

THE FIBONACCI QUARTERLY

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

VOLUME 13



DALHOUSIE LIBRARY NUMBER 3 DEPT.

CONTENTS

Generalized Convolution Arrays V.E. Hoggatt, Jr., and G.E. Bergum	193
Letter to the Editor	198
A Recursively Defined Divisor Function Michael D. Miller	199
Significance of Even-Oddness	
of a Prime's Penultimate Digit William Raymond Griffin	204
Another Property of Magic Squares	205
On Halsey's Fibonacci Function M. W. Bunder	209
Fibonacci Multi-Multigrades	211
On Fibonacci Numbers of the Form $k^2 + 1 \dots H$. C. Williams	213
The Fibonacci Lattice	215
Compositions with Ones and Twos Krishnaswami Alladi and V.E. Hoggatt, Jr.	233
The Rank of Apparition of a Generalized Fibonacci Sequence H. C. Williams	240
On the Solutions to the Diophantine Equation $x^2 + xy - y^2 = \pm D$,	
or the Number of Fibonacci-Type Sequences	
with a Given CharacteristicBrian Peterson and V.E. Hoggatt, Jr.	243
Enumeration of End-Labeled Trees Abbe Mowshowitz and Frank Harary	252
Approximation of Irrationals	
with Farey Fibonacci Fractions Krishnaswami Alladi	255
A Greatest Integer Theorem for Fibonacci Spaces C. J. Everett	260
Primitive Pythagorean Triples with Sum	
or Difference of Legs Equal to a Prime Delano P. Wegener	263
Special Partitions	278
Products and Powers M. W. Bunder	279
A Special Case of the Generalized Fibonacci	
Sequence Over an Arbitrary Ring with Identity	280
Advanced Problems and Solutions Edited by Raymond E. Whitney	281
Elementary Problems and Solutions Edited by A. P. Hillman	285

OCTOBER

1975

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 Gerald E. Bergum Paul F. Byrd L. Carlitz H. W. Gould A. P. Hillman David A. Klarner Leonard Klosinski Donald E. Knuth C. T. Long M. N. S. Swamy D. E. Thoro

WITH THE COOPERATION OF

Maxey Brooke Bro. A. Brousseau Calvin D. Crabill T. A. Davis Franklyn Fuller A. F. Horadam Dov Jarden L. H. Lange James Maxwell Sister M. DeSales McNabb D. W. Robinson Lloyd Walker Charles H. Wall

The California Mathematics Council

All subscription correspondence should be addressed to Professor Leonard Klosinski, Mathematics Department, University of Santa Clara, Santa Clara, California 95053. All checks (\$12.00 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.

Typeset by HIGHLANDS COMPOSITION SERVICE P.O. Box 760 Clearlake Highlands, Calif, 95422

GENERALIZED CONVOLUTION ARRAYS

V. E. HOGGATT, JR.

San Jose State University, San Jose, California 95192

and

G. E. BERGUM South Dakota State University, Brookings, South Dakota 57006

1. INTRODUCTION

Let

(1.2)

$$\left\{a_n\right\}_{n=1}^{\infty}$$
 and $\left\{b_n\right\}_{n=1}^{\infty}$

be any two sequences, then the Cauchy convolution of the two sequences is a sequence $\{c_n\}_{n=1}^{\infty}$ whose terms are given by the rule

(1.1)
$$c_n = \sum_{k=1}^n a_k b_{n-k+1} .$$

When we convolve a sequence with itself *n* times we obtain a new sequence called the n^{th} convolution sequence. The rectangular array whose columns are the convolution sequences is called a convolution array where the n^{th} column of the convolution array is the $(n - 1)^{st}$ convolution sequence and the first column is the original sequence. In Figure 1, we illustrate the first four elements of the convolution array relative to the sequence $\{u_n\}_{n=1}^{\infty}$

<i>u</i> ₁	U_1^2	U_{1}^{3}	u_1^4	
<i>u</i> ₂	$2u_{1}u_{2}$	$3u_{1}^{2}u_{2}$	$4u_{1}^{3}u_{2}$	
U3	$2u_1u_3 + u_2^2$	$3u_1^2u_3 + 3u_1u_2^2$	$4u_1^3u_3 + 6u_1^2u_2^2$	
U ₄	$2u_1u_4 + 2u_2u_3$	$3u_1^2u_4 + 6u_1u_2u_3 + u_2^3$	$4u_1^3u_4 + 12u_1^2u_2u_3 + 4u_1u_2^3$	

Figure 1

Throughout the remainder of this paper, we let

$$R_{mn}(u_1, u_2, \cdots) \equiv R_{mn}$$

be the element in the m^{th} row and n^{th} column of the convolution array. By mathematical induction, it can be shown that

(1.3)
$$R_{1n} = u_1^n$$
,

$$(1.4) R_{2n} = n u_1^{n-1} u_2,$$

(1.5)
$$R_{3n} = nu_1^{n-1}u_3 + \binom{n}{2}u_1^{n-2}u_2^2$$

(1.6)
$$R_{4n} = n u_1^{n-1} u_4 + 2 \binom{n}{2} u_1^{n-2} u_2 u_3 + \binom{n}{3} u_1^{n-3} u_2^3,$$

$$(1.7) R_{5n} = nu_1^{n-1}u_5 + \binom{n}{2}u_1^{n-2}(u_3^2 + 2u_2u_4) + 3\binom{n}{3}u_1^{n-3}u_2^2u_3 + \binom{n}{4}u_1^{n-4}u_2^4,$$

(1.8)
$$R_{6n} = nu_1^{n-1}u_6 + 2\binom{n}{2}u_1^{n-2}(u_2u_5 + u_3u_4) + 3\binom{n}{3}u_1^{n-3}(u_2^2u_4 + u_2u_3^2) + 4\binom{n}{4}u_1^{n-4}u_2^3u_3 + \binom{n}{5}u_1^{n-5}u_2^5,$$

GENERALIZED CONVOLUTION ARRAYS

$$(1.9) \qquad R_{7n} = nu_1^{n-1}u_7 + \binom{n}{2}u_1^{n-2}(u_4^2 + 2u_3u_5 + 2u_2u_6) + \binom{n}{3}u_1^{n-3}(u_3^3 + 3u_2^2u_5 + 6u_2u_3u_4) \\ + \binom{n}{4}u_1^{n-4}(4u_2^3u_4 + 6u_2^2u_3^2) + 5\binom{n}{5}u_1^{n-5}u_2^4u_3 + \binom{n}{6}u_1^{n-6}u_2^6 , \\ (1.10) \qquad R_{8n} = nu_1^{n-1}u_8 + 2\binom{n}{2}u_1^{n-2}(u_2u_7 + u_3u_6 + u_4u_5) + 3\binom{n}{3}u_1^{n-3}(u_2^2u_6 + 2u_2u_3u_5 + u_2u_4^2 + u_3^2u_4) \\ + 4\binom{n}{4}u_1^{n-4}(u_2^3u_5 + 3u_2^2u_3u_4 + u_2u_3^3) + 5\binom{n}{5}u_1^{n-5}(u_2^4u_4 + 2u_2^3u_3^2) \\ + 6\binom{n}{6}u_1^{n-6}u_2^5u_3 + \binom{n}{7}u_1^{n-7}u_2^7 .$$

The purpose of this article is to examine the general expression for R_{mn} and to find a formula for the generating function for any row of the convolution array.

2. PARTITIONS OF m and R_{mn}

A partition of a nonnegative integer m is a representation of m as a sum of positive integers called parts of the partition. The function $\pi(m)$ denotes the number of partitions of m.

The partitions of the integers one through seven are given in Table 1.

т	Partitions of <i>m</i>	π(m)
1	1	1
2	2, 1 + 1	2
3	3, 1 + 2, 1 + 1 + 1	3
4	4, 2 + 2, 1 + 3, 1 + 1 + 2, 1 + 1 + 1 + 1	4
5	5, 2 + 3, 1 + 4, 1 + 1 + 3, 1 + 2 + 2, 1 + 1 + 1 + 2, 1 + 1 + 1 + 1 + 1	7
6	6, 3 + 3, 2 + 4, 1 + 5, 2 + 2 + 2, 1 + 1 + 4, 1 + 2 + 3, 1 + 1 + 1 + 3,	11
	1 + 1 + 2 + 2, 1 + 1 + 1 + 1 + 2, 1 + 1 + 1 + 1 + 1 + 1	
7	7, 1 + 6, 2 + 5, 3 + 4, 1 + 1 + 5, 1 + 2 + 4, 1 + 3 + 3, 2 + 2 + 3,	
	1 + 1 + 1 + 4, 1 + 1 + 2 + 3, 1 + 2 + 2 + 2, 1 + 1 + 1 + 1 + 3,	15
	1+1+1+2+2 1+1+1+1+1+2 1+1+1+1+1+1+1+1+1	

Comparing the partitions of m, for m = 1 through m = 7, with the expressions for R_{mn} it appears as if the following are true.

- 1. The number of terms in R_{mn} is equal to $\pi(m-1)$. 2. The number of expressions whose coefficient is $\binom{n}{j}$, for $j = 1, 2, \dots, m-1$, is the number of partitions of m-1 into j parts.
- 3. The power of u_{t+1} in an expression is the same as the number of times t occurs in the partition of m-1.
- 4. The numerical coefficient of an expression involving $\binom{n}{j}$, for $j = 1, 2, 3, \dots, m 1$, is equal to the product of the factorials of the exponents of the terms of the sequence

$$\left\{ u_n \right\}_{n=1}^{\infty}$$

in the expression divided into *j* factorial. The exponent for u_1 is not included in the product. In [4], it is shown that these are in fact true statements. That is,

(2.1)
$$R_{mn}(u_1, u_2, \dots) = \sum_{k=1}^{m-1} \binom{n}{k} u_1^{n-k} P_{mk}(u_1, u_2, \dots),$$

where

(2.2)
$$P_{mk}(u_1, u_2, u_3, \dots) = \sum_{\pi(m-1)} \frac{k!}{a_2! a_3! \cdots a_{m-1}!} u_2^{\alpha_2} u_3^{\alpha_3} \cdots u_m^{\alpha_m}, \quad k = a_2 + a_3 + \dots + a_m.$$

3. SOME FINITE DIFFERENCES

The first difference of a function f(x) is defined as

(3.1)
$$\Delta f(x) = f(x+1) - f(x).$$

In an analogous fashion, we define recursively the *n*th difference $\Delta^n f(x)$ of $f(x)$ as

$$(3.2) \qquad \qquad \Delta^n f(x) = \Delta(\Delta^{n-1} f(x)).$$

In [3], we find

(3.3)
$$\sum_{x=0}^{m-1} (-1)^x \binom{m-1}{x} f(x) = (-1)^{m-1} \Delta^{m-1} f(0).$$

Using mathematical induction, it is easy to show the following. Theorem 3.1. If $f(x) = \binom{r-x+s}{j}$ then $\Delta^n f(x) = (-1)^n \binom{r-x+s-n}{j-n}$ and Theorem 3.2. If $f(x) = \binom{r+x+s}{j}$ then $\Delta^n f(x) = \binom{r+x+s}{j-n}$. Applying (3.3), we then have Theorem 3.3. If $f(x) = \binom{r-x+s}{j}$ then $\sum_{x=0}^{m-1} (-1)^x \binom{m-1}{x} \binom{r-x+s}{j} = \binom{r+s-m+1}{j-m+1}$. and Theorem 3.4. If $f(x) = \binom{r+x+s}{j}$ then $\sum_{x=0}^{m-1} (-1)^x \binom{m-1}{x} \binom{r+x+s}{j} = (-1)^{m-1} \binom{r+s}{j-m+1}$.

4. THE MAIN THEOREM

Combining (2.1) with Theorem 3.3., we see that, whenever $u_1 = 1$, we then have

$$\sum_{k=0}^{m-1} (-1)^k \binom{m-1}{k} R_{m,n-k+1} = \sum_{k=0}^{m-1} (-1)^k \binom{m-1}{k} \sum_{j=1}^{m-1} \binom{n-k+1}{j} P_{mj}$$
$$= \sum_{j=1}^{m-1} P_{mj} \sum_{k=0}^{m-1} (-1)^k \binom{m-1}{k} \binom{n-k+1}{j} = \sum_{j=1}^{m-1} P_{mj} \binom{n-m+2}{j-m+2} = P_{m,m-1}.$$

Now, the only way to partition m - 1 into m - 1 parts is to let every part of the partition equal one. Hence, by (2.2), we have

$$P_{m,m-1} = u_2^{m-1}$$

so that

(4.1)
$$\sum_{k=0}^{m-1} (-1)^k \binom{m-1}{k} R_{m,n-k+1} = u_2^{m-1}.$$

From (4.1), it is easy to see that the generating function $g_m(x)$ for the sequence $\left\{ R_{m,n+1} \right\}_{n=0}^{\infty}$, where $u_1 = 1$, is of the form

(4.2)
$$g_m(x) = \frac{h_m(x)}{(1-x)^m} = \sum_{n=0}^{\infty} R_{m,n+1}x^n .$$

In order to determine the generating function $g_m(x)$ for the m^{th} row of the convolution array, it is necessary to determine what is commonly called "Pascal's attic." That is, we need to know the values for the columns corresponding to the negative integers and zero subject to the condition of (4.1). With this in mind, we develop the next two theorems.

195

1975]

GENERALIZED CONVOLUTION ARRAYS

Theorem 4.1. If $m \ge 2$ and $u_1 = 1$ then $R_{m,0} = 0$.

Proof. Letting n = m - 2 in (4.1), we have

196

$$(-1)^{m-1}R_{m,o} = \sum_{k=0}^{m-2} (-1)^{k+1} {\binom{m-1}{k}} R_{m,m-k+1} + u_2^{m-1} = \sum_{k=1}^{m-1} (-1)^{m-k} {\binom{m-1}{m-k-1}} R_{mk} + u_2^{m-1} = \sum_{k=1}^{m-1} (-1)^{m+k} {\binom{m-1}{k}} R_{mk} + u_2^{m-1} .$$

By (2.1), using j as the variable of summation, and Theorem 3.4 with r = s = 0, we obtain

$$(-1)^{m-1} R_{m,0} = \sum_{k=1}^{m-1} (-1)^{m+k} {\binom{m-1}{k}} \sum_{j=1}^{m-1} {\binom{k}{j}} P_{mj} + u_2^{m-1}$$
$$= (-1)^m \sum_{j=1}^{m-1} P_{mj} \sum_{k=0}^{m-1} (-1)^k {\binom{m-1}{k}} {\binom{k}{j}} + u_2^{m-1}$$
$$= -\sum_{j=1}^{m-1} P_{mj} {\binom{0}{j-m+1}} + u_2^{m-1} = -P_{m,m-1} + u_2^{m-1} = 0$$

and the theorem is proved.

Theorem 4.2. If $n \ge 1$, $m \ge 2$ and $u_1 = 1$ then

$$R_{m,-n} = \sum_{k=1}^{m-1} (-1)^k \left(\begin{array}{c} n+k-1 \\ k \end{array} \right) P_{mk}$$

Proof. We shall use the strong form of mathematical induction.

Replacing n by m - 3 in (4.1) and following the argument of Theorem 4.1 where we let r = 0 and s = -1 in Theorem 3.4, we have

$$(-1)^{m-1} R_{m,-1} = \sum_{k=0}^{m-2} (-1)^{k+1} {\binom{m-1}{k}} R_{m,m-k-2} + u_2^{m-1} = \sum_{k=1}^{m-1} (-1)^{m+k} {\binom{m-1}{k}} R_{m,k-1} + u_2^{m-1}$$
$$= (-1)^m \sum_{j=1}^{m-1} P_{mj} \sum_{k=1}^{m-1} (-1)^k {\binom{m-1}{k}} {\binom{k-1}{j}} + u_2^{m-1}$$
$$= (-1)^m \sum_{j=1}^{m-1} P_{mj} \sum_{k=0}^{m-1} (-1)^k {\binom{m-1}{k}} {\binom{k-1}{j}} - (-1)^m \sum_{j=1}^{m-1} P_{mj} {\binom{-1}{j}} + u_2^{m-1}$$
$$= -\sum_{j=1}^{m-1} P_{mj} {\binom{-1}{j-m+1}} - (-1)^m \sum_{j=1}^{m-1} P_{mj} {\binom{-1}{j}} + u_2^{m-1}.$$

Reca ıg

$$\begin{pmatrix} -n \\ m \end{pmatrix} = (-1)^m \begin{pmatrix} n+m-1 \\ m \end{pmatrix}$$

if $n \ge 1$, and $m \ge 0$ and $\begin{pmatrix} n \\ -m \end{pmatrix} = 0$ for all n provided $m \ge 1$, we have
 $m-1$

1

١

$$(-1)^{m-1}R_{m,-1} = -P_{m,m-1} - (-1)^m \sum_{j=1}^{m-1} (-1)^j P_{mj} + u_2^{m-1}$$

.

ŕ

so that

$$R_{m,-1} = \sum_{j=1}^{m-1} (-1)^j P_{mj}$$

and the theorem is true for n = 1.

We now assume that the theorem is true for all positive integers less than or equal to t. Replacing n by m - t - 3in (4.1), we see that

$$(-1)^{m-1} R_{m,-(t+1)} = \sum_{k=0}^{m-2} (-1)^{k+1} {\binom{m-1}{k}} R_{m,m-t-k-2} + u_2^{m-1}$$
$$= \sum_{k=1}^{m-1} (-1)^{m+k} {\binom{m-1}{k}} R_{m,-(t-k+1)} + u_2^{m-1}$$
$$= \sum_{j=1}^{m-1} (-1)^{m+j} P_{mj} \sum_{k=1}^{m-1} (-1)^k {\binom{m-1}{k}} {\binom{t-k+j}{j}} + u_2^{m-1}$$

where the last equation is obtained by the induction hypothesis. Multiplying by $(-1)^{m-1}$ and introducing k = 0, one has

$$\begin{split} R_{m,-(t+1)} &= \sum_{j=1}^{m-1} (-1)^{j-1} P_{mj} \sum_{k=0}^{m-1} (-1)^k \binom{m-1}{k} \binom{t-k+j}{j} + \sum_{j=1}^{m-1} (-1)^j \binom{t+j}{j} P_{mj} + (-u_2)^{m-1} \\ &= \sum_{j=1}^{m-1} (-1)^{j-1} P_{mj} \binom{t+j-m+1}{j-m+1} + \sum_{j=1}^{m-1} (-1)^j \binom{t+j}{j} P_{mj} + (-u_2)^{m-1} \\ &= \sum_{j=1}^{m-1} (-1)^j \binom{t+j}{j} P_{mj} , \end{split}$$

where the second equation is obtained by use of Theorem 3.3 with r = t and s = j and the theorem is proved. We are now in a position to calculate the generating function for the m^{th} row of a convolution array when $u_1 = 1$. When m = 1, we see that $R_{1,n} = 1$ for all $n \ge 0$ so that

(4.3)
$$g_1(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x} .$$

By (4.1), we have

$$R_{m,n+1} = \sum_{k=1}^{m-1} (-1)^{k+1} \binom{m-1}{k} R_{m,n-k+1} + u_2^{m-1}$$

so that when $m \ge 2$, we can use (4.2) to obtain

$$g_m(x) = \sum_{n=0}^{\infty} \sum_{k=1}^{m-1} (-1)^{k+1} \binom{m-1}{k} R_{m,n-k+1} x^n + \sum_{n=0}^{\infty} u_2^{m-1} x^n = \sum_{k=1}^{m-1} (-1)^{k+1} \binom{m-1}{k} x^k \times \frac{m-1}{k} x^{m-1} x^{$$

$$\left(\sum_{n=0}^{\infty} R_{m,n-k+1} x^{n-k} + \frac{u_2^{m-1}}{1-x}\right) = \sum_{k=1}^{m-1} (-1)^{k+1} \binom{m-1}{k} x^k \left(g_m(x) + \sum_{n=1}^{k-1} R_{m,-n} x^{-n-1}\right) + \frac{u_2^{m-1}}{1-x}$$

GENERALIZED CONVOLUTION ARRAYS

Hence,

(4.4)
$$g_m(x) = \frac{(1-x)\sum_{k=1}^{m-1}\sum_{n=1}^{k-1}(-1)^{k+1}\binom{m-1}{k}R_{m,-n}x^{k-n-1} + u_2^{m-1}}{(1-x)^m}, \quad m \ge 2$$

For special sequences

 $\left\{ u_n \right\}_{n=1}^{\infty}$

with $u_1 = 1$, the polynomial in the numerator of $g_m(x)$, $m \ge 1$, is predictable from the convolution array of the sequence. This matter will be covered by the authors in another paper which will appear in the very near future.

REFERENCES

- 1. V.E. Hoggatt, Jr., and Marjorie Bicknell, "Convolution Triangles for Generalized Fibonacci Numbers," *The Fibonacci Quarterly*, Vol. 8, No. 2 (April 1970), pp. 158–171.
- 2. V.E. Hoggatt, Jr., and Marjorie Bicknell, "Convolution Triangles," *The Fibonacci Quarterly*, Vol. 10, No. 6 (December 1972), pp. 599-609.
- 3. Charles Jordan, Calculus of Finite Differences, Chelsea Publishing Co., 1947, pp. 131–132.

4. John Riordan, Combinatorial Identities, John Wiley and Sons, Inc., 1968, pp. 188–191.

LETTER TO THE EDITOR

February 20, 1975

Dear Mr. Hoggatt:

I'm afraid there was an error in the February issue of *The Fibonacci Quarterly*. Mr. Shallit's proof that phi is irrational is correct up to the point where he claims that $1/\phi$ can't be an integer. He has no basis for making that claim, as ϕ was defined as a rational number, not an integer.

The proof can, however, be salvaged after the point where p is shown to equal 1. Going back to the equation $p^2 - pq = q^2$, we can add pq to each side, and factor out a q from the right: $p^2 = q(q + p)$. Using analysis similar to Mr. Shallit's, we find that q must also equal 1. Therefore, $\phi = p/q = 1/1 = 1$. However, $\phi^2 - \phi - 1 = -1 \neq 0$; thus, our assumption was false, and ϕ is irrational.

Sincerely, s/David Ross, Student, Swarthmore College

OCT. 1975

A RECURSIVELY DEFINED DIVISOR FUNCTION

MICHAEL D. MILLER

University of California, Los Angeles, California 90024

INTRODUCTION

In this paper, we shall investigate the properties of a recursively defined number-theoretic function γ , paying special attention to its fixed points. An elementary acquaintance with number theory and linear recurrence relations is all that is required of the reader.

Throughout the discussion, p, q, r, s, t, p_1 , p_2 , \cdots will denote prime numbers.

THE FUNCTION γ

We define a function γ on the positive integers by setting $\gamma(1) = 1$, and for N > 1,

$$\gamma(N) = \sum_{d \mid N, d < N} \gamma(d).$$

Example 1:

(1) If p is prime, $\gamma(p) = 1$.

(2) $\gamma(4) = \gamma(1) + \gamma(2) = 2$.

 $(3) \ \gamma(12) = \gamma(1) + \gamma(2) + \gamma(3) + \gamma(4) + \gamma(6) = \gamma(1) + \gamma(2) + \gamma(3) + [\gamma(1) + \gamma(2)] + [\gamma(1) + \gamma(2) + \gamma(3)] = 8.$

The following theorem clearly follows from the definition of γ .

Theorem 1. $\gamma(N)$ depends only on the structure of the prime factorization of N.

That is, if $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_h^{\alpha_h}$, $\gamma(N)$ is independent of the particular primes p_i , and depends only on the set a_1, a_2, \cdots, a_h of exponents. For example, $\gamma(12) = \gamma(20) = \gamma(75)$ since 12, 20, and 75 are each of the form p^2q . By actually determining the divisors of N, we obtain the following results:

N	$\gamma(N)$	N	$\gamma(N)$	N	$\gamma(N)$
р	1	<i>р</i> ⁴	8	p⁴q	48
p²	2	$p^{3}q$	20	p^3q^2	76
pq	3	p^2q^2	26	p³qr	132
р ³	4	p ² qr	44	p^2q^2r	176
p²q	8	pgrs	75	p ² qrs	308
nar	13	D ⁵	16	parst	541

If $N = \rho_1^{\alpha_1} \cdot \rho_2^{\alpha_2} \cdot \dots \cdot \rho_h^{\alpha_h}$, we define the *exponent* of N to be

$$\sum_{i=1}^{h} a_i$$

We now derive expressions for $\gamma(N)$ in a few simple cases, and then proceed to determine the general form. Theorem 2. $\gamma(p^n) = 2^{n-1}$.

Theorem 2.
$$\gamma(p^n) = 2^{n-1}$$
.
Proof. For $n = 1$, the theorem clearly holds. Assume it true for $n = k$. Thus $\gamma(p^k) = 2^{k-1}$. Now,
 $\gamma(p^{k+1}) = \gamma(1) + \gamma(p) + \dots + \gamma(p^k) = 2\gamma(p^k) = 2^k$,

since

$$\gamma(1)+\gamma(p)+\ldots+\gamma(p^{k-1})\,=\,\gamma(p^k).$$

Theorem 3.
$$\gamma(p^n q) = (n+2) \cdot 2^{n-1}$$
.

Proof. $\gamma(p^n q) = \gamma(1) + \gamma(p) + \dots + \gamma(p^{n-1}) + \gamma(q) + \gamma(pq) + \dots + \gamma(p^{n-1}q) + \gamma(p^n) = 2\gamma(p^{n-1}q) + \gamma(p^n).$ Let $a_n = \gamma(p^n q)$. Then

$$a_n - 2a_{n-1} = \gamma(p^n) = 2^{n-1}$$
.

We solve this linear recurrence (using the fact that $a_0 = 1$) to obtain the desired result.

Before proceeding, it will be valuable to make the following observation. If $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_h^{\alpha_h}$, then

$$\gamma(N) = \sum_{d \mid N, d < N} \gamma(d)$$

is a sum involving two types of terms: those involving divisors of N which have $p_1^{\alpha_1}$ as a factor, and those which do not. The sum of all terms of the latter type we recognize as $2\gamma(p_1^{\alpha_1-1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_h^{\alpha_h})$. Each of the remaining terms is of the form $\gamma(p^n d)$, where d properly divides $p_2^{\alpha_2} \cdot \dots \cdot p_h^{\alpha_h}$. Moreover, in each case, d has lower exponent than that of $N/p_1^{\alpha_1}$.

This observation leads us to a proof by induction on the exponent of N in order to find an expression for $\gamma(N)$. We first look at the following example.

Example 2.
$$\gamma(p^n q^2) = 2\gamma(p^{n-1} q^2) + \gamma(p^n) + \gamma(p^n q).$$

Using Theorems 2 and 3, and letting $a_n = \gamma(p^n q^2)$, we rewrite this equation as

$$a_n - 2a_n = 2^{n-1} + (n+2)2^{n-1}$$

Noting that $a_0 = \gamma(q^2) = 2$, we solve to find $a_n = (n^2 + 7n + 8)2^{n-2}$.

An

Using this example and observation as motivation, we now derive the general form of $\gamma(N)$ for any N.

Theorem 4. Let

$$A_n = p_1^n \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_h^{\alpha_h}$$

where a_2, a_3, \dots, a_h are fixed. Then

$$\gamma(A_n) = P(n) \cdot 2^n,$$

where P(n) is a polynomial in *n* of degree $e = a_1 + \dots + a_h$ with positive leading coefficient. *Proof.* We shall use induction on *e*. For e = 0, we have

$$= p_1^n$$
 and $\gamma(A_n) = 2^{n-1} = \frac{1}{2} \cdot 2^n$

by Theorem 2. Now assume the theorem true for e < k, and look at $B_n = p_1^n \cdot C$, where C is of exponent k, and p_1 does not divide C. By an earlier observation,

$$\gamma(B_n)-2\gamma(B_{n-1}) = \sum_{i=1}^m \gamma(p_1^n d_i),$$

where d_1, d_2, \dots, d_m are the proper divisors of C. Now each such proper divisor d_i of C in the summation is of exponent less than k. Thus, by the inductive hypothesis, we can rewrite the right-hand side as

$$\sum_{i=1}^{m} P_i(n) \cdot 2^n = P^*(n) \cdot 2^n,$$

where $P_i(n)$ is a polynomial of degree the exponent of d_i , and $P^*(n)$ is a polynomial of degree k - 1 with positive leading coefficient.

Now let $a_n = \gamma(B_n)$. We thus have a non-homogeneous linear recurrence $a_n - 2a_{n-1} = P^*(n) \cdot 2^n$. We try a particular solution of the form $a_n = Q(n) \cdot 2^n$, where Q(n) is a polynomial of degree k. Hence we need

$$Q(n) \cdot 2^n - 2Q(n-1) \cdot 2^{n-1} = P^*(n) \cdot 2^n$$

or $Q(n) - Q(n - 1) = P^*(n)$. This will always have a solution Q(n), of degree k, with positive leading coefficient. Thus $Q(n) \cdot 2^n$ is indeed a particular solution to the above recurrence relation. The general solution is therefore

[OCT.

A RECURSIVELY DEFINED DIVISOR FUNCTION

$$a_n = c \cdot 2^n + Q(n) \cdot 2^n = 2^n (c + Q(n)),$$

where c is a constant. The theorem is proved.

This theorem, although giving much information about the nature of the function γ , does not explicitly give us a formula from which we can calculate $\gamma(N)$ for various values of N. However, it does tell us that once we know $\gamma(p^n d)$ for d with exponent less than k, we can find $\gamma(p^n d^*)$ with d^* of exponent k by solving a relatively simple (yet most times tedious) difference equation.

Doing this for a few simple cases, we obtain the following results:

$$\frac{N}{p^{n}} \frac{2^{n-1}}{2^{n-1}}$$

$$p^{n}q (n+2) \cdot 2^{n-1}$$

$$p^{n}q^{2} \frac{n^{2} + 7n + 8}{2} \cdot 2^{n-1}$$

$$p^{n}q^{3} \frac{n^{3} + 15n^{2} + 56n + 48}{6} \cdot 2^{n-1}$$

$$p^{n}qr (n^{2} + 6n + 6) \cdot 2^{n-1}$$

$$p^{n}q^{2}r \frac{n^{3} + 13n^{2} + 42n + 32}{2} \cdot 2^{n-1}$$

$$p^{n}qrs (n^{3} + 12n^{2} + 36n + 26) \cdot 2^{n-1}$$

Theorem 5. $\gamma(N)$ is odd if and only if N is a product of distinct primes. **Proof.** Recall the definition of γ : $\gamma(1) = 1$, and

$$\gamma(N) = \sum_{d \mid N, d < N} \gamma(d)$$

for N > 1. We cannot directly apply the Mobius inversion formula to γ , since the latter equation does not hold for N = 1. We thus introduce an auxiliary function η defined as follows:

$$\eta(N) = \begin{cases} 1 \text{ if } N = 1\\ 0 \text{ otherwise} \end{cases}$$

Then, for all positive integers N, we have

$$\gamma(N) = \sum_{d \mid N, d < N} \gamma(d) + \eta(N), \quad \text{or} \quad 2[\gamma(N) - \eta(N)] = 2 \sum_{d \mid N, d < N} \gamma(d) = \sum_{d \mid N} \gamma(d) - \eta(N).$$

Let $F(N) = 2\gamma(N) - \eta(N)$. We can now apply the Mobius inversion formula to F(N) to find that

$$\gamma(N) = \sum_{d \mid N} \mu(N/d) F(d) = 2 \sum_{d \mid N} \mu(N/d) \gamma(d) - \sum_{d \mid N} \mu(N/d) \eta(d) = 2\gamma(N) + 2 \sum_{d \mid N, d < N} \mu(N/d) \gamma(d) - \mu(N).$$

From this, we deduce that

$$\gamma(N) = \mu(N) - 2 \sum_{d \mid N, d < N} \mu(N/d) \gamma(d).$$

Clearly, $\gamma(N)$ is odd if and only if $\mu(N) \neq 0$, that is, if and only if N is a product of distinct primes.

SUPER-PERFECT NUMBERS

We will call a positive integer N > 1 super-perfect if $\gamma(N) = N$.

Theorem 6. p^n is never super-perfect.

Proof. In order for p^n to be super-perfect, we would need $p^n = 2^{n-1}$, by Theorem 2. This forces p = 2, and thus a contradiction.

The following theorem assures us of the existence of infinitely many super-perfect numbers.

Theorem 7. $p^n q$ is super-perfect if and only if p = 2 and n + 2 = 2q.

Proof. By Theorem 3, for $p^n q$ to be super-perfect, we need $(n + 2)2^{n-1} = p^n q$. If n > 2, we must then have p = 2, and after cancellation, we get n + 2 = 2q, as required. For n = 0, 1, or 2, the equation leads to a contradiction. Since p and q are distinct, the first q and n for which n + 2 = 2q are q = 3 and n = 4, which gives $2^4 \cdot 3 = 48$ as the first super-perfect number of this form. As it turns out, it is the only super-perfect number less than 1000.

q	n	$N = p^n q$	(p = 2,
3	4	48	
5	8	1280	
7	12	28672	
11	20	11534336	

Theorem 8. $N = p^n q^2$ is never super-perfect.

Proof. From Example 2, we know that

$$\gamma(p^{n}q^{2}) = (n^{2} + 7n + 8) \cdot 2^{n-2}$$

Assume that

$$p^{n}q^{2} = (n^{2} + 7n + 8) \cdot 2^{n-2}$$

For n > 4, this forces p = 2, which leads to $(2q)^2 = n^2 + 7n + 8$. However, we clearly have the inequality

$$(n+3)^2 < n^2 + 7n + 8 < (n+4)^2$$
 for $n > 4$.

Thus no solution exists in this case. If n = 0, 1, 2, 3, or 4, we get $p^n q^2 = 2, 8, 26, 76, 208$, respectively, none of which are possible.

The following theorems are stated without proof, for the proofs follow the same patterns as above.

Theorem 9. $N = p^n q^3$ is never super-perfect.

Theorem 10. $N = p^n qr$ is super-perfect if and only if p = 2, and $2qr = n^2 + 6n + 6$.

q	r	п	$N = p^{n}qr$	(p = 2)
13	3	6	2496	
37	3	12	454656	
13	11	14	2342912	
73	3	18	57409536	

In all cases, we are faced with trying to find values for *n* which make a given polynomial in *n* have a certain prime factorization structure. This is, in general, a very difficult, and in most cases, an unsolved problem.

ODD SUPER-PERFECT NUMBERS

Recall from Theorem 5 that $\gamma(N)$ is odd only when N is a product of distinct primes. We now use various combinatorial methods to prove:

Theorem 11. There are no odd super-perfect numbers.

Proof. Suppose that p_1, p_2, \dots are distinct primes. Let $a_0 = 1$ and $a_i = \gamma(p_1, p_2, \dots, p_i)$, $i = 1, 2, \dots$. Using Theorem 1 to consolidate terms, we find that

$$a_n = \binom{n}{0} a_0 + \binom{n}{1} a_1 + \dots + \binom{n}{n-1} a_{n-1} = \sum_{i=0}^{n-1} \binom{n}{i} a_i.$$

Then

Let

$$\frac{a_n}{n!} = \sum_{i=0}^{n-1} \frac{a_i}{i!(n-i)!}$$

$$b_n = \frac{a_n}{n!}$$
 and $b(x) = b_i x^i$.

 ∞

We thus have

A RECURSIVELY DEFINED DIVISOR FUNCTION

$$b(x) \cdot e^{x} = \sum_{i=0}^{\infty} b_{i} x^{i} \cdot \sum_{j=0}^{\infty} \frac{x^{j}}{j!} = b_{0} + \sum_{n=1}^{\infty} \sum_{i+j=n}^{\infty} \frac{b_{i}}{j!} x^{n} = b_{0} + \sum_{n=1}^{\infty} \left(\sum_{i=0}^{n-1} \frac{b_{i}}{(n-i)!} + b_{n} \right) x^{n} = 2b(x) - b_{0}$$

.

But $a_0 = b_0 = 1$, so we solve to find that

$$b(x) = \frac{1}{2 - e^{x}} = \frac{1}{2} \left(1 + \frac{e^{x}}{2} + \frac{e^{2x}}{4} + \frac{e^{3x}}{8} + \cdots \right).$$

We now expand each term in the infinite sum in powers of x, and then collect coefficients to obtain

$$b(x) = \frac{1}{2} \sum_{n=0}^{\infty} \sum_{i=0}^{\infty} \frac{i^n}{2^i n!} x^n \qquad (0^\circ = 1) \; .$$

Thus

$$b_n = \frac{1}{2} \sum_{i=0}^{\infty} \frac{i^n}{2^i n!}$$
 and $a_n = \frac{1}{2} \sum_{i=0}^{\infty} \frac{i^n}{2^i}$

In order to proceed, we need the following lemma. *Lemma.* For fixed *k*,

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

converges for |x| < 1, and is equal to

$$\frac{P_k(x)}{(1-x)^{k+1}},$$

where $P_k(x)$ is a monic polynomial of degree k with non-negative coefficients.

Proof. The convergence part of the lemma follows immediately from the ratio test. For k = 0, we have

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x} ,$$

so the lemma holds. Assume it true for k = s. Thus

$$f_s(x) = \sum_{n=0}^{\infty} n^s x^n = \frac{P_s(x)}{(1-x)^{s+1}} .$$

Now

$$f_{s+1}(x) = xf'_{s}(x) = \sum_{n=0}^{\infty} n^{s+1}x^{n} = \frac{x(1-x)^{s+1}P'_{s}(x) + x(s+1)P_{s}(x)(1-x)^{s}}{(1-x)^{2s+2}} = \frac{x(1-x)P'_{s}(x) + x(s+1)P_{s}(x)}{(1-x)^{s+2}}$$

It is straightforward to verify that the numerator is indeed a monic polynomial of degree s + 1 with non-negative coefficients. The lemma follows.

Putting $x = \frac{1}{2}$ in the lemma, we find that

$$a_k = \frac{1}{2} \sum_{n=0}^{\infty} \frac{n^k}{2^n} = \frac{\frac{1}{2}P_k(\frac{1}{2})}{(\frac{1}{2})^{k+1}} = 2^k P_k(\frac{1}{2}).$$

Using the fact that $P_0(x) = 1 = 0!$, we can show (via a simple induction argument) that the sum of the coefficients of $P_k(x)$ is k!. Since $P_k(k) < P_k(1)$, we clearly have $a_k < 2^k k!$.

Comparing $2^k k!$ with the product

of the first k odd primes, we see that k = 1 is the lowest k for which

$$2^k k! < \prod_{j=1}^k p_j .$$

But once this inequality holds for one k, it holds for all larger k. For by multiplying each side by 2(k + 1), we get

$$2^{k+1}(k+1)! < \prod_{i=1}^{k} p_i \cdot 2(k+1) < \prod_{i=1}^{k+1} p_i,$$

since $p_{k+1} > 2(k + 1)$. Therefore, for all k,

$$a_k < \prod_{j=1}^k p_j$$

and in particular, a_k is less than any product of k distinct odd primes. We conclude that no product of distinct odd primes can be super-perfect, and the theorem follows.

SIGNIFICANCE OF EVEN-ODDNESS OF A PRIME'S PENULTIMATE DIGIT

WILLIAM RAYMOND GRIFFIN Dallas, Texas

By elementary algebra one may prove a remarkable relationship between a prime number's penultimate (next-to-last) digit's even-oddness property and whether or not the prime, p, is of the form 4n + 1, or $p \equiv 1 \pmod{4}$, or of the form 4n + 3, or $p \equiv 3 \pmod{4}$, where n is some positive integer.

The relationships are as follows:

A. Primes $\equiv 1 \pmod{4}$

(1) If the prime, p, is of the form $10k \pm 1$, k being some positive integer, then the penultimate digit is *even.* (2) If p is of the form $10k \pm 3$, then the penultimate digit is *odd.*

B. Primes \equiv 3 (mod 4)

(1) If p is of the form $10k \pm 1$, then the penultimate digit is *odd*.

(2) If p is of the form $10k \pm 3$, then the penultimate digit is even.

The beauty of these relationships is that, by inspection *alone*, one may instantly observe whether or not a prime number is \equiv 1, or \equiv 3 (mod 4). These relationships are especially valuable for very large prime numbers—such as the larger Mersenne primes.

Thus, it is seen from inspection of the penultimate digits of the Mersenne primes, as given in [1], that all of the given primes are $\equiv 3 \pmod{4}$. This holds true for *all* Mersenne primes, however large they may be, for, by adding and subtracting 4 from $M_p = 2^p - 1$ and re-arranging, we have

$$M_p = 2^p - 1 + 4 - 4 = 2^p - 4 + 3 = 4(2^{p-2} - 1) + 3 \equiv 3 \pmod{4}.$$

[Continued on Page 208.]

ANOTHER PROPERTY OF MAGIC SQUARES

H. S. HAHN West Georgia College, Carrollton, Georgia 30117

1. INTRODUCTION

Consider $n \times n$ matrices $A = [a_{ij}]$ with complex number entries satisfying

(1)
$$\sum_{i} a_{ij} = \sum_{j} a_{ij} = \sum_{i} a_{ii} = \sum_{i} a_{in-i+1}$$

Definition. Call A (multiplicatively) balanced if

(2)
$$\sum_{j} \prod_{i} a_{ij} = \sum_{i} \prod_{j} a_{ij}$$

and completely balanced if

(3)

$$\sum_{j} \prod_{i} (a_{ij} + z) = \sum_{i} \prod_{j} (a_{ij} + z)$$

for all complex number z.

These two properties are explored for n = 3, 4 and 5. Note that magic squares are our main object and there are millions of them which satisfy (1), of order 5 alone.

2. THEOREM

These squares of order 3 are all completely balanced.

Proof. It is well known (see [2]) that (1) implies

$$\begin{bmatrix} a_{ij} \end{bmatrix} = \begin{bmatrix} k+a & k-a-b & k+b \\ k-a+b & k & k+a-b \\ k-b & k+a+b & k-a \end{bmatrix}$$

where k, a, b are arbitrary parameters.

A direct computation can show (2). An easy way to see this is to change (2) into a determinant as follows:

$$\sum_{j} \prod_{i} a_{ij} - \sum_{i} \prod_{j} a_{ij} = \begin{vmatrix} a_{11} & a_{22} & a_{33} \\ a_{23} & a_{31} & a_{12} \\ a_{32} & a_{13} & a_{21} \end{vmatrix} = \begin{vmatrix} k+a & k & k-a \\ k+a-b & k-b & k-a-b \\ k+a+b & k+b & k-a+b \end{vmatrix} = 0$$

because the first row is the average of the other two rows.

However, the majority of magic squares of order n(>3) are not balanced. For example, the famous Dürer's magic square (Fig. 1) is not balanced and the second one (Fig. 2) is balanced and also completely.

An $n \times n$ matrix A, to be completely balanced, all the coefficients of the polynomial in z, say

$$\sum_{i} c_i z^i$$
 ,

obtained from (3) have to be 0. Equation (2) is merely $c_0 = 0$. If $c_0 = 0$, i.e., A is balanced, to determine whether A

			-						7
16	3	2	13		1	14	7	12	
5	10	11	8		15	4	9	6	
9	6	7	12		10	5	16	3	
4	15	14	1_		L 8	11	2	13	L
c.p.	s. = {	3,984	р	.s. =	9,104	Ļ			
r.p.s	. = 1	1,024							
c. p.:	s. for (colum	n-proc						

Figure 1

is further completely balanced it is sufficient to show, by the fundamental theorem of algebra, that the above polynomial is satisfied by any n different values of z. In fact, checking for n - 4 (n > 3) values of z is enough. For: $c_n = n - n = 0$,

$$c_{n-1} = \sum_{j} \sum_{i} a_{ij} - \sum_{i} \sum_{j} a_{ij} = 0,$$

Figure 2

$$\begin{split} c_{n-2} &= \sum_{j} \sum_{i < k} a_{ij} a_{kj} - \sum_{j} \sum_{i < k} a_{ji} a_{jk} = \frac{1}{2} \left[\sum_{j} \sum_{i \neq k} a_{ij} a_{kj} - \sum_{j} \sum_{i \neq k} a_{ji} a_{jk} \right] \\ &= \frac{1}{2} \left[\sum_{i,j} a_{ij} \sum_{k \neq i} a_{kj} - \sum_{i,j} a_{ji} \sum_{k \neq i} a_{jk} \right] = \frac{1}{2} \left[\sum_{i,j} a_{ij} (S - a_{ij}) - \sum_{i,j} a_{ji} (S - a_{ji}) \right] \\ &= \frac{1}{2} \left[S \sum_{i,j} a_{ij} - \sum_{i,j} a_{ij}^{2} - S \sum_{i,j} a_{ji} + \sum_{i,j} a_{ji}^{2} \right] = 0, \end{split}$$

where S is the row (or column) sum, and

$$c_{n-3} = \sum_{t} \left[\sum_{i < j < k} a_{it} a_{jt} a_{kt} - \sum_{i < j < k} a_{tj} a_{tj} a_{tk} \right] = \frac{1}{6} \sum_{t} \left[\sum_{i \neq j} a_{it} a_{jt} (S - a_{it} - a_{jt}) - \sum_{i \neq j} a_{ti} a_{tj} (S - a_{tj} - a_{tj}) \right]$$
$$= \frac{1}{6} \sum_{t} \left[S \sum_{i \neq j} a_{it} a_{jt} - 2 \sum_{i \neq j} a_{it}^{2} a_{jt} - S \sum_{i \neq j} a_{ti} a_{tj} + 2 \sum_{i \neq j} a_{ti}^{2} a_{tj} \right]$$
$$= \frac{1}{6} \sum_{t} \left[S \sum_{i \neq j} (a_{it} a_{jt} - a_{ti} a_{tj}) - 2 \sum_{i} a_{it}^{2} (S - a_{it}) + 2 \sum_{i} a_{ti}^{2} (S - a_{ti}) \right]$$
$$(\text{the first sum is 0 as in } c_{n-2})$$

$$= \frac{1}{3} \sum_{t} \left[S \sum_{i} (a_{ti}^{2} - a_{it}^{2}) + \sum_{i} (a_{it}^{3} - a_{ti}^{3}) \right] = \frac{1}{3} \left[S \sum_{t,i} (a_{ti}^{2} - a_{it}^{2}) + \sum_{t,i} (a_{it}^{3} - a_{ti}^{3}) \right]$$
$$= 0.$$

The above fact implies the following.

Theorem. Any balanced square of order 4 is completely balanced.

For n(>4) we are unable to show $c_{n-4} = 0$. An obstruction is the appearance of the sum

$$\sum_{t} \left(\sum_{i \neq j} a_{it}^2 a_{jt}^2 - \sum_{i \neq j} a_{ti}^2 a_{tj}^2 \right)$$

in cn-4. Since

$$2\sum_{i\neq j}a_{it}^{2}a_{jt}^{2} = \left(\sum_{i}a_{it}^{2}\right)^{2} - \sum_{i}a_{it}^{4},$$

a sufficient condition for $c_{n-4} = 0$ or a condition that any balanced square of order 5 to be completely balanced may be stated by

(4)
$$\sum_{t} \left(\sum_{i} a_{it}^{2} \right)^{2} = \sum_{t} \left(\sum_{i} a_{ti}^{2} \right)^{2}$$

Incidentally, Eq. (4) is the condition easily satisfied by any doubly magic square, a magic square $[a_{ij}]$ such that $[a_{ij}^2]$ is also a magic square. Summarizing the above argument we state a theorem.

Theorem. If a balanced square of order 5 satisfies the condition (4), then it is completely balanced.

In the theorem (4) is a sufficient condition and we do not know whether it is necessary. All the balanced magic squares of order 5 that we have been able to check turned out to be also completely balanced and they do satisfy (4). Thus, we make a conjecture.

Conjecture. A balanced magic square of order 5 is completely balanced.

3.' CONSTRUCTION OF BALANCED SQUARES

Some magic squares of order 4 or 5 constructed by adding two orthogonal Latin squares seem balanced (also completely). For example:

$$\begin{bmatrix} a & d & b & c \\ d & a & c & b \\ c & b & d & a \\ b & c & a & d \end{bmatrix} + \begin{bmatrix} u & v & x & y \\ x & y & u & v \\ v & u & y & x \\ y & x & v & u \end{bmatrix} = \begin{bmatrix} 1 & 4 & 2 & 3 \\ 4 & 1 & 3 & 2 \\ 3 & 2 & 4 & 1 \\ 2 & 3 & 1 & 4 \end{bmatrix}$$

$$+ \begin{bmatrix} 0 & 5 & 10 & 20 \\ 10 & 20 & 0 & 5 \\ 5 & 0 & 20 & 10 \\ 20 & 10 & 5 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 9 & 12 & 23 \\ 14 & 21 & 3 & 7 \\ 8 & 2 & 24 & 11 \\ 22 & 13 & 6 & 4 \end{bmatrix}$$

$$p.s. = 19,646$$

$$\begin{bmatrix} a & b & c & d & e \\ d & e & a & b & c \\ b & c & d & e \\ e & a & b & c & d \\ c & d & e & a & b \end{bmatrix} + \begin{bmatrix} x & y & s & t & v \\ s & t & v & x & y & s \\ v & x & y & s & t \\ v & s & t & v & x \\ t & v & x & y & s \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \\ 2 & 3 & 4 & 5 & 1 \\ 5 & 12 & 3 & 4 \\ 3 & 4 & 5 & 1 & 2 \end{bmatrix}$$

$$+ \begin{bmatrix} 0 & 5 & 10 & 15 & 20 \\ 10 & 15 & 20 & 0 & 5 \\ 20 & 0 & 5 & 10 & 15 \\ 5 & 10 & 15 & 20 & 0 \\ 15 & 20 & 0 & 5 & 10 \end{bmatrix} = \begin{bmatrix} 1 & 7 & 13 & 19 & 25 \\ 14 & 20 & 21 & 2 & 8 \\ 22 & 3 & 9 & 15 & 16 \\ 10 & 11 & 17 & 23 & 4 \\ 18 & 24 & 5 & 6 & 12 \end{bmatrix}$$

$$p.s. = 607,425 \qquad diagonal p.s. = 599,399$$
Figure 3

ANOTHER PROPERTY OF MAGIC SQUARES

[OCT. 1975]

REMARKS

1. We do not know any nontrivial (all different entries) balanced square of order greater than 5. We constructed a magic square of order 10 from the famous pair of orthogonal Latin squares of that order, but we found it not balanced.

2. We do not know an example of a balanced magic square which is not completely balanced.

3. Magic squares of order 6, 7 and 8 appearing in Andrews' book [1] are not balanced.

4. We did not encounter yet a balanced square whose two-way diagonal product sums are equal to the row product sum (really diabolic one) but at least two diagonal product sums alone can be equal as in Fig. 3.

REFERENCES

1. W.S. Andrews, Magic Squares and Cubes, Dover, 1960.

2. Jack Chernick, "Solution of the General Magic Square," Math. Monthly, March 1938, pp. 172-175.

[Continued from Page 204.]

Likewise, it is obvious by inspection of a table of Fibonacci primes (\geq 5) that they are \equiv 1 (mod 4) and thus expressable as the sum of the square of two smaller integers; specifically, it is well known that

$$U_{p} = U_{(p-1)/2}^{2} + U_{(p-1)/2}^{2} + 1$$

where U_p is a Fibonacci prime (≥ 5).

Thus, it is perceived that the Mersenne and Fibonacci primes (\geq 5) form two mutually exclusive sets; i.e., *no* primes (\geq 5) can be both a Mersenne and a Fibonacci prime.

REFERENCE

 William Raymond Griffin, "Mersenne Primes-The Last Three Digits," J. Recreational Math, 5 (1), p. 53, Jan., 1972.

ON HALSEY'S FIBONACCI FUNCTION

M. W. BUNDER

The University of Wollongong, Wollongong, N.S.W., Australia

Halsey in [1] defined a Fibonacci function by

(1)
$$F_{u} = \sum_{k=0}^{m} \left[(u-k) \int_{0}^{1} x^{u-2k-1} (1-x)^{k} dx \right]^{-1}$$

where m is the integer in the range $(u/2) - 1 \le m \le (u/2)$.

This definition was criticized by Parker [2] for (a) being restricted to rational u's and (b) destroying the relation

(2)
$$F_{u+1} = F_u + F_{u-1}$$
.

Neither of these criticizms are quite fair. Firstly, there is nothing in Halsey's paper to prevent (1) from defining F_u for all real u and secondly (2) is still satisfied for approximately half of the real values of u and it is generalized in the other cases. This we show below.

Firstly, we express F_u in the more convenient form given implicitly by Halsey:

(3)
$$F_{u} = \sum_{k=0}^{m} \left(\begin{array}{c} u - k - 1 \\ k \end{array} \right) \quad ,$$

where $(u/2) - 1 \le m < (u/2)$ and *m* is an integer. Now if $(u/2) - \frac{1}{2} \le m < (u/2)$, then

$$\frac{u+1}{2}-1 \leq m < \frac{u}{2} < \frac{u+1}{2}$$

so that

$$F_{u+1} = \sum_{k=0}^{m} \left(\begin{array}{c} u+1-k-1 \\ k \end{array} \right)$$

with the same *m*.

Also,

$$\frac{u-1}{2} - 1 \le m - 1 < \frac{u}{2} - 1 < \frac{u-1}{2}$$

so that

$$F_{u-1} = \sum_{k=0}^{m-1} \left(\begin{array}{c} u - 1 - k - 1 \\ k \end{array} \right)$$

also with the same m.

Now

209

$$F_{u+1} - F_u = \sum_{k=1}^{m} \frac{(u-k)!}{(u-2k)!k!} - \frac{(u-k-1)!}{(u-2k-1)!k!} = \sum_{k=1}^{m} \frac{(u-k-1)!}{(u-2k)!(k-1)!}$$
$$= \sum_{q=0}^{m-1} \frac{(u-1-q-1)!}{(u-1-2q-1)!q!} \text{, where } q = k-1$$
$$= \sum_{q=0}^{m-1} \left(\begin{array}{c} u-1-q-1 \\ q \end{array} \right) = F_{u-1}.$$

If on the other hand $(u/2) - 1 \le m < (u/2) - \frac{1}{2}$, then

$$\frac{u+1}{2} - 1 < \frac{u}{2} < m+1 < \frac{u+1}{2}$$

so that

$$F_{u+1} = \sum_{k=0}^{m+1} \left(\begin{array}{c} u+1-k-1 \\ k \end{array} \right)$$

where we are still using *m* as in (3). Now

$$F_{u+1} - F_u = \begin{pmatrix} u - m - 1 \\ m + 1 \end{pmatrix} + \sum_{k=1}^m \frac{(u-k)!}{(u-2k)!k!} - \frac{(u-k-1)!}{(u-2k-1)!k!}$$

$$= \begin{pmatrix} u - m - 1 \\ m + 1 \end{pmatrix} + \sum_{q=0}^{m-1} \begin{pmatrix} u - 1 - q - 1 \\ q \end{pmatrix} \text{ as before}$$

$$= \begin{pmatrix} u - m - 1 \\ m + 1 \end{pmatrix} - \begin{pmatrix} u - 1 - m - 1 \\ m \end{pmatrix} + F_{u-1} = F_{u-1} + \frac{(u - m - 1)!}{(u-2m-2)!(m+1)!} - \frac{(u - m - 2)!}{(u-2m-2)!m!}$$

$$= F_{u-1} + \frac{(u - m - 2)!}{(u-2m-3)!(m+1)!} = F_{u-1} + \begin{pmatrix} u - m - 2 \\ m + 1 \end{pmatrix}$$

Thus we have for $2m < u \le 2m + 1$ that (2) applies and for $2m + 1 < u \le 2m + 2$

(5)
$$F_{u+1} = F_u + F_{u-1} + \begin{pmatrix} u - m - 2 \\ m + 1 \end{pmatrix} ,$$

where *m* is an integer.

Equation (5) also reduces to (2) when u is an integer and is also verified by Halsey's tables for F_u .

REFERENCES

- Eric Halsey, "The Fibonacci Number F_u where u is not an Integer," The Fibonacci Quarterly, Vol. 2, No. 2 (April 1965), pp. 147-152.
- 2. Francis D. Parker, "A Fibonacci Function," The Fibonacci Quarterly, Vol. 6, No. 1 (Feb. 1968), pp. 1-2.

FIBONACCI MULTI-MULTIGRADES

DONALD C. CROSS St. Luke's College, Exeter, England

Readers of The Fibonacci Quarterly will probably be familiar with multigrades. Here are two examples:

(1)
$$1^m + 6^m + 8^m = 2^m + 4^m + 9^m$$
 $(m = 1, 2)$

(2)
$$1^m + 5^m + 8^m + 12^m = 2^m + 3^m + 10^m + 11^m$$
 $(m = 1, 2, 3)$

The first example is called a second-order multigrade; the second example, a third-order multigrade. Adding, subtracting, multiplying and dividing do not affect the equality of a multigrade, provided we perform the same operation or operations on each element in it. For example, Eq. (1) above becomes

$$2^{m} + 7^{m} + 9^{m} = 3^{m} + 5^{m} + 10^{m}$$

where m = 1, 2, if we add 1 to each element; Eq. (2) becomes

$$2^{m} + 10^{m} + 16^{m} + 24^{m} = 4^{m} + 6^{m} + 20^{m} + 22^{m}$$

where m = 1, 2, 3, if we multiply each element by 2.

and

This note is concerned with what I call second-order Fibonacci multi-multigrades. (I define [1] a multi-multigrade as a multigrade having three or more "components" as compared with the normal two "components" in a multigrade as in (1) and (2) above.)

Here are some examples of Fibonacci multi-multigrades:

(3)
$$0^m + (3 \cdot 3)^m + (3 \cdot 3)^m = (3 \cdot 1^2)^m + (3 \cdot 1^2)^m + (3 \cdot 2^2)^m = \dots = \dots$$

(4)
$$0^{m} + (3 \cdot 7)^{m} + (3 \cdot 7)^{m} = (3 \cdot 1^{2})^{m} + (3 \cdot 2^{2})^{m} + (3 \cdot 3^{2})^{m} = (7 \cdot 1^{2})^{m} + (7 \cdot 1^{2})^{m} + (7 \cdot 2^{2})^{m} = (1^{2})^{m} + (4^{2})^{m} + (5^{2})^{m}$$

(5)
$$0^{m} + (3 \cdot 19)^{m} + (3 \cdot 19)^{m} = (3 \cdot 2^{2})^{m} + (3 \cdot 3^{2})^{m} + (3 \cdot 5^{2})^{m} = (19 \cdot 1^{2})^{m} + (19 \cdot 1^{2})^{m} + (19 \cdot 2^{2})^{m} = (1^{2})^{m} + (7^{2})^{m} + (8^{2})^{m}$$

(6)
$$0^{m} + (3 \cdot 49)^{m} + (3 \cdot 49)^{m} = (3 \cdot 3^{2})^{m} + (3 \cdot 5^{2})^{m} + (3 \cdot 8^{2})^{m}$$
$$= (49 \cdot 1^{2})^{m} + (49 \cdot 1^{2})^{m} + (49 \cdot 2^{2})^{m} = (2^{2})^{m} + (11^{2})^{m} + (13^{2})^{m}$$
$$0^{m} + [3(F_{2n+4} - F_{n} \cdot F_{n+1})]^{m} + [3(F_{2n+4} - F_{n} \cdot F_{n+1})]^{m} = [3F_{n+1}^{2}]^{m} + [3F_{n+2}^{2}]^{m} + [3F_{n+3}^{2}]^{m}$$
$$= [(F_{2n+4} - F_{n} \cdot F_{n+1})F_{1}^{2}]^{m} + [(F_{2n+4} - F_{n} \cdot F_{n+1})F_{2}^{2}]^{m} + [(F_{2n+4} - F_{n} \cdot F_{n+1})F_{3}^{2}]^{m}$$

$$= [F_n^2]^m + [(F_{n+5} - F_n)^2]^m + [F_{n+5}^2]^m \qquad (m = 1,2).$$

Clearly, we can expand our multigrades by a simple process. If we multiply (4) by 19×49 , (5) by 7×49 and (6) by 7×19 , we get

$$\begin{split} \mathcal{J}^{m} + (3 \cdot 7 \cdot 19 \cdot 49)^{m} + (3 \cdot 7 \cdot 19 \cdot 49)^{m} &= \left[(3 \cdot 19 \cdot 49) 1^{2} \right]^{m} + \left[(3 \cdot 19 \cdot 49) 2^{2} \right]^{m} + \left[(3 \cdot 19 \cdot 49) 3^{2} \right]^{m} \\ &= \left[(7 \cdot 19 \cdot 49) 1^{2} \right]^{m} + \left[(7 \cdot 19 \cdot 49) 1^{2} \right]^{m} + \left[(7 \cdot 19 \cdot 49) 2^{2} \right]^{m} \\ &= \left[(3 \cdot 7 \cdot 49) 2^{2} \right]^{m} + \left[(3 \cdot 7 \cdot 49) 3^{2} \right]^{m} + \left[(3 \cdot 7 \cdot 49) 5^{2} \right]^{m} \\ &= \left[(3 \cdot 7 \cdot 19) 3^{2} \right]^{m} + \left[(3 \cdot 7 \cdot 19) 5^{2} \right]^{m} + \left[(3 \cdot 7 \cdot 19) 8^{2} \right]^{m} \\ &= \dots \\ &= \left[(7 \cdot 19) 2^{2} \right]^{m} + \left[(7 \cdot 19) 11^{2} \right]^{m} + \left[(7 \cdot 19) 13^{2} \right]^{m} \\ &= (7 \cdot 19) 3^{2} \right]^{m} + \left[(7 \cdot 19) 13^{2} \right]^{m} \\ &= (7 \cdot 19) 3^{2} \right]^{m} + \left[(7 \cdot 19) 13^{2} \right]^{m} \\ &= (7 \cdot 19) 3^{2} \right]^{m} + \left[(7 \cdot 19) 13^{2} \right]^{m} \\ &= (7 \cdot 19) 3^{2} \right]^{m} + \left[(7 \cdot 19) 13^{2} \right]^{m} \\ &= (7 \cdot 19) 3^{2} \right]^{m} + \left[(7 \cdot 19) 13^{2} \right]^{m} \\ &= (7 \cdot 19) 3^{2} \right]^{m} \\ &= (7 \cdot 19) 3^{2} \left[(7 \cdot 19) 13^{2} \right]^{m} \\ &= (7 \cdot 19) 3^{2} \right]^{m} \\ &= (7 \cdot 19) 3^{2} \right]^{m} \\ &= (7 \cdot 19) 3^{2} \left[(7 \cdot 19) 13^{2} \right]^{m$$

FIBONACCI MULTI-MULTIGRADES

I give here, by way of example, the following which I recently derived:

 $(F_n^2)^m + [(F_{n+4} - F_n)^2]^m + [3F_{n+2}^2 + 2F_n \cdot F_{n+4} - F_n^2]^m + [F_{n+4}^2 + 3F_{n+2}^2 - F_n^2]^m$ = $(3F_{n+1}^2)^m + (2F_n \cdot F_{n+4})^m + (3F_{n+3}^2)^m + (3F_{n+3}^2 + 2F_n \cdot F_{n+4} - 3F_{n+1}^2)^m ,$

where m = 1, 2, 3, $0^m + (F_{n+5})^m + (F_{n+5} + F_n)^m + (2F_{n+5} + F_n)^m = (F_{n+2})^m + (F_{n+3})^m + (F_{n+6} + F_n)^m + (F_{n+6} + F_{n+2})^m,$ where $m = 1, 2, 3^*.$ $0^m + (F_{n+5} + F_n)^m + (F_{n+5} + F_{n+2})^m + (F_{n+5} + F_{n+3})^m + (F_{n+7} + F_n)^m + (F_{n+7} + F_{n+2})^m$ $= (F_{n+2})^m + (F_{n+3})^m + (2F_{n+5})^m + (3F_{n+5} + F_n)^m + (F_{n+6} + F_n)^m + (F_{n+6} + F_{n+2})^m,$

where $n = 1, 2, 3, 4^{**}$.

REFERENCES

- 1. Donald Cross, "Second- and Third-Order Multi-multigrades," *Journal of Recreational Math.*, Vol. 7, No. 1, Winter 1974, pp. 41–44.
- 2. D.C. Cross, "Multigrades," Recreational Mathematics Magazine, No. 13, Feb. 1963, pp. 7-9.
- D.C. Cross, "The Magic of Squares," *Mathematical Gazette*, Vol. XLV, No. 353, October 1961, pp. 224–227 and Vol. L, No. 372, May 1966, pp. 173–174.

*If we add F_{n+1} to each term, the multigrade reads

$$(F_{n+1})^m + (F_{n+1} + F_{n+5})^m + (F_{n+2} + F_{n+5})^m + (F_{n+2} + 2F_{n+5})^m = (F_{n+3})^m + (F_{n+1} + F_{n+3})^m + (F_{n+2} + F_{n+6})^m + (F_{n+3} + F_{n+6})^m,$$

where *m = 1, 2, 3*.

**If we add F_{n+1} to each term, the multigrade reads

 $(F_{n+1})^m + (F_{n+2} + F_{n+5})^m + (F_{n+3} + F_{n+5})^m + (F_{n+1} + F_{n+3} + F_{n+5})^m + (F_{n+2} + F_{n+7})^m + (F_{n+3} + F_{n+7})^m$ = $(F_{n+3})^m + (F_{n+1} + F_{n+3})^m + (F_{n+1} + 2F_{n+5})^m + (F_{n+2} + 3F_{n+5})^m + (F_{n+2} + F_{n+6})^m + (F_{n+3} + F_{n+6})^m$ where m = 1, 2, 3, 4.

ON FIBONACCI NUMBERS OF THE FORM $k^2 + 1$

H, C. WILLIAMS

University of Manitoba, Winnipeg, Manitoba, Canada

Consider the Diophantine equation

 $(X - Y)^7 = X^5 - Y^5$.

where X, Y are to be integers. We have an infinitude of trivial solutions of (1) given by X = m, Y = m, where m is an integer parameter. We shall concern ourselves here with solutions (X, Y) of (1) for which $X \neq Y$. There is no loss of generality in assuming that X > Y.

Using an idea of Rotkiewicz (cf. Sierpiński [5]), we let d = (X, Y) and X = dx, Y = dy. Substituting this in (1) and rearranging terms, we get

$$d^{2}(x-y)^{6} = (x-y)^{4} + 5xy(x-y)^{2} + 5x^{2}y^{2} .$$

 $d^2 = 5v^4 + 10v^3 + 10v^2 + 5v + 1.$

Since (x,y) = 1, x > y, and (x - y) must divide $5x^2y^2$, we must have x - y = 1. Hence

(3)

(1)

We rewrite (2) as

Putting

v = 2d and $u = [(2v + 1)^2 + 1]/2$.

 $16d^2 = 5[(2y+1)^2+1]^2-4.$

we have the familiar equation

 $v^2 - 5u^2 = -1$.

Now it is well known that if (v, u) is any solution of (3), there exists an integer m such that

$$u = (F_{6m+3})/2$$
,

where the Fibonacci numbers F_n (|n| = 0, 1, 2, ...) are defined by the recurrence relation

$$F_{n+1} = F_n + F_{n-1}$$
 (|n| = 0, 1, 2, ...)

together with the initial conditions $F_0 = 0$, $F_1 = 1$. Thus, in order for (1) to have a solution, we must have an integer m such that

$$F_{6m+3} = (2y+1)^2 + 1$$

In Gryte et al. [3] it was shown, by means of a computer search, that the more general equation

(4)
$$F_n = k^2 + 1$$

has no solution for any *n* such that $5 < n \le 10^6$. In this note we will show that all solutions of (4) are given by $n = \pm 1, 2, \pm 3, \pm 5$. Hence, the only solutions of (1) such that X > Y are (1,0) and (0, -1).

We first note that since $3|F_n$ if and only if 4|n, (4) has no solution if 4|n. From Lucas' [4] identities (52), we see that

$$F_{2m+1} - 1 = F_m L_{m+1}$$
 when $2|m$,
 $F_{2m+1} - 1 = F_{m+1} L_m$ when $2|m$,
 $F_{2m} - 1 = F_{m-1} L_{m+1}$ when $2|m$.

Here L_n (|n| = 0, 1, 2, ...) are the Lucas numbers defined by

2L

$$L_{n+1} = L_n + L_{n-1}$$
 ($|n| = 0, 1, 2, ...$)

together with $L_0 = 2$, $L_1 = 1$. We also have

$$m+1 = L_m + 5F_m = 3L_{m-1} + 5F_{m-1},$$

 $2F_{m+1} = L_m + F_m.$

If p is any prime divisor of F_m and L_{m+1} , then p is a prime divisor of L_m . Since $(F_m, L_m) = 1,2$, we see that p must be 2. From the fact that $2/(L_m, L_{m+1})$, it follows that $(F_m, L_{m+1}) = 1$. Using similar reasoning, it is not difficult to show that $(F_{m+1}, L_m) = 1$. Finally, if $p | (L_{m+1}, F_{m-1}) | and 2/(m)$, then $p | 3L_{m-1}$. In this case it is possible for p = 3. If $p \neq 3$, then $p | (L_{m-1}, F_{m-1}) | and p = 2$, but, since $2/(L_m, L_{m+1})$, this is not possible. If $9 | (L_{m+1}, F_{m+1}) | and p = 2$, but, since $2/(L_m, L_{m+1}) | and p = 3$.

In order to solve (4) we consider two cases.

Case (i). n odd.

Here we have

$$k^2 = F_{(n-1)/2}L_{(n+1)/2}$$
 or $k^2 = F_{(n+1)/2}L_{(n-1)/2}$

In either event, we must have some integer $r = (n \pm 1)/2$ such that $|F_r|$ is an integer square. The only possible values for r are ± 1 , 0, ± 2 , ± 12 (see Wyler [6] or Cohn [1]); hence, it is a simple matter to discover that the only solutions of (4) for odd n are $n = \pm 1, \pm 3, \pm 5$.

Case (ii). *n* even.

that (5)

In this case 4 (n and

$$k^2 = F_{n/2-1}L_{n/2-1}$$

If
$$(F_{n/2-1}, L_{n/2+1}) = 1$$
, we have
 $F_{n/2-1} = t^2$

and
$$n/2 - 1 = \pm 1, 0, 2, 12.$$

The only possible value of n such that (4) is satisfied is n = 2. If $(F_{n/2-1}, L_{n/2+1}) = 3$, we have $F_{n/2-1} = 3s^2$ for some integer s. Putting $r = L_{n/2-1}$ and noting that n/2 - 1 is even, we see from the identity

$$L_m^2 - 5F_m^2 = 4(-1)^m$$

 $r^2 - 45s^4 = 4$.

Since the Diophantine equation

has the fundamental solution
$$x = 7$$
, $y = 1$ and the equation

$$x^2 - 45y^2 = -4$$

 $x^2 - 45y^2 = 4$

has no integer solution, we see from Cohn [2] that the only possible solutions of (5) are given by

$$s^2 = 0, u_1, u_2, u_3$$

where $u_1 = 1$, $u_2 = 7$, $u_3 = 48$. That is, the only solutions of (5) are (±2,0), (±7,±1). It follows that $F_{n/2-1} = 0,3$ and the only possible even value of n such that (4) is satisfied is n = 2.

REFERENCES

- 1. J.H.E. Cohn, "On Square Fibonacci Numbers," J. London Math. Soc., Vol. 39 (1964), pp. 537-540.
- 2. J.H.E. Cohn, "Five Diophantine Equations," *Math. Scand.*, Vol. 21 (1967), pp. 61–70.
- 3. D.G. Gryte, R.A. Kingsley, and H.C. Williams, "On Certain Forms of Fibonacci Numbers," *Proc. of the Second Louisiana Conference on Combinatorics, Graph Theory, and Computing,* Baton Rouge, 1971, pp. 339–344.
- Ed. Lucas, "Théorie des Fonctions numériques Simplement périodiques," Amer. J. of Math., Vol. 1 (1878), pp. 184-240, 289-321.
- 5. W. Sierpiński, Elementary Theory of Numbers, Panstwowe Wydawnictwo Naukowe, Warsaw (1964), p. 94.
- O. Wyler, "Solutions of the problem. In the Fibonacci series F₁ = 1, F₂ = 1, F_{n+1} = F_n + F_{n-1}, the First, Second and Twelfth Terms are Squares. Are There any Offers?", Amer. Math. Monthly, Vol. 71 (1964), pp. 220–222.

THE FIBONACCI LATTICE*

RICHARD P. STANLEY Department of Mathematics, University of California, Berkeley, California 94720

1. DISTRIBUTIVE LATTICES

Our object is to investigate a certain distributive lattice F_1 closely related to the Fibonacci numbers. First we will review some basic properties of distributive lattices and discuss some general combinatorial problems associated with them. Thus this paper can be regarded as a semi-expository survey of some combinatorial aspects of distributive lattices.

In order that the combinatorial invariants we will be considering are finite, we need to restrict ourselves to distributive lattices L satisfying the following property:

(W) L is locally finite with a unique minimal element 0, and only finitely many elements of any given rank (or height).

By *locally finite*, we mean that every segment $[x,y] = \{z | x \le z \le y\}$ of *L* is finite. The *rank k* of an element $x \in L$ is the length of the longest chain between 0 and x. In any distributive lattice, if the length *k* of the longest chain between two elements x and y is finite, then the length of any saturated (or unrefinable) chain between x and y is also k. A distributive lattice satisfying property (*W*) will be called a *W*-distributive lattice.

Recall that an *order ideal* of a partially ordered set P is a subset $I \subseteq P$ such that if $x \in I$ and $y \leq x$, then $y \in I$. By a fundamental theorem of Garrett Birkhoff [2, Ch. III, §3], corresponding to every *W*-distributive lattice L is a partially ordered set P, uniquely determined up to isomorphism, satisfying the following three properties:

(i) Every element of P is contained in a finite order ideal of P,

(ii) P has only finitely many order ideals of any given finite cardinality k,

(iii) L is isomorphic to the set of finite order ideals of P, ordered by inclusion.

Conversely, given any partially ordered set P satisfying (i) and (ii), the lattice of finite order ideals of P (ordered by inclusion) is a *W*-distributive lattice. A partially ordered set satisfying (i) and (ii) is called a *W*-ordered set. The correspondence between *W*-ordered sets P and *W*-distributive lattices L is denoted L = J(P). P is isomorphic to the sub-ordered set of L consisting of all the join-irreducible elements of L. If I is a finite order ideal of P, then the cardinality |I| of I is equal to the rank of I in J(P).

If P is a W-ordered set, then we define a P-partition of n [18] to be an order-reversing map $\sigma: P \rightarrow \{0, 1, 2, \cdots\}$ satisfying

$$\sum_{x\in P}\sigma(x) = n.$$

(In particular, only finitely many elements x of P satisfy $\sigma(x) \ge 0$.) The statement that σ is order-reversing means that if $x \le y$ in P, then $\sigma(x) \ge \sigma(y)$. The parts of σ are the non-zero values $\sigma(x)$ (counting multiplicities). Let a(m,n) denote the number of P-partitions of n with largest part $\le m$. Since P is a W-ordered set, it follows easily that a(m,n) is finite. It can be shown that a(m,n) is the number of order ideals of cardinality n in the direct product $P \times \underline{m}$, where m denotes an m-element chain,

$$\underline{m} = \{1, 2, \cdots, m\}.$$

^{*}Supported by the Air Force Office of Scientific Research AF 44620-70-C-0079, at M.I.T.

THE FIBONACCI LATTICE

Furthermore, let a(n) denote the total number of *P*-partitions of *n*. Hence

$$\lim_{m\to\infty} a(m,n) = a(n),$$

and a(n) is the number of order ideals of cardinality n in the partially ordered set $P \times \underline{N}$, where \underline{N} denotes the natural numbers,

In particular, a(1,n) is equal to the number of order ideals of cardinality n in P (equivalently, the number of elements of rank n in J(P)), since $P \times \underline{1} = P$. In fact, there is a one-to-one correspondence $o \leftrightarrow I(\sigma)$ between order-reversing maps $\sigma : P \rightarrow \{0, 1\}$ satisfying

$$\sum_{x \in P} \sigma(x) = n,$$

and order ideals $I(\sigma)$ of P of cardinality n, viz.,

$$l(\sigma) = \{x | \sigma(x) = 1\}.$$

The number a(1,n) is denoted $j_n(P)$ or simply j_n . If P is finite, then the total number of order ideals of P is denoted j(P), so j(P) = |J(P)|.

If L = J(P) is a *W*-distributive lattice and $I \in L$, then define e(I) to be the number of saturated chains between 0 and *I*. (This number is obviously finite.) It is not difficult to see that e(I) is equal to the number of order-preserving bijections $\sigma : I \to \underline{k}$, where |I| = k. In fact, such a bijection σ corresponds to the saturated chain

(1)
$$\phi \subset \sigma^{-1}(\underline{1}) \subset \sigma^{-1}(\underline{2}) \subset \cdots \subset \sigma^{-1}(\underline{k}).$$

Thus a saturated chain between 0 and I corresponds to a permutation $\sigma^{-1}(1)$, $\sigma^{-1}(2)$, ..., $\sigma^{-1}(k)$ of the elements of I. This provides a systematic basis for studying relationships between sequences and lattice paths which occur frequently in combinatorial theory and probability theory.

2. EXAMPLES

By now the reader may be overwhelmed by a plethora of definitions and anxious to see the point of them. We will give several examples, some of which will be used later, to illustrate the significance of the above concepts.

Example 1. Let $P = \underline{N}$, the natural numbers with their usual ordering. Then a *P*-partition of *n* with largest part $\leq m$ is just an *ordinary partition* of *n* with largest part $\leq m$ [8, Ch. 19]. As is well-known,

$$\sum_{n=0}^{\infty} a(m,n)x^n = \prod_{i=1}^{m} (1-x^i)^{-1} .$$

Similarly a(n) is equal to the total number of partitions of n (usually denoted p(n)), with the corresponding generating function

$$\sum_{n=0}^{\infty} a(n)x^{n} = \prod_{i=1}^{\infty} (1-x^{i})^{-1}.$$

To tie in with subsequent results, we state the trivial formulas

(2)
$$\sum_{|I|=k} e(I) = 1, \qquad \sum_{|I|=k} e(I)^2 = 1,$$

where the sum is over all order ideals I of N of cardinality k.

Example 2. Let *P* be the disjoint union of two copies of \underline{N} , denoted $P = \underline{N} + \underline{N} = 2\underline{N}$. Thus J(P) is isomorphic to the direct product $\underline{N} \times \underline{N} = \underline{N}^2$. Here the numbers a(m,n) are not so significant (in particular,

[OCT.

THE FIBONACCI LATTICE

$$\sum_{n=0}^{\infty} a(m,n)x^n = \prod_{i=1}^{m} (1-x^i)^{-2}.$$

We will rather discuss the numbers e(I), $I \in J(P)$. For any *W*-ordered set *P* and $I \in J(P)$, let I_1, I_2, \dots, I_r be the elements of J(P) which *I covers*, i.e., $I_i < I$ and no $I' \in J(P)$ satisfies $I_i < I' < I$. It follows that

For the lattice N² under consideration, (3) is precisely the "addition formula" for constructing Pascal's triangle.



The numbers e(1) are just the binomial coefficients, and in analogy to (2) we have the well-known formulas

$$\sum_{|I|=k} e(I) = 2^k, \qquad \sum_{|I|=k} e(I)^2 = \binom{2k}{k} .$$

More precisely, for any $I \in J(P)$ the segment [0, I] has the form

$$\underline{a+1} \times \underline{b+1}$$
, and $e(I) = \begin{pmatrix} a+b\\b \end{pmatrix}$

Now $\underline{a+1} \times \underline{b+1} = J(\underline{a} + \underline{b})$. Thus from (1), we have that

$$\left(\begin{array}{c}a+b\\b\end{array}\right)$$

is equal to the number of order-preserving bijections $\sigma : \underline{a} + \underline{b} \rightarrow \underline{a + b}$. The map σ is determined by the image of \underline{a} (or b), so we get the usual combinatorial interpretation of

$$\left(\begin{array}{c}a+b\\b\end{array}\right)$$

as the number of combinations of a + b things taken b at a time.

The above discussion motivates defining a *generalized Pascal triangle* to be a *W*-distributive lattice together with the function *e*. The entries *e(I)* of a generalized Pascal triangle have three features in common with the ordinary binomial coefficients:

(a) They can be obtained by an additive recursion,

(b) They can be interpreted as counting certain types of permutations or sequences.

(c) They can be interpreted as counting certain types of lattice paths in Euclidean space, since every finite distributive lattice can be "imbedded" in a Cartesian grid of sufficiently high dimension.

To illustrate the lattice path interpretation (c), consider the well-known problem of counting the number of lattice paths in an $(n + 1) \times (n + 1)$ array of lattice points from a fixed corner to the opposite corner, such that the path

1975]

(3)

never goes below the diagonal. For instance, in the 4×4 case we have as one path the following:

The total number in the 4×4 case is the number of maximal chains in the following distributive lattice *L*:

Here $L = J(\underline{2} \times \underline{3})$. In the general $(n + 1) \times (n + 1)$ case, the appropriate distributive lattice is $L = J(\underline{2} \times \underline{n})$. The number of maximal chains in $J(\underline{2} \times n)$ is known to be the *Catalan number* $\frac{1}{n + 1} \begin{pmatrix} 2n \\ n \end{pmatrix}$.

Many other known lattice path problems can be formulated in a similar context. We give a further example, arising from a lattice path problem considered by Frankel [6]. Here if we take P to look like







then the generalized Pascal triangle corresponding to *J(P)* looks like

The entries e(1) are all Fibonacci numbers.

Example 3. Let $P = \underline{N}^2$. Then the lattice J(P) is denoted \underline{T} and is called *Young's lattice* (cf. Kreweras [11]). \underline{T} can also be regarded as the lattice of all decreasing sequences $\lambda = (\lambda_1, \lambda_2, \dots)$ (with $\lambda_1 > \lambda_2 > \dots > 0$) of non-negative integers λ_i , all but finitely many equal to 0, ordered coordinatewise. Hence λ may be regarded as a partition of $|\lambda| = \Sigma \lambda_i$. Thus if $\lambda = (\lambda_1, \lambda_2, \dots) \in \underline{T}$ and $\mu = (\mu_1, \mu_2, \dots) \in \underline{T}$, then $\lambda \leq \mu$ if and only if $\lambda_i \leq \mu_i$ for all $i = 1, 2, \dots$. From this it follows that $j_k(\underline{T}) = \rho(k)$, the number of partitions of k. The lattice \underline{T} is intimately connected with the theory of plane partitions and the representation theory of the symmetric group (cf. Stanley [19], and the references cited there). We will merely state some of the remarkable properties of the lattice \underline{T} .

First, we have the beautiful formulas, originally due to MacMahon [13, Sect. 495],

$$\sum_{n=0}^{\infty} a(m,n)x^n = \prod_{i=1}^{\infty} (1-x^i)^{-min(i,m)}, \qquad \sum_{n=0}^{\infty} a(n)x^n = \prod_{i=1}^{\infty} (1-x^i)^{-i}.$$

If $\lambda \in \underline{T}$ and $|\lambda| = k$, then the number $e(\lambda)$ is traditionally denoted f^{λ} and is equal to the degree of the irreducible representation of the symmetric group S_k corresponding to the partition λ . By either group-theoretic or combinatorial means, the following formulas can be proved:

(4)
$$\sum_{|\lambda|=k} e(\lambda) = t_k, \qquad \sum_{|\lambda|=k} e(\lambda)^2 = k!$$

A FIBONACCI LATTICE

Here t_k is the number of elements $\pi \in S_k$ satisfying $\pi^2 = 1$. It is most easily computed from the recursion



7

11

 λ_2, \dots) of <u>T</u> is represented schematically as an array of left-justified squares, with λ_i squares in the *i*th row. This array is called the *graph* of λ . For instance, if $\lambda = (4,3,2,2,0,0,\dots)$, then the graph of λ is

220

to filling in the squares of the graph of λ with the integers 1, 2, ..., $|\lambda|$, such that these integers are increasing in every row and column. Such an array is called a Young tableau of shape λ For instance, one of the Young tableaux of shape (4,3,2,2) is

[OCT.

A FIBONACCI LATTICE

With each square S of the graph of a partition λ , we associate an integer h(S), defined to be the number of squares directly to the right or directly below S, counting S itself exactly once. This number h(S) is called the *hook length* of S. The hook lengths for $\lambda = (4,3,2,2)$ are given by

-				
	7	6	3	1
	5	4	1	
	3	2		
	2	1		

A basic result of Frame, Robinson, and Thrall [5] states that

 $e(\lambda) = k!/h(S_1)h(S_2)\cdots h(S_k),$

where $|\lambda| = k$ and S_1, \dots, S_k are the squares in the graph of λ -

Formulas (4) can be stated in terms of Young tableaux as follows:

(i) The number of Young tableaux with k squares is t_k .

(ii) The number of ordered pairs of Young tableaux of the same shape and with k squares is k!.

For instance, when $k = 3$, we have the follow-			1	23	12 3	13 2	1 2					
We also have the following 3!= 6 pairs:	123	123	12 3	12 3	12 3	13 2	3 1 2	1 2	13 2	12 3	13 2	13 2
							- 3	3				

In view of (i) and (ii), it is natural to ask for an explicit one-to-one correspondence $\pi \to (P, Q)$ between permutations π of 1, 2, ..., k and ordered pairs (P,Q) of Young tableaux of the same shape and with k squares, such that if $\pi \to (P,Q)$, then $\pi^{-1} \to (Q,P)$ (so that $\pi^2 = 1$ if and only if $\pi \to (P,P)$ for some P). Such a correspondence was discovered in a rather vague form by Robinson [14] and later more explicitly by Schensted [16]. Further aspects of this correspondence were considered by Schützenberger [17] and Knuth [9], [10, §5.2.4]. We refer the reader to these sources for the details.

It is natural to try to extend the results about $\underline{T} = J(\underline{N}^2)$ to the lattices $J(\underline{N}^r)$, r > 2. Unfortunately, all the "expected" results turn out to be false, and very little is known about the numbers a(m,n) and e(l).

Example 4. Our final example in this section is when *P* is the *universal binary tree* \underline{T}_2 . This partially ordered set is characterized by the property that it is a *W*-ordered set with 0 such that every element is covered by two elements, and every element except 0 covers one element.



1975]

221

$$\frac{1}{k+1}\left(\begin{array}{c}2k\\k\end{array}\right).$$

We thus have two order-theoretic interpretations of the Catalan numbers: (a) as the number of maximal chains in $J(\underline{2} \times \underline{k})$, and (b) as the number of elements of rank k in $J(\underline{T}_2)$. We state a third interpretation, viz., (c)

$$\frac{1}{k+1} \begin{pmatrix} 2k \\ k \end{pmatrix}$$

is the *total* number of elements in $J(S(\underline{k} - 1))$, where S(P) denotes the set of segments (or intervals) of P, ordered by inclusion*. Thus the Hasse diagram for $S(\underline{k} - 1)$ looks like the "top half" of the distributive lattice $\underline{k-1} \times \underline{k-1}$. For instance, when k = 4 we have S(3) and J(S(3)) as follows:



We leave as an exercise for the reader the result that the number of maximal chains in $J(S(\underline{k}))$ is

$$\frac{\binom{k+1}{2}!}{(2k-1)(2k-3)^2(2k-5)^3\cdots 3^{k-1}1^k}$$

There is an interesting way to see that the number of maximal chains in $J(\underline{2} \times \underline{k})$ is equal to the number of order ideals of $S(\underline{k-1})$. Draw the Hasse diagram of $J(\underline{2} \times \underline{k})$, pick a maximal chain C, and rotate the Hasse diagram 90° so there is one vertex on top and k-1 on the bottom. Remove the "bottom zigzag" of this rotated Hasse diagram. Then the resulting diagram H is the Hasse diagrams of $S(\underline{k-1})$. Let I be the smallest order ideal of H which contains all the elements in the intersection $C \cap H$. It is easily seen that this correspondence $C \to I$ between maximal chains C in $J(\underline{2} \times \underline{k})$ and order ideals I of $H \cong S(\underline{k-1})$ as a bijection. As an example, we take k = 5 and C as shown at the top of the following page (indicated by wiggly lines).

The corresponding order ideal of $S(\underline{4})$ consists of the labeled elements on the right.



*There are two other lattices associated with the Catalan numbers, due to D. Tamari [21] (first published in [7]) and G. Kreweras [12], but since these lattices are not distributive we will not discuss them here.



The above correspondence between order ideals and maximal chains generalizes straightforwardly to show that if L = J(P) is any finite planar distributive lattice (equivalently, P has no antichains of cardinality ≥ 3), then the number of maximal chains in L is equal to the number of order ideals in the partially ordered set obtained by rotating the Hasse diagram of L 90° and removing the "bottom zigzag." We state without proof one amusing consequence of this observation, based on a problem of Berlekamp [22, p. 341, problem 3] (see also Carlitz, Roselle, and Scoville [4]). Write down the graph of some partition λ . Let S be a square of this graph with coordinates (i,j) (i.e., S is in the *i*th row and *j*th column). Then the squares (i',j') satisfying $i' \ge j$ and $j' \ge j$ form the graph of a partition μ (S). In the square S write the number of elements ν of the Young lattice \underline{T} satisfying $\nu \leq \mu$. For example, if $\lambda = (3,3,2,1)$, then we get the array shown above right. The entry 9, for instance, corresponds to $\mu = (2,2,1)$ with the nine partitions $\nu \leq \mu$ given by (2,2,1), (2,1,1), (2,2), (1,1,1), (2,1), (2), (1,1), (1), ϕ . Now "border" the bottom and right of this array with a rookwise connected line of squares containing the integer 1. Thus for the above array, we get the array shown in the lower right. For any entry in this new array, consider the largest square of which it is the upper left-hand corner. For instance, the entries 5 (either one), 9, and 28 give the square arrays

5	2	9	3	1	28	9	3
2	1	5	2	1	14	5	2
		2	1	1	5	2	1

						2	1	1	5	2	1				
Then	we	have	the	following	result:	The	dete	rminar	nt of	each	of	these	square	arrays	is
equal	to o	one.													

We now return to the partially ordered set T_2 . Here no simple expression for the generating function

$$\sum_{n=0}^{\infty} a(n) x^n$$

28	9	3
14	5	2
5	2	
2		

	28	9	3]
	14	5	2	1
;	5	2	1	1
5	2	1	1	
	1	1		

is known. On the other hand, it is easy to show (we will not do so here) that

$$\sum_{|I|=k} e(I) = k! \; .$$

The numbers e(I) can be evaluated in a manner analogous to $e(\lambda)$, $\lambda \in \underline{T}$. In fact, if P is any finite rooted tree (considered as a partially ordered set) and $x \in P$, define

$$h(x) = \operatorname{card} \{ y | y \in P, y \ge x \}.$$

Then an easy induction argument shows

$$e(P) = k!/h(x_1)h(x_2) \cdots h(x_k),$$

where P = |k| and the x_i 's are the elements of P. For example, see the array on the right. So for this partially ordered set P_r

 $e(P) = 9!/9 \cdot 4 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 \cdot 1 = 420.$

A discussion of these and related results may be found in [18, §22].

The lattice $J(\underline{T}_2)$ is closely connected with the well-known problem of parenthesizing a string of k letters (say x's). A bibliography of this problem is



given by Brown [3], though the following lattice-theoretic interpretation appears to be new. We define an order relation \underline{A}_2 on all finite parenthesized strings of x's (excluding the void string) as follows: Given two strings S_1 and S_2 , then $S_1 \leq S_2$ if and only if S_2 can be obtained from S_1 by substituting for each occurrence of x in S_1 some parenthesized string S (which depends on the particular x in S_1 being substituted for). For instance, if $S_1 = (xx)/(x(xx))$ and $S_2 = (x(xx))/(((xx)x)/(xx))$, then $S_1 \leq S_2$ since we have substituted for the five x's in S_1 the strings x, xx, (xx)x, x, x. The order relation A_2 looks as follows:



The basic result about \underline{A}_2 is that it is a distributive lattice isomorphic to $J(\underline{T}_2)$. In fact, the join-irreducible elements of \underline{A}_2 are elements like x(((xx)x)x) which are build up from x by multiplying successively by x either on the left or on the right. Thus for instance the following order ideal of \underline{T}_2 corresponds to the elements

 $a_6 = a_4 a_5 = (a_1 a_2)(a_1 a_3) = ((xx)(x(xx)))((xx)((xx)x)))$ of \underline{A}_2 .



In contrast to the difficulties involved in extending results about $J(\underline{N}^2)$ to $J(\underline{N}^r)$, our results on $J(\underline{T}_2)$ easily generalize to $J(\underline{T}_r)$, where \underline{T}_r is the *universal r-ary tree* (whose definition is evident). For instance,

$$j_k = \frac{1}{k(r-1)+1} \binom{kr}{k}, \qquad \sum_{|I|=k} e(I) = 1 \cdot r \cdot (2r-1)(3r-2) \cdots ((k-1)r - (k-2)).$$

Moreover, the numbers e(I) can be computed for $J(\underline{T}_r)$ in exactly the same way as for $J(\underline{T}_2)$, since I is a rooted tree. Finally if \underline{A}_r denotes the set of all finite strings of x's parenthesized in accordance with an *r*-ary operation and ordered analogously to \underline{A}_2 , then $\underline{A}_r = J(\underline{T}_r)$.

3. COVER CHARACTERIZATIONS

Most of the distributive lattices we have been considering have an interesting property which we call a "cover characterization." A W-distributive lattice L is said to have a cover characterization if there exists a function f(k,n) such that if an element x of L of rank k covers n elements, then x is covered by f(k,n) elements. If f(k,n) is independent of k (in which case we simply write f(n)), then we say that L has a strong cover characterization. The function f(k,n)(or f(n)) is called the cover function of L.

It is easy to see (by inductively building L from the bottom up) that there can be at most one distributive lattice L (up to isomorphism) with a given cover function f(k,n). It is not difficult to verify that the following lattices have the indicated cover function.

$$\underbrace{L}_{\underline{N}^{r}} = \underbrace{J(r\underline{N})}_{I(\underline{N}^{2})} + \underbrace{r}_{r} \\ \underbrace{J(\underline{N}^{2})}_{r} = \underbrace{J(r\underline{N}^{2})}_{I(\underline{N}^{2})} + r \\ \underbrace{2^{r}}_{I(\underline{r})} = \underbrace{J(r\underline{1})}_{I(\underline{r})} - n + r \\ \underbrace{J(T_{r})}_{r} = \underbrace{J(sT_{r})}_{r} + (r - 1)k + s$$

On the other hand, the lattices \mathcal{M}^r , r > 2, do not have a cover characterization.

An interesting problem is to determine which functions f(k,n) can be the cover functions of a distributive lattice. For instance, given a function a(n), for what functions b(k) is f(n,k) = a(n) + b(k) a cover function? The following proposition is useful in ruling out various functions. The proof is left to the reader.

Proposition 1. Let L be a W-distributive lattice such that u(i,j) elements of rank i cover exactly j elements, and v(i,j) elements of rank i are covered by exactly j elements. Then for all $i \ge j \ge 0$,

$$\sum_{k=0}^{\infty} u(i,k) \begin{pmatrix} k \\ j \end{pmatrix} = \sum_{k=0}^{\infty} v(i-j,k) \begin{pmatrix} k \\ j \end{pmatrix}.$$

1975]

A FIBONACCI LATTICE

(Each sum has only finitely many non-zero terms.) \Box

Thus, for instance, using Proposition 1, it can be shown that if L is a W-distributive lattice with the cover function f(n) = an + b, then $u(5, 1) = -(b/3)(a + 1)(2a^3 - 2a^2 - 3)$. Hence u(5, 1) < 0 if $|a| \ge 2$, so in this case L does not exist. We in fact conjecture that if L has a strong cover characterization with a *non-decreasing* cover function f(n) (i.e., $f(i + 1) \ge f(i)$), with f(0) > 0, then f(n) = a or f(n) = n + a.

One positive result is the determination of all *finite* distributive lattices with a strong cover characterization.

Proposition 2. If *L* is a finite distributive lattice with a strong cover characterization, then *L* is a boolean algebra 2^{r} . **Proof.** Suppose *L* is a finite distributive lattice with a cover function f(n). Let *r* be the number of elements covered by the top element 1 of *L*. Then f(r) = 0. Let *I* be the meet of all elements covered by the top element 1 of *L*. Then *f*(*r*) = 0. Let *I* be the meet of all elements covered by the top element 1 of *L*. Then *f*(*r*) = 0. Let *I* be the meet of all elements covered by the top element 1 of *L*. Then *f*(*r*) = 0. Let *I* be the meet of all elements covered by the top element 1 of *L*. Then *f*(*r*) = 0. Let *I* be the meet of all elements covered by *r* elements. Suppose *I* covers *s* elements, so f(s) = r. Under the assumption s > 0, we will show that there is an element I' > I such that *I'* covers *s* elements. Then *I'* must be covered by *r* elements, which is impossible since the join of these *r* elements would lie above 1. Hence s = 0, and *L* is a boolean algebra.

Assume s > 0. Let L = J(P). If M is the set of maximal elements of P, then I is the order ideal P - M. Since s > 0, $I \neq \phi$. Let $x \in I$. Then there is some $x_1 \in M$ satisfying $x_1 > x$. Let x_2, \dots, x_r be the remaining elements of M (in any order). Define $I_k = M \cup \{x_1, x_2, \dots, x_k\}$. Then each I_k is an order ideal of P, and the number of maximal elements of I_k is at most one more than the number of maximal elements of I_{k-1} . Since I_1 has < s maximal elements and I_r has r maximal elements, some I_k has s maximal elements. This I_k is the desired I', and the proof follows. \Box

Using Proposition 1, one can determine the number j_k of elements of rank k of a W-distributive lattice L with a cover function f(k,n), without explicitly determining L. Is there a method for computing

$$\sum_{|I|=k} e(I)$$
 and $\sum_{|I|=k} e(I)^2?$

There is some evidence for believing that these numbers will have a relatively simple form. In particular, if f(k,n) = q(k) (independent of n), then it is trivial that

$$\sum_{|I|=\kappa} e(I) = g(0)g(1) \cdots g(k-1).$$

4. THE FIBONACCI LATTICE

Let \underline{K}_1 denote the set of ordered pairs (m,n) of integers $1 \le m$, $0 \le n \le 1$, under the order relation (m,n) < (m',n') if and only if n = 0 and $m \le m'$. Thus \underline{K}_1 looks as is shown on the right.

The lattice $J(\underline{K}_1)$ of finite order ideals of \underline{K}_1 is called the *Fibonacci lattice* and is denoted \underline{F}_1 . Thus we have the generalized Pascal triangle at the top of the next page.

Proposition 3. The number f_k of elements of \underline{F}_1 of rank k is the k^{th} Fibonacci number $(f_0 = f_1 = 1, f_k = f_{k-1} + f_{k-2}$ if $k \ge 2)$.

Proof. We will give three different proofs, reflecting three different properties of the Fibonacci numbers.



First proof. Clearly $f_0 = f_1 = 1$. Let / be an order ideal of \underline{K}_1 of cardinality k > 1. If the minimal element 0 is removed from \underline{K}_1 , there results an isolated point x and an isomorphic copy \underline{K}'_1 of \underline{K}_1 . If / contains x, then $I - \{0, x\}$ is an order ideal of \underline{K}'_1 of cardinality k - 2. If / doesn't contain x, then $I - \{0\}$ is an order ideal of \underline{K}'_1 of cardinality k - 1. Conversely if I' is any order ideal of \underline{K}'_1 , then $I' \cup \{0\}$ and $I' \cup \{0, x\}$ are order ideals of \underline{K}_1 . Hence $f_k = f_{k-1} + f_{k-2}$.

Second proof. Define $x_i = (i, 0) \in \underline{K}_1$. Let *I* be an order ideal of \underline{K}_1 of cardinality *k*. Let *i* be the least integer such that $x_{k-i} \in I$. Then x_1, x_2, \dots, x_{k-i} are in *I*, and the remaining *i* elements of *I* are of the form $(m_j, 1), j = 1, 2, \dots, i$, where the m_j 's are an arbitrary *i*-subset of $1, 2, \dots, k - i$. Hence


We will denote order ideals I of \underline{K}_1 (or elements of \underline{F}_1) by the notation $k_1 k_2 \cdots k_r$, where $k_1 + \cdots + k_r$ is the ordered partition defined above. Thus for instance the order ideal $122112 \in \underline{F}_1$ is given on the right.

By modifying the second proof of Proposition 3, one can establish the following result.

Proposition 4. The number of elements of \underline{F}_i of rank k which cover exactly i elements is

$$\begin{pmatrix} k-i-1\\ i-1 \end{pmatrix} + \begin{pmatrix} k-i\\ i-1 \end{pmatrix}$$

(with a binomial coefficient equaling 0 if any entry is negative). The number of elements of \underline{F}_1 of rank k which are covered by exactly *i* elements is 0 if k - i is even, while if k - 1 is odd this number is

$$\binom{(k+i-1)/2}{(k-i+1)/2}.\square$$

1975]

We now consider the problem of evaluating the sums

$$\sum_{|I|=k} e(I) \text{ and } \sum_{|I|=k} e(I)^2.$$

Surprisingly, these sums turn out to be the same as for the Young lattice \underline{T} ! Although coincidences in mathematics are suspect, I can offer no other explanation for this phenomenon. The evaluation of these sums for \underline{F}_1 is much easier than for T.

Proposition 5. We have

$$\sum_{|I|=k} e(I) = t_k \text{ and } \sum_{|I|=k} e(I)^2 = k! ,$$

where the sums are over all order ideals / of \underline{K}_1 of cardinality k, and where t_k is the number of elements π in the symmetric group S_k satisfying $\pi^2 = 1$.

Proof. Let

$$h_k = \sum_{|I|=k} e(I)$$
 and $g_k = \sum_{|I|=k} e(I)^2$.

Let x be the unique maximal element of \underline{K}_1 which covers 0. We divide all order-preserving bijections $\sigma: I \to \underline{k}$ (*I* an order ideal of \underline{K}_1) into two classes: (a) $x \notin I$, and (b) $x \in I$. Since $\underline{K}_1 - \{0, x\}$ is isomorphic to \underline{K}_1 , the number of σ of type (a) is h_{k-1} . If $x \in I$, then $\sigma(x)$ can be any of 2, 3, ..., k, so the number of σ of type (b) is $(k - 1)h_{k-2}$. Hence $h_k = h_{k-1} + (k - 1)h_{k-2}$. Moreover, by inspection $h_0 = h_1 = 1$, so $h_k = t_k$.

Similarly the number of pairs (σ, τ) of order-preserving bijections of / onto \underline{k} , for all / with $x \notin I$, is g_{k-1} . If $x \in I$, then there are $(k - 1)^2$ ways of specifying $\sigma(x)$ and $\tau(x)$, so there are $(k - 1)^2 g_{k-2}$ pairs in this case. Hence $g_k = g_{k-1} + (k - 1)^2 g_{k-2}$. Since $g_0 = g_1 = 1$, we have $g_k = k!$. \Box

In analogy with the definition of a Young tableau, we define a *Fibonacci* tableau (I, σ) to be a finite order ideal / of \underline{K}_1 , together with an orderpreserving bijection $\sigma : I \to \underline{k}$, where |I| = k. The order ideal / is called the shape of the tableau, and k is called the size of (I, σ) . Thus for example, the tableau on the right is a Fibonacci tableau of shape 212211 and size 9.

Proposition 5 can then be restated as follows: The number of Fibonacci tableaux of size k is t_k , and the number of ordered pairs of Fibonacci tableaux of size k and of the same shape is k!. There is a very simple alternative proof that the number of Fibonacci tableaux of size k is t_k – we construct

a one-to-one correspondence $\Omega : (I, \sigma) \to \pi$ between Fibonacci tableaux (I, σ) of size k and elements $\pi \in S_k$ satisfying $\pi^2 = 1$. Namely, we define π by the condition $\pi(i) = j$ for i > j if and only if some maximal element z of \underline{K}_1 satisfies $\sigma(z) = i$ and the unique element y covered by z satisfies $\sigma(y) = j$. Thus for the Fibonacci tableau illustrated above, $\pi = (19)(2)(34)(57)(6)(8)$. It is easily seen that this construction establishes the desired one-to-one correspondence.

Similarly one would like to prove the second formula of Proposition 5 by constructing a one-to-one correspondence $\psi : (I, \sigma, \tau) \to \pi$ between ordered pairs $((I, \sigma), (I, \tau))$ of Fibonacci tableaux of size k and of the same shape I, and elements $\pi \in S_k$. The correspondence ψ should satisfy the following two properties: (a) If $\psi(I, \sigma \tau) = \pi$, then $\psi(I, \tau, \sigma)$ = π^{-1} , and (b) $\psi(I, \sigma, \sigma) = \Omega(I, \sigma)$. This correspondence would be a "Fibonacci analogue" of Schensted's correspondence for Young tableaux (see Example 3). Such a correspondence was found by E. Bender (private communication), as follows: Let $x = (m, n) \in I$, and define x' = (m, 1 - n). Then π is defined by the conditions

$$\pi(\sigma(x)) = \begin{cases} \tau(x), & \text{if } x' \notin I \\ \tau(x'), & \text{if } x' \in I \end{cases}.$$

We next consider the problem of evaluating the numbers e(I) themselves, where I is the shape of a Fibonacci tableau. A finite order ideal I of K_1 is a rooted tree, so from (5) we have

$$e(I) = k! / \prod_{x \in I} h(x),$$

where |l| = k, and $h(x) = \operatorname{card} \{ y | y \in l, y \ge x \}$. It is easily seen that the above expression for e(l) is equal to the product $n_1 \cdot n_2 \cdots n_r$ where the n_i 's are those integers such that $k > n_1 > n_2 > \cdots > n_r > 0$ and $(k - n_i - i + 1, 1) \in l$. It follows that no two of the n_i 's can be consecutive integers. Conversely, given a set of integers $k > n_1 > n_2 > \cdots > n_r > 0$, no two consecutive, there is a unique order ideal / of \underline{K}_1 of cardinality k such that $(m, 1) \in l$ if and only if m has the form $k - n_i - i + 1$. We therefore obtain the following result:

Proposition 6. The set of numbers e(I), including multiplicities, as I ranges over all order ideals of \underline{K}_1 of cardinality k is equal to the set of numbers

where S ranges over all subsets of $\{1, 2, \dots, k-1\}$ containing no two consecutive integers.

For instance, when k=5 we have the eight sets S given by ϕ , $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$, $\{1,3\}$, $\{1,4\}$, $\{2,4\}$. Hence the numbers e(I), |I| = 5, are given by 1, 1, 2, 3, 4, 3, 4, 8.

Combining Propositions 5 and 6, we obtain the formulas

$$\sum_{S} \prod_{n \in S} n = t_k, \qquad \sum_{S} \prod_{n \in S} n^2 = k!,$$

where both sums are over all subsets S of $\{1, 2, \dots, k-1\}$ containing no two consecutive integers. Both these formulas can be easily proved directly by induction on k.

Let us now turn to the problem of counting the number a(m,n) of \underline{K}_1 -partitions of n with largest part $\leq m$. A \underline{K}_1 -partition is called a *protruded partition* [18, §24]. For instance, there are six protruded partitions of 3, as follows:



Proposition 7. Let a(m,n) be the number of protruded partitions of n with largest pair $\leq m$. Then

$$\sum_{n=0}^{\infty} a(m,n)x^n = \prod_{i=1}^{m} (1-x^i-x^{i+1}-x^{i+2}-\dots-x^{2i})^{-1}$$

Proof. A protruded partition of *n* with largest part $\leq m$ can be regarded as two sequences a_1, a_2, \dots and b_1, b_2, \dots of non-negative integers satisfying

$$\Sigma a_j + \Sigma b_j = n, \qquad m \ge a_1 \ge a_2 \ge a_3 \ge \cdots, \qquad a_j \ge b_j$$

Let k_i be the number of a_j 's which are equal to *i*. If some $a_j = i$, then b_j can be any of 0, 1, 2, ..., *i*, so $a_j + b_j$ is one of i, i + 1, i + 2, ..., 2i. Thus

$$\sum_{n=0}^{\infty} a(m,n)x^{n} = \prod_{i=1}^{m} \left(\sum_{k_{i}=0}^{\infty} (x^{i} + x^{i+1} + \dots + x^{2i})^{k_{i}} \right) = \sum_{i=1}^{m} (1 - x^{i} - x^{i+1} - \dots - x^{2i})^{-1}.$$

On the following page, we give a table of a(m,n) for $m,n \leq 10$.

Many features of the theory of ordinary partitions carry over to protruded partitions. We state one such result here. For a proof, see [18, §24]. A classical identity in the theory of ordinary partitions is

1975]

A FIBONACCI LATTICE

n ^m	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	2	3	3	3	3	3	3	3	3	3
3	3	5	6	6	6	6	6	6	6	6
4	5	10	12	13	13	13	13	13	13	13
5	8	17	22	24	25	25	25	25	25	25
6	13	31	42	47	49	50	50	50	50	50
7	21	53	75	86	91	93	94	94	94	94
8	34	92	135	159	170	175	177	178	178	178
9	55	156	238	285	309	320	325	327	328	328
10	89	265	416	509	558	582	593	598	600	601
$\sum_{n=0}^{\infty} \frac{q^n}{(1-x)(1-x^2)\cdots(1-x^n)} = \prod_{i=0}^{\infty} (1-qx^i)^{-1} .$										

The corresponding identity for protruded partitions is

$$\sum_{n=0}^{\infty} \frac{q^n}{(1-x-x^2)(1-x^2-x^3-x^4)\cdots(1-x^n-x^{n+1}-\cdots-x^{2n})}$$

= $\sum_{i=0}^{\infty} (1-qx^i)^{-1} \sum_{j=0}^{\infty} \frac{x^{j(j+1)}q^j}{(1-x)(1-x^2)\cdots(1-x^j)(1-x-x^2)(1-x-x^3)\cdots(1-x-x^{j+1})}$

By inspection, the Fibonacci lattice \underline{F}_1 does not have a cover characterization. It does possess, however, a different type of property, viz., it is an extremal distributive lattice [20]. This means that if L is any locally finite distributive lattice with 0 having the same number r_k of join-irreducibles of rank k as \underline{F}_1 (namely, $r_1 = 1$, $r_2 = r_3 = \dots = 2$), then $j_k(L) \leq j_k(\underline{F}_1)$. In fact, \underline{F}_1 is precisely the distributive lattice $L(1, 2, 2, 2, \dots)$ constructed in [20].

Recall the result $\underline{A}_2 \simeq J(\underline{T}_2)$ discussed in Example 4, where \underline{A}_2 is the lattice of parenthesized strings. Consider the related problem of parenthesizing a string of k x's subject to the commutative law (but not of course the associative law). For instance, when k = 6 there are 6 distinct strings, viz., $x(x(x \cdot x^3)), x(x^2 \cdot x^3), x^2(x \cdot x^3), x^2 \cdot x^2 \cdot x^2, x(x(x^2 \cdot x^2)))$ and $x^3 \cdot x^3$ (an expression such as x^3 has an unambiguous meaning since x(xx) = (xx)x by commutativity). The problem of counting the number N'_k of such strings was first considered by Wedderburn [23], who obtained a recursion for N'_k . It is unlikely that a simple expression for N'_k exists. For an historical survey of this problem, see Becker [1].

Let \underline{C}_1 be the partially ordered set of strings of x's subject to commutativity, ordered in the same way as in \underline{A}_2 . It has been conjectured (e.g., by myself and by E. Bender) that $\underline{C}_1 \simeq J(\underline{F}_1)$. The reason for this conjecture is the following: It is not hard to see that the sub-ordered set P of \underline{C}_1 consisting of those elements which cover exactly one element is isomorphic to \underline{F}_1 . Hence if \underline{C}_1 were a distributive lattice, we would have $\underline{C}_1 \simeq J(\underline{F}_1)$. Unfortunately, it turns out that \underline{C}_1 is not even a lattice. In particular, the elements $y = (x \cdot x^3)(x^3(x \cdot x^3))$ and $z = (x(x \cdot x^3))(x^3 \cdot x^3)$ lie above exactly the same set of elements of P. If \underline{C}_1 were a lattice, the elements of P would be the join-irreducibles, so y and z would lie above the same set of join-irreducibles, which is impossible.

In conclusion we mention the problem of extending the lattice $\underline{F}_1 = J(\underline{K}_1)$ to a sequence of lattices $\underline{F}_r = J(\underline{K}_r)$. There are several possible definitions of \underline{K}_r . The one which seems to work best is the following: \underline{K}_r is the unique locally finite partially ordered set with 0 such that when 0 is removed from \underline{K}_r , there results a partially ordered set isomorphic to a disjoint union of r_1 and K_r . For example, see the following page for what K_2 and K_3 look like.

Most of the results we have obtained for \underline{F}_1 generalize straightforwardly to $\underline{F}_r = J(\underline{K}_r)$. For instance,

$$\sum_{n=0}^{\infty} a(m,n)x^n = \prod_{i=1}^m \left(1 - x^i \left(\frac{r+i}{r} \right) x \right)^{-1},$$

230

4

(6)



where

denotes the Gaussian coefficient,

$$\binom{k}{j}_{x} = \frac{(1-x^{k})(1-x^{k-1})\cdots(1-x^{k-j+1})}{(1-x^{j})(1-x^{j-1})\cdots(1-x)}$$

Similarly the numbers

$$\sum_{|I|=k} e(I) \quad \text{and} \quad \sum_{|I|=k} e(I)^2$$

satisfy simple recurrence relations, but they seem difficult to evaluate explicitly.

The limiting case \underline{K}_{∞} (where \underline{K}_{∞} with 0 removed is isomorphic to a disjoint union of \underline{K}_{∞} and \underline{N}) seems of some interest. The distributive lattice $\underline{F}_{\infty} = J(\underline{K}_{\infty})$ is isomorphic to the set of all sequences (n_1, n_2, \dots) of non-negative integers such that all but finitely many n_i are equal to 0 and such that $n_i = 0 \Rightarrow n_{i+1} = 0$, ordered coordinatewise. The following formulas can be verified:

(7)
$$j_k = 2^{k-1}, \quad k > 0, \qquad \sum_{n=0}^{\infty} a(m,n)x^n = \prod_{i=1}^m \left(1 - \frac{x^i}{(1-x)(1-x^2)\cdots(1-x^i)}\right)^{-1}$$

$$\sum_{|I|=k} e(I) = B_k, \qquad \sum_{|I|=k} e(I)^2 = C_k.$$

Here B_k is a Bell number, (also called an exponential number) defined by

$$B_0 = 1, \quad B_{k+1} = \sum_{i=0}^{k} {\binom{k}{i}} B_i, \quad \text{or by} \quad \sum_{i=0}^{\infty} B_k x^k / k! = e^{e^{x} - 1}$$

[15]. Similarly C_k is defined by

$$C_0 = 1, \quad C_{k+1} = \sum_{0}^{k} {\binom{k}{i}}^2 C_i, \quad \text{or by} \quad \sum_{0}^{\infty} C_k x^k / k!^2 = I_0 (2\sqrt{I_0 (2x^{\frac{1}{2}}) - 1}),$$

A FIBONACCI LATTICE

where

$$I_{0}(z) = \sum_{0}^{\infty} z^{2k} / 2^{2k} k!^{2}$$

is the *0th*-order modified Bessel function.

Proposition 7 and Eqs. (6) and (7) are actually special cases of the following general result. Suppose P and Q are W-ordered sets such that P has a 0 which when removed results in a partially ordered set isomorphic to a disjoint union of P and Q. Let a(m,n) (resp. b(m,n)) be the number of P-partitions (resp. Q-partitions) of n with largest part *≤ m.* Then

$$\sum_{n=0}^{\infty} a(m,n)x^{n} = \prod_{i=1}^{m} (1-x^{i}U_{i}(x))^{-1} ,$$

where

$$U_m(x) = \sum_{n=0}^{\infty} b(m,n)x^n .$$

The proof is left to the reader.

REFERENCES

- 1. H. W. Becker, Problem 4277 (solution), Amer. Math. Monthly, 56 (1949), pp. 697–699.
- 2. Garrett Birkhoff, Lattice Theory, 3rd Ed., American Mathematical Society, Providence, 1967.
- W. G. Brown, "Historical Note on a Recurrent Combinatorial Problem," Amer. Math. Monthly, 72 (1965) 973-3. 977.
- 4. L. Carlitz, D. P. Roselle, and R. A. Scoville, "Some Remarks on Ballot-Type Sequences of Positive Integers," J. Combinatorial Theory, 11 (1971), pp. 258-271.
- 5. J. S. Frame, G. de B. Robinson, and R. M. Thrall, "The Hook Lengths of Sn," Canadian J. Math., 6 (1954), pp. 316-325.
- E. T. Frankel, "Fibonacci Numbers as Paths of a Rook on a Chessboard," The Fibonacci Quarterly, Vol. 8, No. 6. 5 (Dec. 1970), pp. 538-541.
- 7. H. Friedman and D. Tamari, "Problémes d'associativité: une Structure de Trellis Finis Induite par une loi demiassociative," J. Combinatorial Theory, 2 (1967), pp. 215-242.
- 8. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 4th ed., Oxford, 1960.
- D. E. Knuth, "Permutations, Matrices, and Generalized Young Tableaux," Pacific J. Math., 34 (1970), pp. 709-9. 727.
- 10. D. E. Knuth, The Art of Computer Programming, Vol. 3 (to appear), Addison-Wesley, Reading, Mass.
- 11. G. Kreweras, "Sur une Classe de Problémes de Denombrement lies au Trellis des Partitions des Entiers," Cahiers du BURO, 6 (1965).
- 12. G. Kreweras, "Sur les Partitions non-croissées d'un Cycle," Discrete Math., 1 (1972), pp. 333-350.
- 13. P. A. MacMahon, Combinatory Analysis, Vols. 1-2, Cambridge University Press, 1915, 1916; reprinted by Chelsea, New York, 1960.
- 14. G. de B. Robinson, "On the Representations of the Symmetric Group," Amer. J. Math., 60 (1938), pp. 745-760.
- 15. G. C. Rota, "The Number of Partitions of a Set," Amer. Math. Monthly, 71 (1964), pp. 498-504.
- 16. C. Schensted, "Longest Increasing and Decreasing Subsequences," Canadian J. Math., 13 (1961), pp. 179-191.
- 17. M. P. Schützenberger, "Quelques Rémarques sur une Construction de Schensted," Math. Scand., 12 (1963), pp. 117-128.
- R. P. Stanley, "Ordered Structures and Partitions," *Memoirs of the Amer. Math. Society*, 119 (1972).
 R. P. Stanley, "Theory and Application of Plane Partitions," Parts 1 and 2, *Studies in Applied Math.*, L (1971), pp. 167–188, 259–279.
- R. P. Stanley, "An Extremal Problem for Finite Topologies and Distributive Lattices," J. Combinatorial Theory 20. (to appear).
- 21. D. Tamari, "Monoides Préordonnés et chaînes de Malcev." These, Université de Paris (1951).
- 22. W. T. Tutte, ed., Recent Progress in Combinatorics, Academic Press, New York, 1969.
- 23. J. H. Wedderburn, "The Functional Equation $q(x^2) = 2x + [q(x)]^2$," Ann. of Math.,(2), 24 (1922), pp. 121-140.

COMPOSITIONS WITH ONES AND TWOS

KRISHNASWAMI ALLADI*

Vivekananda College, Madras 600004, India

and

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

A great deal of literature has been published on the compositions of integers. In this paper, we attempt to throw some new light by discussing compositions which lead to recurrence relations. Actually, in this article we restrict our attention to compositions using *only* ones and twos. Compositions using 1, 2, and 3, ..., or 1 and 3 will lead to more general recurrences, but this will form the subject of later investigations.

Definition 1. Denote by C_n for positive integral *n*, the number of compositions of *n* using only 1 and 2.

We make the convention that whenever we refer to the word "composition" in this paper, we mean compositions with 1 and 2 unless specially mentioned.

Examples:

n	Compositions of <i>n</i>	C_n
1	1	1
2	2, 1 + 1	2
3	2 + 1, 1 + 2, 1 + 1 + 1	3
4	2 + 2, 2 + 1 + 1, 1 + 2 + 1, 1 + 1 + 2, 1 + 1 + 1 + 1	5
5	2 + 2 + 1, 2 + 1 + 2, 1 + 2 + 2, 2 + 1 + 1 + 1,	8
	1 + 2 + 1 + 1, 1 + 1 + 2 + 1, 1 + 1 + 1 + 2,	
	1+1+1+1+1	

The Fibonacci enthusiast will immediately recognize the Fibonacci number pattern in the sequence C_n . So we have Theorem 1. $C_n = F_{n+1}, \quad n = 1, 2, 3, \cdots$,

where the F_n are the Fibonacci numbers,

 $F_{n+2} = F_{n+1} + F_n, \qquad F_1 = F_2 = 1.$

Proof 1. It is quite clear from the table that Theorem 1 holds for $n = 1, 2, \dots, 5$. Let $C_m(1)$ and $C_m(2)$ denote the number of compositions of m that end in 1 or 2, respectively. We then have, trivially,

(1)
$$C_{n+1} = C_{n+1}(1) + C_{n+1}(2)$$

Pick a composition of (n + 1), ending in a one. If we remove the one at the end, we get a composition of *n*. Conversely, to a composition of *n* by adding a one at the end we get a composition for (n + 1). Therefore,

(2)
$$C_{n+1}(1) = C_n$$

Now consider a composition of (n + 1) ending in a two. If we remove the two at the end, we get a composition for (n + 1). Conversely, we could get a composition for (n + 1) from (n - 1), by adding a two or two ones. The latter case has been counted by (2) and so we have

(3)
$$C_{n+1}(2) = C_{n-1}$$
.

*Fibonacci Scholar, Summer, 1974.

2

(4)

Now, (2) and (3) together with (1) establish Theorem 1 by induction.

Proof 2. Consider the generating function

$$C(x) = \frac{x + x^2}{1 - (x + x^2)} .$$

Clearly,

$$C(x) = \sum_{n=0}^{\infty} (x + x^2)^{n+1} = \sum_{n=1}^{\infty} (x + x^2)^n.$$

If we now collect the terms with exponent n, we get C_n terms! This gives

$$C(x) = \sum_{n=1}^{\infty} C_n x^n$$

But we also find from (4) that

$$C(x) = \frac{1}{1 - (x + x^2)} - 1 = \sum_{n=1}^{\infty} F_n x^{n-1} - 1 = \sum_{n=1}^{\infty} F_{n+1} x^n = \sum_{n=1}^{\infty} C_n x^n$$

This proves that $C_n = F_{n+1}$, establishing Theorem 1.

Let $f_1(n)$ and $f_2(n)$ denote the number of ones and the number of twos in the compositions, respectively. Let p(n) denote the number of "+" signs that occur in the compositions of n.

Theorem 2.

 $f_1(n + 1) = f_1(n) + f_1(n - 1) + F_{n+1}, \quad f_2(n + 1) = f_2(n) + f_2(n - 1) + F_n$. **Proof.** Split all the compositions of (n + 1) as

$$C_{n+1} = C_{n+1}(1) + C_{n+1}(2)$$

Since $C_{n+1}(2) = C_{n-1}$, we have $f_1(n-1)$ ones since a "2" is not going to affect the counting of ones. We have also by (2) that $C_{n+1}(1) = C_n$, and we have an extra "1" in each composition counted by $C_{n+1}(1)$. So we have counted $f_1(n) + C_n$ ones, proving

$$f_1(n+1) = f_1(n) + f_1(n-1) + F_{n+1}$$

Now, going back to $C_{n+1}(1)$ and $C_{n+1}(2)$ and using (3) and (2), we can get by similar arguments that

 $f_2(n+1) = f_2(n) + f_2(n-1) + F_n \, .$

This proves Theorem 2.

Theorem 3. $f_2(n+1) = f_1(n)$.

Proof. One can verify Theorem 3 for n = 1, 2, 3. Now, by Theorem 2, we have

(5)
$$f_1(n) = f_1(n-1) + f_1(n-2) + F_n,$$

(6)
$$f_2(n+1) = f_2(n) + f_2(n-1) + F_n$$

Now, Eqs. (5) and (6) establish Theorem 3 by induction.

Theorem 4. The sequence $f_1(n)$ is the Fibonacci convolution sequence.

Proof. By induction and from Theorem 2.

Theorem 5. The sequence p(n) is the convolution sequence of C_n .

Proof. First let us find the generating functions of the sequence $f_1(n)$ and $f_2(n)$. We have by Theorem 3 and Theorem 4 that

$$\sum_{n=1}^{\infty} f_1(n) x^n = \frac{x}{[1-(x+x^2)]^2}$$

and

$$\sum_{n=1}^{\infty} f_2(n) x^n = \frac{x^2}{\left[1 - (x + x^2)\right]^2} .$$

From the definition of p(n) it trivially follows that

(7)
$$p(n) = f_1(n) + f_2(n) - C_n$$

so that we have by (7) that

$$\sum_{n=1}^{\infty} p(n)x^n = \frac{x}{[1-(x+x^2)]^2} + \frac{x^2}{[1-(x+x^2)]^2} - \frac{x+x^2}{1-(x+x^2)} = \frac{(x+x^2)-(x+x^2)[1-(x+x^2)]}{[1-(x+x^2)]^2} = \frac{(x+x^2)^2}{[1-(x+x^2)]^2} = \frac{(x+x^2)^2}{[1-($$

proving Theorem 5.

We next shift our attention to compositions with special properties. A composition of n is defined to be "palindromic" if written in reverse order it remains unchanged.

Examples: 1 + 2 + 2 + 1 is a palindromic composition of 6 while 1 + 2 + 1 + 2 is not.

Let $\Pi(n)$ denote the number of palindromic compositions of n, $\Pi(n, 1)$ the number of those ending with 1, and $\Pi(n, 2)$ the number of those ending with 2. Let $\Pi_1(n)$ and $\Pi_2(n)$ denote the number of ones and the number of twos in all the palindromic compositions of n, respectively. Let $\Pi_+(n)$ denote the number of "+" signs in the palindromic compositions of n.

Theorem 6.
$$\Pi(n+1) = \Pi(n-1) + \Pi(n-3),$$

and the sequence $\Pi(n)$ is an alternation of Fibonacci sequences

To be more precise,

 $\Pi(2n+1) = F_n, \qquad \Pi(2n) = F_{n+2}.$

Proof. We can split

(8) $\Pi(n+1) = \Pi(n+1, 1) + \Pi(n+1, 2).$

Since $\Pi(n + 1, 1)$ counts the palindromic compositions ending in a 1, by removing the 1's on both sides we get a palindromic composition for (n - 1). So we have

(9)
$$\Pi(n+1, 1) = \Pi(n-1)$$

and

(10)
$$\Pi(n+1,2) = \Pi(n-3)$$

by similar arguments. Now (9), (10) and (8) together yield Theorem 6. The Π -functions also obey

(11) $\Pi(n+2) = \Pi(n+1) + (-1)^n \Pi(n).$

Examples:

n	Palimdromic Compositions of <i>n</i>	$\Pi(n)$
1	1	1
2	2, 1 + 1	2
3	1 + 1 + 1	1
4	2 + 2, 1 + 2 + 1, 1 + 1 + 1 + 1	3
5	2 + 1 + 2, 1 + 1 + 1 + 1 + 1	2
6	2 + 2 + 2, 2 + 1 + 1 + 2, 1 + 2 + 2 + 1,	5
	1 + 1 + 2 + 1 + 1, 1 + 1 + 1 + 1 + 1 + 1	

We now define enumerating polynomials on the above compositions. For a certain n, $\phi_n(x)$ contains the term "ax ^b" if there are "a" compositions with "b" + signs. The sequence of polynomials $\phi_n(x)$ is:

1. x + 1, x^2 , $x^3 + 2x^2 + x$, $x^2(x^2 + 1)$, $x^5 + x^4 + 2x^3 + x^2$, ...

obeying the recurrence

(12)

 $\phi_{n+2}(x) \, = \, x^2 [\phi_n(x) + \phi_{n-2}(x)]$

 $\phi_{n+2}(x) = \prod (n+2).$

and this is quite obvious, for

(13)

Theorem 7.

(14) $\Pi_{+}(n+2) = \Pi_{+}(n) + \Pi_{+}(n-2) + 2\Pi_{-}(n+2),$ (15) $\Pi_{+}(n+2) = \Pi_{+}(n) + \Pi_{+}(n-2) + 2\Pi_{-}(n),$

(16)
$$\Pi_2(n+2) = \Pi_2(n) + \Pi_2(n-2) + 2\Pi(n-2).$$

Proof. First we prove (14). From the definition of $\phi_n(x)$ it is evident that

$$\frac{d\phi_n(x)}{dx}\Big|_{atx=1} = \Pi_+(n)$$

By (12) we have

$$\frac{d\phi_{n+2}(x)}{dx} = x^2 \left[\frac{d\phi_n(x)}{dx} + \frac{d\phi_{n-2}(x)}{dx} \right] + 2x \left[\phi_n(x) + \phi_{n-2}(x) \right] .$$

Now, using (13) and Theorem 6 we get

 $\Pi_+(n+2) \,=\, \Pi_+(n) + \Pi_+(n-2) + 2\Pi(n+2) \,.$

We prove (15) and (16) combinatorially. Split the compositions of (n + 2) as

$$\Pi(n+2) = \Pi(n+2, 1) + \Pi(n+2, 2).$$

We know

$$\Pi(n+2, 1) = \Pi(n)$$
, and $\Pi(n+2, 2) = \Pi(n-2)$.

Now, in the compositions counted by $\Pi(n + 2, 2)$, the extra 2 does not affect the counting of 1's. Therefore, we have counted $\Pi_1(n - 2)$ "ones." The compositions counted by $\Pi(n + 2, 1)$ contain two extra ones, compared to those counted by $\Pi(n)$, and so we count $\Pi_1(n) + 2\Pi(n)$ ones. This proves

 $\Pi_1(n+2) = \Pi_1(n) + \Pi_1(n-2) + 2\Pi(n).$

By the same arguments we find the compositions counted by $\Pi(n + 2, 1)$ contains the same number of twos as those counted by $\Pi(n)$ and so we have counted $\Pi_2(n)$ twos. But the compositions counted by $\Pi(n + 2, 2)$ contain two extra 2's compared to those counted by $\Pi(n - 2)$ giving $\Pi_2(n - 2) + 2\Pi(n - 2)$. Putting these together,

 $\Pi_2(n+2) = \Pi_2(n) + \Pi_2(n-2) + 2\Pi(n-2).$

Theorem 8. (17) $\Pi_{+}(n) = \Pi_{+}(n-1) + (-1)^{n-2} \Pi(n-2) + \Pi(n),$ (18) $\Pi_{1}(n+1) = \Pi_{1}(n) + (-1)^{n-1} \Pi_{1}(n-1) + \Pi(n),$ (19) $\Pi_{2}(n+2) = \Pi_{2}(n+1) + (-1)^{n} \Pi_{2}(n) + (-1)^{n} \Pi(n).$

Proof. We know by Theorem 7 that the following hold:

$$\Pi_{+}(n+2) - \Pi_{+}(n) - \Pi_{+}(n-2) = 2\Pi(n+2)$$

$$\Pi_{+}(n+1) - \Pi_{+}(n-1) - \Pi_{+}(n-3) = 2\Pi(n+1)$$

$$\Pi_{+}(n) - \Pi_{+}(n-2) - \Pi_{+}(n-4) = 2\Pi(n) .$$

We also know that the Π -functions satisfy

 $\Pi_{+}(n+2) = \Pi_{+}(n+1) + (-1)^{n} \Pi(n).$

If we put these together we get

 $\Pi_{+}(n+2) - \Pi_{+}(n) - \Pi_{+}(n-2) = \Pi_{+}(n+1) - \Pi_{+}(n-1) - \Pi_{+}(n-3) + (-1)^{n} [\Pi_{+}(n) - \Pi_{+}(n-2) - \Pi_{+}(n-4)].$

Assume that for a fixed n, (14) holds for n and (n - 2). This means that we get from the above the following:

$$\Pi_{+}(n+2) - \Pi_{+}(n-1) - (-1)^{n-2} \Pi_{+}(n+2) - \Pi(n) - \Pi_{+}(n-3) - (-1)^{n-4} \Pi_{+}(n-4) - \Pi(n-2)$$

 $= \Pi_+(n+1) - \Pi_+(n-1) - \Pi_+(n-3) + (-1)^n \left[\Pi_+(n) - \Pi_+(n-2) - \Pi_+(n-4) \right]$

which simplifies to

$$\Pi_{+}(n+2) = \Pi_{+}(n+1) + (-1)^{n} \Pi_{+}(n) + \Pi(n+2)$$

establishing (17) for (n + 2). Now one can verify (17) for $n = 0, 1, 2, \dots, 5$, and so (17) holds by induction. Now, to prove (18), we observe from Theorem 7 that

$$\Pi_{1}(n+2) - \Pi_{1}(n) - \Pi_{1}(n-2) = 2\Pi(n)$$

$$\Pi_{1}(n+1) - \Pi_{1}(n-1) - \Pi_{1}(n-3) = 2\Pi(n-1)$$

$$\Pi_{1}(n) - \Pi_{1}(n-2) - \Pi_{1}(n-4) = 2\Pi(n-2).$$

If we again use (11) we find

$$\Pi_{1}(n+2) - \Pi_{1}(n) - \Pi_{1}(n-2) = \Pi_{1}(n+1) - \Pi_{1}(n-1) - \Pi_{1}(n-3) + (-1)^{n} [\Pi_{1}(n) - \Pi_{1}(n-2) - \Pi_{1}(n-4)].$$

Now, if we assume that for a fixed *n*, Eq. (18) holds for $(n-2)$ and *n*, then we have

$$\Pi_{1}(n+2) - \Pi_{1}(n-1) - (-1)^{n-2} \Pi_{1}(n-2) - \Pi_{1}(n-1) - \Pi_{1}(n-3) - (-1)^{n} \Pi_{1}(n-4) - \Pi(n-3) - (-1)^{n-2} \Pi_{1}(n-4) - (-1)^{n-2} \Pi_{1}(n-4$$

$$= \Pi_{1}(n+1) - \Pi_{1}(n-1) - \Pi_{1}(n-3) + (-1)^{\prime\prime} [\Pi_{1}(n) - \Pi_{1}(n-2) - \Pi_{1}(n-4)]$$

which simplifies to

$$\Pi_1(n+2) = \Pi_1(n+1) + (-1)^n \Pi_1(n) + \Pi(n+1)$$

establishing (18) for (n + 2). Again one can verify (18) for n = 1, 2, 3, 4, 5, and so (18) holds by induction for all positive integral n.

We prove (19) with the aid of (17) and (18). From the definitions of Π_1 , Π_2 , and Π_1 we get

$$\Pi_{2}(n) = \Pi_{+}(n) + \Pi(n) - \Pi_{1}(n).$$

If (19) were to hold, we must have

$$\begin{split} \Pi_+(n+2) + \Pi(n+2) - \Pi_1(n+2) &= \Pi_+(n+1) + \Pi(n+1) - \Pi_1(n+1) \\ &+ (-1)^n [\Pi_+(n) + \Pi(n) - \Pi_1(n)] + (-1)^n \Pi(n) \,. \end{split}$$

Since (17) and (18) holds, we have

$$\Pi_{+}(n+1) + (-1)^{n} \Pi_{+}(n) + \Pi(n+2) + \Pi(n+2) - \Pi_{1}(n+1) - (-1)^{n} \Pi_{1}(n) - \Pi(n+1)$$

 $= \Pi_+(n+1) + \Pi(n+1) - \Pi_1(n+1) + (-1)^n [\Pi_+(n) + \Pi(n) - \Pi_1(n)] + (-1)^n \Pi(n)$

which reduces to

$$2\Pi(n+2) = 2\Pi(n+1) + 2(-1)^n \Pi(n)$$

which we know is true. This establishes (19) and so Theorem 8. Note that we could have proved (19) in the same way as we did (17) and (18).

Definitions. If in a composition of *n*, a 2 follows a 1, we say it is a "rise," and if a 1 follows a 2, it is a "fall." Two 1's or two 2's contribute a "straight."

Let R(n), F(n), and S(n) denote the number of rises, falls, and straights, respectively, in the compositions of n. It is easy to establish that

(20) R(n) = F(n)and p(n) = R(n) + F(n) + S(n).

Theorem 9.

$$R(n+2) = R(n+1) + R(n) + F_n$$

and R(n) is the Fibonacci convolution sequence displaced.

Proof. Partition the compositions of (n + 2) as

$$C_{n+2} = C_{n+2}(1) + C_{n+2}(2).$$

We know

 $C_{n+2}(1) = C_{n+1}$, and $C_{n+2}(2) = C_n$.

The 1 at the end of the compositions counted by $C_{n+2}(1)$ will not affect the counting of rises counted in the compositions included in C_{n+1} . But the 2 at the end of the compositions counted by $C_{n+2}(2)$ will contribute an extra rise if and only if the compositions counted by C_n end in a 1. This is true for $C_n(1) = F_n$ compositions. This proves

(21) $R(n+2) = R(n+1) + R(n) + F_n.$

The form of the recurrence in (21) and induction establishes the second part of Theorem 9. Theorem 10. $S(n + 1) = S(n) + S(n - 1) + L_{n-1}$,

where $L_n = F_{n+1} + F_{n-1}$ are Lucas numbers. Further,

$$S(n) = R(n+1) + R(n-1).$$

Proof. Partition as before

$$C_{n+1} = C_{n+1}(1) + C_{n+1}(2).$$

We know that $C_{n+1}(1) = C_n$. The extra 1 at the end, in the compositions counted by $C_{n+1}(1)$ will give an extra "straight" if the corresponding composition counted by C_n ends in 1. So we have $C_n(1) = F_n$ extra "straights." Now,

$$C_{n+1}(2) = C_{n-1} = F_n$$

and so the 2 at the end of the compositions counted by $C_{n+1}(2)$ will contribute an extra "straight," if the corresponding compositions counted by C_{n-1} end in 2. This happens for $C_{n-1}(2) = F_{n-2}$ compositions, and so we have

(23) $S(n+1) = S(n) + F_n + S(n-1) + F_{n-2} = S(n) + S(n-1) + L_{n-1}.$

We can establish the second part of Theorem 10 by induction on (22). Let

$$S(n) = R(n + 1) + R(n - 1)$$

for $n = 1, 2, 3, \dots, m$. We know by (23) that

$$S(m + 1) = S(m) + S(m - 1) + L_{m-1}$$

which can be split up as

$$S(m + 1) = R(m + 1) + R(m - 1) + R(m) + R(m - 2) + F_m + F_{m-2}$$

This can be grouped as

$$S(m+1) = R(m+1) + R(m) + F_m + R(m-1) + R(m-2) + F_{m-2}$$

$$= R(m + 2) + R(m)$$

by Theorem 9, establishing (22) for n = m + 1.

This proves the theorem.

Theorem 11. The sequence *S(n)* is a convolution of the Fibonacci and Lucas sequences.

Proof. One could say that Theorem 11 follows by observing the form of (23). We, however, use generating functions to prove Theorem 11.

By Theorem 9 we know the "R" to be the displaced Fibonacci convolution sequence. So

$$\sum_{n=1}^{\infty} S(n)x^n = \sum_{n=1}^{\infty} [R(n+1) + R(n-1)]x^n$$
$$= \frac{x^2}{[1-(x+x^2)]^2} + \frac{x^4}{[1-(x+x^2)]^2} = \frac{x(x+x^3)}{[1-(x+x^2)]^2} = \frac{x}{1-(x+x^2)} \cdot \frac{x+x^3}{1-(x+x^2)}$$

which says that the S(n) is the convolution of the Fibonacci and Lucas sequences shown below:

Lucas (with extra 1): 1, 1, 3, 4, 7, 11, 18, 29, ... Fibonacci: 1, 1, 2, 3, 5, 8, 13, 21, ...

This completes the proof.

We can actually state a stronger form of Theorem 10. If $S_1(n)$ and $S_2(n)$ are defined to be the number of "straights" counted as 1 + 1 and 2 + 2, respectively, in the compositions of n, then it is obvious that

 $S(n) = S_1(n) + S_2(n).$

We also know

S(n) = R(n + 1) + R(n).

It is indeed remarkable that

Theorem 12. $R(n + 1) = S_1(n)$ and $R(n) = S_2(n)$.

Tables:

n	Cn	$f_1(n)$	$f_2(n)$	p(n)	R(n)	S(n)	$\Pi(n)$	$\Pi_1(n)$	$\Pi_{\mathfrak{z}}(n)$	$\Pi_{+}(n)$
1	1	1	0	0	0	0	1	1	0	0
2	2	2	1	1	0	1	2	2	1	1
3	3	5	2	4	1	2	1	3	0	2
4	5	10	5	10	2	6	3	6	3	6
5	8	20	10	22	5	12	2	6	2	6
6	13	38	20	63	10	25	5	14	8	17
•	•••				•••	•••	••••			

Krishnaswami Alladi would like to thank Prof. V. E. Hoggatt, Jr., for the award of a Fibonacci Scholarship during the tenure of which this work was done.

THE RANK OF APPARITION OF A GENERALIZED FIBONACCI SEQUENCE

H. C. WILLIAMS

University of Manitoba, Winnipeg, Manitoba, Canada

1. INTRODUCTION

In [4] Waddill and Sacks discuss a generalized Fibonacci sequence $\{K_n\}$, where $K_0 = 0$, $K_1 = 1$, $K_2 = 1$, and

$$K_{n+1} = K_n + K_{n-1} + K_{n-2}$$
.

Several other properties of this sequence, often called the Tribonacci Sequence, may be easily deduced from the more general results of Miles [2] and Williams [5].

We give here the definition of the rank of apparition of an integer m in the sequence $\{K_n\}$.

Definition. The rank of apparition of an integer *m* in the sequence $\{K_n\}$ is the least positive integer ρ for which

$$K_{\rho-1} \equiv K_{\rho} \equiv 0 \pmod{m}$$

This definition is analogous to that for the ordinary Fibonacci sequence (see, for example, Vinson [3]). In [5] it was shown that such a rank of apparition always exists for any integer m; the purpose of this note is to determine, more precisely than was done in [5], the rank of apparition of any prime p.

2. PRELIMINARY RESULTS

We shall require a theorem of Cailler [1], which we only state here. *Theorem.* Let R,S be given integers and let p(>3) be a prime such that (p,R) = 1. Let $\Delta = 4R^3 + 27S^2$ and put q equal to the value of the Legendre symbol $(3\Delta | p)$.

If $p \equiv -q \pmod{3}$, there is only one root in GF[p] of

(2.1)
$$x^3 + Rx + S \equiv 0 \pmod{p}$$
.

If $p \equiv q \pmod{3}$, put m = (p - q)/3. There are three roots of (2.1) in GF[p] if

If (2.2) is not satisfied, there are no roots of (2.1) in GF[p]. Here U_n is the Lucas Function defined by the recurrence relation

 $U_m \equiv 0 \pmod{p}$.

$$U_{n+1} = PU_n - QU_{n-1}$$

and the initial conditions $U_0 = 0$, $U_1 = 1$. P and Q are determined from the relations

$$3Q \equiv -R$$
, $RP \equiv -3S \pmod{p}$.

We also require the following

Theorem. (Williams [5]). If $K_{n-1} \equiv K_n \equiv 0 \pmod{m}$ and ρ is the rank of apparition of *m*, then ρ is a divisor of *n*. Finally, we need the fact [5] that

(2.3)

$$K_{n} = \frac{1}{D} \begin{vmatrix} 1 & a & a^{n+1} \\ 1 & \beta & \beta^{n+1} \\ 1 & \gamma & \gamma^{n+1} \end{vmatrix}$$
$$x^{3} - x^{2} - x - 1 = 0$$

240

where α , β , γ are the three roots of

and D is the value of the Vandermonde determinant

$\begin{vmatrix} 1 & a & a^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{vmatrix}.$

3. THE MAIN RESULT

Let F(x) be the polynomial $x^3 - x^2 - x - 1$. If F(x) is irreducible modulo p, let $G = GF[p^3]$ be the splitting field of $F(x) \pmod{p}$ and let θ , $\phi = \theta^p$, $\psi = \theta^{p^2}$ be the roots of F(x) = 0

(3.1)

in G. Then in G we have

$$\theta \phi \psi = 1 = \theta^{1+p+p^2} = \phi^{1+p+p^2} = \psi^{1+p+p^2}$$

From (2.3) we have

If $p \equiv 1 \pmod{3}$,

$$K_{p^2+p} = K_{p^2+p+1} = 0.$$

hence,

$$\theta^{(p^2+p+1)/3} = \theta^{p(p^2+p+1)/3} = \phi^{(p^2+p+1)/3} = \psi^{(p^2+p+1)/3}$$

 $\theta^{(p^2+p+1)(p-1)/3} = 1$:

and

$K_{(p^2+p-2)/3} = K_{(p^2+p+1)/3} = 0.$

If F(x) is factorable modulo p into a linear and irreducible quadratic factor, let $G = GF[p^2]$ be the splitting field of F(x) and let $\theta \in GF[p]$, ϕ , $\psi = \phi^p$ be the roots of (3.1) in G. If $p \equiv 1 \pmod{3}$,

$$\phi^{(p^2-1)/3}\theta^{(p-1)/3} = 1;$$

thus,
$$\theta^{(p^2-1)/3} = \phi^{(p^2-1)/3} = \psi^{(p^2-1)/3}$$

and
(3.2)
$$K_{(p^2-4)/3} = K_{(p^2-1)/3} = 0.$$

If $p \equiv -1 \pmod{3}$, we use the simple fact that
(3.3)
$$x^2(x-1)^3 = 4,$$

if $F(x) = 0$. Hence, in G
$$(\phi^2 (\phi - 1)^3)^{(p^2-1)/3} = 4^{(p^2-1)/3}$$

and

We again have (3.2).

If F(x) is factorable modulo p into three linear factors, let θ , ϕ , $\psi \in GF[p]$ be the roots of (3.1). We have $\theta^{p-1} \equiv \phi^{p-1} \equiv \psi^{p-1} \equiv 1 \pmod{p}$

and

$$K_{p-2} \equiv K_{p-1} \equiv 0 \pmod{p}.$$

 $\phi^{(p^2-1)/3} = \theta^{(p^2-1)/3} = \psi^{(p^2-1)/3}$

If
$$p \equiv 1 \pmod{3}$$
, from (3.3)
 $\theta^{2(p-1)/3} \equiv 4^{(p-1)/3} \equiv \phi^{2(p-1)/3} \equiv \psi^{2(p-1)/3} \pmod{p};$

hence, we have

$$K_{(p-4)/3} \equiv K_{(p-1)/3} \equiv 0 \pmod{p}.$$

 $\theta^{(p-1)/3} \equiv \phi^{(p-1)/3} \equiv \psi^{(p-1)/3} \pmod{p}$

Since

and

$$(-6)^{3}F(x) \equiv (-6x+2)^{3} + 48(-6x+2) + 304$$

we can put together the above results and the theorems of Section 2 to obtain the following

Theorem. (The law of apparition for the Tribonacci sequence). Let U_n be defined by the linear recurrence

THE RANK OF APPARITION OF A GENERALIZED FIBONACCI SEQUENCE

$$U_{n+1} = 19U_n - 16U_{n-1}$$

and the initial values $U_0 = 0$, $U_1 = 1$.

If p is a prime $(\neq 2,3,11)$ and $p \equiv -(33|p) \pmod{3}$, the rank of apparition ρ of p is a divisor of $(p^2 - 1)/3$. If $p \equiv (33|p) \equiv 1 \pmod{3}$, ρ is a divisor of (p - 1)/3 when p divides $U_{(p-1)/3}$; if p does not divide $U_{(p-1)/3}$, ρ is a divisor of $(p^2 + p + 1)/3$. If $p \equiv (33|p) \equiv -1 \pmod{3}$, ρ is a divisor of p - 1 when $U_{(p+1)/3}$ is divisible by p; if p does not divide $U_{(p+1)/3}$, ρ is a divisor of $p^2 + p + 1$. If p = 2, $\rho = 4$; if p = 3, $\rho = 13$; and, if p = 11, $\rho = 110$. The last results were obtained by direct calculation.

		4. TABLE
We give here a table	of values of <i>p</i> and	ρ for all $\rho \leq 347$.

give here a table of values of ρ and ρ for all $\rho \leq 347$.									
	р	ρ	р	ρ	p	ρ	p	ρ	
	2	4	67	1519	157	8269	257	256	
	3	13	71	5113	163	54	263	23056	
	5	31	73	1776	167	9296	269	268	
	7	16	79	1040	173	2494	271	24480	
	11	110	83	287	179	32221	277	12788	
	13	56	89	8011	181	10981	281	13160	
1	17	96	97	3169	191	36673	283	13348	
	19	120	101	680	193	1552	293	28616	
	23	553	103	17	197	3234	307	10472	
	29	140	107	1272	199	66	311	310	
	31	331	109	330	211	1855	313	32761	
	37	469	113	12883	223	16651	317	100807	
	41	560	127	1792	227	17176	331	36631	
	43	308	131	5720	229	17557	337	5408	
	47	46	137	18907	233	9048	347	40136	

REFERENCES

- 1. C. Cailler, "Sur les congruences du troisiéme degré," L'Enseig. Math., Vol. 10 (1908), pp. 474-487.
- E.P. Miles, Jr., "Generalized Fibonacci Numbers and Associated Matrices," Amer. Math. Monthly, Vol. 67 (1960), pp. 745-752.
- 3. J. Vinson, "The Relation of the Period Modulo *m* in the Fibonacci Sequence," *The Fibonacci Quarterly*, Vol. 1, No. 2 (April 1963), pp. 37–45.
- 4. M.E. Waddill and L. Sacks, "Another Generalized Fibonacci Sequence," *The Fibonacci Quarterly*, Vol. 5, No. 2, (April 1967), pp. 209–222.
- 5. H.C. Williams, "A Generalization of the Fibonacci Numbers," *Proc. Louisiana Conference on Combinatorics, Graph Theory, and Computing,* Louisiana State University, Baton Rouge, Mar. 1–5, 1970, pp. 340–356.

ON THE SOLUTIONS TO THE DIOPHANTINE EQUATION $x^2 + xy - y^2 = \pm D$, OR THE NUMBER OF FIBONACCI-TYPE SEQUENCES WITH A GIVEN CHARACTERISTIC

BRIAN PETERSON and V.E. HOGGATT, JR. San Jose State University, San Jose, California 95192

In this paper we are concerned with a question that has already been answered, involving Fibonacci-type sequences and their characteristic numbers. We are only interested in primitive sequences .(consecutive pairs of terms have no common factors) and for these sequences we ask: What numbers can be the characteristic of a sequence, and given such a number, how many sequences have it?

Thoro [1] has shown that D may be the characteristic of a sequence if and only if D has prime power decomposition

$$D = 5^e \rho_1^{\alpha_1} \rho_2^{\alpha_2} \cdots \rho_n^{\alpha_n}$$

where e = 0 or 1 and $p_i = 10m \pm 1$ for all *i*, while Levine [2] has shown that for such *D*, there are exactly 2^n primitive sequences possessing it. Levine's proof involves the use of quadratic fields and rings of integers in such fields.

Our purpose, here partly fulfilled, is to construct an elementary proof. In this paper, we show the ideas of our argument, and the difficulties encountered.

In what follows, F_n and L_n are the n^{th} Fibonacci and Lucas numbers, respectively, while H_n, H_n^*, A_n, B_n , etc., will represent the n^{th} term of some general Fibonacci-type sequence. It can be shown that any sequence has a "pivotal" element, such that it and all of the elements after (or before) it are of the same sign, which we take positive when convenient, while the element before (or after) it is of the opposite sign and all the elements before it have alternating signs. With the exception of the Fibonacci sequence $\{\dots, 1, 0, 1, 1, 2, \dots\}$, we will always assume that for a sequence

$$\left\{ H_n \right\}_{n=-\infty}^{\infty}$$

 H_0 is the pivotal element. Finally, if $\{H_n\}$ is a sequence, then by $\{\overline{H}_n\}$ we will mean the conjugate sequence whose terms are given by

$$\overline{H}_n = (-1)^n H_{-n}$$

Henceforth, when we say sequence, unless otherwise stated, we will mean Fibonacci-type sequence.

We begin by stating the identity

$$F_{m+1}F_{n+1} + F_mF_n = F_{m+n+1}$$

which can be proved by induction on either *m* or *n*. There are several similar identities:

(2)
$$L_{m+1}F_{n+1} + L_mF_n = L_{m+n+1}$$

(3)
$$H_{m+1}F_{n+1} + H_mF_n = H_{m+n+2}$$

(4) $L_{m+1}L_{n+1} + L_mL_n = 5F_{m+n+1}$

and in general,

(1)

(5)
$$H_{m+1}H_{n+1}^* + H_mH_n^* = G_{m+n+1}$$

gives the terms of a sequence $\{G_n\}$. What we have, then, is a way of combining pairs of sequences to obtain a new sequence, a type of multiplication of sequences. We will see shortly that this operation is commutative and associative, as may already be apparent.

We will need to recall a few notions concerning sequences.

ON THE SOLUTIONS TO THE DIOPHANTINE EQUATION $x^2 + xy - y^2 = \pm D$, OR THE NUMBER OF FIBONACCI-TYPE SEQUENCES

[OCT.

For any sequence, there is a positive number C, called the characteristic number for the sequence, such that

(6)
$$H_{n-1}H_{n+1} - H_n^2 = \pm C,$$

where the sign varies according as n is even or odd.

Also, for any sequence, there is a function which generates the terms with non-negative subscripts, given by

(7)
$$\frac{H_0 + H_{-1}x}{1 - x - x^2} = \sum_{n=0}^{\infty} H_n x^n.$$

Recall, too, that given any two sequences $\{H_n\}$ and $\{H_n^*\}$, we can form what is called the convolution of the sequences, given by the sequence

 $\{C_n\}_{n=0}^{\infty}$

which is not Fibonacci-type and which has terms given by

The terms of $\{C_n\}$ satisfy the recurrence

$$C_{n+4} - 2C_{n+3} - C_{n+2} + 2C_{n+1} + C_n =$$

and are generated by the product of the generating functions for $\{H_n\}$ and $\{H_n^*\}$,

(10)
$$\frac{(H_0 + H_{-1}x)(H_0^* + H_{-1}^*x)}{(1 - x - x^2)^2} = \sum_{n=0}^{\infty} C_n x^n$$

We will now see that the convolution of the sequences $\{H_n\}$ and $\{H_n^*\}$ is closely related to the sequence $\{G_n\}$ given by Eq. (5). For a Fibonacci-type sequence $\{A_n\}$ we have

(11)
$$A_{n+2} - A_{n+1} - A_n = 0.$$

The sequence $\{C_n\}$ above does not satisfy Eq. (11), but if we let $C_{n+2} - C_{n+1} - C_n = \Delta_n$ (12)

then we observe that

(9)

$$\Delta_{n+2} - \Delta_{n+1} - \Delta_n = (C_{n+4} - C_{n+3} - C_{n+2}) - (C_{n+3} - C_{n+2} - C_{n+1}) - (C_{n+2} - C_{n+1} - C_n)$$

= $C_{n+4} - 2C_{n+3} - C_{n+2} + 2C_{n+1} + C_n = 0.$

So the $\{\Delta_n\}$ forms a Fibonacci-type sequence. Since two adjacent terms of a sequence determine the sequence, we have only to look at Δ_0 and Δ_1 to know all about $\{\Delta_n\}$. We will see that $\Delta_0 = G_1$ and $\Delta_1 = G_2$.

From Eq. (8) and then (5), we see that

$$\Delta_0 = C_2 - C_1 - C_0 = (H_2 H_0^* + H_1 H_1^* + H_0 H_2^*) - (H_1 H_0^* + H_0 H_1^*) - (H_0 H_0^*)$$

= $(H_2 - H_1 - H_0)H_0^* + (H_1 - H_0)H_1^* + H_0 H_2^* = (0)H_0^* + (H_{-1})H_1^* + H_0 H_2^* = G_1$

and, since

$$C_{3} = H_{3}H_{0}^{*} + H_{2}H_{1}^{*} + H_{1}H_{2}^{*} + H_{0}H_{3}^{*},$$

$$\Delta_{1} = C_{3} - C_{2} - C_{1} = (H_{3} - H_{2} - H_{1})H_{0}^{*} + (H_{2} - H_{1} - H_{0})H_{1}^{*} + (H_{1} - H_{0})H_{2}^{*} + H_{0}H_{3}^{*}$$

$$= (0)H_{0}^{*} + (0)H_{1}^{*} + (H_{-1})H_{2}^{*} + H_{0}H_{3}^{*} = G_{2} .$$

Thus, we have (13)

$$G_n = C_{n+1} - C_n - C_{n-1}$$

which can be interpreted in terms of generating functions. Using Eq. (10), we have

244

$$(1 - x - x^2) \frac{(H_0 + H_{-1}x)(H_0^* + H_{-1}^*x)}{(1 - x - x^2)^2} = \sum_{n=0}^{\infty} C_n x^n = \sum_{n=1}^{\infty} C_{n-1}x^n - \sum_{n=2}^{\infty} C_{n-2}x^n$$
$$= C_0 + (C_1 - C_0)x + \sum_{n=2}^{\infty} (C_n - C_{n-1} - C_{n-2})x^n$$

or,

(14)
$$\frac{(H_0 + H_{-1}x)(H_0^* + H_{-1}^*x)}{1 - x - x^2} = C_0 + (C_1 - C_0)x + \sum_{n=2}^{\infty} G_{n-1}x^n.$$

Thus, we see that, if we simply multiply the numerators of the generating functions for $\{H_n\}$ and $\{H_n^*\}$, we obtain, except for the first couple of terms, a generating function for $\{G_n\}$.

From this, it follows immediately that our operation of multiplying sequences is commutative and associative, since multiplication of polynomials is commutative and associative.

Next, we will show that, when we multiply sequences, the product of their characteristic numbers give the characteristic of the product. Unfortunately, we have no neat way to show this, so we indicate the steps in the rather messy but elementary calculation. If we let

$$\left\{ A_n \right\} = \left\{ \cdots, a, b, a+b, \cdots \right\} \quad \text{and} \quad \left\{ C_n \right\} = \left\{ \cdots, c, d, c+d, \cdots \right\},$$
which we denote $\left\{ A_C \right\}$ has

then their product, which we denote $\{AC_n\}$, has $\{AC_n\} = \{\dots, bd + ac, (a+b)d + bc, (a+2b)d + (a+b)c, \dots\}$. Ignoring the question of sign, $\{A_n\}$ has characteristic $a^2 + ab - b^2$, and $\{C_n\}$ has characteristic $c^2 + cd - d^2$. We compute the characteristic of $\{AC_n\}$, and find it is the product of these, as follows:

$$\begin{bmatrix} bd + ac \end{bmatrix} \begin{bmatrix} (a + 2b)d + (a + b)c \end{bmatrix} - \begin{bmatrix} (a + b)d + bc \end{bmatrix}^{2}$$

=
$$\begin{bmatrix} abd^{2} + 2b^{2}d^{2} + abcd + b^{2}cd + a^{2}cd + 2abcd + a^{2}c^{2} + abc^{2} \end{bmatrix} - \begin{bmatrix} a^{2}d^{2} + b^{2}d^{2} + 2abd^{2} + b^{2}c^{2} + 2abcd + 2b^{2}cd \end{bmatrix}$$

$$= a^2c^2 + a^2cd - a^2d^2 + abc^2 + abcd - abd^2 - b^2c^2 - b^2cd + b^2d^2 = (a^2 + ab - b^2)(c^2 + cd - d^2).$$

Thus, the characteristic of the product is the product of the characteristics.

These are the tools we wish to use in our argument, which rests upon something we have so far been unable to show with an elementary proof. We want to show that, for a prime $p = 10m \pm 1$, exactly two sequences have p as their characteristic, and that these are conjugate to one another. Then we would like to show that these are the atoms from which we can build the whole universe of sequences.

Suppose that we are successful in dealing with this basic problem of showing that exactly two sequences correspond to a prime $p = 10m \pm 1$. Then, we have several lemmas that show that we can build from the sequences corresponding to prime characteristics.

Lemma 1. The product of a sequence, $\{A_n\}$ and its conjugate $\{\overline{A}_n\}$ is not primitive, unless it is the sequence $\{F_n\}$.

Proof. Let a, b, c > 0 and let

$$\{A_n\} = \{\dots, -a, b, c, \dots\};$$

i.e., b is the pivotal element of $\{A_n\}$. Then,
$$\{A_n\} = \{\dots, -c, b, a, \dots\}$$
 and
$$A_0\overline{A}_1 + A_{-1}\overline{A}_0 = ba + (-a)b = 0,$$

so $\{A\overline{A}\}$ has a zero. But only a multiple of the Eibonacci sequence can have a zero. Since the ch

so $\{A\overline{A}_n\}$ has a zero. But, only a multiple of the Fibonacci sequence can have a zero. Since the characteristic of $\{A\overline{A}_n\}$ is the product of the characteristics of $\{A_n\}$ and $\{\overline{A}_n\}$, which are easily seen to be the same, we see that $\{A\overline{A}_n\} = \{cF_n\}$, where c is the characteristic of $\{A_n\}$. Since $c \neq 1$ as long as $\{A_n\} \neq \{F_n\}$, we see that $\{A\overline{A}_n\}$ is not primitive. Lemma 2. If we write $\{A_n^m\}$ for the product $\{AAA \cdots A_n\}$ where A appears m times, then if

1975]

245

ON THE SOLUTIONS TO THE DIOPHANTINE EQUATION $x^2 + xy - y^2 = \pm D$ OR THE NUMBER OF FIBONACCI-TYPE SEQUENCES

$$\frac{a+bx}{1-x-x^2} = \sum_{n=0}^{\infty} A_n x^n$$

so that

$$(a + bx)^m / (1 - x - x^2)$$

generates $\left\{ A_{n}^{m} \right\}$ except for the first few terms, then we can write

$$\frac{(a+bx)^m}{1-x-x^2} = p_{m-1}(x) + \frac{(A_m + B_m x)x^{m-1}}{1-x-x^2}$$

where $P_{m-1}(x)$ is a polynomial of degree m-1 and B_m , A_m are consecutive terms of $\{A_n^m\}$. **Proof.** We delete. The idea is to expand $(a + bx)^m$ and then divide by $(1 - x - x^2)$ and get the remainder, which is linear.

Lemma 3. Given $\{A_n\}$ and all its powers $\{A_n^m\}$ as above, the A_m 's and B_m 's introduced there satisfy the following recurrences:

$$A_{m+1} = (a + b)A_m + aB_m$$

$$B_{m+1} = aA_m + bB_m$$

$$A_{m+2} = (a + 2b)A_{m+1} + cA_m$$

$$B_{m+2} = (a + 2b)B_{m+1} + cB_m$$

where $c = a^2 - ab - b^2$ is the characteristic of $\{A_n\}$. *Proof.* If

$$\frac{(a+bx)^m}{1-x-x^2} = p_{m-1}(x) + \frac{(A_m + B_m x)x^{m-1}}{1-x-x^2}$$

then

$$\frac{(a+bx)^{m+1}}{1-x-x^2} = (a+bx)p_{m-1}(x) + \frac{(a+bx)(A_m+B_mx)}{1-x-x^2}$$

$$= p'_m(x) + \frac{(aA_m+(bA_m+aB_m)x+bB_mx^2)x^{m-1}}{1-x-x^2}$$

$$= p'_m(x) + x^{m-1} \left[aA_m + \frac{((a+b)A_m+aB_m)x+(aA_m+bB_m)x^2}{1-x-x^2} \right]$$

$$= p_m(x) + x^m \left[\frac{((a+b)A_m+aB_m)+(aA_m+bB_m)x}{1-x-x^2} \right]$$

and

 $A_{m+1} = (a+b)A_m + aB_m$ $B_{m+1} = aA_m + bB_m .$

Now, using these, we have

$$A_{m+2} = (a + b)A_{m+1} + aB_{m-1} = (a + b)A_{m+1} + a(aA_m + bB_m)$$

= (a + b)A_{m+1} + a²A_m + b(aB_m) = (a + b)A_{m+1} + a²A_m + b(A_{m+1} - (a + b)A_m)
= (a + 2b)A_{m+1} + (a² - ab - b²)A_m ,

[OCT.

$$B_{m+2} = aA_{m+1} + bB_{m+1}$$

= $a((a + b)A_m + aB_m) + bB_{m+1}$
= $(a + b)(aA_m) + a^2B_m + bB_{m+1}$
= $(a + b)(B_{m+1} - bB_m) + a^2B_m + bB_{m+1}$
= $(a + 2b)B_{m+1} + (a^2 - ab - b^2)B_m$.

Lemma 4. If a sequence is primitive, then its product with itself either is primitive or has 5 as a factor. *Proof.* We have a sequence generated by

$$(a + bx)/(1 - x - x^2),$$

where (a,b) = 1. Note that (a,b) means the greatest common divisor of a and b, and that for a sequence to be primitive is to say that any pair of consecutive terms are relatively prime. Now,

$$\frac{(a+bx)^2}{1-x-x^2} = a^2 + \frac{[(a^2+2ab)+(a^2+b^2)x]x}{1-x-x^2}$$

so we must consider $(a^2 + 2ab, a^2 + b^2)$. We suppose that some prime p divides both $a^2 + 2ab$ and $a^2 + b^2$. If p | a(a + 2b) and $p | (a^2 + b^2)$, then

$$p|(a^2+2ab-a^2-b^2) = 2ab-b^2$$
, or, $p|b(2a-b)$.

If $p \mid a$, then since $p \mid (a^2 + b^2)$, $p \mid b$, and if $p \mid b$, then $p \mid a$ for the same reason. But, (a,b) = 1, so p cannot divide both a and b, and $p \mid (a + 2b)$, $p \mid (2a - b)$. So,

$$p | [(a + 2b) + 2(2a - b)] = 5a$$

and $p \mid 5$ because p does not divide a and p is a prime. Then, we may conclude that $(a^2 + 2ab, a^2 + b^2)$ is a power of 5. But, we will show that $(a^2 + 2ab, a^2 + b^2)$ must divide D, the characteristic of our given primitive sequence. Since D contains at most one factor of 5, we will have the desired result.

Note that $D = \pm (a^2 - ab - b^2)$, we suppose that $d \neq 1$ and that $d \mid (a^2 + 2ab)$, $d \mid (a^2 + b^2)$. Then,

$$d | [a(a^2 + 2ab) - (a + b)(a^2 + b^2)] = a^2b - ab^2 - b^3 = Db$$

and

$$d | [b(a^2 + 2ab) - a(a^2 + b^2)] = -a^3 + a^2b + ab^2 = -Da.$$

We let (D,d) = d'. Then d/d'|Db/d' and d/d'|Da/d', but since (d/d', D/d') = 1, d/d'|b and d/d'|a, and since (a,b) = 1, d/d' = 1 or d = d' so that, since (D,d) = d, we see that d|D.

Lemma 5. If $\{H_n\}$ has starting pair b,a and (a,b) = 1, then

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

if and only if $\{H_n\} = \{H'L_n\}$; i.e., $\{H_n\}$ is the product of some $\{H'_n\}$ with the Lucas sequence. *Proof.* The if part is easy. Let $\{H_n\} = \{H'L_n\}$. Then

$$\left\{ H_n^2 \right\} = \left\{ H'LH'L_n \right\} = \left\{ H'^2L_n^2 \right\}.$$

But, $\left\{L_n^2\right\} = \left\{5F_n\right\}$ so

$$\left\{ H_n^2 \right\} = \left\{ H_n^{\prime 2} \right\} \cdot \left\{ 5F_n \right\} = \left\{ 5H_n^{\prime 2} \right\}$$

and clearly 5 divides each term, including $a^2 + 2ab$ and $a^2 + b^2$.

Now, for the only if part. We let (a,b) = 1 and

$$(a^2 + 2ab, a^2 + b^2) = 5.$$

Since $5|(a^2 + 2ab)$ and $5|(a^2 + b^2)$,

$$5 | [(a^2 + b^2) - (a^2 + 2ab)] = b^2 - 2ab.$$

1975]

ON THE SOLUTIONS TO THE DIOPHANTINE EQUATION $x^2 + xy - y^2 = \pm D$ OR THE NUMBER OF FIBONACCI-TYPE SEQUENCES

248 Now,

5|a(a+2b) and 5|b(b-2a).

If 5|a, then since $5|(a^2 + b^2)$, 5|b, and if 5|b, then 5|a for the same reason. So, 5 cannot divide both a and b, and 5|(a + 2b) = 5M, 5|(b - 2a) = 5M', so a = M + 2M' and b = 2M - M'.

Now we set up the system of equations

$$a = rL_{k+1} + sL_k$$
$$b = rL_k + sL_{k-1}$$

which we know has solutions. We will show that r and s are integers which will complete the proof of Lemma 5. We use Cramer's rule.

$$r = \frac{\begin{vmatrix} a & L_{k} \\ b & L_{k-1} \end{vmatrix}}{\begin{vmatrix} L_{k+1} & L_{k} \\ L_{k} & L_{k-1} \end{vmatrix}} = \frac{\begin{vmatrix} M+2M' & L_{k} \\ 2M-M' & L_{k-1} \end{vmatrix}}{(-1)^{k+1}5} = \frac{(M+2M')L_{k-1} + (M'-2M)L_{k}}{(-1)^{k+1}5}$$
$$= \frac{(2L_{k-1} + L_{k})M' + (L_{k-1} - 2L_{k})M}{(-1)^{k+1}5} = \frac{5F_{k}M' - 5F_{k-1}M}{(-1)^{k+1}5}$$
$$= (-1)^{k+1}(F_{k}M' - F_{k-1}M) \quad .$$

Similarly, s is found as

$$s = \frac{\begin{vmatrix} L_{k+1} & a \\ L_{k} & b \end{vmatrix}}{\begin{vmatrix} L_{k+1} & L_{k} \\ L_{k} & L_{k-1} \end{vmatrix}} = (-1)^{k+1} (F_{k}M - F_{k+1}M'),$$

so that we see both r and s are integers.

Lemma 6. If $(A_k, B_k) = 1$ and $(A_{k+1}, B_{k+1}) = 1$, then $(A_{k+2}, B_{k+2}) = 1$. *Proof.* We let $p | A_{k+2}$ and $p | B_{k+2}, p$ a prime. Then, certainly p divides the characteristic of the sequence

$$\{\cdots, B_{k+2}, A_{k+2}, \cdots\}$$

and since this is just the $(k + 2)^{nd}$ power of the characteristic of $\{\dots, b, a, \dots\}$ and p is a prime,

$$p \mid D = a^2 - ab - b^2$$

Now, since

$$A_{k+2} = (a + 2b)A_{k+1} + DA_k$$

 $B_{k+2} = (a + 2b)B_{k+1} + DB_k$

we have that

lf

then

$$p|(a + 2b)A_{k+1}$$
 and $p|(a + 2b)B_{k+1}$.

If p does not divide (a + 2b), then $p | A_{k+1}$ and $p | B_{k+1}$, but $(A_{k+1}, B_{k+1}) = 1$, so p | (a + 2b). But, we can show that (a + 2b, D) = 1.

Certainly (a,D) = 1 because anything thad divides both a and D must divide b and (a,b) = 1. So, $(a + 2b,D) = (a(a + 2b),D) = (a^2 + 2ab, a^2 - ab - b^2).$

 $p|(a^2+2ab)$ and $p|(a^2-ab-b^2)$,

$$p\left|(3ab+b^2)\right| = b(3a+b)$$

and since p does not divide b, we must have p | (3a + b) so p | (6a + 2b). Now, since p | (a + 2b), we see that p | 5a and

[OCT.

WITH A GIVEN CHARACTERISTIC

since $p \not| a, p \mid 5$, or, p = 5.

If $5|A_{k+2}$ and $5|B_{k+2}$, then $5|D^{k+2}$, the characteristic of $\{\dots, B_{k+2}, A_{k+2}, \dots\}$. But then 5|D and $25|D^2$. Thus, D^2 cannot be the characteristic of a primitive sequence (borrowing Thoro's result [1]). So, we may have had (a,b) = 1, but we would not have had

$$(a^2 + 2ab, a^2 + b^2) = 1.$$

Thus, nor would we have had $(A_{k+1}, B_{k+1}) = 1$. So we see that (a + 2b, D) = 1, and thus $(A_{k+2}, B_{k+2}) = 1$. Notice that Lemma 6 shows that if a primitive sequence is not a Lucas mixture, then all of its powers are primitive. Our final sequence building lemma is

Lemma 7. If $\{A_n\}$ has starting pair b, a with (a, b) = 1, and $\{C_n\}$ has starting pair d, c with (c, d) = 1, and if $(D_1, D_2) = 1$, where $D_1 = a^2 - ab - b^2$ and $D_2 = c^2 - cd - d^2$, then $\{AC_n\}$ is primitive. *Proof.* $\{AC_n\}$ is generated by

$$\frac{(a+bx)(c+dx)}{1-x-x^2} = ac + \frac{[(ad+bc+ac)+(bd+ac)x]x}{1-x-x^2}$$

We must show that

We let p | (ad + bc + ac) and p | (bd + ac). Then

$$p | [d(ad + bc + ac) - c(bd + ac)] = -a(c^2 - cd - d^2) = -aD_2$$

$$p | [b(ad + bc + ac) - a(bd + ac)] = -c(a^2 - ab - b^2) = -cD_1$$

Also,

$$p \setminus [(ad + bc + ac) - (bd + ac)] = ad + bc - bd,$$

SO

$$p \left[c(ad + bc - bd) - d(bd + ac) \right] = b(c^2 - cd - d^2) = bD_2$$

and

$$p[a(ad + bc - bd) - b(bd + ac)] = d(a^2 - ab - b^2) = dD_1$$

Thus we have that $p | aD_2$ and $p | bD_2$, and since it is impossible for p to divide both a and b, $p | D_2$. Likewise, $p | D_1$. But this cannot be, since $(D_1, D_2) = 1$. So, $\{AC_n\}$ is primitive.

Note that, while Lemma 7 tells that, given a pair of primitive sequences with characteristics C_1 and C_2 relatively prime, we can construct a sequence with characteristic C_1C_2 that is also primitive, it does not say that, given two distinct pairs of sequences, their products are different.

There is also the question of whether, given a sequence with characteristic $C_1 C_2$, it can be factored into a product of sequences with characteristics C_1 and C_2 . This question corresponds to the problem of unique factorization in integral domains. In Levine's proof [2], he was able to use the well-known fact that factorization is unique in a certain integral domain, the "algebraic integers" in the algebraic number field Q(a), the rational numbers extended by $a = (1 + \sqrt{5})/2$. We have so far been unable to show that we have unique factorization by means similar to those we have employed above.

As for the problem of knowing that exactly two sequences correspond to any prime characteristic $p = 10m \pm 1$, we have at least shown where to look for sequences having a given characteristic.

Lemma 8. If $\{H_n\}$ has characteristic C, then $\{H_n\}$ has a term in the interval $-\sqrt{C} \le x \le \sqrt{C}$.

Proof. We suppose that $\{H_n\}$ has no terms in the interval $-\sqrt{C} \le x \le \sqrt{C}$. Then let H_k be the first term greater than \sqrt{C} . We ask, where does H_{k+1} lie? If $H_{k+1} < 0$, then by assumption $H_{k+1} < -\sqrt{C}$, and, in fact,

$$H_{k+1} < -(H_k + \sqrt{C})$$

or else H_{k+2} will be in the interval $-\sqrt{c} \le x \le \sqrt{c}$. If $H_{k+1} \ge 0$, then $H_{k+1} > \sqrt{c}$ and, in fact, $H_{k+1} > 2H_k$ or else H_{k-1} will be less than or equal to H_k and yet non-negative. This cannot be, because if $H_{k-1} < H_k$, then

$$-\sqrt{C} \leq H_{k-1} \leq \sqrt{C}$$
,

and if $H_{k-1} = H_k$, then $H_{k-2} = 0$ and 0 is in the interval. So, in Case 1, where $H_{k+1} < 0$, we have

$$H_{k+1} < -(H_k + \sqrt{C}),$$

but all we will use is $|H_{k+1}| > |H_k|$. We let

$$H_k = a, \quad H_{k+1} = -b, \quad b > a > 0;$$
 then $H_{k+2} = a - b < 0.$ Since

$$H_k H_{k+2} - H_{k+1}^2 = a^2 - ab - b^2 < 0,$$

we see that

$$a^2 - ab - b^2 = -C$$
, or, $C = b^2 + ab - a^2$.

Now, since a < b, we have

$$a < b$$

$$2a < 3b$$

$$2a^{2} < 3ab$$

$$a^{2} - 2ab + b^{2} < b^{2} + ab - a^{2} = C$$

$$H_{k+2}^{2} < C$$

or $|H_{k+2}| < \sqrt{C}$, and H_{k+2} is in $-\sqrt{C} \le x \le \sqrt{C}$. Now, in Case 2, where $H_{k+1} \ge 0$, we have $H_{k+1} > 2H_k$. We let

$$H_k = a, \quad H_{k+1} = 2a + b,$$

where a, b > 0. Then $H_{k-1} = a + b$, and since

$$H_{k-1}H_{k+1} - H_k^2 = (a+b)(2a+b) - a^2 = a^2 + 3ab + b^2 > 0$$

we have

$$C = a^2 + 3ab + b^2$$
.

But then $H_k^2 < C$ because

$$C - H_k^2 = 3ab + b^2 > 0,$$

so $|H_k| < \sqrt{c}$, contrary to assumption. We are forced to conclude that $\{H_n\}$ has a term in the interval $-\sqrt{c} \le x \le \sqrt{c}$.

Lemma 8 tells us where to look. Now we only have to know what we are looking for. Finding a sequence with characteristic C is the same as finding a solution to the diophantine equation

$$y^2 + xy - x^2 = \pm C,$$

because then y, x, x + y will be consecutive terms of a sequence with characteristic C. We convert this equation to an equivalent one as follows:

(15)

$$y^{2} + xy - x^{2} = \pm C$$

$$4y^{2} + 4xy - 4x^{2} = \pm 4C$$

$$4y^{2} + 4xy + x^{2} - 5x^{2} = \pm 4C$$

$$(2y + x)^{2} - 5x^{2} = \pm 4C$$
(16)

$$y^{2} - 5x^{2} = \pm 4C$$

If y and x solve (15), then 2y + x and x solve (16). If Y and X solve (16), then (Y - X)/2 and X solve (15). (Note that (Y - X)/2 must be an integer since Y and X must be of the same parity to solve (16).)

If y and x solve (15), then $y = H_{k-1}$, $x = H_k$ give a sequence with characteristic C. Then

$$2y + x = 2H_{k-1} + H_k = H_{k-1} + H_{k+1}.$$

250

[OCT.

WITH A GIVEN CHARACTERISTIC

This is often called the generalized Lucas number, corresponding to the sequence $\{H_n\}$, and is written

$$H_{k-1} + H_{k+1} = \mathfrak{L}_k.$$

Now our problem is reduced to that of looking for solutions to (16) with $0 \le X \le \sqrt{C}$. That is, we need not consider $-\sqrt{C} \le X \le 0$, because the only X term in (16) is a square term.

If we find a solution X_0 , it has a corresponding Y_0 . But this Y_0 may be taken to be positive or negative. Also, there is possibly a Y_0^* , different from Y_0 numerically, that also corresponds to X_0 . In this event, we would have that (X_0, Y_0) solves (16) for +4C, and (X_0, Y_0^*) with the -4C, or vice-versa. So, with a given X_0 , there may be four Y's that correspond, but no more.

Given a solution (X_0, Y_0) , we can obtain a sequence by letting

$$H_k = X_0, \qquad H_{k-1} = (Y_0 - X_0)/2.$$

Also, any sequence containing X_0 and having characteristic C is obtainable in this way. To see this, we let $A_k = X_0$, and observe that $(A_k, 2A_{k-1} + A_k)$ solves (16), so that $2A_{k-1} + A_k$ was one of the (possibly four) Y's that went with X_0 . Then we would have set

$$H_k = A_k, \qquad H_{k-1} = [(2A_{k-1} + A_k) - A_k]/2 = A_{k-1}$$

As for the choice of (X_0, Y_0) or $(X_0, -Y_0)$ to construct a sequence, we will obtain a sequence or its own conjugate. By taking (X_0, Y_0) , we obtain

$$H_k = X_0, \qquad H_{k-1} = (Y_0 - X_0)/2,$$

so $H_{k+1} = (Y_0 + X_0)/2$. By taking $(X_0, -Y_0)$, we obtain

$$\overline{H}_{k} = X_{0}, \qquad \overline{H}_{k-1} = (-Y_{0} - X_{0})/2 = -H_{k+1}$$

so $\{\overline{H}_n\}$ is conjugate to $\{H_n\}$.

Similarly, if we take $(-X_0, Y_0)$ or $(-X_0, -Y_0)$, we get nothing new.

As for the choice between (X_0, Y_0) and (X_0, Y_0^*) , at this point we have to say try them both. We believe that this still yields the same sequence, but as yet have no proof. This corresponds to situations in which the same number (up to absolute value) occurs twice in a sequence; for example, $\dots, -7, 5, -2, 3, 1, 4, 5, 9, \dots$ has two 5's.

At any rate, the problem of finding sequences with a given characteristic is reduced to that of finding solutions in a bounded interval to a particular diophantine equation.

REFERENCES

- Dmitri E. Thoro, "A Diophantine Algorithm," (Abstract) American Mathematical Monthly, Vol. 71, No. 3, June-July, 1964, pp. 716–717.
- Eugene Levine, "Fibonacci Sequences with Identical Characteristic Values," The Fibonacci Quarterly, Vol. 6, No. 5 (Nov. 1968), pp. 75–80).

1975]

ENUMERATION OF END-LABELED TREES*

ABBE MOWSHOWITZ

Dept. of Computer Science, University of British Columbia, Vancouver, Canada V6TIWE

and FRANK HABARY

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48104 And Department of Mathematics, Technion, Israel Institute of Technology, Haifa, Israel

Labeled trees with unlabeled endpoints were counted by Harary, Mowshowitz and Riordan [3]. Moon [5] enumated connected labeled graphs with unlabeled endpoints. In the present note we examine the complementary problem of counting trees in which only the endpoints are labeled, and in so doing develop a general technique for counting certain classes of partially labeled graphs.

Let G = (V, X) be a graph where $V = \{v_1, v_2, \dots, v_p\}$ is the set of points, and X its set of lines; see [2]. A partial labeling of G is an injection f of $N = \{1, 2, \dots, n\}$ into V for $n \le p$. A graph G together with a partial labeling f will be called partially labeled. Two partially labeled graphs (G, f_1) and (G, f_2) are identical if there is an automorphism γ of G such that $f_2(i) = \gamma(f_1(i))$ for $1 \le i \le n$.

A partially labeled tree (T, f) will be called *end-labeled* if f(N) is the set of endpoints of T. Let t(p) and T(p) denote the number of end-labeled trees and end-labeled rooted trees, respectively, having p points.

 Theorem 1.

 (1)
 t(p) = B(p-2)

 and

 (2)
 T(p) = B(p-1),

 where

$$B(n) = \sum_{k=1}^{n} S(n,k)$$

is a Bell number, i.e., S(n,k) is a Stirling number of the second kind.

Both (1) and (2) follow from the same line of argument so that only (1) will be proved. We will present two derivations of this simple result; the second illustrates a general principle for enumerating partially labeled graphs.

First Proof. Let (T,f) be a p-point end-labeled tree with $V - f(N) = \{v_{n+1}, \dots, v_p\}$, so that T may be regarded as a labeled tree. Consider the Prufer sequence $(i_1, i_2, \dots, i_{p-2})$ associated with T (see for example Moon [6] or Harary and Palmer [4]). Each i_j ($1 \le j \le p - 2$) satisfies $n + 1 \le i_j \le p$, so that the sequence $(i_1, i_2, \dots, i_{p-2})$ may be regarded as a distribution of p - 2 distinct objects into p - n identical cells with no cell empty. The number of such distributions is of course S(p - 2, p - n), and hence

$$t(p) = \sum_{n=2}^{p-1} S(p-2, p-n),$$

as asserted.

The second method requires several lemmas. Let U be the set of endpoints of a tree T, and let $\Gamma = \Gamma(T)$ denote its automorphism group. Furthermore, let us define $\Gamma^* = \Gamma^*(T)$ to be the restriction of Γ to U. Then Γ^* is well-defined since U is invariant under any automorphism of T.

^{*}This research was supported in part by grant NRC A-7328 from the National Research Council of Canada and in part by grant 73-2502 from the U.S. Air Force Office of Scientific Research.

ENUMERATION OF END-LABELED TREES

Lemma 1. For any tree T, $\Gamma(T)$ is isomorphic to $\Gamma^*(T)$.

Proof. It is clear that the mapping h defined by $\gamma \rightarrow \gamma|_U$ for any $\gamma \in \Gamma(T)$ is a homomorphism of Γ onto Γ^* . Now let γ be an arbitrary nontrivial automorphism of T. It is easy to show (see for example Prins [5, p. 17]) that there exist endpoints u and v ($u \neq v$) such that $\gamma(u) = v$. Hence, h has a trivial kernel.

Lemma 2. Let T be a tree with n endpoints. The number of distinct end-labeled copies of T is $n!/|\Gamma(T)|$.

Proof. Using Lemma 1, this follows from the argument which establishes the analogous result for labeled graphs (see for example Chao [1] or Harary and Palmer [4, p. 4]).

Second Proof of Theorem 1. Let $t^*(p,n)$ and t(p,n) be the number of labeled and end-labeled trees, respectively, having p points n of which end-points. It is well-known that

$$t^{*}(\rho,n) = \sum \frac{\rho!}{|\Gamma(T)|}$$

and by Lemma 2,

$$t(p,n) = \sum \frac{n!}{|\Gamma(T)|}$$

where both summations are over all p-point trees T with n end-points. From (3) we obtain

$$\sum \frac{1}{|\Gamma(T)|} = \frac{1}{p!} t^*(p,n) ;$$

substituting in (4) gives

Hence,

(3)

(4)

$$t(p) = \frac{1}{p!} \sum_{n=2}^{p-1} n! t^*(p,n)$$

 $t(p,n) = \frac{n!}{p!} t^*(p,n).$

and the result follows from the fact that

(see Moon [4] for several derivations of this formula).

This method of proof illustrates a general counting principle for partially labeled graphs. Let G = (V, X) be a graph which satisfies some given condition A; let S be a property defined on V; and S(G) the subset of V consisting of all points satisfying property S. Denote by $C^*(p,n)$ the number of p-point labeled graphs satisfying condition A for which |S(G)| = n, and by $C_S(p)$ the number of p-point S-labeled graphs (only the points in S(G) are labeled) satisfying condition A.

Then the next result is an immediate extension of Theorem 1, in which S(G) plays the role of the endpoints of a tree.

Theorem 2. If S(G) is invariant under every automorphism of G, and for each nontrivial automorphism γ of G, there exist distinct points u and v in S(G) such that $\gamma(u) = v$, then

$$C_{\mathcal{S}}(p) = \frac{1}{p!} \sum n! C^*(p,n),$$

where the summation is taken over all *n* such that n = |S(G)| for some *p*-point graph *G* satisfying condition *A*.

Note that this counting technique is useful only when the number of labeled graphs G satisfying a condition A can be enumerated according to the order of S(G).

REFERENCES

- 1. C. Y. Chao, "On Groups and Graphs," Trans. Amer. Math. Soc., 1.18 (1965), pp. 488-497.
- 2. F. Harary, Graph Theory, Addison-Wesley, Reading, 1969.
- F. Harary, A. Mowshowitz and J. Riordan, "Labeled trees with Unlabeled End-points," J. Combinatorial Theory, 6 (1969), pp. 60-64.
- 4. F. Harary and E.M. Palmer, Graphical Enumeration, Academic Press, New York, 1973.
- 5. J.W. Moon, "Connected Graphs with Unlabeled End-points," J. Combinatorial Theory 6 (1969), pp. 65–66.

ENUMERATION OF END-LABELED TREES

6. J.W. Moon, *Counting Labeled Trees,* Canadian Mathematical Congress, Montreal, 1970.

7. G. Prins, "On the Automorphism Group of a Tree, Doctoral Dissertation, University of Michigan, 1957.

[Continued from Page 278.]

$$U(2n + 1) = 2T_n + p(n).$$

Secondly, if one places all the partition summands in a line separated by plusses, then one deletes the plus signs at the end of each partition, so that

$$P(n) = U(n) + S(n) - p(n),$$

leading to

$$P(2n) = U(2n) + S(2n) - p(2n) = 2T_n + T_n - p(2n) = 3T_n - n - 1, \quad n \ge 1.$$

Equivalently,

$$P(2n+2) = 3T_{n+1} - (n+1) - 1 = \frac{3(n+1)(n+2)}{2} - n - 2$$
$$= \frac{3(n+1)n}{2} + \frac{3(n+1)2 - 2(n+2)}{2}$$
$$= 3T_n + 2n + 1, \quad n \ge 0.$$

More easily, we have

$$P(2n + 1) = U(2n + 1) + S(2n + 1) - p(2n + 1) = 2T_n + p(2n + 1) + T_n - p(2n + 1) = 3T_n$$

which finishes the proof.

We note that the generating function for each sequence given is easily written since the triangular numbers are involved, as

$$\sum_{n=0}^{\infty} P(2n+1)x^n = \frac{3}{(1-x)^3}$$
$$\sum_{n=0}^{\infty} P(2n+2)x^n = \frac{4-x^2}{(1-x)^3}$$

APPROXIMATION OF IRRATIONALS WITH FAREY FIBONACCI FRACTIONS

KRISHNASWAMI ALLADI

Vivekananda College, Madras 600004, India

Department of Mathematics, Institute of Advanced Studies, Australian National University, Canberra, Australia

The author in [1] had defined the Farey sequence of Fibonacci Numbers as follows:

A Farey sequence of Fibonacci Numbers of order f_n is the set of all possible fractions f_i/f_j $j \le n$ put in ascending order of magnitude $\{n, i, j \ge 0\}$, are positive integers; f_n denotes the n^{th} Fibonacci Number, $0/f_{n-1}$ is the first fraction. This set is denoted by $f \cdot f_n$.

We also defined an "INTERVAL" in $f \cdot f_n$ to consist of all fractions in $f \cdot f_n$ between fractions of the form

$$\left(\begin{array}{c} \frac{1}{f_{j}}\,,\,\frac{1}{f_{j-1}} \end{array}\right) \quad i \leq n \qquad (f_{j-1}\,,\,f_{j}) \quad j > 0 \ ,$$

j a positive integer. Two symmetry properties were established:

(1) Let h/k, h'/k', h''/k'' be three consecutive fractions in $f \cdot f_n$ all greater than 1. Further let $f_{j-1} < h/k < h'/k' < h''/k'' < f_j$. Then

(a)
$$\frac{h+h''}{k+k''} = \frac{h'}{k'} ,$$

(b)
$$kh' - hk' = f_{j-2}$$

(1*) Let h/k, h'/k', h''/k'' be three consecutive fractions in $f \cdot f_n$ all less than 1. Further let $1/f_i < h/k < h'/k' < h''/k'' < 1/f_{i-1}$. Then h + h'' = h'

(a)
$$\frac{n'+n'}{k+k''} = \frac{n'}{k'}$$
(b) $kh' - hk' = f_{i-2}$.

Many other relations of symmetries besides these are proved in [1]. 1(a), 1(b) are similar to properties which are preserved by the Farey Sequence also. Actually instead of arranging Fibonacci fractions, in ascending order, we had arranged fractions of the sequence $U_n = U_{n-1} + U_{n-2} U_1 > U_0 > 0$ integers, still some of the properties will remain. However, with the Fibonacci Sequence we get more symmetries.

The problem we discuss in this paper is the approximation of irrationals with Farey Fibonacci Fractions. We prove some theorems on best approximations.

Definition. Consider any $f \cdot f_n$. Form a new ordered set $ff_{n,1}$ consisting of all rationals in $f \cdot f_n$, together with mediants of consecutive rationals in $f \cdot f_n$. Define recursively $f \cdot f_{n,r+1}$ as all the rationals in $f \cdot f_{n,r}$ together with mediants of consecutive rationals in $f \cdot f_{n,r}$. The first rational in $f \cdot f_{n,r+1}$ is rewritten as O/f_{n+r} . We now define

$$F \cdot F_n = \bigcup_{r=1}^{n} f \cdot f_{n,r}$$

Propositions. $F \cdot F_n$ is dense in $(0, \infty)$ in the sense that its closure gives the interval $(0, \infty)$. This implies that every irrational " θ " can be approximated by a sequence of rationals h/k in $F \cdot F_n$. Without loss of generality we consider only the case $\theta > 0$, for $\theta < 0$ can be approximated by -h/k where h/k belong to $F \cdot F_n$. They are all quite obvious, and can be easily seen from (1) and (1*).

We now begin with a theorem on best approximation.

Theorem 1. (a) Let θ be an irrational > 1, say $f_{i-1} < \theta < f_i$. Then there exist infinitely many rationals $h/k \in F \cdot F_n$ for each "n" such that

$$\left| \theta - \frac{h}{k} \right| < \frac{f_{i-2}}{\sqrt{5}k^2}$$

(b) Let θ be an irrational < 1, say $1/f_i < \theta < 1/f_{i-1}$. Then there exist infinitely many $h/k \in F \cdot F_n$ for every "n" such that

$$\left|\theta-\frac{h}{k}\right|<\frac{f_{i-2}}{\sqrt{5}k^2}$$

Moreover the constant $\sqrt{5}$ is the best possible in the sense that the assertion fails if $\sqrt{5}$ is replaced by a bigger constant.

Proof. We prove only Theorem 1(a). The proof of 1(b) is similar. In proving the theorem we follow the proof of Hurwitz theorem as given in Niven's book [2].

We need the well known lemma

Lemma, It is impossible to find integers x, y such that the two inequalities simultaneously hold.

$$\frac{1}{xy} \ge \frac{1}{\sqrt{5}} \left(\frac{1}{x^2} + \frac{1}{y^2} \right); \qquad \frac{1}{x(x+y)} \ge \frac{1}{\sqrt{5}} \left(\frac{1}{x^2} + \frac{1}{(x+y)^2} \right)$$

We don't give the proof of the lemma as it is known.

Now let " θ " lie between two consecutive fractions of $f \cdot f_{n,r}$, i.e., $a/b < \theta < c/d$. It is clear that

$$\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$$
 and $\frac{a+c}{b+d} \in f \cdot f_{n,r+1}$.

Now we shall show that at least one of these fractions, say h/k, satisfies

$$\left| \theta - \frac{h}{k} \right| < \frac{f_{i-2}}{\sqrt{5k^2}}$$

Case 1. Let

and let

$$\frac{a}{b} < \frac{a+c}{b+d} < \theta < \frac{c}{d},$$

$$-\frac{a}{b} \ge \frac{f_{i-2}}{\sqrt{5}b^2}; \qquad \theta - \frac{a+c}{b+d} \ge \frac{f_{i-2}}{\sqrt{5}(b+d)^2}; \qquad \frac{c}{d} - \theta \ge \frac{f_{i-2}}{\sqrt{5}d^2}$$

These three inequalities give rise to

θ

$$\frac{c}{d} - \frac{a}{b} \ge \frac{f_{i-2}}{\sqrt{5}} \left(\frac{1}{b^2} + \frac{1}{d^2} \right) \qquad \text{and} \qquad \frac{c}{d} - \frac{a+c}{b+d} \ge \frac{f_{i-2}}{\sqrt{5}} \left(\frac{1}{d^2} + \frac{1}{(b+d)^2} \right)$$

Now by properties 1(a) and 1(b) we get

$$\frac{1}{bd} \geq \frac{1}{\sqrt{5}} \left(\frac{1}{b^2} + \frac{1}{d^2} \right); \qquad \frac{1}{d(b+d)} \geq \frac{1}{\sqrt{5}} \left(\frac{1}{d^2} + \frac{1}{(b+d)^2} \right)$$

which is a contradiction according to the lemma. Proceed similarly for the case

$$\frac{a}{b} < \theta < \frac{a+c}{b+d} < \frac{c}{d} \, .$$

Hence at least one of the three fractions, say h/k, gives

$$\left| \theta - \frac{h}{k} \right| < \frac{f_{i-2}}{\sqrt{5}k^2}$$
 .

One can very esasily see that there are infinitely many of them in $F \cdot F_n$ from the Propositions given and from the very definition of $F \cdot F_n$.

It is easy to see that $\sqrt{5}$ is the best possible constant. Consider the case when

$$\theta = \frac{1+\sqrt{5}}{2} \quad .$$

Now $f_{i-2} = 1$, and so we have

$$\left| \left| \theta - \frac{h}{k} \right| < \frac{1}{\sqrt{5}k^2}$$

for infinitely many h/k in $F \cdot F_n$. We can't obviously improve $\sqrt{5}$. This follows from the classical theorem of Hurwitz [2].

Note. (A) The counter example $(1 + \sqrt{5})/2$ which Hurwitz gave is actually the

$$\lim_{n \to \infty} \frac{f_{n+1}}{f_n}$$

(B) In the interval $\binom{1}{3}$, 3) $F \cdot F_n$ provides the same approximation as do the Farey Fractions for $f_{i-2} = 1$. In Theorem 1 the constant $\sqrt{5}$ was seen as the best possible over the interval $(0, \infty)$. That is if $\sqrt{5}$ were replaced by

a larger constant the theorems do not hold for all irrationals " θ " > 0. Now our question is the following: Is $\sqrt{5}$ the best possible constant for every "INTERVAL" (f_{i-1}, f_i) ? The answer is in the affirmative in the sense that if $\sqrt{5}$ is replaced by a larger constant the theorem fails to hold in all "INTERVALS"

$$(f_{i-1}, f_i)$$
 and $\left(\frac{1}{f_i}, \frac{1}{f_{i-1}}\right), \quad i = 2, \cdots, \infty.$

We now state and prove our final pair of theorems which are much stronger than Theorem 1.

Theorem 2a. Consider any "INTERVAL" $\{f_{i-1}, f_i\}$. Let θ be an irrational which belongs to this interval. Then for any "n" there exists infinitely many

$$\frac{n}{k} \in F \cdot F_n$$

such that

$$\left| \theta - \frac{h}{k} \right| < \frac{f_{i-2}}{\sqrt{5}k^2} .$$

The constant $\sqrt{5}$ is the best possible in the sense that if $\sqrt{5}$ are replaced by a larger constant the assertion fails for each "n" for some θ belonging to this interval.

Proof. The existence has already been established in Theorem 1. We shall concentrate on the bound

$$\frac{f_{i-2}}{\sqrt{5}}$$

 $\frac{f_{i-2}}{\sqrt{5}}$

If we show that

is the best possible constant when
$$n = 1$$
, it proves the theorem for using properties 1a, 1*a one can show $F \cdot F_{n+1}^* \subset F \cdot F_n$, where
Consider the interval
$$\begin{cases}
 F \cdot F_n^* = \left\{ x \in F \cdot F_n | x \ge 1 \right\} \\
 \left\{ \begin{array}{c}
 f_{i-1}, f_i \\
 1 \end{array} \right\}
\end{cases}$$

 $\left(\left. \frac{f_{i-1}}{1}, \frac{f_i}{1} \right) \right)$.

and call "s" the set

Let

APPROXIMATIONS OF IRRATIONALS WITH FAREY FIBONACCI FUNCTIONS

$$s_1 = \left(\frac{f_{i-1}}{1}, \frac{f_{i-1}+f_i}{11}, \frac{f_i}{1}\right).$$

Defined recursively let s_{r+1} consist of all fractions in s_r , together with the mediants of consecutive fractions in s_r . Let

$$S = \bigcup_{r=1}^{\infty} s_r.$$

Similarly let

$$s' = \left(\frac{1}{7}, \frac{2}{7} \right)$$
 and $s'_1 = \left(\frac{1}{7}, \frac{1+2}{7+7}, \frac{2}{7} \right).$

Define s'_{r+1} as all fractions in s'_r together with mediants of consecutive fractions in s'_r . Now let

$$S' = \bigcup_{r=1}^{\infty} s'_r \quad .$$

What we are interested here is S and not $F \cdot F_n$. If we compare the sets s_r , and s'_r , the following can easily be seen. (i) A one-one onto map can be established between s_r and s'_r as follows. Map

$$\frac{\nu 1 + \mu \cdot 2}{\nu \cdot 1 + \mu \cdot 1} \rightarrow \frac{\nu f_{i-1} + \mu f_i}{\nu \cdot 1 + \mu \cdot 1} \,.$$

We call two such numbers corresponding numbers.

(ii) The map says that to every $(p/q) \in s_r$ there exists a unique $(p'/q) \in s'_r$ and conversely

(iii) The distance between the consecutive numbers in s_r is f_{i-2} times the distance between consecutive numbers in s'_r .

Now let

$$\theta_0 = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \theta_1 = \frac{1+\sqrt{5}}{2} - 1.$$

Clearly

$$f_{i-1} + f_{i-2}\theta_1 = \theta'$$

is in s_r . Now if there exist infinitely many h_r/k_r in S with

$$\left| \theta' - \frac{h_r}{k_r} \right| < \frac{t_{i-2}}{ak_r^2}, \quad a > \sqrt{5} \quad r = 1, 2, \cdots$$

that (i), (ii), (iii) would imply that there exists infinitely many corresponding numbers h'_r/k_r in S' with

$$\left|\theta'-\frac{h'_r}{k_r}\right|<\frac{1}{ak_r^2}\qquad ext{with}\qquad a>\sqrt{5},$$

which is a contradiction according to Hurwitz theorem. Hence the theorem fails for θ' if $\sqrt{5}$ is replaced by a bigger constant.

Theorem 2b. Consider any interval

$$\left(\begin{array}{c} \frac{1}{f_{j}}, \frac{1}{f_{j-1}}\end{array}\right)$$
.

Let

$$\theta \in \left(\frac{1}{f_i}, \frac{1}{f_{i-1}} \right)$$

be an irrational. Then there exists infinitely many h/k in $F \cdot F_n$ for all $n \ge i$ such that

$$\left|\theta-\frac{h}{k}\right| < \frac{f_{i-2}}{\sqrt{5}k^2}$$

The constant here again in the best possible in the same sense as Theorem 2a.

Proof. The existence is already known. We just prove the converse for $F \cdot F_i$. It automatically follows for the other cases. Now let

$$s'' = \left(\frac{1}{f_i}, \frac{1}{f_{i-1}}\right) \qquad .$$

Let

1975]

$$s_{1}^{\prime\prime} = \left(\begin{array}{c} \frac{1}{f_{i}}, \frac{1+1}{f_{i-1}+t_{i}}, \frac{1}{f_{i-1}} \end{array} \right) \, .$$

Define recursively $s_{r+1}^{\prime\prime}$ as all fractions in $s_r^{\prime\prime}$ together with mediants of consecutive fractions in $s_r^{\prime\prime}$. Now

$$S'' = \bigcup_{r=1}^{\infty} s_r'' \; .$$

 $\frac{h}{k} \to \frac{k}{h} \; .$

Clearly a one-one onto map exists between $\mathcal{S}^{\prime\prime}$ and \mathcal{S}_{\cdot} Map

Consider the irrational $1/\theta' = \theta''$. Let there exist infinately many

with

$$\left|\theta'' - \frac{h_r}{k_r}\right| < \frac{f_{i-2}}{ak_r^2}$$

 $\frac{h}{k} \in F \cdot F_i$

Now if

$$\theta'' = \frac{h_r}{k_r} + \frac{\delta f_{i-2}}{ak_r^2}$$

then $|\delta| < 1/a$, Now this gives that

$$\left| \theta' - \frac{k_r}{h_r} \right| < \frac{f_{i-2}}{a \left(h_r + \frac{\delta f_{i-2}}{k_r} \right) (h_r)}$$

for infinitely many k_r/h_r in S. Now choose any $\beta > \delta$ with $\sqrt{5} < \beta < a$. Then we get

$$\left|\theta' - \frac{k_r}{h_r}\right| < \frac{f_{i-2}}{\beta h_r^2}$$

for infinitely many k_r/h_r in *S*, i.e., for all $r > r_0$ ($\beta > \sqrt{5}$).

This is a contradiction according to Theorem 2a and so Theorem 2b is proved.

REFERENCES

- K. Alladi, "A Farey Sequence of Fibonacci Numbers," *The Fibonacci Quarterly*, Vol. 12, No. 1 (February 1975) pp. 1–10.
- 2. Ivan Niven, "An Introduction to Diophantine Approximations," Chapter 1, Interscience, John Wiley and Sons.

I would like to thank Professors B.H. Neumann, F.R.S., and Kurt Mahler, F.R.S., for my award of a visiting scholarship in Canbena during the tenure of which this work was done.

A GREATEST INTEGER THEOREM FOR FIBONACCI SPACES

C. J. EVERETT

Los Alamos Scientific Laboratory, University of California, Los Alamos, New Mexico 87544

1. INTRODUCTION

If $S = \{s_j\}$ is any integer sequence of a Fibonacci space [2] based on a polynomial

$$f(x) = -a_0 - \dots - a_{n-1}x^{n-1} + x^n = (x - r_1) \cdots (x - r_n),$$

 $a_i \in Z$, r_1 real, r_i distinct, $|r_i| < 1$ for $i \ge 2$, then

$$[r_{1}^{K}s_{0} + F] = s_{k+0}$$

with any fixed k, and F on (0,1), for all \mathfrak{a} sufficiently large. This is a broad generalization, in an asymptotic sense, of a conjecture by D. Zeitlin [3] concerning the case

 $f(x) = -1 - Mx + x^2$, $M \ge 1$, F = M/(M + 1), and $S = \{0, 1, M, \dots\}$,

defined by $u_{\ell} + Mu_{\ell+1} = u_{\ell+2}$. The latter is shown to be true in all cases but one, and in slightly revised form in the remaining case.

2. A GENERAL ASYMPTOTIC THEOREM

With the polynomial

$$f(x) = -a_0 - a_1 x - \dots - a_{n-1} x^{n-1} + x^n = (x - r_1) \dots (x - r_n),$$

 a_i integers, r_1 real, r_i distinct, $|r_i| < 1$ for $i \ge 2$, we associate the *n*-space C(f) of all (complex) sequences $S = \{s_0, s_1, \dots\}$ in which s_0, \dots, s_{n-1} are arbitrary, but having

$$a_{0}s_{j} + \dots + a_{n-1}s_{j+n-1} = s_{j+n}; \quad j \ge 0$$

The *n* geometric sequences

$$R_i = \{1, r_i, r_i^2, \dots\}$$

form a basis for the space $\mathcal{C}(f)$, in terms of which an arbitrary integral sequence \mathcal{S} may be expressed in the form

$$S = c_1 R_1 + \dots + c_n R_n, \qquad \text{i.e.}, \qquad s_{\ell} = c_1 r_1^{\ell} + \dots + c_n r_n^{\ell}; \quad \ell \ge 0.$$

Since $|r_i| < 1$, $i \ge 2$, we may write

$$s_{\Omega} = c_1 r_1^{\Omega} + e_{\Omega}; \qquad e_{\Omega} \rightarrow 0$$

These results may be found in [2]. That c_1 (and hence e_2) are real is shown in an Appendix. As an immediate consequence, we have the asymptotic

Theorem 1. Let F be an arbitrary constant on the open interval (0,1), and $S = \{s_j\}$ an integral sequence of the space C(f). Then for fixed $k \ge 0$, one has the greatest integer

$$[r_1^k s_0 + F] = s_{k+0}$$

for all $\mathfrak L$ sufficiently large.

Proof. Using (1), we have only to prove

$$c_{1}r_{1}^{k+1} + e_{k+2} \leq r_{1}^{k}(c_{1}r_{1}^{2} + e_{2}) + F < c_{1}r_{1}^{k+2} + e_{k+2} + 1$$

for large 2, i.e.,

(1)

$$e_{k+\varrho} - r_1^k e_{\varrho} \leq F < e_{k+\varrho} - r_1^k e_{\varrho} + 1$$

and this is obvious since $e_{\ell} \rightarrow 0$ and 0 < F < 1.

This research was performed under the auspices of the U.S. Atomic Energy Commission.

260

OCT. 1975

3. THE ZEITLIN CONJECTURE

For the integer $M \ge 1$, let

 $f(x) = 1 - Mx + x^2 = (x - a)(x - b), \quad a > b, \text{ and } F = M/(M + 1).$ The roots a, b have the properties

 $a > M, \quad b < 0, \quad |b| = (\rho - M)/2 < 1, \quad ab = -1, \quad a - b = \rho; \quad \rho \equiv (M^2 + 4)^{\frac{1}{2}}.$ The sequence $U = \{u_0, u_1, \dots\}$ is defined recursively by

$$u_0 = 0, \quad u_1 = 1, \quad u_{\ell} + M u_{\ell+1} = u_{\ell+2}; \quad \ell \ge 0,$$

and is well known [2], p. 103, to be related to the roots by $u_{\ell} = \rho^{-7} (a^{\ell} - b^{\ell}); \quad \ell \ge 0.$

From this we find

$$a^{k}u_{\varrho} = \rho^{-1}(a^{k+\varrho} - b^{k+\varrho}) - \rho^{-1}b^{\varrho}(a^{k} - b^{k}),$$

or (2)

2) $a^k u_{\ell} = u_{k+\ell} - b^{\ell} u_k$. *Theorem 2.* For the sequence *U*, one has the greatest integer

$$[a^k u_{\mathfrak{Q}} + F] = u_{k+\mathfrak{Q}}$$

for $x \ge 2$, k = 1, and for $x \ge k \ge 2$ except possibly in the case x odd $\ge k$ odd ≥ 3 when $M \ge 2$.

Proof. We only sketch the argument, which closely follows that in [1]. In all cases, the final verification consists in the laborious comparison of two polynomials in M, for $M \ge 1$. The required relation

$$u_{k+\mathfrak{Q}} \leq a^{\kappa} u_{\mathfrak{Q}} + F < u_{k+\mathfrak{Q}} + 1$$

is seen from (2) to be equivalent to

$$-1/(M+1) < b^{\chi}u_{k} \leq M/(M+1)$$

Case I. $\& \ge 2$, k = 1. For & even, it suffices to prove $b^2 \le M/(M + 1)$. For & odd, $|b|^3 \le 1/(M + 1)$ suffices. These are found to hold upon replacing |b| by its value $(\rho - M)/2$ and rationalizing.

Case II. $\mathfrak{L} \ge k \ge 2$. For \mathfrak{L}, k even, it suffices to show $b^k u_k \le M/(M + 1)$. But

$$b^{k}u_{k} = b^{k}\rho^{-1}(a^{k}-b^{k}) = \rho^{-1}(1-b^{2k}) < M/(M+1)$$

will hold for all k iff $\rho^{-1} < M/(M + 1)$, which is verified as before. For \mathfrak{L} even $\ge k$ odd ≥ 2 , $b^{k+1}u_k < M/(M + 1)$ suffices. Now,

$$b^{k+1}u_k = |b|\rho^{-1}(1+b^{2k})$$

by an ananogous step, so we need only show that

$$|b|\rho^{-1}(1+b^6) \leq M/(M+1)$$

This is the most laborious verification.

For \mathfrak{L} odd $\ge k$ even ≥ 2 , it suffices to prove $-b^{k+1}u_k < 1/(M+1)$. Here we find

$$-b^{k+1}\rho^{-1}(a^k-b^k) = |b|\rho^{-1}(1-b^{2k}) < 1/(M+1).$$

since in the limit, $|b|\rho^{-1} < 1/(M + 1)$. This is easy. Finally,

suppose 2 odd
$$\geq k$$
 odd ≥ 2 , and $M = 1$. It suffices to prove

$$-b^{\kappa}u_{k} \equiv \rho^{-1}(1+b^{2\kappa}) < 1/(M+1), \quad k \ge 3,$$

and this is true since $\rho^{-1}(1+b^6) < 1/(M+1)$ is verifiable when M = 1 (and only then).

The relation of Theorem 2 may fail in the remaining case, as is easily seen from the example M = 2, x = k = 3, where . ?

$$[a^{\circ}u_3 + F] = 71 = 1 + u_6.$$

Indeed it always fails for $M \ge 2$, $\ell = k$ odd ≥ 3 , as appears in the final

Theorem 3. For the sequence U, with $M \ge 2$, \mathfrak{L} odd $\ge k$ odd ≥ 2 , the value of $[a^k u_{\mathfrak{L}} + F]$ is either $u_{k+\mathfrak{L}}$ or $u_{k+\mathfrak{L}}$ + 1, according as $|b|^{\varrho}u_{k} < 1/(M+1)$ or $1/(M+1) \le |b|^{\varrho}u_{k}$, the latter always obtaining for $\varrho = k$.

Proof. Using (2), the relations of the theorem are found to be equivalent, respectively, to

A GREATEST INTEGER THEOREM FOR FIBONACCI SPACES

We note first that $|b|^{\ell}u_k$ is always between -M/(M + 1) and (M + 2)/(M + 1). The first is obvious. For the second, it suffices to prove $|b|^k u_k < (M + 2)/(M + 1)$, k odd ≥ 3 . But

$$|b|^{k}u_{k} = \rho^{-1}(1+b^{2k}) \leq (M+2)/(M+1)$$

holds provided

$$p^{-1}(1+b^6) < (M+2)/(M+1),$$

which may be verified as in Theorem 2, Case II, second part.

Hence for fixed k, we consider the relation of $|b|^{\varrho}u_k$ to 1/(M + 1) as ϱ increases from k. Now if at the start we had

$$|b|^{\kappa}u_{k} \equiv \rho^{-1}(1+b^{2\kappa}) < 1/(M+1)$$

this would imply $\rho^{-1} < 1/(M+1)$, which is false for all $M \ge 2$. The theorem follows.

ĥ

APPENDIX Reality of c_1 , e_{Ω}

 $\begin{vmatrix} R_1 \\ \vdots \\ R_n \end{vmatrix} = \begin{vmatrix} 1 & r_1 & \cdots & r_1^{n-1} \\ \vdots & & & \\ 1 & r_n & \cdots & r_n^{n-1} \end{vmatrix} \begin{vmatrix} U_0 \\ \vdots \\ U_{n-1} \end{vmatrix} ,$

From [2] we write

(3)

where

$$U_{0} = \left\{ 1, 0, \cdots, 0, a_{0}, \cdots \right\}, \cdots, U_{n-1} = \left\{ 0, 0, \cdots, 1, a_{n-1}, \cdots \right\}$$

is an obvious basis, and the matrix determinant Δ is that of Vandermonde. Inversion gives

$$\begin{vmatrix} U_{0} \\ \vdots \\ U_{n-1} \end{vmatrix} = \begin{vmatrix} r_{01} & \cdots & r_{0n} \\ \vdots & \vdots \\ r_{n-1,1} & \cdots & r_{n-1,n} \end{vmatrix} \begin{vmatrix} R_{1} \\ \vdots \\ R_{n} \end{vmatrix}$$

where

(4)

$$r_{jk} = (-1)^{J^{+\kappa}} R_{kj} / \Delta,$$

and R_{kj} is the *k,j*-minor of the matrix in (3). Since

$$S = |s_0 \cdots s_{n-1}| \cdot \begin{vmatrix} U_0 \\ \vdots \\ U_{n-1} \end{vmatrix} = |s_0 \cdots s_{n-1}| \cdot |r_{jk}| \cdot \begin{vmatrix} R_1 \\ \vdots \\ R_n \end{vmatrix}$$

we see that

$c_1 = s_0 r_{01} + \dots + s_{n-1} r_{n-1,1}$

involving the first column of the inverse in (4). But each $r_{j,1}$ involves the quotient R_{1j}/Δ . The latter is real, since any complex roots r_i occur in pairs of conjugates.

REFERENCES

- 1. Robert Anaya and Janice Crump, "A Generalized Greatest Integer Function Theorem," *The Fibonacci Quarter-* /y, Vol. 10, No. 2 (February 1972), pp. 207–211.
- E.D. Cashwell and C.J. Everett, "Fibonacci Spaces," *The Fibonacci Quarterly*, Vol. 4, No. 2 (April 1966), pp. 97
 –115.

3. D. Zeitlin, "A Conjecture for Integer Sequences," Am. Math. Soc. Notices, Abstract 72T-A282.

262
PRIMITIVE PYTHAGOREAN TRIPLES WITH SUM OR DIFFERENCE OF LEGS EQUAL TO A PRIME*

DELANO P. WEGENER Central Michigan University, Mt. Pleasant, Michigan 48858

1. INTRODUCTION

A pythagorean triple is a triple of natural numbers (x, y, z) such that $x^2 + y^2 = z^2$. Such a triple is called a primitive pythagorean triple if the components are relatively prime in pairs. It is well known [5, pp. 4–6] that all primitive pythagorean triples are given, without duplication, by:

(1.1)
$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2$$

where *m* and *n* are relatively prime natural numbers which are of opposite parity and satisfy m > n. Conversely, if *m* and *n* (m > n) are relatively prime natural numbers of opposite parity, then they generate a primitive pythagorean triple according to (1.1).

In this paper I will adhere to the following conventions:

- (a) The first entry of a pythagorean triple will be the even leg of the triple.
- (b) The second entry of a pythagorean triple will be the odd leg of the triple.
- (c) The third entry of a pythagorean triple will be the hypotenuse and will never be called a leg of the triple.
- (d) The natural numbers m and n in Eq. (1.1) will be called the generators of the triple (x, y, z).

Since every prime of the form 4k + 1 can be written as the sum of two relatively prime natural numbers [6, p. 351] it follows that there are infinitely many primitive pythagorean triples with the hypotenuse equal to a prime. It is also easy to see that there are infinitely many primitive pythagorean triples with the odd leg equal to a prime, by noting that for any odd prime p, m = (p + 1)/2 and n = (p - 1)/2 generate a primitive pythagorean triple with the odd leg equal to a prime, by noting that for any odd prime p, m = (p + 1)/2 and n = (p - 1)/2 generate a primitive pythagorean triple with the odd leg equal to a prime. It is completely trivial to show that the even leg is never a prime. Thus it is an easy problem to determine whether there are an infinite number of primitive pythagorean triples with any one of its components equal to a prime. However, the problem changes drastically if we try to determine whether there are an infinite number of primitive pythagorean triples with more than one component or some linear combination of the components equal to a prime. For example Waclaw Sierpinski [5, p. 6], [7, p. 94] raised the following question:

SIERPINSKI'S PROBLEM: Are there an infinite number of primitive pythagorean triples with both the hypotenuse and the odd leg equal to a prime?

This problem is equivalent to asking for an infinite number of solutions, in primes, to the Diophantine equation $q^2 = 2p - 1$. This equivalence is easily proved by noting that if (t,q,p) is a primitive pythagorean triple with p and q both prime, then

$$q^2 = p^2 - t^2 = (p - t)(p + t).$$

Since q is prime and p + t > p - t > 0, it follows that $q^2 = p + t$ and p - t = 1. Hence $q^2 = 2p - 1$. Conversely, if $q^2 = 2p - 1$, then (p - 1, q, p) is a primitive pythagorean triple. Other than this simple transformation, it seems that no progress has been made toward a solution to Sierpinski's problem.

As a result of his involvement with Sierpinski's Problem, Professor I.A. Barnett was quite naturally led to the following similar questions.

^{*}The research for this paper was supported in part by Ohio University Research Grant number OUR 252.

PRIMITIVE PYTHAGOREAN TRIPLES WITH SUM

OUESTION A: Are there an infinite number of primitive pythagorean triples for which the sum of the legs is a prime?

QUESTION B: Are there an infinite number of primitive pythagorean triples for which the absolute value of the difference of the legs is a prime?

QUESTION C: Are there an infinite number of primitive pythagorean triples for which both the sum of the legs and the absolute value of the difference of the legs are prime?

Questions A and B are both answered in the affirmative [8]. In this paper we present a complete characterization of those triples which have either the sum or the difference of the legs equal to a prime. Question C is much more difficult and is discussed in some detail in this author's Ph.D. dissertation. The results related to Question C will be the subject of a future paper.

A few basic facts about the integral domain

$$Z[\sqrt{2}] = \left\{ a + b\sqrt{2} \mid a, b \in Z \right\}$$

and about the Pell equation $u^2 - 2v^2 = p$, where p is a prime, will facilitate the discussion of Questions A and B. The facts about the integral domain $Z[\sqrt{2}]$ will simply be stated with references to the proofs. However, the discussion of $u^2 - 2v^2 = p$ in Section 3 will be more detailed because it is quite elementary and is significantly different from the usual discussions of this particular Pell equation.

2. THE INTEGRAL DOMAIN $Z[\sqrt{2}]$

For the remainder of this article, I will follow the usual custom of referring to elements of $Z[\sqrt{2}]$ as integers and elements of Z as rational integers and I will use the following notation:

 $a = a + b\sqrt{2}$

 $\overline{a} = a - b\sqrt{2}$

 $N(a) = a\overline{a}$

 $R(\alpha) = a$

I(a) = b

 $\epsilon = 1 + \sqrt{2}$

 $e^{-1} = -1 + \sqrt{2}$

t	h	e	n
•	••	•	

is called the conjugate of a.

is called the norm of a.

is called the rational part of a.

is called the irrational part of a.

is called the fundamental unit in $Z[\sqrt{2}]$.

is called the inverse of ϵ .

As usual, a unit of $Z[\sqrt{2}]$ is defined to be a non-zero element of $Z[\sqrt{2}]$ which has an inverse in $Z[\sqrt{2}]$, or equivalently, an element of $Z[\sqrt{2}]$ whose norm is ± 1 . The set of units of $Z[\sqrt{2}]$ is precisely the set of

$$\{+\epsilon^{\eta} \mid n \in Z\}$$

[4, p. 235], [2, p. 209] and for this reason e is called the fundamental unit of $Z[\sqrt{2}]$.

If a and δ are integers and there is a unit γ such that $a = \delta \gamma$, then a is called an associate of δ . A non-zero element of $Z[\sqrt{2}]$, which is not a unit, is a prime if and only if it is divisible only by units and associates of itself. It is easily shown that if a and δ are associates, then

$$N(a) = +N(\delta),$$

but the converse is in general not true. However, if α and δ are both primes and $N(\alpha) = \pm N(\delta)$, then α is an associate of either δ or $\overline{\delta}$. The primes of $Z[\sqrt{2}]$ are all associates of:

(1) $\sqrt{2}$

(2) All rational primes of the form $8k \pm 3$. These are frequently called prime of the second degree.

(3) All conjugate factors of rational primes of the form $8k \pm 1$. These are frequently called primes of the first degree. This result is found in any discussion of the integral domain $Z[\sqrt{2}]$, for example [4, p. 240], [2, p. 221].

Each of the properties, listed below, in Lemma 2.1, is an elementary consequence of the definitions of the symbols involved. Consequently, they are listed without proof.

Lemma 2.1: If a and β are integers, then

$$a + \overline{a} = 2R(a)$$

$$a - \overline{a} = 2\sqrt{2}I(a)$$

$$R(a\beta) = R(a)R(\beta) + 2I(a)I(\beta)$$

$$I(a\beta) = I(a)R(\beta) + R(a)I(\beta)$$

$$R(a\overline{\beta}) = R(a)R(\beta) - 2I(a)I(\beta)$$

$$I(a\overline{\beta}) = R(\beta)I(a) - R(a)I(\beta)$$

$$R(a\epsilon) = R(a) + 2I(a)$$

$$I(a\epsilon) = R(a) + I(a)$$

3. THE PELL-TYPE EQUATION
$$u^2 - 2v^2 = p$$

Most number theory books have some discussion of the Pell equation and Pell-type equations. A particularly good discussion is to be found in Chapter VI of [3] and a very detailed history is found in Chapter XII of [1]. In this paper we only need consider the very special Pell-type equation

$$u^2 - 2v^2 = \rho,$$

where *p* is a rational prime.

As usual, any two rational integers u = a, v = b will be called a solution of Eq. (3.1) if $a^2 - 2b^2 = p$. It follows from the previous section that u = a, v = b is a solution if and only if

$$N(a+b\sqrt{2}) = p$$
.

From the discussion of primes in $Z[\sqrt{2}]$, it is clear that Eq. (3.1) has a solution if and only if the rational prime p is of the form $8k \pm 1$.

lf

(3.1)

$$N(a+b\sqrt{2}) = p$$

then the four solutions

u = a, v = b; u = a, v = -b; u = -a, v = b; u = -a, v = -b

are said to be the solutions obtained from $a + b\sqrt{2}$. Notice that the same four solutions are obtained from each of

$$+b\sqrt{2}$$
, $\overline{a+b\sqrt{2}}$, $-(a+b\sqrt{2})$ and $\overline{-(a+b\sqrt{2})}$.

It is easily shown [4, p. 242] that if $a = a + b\sqrt{2}$ and N(a) = p, then all solutions of Eq. (1.2) are obtained from $\left\{ ae^{2t} | t \in Z \right\}$

 $\left\{a\epsilon^{2t} \mid t \in Z\right\}$

а

yields a solution of Eq. (3.1).

The equation

 $u^2 - 2v^2 = p$

PRIMITIVE PYTHAGOREAN TRIPLES WITH SUM

may easily be transformed to the equation

$$\frac{u^2}{(\sqrt{\bar{p}})^2} - \frac{v^2}{(\sqrt{p/2})^2} = 1,$$

which is the standard equation of a hyperbola. Thus integer solutions of Eq. (3.1) are easily associated with lattice points on the above hyperbola. Figure 1 is a graph of this hyperbola. Reference to Fig. 1 makes it clear that if u = a > 0 and v = b > 0 is a solution of Eq. (3.1), and then

$$\sqrt{p} < a < \sqrt{2p}$$
 and $0 < b < \sqrt{p/2}$

are equivalent. The remainder of this section will show that there is exactly one solution which satisfies these conditions.





If p is a rational prime of the form $8k \pm 1$, then the set

$$S = \{ (u,v) \mid u \in Z, v \in Z, u > 0, v > 0, u^2 - 2v^2 = p \}$$

is infinite and contains an element (a, b) with minimal first component. Since

$$(a + b\sqrt{2})\epsilon^{-2} = (3a - 4b) + (3b - 2a)\sqrt{2}$$

it follows that

u = 3a - 4b and v = 3b - 2a

satisfy

$$u^2 - 2v^2 = p.$$

[OCT.

Note that

$$a^2 - 2b^2 = p > 0$$

implies that $b < a/\sqrt{2}$. Thus

$$3a-4b > 3a-4a\sqrt{2} = a(3-2\sqrt{2}) > 0.$$

Hence either

$$(3a - 4b, 3b - 2a)$$
 or $(3a - 4b, 2a - 3b)$

is in S. In either case we have

which implies that

$$4b^2 \leq a^2 = p + 2b^2$$
,

 $a \leq 3a - 4b$,

and this in turn implies that $b < \sqrt{p/2}$. Hence there is at least one solution u = a, v = b of $u^2 - 2v^2 = p$ with

$$\sqrt{p} < a < \sqrt{2p}$$
 and $0 < b < \sqrt{p/2}$

To show that there is only one solution of (3.1) which satisfies the above inequalities it is helpful to observe that: For every $\beta \in Z[\sqrt{2}]$,

$$\begin{aligned} R(\beta\epsilon^2) &= 3R(\beta) + 4I(\beta) \\ I(\beta\epsilon^2) &= 2R(\beta) + 3I(\beta) \\ R(\beta\epsilon^{-2}) &= 3R(\beta) - 4I(\beta) \\ I(\beta\epsilon^{-2}) &= 3I(\beta) - 2R(\beta). \end{aligned}$$

It follows from these equalities that if $R(\beta) > 0$ and $I(\beta) > 0$, then

$$R(\beta\epsilon^{-2}) < R(\beta\epsilon^{2})$$
 and $R(\beta\epsilon^{2t}) < R(\beta\epsilon^{2t+2})$

for all $t \ge 0$. Note also that if $R(\beta) > 0$, then $I(\beta) < 0$ implies that

$$R(\beta\epsilon^{-2t}) < R(\beta\epsilon^{-2t-2})$$

for all t > 0.

Let $a = a + b\sqrt{2}$ with

 \sqrt{p} < a < $\sqrt{2p}$ and θ < b < $\sqrt{p/2}$

and let u = a, v = b be a solution of (3.1). Then

$$a\epsilon^2 = (3a + 4b) + (2a + 3b)\sqrt{2}$$

and

 $a\epsilon^{-2} = (3a - 4b) + (3b - 2a)\sqrt{2}$.

Clearly

$$3a-4b < 3a+4b$$

and from the previous remarks it follows that the rational parts of ae^{2t} , $t \ge 0$, form a strictly increasing sequence. If we assume that $3b - 2a \ge 0$, then $9b^2 \ge 4a^2$ and hence

 $-4p + b^2 = -4(a^2 - 2b^2) + b^2 > 0.$

But then $b^2 \ge 4p$ and

$$b \ge 2\sqrt{p} > (1/\sqrt{2})\sqrt{p} = \sqrt{p/2}$$
.

1975]

[OCT.

This contradiction shows that 3b - 2a < 0 and from the previous remarks it follows that the rational parts of ae^{-2t} , t > 1, form an increasing sequence.

If we assume $3a - 4b \le a$, then $a^2 \le 4b^2$ and hence

$$p - 2b^2 = a^2 - 2b^2 - 2b^2 = a^2 - 4b^2 \leq 0.$$

But then $\sqrt{p/2} \le b$ and we conclude that

$$3a-4b > a > \sqrt{p} > 0$$
.

It now follows that if

$$3a-4b > \sqrt{2p}$$
 ,

then the rational part of ae^{2t} will be greater than $\sqrt{2p}$ for all $t \neq 0$. If we assume

 $3a-4b \leqslant \sqrt{2p}$,

$$17a^2 - 10p \le 24a\sqrt{(a^2 - p)/2}$$
 .

Note that

$$17a^2 - 10p = 7a^2 + 20b^2 > 0.$$

Squaring both sides again and simplifying yields

$$a^4 - 52a^2p + 100p^2 \leq 0$$
,

which can be written as

$$(a^2 - 10p)^2 \leq 32a^2p$$
.

This is a contradiction because

$$a^2 - 10p < 2p - 10p = -8p$$

and hence

$$(a^2 - 10p)^2 > 64p^2 = (32p)(2p) > 32pa^2$$

Thus

$$3a-4b > \sqrt{2p}$$

This establishes that there is at most one solution u = a, v = b such that $\sqrt{p} < a < \sqrt{2p}$. The material in this section is summarized in Lemma 3.2 below:

Lemma 3.2. If p is a rational prime of the form $8k \pm 1$, the equation $u^2 - 2v^2 = p$ has exactly one solution u = a, v = b such that the following two equivalent statements are true:

(i)
$$\sqrt{p} < a < \sqrt{2p}$$

(ii)
$$0 < b < \sqrt{p/2}$$
.

The equation $u^2 - 2v^2 = p$ has infinitely many solutions, all of which are obtained from

$$(a + b\sqrt{2})e^{2t}$$

where t is any rational integer and u = a, v = b is any solution of $u^2 - 2v^2 = p$.

OR DIFFERENCE OF LEGS EQUAL TO A PRIME

The unique solution which satisfies (i) and (ii) will be called the *fundamental solution* of $u^2 - 2v^2 = p$.

4. PRIMITIVE PYTHAGOREAN TRIPLES WITH SUM OF LEGS EQUAL TO A PRIME

The theorems of this section show that if (x,y,z) is a primitive pythagorean triple with x + y equal to a prime p, then p is of the form $8k \pm 1$, and conversely, if p is a prime of the form $8k \pm 1$, then there is a unique primitive py-thagorean triple (x,y,z) such that x + y = p. Since there are infinitely many primes of the form $8k \pm 1$, this yields an affirmative answer to Question A of Section 1.

Theorem 4.1. If (x, y, z) is a primitive pythagorean triple and p is a prime divisor of x + y or |x - y|, then p is of the form 8k + 1.

Proof. Suppose p divides x + y or |x - y|. Note this implies (x,p) = (y,p) = 1, and $x = \pm y \pmod{p}$ so that

(1)
$$2x^2 = x^2 + y^2 = z^2 \pmod{p}.$$

By definition, x^2 is a quadratic residue of p. The congruence (1) implies $2x^2$ is also a quadratic residue of p. If p were of the form $8k \pm 3$, then 2 would be a quadratic nonresidue of p [3, pp. 136–139] and since x^2 is a quadratic residue of p, $2x^2$ would be a quadratic nonresidue of p, contradicting (1). Thus p must be of the form $8k \pm 1$.

Corollary. If x and y are the legs of a primitive pythagorean triple, then both x + y and |x - y| are of the form 8k + 1.

This corollary is immediate from the theorem but it should be pointed out that the corollary may be proved directly by considering the following two cases:

$$m = 2r, \quad n = 2t + 1$$

 $m = 2r, + 1, \quad n = 2t,$

where *m* and *n* are the generators of the primitive pythagorean triple.

Theorem 4.2. For every prime p of the form $8k \pm 1$ there exists a primitive pythagorean triple (x, y, z) such that x + y = p.

Proof. Let p be a prime of the form $8k \pm 1$ and let u = a, v = b be the fundamental solution of $u^2 - 2v^2 = p$. Let m = a - b and n = b. Note (m, n) = 1 because (a, b) = 1. Clearly m and n are of opposite parity because m + n = a = 1 (mod 2). If $m \le n = b$, then

$$p + 2b^2 = a^2 = (n + m)^2 \leq 4b^2$$

and thus $b \ge p/2$, a contradiction. Hence m > n. Thus m and n generate the primitive pythagorean triple

$$x = 2mn$$
, $y = m^2 - n^2$, $z = m^2 + n^2$.

For this triple

$$x + y = 2mn + m^2 - n^2 = (m + n)^2 - 2n^2 = a^2 - 2b^2 = p.$$

Theorem 4.3. If p is a prime of the form $8k \neq 1$, then there is exactly one primitive pythagorean triple (x, y, z) such that x + y = p.

Proof. Let m and n generate a primitive pythagorean triple (x, y, z) such that x + y = p. Then

PRIMITIVE PYTHAGOREAN TRIPLES WITH SUM

Since m > n it follows that

$$p = (m + n)^2 - 2n^2 > (2n)^2 - 2n^2 = 2n^2$$
,

which implies that $n < \sqrt{p/2}$. Thus u = m + n, v = n is the fundamental solution of $u^2 - 2v^2 = p$, and hence, by Lemma 3.2, m and n are uniquely determined.

5. PRIMITIVE PYTHAGOREAN TRIPLES WITH DIFFERENCE OF LEGS EQUAL TO A PRIME

The material in this section is related to Question B of Section 1. The first theorem provides an affirmative answer to Question B by showing that every prime of the form $8k \pm 1$ is equal to the difference of the legs of some primitive pythagorean triple. The second theorem shows that for every prime of the form $8k \pm 1$ there is an infinite number of primitive pythagorean triples with the difference of legs equal to that prime. W.P. Whitlock, Jr. [8] discusses briefly these same two theorems and points out that these methods were essentially known to Frenicle. The remainder of this section is devoted to the characterization of all primitive pythagorean triples with difference of legs equal to a prime.

Theorem 5.1. For every prime p of the form $8k \pm 1$ there is a primitive pythagorean triple (x, y, z) such that |x - y| = p.

Proof. Let p be any prime of the form $8k \pm 1$ and let u = a, v = b be the fundamental solution of $u^2 - 2v^2 = p$. Then, as in Theorem 4.2, it is easily shown that m = a + b and n = b generate a primitive pythagorean triple (x, y, z) with x - y = -p.

If ρ is a prime of the form $8k \pm 1$, then, as pointed out in Section 4, there is a unique primitive pythagorean triple (x, y, z) such that $x + y = \rho$. The fact that there is no such uniqueness when discussing the difference of legs follows from the theorem below.

Theorem 5.2. If m,n (m > n) generate a primitive pythagorean triple (x,y,z) then M = 2m + n and N = m generate a primitive pythagorean triple (X, Y, Z) such that |X - Y| = |x - y|.

The proof is computational and is left to the reader.

The previous two theorems make it easy to show that for each prime p of the form $8k \pm 1$ there is an infinite number of primitive pythagorean triples (x, y, z) such that |x - y| = p. This is done by defining an infinite sequence

$$\{T_j(p)\}$$

of primitive pythagorean triples (x_i, y_i, z_i) such that $|x_i - y_i| = p$ for all j.

Definition 1. Let p be a fixed prime of the form $8k \pm 1$ and let a and b be the unique natural numbers such that

 $a^2 - 2b^2 = p$, $\sqrt{p} < a < \sqrt{2p}$, and $0 < b < \sqrt{p/2}$.

Define the sequence $\{T_i(p)\}$ as follows:

Let $T_o(p)$ be the primitive pythagorean triple generated by $m_0^* = a + b$ and n = b. For all $j \ge 1$, define $T_j(p)$ to be the primitive pythagorean triple generated by

 $m_i = 2m_{i-1} + n_{i-1}$, and $n_i = m_{i-1}$.

Figures 2 and 3 illustrate the sequence $\{T_i(p)\}$.

An examination of a table of primitive pythagorean triples shows that for each prime p of the form $8k \pm 1$ there are primitive pythagorean triples (x, y, z) with |x - y| = p which are not in $\{T_j(p)\}$. The next theorem will be used to show that for each prime p of the form $8k \pm 1$ there is in fact another infinite sequence $\{T_j(p)\}$ of primitive



1975]

OR DIFFERENCE OF LEGS EQUAL TO A PRIME

271



PRIMITIVE PYTHAGOREAN TRIPLES WITH SUM

272

pythagorean triples (x_j, y_j, z_j) such that

$$|x_j - y_j| = p$$

for $j \ge 1$ and

 $x'_i + y'_i = p$

for *j = 0,*

Theorem 5.3. If m and n (m > n) generate a primitive pythagorean triple (x, y, z), then M = 2m - n and N = .m generate a primitive pythagorean triangle (X, Y, Z) such that |X - Y| = x + y.

The proof is computational and is left to the reader.

Definition 2. Let p, a and b be the same as in the construction to $\{T_j(p)\}$. Define the sequence $\{T'_j(p)\}$ as follows: Let $T'_0(p)$ be the triple generated by $m'_0 = a - b$ and $n'_0 = b$. Let $T'_1(p)$ be the triple generated by

$$m'_1 = 2m'_0 - n'_0$$
 and $n'_1 = m'_0$

For all $j \ge 2$, define $T'_i(p)$ to be the primitive pythagorean triple generated by

$$m'_{j} = 2m'_{j-1} + n'_{j-1}$$
 and $n'_{j} = m'_{j-1}$

Figures 2 and 3 illustrate the sequence $\left\{ \Gamma_{i}(p) \right\}$

Theorem 5.4. Let p be a prime of the form 8k + 1. If T is the set of triples

 $\left\{ T_{j}(p) \mid j = 0, \, 1, \, 2, \, \cdots \right\}$

and \mathcal{T}' is the set of triples $\{\mathcal{T}'_j(p)| j = 1, 2, \cdots\}$, then $\mathcal{T} \cap \mathcal{T}' = \phi$.

Proof. Suppose there is a $T_r(p)$ in T and a $T'_s(p)$ in T' such that $r \ge 1$, $s \ge 2$ and $T_r(p) = T'_s(p)$. Then $m_r = m'_s$ and $n_r = n'_s$ and hence

$$m_{r-1} = n_r = n'_s = m'_{s-1}$$
,

which in turn implies

$$2m'_{s-1} + n_{r-1} = 2m_{r-1} + n_{r-1} = m_r = m'_s = 2m'_{s-1} + n'_{s-1}$$

and thus $n_{r-1} = n'_{s-1}$. Hence

$$T_{r-1}(p) = T'_{s-1}(p).$$

Repeating this argument a finite number of times results in one of the following cases:

Case 1. $T_{0}(p) = T'_{s-r}(p)$ if s > r+1.

Case 2. $T_{0}(p) = T'_{1}(p)$ if s = r + 1.

Case 3.
$$T_{r-s}(p) = T'_{1}(p)$$
 if $s < r + 1$.

To complete the proof it suffices to show that each of these cases is impossible. In Case 1,

$$b = n_0 = n'_{s-r} = m'_{s-r-1} > n'_{s-r-1} = \cdots = m'_0 > n'_0 = b,$$

a contradiction. In Case 3;

$$m_{r-s-1} = n_{r-s} = n'_1 = m'_0$$

and

274

$$2m_{r-s-1} + n_{r-s-1} = m_{r-s} = m'_1 = 2m'_0 = n'_0.$$

Hence

$$0 < n_{r-s-1} = -n_0' < 0$$

which is again a contradiction.

The above description of the sequences

$$\{T_j(p)\}$$
 and $\{T'_j(p)\}$

gives a convenient method for constructing a triple of the sequence from the preceding triple. It is also possible to give an explicit formula for a triple in the sequence in terms of the fundamental solution of $u^2 - 2v^2 = p$. Certain properties of the triples in the sequence become more accessible when viewed in this way. One such property is stated in Theorem 5.6.

Theorem 5.5. Let p be a prime of the form $8k \pm 1$. Let u = a, v = b be the fundamental solution of

$$u^2 - 2v^2 = p$$

and let

.

$$a = a + b\sqrt{2}$$
.

(1) For $j \ge 0$, $T_j(p)$ is generated by:

$$m_{j} = R(ae^{j}) + I(ae^{j}) = I(ae^{j+1})$$
$$n_{j} = I(ae^{j}).$$

(2) For j > 0, $T'_j(p)$ is generated by:

$$m'_{j} = R(\overline{a}e^{j}) + I(\overline{a}e^{j}) = I(\overline{a}e^{j+1})$$
$$n'_{j} = I(\overline{a}e^{j}).$$

(3) For $j \ge 0$, $T_j(p)$ is generated by:

$$m_{j} = \frac{e^{j+1} - \overline{e}^{j+1}}{2\sqrt{2}} a + \frac{e^{j+1} + \overline{e}^{j+1}}{2} b$$
$$n_{j} = \frac{e^{j} - \overline{e}^{j}}{2\sqrt{2}} a + \frac{e^{j} + \overline{e}^{j}}{2} b$$

(4) For j > 0, $T'_j(p)$ is generated by:

$$\begin{split} m'_{j} &= \frac{\epsilon^{j+1} - \overline{\epsilon}^{j+1}}{2\sqrt{2}} \ a - \frac{\epsilon^{j+1} + \overline{\epsilon}^{j+1}}{2} \ b \\ n'_{j} &= \frac{\epsilon^{j} - \overline{\epsilon}^{j}}{2\sqrt{2}} \ a - \frac{\epsilon^{j} + \overline{\epsilon}^{j}}{2} \ b \ . \end{split}$$

Ξ.

۰.

Ċ

Proof (of (1)). By construction, $T_o(p)$ is generated by

$$m_0 = a + b = R(a\epsilon^0) + I(a\epsilon^0)$$

and

$$n_0 = b = I(ae^0).$$

Make the induction hypothesis that $T_i(\rho)$ is generated by

$$m_j = R(\alpha \epsilon^j) + I(\alpha \epsilon^j)$$
 and $n_j = I(\alpha \epsilon^j)$.

Then by construction, $T_{j+1}(p)$ is generated by

$$m_{j+1} = 2R(a\epsilon^j) + 3I(a\epsilon^j)$$
 and $n_j = R(a\epsilon^j) + I(a\epsilon^j)$.

By Lemma 2.1,

$$R(a\epsilon^{j+1}) = R(a\epsilon^{j}) + 2I(a\epsilon^{j}) \quad \text{and} \quad I(a\epsilon^{j+1}) = R(a\epsilon^{j}) + I(a\epsilon^{j}).$$

Now it is clear that

$$m_{j+1} = R(a\epsilon^{j+1}) + l(a\epsilon^{j+1}) + l(a\epsilon^{j+1})$$

and

$$n_{j+1} = I(a\epsilon^{j+1}).$$

It follows directly from Lemma 2.1, that

$$m_i = R(a\epsilon^j) + I(a\epsilon^j) = I(a\epsilon^{j+1}).$$

Thus the formulae in (1) hold for all $j \ge 0$. The formulae in (2) are proved in exactly the same way. The formulae in (3) are proved by using Lemma 2.1 to get

$$\begin{split} m_j &= R(a\epsilon^j) + I(a\epsilon^j) = I(a\epsilon^{j+1}) = I(\epsilon^{j+1})R(a) + R(\epsilon^{j+1})I(a) = \frac{\epsilon^{j+1} - \overline{\epsilon}^{j+1}}{2\sqrt{2}} \ a + \frac{\epsilon^{j+1} + \overline{\epsilon}^{j+1}}{2} \ b, \\ n_j &= I(a\epsilon^j) = I(\epsilon^j)R(a) + R(\epsilon^j)I(a) = \frac{\epsilon^j - \overline{\epsilon}^j}{2\sqrt{2}} \ a + \frac{\epsilon^j + \overline{\epsilon}^j}{2} \ b \ . \end{split}$$

The formulae in (4) follow from (2) in exactly the same manner.

In Theorem 5.4 it was shown that the sequences $\{T_j(p)\}$ and $\{T'_j(p)\}$ were disjoint. With Theorem 5.5 it is possible to show that these sequences are exhaustive in the sense that they contain every primitive pythagorean triple (x, y, z) with |x - y| = p. To prove this result, stated below as Theorem 5.6, it will be shown that if (x, y, z) has |x - y| = p, then its generators must be the same as those listed in Theorem 5.5.

Theorem 5.6. Let p be a rational prime of the form $8k \pm 1$. If T = (x, y, z) is a primitive pythagorean triple such that |x - y| = p, then T is in one of the sequences $\{T_j(p)\}$ or $\{T'_j(p)\}$.

Proof. Let u = a, v = b be the fundamental solution of $u^2 - 2v^2 = p$ and let $a = a + b\sqrt{2}$. If *m* and *n* are the generators of T = (x, y, z) then

$$y - x = (m - n)^2 - 2n^2$$
.

275

PRIMITIVE PYTHAGOREAN TRIPLES WITH SUM

Hence

$$N(a) = p = \pm N([m - n] + n \cdot /2).$$

Since
$$a$$
 is a prime, it follows that either a or \overline{a} is an associate of

$$(m-n)+n\sqrt{2}$$
.

If a is an associate of $(m - n) + n\sqrt{2}$, then by definition there is an integer t such that

$$a\epsilon^{\tau} = (m-n) + n\sqrt{2}$$

or

$$-a\epsilon^t = (m-n) + n\sqrt{2}$$
.

This second equality is impossible because

$$-a\epsilon^t < 0 < (m-n) + n\sqrt{2}$$
 .

Thus if a is an associate of $(m - n) + n\sqrt{2}$, then

$$a\epsilon^t = (m-n) + n\sqrt{2}$$

for some integer t. Note that t < 0 implies that

$$a > ae^{t} = (m-n) + n\sqrt{2} \ge a + b\sqrt{2} = a$$

which is a contradiction. Thus if a is an associate of $(m - n) + n\sqrt{2}$, there is an integer $t \ge 0$ such that

$$a\epsilon^t = (m-n) + n\sqrt{2} .$$

It is now clear that, in this case, T is generated by

$$m = R(ae^{t}) + I(ae^{t})$$

 $n = I(a\epsilon^t),$

and

with $t \ge 0$, so that T is in $\left\{ T_j(p) \right\}$.

If \overline{a} is an associate of $(m - n) + n\sqrt{2}$, then by definition, there exists an integer t such that

$$\overline{a}\epsilon^t = (m-n) + n\sqrt{2},$$

 $-\overline{a}\epsilon^t = (m-n) + n\sqrt{2}$.

or

This last equality is impossible, because
$$a > 0$$
 and $a\overline{a} = p$ imply that $\overline{a} > 0$, and hence

$$-\overline{a}\epsilon^t < 0 < (m-n) + n\sqrt{2}$$

Note that if

$$\overline{a}e^{t} = (m-n) + n\sqrt{2}$$
 and $t \leq 0$,

then

$$\overline{a} \ge \overline{a} \epsilon^t = (m-n) + n\sqrt{2} \ge a + h\sqrt{2} = a > \overline{a}$$

which is impossible.

Thus if \overline{a} is an associate of $(m - n) + n\sqrt{2}$, then there is an integer t > 0 such that

$$\overline{a}\epsilon^t = (m-n) + n\sqrt{2}$$
.

Clearly, in this case, T is generated by

$$m = R(\overline{a}e^t) + I(\overline{a}e^t)$$
 and $n = I(\overline{a}e^t)$,

with t > 0, so that T is in $\{T'_j(p)\}$. This completes the proof.

In the description of the two sequences $\{T_j(p)\}$ and $\{T'_j(p)\}$ it is obvious that the sequence $\{T'_j(p)\}$ is closely related to the unique primitive pythagorean triple (x, y, z) with x + y = p. The following theorem is used to show that the sequence $\{T_j(p)\}$ is also related to the unique primitive pythagorean triple (x, y, z) with x + y = p. The following theorem is used to show that the sequence $\{T_j(p)\}$ is also related to the unique primitive pythagorean triple (x, y, z) with x + y = p. Theorem 5.7. If m and n (m > n) generate a primitive pythagorean triple (x, y, z), then M = 2n + m and N = n generate a primitive pythagorean triple (X, Y, Z) such that |X - Y| = x + y.

The proof is computational and is left to the reader.

If p is a prime of the form $8k \neq 1$, then as in Theorem 4.2, the unique primitive pythagorean triple (x, y, z) with x + y = p, is generated by m = a - b and n = b, where u = a, v = b is the fundamental solution of $u^2 - 2v^2 = p$. By Theorem 5.7,

$$M = 2n + m = a + b$$
 and $N = n = b$

generate a primitive pythagorean triple (X, Y, Z) such that

$$|X-Y| = x+y = p.$$

An examination of the generators M and N shows that (X, Y, Z) is the triple labeled $T_o(p)$ in the discussion of $\{T_j(p)\}$.

6. SUMMARY

In this paper it has been shown that the sum and the difference of the legs of a primitive pythagorean triple must be of the form $8k \pm 1$, Conversely, if p is a prime of the form $8k \pm 1$, there is a unique primitive pythagorean triple (x, y, z) with x + y = p, but there are two infinite disjoint sequences of primitive pythagorean triples with the difference of the legs equal to p for each triple in the sequences. Furthermore, every primitive pythagorean triple (x, y, z)with |x - y| = p is in one of these sequences. Figure 2 outlines a general method for constructing these triples and Fig. 3 illustrates the procedure with p = 137. Finally, explicit formulae for the generators of each triple in the sequences are given in terms of the fundamental solution of $u^2 - 2v^2 = p$.

REFERENCES

- 1. L.E. Dickson, History of the Theory of Numbers, Vols. I and II, Chelsea, New York, N.Y., 1966.
- 2. G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers, 4th ed., Clarendon Press, Oxford, 1960.
- 3. T. Nagell, Introduction to Number Theory, Chelsea, New York, N.Y., 1964.
- 4. L.W. Reid, The Elements of the Theory of Algebraic Numbers, Macmillan, New York, N.Y., 1910.
- 5. W. Sierpinski, "Pythagorean Triangles," *Scripta Mathematica Studies,* No. 9, Yeshiva University, New York, N.Y., 1962.
- 6. W. Sierpinski, *Elementary Theory of Numbers,* Panstwowe Wydawnnictwo Naukowe, Poland, 1964.
- 7. W. Sierpinski, *A Selection of Problems in the Theory of Numbers,* Pergamon Press, Macmillan, New York, N.Y., 1964.
- 8. W.P. Whitlock, Jr., "Pythagorean Triangles with a Given Difference or Sum of Sides," *Scrip. Math.*, Vol. II (1945), pp. 75–81.

SPECIAL PARTITIONS

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

In this paper, we discuss the partitions p(n) of non-negative integers n, using summands 1 and 2. These are collections of 1 and 2 whose sum is n without regard to order.

Example.

$$5 = 2 + 2 + 1 = 1 + 1 + 1 + 1 + 1 = 2 + 1 + 1 + 1$$

thus *p(5) = 3.*

Theorem.

$$p(2n+1) = p(2n) = n+1$$
 for $n \ge 0$.

Proof. Clearly, p(0) = 1, using no ones or twos, and p(1) = 1. First, 2n is the sum of n two's. Each two can be replaced by a pair of ones. This can be done in n distinct ways, making (n + 1) possible partitions. Second, 2n + 1 is the sum of n two's and a one. Thus, it also has (n + 1) distinct partitions.

Theorem. If all the partitions of n are displayed simultaneously, then there are U(n) ones, S(n) twos, and P(n) plus signs, where

$$U(2n) = 2T_n ,$$

$$U(2n + 1) = 2T_n + p(n) ,$$

$$S(2n + 1) = S(2n) = T_n ,$$

$$P(2n + 1) = 3T_n ,$$

$$P(2n + 2) = 3T_n + 2n + 1 ,$$

where T_n is the n^{th} triangular number, $n \ge 0$.

Proofs. Let us start with S(2n), n > 0. Clearly, there are n twos and each two is sequentially replaced by a pair of ones in succeeding partitions until there are no twos. Thus

$$S(2n) = n + (n - 1) + \dots + 2 + 1 = T_n$$

Clearly, (2n + 1) also has n twos and a one so that the number of twos in all specialized partitions of (2n + 1) is also T_n .

Next, consider N = 2n. From the sequential construction of the partitions beginning with *n* twos it is clear that the number of ones is $2T_n$. However, for N = 2n + 1 we need an extra one for each partition; thus

[Continued on page 254.]

PRODUCTS AND POWERS

M. W. BUNDER The University of Wollongong, Wollongong, N.S.W., Australia

The generalized Fibonacci sequence is defined by

$$w_n = pw_{n-1} + qw_{n-2}$$

(1) with

> wo = a $w_f = b$. and

In Horadam's notation [1], w_n is written $w_n(a,b;p,-q)$.

In this note we see what happens when we replace the sum and products in (1) by a product and powers; i.e.,

(2)
$$z_n = z_{n-1}^p \cdot z_{n-2}^q$$

with

$$z_0 = a$$
 and $z_1 = b$.

(We can write z_n as $z_n(a,b; p,q)$.)

The sequence becomes *a,b, ab, ab*², a^2b^3 , a^3b^5 , a^5b^8 , ... in the case where p = q = 1 so that

$$z_n(a,b; 1, 1) = a^{F_{n-1}} \cdot b^{F_n}$$

The general case gives the sequence

a, b,
$$a^{p}b^{q}$$
, a^{pq} , $b^{p+q^{2}}$, $a^{p^{2}+pq^{2}}$, $b^{2pq+q^{3}}$, ...

with

$$z_n(a,b;p,q) = a^{W_n(1,0;p,-q)} \cdot b^{W_n(0,1;p,-q)}.$$

REFERENCE

1. A.F. Horadam, "Generating Functions for Powers of a Certain Generalized Sequence of Numbers," Duke Math. Journal., Vol. 32, No. 3, pp. 437-446, Sept. 1965.

A SPECIAL CASE OF THE GENERALIZED FIBONACCI SEQUENCE OVER AN ARBITRARY RING WITH IDENTITY

M. W. BUNDER

The University of Wollongong, Wollongong, N.S.W., Australia

DeCarli [1] introduced the sequence $\{M_n\}$ of elements of an arbitrary ring with identity S by

$$M_{n+2} = A_1 M_{n+1} + A_0 M_n$$
 for $n \ge 0$,

where M_0 , M_1 , A_0 and A_1 are arbitrary elements of S. He considers in particular the case which he calls the sequence $\{F_n\}$ with

 $F_{n+2} = A_1 F_{n+1} + A_0 F_n \quad \text{for} \quad n \ge 0,$

where $F_0 = 0$ (the zero of the ring) $F_1 = I$ (the identity) and A_0 and A_1 are arbitrary elements of S. A number of DeCarli's theorems can be simplified in the special case where $A_0A_1 = A_1A_0$. We use the following theorems which are easily proved by induction.

Theorem 1.	$A_0F_n = F_nA_0,$	$A_1F_n = 1$	F _n A₁ for	all <i>n.</i>
Theorem 2.	$F_n F_m = F_m F_n$	for all	<i>m</i> and <i>n</i> .	

Thus DeCarli's Theorem 3

$$F_nF_{n+r} - F_{n+r}F_n = F_nF_rA_0F_{n-1} - F_{n-1}A_0F_1F_n$$

becomes trivial.

Also we can prove that F_n commutes with any element of S which commutes with A_0 and A_1 . In particular when A_0 and A_1 commute with all elements of S so does F_n .

The two parts of DeCarli's Corollary 1 can thus be rewritten as

$$F_{n+1}F_{n-1} - F_n^2 = A_0(F_{n-1}^2 - F_nF_{n-2}).$$

In the same way as above for the general sequence, if M_0 , M_1 , A_0 and A_1 all commute with each other then all M_0 's commute with each other and with A_0 and A_1 .

REFERENCE

D.J. DeCarli, "A Generalized Fibonacci Sequence Over an Arbitrary Ring," *The Fibonacci Quarterly*, Vol. 8, No. 2 (March 1970), pp. 182–184.

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 problem.

H-252 Proposed by V.E. Hoggatt, Jr., San Jose State College, San Jose, California.

Let $A_{n \times n}$ be an $n \times n$ lower semi-matrix and $B_{n \times n}$, $C_{n \times n}$ be matrices such that $A_{n \times n} B_{n \times n} = C_{n \times n}$. Let $A_{k \times k}$, $B_{k \times k}$, $C_{k \times k}$ be the $k \times k$ upper left submatrices of $A_{n \times n}$, $B_{n \times n}$, and $C_{n \times n}$. Show $A_{k \times k} B_{k \times k} = C_{k \times k}$ for k = 1, 2, ..., n

H-253 Proposed by L. Carlitz, Duke University, Durham, North Carolina.

Show that

$$\sum_{i=0}^{k} \binom{(\beta-1)n+t+1}{t} \sum_{j=0}^{n-k-1} \binom{n-k-1}{j} \sum_{m=0}^{j} (-1)^{n+m+k+1} \binom{j}{m} \\ \cdot \sum_{r=0}^{n+m-t-j-1} \binom{j}{n+m-j-t-r-1} \binom{2j+r-1}{r} = 2^{n-k-1} \binom{\beta n}{k}$$

where β is an arbitrary complex number and n and k are positive integers, k < n.

This identity, in the case $\beta = 2$, arose in solving a certain combinatorial problem in two different ways.

H-254 Proposed by R. Whitney, Lock Haven State College, LockHaven, Pennsylvania.

Consider the Fibonacci-Pascal Type Triangle given below.



Find a formula for the row sums of this array.

SOLUTIONS ENUMERATION

H-226 Proposed by L. Carlitz and R. Scoville, Duke University, Durham, North Carolina.

(i) Let k be a fixed positive integer. Find the number of sequences of integers (a_1, a_2, \dots, a_n) such that

$$0 \leq a_i \leq k$$
 $(i = 1, 2, \cdots, n)$

and if $a_i > 0$ then $a_i \neq a_{i-1}$ for $i = 2, \dots, n$.

(ii) Let k be a fixed positive integer. Find the number of sequences of integers (a_1, a_2, \dots, a_n) such that

$$0 \leq a_j \leq k \qquad (i = 1, 2, \cdots, n)$$

and if $a_i > 0$ then $a_i \neq a_{i-1}$ for $i = 2, \dots, n$; moreover $a_i = 0$ for exactly r values of i. Solution by the Proposers.

Part (i).

282

Let $f_i(n)$ denote the number of such sequences with $a_n = j$. Then clearly

and

$$\begin{cases} f_0(n+1) = f_0(n) + kf_1(n) \\ f_1(n+1) = f_0(n) + (k-1)f_1(n) . \\ \end{cases}$$

$$\begin{cases} f_0(n+2) = kf_0(n+1) + f_0(n) \\ f_1(n+2) = kf_1(n+1) + f_1(n) . \end{cases}$$

 $f_0(1) = 1, \quad f_0(2) = k+1, \quad f_1(1) = 1, \quad f_1(2) = k.$

 $f_1(n) = \dots = f_k(n)$

It follows that

(*)

Also

It is convenient to take

$$f_0(0) = 0, \qquad f_1(0) = 1;$$

then (*) holds for all $n \ge 0$. We now take

$$\begin{split} F_{\mathfrak{o}}(x) &= \sum_{n=0}^{\infty} f_{\mathfrak{o}}(n) x^{n} = 1 + x + x^{2} \sum_{0}^{\infty} (k f_{\mathfrak{o}}(n+1) + f_{\mathfrak{o}}(n)) x \\ &= 1 - (k-1) x + (k x + x^{2}) \sum_{0}^{\infty} f_{\mathfrak{o}}(n) x^{n} \,, \end{split}$$

 $F_0(x) = \frac{1-(k-1)x}{1-kx-x^2}$.

Similarly

$$F_1(x) = \sum_{n=0}^{\infty} f_1(n)x^n = x + \sum_{0}^{\infty} (kf_1(n+1) + f_1(n))x^n$$

which yields

$$F_1(x) = \frac{x}{1-kx-x^2}$$

Let $S(n) = f_0(n) + kf_1(n)$ denote the total number of sequences satisfying the stated conditions. Then

$$\sum_{0}^{\infty} S(n)x^{n} = \frac{1+x}{1-kx-x^{2}}$$

Since

$$\frac{1}{1-kx-x^2} = \sum_{r=0}^{\infty} x^r (k+x)^r = \sum_{r=0}^{\infty} x^r \sum_{j=0}^{r} {r \choose j} k^{r-j} x^j = \sum_{n=0}^{\infty} x^n \sum_{2j \le n} {n-j \choose j} k^{n-2j},$$

it follows that

[OCT.

$$S(n) = \sum_{2j \leq n} {\binom{n-j}{j} k^{n-2j} + \sum_{2j < n} {\binom{n-j-1}{j} k^{n-2j-1}}$$

Part (ii)

Let $f_j(n,r)$ denote the number of such sequence with $a_n = j$. Then clearly

$$f_1(n,r) = \cdots = f_k(n,r)$$

and

$$\begin{cases} f_0(n+1,r) = f_0(n,r-1) + kf_1(n,r-1) \\ f_1(n+1,r) = f_0(n,r) + (k-1)f_1(n,r) \end{cases} \quad (n \ge 1, r \ge 0),$$

where $f_i(n, -1) = 0$. Clearly

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

Put

$$F_{i}(z,x) = \sum_{n=1}^{\infty} \sum_{r=0}^{n} f_{i}(n,r)z^{n}x^{r} \qquad (i = 1, 2).$$

Then

$$F_{0}(z,x) = zx + \sum_{n=1}^{\infty} \sum_{r=1}^{n+1} (f_{0}(n,r-1) + kf_{1}(n,r-1))z^{n+1}x^{r} = zx + zxF_{0}(z,x) + kzxF_{1}(z,x),$$

$$F_{1}(z,x) = z + \sum_{n=1}^{\infty} \sum_{r=0}^{n} (f_{0}(n,r) + (k-1)f_{1}(n,r))z^{n+1}x^{r} = z + zF_{0}(z,x) + (k-1)zF_{1}(z,x).$$

Thus

$$\begin{cases} (1-zx)F_0(z,x) - kzxF_1(z,x) = zx \\ -zF_0(z,x) + (1-(k-1)z)F_1(z,x) = z. \end{cases}$$

It follows that

(*)
$$\begin{cases} F_0(z,x) = \frac{zx + z^2 x}{1 - (x + k - 1)z - z^2 x} \\ F_1(z,x) = \frac{z}{1 - (x + k - 1)z - z^2 x} \end{cases}$$

We have

$$\frac{1}{1 - (x + k - 1)z - z^2 x} = \sum_{n=0}^{\infty} z^n (x + k - 1 + zx)^n = \sum_{j,s=0}^{\infty} {j + s \choose s} (x + k - 1)^j x^s z^{j+2s}$$
$$= \sum_{n=0}^{\infty} z^n \sum_{2s \le n} {n - s \choose s} (x + k - 1)^{n-2s} x^s .$$

Hence

$$\sum_{r=0}^{n+1} f_1(n+1,r)x^r = \sum_{2s \le n} {\binom{n-s}{s}} x^{s}(x+k-1)^{n-2s} = \sum_{2s \le n} {\binom{n-s}{s}} x^s \sum_{t=0}^{n-2s} {\binom{n-2s}{t}} (k-1)^{n-2s-t}x^t$$
$$= \sum_{r=0}^n x^r \sum_{s=0}^r {\binom{n-s}{s}} {\binom{n-2s}{r-s}} (k-1)^{n-r-s} ,$$

so that

284

$$f_1(n+1,r) = \sum_{s=0}^{r} {n-s \choose s} {n-2s \choose r-s} (k-1)^{n-r-s}.$$

It is evident from (*) that

$$f_0(n+1,r+1) = f_1(n+1,r) + f_1(n,r-1).$$

Thus

$$f_0(n+1,r+1) = \sum_{s=0}^r \binom{n-s}{s} \binom{n-2s}{r-s} (k-1)^{n-r-s} + \sum_{s=0}^{r-1} \binom{n-s-1}{s} \binom{n-2s-1}{r-s-1} (k-1)^{n-r-s}.$$

Let $S(n,r) = f_0(n,r) + kf_1(n,r)$ denote the total number of sequences satisfying the stated conditions. Then

...

$$S(n+1,r) = k \sum_{s=0}^{r} \binom{n-s}{s} \binom{n-2s}{r-s} (k-1)^{n-r-s} + \sum_{s=0}^{r-1} \binom{n-s}{s} \binom{n-2s}{r-s-1} (k-1)^{n-r-s+1} + \sum_{s=0}^{r-2} \binom{n-s-1}{s} \binom{n-2s-1}{r-s-2} (k-1)^{n-r-s+1}$$

We remark that if we sum over r we get

$$\sum_{r=0}^{n+1} S(n+1,r) = k \sum_{2s \le n} {\binom{n-s}{s}} k^{n-2s} + \sum_{2s \le n} {\binom{n-s}{s}} k^{n-2s} + \sum_{2s \le n} {\binom{n-s-1}{s}} k^{n-2s-1}$$
$$= \sum_{2s \le n+1} {\binom{n-s+1}{s}} k^{n-2s+1} + \sum_{2s \le n} {\binom{n-s}{s}} k^{n-2s} .$$

Editorial Note: G. Wulczyn solved H-221 (previous issue).

ELEMENTARY PROBLEMS AND SOLUTIONS

Edited by A. P. HILLMAN University of New Mexico, Albuquerque, New Mexico 87131

Send all communications regarding Elementary Problems to Professor A.P. Hillman; 709 Solano Dr., S.E.; Albuquerque, New Mexico 87108. Each solution or problem should be on a separate sheet (or sheets). Preference will be given to those typed with double spacing 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-310 Proposed by Daniel Finkel, Brooklyn. New York.

Find some positive integers *n* and *r* such that the binomial coefficient $\binom{n}{r}$ is divisible by $n \neq 1$.

B-311 Proposed by Jeffrey Shallit, Wynnewood, Pennsylvania.

Let k be a constant and let $\left\{ a_n \right\}$ be defined by

$$a_n = a_{n-1} + a_{n-2} + k$$
, $a_0 = 0$, $a_1 = 1$.

Find

$$\lim_{n \to \infty} (a_n / F_n).$$

B-312 Proposed by J.A.H. Hunter, Fun with Figures, Toronto, Ontario, Canada.

Solve the doubly-true alphametic

Unity is not normally considered so, but here our ONE is prime!

B-313 Proposed by Verner E. Hoggatt, Jr., California State University, San Jose, California. Let

$$M(x) = L_1 x + (L_2 / 2) x^2 + (L_3 / 3) x^3 + \cdots$$

Show that the Maclaurin series expansion for $e^{M(x)}$ is $F_1 + F_2 x + F_3 x^2 + \cdots$.

B-314 Proposed by Herta T. Freitag, Roanoke, Virginia.

Show that $L_{2p^k} \equiv 3 \pmod{10}$ for all primes $p \ge 5$.

SOLUTIONS

DIFFERENTIATING FIBONACCI GENERATING FUNCTION

B-279 (Correction of typographical error in Vol. 12, No. 1 (February 1974).

Find a closed form for the coefficient of x^n in the Maclaurin series expansion of

$$(x + 2x^2)/(1 - x - x^2)^2$$
.

Solution by Paul S. Bruckman, University of Illinois, Chicago Circle, Illinois.

Let

$$F(x) = (1 - x - x^2)^{-1} = \sum_{n=0}^{\infty} F_{n+1}x^n$$

be the well-known generating function for the Fibonacci numbers. Differentiating term by term, we have formally:

$$F'(x) = (1+2x)(1-x-x^2)^{-2} = \sum_{n=1}^{\infty} nF_{n+1}x^{n-1}$$

Therefore,

$$(x+2x^2)(1-x-x^2)^{-2} = \sum_{n=0}^{\infty} nF_{n+1}x^n$$

Hence, the required coefficient is equal to nF_{n+1} , $n = 0, 1, 2, \cdots$.

Also solved by Clyde A. Bridger, Charles Chouteau, Edwin T. Hoefer, A.C. Shannon, and the Proposer.

GOLDEN POWERS OF 2

B-286 Proposed by Herta T. Freitag, Roanoke, Virginia.

Let g be the "golden ratio" defined by

$$g = \lim_{n \to \infty} (F_n / F_{n+1}).$$

Simplify

$$\sum_{i=0}^{n} \binom{n}{i} g^{2n-3i}.$$

Solution by Graham Lord, Temple University, Philadelphia, Pennsylvania.

As $1/g = a = (1 + \sqrt{5})/2$ then the sum equals

$$g^{2n} \cdot \sum_{0}^{n} {n \choose i} \cdot (a^3)^i$$

that is $g^{2n} \cdot (1 + a^3)^n$, which simplifies to 2^n .

Also solved by W.G. Brady, Paul S. Bruckman, Ralph Garfield, Frank Higgins, A.C. Shannon, Martin C. Weiss, David Zeitlin, and the Proposer.

SIMPLIFIED

B-287 Proposed by Herta T. Freitag, Roanoke, Virginia.

Let g be as in B-286. Simplify

$$g^{2}\left\{(-1)^{n-1}[F_{n-3}-gF_{n-2}]+g+2\right\}.$$

[OCT.

Solution by Paul S. Bruckman, University of Illinois, Chicago Circle, Illinois.

Since $g = 1/a = -\beta$,

$$F_{n-3} - gF_{n-2} = 5^{-\frac{1}{2}} \left\{ a^{n-3} - \beta^{n-3} - a^{-1}a^{n-2} - \beta \cdot \beta^{n-2} \right\} = 5^{-\frac{1}{2}} \left\{ \beta^{n-2} \right\} \left\{ a - \beta \right\} = \beta^{n-2} = (-1)^{n-2}g^{n-2}.$$

Also, since $\beta^2 = \beta + 1$, then $g^2 = 1 - g$. Hence,

$$g^{2}(g+2) = (1-g)(2+g) = 2-g-g^{2} = 2-g-1+g = 1.$$

Therefore, the given expression reduces to:

$$g^{2}(-1)^{n-1}(-1)^{n-2}g^{n-2} + 1 = 1 - g^{n}$$

Also solved by Ralph Garfield, Frank Higgins, and the Proposer.

A MULTIPLE OF L2n

B-288 Proposed by Paul S. Bruckman, University of Illinois, Chicago Circle, Illinois.

Prove that $F_{2n(4k+1)} \equiv F_{2n} \pmod{L_{2n}}$ for all integers *n* and *k*.

Solution by Graham Lord, Temple University, Philadelphia, Pennsylvania.

If p is even then

$$F_{m+p} - F_{m-p} = L_m F_p.$$

Replace p by 4nk and m by 2n(2k + 1) to get

The required congruence follows with an application of Carlitz' result: L_a divides L_b iff b = a(2c - 1), a > 1. ("A Note on Fibonacci Numbers," *The Fibonacci Quarterly*, Vol. 2, No. 1, 1964, pp. 15–28.)

Also solved by Clyde A. Bridger, Ralph Garfield, Frank Higgins, A.C. Shannon, Gregory Wulczyn, David Zeitlin, and the Proposer.

A MULTIPLE OF L2n+1

B-289 Proposed by Paul S. Bruckman, University of Illinois, Chicago Circle, Illinois.

Prove that $F_{(2n+1)(4k+1)} \equiv F_{2n+1} \pmod{L_{2n+1}}$, for all integers *n* and *k*.

Solution by Graham Lord, Temple University, Philadelphia, Pennsylvania.

If p is even then

$$F_{m+p} - F_{m-p} = L_m F_p.$$

Replace p by 2k(2n + 1) and m by (2n + 1)(2k + 1) to get

$$F_{(2n+1)(4k+1)} - F_{2n+1} = L_{(2n+1)(2k+1)}F_{2k(2n+1)}$$

The required congruence follows with an application of Carlitz' result: L_a divides L_b iff b = a(2c - 1), a > 1. ("A Note on Fibonacci Numbers," The Fibonacci Quarterly, Vol. 12, No. 1, 1964, pp. 15–28.)

Also solved by Clyde A. Bridger, Ralph Garfield, Frank Higgins, A.C. Shannon, Gregory Wulczyn, David Zeitlin, and the Proposer.

CONVOLUTED F2n

B-290 Proposed by V.E. Hoggatt, Jr., San Jose State University, San Jose, California.

Obtain a closed form for

$$2n+1+\sum_{k=1}^n \ (2n+1-2k)F_{2k}\,.$$

Solution by Graham Lord, Temple University, Philadelphia, Pennsylvania.

The sum of the first k odd indexed Fibonacci numbers is F_{2k} and that of the first k even indexed ones is F_{2k+1} – 1, where $k \ge 1$.

Therefore,

$$2n + 1 + \sum_{k=1}^{n} (2n + 1 - 2k)F_{2k} = 2n + 1 + F_{2n+1} - 1 + 2\sum_{k=1}^{n-1} (F_2 + F_4 + \dots + F_{2k})$$
$$= 2n + F_{2n+1} + 2\sum_{k=1}^{n-1} (F_{2k+1} - 1)$$
$$= 2n + F_{2n+1} + 2(F_{2n} - F_1 - n + 1)$$
$$= F_{2n+1} + 2F_{2n} = L_{2n+1}.$$

Also solved by W.G. Brady, Paul S. Bruckman, Herta T. Freitag, Ralph Garfield, Frank Higgins, A.C. Shannon, Gregory Wulczyn, and the Proposer.

TRANSLATED RECURSION

B-192 Proposed by Phil Mana, University of New Mexico, Albuquerque, New Mexico.

Find the second-order recursion relation for $\{z_n\}$ given that

$$z_n = \sum_{k=0}^n \binom{n}{k} y_k \quad \text{and} \quad y_{n+2} = ay_{n+1} + by_n,$$

where a and b are constants.

Solution by A.C. Shannon, New South Wales Institute of Technology, N.S.W., Australia.

Let $y_n = Aa^n + B\beta^n$, where A, B depend on y_1 , y_2 and $a_n\beta$ are the roots of the auxiliary equation

$$0 = x^2 - ax - b.$$

Then

$$z_n = \sum_{k=0}^n \binom{n}{k} (Aa^k + B\beta^k) = A(1+a)^n + B(1+\beta)^n$$

$$= ((1 + \alpha) + (1 + \beta))z_{n-1} - (1 + \alpha)(1 + \beta)z_{n-2} = (a + 2)z_{n-1} - (a - b + 1)z_{n-2}$$

since $a = a + \beta$ and $b = -a\beta$.

Also solved by W.G. Brady, Paul S. Bruckman, Ralph Garfield, Frank Higgins, David Zeitlin, and the Proposer.

SUSTAINING MEMBERS

*H. L. Alder G. L. Alexanderson *J. Arkin Leon Bankoff Murray Berg Gerald Bergum David G. Beverage *Marjorie Bicknell C. A. Bridger *Bro. A. Brousseau Paul F. Byrd C. R. Burton L. Carlitz G. D. Chakerian P. J. Cocuzza N. S. Cox D. E. Daykin M. J. DeLeon J. E. Desmond M. H. Diem N. A. Draim J. L. Ercolano D. R. Farmer D. C. Fielder Harvey Fox E. T. Frankel

C. L. Gardner R. M. Giuli G. R. Glabe H. W. Gould Nicholas Grant William Grieg David Harahus V. C. Harris Frank Higgins A. P. Hillman *V. E. Hoggatt, Jr. *A. F. Horadam Virginia Kelemen R. P. Kelisky C. H. Kimberling *Kenneth Kloss J. Lahr George Ledin, Jr. H. T. Leonard, Jr. *C. T. Long D. P. Mamuscia E. T. Manning James Maxwell R. K. McConnell. Jr. *Sister M. DeSales McNabb L. P. Meissner

F. J. Ossiander Fanciulli Pietro M. M. Risueno T. C. Robbins M. Y. Rondeau F. G. Rothwell H. D. Seielstad C. E. Serkland A. G. Shannon J. A. Shumaker D. Singmaster C. C. Styles M. N. S. Swamy L. Taylor *D. E. Thoro H. L. Umansky Marcellus Waddill *L. A. Walker J. B. Westbury Raymond Whitney Paul Willis C. F. Winans E. L. Yang Charles Ziegenfus

*Charter Members

ACADEMIC OR INSTITUTIONAL MEMBERS

DUKE UNIVERSITY Durham, North Carolina

SACRAMENTO STATE COLLEGE Sacramento, California

SAN JOSE STATE UNIVERSITY San Jose, California ST. MARY'S COLLEGE St. Mary's College, California

UNIVERSITY OF SANTA CLARA Santa Clara, California

WASHINGTON STATE UNIVERSITY Pullman, Washington

THE BAKER STORE EQUIPMENT COMPANY THE CALIFORNIA MATHEMATICS COUNCIL



¢

0

BINDERS NOW AVAILABLE

The Fibonacci Association is making available a binder which can be used to take care of one volume of the publication at a time. This binder is described by the company producing it as follows:

"... The binder is made of heavy weight virgin vinyl, electronically sealed over rigid board equipped with a clear label holder extending 2³/4" high from the bottom of the backbone, round cornered, fitted with a 1¹/₂" multiple mechanism and 4 heavy wires."

The name, *FIBONACCI QUARTERLY*, is printed in gold on the front of the binder and the spine. The color of the binder is dark green. There is a small pocket on the spine for holding a tab giving year and volume. These latter will be supplied with each order if the volume or volumes to be bound are indicated.

The price per binder is \$3.50 which includes postage (ranging from 50c to 80c for one binder). The tabs will be sent with the receipt or invoice.

All orders should be sent to: Brother Alfred Brousseau, Managing Editor, St. Mary's College, Moraga, California 94575.