}{l} n \equiv 0 \pmod{3} \\ n \equiv 2 \pmod{4} \\ n \equiv 0 \pmod{5} \end{array} \right\} n \equiv 30 \pmod{60} .$ 

Let n = 30 + 60k. By Lemmas 1 and 2,

$$F_n = F_{60k+30} \equiv 20kF_{29} + (60k + 1)F_{30} \pmod{100}$$
.

But this reduces to  $F_n \equiv 20k + 40 \pmod{100}$ . Now  $F_n \equiv n \equiv 30 + 60k \pmod{100}$  implies  $20k + 40 \equiv 60k + 30 \pmod{100}$ , or  $40k \equiv 10 \pmod{100}$ , which is impossible. If  $n \equiv 3 \pmod{4}$ , we get two combinations:

The first congruence results in

$$F_n = F_{55+60k} \equiv 40k + 45 \pmod{100}$$
,

and  $F_n \equiv n = 55 + 60k$  implies  $20k \equiv 90 \pmod{100}$ , which is impossible. The second congruence results in

$$F_n = F_{35+60k} \equiv 40k + 65 \pmod{100}$$

and  $F_n \equiv n = 35 + 60k$  implies  $20k \equiv 30 \pmod{100}$ , which is also impossible. Suppose  $n \equiv 5 \pmod{60}$ . Let n = 5 + 60k. Then  $F_n = F_{5+60k}$ , so

$$F_n \equiv 20k \cdot F_4 + (60k + 1) \cdot F_5 \equiv 60k + 5 \equiv n \pmod{100}$$

90

[Feb.

Suppose  $n \equiv 25 \pmod{60}$ . Let n = 25 + 60k. Then

$$F_n = F_{25} + 60k$$
,

 $\mathbf{so}$ 

1974]

$$F_n \equiv 20k \cdot F_{24} + (60k + 1) \cdot F_{25} \equiv 60k + 25 \equiv n \pmod{100}$$

Finally, if  $n \equiv 0 \pmod{300}$ , then 300 divides n, so  $F_{300}$  divides  $F_n$ . By Lemma 1,  $F_{300} \equiv 0 \pmod{100}$ , and thus  $F_n \equiv 0 \equiv n \pmod{100}$ .

This result completes the proof of the theorem.

Corollary. If p is a prime  $\geq 5$ , then  $F_{p^2} \equiv p^2 \pmod{100}$ .

<u>Proof.</u> By the theorem,  $F_5 \equiv 5 \pmod{100}$ . If p is a prime >5, then

 $p \equiv 1, 3, 7, 9, 11, 13, 17, \text{ or } 19 \pmod{20}$ .

Thus  $p^2 \equiv 1$  or 9 (mod 20). Since  $p^2 \equiv 1 \pmod{3}$ , it follows that  $p^2 \equiv 1$  or 49 (mod 60).

#### REFERENCES

1. G. H. Hardy and E. H. Wright, An Introduction to the Theory of Numbers,

- 2. S. L. Basin and V. E. Hoggatt, Jr., "A Primer on the Fibonacci Sequence, Part I," Fibonacci Quarterly, Vol. 1, No. 1 (Feb. 1963), pp. 65-72.
- 3. Dov Jarden, Recurring Sequences, Riveon Lematematika, Jerusalem, Israel, 1958.

**\*\*\*** 

## FIBONACCIAN PATHOLOGICAL CURVES

#### SANTOSH KUMAR Armament Research and Development Establishment, Poona, India

There are many curves which possess peculiar properties not possessed by ordinary curves. These are the so-called "pathological curves" of mathematics. In the present note a few curves which are not normal and healthy and which possess idiosyncrasies have been generated and analyzed. It may be pointed out that these curves cannot be analyzed with the help of ordinary calculus.

We generate Fibonaccian pathological curves as follows. Start with a square with side of length  $H_n$ , where  $H_n$  is the generalized Fibonacci number obtained by the recurrence relation

$$H_n = H_{n-1} + H_{n-2}$$
,  $n > 2$ ,

where  $H_1$  and  $H_2$  are any positive integers. Divide each side of the square into three parts, two of length  $H_{n-2}$  and one part of length  $H_{n-3}$ , as shown in Fig. 1.



Fig. 1

On each section with length  $H_{n-3}$  erect a square outwards. Erase the basic side of this new figure and call this curve  $S_1$ . In  $S_1$ , shown in Fig. 2, we will have the sides of length  $H_{n-2}$  and  $H_{n-3}$ .



Again, each side is divided into three parts. The sides of  $S_1$  will be divided as follows:

$$\begin{split} \mathbf{H}_{n-2} &= \mathbf{H}_{n-4} + \mathbf{H}_{n-5} + \mathbf{H}_{n-4} \\ \mathbf{H}_{n-3} &= \mathbf{H}_{n-5} + \mathbf{H}_{n-6} + \mathbf{H}_{n-5} \,. \end{split}$$

Again we will form a square on the middle part, forming curve  $S_2$  as shown in Fig. 3.

We continue dividing each side into lengths equal to two lower Fibonacci numbers and constructing squares on the middle parts until finally we get sides of length  $H_2$  and  $H_1$ , and have formed the curve S. We called the curve S the Fibonaccian Pathological Curve.

In such a construction, it is of interest to find the total length  $L_r$  and the rate of increase of area  $\triangle A_r$  of the curve  $S_r$  at the r<sup>th</sup> successive subdivision. It can be seen that, for n > 3r,

$$\mathbf{L}_{\mathbf{r}} = 4 \left( 2^{\mathbf{r}} \mathbf{H}_{n-2\mathbf{r}} + {\binom{\mathbf{r}}{1}} 2^{\mathbf{r}-1} \cdot 3\mathbf{H}_{n-2\mathbf{r}-1} + {\binom{\mathbf{r}}{2}} 2^{\mathbf{r}-2} \cdot 3^{2}\mathbf{H}_{n-2\mathbf{r}-2} + \cdots + 3^{\mathbf{r}} \mathbf{H}_{n-3\mathbf{r}} \right)$$
  
$$\Delta \mathbf{A}_{\mathbf{r}} = 4 \left( 2^{\mathbf{r}} \mathbf{H}_{n-2\mathbf{r}-3}^{2} + {\binom{\mathbf{r}}{1}} 2^{\mathbf{r}-1} \cdot 3\mathbf{H}_{n-2\mathbf{r}-4}^{2} + {\binom{\mathbf{r}}{2}} 2^{\mathbf{r}-2} \cdot 3^{2} \mathbf{H}_{n-2\mathbf{r}-5}^{2} + \cdots + 3^{\mathbf{r}} \mathbf{H}_{n-3\mathbf{r}-3}^{2} \right) .$$

It is of interest to note that  $H_1$  and  $H_2$  can be chosen as arbitrarily small positive numbers, and the curve after allowing all successive subdivisions will be a continuous curve which is not differentiable anywhere. It may be noted that an inwards curve can also be

# FIBONACCIAN PATHOLOGICAL CURVES

Feb. 1974



generated on similar lines, but, due to lack of symmetry, the expression for obtaining the total area after r successive subdivisions is difficult to obtain.

~~

\$

## IRREDUCIBILITY OF LUCAS AND GENERALIZED LUCAS POLYNOMIALS

GERALD E. BERGUM South Dakota State University, Brookings, South Dakota 57006 and VERNER E. HOGGATT, JR. San Jose State University, San Jose, California 95192

## 1. INTRODUCTION

In [5], Webb and Parberry discuss several divisibility properties for the sequence  $\{F_n(x)\}$  of Fibonacci polynomials defined recursively by

(1) 
$$F_0(x) = 0$$
,  $F_1(x) = 1$ ,  $F_{n+2}(x) = xF_{n+1}(x) + F_n(x)$ ,  $n \ge 0$ .

In particular, Webb and Parberry prove that  $F_p(x)$  is irreducible over the integral domain of the integers if and only if p is a prime.

In [1], Bergum and Kranzler develop many relationships which exist between the sequence  $\{F_n(x)\}$  of Fibonacci polynomials and the sequence  $\{L_n(x)\}$  of Lucas polynomials defined recursively by

(2) 
$$L_0(x) = 2$$
,  $L_1(x) = x$ ,  $L_{n+2}(x) = xL_{n+1}(x) + L_n(x)$ ,  $n \ge 0$ .

Specifically, Bergum and Kranzler show that

(3) 
$$L_n(x) \mid L_m(x)$$
 iff  $m = (2k - 1)n, k \ge 1.$ 

With n = 1, we see that  $x | L_n(x)$  for all odd integers m so that the result of Webb and Parberry does not hold for the sequence  $\{L_n(x)\}$ .

In [4], Hoggatt and Long show that the result of Webb and Parberry does hold for the sequence  $\{U_n(x,y)\}$  of generalized Fibonacci polynomials defined by the recursion

$$(4) \quad U_0(x,y) = 0, \quad U_1(x,y) = 1, \quad U_{n+2}(x,y) = xU_{n+1}(x,y) + yU_n(x,y), \quad n \ge 0.$$

The purpose of this paper is to obtain necessary and sufficient conditions for the irreducibility of the elements of the sequence  $\{L_n(x)\}$  as well as the elements of the sequence  $\{V_n(x, y)\}$  of generalized Lucas polynomials defined by the recursion

(5) 
$$V_0(x,y) = 2$$
,  $V_1(x,y) = x$ ,  $V_{n+2}(x,y) = xV_{n+1}(x,y) + yV_n(x,y)$ ,  $n \ge 0$ .

The first few terms of the sequence  $\left\{ \, V_{n}^{}(x,y) \right\}$  are

| n | V <sub>n</sub> (x, y)                                    |
|---|----------------------------------------------------------|
| 1 | х                                                        |
| 2 | $x^2 + 2y$                                               |
| 3 | $x^3 + 3xy$                                              |
| 4 | $x^4 + 4x^2y + 2y^2$                                     |
| 5 | $x^5 + 5x^3y + 5xy^2$                                    |
| 6 | $x^{6} + 6x^{4}y + 9x^{2}y^{2} + 2y^{3}$                 |
| 7 | $x^7 + 7x^5y + 14x^3y^2 + 7xy^3$                         |
| 8 | $x^{8} + 8x^{6}y + 20x^{4}y^{2} + 16x^{2}y^{3} + 2y^{4}$ |
| 9 | $x^9 + 9x^7y + 27x^5y^2 + 30x^3y^3 + 9xy^4$ .            |

Observe that  $L_n(x) = V_n(x, 1)$  so that with y = 1, we also have the first nine terms of the sequence  $\{L_n(x)\}$ .

# 2. IRREDUCIBILITY OF L<sub>n</sub>(x)

The basic fact that we shall use is found in [2, p. 77] and is Theorem 2.1. (Eisenstein's irreducibility criterion.) For a given prime p, let

$$F(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

be any polynomial with integral coefficients such that

 $a_{n-1} \equiv a_{n-2} \equiv \cdots \equiv a_0 \equiv 0 \pmod{p}, a_n \neq 0 \pmod{p}, a_0 \neq 0 \pmod{p^2}$ 

then F(x) is irreducible over the field of rationals.

To establish our first irreducibility theorem, we use the following.

Lemma 2.1. Every coefficient of  $L_{2n}(x)$ , except for the leading coefficient, is divisible by 2 and 4 does not divide the constant term.

<u>Proof.</u> If n = 1 then  $L_2(x) = x^2 + 2$  and the lemma is obviously true. Assume the lemma is true for n.

In [1], we find

(6) 
$$L_{2k}(x) = L_k^2(x) - 2(-1)^K$$
  
Hence,  
(7)  $L_{2n+1}(x) = L_{2n}^2(x) - 2$ .

By the induction hypothesis, it is obvious that  $L_{2^{n+1}}(x)$  is monic and every coefficient of  $L_{2^{n+1}}(x)$  is divisible by 2. Furthermore, since  $L_{2^n}(x)$  has constant term +2 we see that  $L_{2^n}^2(x)$  has constant term +4, thus  $L_{2^{n+1}}(x)$  has constant term +2. Therefore, the constant term of  $L_{2^{n+1}}(x)$  is divisible by 2 but not by 4 and the lemma is proved.

An immediate result of Lemma 2.1 with the aid of Theorem 2.1 is

Theorem 2.2. The Lucas polynomial  $L_{2k}(x)$  is irreducible over the rationals for  $k \ge 1$ . Although  $L_p(x)$  is not irreducible if p is a prime, we can show that  $L_p(x)/x$  is irreducible for every odd prime p.

97

First we note, as is pointed out in [1], that

(8) 
$$L_n(x) = \alpha^n + \beta^n ,$$

where  $\alpha = (x + \sqrt{x^2 + 4})/2$  and  $\beta = (x - \sqrt{x^2 + 4})/2$ . Hence, if n = 2m + 1 we have

$$\begin{split} \mathbf{L}_{n}(\mathbf{x}) &= (\mathbf{x} + \sqrt{\mathbf{x}^{2} + 4})^{n} / 2^{n} + (\mathbf{x} - \sqrt{\mathbf{x}^{2} + 4})^{n} / 2^{n} \\ &= 2^{-n} \Biggl( \sum_{k=0}^{n} \binom{n}{k} \mathbf{x}^{n-k} (\mathbf{x}^{2} + 4)^{k/2} + \sum_{k=0}^{n} \binom{n}{k} (-1)^{k} \mathbf{x}^{n-k} (\mathbf{x}^{2} + 4)^{k/2} \Biggr) \\ &= 2^{-(n-1)} \sum_{k=0}^{m} \binom{n}{2k} \mathbf{x}^{n-2k} (\mathbf{x}^{2} + 4)^{k} \\ &= 2^{-(n-1)} \sum_{k=0}^{m} \sum_{s=0}^{k} \binom{n}{2k} \binom{k}{s} \mathbf{x}^{n-2s} 2^{2s} . \end{split}$$

Therefore,

(9)

(10) 
$$L_n(x)/x = 2^{-(n-1)} \sum_{k=0}^m \sum_{s=0}^k {n \choose 2k} {k \choose s} x^{n-2s-1} 2^{2s}, \quad n = 2m + 1.$$

For each s,  $0 \le s \le m$ , we see that the coefficient of  $x^{n-2s-1}$  is

(11) 
$$2^{-(n-2s-1)} \sum_{k=s}^{m} {n \choose 2k} {k \choose s}, \quad n = 2m + 1$$

When s = 0, we have the leading coefficient of  $L_n(x)$  which is 1 so that

(12) 
$$2^{-(n-1)} \sum_{k=0}^{m} {n \choose 2k} {k \choose 0} = 1, \quad n = 2m + 1.$$

When s = m in (11), we have the constant term of  $L_n(x)$  which is n. If we now let n be an odd prime p and recall that p divides

$$\begin{pmatrix} p\\ 2k \end{pmatrix}$$

# 98 IRREDUCIBILITY OF LUCAS AND GENERALIZED LUCAS POLYNOMIALS [Feb.

if p is a prime, then p is a factor of (11) for each value of s,

$$1 \leq s \leq \frac{(p-3)}{2}$$

Hence, by Eisenstein's criterion, the following is true.

<u>Theorem 2.3.</u> The polynomials  $L_p(x)/x$  are irreducible over the rationals if p is an odd prime.

By (11) and the fact that the coefficients of L (x) are integers, we have Corollary 2.1. If n = 2m + 1 then  $2^{n-2s-1}$  divides

$$\sum_{k=s}^{m} \binom{n}{2k} \binom{k}{s}$$

for any s such that  $0 \le s \le m$ .

Using (3) together with Theorems 2.2 and 2.3, we have

<u>Theorem 2.4</u>. (a) The Lucas polynomials  $L_n(x)$ ,  $n \ge 1$ , are irredicuble over the rationals if and only if  $n = 2^k$  for some integer  $k \ge 1$ .

(b) The polynomials  $L_n(x)/x$ , n odd, are irreducible over the rationals if and only if n is a prime.

# 3. IRREDUCIBILITY OF $V_n(x, y)$

It is a well known fact that

$$U_n(x, y) = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$
,  $n \ge 0$ 

and (14)

$$V_n(x,y) = \alpha^n + \beta^n, \qquad n \ge 0$$
,

where  $\alpha = (x + \sqrt{x^2 + 4y})/2$  and  $\beta = (x - \sqrt{x^2 + 4y})/2$ . In [4], we find

Lemma 3.1. (a) For  $n \ge 0$ ,

$$U_{n}(x,y) = \sum_{k=0}^{\left[\binom{(n-1)}{2}} \binom{n-k-1}{k} x^{n-2k-1} y^{k}.$$

(b) For  $n \ge 0$ ,  $m \ge 0$ ,

$$(U_{m}(x, y), U_{n}(x, y)) = U_{(m, n)}(x, y).$$

Using (13) and (14), a straightforward argument yields

99

Lemma 3.2. (a) 
$$V_n(x, y) = yU_{n-1}(x, y) + U_{n+1}(x, y), \quad n \ge 1$$
;  
(b)  $U_{2n}(x, y) = U_n(x, y)V_n(x, y), \quad n \ge 0$ ;  
(c)  $U_{2n}(x, y)V_{(2k+1)n+1}(x, y) + y^{2n}V_{(2k-1)n}(x, y)$   
 $= V_{(2k+1)n}(x, y)U_{2n+1}(x, y) .$ 

Using (a) of Lemma 3.1 and 3.2, we have, for  $n \ge 1$ , that

$$V_{n}(x, y) = \sum_{k=0}^{\left[(n-2)/2\right]} {\binom{n-k-2}{k}} x^{n-2k-2} y^{k+1} + \sum_{k=0}^{\left[n/2\right]} {\binom{n-k}{k}} x^{n-2k} y^{k}$$

$$(15) = \sum_{k=1}^{\left[n/2\right]} {\binom{n-k-1}{k-1}} x^{n-2k} y^{k} + \sum_{k=0}^{\left[n/2\right]} {\binom{n-k}{k}} x^{n-2k} y^{k}$$

$$= \sum_{k=1}^{\left[n/2\right]} {\binom{n-k-1}{k-1}} \frac{n}{k} x^{n-2k} y^{k} + x^{n}.$$

Hence,

<u>Lemma 3.3</u>. (a) For  $n \ge 1$ ,  $V_n(x, y^2)$  is homogeneous of degree n.

(b) If n is odd then x is a factor of  $V_n(x,y^2)$  and  $V_n(x,y^2)/x$  is homogeneous of degree  $\,n$  – 1.

By (b) of Lemma 3.1,  $(U_{2n}(x, y), U_{2n+1}(x, y)) = 1$ . Using this fact together with (b) of Lemma 3.2 and induction on k in (c) of Lemma 3.2, one obtains

<u>Lemma 3.4</u>. If  $k \ge 1$  then  $V_n(x,y) | V_{(2k-1)n}(x,y)$ .

In [3, p. 376, Problem 5], we find

Lemma 3.5. A homogeneous polynomial f(x, y) over a field F is irreducible over F if and only if the corresponding polynomial f(x, 1) is irreducible over F.

Using Lemmas 3.3 and 3.5 with Theorem 2.4, we have

<u>Theorem 3.1</u>. (a) The polynomials  $V_n(x, y^2)$  are irreducible over the rationals if and only if  $n = 2^k$  for some integer  $k \ge 1$ .

(b) The polynomials  $V_n(x, y^2)/x$ , n odd are irreducible over the rationals if and only if n is an odd prime.

Since f(x, y) is irreducible if  $f(x, y^2)$  is irreducible and x is a factor of  $V_n(x, y)$  for n odd by (15), we apply Lemma 3.4 and Theorem 3.1 to obtain

<u>Theorem 3.2.</u> (a) The polynomials  $V_n(x, y)$  are irreducible over the rationals if and only if  $n = 2^k$  for some integer k greater than or equal to one.

(b) The polynomials  $V_n(x,y)/x$ , n odd, are irreducible over the rationals if and only if n is an odd prime.

Letting y = 1 and n = 2m + 1 in (15), we see that

(16) 
$$L_{n}(x)/x = \sum_{k=1}^{m} {\binom{n-k-1}{k-1}} \frac{n}{k} x^{n-2k-1} + x^{n-1}$$

Comparing the coefficients of  $x^{n-2s-1}$  in (16),  $1 \le s \le m$ , with the result obtained in (11), we have

Corollary 3.1. If n = 2m + 1 and  $1 \le s \le m$  then

$$2^{-(n-2s-1)} \sum_{k=s}^{m} {n \choose 2k} {k \choose s} = {n - s - 1 \choose s - 1} \frac{n}{s}$$

#### REFERENCES

- 1. G. Bergum and A. Kranzler, Linear Recurrences-Identities and Divisibility Properties, unpublished.
- 2. G. Birkhoff and S. MacLane, A Survey of Modern Algebra, The MacMillan Company, New York, N Y., 1965.
- 3. G. Birkoff and S. MacLane, Algebra, The MacMillan Company, New York, N. Y., 1967.
- 4. V. E. Hoggatt, Jr., and C. T. Long, "Divisibility Properties of Generalized Fibonacci Polynomials," Fibonacci Quarterly, to appear April, 1974.
- 5. W. A. Webb and E. A. Parberry, "Divisibility Properties of Fibonacci Polynomials," Fibonacci Quarterly, Vol. 7 (Dec. 1969), pp. 457-463.

## ELEMENTARY PROBLEMS AND SOLUTIONS

Edited by A. P. HILLMAN University of New Mexico, Albuquerque, New Mexico 87131

Send all communications regarding Elementary Problems and Solutions to Professor A. P. Hillman, Dept. of Mathematics and Statistics, University of New Mexico, Albuquerque, New Mexico 87131. 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 four months of the publication date.

#### DEFINITIONS

The Fibonacci numbers 
$$F_n$$
 and the Lucas numbers  $L_n$  satisfy  
 $F_{n+2} = F_{n+1} + F_n$ ,  $F_0 = 0$ ,  $F_1 = 1$  and  $L_{n+2} = L_{n+1} + L_n$ ,  $L_0 = 2$ ,  $L_1 = 1$ .

#### PROBLEMS PROPOSED IN THIS ISSUE

B-274 Proposed by C. B. A. Peck, State College, Pennsylvania.

Approximate  $(\sqrt{5} - 1)/2$  to within 0.002 using at most three distinct familiar symbols. (Each symbol may represent a number or an operation and may be repeated in the expression.)

B-275 Proposed by Warren Cheves, Littleton, North Carolina.

Show that

$$F_{mn} = L_m F_{m(n-1)} + (-1)^{m+1} F_{m(n-2)}$$

B-276 Proposed by Graham Lord, Temple University, Philadelphia, Pennsylvania. Find all the triples of positive integers m, n, and x such that

 $F_{b} = x^{m}$  where  $h = 2^{n}$  and m > 1.

- *B-277* Proposed by Paul S. Bruckman, University of Illinois, Chicago Circle, Ill. Prove that  $L_{2n(2k+1)} \equiv L_{2n} \pmod{F_{2n}}$ .
- B-278 Proposed by Paul S. Bruckman, University of Illinois, Chicago Circle, Ill.

Prove that  $L_{(2n+1)(4k+1)} \equiv L_{2n+1} \pmod{F_{2n+1}}$ .

B-279 Proposed by Richard M. Grassl, University of New Mexico, Albuquerque, New Mexico.

Find a closed form for the coefficient of  $x^n$  in the Maclaurin series expansion of

$$(x + 2x)/(1 - x - x^2)^2$$
.

# SOLUTIONS SEVEN DO'S FOR TWO SUSY'S

B-250 Proposed by Guy A.R. Guillotte, Montreal, Quebec, Canada.

## DO YOU LIKE SUSY

In this alphametic, each letter stands for a particular but different digit, nine digits being shown here. What do you make of the perfect square sum SUSY ?

Solution by Raymond E. Whitney, Lock Haven State College, Lock Haven, Pa.

There are four possible SUSY's. They are 2025, 3136, 6561, 8281. SUSY = 2025 leads to the six solutions shown below:

| 76   | 86   | 49   | 89   | 98   | 48          |
|------|------|------|------|------|-------------|
| 560  | 560  | 590  | 590  | 580  | 58 <b>0</b> |
| 1389 | 1379 | 1386 | 1346 | 1347 | 1397        |
| 2025 | 2025 | 2025 | 2025 | 2025 | 2025        |

SUSY = 3136 leads to one solution:

# $57 \\ 671 \\ 2408 \\ \overline{3136}$

The other two 4-digit numbers lead to no solutions. Thus the likelihood is that SUSY = 2025 and she is definitely 2025 or 3136.

Also solved by Richard Blazej, Donald Braffitt, Paul S. Bruckman, Juliana D. Chan, Warren Cheves, Herta T. Freitag, Ralph Garfield, Myron Hlynka, J. A. H. Hunter, John W. Milsom, C. B. A. Peck, Jim Pope, Richard W. Sielaff, Charles W. Trigg, Lawrence Williams, David Zeitlin, and the Proposer.

#### FAIR GAME

B-251 Proposed by Paul S. Bruckman, San Rafael, California.

A and B play a match consisting of a sequence of games in which there are no ties. The odds in favor of A winning any one game is m. The match is won by A if the number of games won by A minus the number won by B equals 2n before it equals -n. Find m in terms of n given that the match is a fair one, i.e., the probability is 1/2 that A will win the match.

# 1974] ELEMENTARY PROBLEMS AND SOLUTIONS

Solution by Dennis Staples, The American School in Japan, Tokyo, Japan.

The game specifies that A wins whenever A's wins - B's wins reaches 2n before it reaches -n. Said another way, A wins whenever A's wins - B's wins + n reaches 3n before it reaches 0.

Recalling the notion of Markov chains, let u(i) be the probability that A reaches 3n (in other words, wins), given that i = A's wins - B's wins + n. Using techniques designed for solution of Markov chain problems, it can be found that

$$u(i) = \frac{\left(\frac{1 - m}{m}\right)^{i} - \left(\frac{1 - m}{m}\right)^{3n}}{1 - \left(\frac{1 - m}{m}\right)^{3n}} .$$

Since A and B begin competition when i = n, and since A's chances of winning are to be 1/2,

$$\frac{1}{2} = \frac{\left(\frac{1-m}{m}\right)^n - \left(\frac{1-m}{m}\right)^{3n}}{1 - \left(\frac{1-m}{m}\right)^{3n}}$$

$$1 - \left(\frac{1-m}{m}\right)^{3n} = 2\left(\frac{1-m}{m}\right)^n - 2\left(\frac{1-m}{m}\right)^{3n}$$

$$\left(\frac{1-m}{m}\right)^{3n} - 2\left(\frac{1-m}{m}\right)^n + 1 = 0$$

This is a rather familiar equation, and it can be easily shown that the roots, (1 - m)/m, are equal to the following when n = 1:

$$-1, \quad \frac{-1 + \sqrt{5}}{2}, \quad \text{or} \quad \frac{-1 - \sqrt{5}}{2}$$

.

Of these values, only  $(-1 + \sqrt{5})/2 = 0.618 \cdots$  is acceptable in the case we are considering. Thus, when n = 1,

$$\frac{1 - m}{m} = 0.618 \cdots$$

$$1 - m = (0.618 \cdots) m$$

$$m = \frac{1}{1.618 \cdots} = 0.618 \cdots$$

For the general case,

m = 
$$\left(\frac{1}{1.618\cdots}\right)^{1/n}$$
 =  $(0.618\cdots)^{1/n}$ 

Also solved by Ralph Garfield and the Proposer.

## SOMEWHAT ALTERNATING SUM OF TRINOMIALS

B-252 Proposed by Wray G. Brady, Slippery Rock State College, Slippery Rock, Pennsylvania.

Prove that

$$\sum_{i+j+k=n} \frac{(-1)^{k}}{i! \; j! \; k!} = \frac{1}{n!}$$

Solution by Harvey J. Hindin, Dix Hills, New York.

The multinomial theorem (G. Chrystal, <u>Textbook of Algebra</u>, Part 2, Dover Reprint, New York, 1961, page 12), may be stated as:

(1) 
$$(x + y + z)^n = \sum_{i+j+k=n} \frac{n!}{i! j! k!} x^i y^j z^k$$
.

If we let x = y = 1, and z = -1, we have:

(2) 
$$(1 + 1 - 1)^n = 1 = n! \sum_{i+i+k=n} \frac{(-1)^k}{i!j!k!}$$

 $\mathbf{or}$ 

(3) 
$$\sum_{i+j+k=n} \frac{(-1)^{k}}{i! \, j! \, k!} = \frac{1}{n!} \qquad Q. E. D.$$

Problem 34, page 20 of Chrystal is similar.

Also solved by Paul S. Bruckman, Michael Capobianco, Timothy B. Carroll, Herta T. Freitag, Ralph Garfield, Lawrence D. Gould, Myron Hlynka, Graham Lord, C. B. A. Peck, Raymond E. Whitney, David Zeitlin, and the Proposer.

## TRINOMIAL EXPANSION WITH F'S AND L'S

B-253 Proposed by Wray G. Brady, Slippery Rock State College, Slippery Rock, Pennsylvania.

Prove that

[Feb.

$$\sum_{i+j+k=n} \frac{(-1)^{k} L_{j+2k}}{i! \; j! \; k!} = 0 = \sum_{i+j+k=n} \frac{(-1)^{k} F_{j+2k}}{i! \; j! \; k!}$$

Solution by C. B. A. Peck, State College, Pennsylvania.

In the trinomial expansion

$$\sum_{i+j+k=n} x^{i} y^{j} z^{k} \binom{n}{i,j,k} = (x + y + z)^{n}$$

where

$$\binom{n}{i,j,k} = n! / i! j! k!$$

with i + j + k = n, let x = 1,  $y = \alpha(\beta)$ ,  $z = -\alpha^2(-\beta^2)$ . From the Binet formulas, the two expressions are proportional to  $(1 + \alpha - \alpha^2)^n \pm (1 + \beta - \beta^2)^n = 0^n \pm 0^n = 0$ .

<u>Comment.</u> A number of solvers pointed out that the F's or L's could be replaced by generalized Fibonacci numbers.

Also solved by Paul S. Bruckman, Timothy B. Carroll, Herta T. Freitag, Ralph Garfield, Harvey J. Hindin, Graham Lord, David Zeitlin, and the Proposer.

#### MORE OR LESS LUCAS

B-254 Proposed by Clyde A. Bridger, Springfield, Illinois.

Let  $A_n = a^n + b^n + c^n$  and  $B_n = d^n + e^n + i^n$ , where a, b, and c are the roots of  $x^3 - 2x - 1$  and d, e, and f are the roots of  $x^3 - 2x^2 + 1$ . Find recursion formulas for the  $A_n$  and for the  $B_n$ . Also express  $B_n$  in terms of  $A_n$ .

Solution by Graham Lord, Temple University, Philadelphia, Pennsylvania.

The roots of  $x^3 - 2x - 1$  are -1,  $\alpha$ ,  $\beta$  and of  $x^3 - 2x^2 + 1$  are 1,  $\alpha$ ,  $\beta$  where  $\alpha$ ,  $\beta$  have their usual (Fibonacci) meaning. Hence if  $L_n$  is the n<sup>th</sup> Lucas number, then

$$A_n = (-1)^n + L_n$$
 and  $B_n = 1 + L_n$ 

Consequently from the properties of  $L_n$  for  $n \ge 0$ :

$$\begin{aligned} A_{n+3} &= 2A_{n+1} + A_n , \\ B_{n+3} &= 2B_{n+2} - B_n , \end{aligned}$$

and

1974]

105

 $B_{n} = \begin{cases} A_{n} & n \text{ even} \\ A_{n} + 2 & n \text{ odd} \end{cases}$ 

 $\mathbf{or}$ 

106

$$B_n = A_n + 1 - (-1)^n Q. E. D.$$

Also solved by Richard Blazej, Paul S. Bruckman, Timothy B. Carroll, Herta T. Freitag, Ralph Garfield, Robert McGee and Juliana D. Chan, Raymond E. Whitney, Gregory Wulczyn, David Zeitlin, and the Proposer.

#### FIBONACCI CONVOLUTION REVISITED

B-255 Proposed by L. Carlitz and Richard Scoville, Duke University, Durham, North Carolina.

Show that

$$\sum_{2k \le n} k \binom{n - k}{k} = \sum_{k=0}^{n} F_k F_{n-k} = [(n - 1)F_{n+1} + (n + 1)F_{n-1}]/5$$

Solution by C. B. A. Peck, State College, Pennsylvania.

The l.h. result is proved by Carlitz in the <u>Fibonacci Quarterly</u>, Vol. VII, No. 3, pp. 285-286 (proposed by Hoggatt as H-131 in Vol. VI, No. 2, p. 142), so we confine ourselves to the r.h. result (stated by Wall in Vol. I, No. 4, p. 28). The result for n = 0 is just  $F_0F_{0=0} = 0.0 = 0 = [-1.1 + 1.1]/5 = [(0 - 1)F_{0+1} + (0 + 1)F_{0-1}]/5$ . and for n = 1 is  $F_0F_{1-0} + F_1F_{1-1} = 0.1 + 1.0 = 0 = [0.2 + 2.0]/5 = [(1 - 1)F_{1+1} + (1 + 1)F_{1-1}]/5$ . Suppose the result true for all n up to some  $m \ge 1$ . Then

$$\sum_{k=0}^{m+1} F_k F_{m+1-k} = \sum_{k=0}^{m} F_k F_{m-k} + \sum_{k=0}^{m-1} F_k F_{m-1-k} + F_{m+1} F_{m+1-(m+1)} + F_m F_{m-1-m}$$
$$= [(m - 1)F_{m+1} + (m + 1)F_{m-1} + (m - 2)F_m + mF_{m-2} + F_m 5]/5$$
$$= [m F_{m+2} + (m + 2)F_m]/5 ,$$

so that by the Second Principle of Finite Induction, the right-hand result is true.

Also solved by Paul S. Bruckman, Timothy B. Carroll, Herta T. Freitag, Ralph Garfield, Phil Tracy, and the Proposer.
## ADVANCED PROBLEMS AND SOLUTIONS

# Edited by RAYMOND E. WHITNEY Lock Haven State College, Lock Haven, Pennsylvania 17745

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-230 Proposed by Gregory Wulczyn, Bucknell University, Lewisburg, Pa.

(a) If 5 is a quadratic nonresidue of a prime p (p  $\neq$  5), then p | F<sub>k(p+1)</sub>, k a positive integer.

(b) If 5 is a quadratic residue of a prime p, then  $p|F_{k(p-1)}$ , k a positive integer.

H-231 Proposed by L. Carlitz, Duke University, Durham, North Carolina.

1. Let  $A_0 = 0$ ,  $A_1 = 1$ ,  $\begin{cases} A_{2k+1} &= A_{2k} + A_{2k-1} \\ A_{2k+2} &= A_{2k+1} - A_{2k} \end{cases}.$ Find A<sub>n</sub>.  $\begin{array}{l} {\rm A}_{\rm n}. \\ {\rm 2. \ Let \ B_0 = 2, \ B_1 = 3,} \\ \\ {\rm A}_{\rm 2k+1} = {\rm B}_{2k} + {\rm B}_{2k-1} \\ {\rm B}_{2k+2} = {\rm B}_{2k+1} - {\rm B}_{2k} \end{array} . \end{array}$ 

Find B<sub>n</sub>.

H-232 Proposed by R. Garfield, the College of Insurance, New York, New York.

Define a sequence of polynomials,  $\left\{ \, \mathrm{G}_{k}(x) \right\}_{k=0}^{\infty}$  as follows:

$$\frac{1}{1 - (x^2 + 1)t^2 - xt^3} = \sum_{k=0}^{\infty} G_k(x) t^k .$$

- 1. Find a recursion formula for  $G_k(x)$ .
- 2. Find  $G_k(1)$  in terms of the Fibonacci numbers.
- 3. Show that when x = 1, the sum of any 4 consecutive G numbers is a Lucas number.

H-233 Proposed by A. G. Shannon, NSW Institute of Technology, Broadway, and The University of New England, Armidale, Australia.

 $\label{eq:constraint} The notation of \ensuremath{\, Carlitz}^* \mbox{ suggests the following generalization of Fibonacci numbers. Define$ 

$$f_n^{(r)} = (a^{nk+k} - b^{nk+k})/(a^k - b^k)$$
,

where k = r - 1, and a, b are the zeros of  $x^2 - x - 1$ , the auxiliary polynomial of the ordinary Fibonacci numbers,  $f_n^{(2)}$ .

Show that

$$\sum_{n=0}^{\infty} f_n^{(r)} x^n = 1/(1 - (a^k + b^k)x + (a^k b^k)x^2) .$$

Let  $f_k = (a^{k+1} - b^{k+1})/(a - b)$ , and prove that

(b)

(a)

$$f_{n}^{(r)} = \sum_{0 \leq m+s \leq n} {m \choose s} {n-m \choose s} f_{k-1}^{2s} f_{k-2}^{m-s} f_{k}^{n-m-s} .$$

(Note that when r = 2 (and so k = 1),  $f_k$  =  $f_{k-1}$  = 1,  $f_{k-2}$  = 0, and (b) reduces to the well known

$$f_n^{(2)} = \sum_{0 \le 2m \le n} {n - m \choose m} .$$

# SOLUTIONS SUCCESS!

# BUCCEBB.

Editorial Note. We previously listed H-61, H-73, and H-77 as unsolved. However, this is incorrect. H-61 is solved in Vol. 5, No. 1, pp. 72-73. H-73 is solved in Vol. 5, No. 3, pp. 255-256. H-77 is solved in Vol. 5, No. 3, pp. 256-258.

#### ANOTHER OLDIE

H-62 Proposed by H. W. Gould, West Virginia University, Morgantown, W. Va.

Find all polynomials f(x) and g(x), of the form

$$f(x + 1) = \sum_{j=0}^{r} a_{j} x^{j}, \quad a_{j} \text{ an integer,}$$

<sup>\*</sup>L. Carlitz, "The Characteristic Polynomial of a Certain Matrix of Binomial Coefficients," Fibonacci Quarterly, Vol. 3 (1965), pp. 81-89.

$$g(x) = \sum_{j=0}^{s} b_j x^j$$
,  $b_j$  an integer,

such that

$$\begin{split} 2 \Big\{ x^2 f^3(x + 1) &- (x + 1)^2 g^3(x) \Big\} &+ 3 \Big\{ x^2 f^2 (x + 1) - (x + 1)^2 g^2(x) \Big\} \\ &+ 2 (x + 1) \Big\{ x f(x + 1) - (x + 1) g(x) \Big\} = 0 \;. \end{split}$$

H-87 Proposed by Monte Boisen, Jr., San Jose State University, San Jose, Calif.

Show that, if

$$u_0 = u_2 = u_3 = \cdots = u_{n-1} = 1$$

and

$$u_k = u_{k-1} + u_{k-2} + \cdots + u_{k-n}$$
  $k \ge n$ ,

then

$$\frac{1 - x^2 - 2x^3 - \dots - (n - 2)x^{n-1}}{1 - x - x^2 - \dots - x^n} = \sum_{k=0}^{\infty} u_k x^k .$$

Solution by Clyde A. Bridger, Springfield, Illinois.

Write

$$g(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_{n-1} x^{n-1} ,$$
  

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$
  

$$g/f = q(x) = A_0 + A_1 x + A_2 x^2 + \dots + A_n x^n + A_{n+1} x^{n+1} + \dots$$

and

where  $a_0$  and  $a_n$  are not zero, at least one  $c_i$  is not zero, and f(x) = 0 has no multiple roots.

Then g/f generates a recurrence of length n, as is at once apparent by either long division or by equating coefficients of like powers of x in  $g(x) = f(x) \cdot q(x)$ . The first n A's depend entirely on the c's, as the following set of equations shows.

$$c_{0} = a_{0}A_{0}$$

$$c_{1} = a_{0}A_{1} + a_{1}A_{0}$$

$$c_{2} = a_{0}A_{2} + a_{1}A_{1} + a_{2}A_{0}$$

$$\vdots \vdots \vdots \vdots \vdots \vdots \vdots \vdots \vdots$$

$$c_{n-1} = a_{0}A_{n-1} + a_{1}A_{n-2} + \dots + a_{n-1}A_{0}$$

$$0 = a_{0}A_{n} + a_{1}A_{n-1} + \dots + a_{n}A_{0}$$

$$\vdots \vdots \vdots$$

$$0 = a_{0}A_{k} + a_{1}A_{k-1} + \dots + a_{k}A_{0} \quad (k \ge n)$$

$$\vdots \vdots \vdots$$

109

,

1974]

Beginning with the  $(n + 1)^{st}$  equation,  $A_n$  can be expressed directly in terms of the n - 1 preceding A's. The general term  $A_k$  for any  $k \ge n$  provides the formula or difference equation that the fraction g/f generates.

To solve the given problem, one sets  $c_0 = 1$  and  $c_i = -(n - 1)$  for i = 1 to i = n - 11,  $a_0 = 1$ ,  $a_i = -1$  for i = 1 to n, and  $A_i = u_i$ .

### FIT TO A "T"

H-197 Proposed by Lawrence Somer, University of Illinois, Urbana, Illinois.

Let

$$\left\{ u_{n}^{\left( t\right) }\right\} _{n=1}^{\infty}$$

be the t-Fibonacci sequences with positive entries satisfying the recursion relationship:

$$u_n^{(t)} = \sum_{i=1}^t u_{n-i}$$

Find

$$\lim_{\substack{t \to \infty \\ n \to \infty}} \frac{u_{n+1}^{(t)}}{u_n^{(t)}}$$

Solution by the Proposer.

By analyzing the convergents of continued fractions, one can easily see that for any fixed t, and any initial entries,  $u_1^{(t)}$ ,  $u_2^{(t)}$ ,  $\cdots$ ,  $u_t^{(t)}$ , (t)

$$\lim_{n \to \infty} \frac{u_{n+1}^{(t)}}{u_{n}^{(t)}}$$

will be a constant. Let

$$u_1^{(t)} = 1, \quad u_2^{(t)} = 2, \quad \cdots, \quad u_t^{(t)} = 2^t$$

For this choice we have

$$u_{t+1}^{(t)} = 2^{t+1} - 1$$
 and  $u_{t+2}^{(t)} = 2^{t+2} - 3$ .

Let

$$\psi = \lim_{n \to \infty} \frac{u_{n+1}^{(t)}}{u_n^{(t)}}$$

If one examines the convergents of the continued fractions, he finds

$$\frac{u_{t+1}^{(t)}}{u_t^{(t)}} < \psi < \frac{u_{t+2}^{(t)}}{u_{t+1}^{(t)}}$$

for large enough n. Thus

$$\frac{2^{t+1}-1}{2^t} < \psi < \frac{2^{t+2}-3}{2^{t+1}-1}$$

 $\mathbf{or}$ 

$$2 - \frac{1}{2^{t}} < \psi < 2 - \frac{1}{2^{t+1} - 1}$$

and

$$\lim_{t \to \infty} \psi = 2.$$

It thus follows that the desired limit is 2.

Also solved by P. Tracy and one unsigned solver.

### PELL-MELL

H-198 Proposed by E. M. Cohn, National Aeronautics and Space Administration, Washington, D.C.

There is an infinite sequence of square values for triangular numbers,\*

$$k^2 = m(m + 1)/2$$
.

Find simple expressions for k and m in terms of Pell numbers,  $P_n (P_{n+2} = 2P_{n+1} + P_n,$ where  $P_0 = 0$  and  $P_1 = 1$ ).

Solution by the Proposer.

Since (m, m + 1) = 1, the odd factor must be a square, say  $(2s + 1)^2$ . Then the even factor is  $(2s^2 + 2s)$  or  $(2s^2 + 2s + 1)$ . (After division by 2.)

Let  $k^2/(2s + 1)^2 = q^2$ , so that either

$$2s^2 + 2s - q^2 = 0$$

 $\mathbf{or}$ 

$$2s^2 + 2s + 1 - q^2 = 0$$

Solving for s and re-arranging,

$$(2s + 1)^2 = 2q^2 \pm 1$$
  
k =  $q\sqrt{2q^2 \pm 1}$ 

.

\*A. W. Sylvester, Amer. Math. Monthly, 69 (1962), p. 168.

111

#### 1974]

#### ADVANCED PROBLEMS AND SOLUTIONS

It has been shown\* that  $q_n = P_n$  for Diophantine solutions of such discriminants, and that the discriminant itself equals  $P_{n+1} - P_n$ . Furthermore,  $P_n(P_{n+1} - P_n) = \frac{1}{2}P_{2n}$ . Thus

$$k_n = \frac{1}{2}P_{2n}$$

For even n,

$$m_n = 2 P_n^2 ,$$

and for odd n,

$$m_n = 2P_n^2 \pm 1$$
.

Since even Pell numbers are alternately congruent to  $0 \pmod{4}$  and  $2 \pmod{4}$ , pairs of values of k are of different parity.

Also solved by P. Bruckman, who also solved H-192, H-193, and H-194.

\*E. M. Cohn, submitted to the Fibonacci Quarterly.

#### HERE AT LAST!! - FIBONACCI NOTE SERVICE

The Fibonacci Quarterly is offering a service in which it will be possible for its readers to secure background notes for articles. This will apply to the following:

(1) Short abstracts of extensive results, derivations, and numerical data.

(2) Brief articles summarizing a large amount of research.

(3) Articles of standard size for which additional background material may be obtained. Articles in the Quarterly for which this note service is available will indicate the fact, together with the number of pages in question. Requests for these notes should be made to

> Brother Alfred Brousseau St. Mary's College Moraga, California 94574

The notes will be Xeroxed.

The price for this service is four cents a page (including postage, materials and labor). This service will begin with the April, 1974 issue, coming soon.

 $\sim \sim \sim \sim$