The Fibonacci Quarterly

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

VOLUME 20
NUMBER 4

NOVEMBER
1982

CONTENTS

The Fibonacci Quarterly

Founded in 1963 by Verner E. Hoggatt, Jr. (1921-1980),
Br. Alfred Brousseau, and I.D. Ruggles

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION DEVOTED TO THE STUDY OF INTEGERS WITH SPECIAL PROPERTIES

EDITORIAL POLICY

The principal purpose of *The Fibonacci Quarterly* is to serve as a focal point for widespread interest in the Fibonacci and related numbers, especially with respect to new results, research proposals, and challenging problems.

The *Quarterly* seeks articles that are intelligible yet stimulating to its readers, most of whom are university teachers and students. These articles should be lively and well motivated, with innovative ideas that develop enthusiasm for number sequences or the exploration of number facts.

Articles should be submitted in the format of the current issues of the *Quarterly*. They should be typewritten or reproduced typewritten copies, double spaced with wide margins and on only one side of the paper. Articles should be no longer than twenty-five pages. The full name and address of the author must appear at the beginning of the paper directly under the title. Illustrations should be carefully drawn in India ink on separate sheets of bond paper or vellum, approximately twice the size they are to appear in the *Quarterly*. Authors who pay page charges will receive two free copies of the issue in which their article appears.

Two copies of the manuscript should be submitted to GERALD E. BERGUM, DEPARTMENT OF MATHEMATICS, SOUTH DAKOTA STATE UNIVERSITY, BROOKINGS, SD 57007. The author is encouraged to keep a copy for his own file as protection against loss.

Address all subscription correspondence, including notification of address changes, to SUBSCRIPTION MANAGER, THE FIBONACCI ASSOCIATION, UNIVERSITY OF SANTA CLARA, SANTA CLARA, CA 95053.

Annual domestic Fibonacci Association membership dues, which include a subscription to *The Fibonacci Quarterly,* are $20 for Regular Membership, $28 for Sustaining Membership I, $44 for Sustaining Membership II, and $50 for Institutional Membership; foreign rates, which are based on international mailing rates, are somewhat higher than domestic rates (please write for details). *The Quarterly* is published each February, May, August and November.

All back issues of *The Fibonacci Quarterly* are available in microfilm or hard copy format from UNIVERSITY MICROFILMS INTERNATIONAL, 300 North Zeeb Road, Dept P.R., ANN ARBOR, MI 48106.

SEQUENCE TRANSFORMS RELATED TO REPRESENTATIONS USING GENERALIZED FIBONACCI NUMBERS

V. E. HOGGATT, JR. (Deceased)
and
MARJORIE BICKNELL-JOHNSON
San Jose State University, San Jose, CA 95192

1. INTRODUCTION

We make use of the sequences $A = \{a_n\}$ and $B = \{b_n\}$, where (a_n, b_n) are safe-pairs in Wythoff's game, described by Ball [1], and, more recently, by Horadam [2], Silber [3], and Hoggatt & Hillman [4] to develop properties of sequences whose subscripts are given by a_n and b_n.

Let $U = \{u_i\}_{i=1}^{\infty}$. We define A and B transforms by

$$\begin{aligned} AU &= \{u_{a_i}\}_{i=1}^{\infty} = \{u_1, u_3, u_4, u_6, \ldots, u_{a_i}, \ldots\}, \\ BU &= \{u_{b_i}\}_{i=1}^{\infty} = \{u_2, u_5, u_7, \ldots, u_{b_i}, \ldots\}. \end{aligned} \tag{1.1}$$

Notice that, for $N = \{n_i\}$, $n_i = i$, the set of natural numbers, we have

$$AN = \{n_{a_i}\} = \{a_i\} = A,$$

$$BN = \{n_{b_i}\} = \{b_i\} = B.$$

Next, we list the first fifteen Wythoff pairs, and some of their properties which will be needed.

n:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a_n:	1	3	4	6	8	9	11	12	14	16	17	19	21	22	24
b_n:	2	5	7	10	13	15	18	20	23	26	28	31	34	36	39

Notice that we begin with $a_1 = 1$, and a_k is always the smallest integer not yet used. We find $b_n = a_n + n$. We list the following properties:

$$a_k + k = b_k \tag{1.2}$$

$$a_n + b_n = a_{b_n} \tag{1.3}$$

$$a_{a_n} + 1 = b_n \tag{1.4}$$

$$a_{k+1} - a_k = \begin{cases} 2, & k = a_n \\ 1, & k = b_n \end{cases} \tag{1.5}$$

$$b_{k+1} - b_k = \begin{cases} 3, & k = a_n \\ 2, & k = b_n \end{cases} \tag{1.6}$$

Further, (a_n, b_n) are related to the Fibonacci numbers in several ways, one being that, if $A = \{a_n\}$ and $B = \{b_n\}$, then A and B are the sets of positive integers for which the smallest Fibonacci number used in the unique Zeckendorf representation occurred respectively with an even or odd subscript [6].

2. A AND B TRANSFORMS OF A SPECIAL SET U (FIBONACCI CASE)

Let $U = \{u_i\}$, where

$$u_{m+1} - u_m = \begin{cases} p, & \text{if } m = a_k \\ q, & \text{if } m = b_k \end{cases} \tag{2.1}$$

Actually, we can write an explicit formula for u_m in terms of u_1, p, and q, as in the following theorem.

<u>*THEOREM 2.1:*</u> $u_m = (2m - 1 - a_m)q + (a_m - m)p + u_1$.

<u>*PROOF:*</u> $u_m = (u_m - u_{m-1}) + (u_{m-1} - u_{m-2}) + (u_{m-2} - u_{m-3}) + \cdots + (u_3 - u_2) + (u_2 - u_1) + u_1$

$= (\text{no. of } b_j\text{'s less than } m)q + (\text{no. of } a_j\text{'s less than } m)p + u_1$

$= (2m - 1 - a_m)q + (a_m - m)p + u_1$

by the following lemma.

<u>*LEMMA 1:*</u> *The number of b_j's less than n is $(2n - 1 - a_n)$, and the number of a_j's less than n is $(a_n - n)$.*

<u>*PROOF:*</u>

a_n:	1	3	4	6	8	9
n:	1	2	3	4	5	6
$a_n - n$:	0	1	1	2	3	3
a_j's less than n:	0	1	1	2	3	3

Notice that the lemma holds for $n = 1, 2, \ldots, 6$. Assume that the number of a_j's less than k is given by $a_k - k$. Then the number of a_j's less than $(k + 1)$ has to be either $(a_k - k)$ or $(a_k - k) + 1$. If $k = b_i$, then

$$a_{k+1} - (k + 1) = a_k + 1 - (k + 1) = a_k - k$$

by (1.5), while if $k = a_i$, then

$$a_{k+1} - (k + 1) = a_k + 2 - (k + 1) = a_k - k + 1,$$

giving the required result for $a_{k+1} - (k + 1)$. Thus, by mathematical induction, the number of a_j's less than n is given by $a_n - n$. But, the number of integers less than n is made up of the sum of the number of a_j's less than n and the number of b_j's less than n, since A and B are disjoint and cover the natural numbers. Thus,

$$n - 1 = (a_n - n) + (\text{number of } b_j\text{'s less than } n),$$

so that the number of b_j's less than n becomes $(2n - 1 - a_n)$.

We return to our sequence U and consider the A and B transforms. In particular, what are the differences of successive terms in the transformed sequences AU and BU?

For AU,

$$u_{a_{m+1}} - u_{a_m} = \begin{cases} q + p, & \text{if } m = a_k \\ \quad p, & \text{if } m = b_k \end{cases} \tag{2.2}$$

Equation (2.2) is easy to establish by (1.5), since when $m = a_k$, $a_{m+1} = a_m + 2$, so that

$$u_{a_{m+1}} - u_{a_m} = (u_{a_m+2} - u_{a_m+1}) + (u_{a_m+1} - u_{a_m}) = (u_{b_i+1} - u_{b_i}) + p = q + p,$$

where we write $a_m + 1 = b_i$, because $a_m + 1 \neq a_k$ and A and B are disjoint and cover the natural numbers. For the second half of (2.2), since $a_{m+1} = a_m + 1$ by (1.5), we can apply (2.1) immediately.

For BU,

$$u_{b_{m+1}} - u_{b_m} = \begin{cases} 2p + q, & \text{if } m = a_k \\ \ p + q, & \text{if } m = b_k \end{cases} \tag{2.3}$$

We can establish (2.3) easily by (1.6), since when $m = a_k$, $b_{m+1} = b_m + 3$, and $b_m + 2 = a_i$, $b_m + 1 = a_j$ for some i and j, so we can write

$$\begin{aligned} u_{b_{m+1}} - u_{b_m} &= (u_{b_m+3} - u_{b_m+2}) + (u_{b_m+2} - u_{b_m+1}) + (u_{b_m+1} - u_{b_m}) \\ &= (u_{a_i+1} - u_{a_i}) + (u_{a_j+1} - u_{a_j}) + (u_{b_m+1} - u_{b_m}) \\ &= p + p + q = 2p + q. \end{aligned}$$

For the case $m = b_k$, $b_{m+1} = b_m + 2$ and $b_m + 1 = a_i$ for some i, causing

$$\begin{aligned} u_{b_{m+1}} - u_{b_m} &= (u_{b_m+2} - u_{b_m+1}) + (u_{b_m+1} - u_{b_m}) \\ &= (u_{a_i+1} - u_{a_i}) + (u_{b_m+1} - u_{b_m}) \\ &= p + q. \end{aligned}$$

Notice that we have put one b_i subscript on BU and one a_i subscript on AU. Now if we applied B twice, $BBU = \{u_{b_{b_i}}\}$ would have two successive b-subscripts, and we could record how many b-subscripts occurred by how many times we applied the B transform. Thus, a sequence of A and B transforms gives us a sequence of successive a- and b-subscripts. Further, we can easily handle this by matrix multiplication. Let the finally transformed sequence be denoted by $U^* = u^*_{(ab)_i}$ and define the difference of successive elements by

$$u^*_{(ab)_{i+1}} - u^*_{(ab)_i} = \begin{cases} p', & \text{if } i = a_k \\ q', & \text{if } i = b_k \end{cases}$$

and define the matrix $Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Then AU has $p' = p + q$, $q' = p$, and

$$Q\begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} p + q \\ p \end{pmatrix} = \begin{pmatrix} p' \\ q' \end{pmatrix},$$

and BU has $p' = 2p + q$, $q' = p + q$, and

$$Q^2\begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} 2p + q \\ p + q \end{pmatrix} = \begin{pmatrix} p' \\ q' \end{pmatrix}.$$

Now, the Q-matrix has the well-known and easily established formula

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

for the Fibonacci numbers $F_1 = F_2 = 1$, $F_{n+2} = F_{n+1} + F_n$.

Suppose we do a sequence of A and B transforms,

$$AABAAAU = A^2B^1A^3U.$$

Then the difference of successive terms, p' and q', are given by

$$Q^7\begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} F_8 & F_7 \\ F_7 & F_6 \end{pmatrix}\begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} F_8p + F_7q \\ F_7p + F_6q \end{pmatrix} = \begin{pmatrix} p' \\ q' \end{pmatrix}.$$

Note that each A transform contributes Q^1 but a B transform contributes Q^2 to the product. Also, the sequence considered has successively 3 a-subscripts, one b-subscript, and 2 a-subscripts, so that $u^*_{(ab)_i}$ has six subscripted subscripts, or,

$$u^*_{(ab)_i} = u_{a_{a_{a_{b_{a_{a_i}}}}}}.$$

Also notice that the order of the A and B transforms does not matter. Thus, if U^* is formed after m A transforms and n B transforms in any order, then the matrix multiplier is Q^{m+2n}, and

$$p' = F_{m+2n+1}p + F_{m+2n}q, \qquad q' = F_{m+2n}p + F_{m+2n-1}q.$$

Comments on A and B Transforms

Let W be the weight of the sequence of A and B transforms, where each B is weighted 2 and each A weighted 1. Thus, the number of different sequences with weight W is the number of compositions of W using 1's and 2's, so that the number of distinct sequences of A and B transforms of weight W is F_{W+1}. Thus, u_1 in Theorem 2.1 can be any number 1, 2, ..., F_{W+1} for sequences of A and B transforms of weight W.

3. A, B, AND C TRANSFORMS (TRIBONACCI CASE)

The Tribonacci numbers T_n are

$$T_0 = 0,\ T_1 = 1,\ T_2 = 1,\ T_{n+3} = T_{n+2} + T_{n+1} + T_n, \qquad n \geqslant 0.$$

Divide the positive integers into three disjoint subsets $A = \{A_k\}$, $B = \{B_k\}$, and $C = \{C_k\}$ by examining the smallest term T_k used in the unique Zeckendorf representation in terms of Tribonacci numbers. Let $n \in A$ if $k \equiv 2 \bmod 3$, $n \in B$ if $k \equiv 3 \bmod 3$, and $n \in C$ if $k \equiv 1 \bmod 3$. The numbers A_n, B_n, and C_n were considered in [6]. We list the first few values.

TABLE 3.1

n	A_n	B_n	C_n
1	1	2	4
2	3	6	11
3	5	9	17
4	7	13	24
5	8	15	28
6	10	19	35
7	12	22	41
8	14	26	48
9	16	30	55
10	18	33	61

Notice that we begin with $A_1 = 1$ and A_k is the smallest integer not yet used in building the array. Some basic properties are:

$$A_n + B_n + n = C_n \tag{3.1}$$

$$A_{A_n} + 1 = B_n, \qquad A_{B_n} + 1 = C_n \tag{3.2}$$

$$A_{n+1} - A_n = \begin{cases} 2, & n \in A \\ 2, & n \in B \\ 1, & n \in C \end{cases} \tag{3.3}$$

$$B_{n+1} - B_n = \begin{cases} 4, & n \in A \\ 3, & n \in B \\ 2, & n \in C \end{cases} \tag{3.4}$$

$$C_{n+1} - C_n = \begin{cases} 7, & n \in A \\ 6, & n \in B \\ 4, & n \in C \end{cases} \tag{3.5}$$

Let the special sequence $U = \{u_i\}$, where

$$u_{m+1} - y_m = \begin{cases} p, & m \in A \\ q, & m \in B \\ r, & m \in C \end{cases} \tag{3.6}$$

We can write an explicit formula for u_m in terms of u_1, p, q, and r.

<u>*THEOREM 3.1:*</u> $u_m = (2m - 1 - A_m)r + (2A_m - B_m)q + (B_m - A_m - m)p + u_1$.

<u>*PROOF:*</u> $u_m = (u_m - u_{m-1}) + (u_{m-1} - u_{m-2}) + \cdots + (u_3 - u_2) + (u_2 - u_1) + u_1$

$= (\text{no. of } C_j\text{'s less than } m)r + (\text{no. of } B\text{ 's less than } m)q$

$+ (\text{no. of } A_j\text{'s less than } m)p + u_1.$

But, Theorem 4.5 of [6] gives $(2m - 1 - A_m)$ as the number of C_j's less than m, $(2A_m - B_m)$ as the number of B_j's less than m, and $(B_m - A_m - m)$ as the number of A_j's less than m, establishing Theorem 3.1.

We now return to our special sequence U of (3.6) and consider A, B, and C transforms as in Section 2. For AU,

$$u_{A_{m+1}} - u_{A_m} = \begin{cases} p + q, & m \in A \\ p + r, & m \in B \\ p, & m \in C \end{cases} \tag{3.7}$$

To establish (3.7), recall (3.3). If $m \in A$, then

$$\begin{aligned} u_{A_{m+1}} - u_{A_m} &= u_{A_m+2} - u_{A_m+1} + u_{A_m+1} - u_{A_m} \\ &= u_{B_n+1} - u_{B_n} + u_{A_m+1} - u_{A_m} \\ &= q + p. \end{aligned}$$

If $m \in B$,

$$\begin{aligned} u_{A_{m+1}} - u_{A_m} &= u_{A_m+2} - u_{A_m+1} + u_{A_m+1} - u_{A_m} \\ &= u_{C_n+1} - u_{C_n} + u_{A_m+1} - u_{A_m} \\ &= r + p. \end{aligned}$$

If $m \varepsilon C$,

$$u_{A_{m+1}} - u_{A_m} = u_{A_m+1} - u_{A_m} = p.$$

Now, matrix T,

$$T = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

can be used to write AU, since

$$T \cdot \begin{pmatrix} p \\ q \\ r \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} p \\ q \\ r \end{pmatrix} = \begin{pmatrix} p + q \\ p + r \\ p \end{pmatrix}. \tag{3.8}$$

Notice that the characteristic polynomial of T is $x^3 - x^2 - x - 1 = 0$, while the characteristic polynomial of Q of Section 2 is $x^2 - x - 1 = 0$.

In an entirely similar manner, for BU one can establish

$$u_{B_{m+1}} - u_{B_m} = \begin{cases} 2p + q + r, & m \varepsilon A \\ 2p + q, & m \varepsilon B \\ p + q, & m \varepsilon C \end{cases} \tag{3.9}$$

and for CU,

$$u_{C_{m+1}} - u_{C_m} = \begin{cases} 4p + 2q + r, & m \varepsilon A \\ 3p + 2q + r, & m \varepsilon B \\ 2p + q + r, & m \varepsilon C \end{cases} \tag{3.10}$$

We compute BU as

$$T^2 \cdot \begin{pmatrix} p \\ q \\ r \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 \\ 2 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} p \\ q \\ r \end{pmatrix} = \begin{pmatrix} 2p + q + r \\ 2p + q \\ p + q \end{pmatrix}$$

and CU as

$$T^3 \cdot \begin{pmatrix} p \\ q \\ r \end{pmatrix} = \begin{pmatrix} 4 & 2 & 1 \\ 3 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix} \begin{pmatrix} p \\ q \\ r \end{pmatrix} = \begin{pmatrix} 4p + 2q + r \\ 3p + 2q + r \\ 2p + q + r \end{pmatrix}.$$

We note that

$$T^n = \begin{pmatrix} T_{n+1} & T_n & T_{n-1} \\ T_n + T_{n-1} & T_{n-1} + T_{n-2} & T_{n-2} + T_{n-3} \\ T_n & T_{n-1} & T_{n-2} \end{pmatrix}, \tag{3.11}$$

which could be proved by mathematical induction.

We may now apply A, B, and C transforms in sequences. If we assign 1 as weight for A, 2 as weight for B, and 3 as weight for C, then there are T_{n+1} sequences of A, B, and C of weight n corresponding to the compositions of n in terms of 1's, 2's, and 3's. Since any positive integer in sequence A_n, B_n, or C_n can be brought to u_1 by a unique sequence of A, B, or C transforms, there is a unique correspondence between the positive integers and the compositions of n in terms of 1's, 2's, and 3's.

4. A, B, AND C TRANSFORMS OF THE SECOND KIND

We now consider the sequence defined by

$$U_1 = 1,\ U_2 = 2,\ U_3 = 3,\ U_{n+3} = U_{n+2} + U_n,$$

with characteristic polynomial $x^3 - x - 1 = 0$. We define $A = \{A_n\}$, $B = \{B_n\}$, $C = \{C_n\}$, and let $H = \{H_n\}$ be the complement of $B = A \cup C$, where A, B, and C are disjoint and cover the set of positive integers, as follows:

$$\begin{aligned} A_n &= \text{smallest positive integer not yet used} \\ B_n &= A_n + n \\ C_n &= B_n + H_n = A_n + B_n - (\text{number of } C_j\text{'s less than } A_n) \end{aligned} \tag{4.1}$$

This array has many interesting properties [6], [8], but here the main theme is the representations in terms of the sequence U_n above. We list the first terms in the array for n, A, B, C, and H in the following table.

TABLE 4.1

n	A_n	B_n	H_n	C_n
1	1	2	1	3
2	4	6	3	9
3	5	8	4	12
4	7	11	5	16
5	10	15	7	22
6	13	19	9	28

Here we can also obtain sets A, B, and C by examining the smallest term U_k used in the unique Zeckendorf representation of an integer N in terms of the sequence U_k. We let $N \in A$ if $k \equiv 1 \bmod 3$, $N \in B$ if $k \equiv 2 \bmod 3$, and $N \in C$ if $k \equiv 3 \bmod 3$.

From Theorem 7.4 of [6], we have:

$$A_{n+1} - A_n = \begin{cases} 3, & n = A_k \\ 1, & n = B_k \\ 2, & n = C_k \end{cases} \tag{4.2}$$

$$B_{n+1} - B_n = \begin{cases} 4, & n = A_k \\ 2, & n = B_k \\ 3, & n = C_k \end{cases} \tag{4.3}$$

$$C_{n+1} - C_n = \begin{cases} 6, & n = A_k \\ 3, & n = B_k \\ 4, & n = C_k \end{cases} \tag{4.4}$$

Let the special sequence $U = \{u_i\}$, where

$$u_{m+1} - u_m = \begin{cases} p, & m \in A \\ q, & m \in B \\ r, & m \in C \end{cases} \tag{4.5}$$

We can now write an explicit formula for u_m in terms of u_1, p, q, and r.

<u>*THEOREM 4.1:*</u> $u_m = (C_m - B_m - m)p + (C_m - 2A_m - 1)q + (3B_m - 2C_m)r + u_1$.

<u>*PROOF:*</u> $u_m = (u_m - u_{m-1}) + (u_{m-1} - u_{m-2}) + \cdots + (u_3 - u_2) + (u_2 - u_1) + u_1$

$= (\text{no. of } A_j\text{'s less than } m)p + (\text{no. of } B_j\text{'s less than } m)q$

$+ (\text{no. of } C_j\text{'s less than } m)r + u_1.$

Corollary 7.4.1 of [6] gives the number of A_j's less than m as $C_m - B_m - m$, the number of B_j's less than m as $C_m - 2A_m - 1$, and the number of C_j's less than m as $3B_m - 2C_m$. Each of these is zero for $m = 1$.

We again return to our special sequence U of (4.5) and consider A, B, and C transforms as in Section 2. We write the matrix Q^* and consider the AU, BU, and CU transforms:

$$Q^* = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

For AU, we have

$$Q^{*2}V = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} p \\ q \\ r \end{pmatrix} = \begin{pmatrix} p + q + r \\ p \\ p + q \end{pmatrix}$$

and

$$u_{A_{m+1}} - u_{A_m} = \begin{cases} p + q + r, & m \in A \\ p, & m \in B \\ p + q, & m \in C \end{cases} \tag{4.6}$$

For BU, we write the matrix multiplication $Q^{*3}V$,

$$Q^{*3}V = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} p \\ q \\ r \end{pmatrix} = \begin{pmatrix} 2p + q + r \\ p + q \\ p + q + r \end{pmatrix}$$

and

$$u_{B_{m+1}} - u_{B_m} = \begin{cases} 2p + q + r, & m \in A; \\ p + q, & m \in B; \\ p + q + r, & m \in C. \end{cases} \tag{4.7}$$

For CU, we write $Q^{*4}V$,

$$Q^{*4}V = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 1 & 1 \\ 2 & 1 & 1 \end{pmatrix}\begin{pmatrix} p \\ q \\ r \end{pmatrix} = \begin{pmatrix} 3p + 2q + r \\ p + q + r \\ 2p + q + r \end{pmatrix}$$

and

$$u_{C_{m+1}} - u_{C_m} = \begin{cases} 3p + 2q + r, & m \in A; \\ p + q + r, & m \in B; \\ 2p + q + r, & m \in C. \end{cases} \tag{4.8}$$

Here, as a bonus, we can work with the transformation HU by using the matrix Q^* itself. Since $A \cup B \cup C = N$, using H and B transforms corresponds to the number of compositions of n using 1's and 3's, which is given in terms of the sequence U_n, defined at the beginning of this section by U_{n-1}.

REFERENCES

1. W. W. Rouse Ball. *Mathematical Recreations and Essays* (revised by H. S. M. Coxeter), pp. 36-40. New York: Macmillan, 1962.
2. A. F. Horadam. "Wythoff Pairs." *The Fibonacci Quarterly* 16, No. 2 (April 1978):147-151.
3. R. Silber. "A Fibonacci Property of Wythoff Pairs." *The Fibonacci Quarterly* 14, No. 4 (Nov. 1976):380-384.
4. V. E. Hoggatt, Jr., & A. P. Hillman. "A Property of Wythoff Pairs." *The Fibonacci Quarterly* 16, No. 5 (Oct. 1978):472.
5. V. E. Hoggatt, Jr., & Marjorie Bicknell-Johnson. "A Generalization of Wythoff's Game." *The Fibonacci Quarterly* 17, No. 3 (Oct. 1979):198-211.
6. V. E. Hoggatt, Jr., & Marjorie Bicknell-Johnson. "Lexicographic Ordering and Fibonacci Representations." *The Fibonacci Quarterly* 20, No. 3 (Aug. 1982):193-218.
7. V. E. Hoggatt, Jr., & A. P. Hillman. "Nearly Linear Functions." *The Fibonacci Quarterly* 17, No. 1 (Feb. 1979):84-89.
8. V. E. Hoggatt, Jr., & Marjorie Bicknell-Johnson. "A Class of Equivalent Schemes for Generating Arrays of Numbers." *The Fibonacci Quarterly*, to appear.

*****

SELF-GENERATING SYSTEMS

RICHARD M. GRASSL
University of New Mexico, Albuquerque, NM 87131
(Submitted September 1980)

Let $S = a_1, a_2, \ldots,$ and $T = b_1, b_2, \ldots$ be sequences of integers, and let g be an integer. Then gS and $S + T$ denote the sequences $ga_1, ga_2, \ldots$ and $a_1 + b_1, a_2 + b_2, \ldots,$ respectively. Also $\{S\}$ denotes the set $\{a_1, a_2, \ldots\}$.

If the a_n of S are positive and strictly increasing, the characteristic sequence $\chi S = c_1, c_2, \ldots$ has $c_n = 1$ when n is in $\{S\}$ and $c_n = 0$ otherwise. Also ΔS denotes the sequence $d_1, d_2, \ldots$ with $d_n = a_{n+1} - a_n$.

DEFINITION: A system $S_1, S_2, \ldots, S_r$ of sequences of strictly increasing positive integers is *self-generating* if the sets $\{S_1\}, \{S_2\}, \ldots, \{S_r\}$ partition $Z^+ = \{1, 2, 3, \ldots\}$ and there is an $r \times r$ matrix (d_{hk}) with positive integral entries such that

$$\Delta S_h = d_{h1}(\chi S_1) + d_{h2}(\chi S_2) + \cdots + d_{hr}(\chi S_r) \qquad \text{for } 1 \leqslant h \leqslant r.$$

Hoggatt and Hillman in [2] and [3] used shift functions based on certain linear homogeneous recursions to obtain self-generating systems. In Theorem 5 of Section 7 below, we generalize on their work by increasing the set of recursions for which similar results follow. Examples are given in Section 8.

1. THE RECURSIVE SEQUENCE U

In the following, d and $p_1, p_2, \ldots, p_d$ are fixed integers with $d \geqslant 2$ and $p_1 \geqslant p_2 \geqslant \cdots \geqslant p_{d-1} \geqslant p_d = 1$. Also u_n is defined for all integers n by initial conditions

$$u_1 = 1,\ u_0 = u_{-1} = u_{-2} = \cdots = u_{2-d} = 0 \tag{1}$$

and the recursion

$$u_{n+d} = p_1 u_{n+d-1} + p_2 u_{n+d-2} + \cdots + p_d u_n. \tag{2}$$

For each integer i, let U_i denote the sequence $u_{i+1}, u_{i+2}, \ldots$ and let U_0 be written as U.

Hoggatt and Hillman obtained self-generating systems using such recursions for the case $d = 2$ in [3] and for general d with $p_1 = p_2 = \cdots = p_d = 1$ in [2].

In the representations discussed below, we want U to be an increasing sequence of positive integers with 1 as the first term. This is clearly true when $p_1 > 1$. If $p_1 = 1$, then $u_1 = u_2 = 1$ and one of these terms must be deleted; this is equivalent to changing the initial conditions (1) to the conditions $u_h = 2^{h-1}$ for $1 \leqslant h \leqslant d$ of [2]. Since the case $p_1 = 1$ is that of [2], we avoid notational complications by assuming that $p_1 > 1$ in what follows.

The representations introduced next are similar to those of the papers in the special January 1972 issue of this Quarterly as well as those of [2] and [3].

2. CANONICAL REPRESENTATIONS

Let $N = \{0, 1, 2, \ldots\}$. If $X = x_1, x_2, \ldots$ and $Y = y_1, y_2, \ldots$ are sequences of numbers with $x_n = 0$ for $n > h$, let

$$X \cdot Y = x_1y_1 + x_2y_2 + \cdots + x_hy_h.$$

In this section the only properties of $U = u_1, u_2, \ldots$ needed are $u_1 = 1$ and the fact that U is an increasing sequence of integers.

With respect to U, we define inductively for each m in N a sequence $E_m = e_{m1}, e_{m2}, \ldots$ of nonnegative integers as follows. Let all the terms of E_0 be zero. Assume that E_h has been defined for $0 \leqslant h < m$. Since the u_n are unbounded and $u_1 = 1 \leqslant m$, there is a largest k such that $u_k \leqslant m$. For this k, let $t = m - u_k$. Then E_t is defined, and we let $e_{mk} = 1 + e_{tk}$ and $e_{mn} = e_{tn}$ for $n \neq k$. Clearly $E_m \cdot U = m$, i.e., we have the representation

$$m = e_{m1}u_1 + e_{m2}u_2 + \cdots . \tag{3}$$

It is also clear that when $m = u_k$ with $k \geqslant 1$, $e_{mk} = 1$ and $e_{ms} = 0$ for $s \neq k$.

For $n \geqslant 2$, let q_n and r_n be the integers (guaranteed by the division algorithm) such that

$$m - (e_{m,n+1}u_{n+1} + e_{m,n+2}u_{n+2} + \cdots) = q_nu_n + r_n, \quad 0 \leqslant r_n < u_n.$$

Then the definition of E_m implies that

$$q_n = e_{mn} \quad \text{and} \quad r_n = e_{m1}u_1 + e_{m2}u_2 + \cdots + e_{m,n-1}u_{n-1}.$$

Hence

$$e_{m1}u_1 + e_{m2}u_2 + \cdots + e_{m,n-1}u_{n-1} < u_n \text{ for } n \geqslant 2. \tag{4}$$

We next show that (4) and the fact that each e_{mh} is a nonnegative integer characterize E_m.

<u>*LEMMA 1*</u>*: Let $E = e_1, e_2, \ldots$ and $E' = e_1', e_2', \ldots$ be sequences of nonnegative integers with $e_n = 0 = e_n'$ for n greater than some r. Also let*

$$e_1u_1 + e_2u_2 + \cdots + e_{n-1}u_{n-1} < u_n$$

and

$$e_1'u_1 + e_2'u_2 + \cdots + e_{n-1}'u_{n-1} < u_n \text{ for } n \geqslant 2 \tag{5}$$

and $E \cdot U = E' \cdot U$. *Then* $E = E'$.

PROOF: Since $e_n = 0 = e_n'$ for $n > r$, $E \neq E'$ implies that there is a largest n with $e_n \neq e_n'$, and we let t be this n. Without loss of generality, we let $e_t < e_t'$. Upon deletion of the equal terms in $E \cdot U = E' \cdot U$, we have

$$e_1u_1 + \cdots + e_tu_t = e_1'u_1 + \cdots + e_t'u_t.$$

Since $u_1 = 1$, this implies that $t > 1$. Then

$$\begin{aligned} u_t &\leqslant (e_t' - e_t)u_t = e_t'u_t - e_tu_t \\ &= (e_1u_1 + \cdots + e_{t-1}u_{t-1}) - (e_1'u_1 + \cdots + e_{t-1}'u_{t-1}). \end{aligned}$$

Since each $e_n' \geqslant 0$, this implies that

$$u_t \leqslant e_1u_1 + \cdots + e_{t-1}u_{t-1},$$

contradicting (5) and proving that $E = E'$.

The following definition introduces another characteristic property of the E_m which will be needed below.

DEFINITION: A sequence $E = e_1, e_2, \ldots$ is *compatible* [with respect to the recursion (2)] if, for any h in Z^+ and any integer k with $1 \leqslant k \leqslant d$, the sequence of k differences

$$p_1 - e_{h+k-1},\ p_2 - e_{h+k-2},\ \ldots,\ p_k - e_h \tag{6}$$

has the two following properties:

I. If $h = 1$ or $k = d$, at least one difference in (6) is nonzero.

II. If some difference in (6) is nonzero, the first nonzero difference is positive.

THEOREM 1: For each m in Z^+, E_m is compatible. Also if $E = e_1, e_2, \ldots$ is a compatible sequence with $e_n = 0$ for n greater than some n_0 and $E \cdot U = m$ then $E = E_m$.

PROOF: We first show that E_m is compatible. Let $E = E_m$. If $h = 1$ or $k = d$ and all the differences in (6) were zero, then it would follow from (1) and (2) that

$$u_{h+k} = e_{h+k-1}u_{h+k-1} + e_{h+k-2}u_{h+k-2} + \cdots + e_hu_h.$$

Since this would contradict (4), we have shown than I holds.

To prove II, we assume it false and seek a contradiction. Then we can assume that in (6) the first nonzero difference is $p_g - e_{h+k-g}$ and also that $e_{h+k-g} \geqslant 1 + p_g$. These assumptions would imply

$$\sum_{j=h}^{h+k-1} e_j u_j \geqslant \sum_{j=h+k-g}^{h+k-1} e_j u_j \geqslant u_{h+k-g} + \sum_{j=1}^{g} p_j u_{h+k-j}.$$

Here, if one uses the recursion (2) to replace u_{h+k-g} by $\sum_{j=1}^{d} p_j u_{h+k-g-j}$, one finds, since $p_1 \geqslant p_2 \geqslant \cdots \geqslant p_d$, that

$$\begin{aligned}\sum_{j=h}^{h+k-1} e_j u_j &\geqslant \sum_{j=1}^{d} p_j u_{h+k-g-j} + \sum_{j=1}^{g} p_j u_{h+k-j}\\ &\geqslant \sum_{j=g+1}^{d} p_j u_{h+k-j} + \sum_{j=1}^{g} p_j u_{h+k-j} = u_{h+k}.\end{aligned}$$

This contradicts (4), and thus II holds, and E_m is compatible.

Second, assume that E is compatible, the desired n_0 exists, and $E \cdot U = m$. It suffices to show that $u_n > e_1u_1 + e_2u_2 + \cdots + e_{n-1}u_{n-1}$ for $n \geqslant 2$, since this, the hypothesis $E \cdot U = m$, (4), and Lemma 1 imply that $E = E_m$. We prove these inequalities by induction on n. The hypotheses I and II with $h = 1 = k$ imply that $p_1 > e_1$. Hence, $u_2 = p_1 > e_1 = e_1u_1$, and the case $n = 2$ is true. Assume that $n > 2$ and that the desired inequalities are true for 2, 3, ..., $n - 1$. Using I and II, one finds a k in $\{1, 2, \ldots, d\}$ such that

$$p_k \geqslant 1 + e_{n-k} \quad \text{and} \quad p_j = e_{n-j} \quad \text{for } 1 \leqslant j < k. \tag{7}$$

Using the hypothesis of the induction and $n - k < n$, one has

$$u_{n-k} > \sum_{j=1}^{n-k-1} e_j u_j. \tag{8}$$

Using (2), (7), and (8), one sees that

$$u_n = \sum_{j=1}^{d} p_j u_{n-j} \geqslant u_{n-k} + \sum_{j=1}^{k} e_{n-j}u_{n-j} > \sum_{j=1}^{n-k-1} e_j u_j + \sum_{j=1}^{k} e_{n-j}u_{n-j} = \sum_{j=1}^{n-1} e_j u_j.$$

This establishes the desired inequality for n and completes the proof of the theorem.

<u>LEMMA 2</u>: *Let $k \geqslant 1$, $w = u_k$. Also define the sequence $F = f_1, f_2, \ldots$ by*

$$f_1 = p_r - 1, \text{ where } r \in \{1, 2, \ldots, d\} \text{ and } r \equiv k - 1 \pmod{d};$$

$f_n = 0$ *for* $n \geqslant k$;

$f_n = 0$ *for* $n \equiv k \pmod{d}$;

$f_n = p_j$ *when* $k - n \equiv j \pmod{d}$, $1 < n < k$, *and* $n \not\equiv k \pmod{d}$.

Then $E_{w-1} = F$.

PROOF: Obviously F is compatible. Since $p_d = 1$, repeated use of (2) gives

$$u_z = u_{z-qd} + \sum_{h=0}^{q-1} \sum_{k=1}^{d-1} p_k u_{z-hd-k} \text{ for } q \in Z^+. \tag{9}$$

Now let $q \in N$, $r \in \{1, 2, \ldots, d\}$, and $z = qd + r + 1$. Then

$$u_{z-qd} = u_{r+1} = p_1 u_r + p_2 u_{r-1} + \cdots + p_r u_1$$

follows from (2). Hence, (9) can be rewritten as

$$u_z = u_{qd+r+1} = \sum_{h=0}^{q-1} \sum_{k=1}^{d-1} p_k u_{z-hd-k} + \sum_{k=1}^{r} p_k u_{r+1-k}. \tag{10}$$

Now, $F \cdot U = w - 1$ follows from (10), and then Theorem 1 gives us the desired $E_{w-1} = F$.

3. PARTITIONING Z^+

Let $m \in Z^+$. Then $e_{mk} \neq 0$ for some k and we define z_m as follows: if $e_{m1} > 0$, $z_m = 1$, and if $e_{m1} = 0$, then z_m is the largest h such that $e_{ms} = 0$ for $1 \leqslant s < h$. For $1 \leqslant t \leqslant d$, let $V_t = \{m : z_m \equiv t \pmod{d}\}$. Clearly, V_1, V_2, ..., V_d form a partitioning of Z^+.

4. THE SHIFT FUNCTIONS σ^i

Let Z be the set of all integers. Recall that U_i denotes the sequence u_{i+1}, u_{i+2}, ... For each i in Z, let σ^i be the function from N to Z with

$$\sigma^i(m) = E_m \cdot U_i = e_{m1} u_{i+1} + e_{m2} u_{i+2} + \cdots \quad \text{for all } m \text{ in } N.$$

The following properties are easy to verify:

(i) $\sigma^i(m)$ satisfies the recursion (2) for fixed m in N and varying i.

(ii) $\sigma^i(0) = 0$ for all i in Z.

(iii) $\sigma^i(u_k) = u_{k+i}$ for i in Z and k in Z^+.

(iv) $\sigma^{i+1}(m) = \sigma(\sigma^i(m))$ for m and i in N. The proof of this depends on the fact that the canonical representation of $\sigma^i(m)$ is, in fact, E_m shifted i times.

(v) $\sigma^0(m) = m$ for m in N.

5. DIFFERENCING σ^i

For i in Z and m in Z^+, let the backward difference $\nabla\sigma^i(m)$ be defined by

$$\nabla\sigma^i(m) = \sigma^i(m) - \sigma^i(m-1) = E_m \cdot U_i - E_{m-1} \cdot U_i.$$

For i in Z and n in Z^+, let $D_{in} = \nabla\sigma^i(u_n)$. If $u_n = w$, then $E_w = e_1, e_2, \ldots$ with $e_n = 1$ and $e_t = 0$ for $t \neq n$ and $E_{w-1} = f_1, f_2, \ldots, f_{n-1}, 0, 0, \ldots$ with the f_j as described in Lemma 2. Then

$$D_{in} = u_{i+n} - \sum_{j=1}^{n-1} f_j u_{i+j}.$$

Let $n \equiv k \pmod{d}$ with k in $\{1, 2, \ldots, d\}$. Temporarily, let $i \geqslant 2$. Then, using (10) with $z = i + n$, the formulas of Lemma 2 for the f_j, and the recursion (2), one finds that

$$D_{in} = u_{i+1} \quad \text{if } k = 1, \tag{11}$$

and if $k \neq 1$,

$$\begin{aligned} D_{in} &= u_{i+1} + p_k u_i + p_{k+1} u_{i-1} + \cdots + p_d u_{i+k-d} \\ &= u_{i+1} + u_{i+k} - p_1 u_{i+k-1} - \cdots - p_{k-1} u_{i+1}. \end{aligned} \tag{12}$$

For fixed n and varying i, the D_{in} satisfy the same recursion (2) as the u's. Hence, the truth of (11) and (12) for $i \geqslant 2$ implies these formulas for all integers i. In particular, these formulas imply the following lemma.

LEMMA 3: $D_{in} = D_{ik}$ *if* $n \equiv k \pmod{d}$.

Next we show that $\nabla\sigma^i(m)$ depends only on i and the k such that $m \in V_k$.

THEOREM 2: *Let* $m \in V_k$. *Then* $\nabla\sigma^i(m) = D_{ik}$.

PROOF: Let $E_m = e_1, e_2, \ldots$. Since $m \in V_k$, there is a positive integer z such that $z \equiv k \pmod{d}$, $e_z > 0$, and $e_s = 0$ for $1 \leqslant s < z$. Let $w = e_z$ and $E_{w-1} = f_1, f_2, \ldots, f_{z-1}, 0, 0, \ldots$. Using Theorem 1, one finds that

$$E_{m-1} = f_1, f_2, \ldots, f_{z-1}, e_z - 1, e_{z+1}, e_{z+2}, \ldots$$

and hence,

$$\nabla\sigma^{i}(m) = E_m \cdot U_i - E_{m-1} \cdot U_i = D_{iz}.$$

Then Lemma 3 implies that $\nabla\sigma^{i}(m) = D_{ik}$ as desired.

The two following results are not needed for the main theorem (Theorem 5 below) but they generalize on work of [2] and [3].

<u>LEMMA 4</u>: *For $1 \leqslant i < d$, $\nabla\sigma^{-i}(m)$ is 1 for m in V_{i+1} and is 0 otherwise.*

<u>PROOF</u>: Temporarily, let $k \neq 1$. By Theorem 2 and (12), for m in V_k,

$$\begin{aligned}\nabla\sigma^{-i}(m) &= u_{k-i} - p_1 u_{k-i-1} - \cdots - p_{k-1}u_{-i+1} + u_{-i+1}\\ &= (u_{k-i} - p_1 u_{k-i-1} - \cdots - p_{k-i}u_0) - p_{k-i+1}u_{-1} - \cdots\\ &\qquad - p_{k-1}u_{-i+1} + u_{-i+1}.\end{aligned}$$

For $k = i + 1$, this becomes

$$\nabla\sigma^{-i}(m) = u_1 - p_1 u_0 - p_2 u_{-1} - \cdots - p_i u_{-i+1} + u_{-i+1} = u_1 = 1,$$

since

$$u_0 = u_{-1} = \cdots = u_{2-d} = 0.$$

For $k \neq i + 1$, i.e., for m not in V_k, $\nabla\sigma^{-i}(m) = 0$, since

$$u_{k-i} = p_1 u_{k-i-1} + \cdots + p_{k-i}u_0$$

by (1) and (2). The same results are obtained for $k = 1$ from (11).

<u>THEOREM 3</u>: *Let $|S|$ denote the number of elements in the set S. Then*

(i) $\sigma^{-i}(m) = |V_{i+1} \cap \{1, 2, \ldots, m\}|$ *for* $i = 1, 2, \ldots, d-1$.

(ii) $m - \sigma^{-1}(m) - \sigma^{-2}(m) - \cdots - \sigma^{-(d-1)}(m) = |V_1 \cap \{1, 2, \ldots, m\}|$.

<u>PROOF</u>: For (i),

$$\begin{aligned}\nabla\sigma^{-i}(1) + \nabla\sigma^{-i}(2) + \cdots + \nabla\sigma^{-i}(m) &= [\sigma^{-i}(1) - \sigma^{-i}(0)] + [\sigma^{-i}(2) - \sigma^{-i}(1)]\\ &\qquad + \cdots + [\sigma^{-i}(m) - \sigma^{-i}(m-1)]\\ &= \sigma^{-i}(m) - \sigma^{-i}(0) = \sigma^{-i}(m).\end{aligned}$$

For fixed i, by Lemma 4, $\nabla\sigma^{-i}(1) + \cdots + \nabla\sigma^{-i}(m)$ is the number of integers in $V_{i+1} \cap \{1, 2, \ldots, m\}$. But the telescoping sum shows this to be $\sigma^{-i}(m)$. Part (ii) follows from (i).

6. A PARTITIONING OF N

For $i = 1, 2, \ldots, d$ and $j = 0, 1, \ldots, p_i - 1$, let B_{ij} be the sequence $b_0, b_1, \ldots$ with $b_m = u_{i+1} + j - p_i + \sigma^i(m)$. When the dependence of b_m on i and j has to be indicated, we will write b_m as b_{ijm}.

THEOREM 4: The $p_1 + p_2 + \cdots + p_d$ subsets $\{B_{ij}\}$ partition N.

PROOF: Let $s \in N$. We need to show that there is a unique ordered triple (i, j, m) such that

$$s = u_{i+1} + j - p_i + \sigma^i(m). \tag{13}$$

Let $E_s = e_1, e_2, \ldots$ and for the sought after m, let $E_m = f_1, f_2, \ldots$, i.e., let $e_{sk} = e_k$ and $e_{mk} = f_k$. With this notation and using (1) and (2), one can rewrite (13) as

$$s = p_1u_i + p_2u_{i-1} + \cdots + p_{i-1}u_2 + p_iu_1 + j - p_i + f_1u_{i+1} + f_2u_{i+2} + \cdots .$$

Since $u_1 = 1$, $p_iu_1 + j - p_i = ju_1$ and the equation takes the form

$$s = ju_1 + p_{i-1}u_2 + p_{i-2}u_3 + \cdots + p_1u_i + f_1u_{i+1} + f_2u_{i+2} + \cdots . \tag{14}$$

Using the condition of Theorem 1 that $E_m = f_1, f_2, \ldots$ must be compatible, together with the fact that $j \leqslant p_i - 1$, one sees that the sequence

$$S = j, p_{i-1}, p_{i-2}, \ldots, p_1, f_1, f_2, \ldots$$

must be compatible. Since the right side of (14) is $S \cdot U$, Theorem 1 (with m replaced by s) tells us that (13) is equivalent to $S = E_s$.

If there is no i with $2 \leqslant i \leqslant d$ and

$$(p_1, p_2, \ldots, p_{i-1}) = (e_i, e_{i-1}, \ldots, e_2) \tag{15}$$

then the sequence $e_2, e_3, \ldots$ is compatible and $E_s = S$ holds if and only if $i = 1$, $j = e_1$, and the sequence $e_2, e_3, \ldots$ is the sequence $f_1, f_2, \ldots$.

Now assume that (15) holds for some i in $\{2, 3, \ldots, d\}$ but not for any larger integer in this set. We wish to show that the sequence

$$e_{i+1}, e_{i+2}, \ldots \tag{16}$$

is compatible. Since $e_1, e_2, \ldots$ is compatible, (16) can fail to be compatible only if there is an integer g with

$$(p_1, p_2, \ldots, p_g) = (e_{i+g}, e_{i+g-1}, \ldots, e_{i+1}) \text{ and } i \leqslant g < d. \tag{17}$$

Then condition II (of the definition of a compatible sequence) with $h = i$ and

$k = 1 + g$ would imply that $e_i \leqslant p_{g+1}$. If $e_i < p_{g+1}$, (15) gives us the contradiction $p_1 = e_i < p_{g+1} \leqslant p_1$. Now condition I implies that $g + 1 < d$. Also $e_i = p_{g+1}$ similarly implies that $p_1 = p_2 = \cdots = p_{g+1}$. This, (17), and the equality $p_1 = e_i$ from (15) would give us

$$(p_1, p_2, \ldots, p_{g+1}) = (e_{i+g}, e_{i+g-1}, \ldots, e_i).$$

As before, condition II with $h = i - 1$ and $k = 2 + g$ implies that $p_{g+2} = p_1$, and hence that

$$(p_1, p_2, \ldots, p_{g+2}) = (e_{i+g}, e_{i+g-1}, \ldots, e_{i-1}).$$

This process would continue until we had

$$(p_1, p_2, \ldots, p_{i+g-1}) = (e_{i+g}, e_{i+g-1}, \ldots, e_2),$$

which contradicts the fact that the i in (15) is maximal.

Hence $e_{i+1}, e_{i+2}, \ldots$ satisfies I and II and so is compatible. Then $E_s = S$ holds if and only if i is the maximal i for (15), $j = e_1$, and

$$f_1, f_2, \ldots = e_{i+1}, e_{i+2}, \ldots .$$

This completes the proof.

7. SELF-GENERATING SYSTEM

For $i = 1, 2, \ldots, d$ and $j = 1, 2, \ldots, p_i$, let A_{ij} be the sequence

$$a_{ij1}, a_{ij2}, \ldots$$

with $a_{ijm} = 1 + b_{i,j-1,m-1}$ (the b's are as in Section 6). When both i and j are known from the context, we may write a_{ijm} as a_m.

THEOREM 5: The sequences A_{ij} for $1 \leqslant i \leqslant d$ and $1 \leqslant j \leqslant p_i$ form a self-generating system.

PROOF: From the definition of the sets $\{B_{i,j-1}\}$ in Section 6 and V_k in Section 3, it follows that

$$V_1 = \{A_{d1}\} \cup T, \tag{18}$$

where T is the union of the $\{A_{ij}\}$ for $1 \leqslant i < d$ and $1 \leqslant j < p_i$, and that

$$V_{h+1} = \{A_{h,p_h}\} \text{ for } h = 1, 2, \ldots, d - 1.$$

Since the $\{B_{ij}\}$ form a partition of N (or, equivalently, since the V's partition Z^+), the $\{A_{ij}\}$ partition Z^+. Since $b_{ijm} = u_{i+1} + j - p_i + \sigma^i(m)$,

$$\begin{aligned}\nabla b_{ijm} = b_{i,j,m} - b_{i,j,m-1} &= (u_{i+1} + j - p_i + \sigma^i(m)) - (u_{i+1} + j - p_i + \sigma^i(m-1)) \\ &= \sigma^i(m) - \sigma^i(m-1) = \\ &= \nabla\sigma^i(m).\end{aligned}$$

Then by Theorem 2 we have

$$\nabla b_{ijm} = \nabla\sigma^i(m) = D_{ik} \text{ if } m \in V_k.$$

Since $a_{ijm} = 1 + b_{i,j-1,m-1}$, ΔA_{ij} is the sequence $d_1, d_2, \ldots$ with

$$d_m = a_{i,j,m+1} - a_{i,j,m} = b_{i,j-1,m} - b_{i,j-1,m-1} = D_{ik}$$

when $m \in V_k$. Since each V_k is an $\{A_{ij}\}$ or a union of $\{A_{ij}\}$,

$$\Delta A_{ij} = \sum_{\substack{1 \leq h \leq d \\ 1 \leq k \leq p_h}} d_{ijhk} \chi A_{hk}$$

where $d_{ijhk} = D_{is}$ when $\{A_{hk}\}$ is a subset of V_s.

8. EXAMPLE

For $d = 3$ and $p_1 = p_2 = 3$, $p_3 = 1$, we have $u_{n+3} = 3u_{n+2} + 3u_{n+1} + u_n$ and $U = 1, 3, 12, 46, 177, \ldots$. As an illustration of the canonical representation in Section 1, for $m = 136$, we have $E_m = 2, 2, 3, 2, 0, 0, \ldots$ and $\sigma(m) = 2u_2 + 2u_3 + 3u_4 + 2u_5 = 522$. The following is a table of the $\sigma^i(m)$ for the i's involved in Theorem 5.

m	0	1	2	3	4	5	6	7	8	9	10	11	12
$\sigma(m)$	0	3	6	12	15	18	24	27	30	36	39	42	46
$\sigma^2(m)$	0	12	24	46	58	70	92	104	116	138	150	162	177
$\sigma^3(m)$	0	46	92	177	223	269	354	...					

The $p_1 + p_2 + p_3 = 7$ subsets partitioning Z^+ are:

$\{A_{11}\} = \{\sigma(m) + 1\} = \{1, 4, 7, 13, 16, 19, 25, 28, 31, 37, 40, \ldots\}$
$\{A_{12}\} = \{\sigma(m) + 2\} = \{2, 5, 8, 14, 17, 20, 26, 29, 32, 38, 41, \ldots\}$
$\{A_{13}\} = \{\sigma(m) + 3\} = \{3, 6, 9, 15, 18, 21, 27, 30, 33, 39, 42, \ldots\}$
$\{A_{21}\} = \{\sigma^2(m) + 10\} = \{10, 22, 34, 56, 68, 80, 102, \ldots\}$
$\{A_{22}\} = \{\sigma^2(m) + 11\} = \{11, 23, 35, 57, 69, 81, 103, \ldots\}$
$\{A_{23}\} = \{\sigma^2(m) + 12\} = \{12, 24, 36, 58, 70, 82, 104, \ldots\}$

and

$\{A_{31}\} = \{\sigma^3(m) + 46\} = \{46, 92, 138, 223, \ldots\}$.

The following is a table of D_{ik} for $-2 \leqslant i \leqslant 3$ and $1 \leqslant k \leqslant 3$.

$k \backslash i$	-2	-1	0	1	2	3
1	0	0	1	3	12	46
2	0	1	1	6	22	85
3	1	0	1	4	15	58

Since $V_1 = A_{11} \cup A_{12} \cup A_{21} \cup A_{22} \cup A_{31}$, $V_2 = A_{13}$, and $V_3 = A_{23}$, we have

$$\begin{aligned}\Delta A_{1j} &= D_{11}(\chi A_{11}) + D_{11}(\chi A_{12}) + D_{12}(\chi A_{13}) + D_{11}(\chi A_{21})\\ &\quad + D_{11}(\chi A_{22}) + D_{13}(\chi A_{23}) + D_{11}(\chi A_{31})\\ \Delta A_{2j} &= D_{21}(\chi A_{11}) + D_{21}(\chi A_{12}) + D_{22}(\chi A_{13}) + D_{21}(\chi A_{21})\\ &\quad + D_{21}(\chi A_{22}) + D_{23}(\chi A_{23}) + D_{21}(\chi A_{31})\\ \Delta A_{3j} &= D_{31}(\chi A_{11}) + D_{31}(\chi A_{12}) + D_{32}(\chi A_{13}) + D_{31}(\chi A_{21})\\ &\quad + D_{31}(\chi A_{22}) + D_{33}(\chi A_{23}) + D_{31}(\chi A_{31})\end{aligned}$$

and the 7×7 matrix (d_{hk}) for the self-generating system $A_{11}, A_{12}, A_{13}, A_{21}, A_{22}, A_{23}, A_{31}$ is

$$\begin{pmatrix} 3 & 3 & 6 & 3 & 3 & 4 & 3\\ 3 & 3 & 6 & 3 & 3 & 4 & 3\\ 3 & 3 & 6 & 3 & 3 & 4 & 3\\ 12 & 12 & 22 & 12 & 12 & 15 & 12\\ 12 & 12 & 22 & 12 & 12 & 15 & 12\\ 12 & 12 & 22 & 12 & 12 & 15 & 12\\ 46 & 46 & 85 & 46 & 46 & 58 & 46 \end{pmatrix}$$

As an illustration of Theorem 3(i), with $i = 1$ and $m = 20$,

$$\begin{aligned}\sigma^{-1}(20) &= \sigma^2(20) - 3\sigma(20) - 3\sigma^0(20)\\ &= 2u_3 + 2u_4 + u_5 - 3(2u_2 + 2u_3 + u_4) - 60\\ &= 5 = |V_2 \cap \{1, 2, \ldots, 20\}|,\end{aligned}$$

where $V_2 = \{n : z_n \equiv 2 \pmod 3\} = \{3, 6, 9, 15, 18\}$ since the only sequences E_n, with $n \leqslant 20$ and $z_n \equiv 2 \pmod 3$ are:

$$E_3 = 0,\ 1,\ 0,\ 0,\ \ldots$$
$$E_6 = 0,\ 2,\ 0,\ 0,\ \ldots$$
$$E_9 = 0,\ 3,\ 0,\ 0,\ \ldots$$
$$E_{15} = 0,\ 1,\ 1,\ 0,\ \ldots$$
$$E_{18} = 0,\ 2,\ 1,\ 0,\ \ldots$$

REFERENCES

1. L. Carlitz, Richard Scoville, & V. E. Hoggatt, Jr. "Fibonacci Representations." *The Fibonacci Quarterly* 10, No. 1 (1972):29-42.
2. V. E. Hoggatt, Jr., & A. P. Hillman. "Nearly Linear Functions." *The Fibonacci Quarterly* 17, No. 1 (1979):84-89.
3. V. E. Hoggatt, Jr., & A. P. Hillman. "Recursive, Spectral, and Self-Generating Sequences." *The Fibonacci Quarterly* 18, No. 2 (1980):97-103.
4. See the special issue of *The Fibonacci Quarterly* (Vol. 10, No. 1 [1972]) on Representations.

★★★★★

POSSIBLE PERIODS OF PRIMARY FIBONACCI-LIKE SEQUENCES WITH RESPECT TO A FIXED ODD PRIME

LAWRENCE SOMER
1400 20th St., NW #619, Washington, D.C. 20036
(Submitted February 1981)

1. INTRODUCTION

Let $\{u_n\}$ be a primary Fibonacci-like sequence (PFLS) defined by the recursion relation

$$u_{n+2} = au_{n+1} + bu_n, \tag{1}$$

where $u_0 = 0$, $u_1 = 1$, and a and b are integers. We will call a and b the parameters of the recurrence. We will denote such a sequence as $u(a, b)$. Two of the most important questions concerning these sequences are: For a given PFLS $u(a, b)$, which odd primes have a maximal rank of apparition? and For which odd primes does the PFLS $u(a, b)$ have a maximal period modulo p? No definitive results are known for these questions. What we propose to do in this paper is to first present the best known results concerning these questions. Then we will turn the questions around and fix the odd prime and ask which PFLS's have maximal ranks of apparition and maximal periods with respect to that prime. In a previous paper [6], the author obtained partial results by considering only those PFLS's $u(a, b)$ for which $b = 1$.

Before proceeding further, we will need a few definitions. We will let $\mu(a, b, p)$ denote the period of the PFLS $u(a, b)$ reduced modulo p, where p is an odd prime. Moreover, $\alpha(a, b, p)$ will denote the rank of apparition of p in the PFLS $u(a, b)$. Let $s(a, b, p)$ be the multiplier of the PFLS $u(a, b)$ modulo p. If $k = \alpha(a, b, p)$, then $s(a, b, p) \equiv u_{k+1} \pmod{p}$. Then

$$\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p)$$

is the exponent of the multiplier $s(a, b, p)$ modulo p. Let the characteristic polynomial of the PFLS $u(a, b)$ be

$$x^2 - ax - b = 0. \tag{2}$$

Let $r_1 = (a + \sqrt{a^2 + 4b})/2$ and $r_2 = (a - \sqrt{a^2 + 4b})/2$ be the roots of this polynomial. Then by the Binet equations

$$u_n = (r_1^n - r_2^n)/(r_1 - r_2). \tag{3}$$

Let

$$D = a^2 + 4b = (r_1 - r_2)^2$$

be the discriminant of the characteristic polynomial. Throughout this paper K will denote the algebraic number field $Q(\sqrt{D})$. R will denote the integers of K. Further, Z_p and $\mathrm{GF}(p^2)$ will denote the Galois fields with p and p^2 elements, respectively. Finally, $\mathrm{ord}_p(d)$ will denote the exponent of d modulo p.

2. PRELIMINARY RESULTS

The following well-known results will be necessary for our later theorems.

LEMMA 1: *Let p be a prime. In the* PFLS *$u(a, b)$, suppose that $b \not\equiv 0 \pmod p$. Then the* PFLS *$u(a, b)$ is purely periodic modulo p and if $u \equiv 0 \pmod p$, then*

$$\alpha(a, b, p) \mid k. \tag{4}$$

If $b \equiv 0$ and $a \not\equiv 0 \pmod p$, then the rank of apparition of p in $u(a, b)$ is undefined and $u(a, b)$ reduced modulo p is of the form

$$(0, 1, a, a^2, a^3, \ldots).$$

If $b \equiv 0$ and $a \equiv 0 \pmod p$, then $u(a, b)$ reduced modulo p is of the form

$$(0, 1, 0, 0, 0, \ldots).$$

PROOF: Suppose the pair (u_k, u_{k+1}) is the first pair of consecutive terms to repeat and $k \neq 0$. Let $m = \mu(a, b, p)$. Then $u_{k+m} \equiv u_k$ and $u_{k+1+m} \equiv u_{k+1} \pmod p$. However, by the recursion relation (1),

$$bu_{k-1} = u_{k+1} - au_k.$$

Since $b \not\equiv 0 \pmod p$,

$$u_{k-1} \equiv (u_{k+1} - au_k)/b \pmod p.$$

Thus, the pair (u_{k-1}, u_k) also repeats, which is a contradiction if $k \neq 0$. Thus, the pair (u_0, u_1) repeats. Hence, $u(a, b)$ is purely periodic modulo p. A similar argument shows that if $u_k \equiv 0 \pmod p$, then $\alpha(a, b, p) \mid k$. The rest of the lemma follows by direct verification.

LEMMA 2: *Let p be an odd prime. In the* PFLS *$u(a, b)$, suppose $b \not\equiv 0 \pmod p$. Then*

$$u_{p-(D/p)} \equiv 0 \pmod p,$$

where (D/p) is the Legendre symbol for the quadratic character of D modulo p. Further,

$$u_p \equiv (D/p) \pmod p.$$

PROOF: See [1, pp. 315-317] or [2, p. 45].

COROLLARY: Let p be an odd prime. Consider the PFLS $u(a, b)$. *Suppose* $b \not\equiv 0 \pmod{p}$. *Then if* $(D/p) = 1$,

$$\alpha(a, b, p) \mid p - 1$$

and $p - 1$ *is the maximal value for* $\alpha(a, b, p)$. *Further, if* $(D/p) = 1$,

$$\mu(a, b, p) \mid p - 1$$

and $p - 1$ *is the maximal value for* $\mu(a, b, p)$. *If* $(D/p) = -1$,

$$\alpha(a, b, p) \mid p + 1$$

and $p + 1$ *is the maximal value for* $\alpha(a, b, p)$. *Moreover, if* $(D/p) = -1$,

$$\mu(a, b, p) \mid p^2 - 1$$

and $p^2 - 1$ *is the maximal value for* $\mu(a, b, p)$.

3. SPECIAL PRIMES HAVING MAXIMAL PERIODS AND RANKS OF APPARITION

We will now see that given specific PFLS's $u(a, b)$, there exists a class of primes dependent on the parameters a and b with maximal ranks of apparition and maximal periods. In the case of ranks of apparition, we will also obtain the next best result, namely half-maximal ranks of apparition. We now present the following results.

LEMMA 3: Let p be an odd prime. Consider the PFLS $u(a, b)$. *Suppose* $p \nmid abD$.

(i) *If* $(-b/p) = 1$, *then*

$$u_{(p-(D/p))/2} \equiv 0 \pmod{p}.$$

(ii) *If* $(-b/p) = -1$, *then*

$$u_{(p-(D/p))/2} \not\equiv 0 \pmod{p}.$$

PROOF: See D. H. Lehmer [5] or Robert P. Backstrom [1].

THEOREM 1: Let p be an odd prime. Consider the PFLS $u(a, b)$. *Suppose* $p \nmid abD$.

(i) *If r is a prime and $p = 2r + 1$ is a prime such that* $(-b/p) = (D/p) = 1$, *then*

$$\alpha(a, b, p) = r = (p - 1)/2.$$

(ii) *If s is a prime and $p = 2s - 1$ is a prime such that $(-b/p) = (D/p) = -1$, then*

$$\alpha(a, b, p) = p + 1.$$

(iii) *If s is a prime and $p = 2s - 1$ is a prime such that $(-b/p) = 1$ and $(D/p) = -1$, then*

$$\alpha(a, b, p) = s = (p + 1)/2.$$

(iv) *If r is a prime and $p = 2r + 1$ is a prime such that $(-b/p) = -1$ and $(D/p) = 1$, then*

$$\alpha(a, b, p) = p - 1.$$

PROOF: See Backstrom [1]. This proof relies heavily on Lemma 3.

COROLLARY: Let p be an odd prime. Consider the PFLS *$u(a, b)$. Suppose $p \nmid abD$.*

(i) *If r is a prime and $p = 2r + 1$ is a prime such that $(-b/p) = (D/p) = 1$,*

$$\mu(a, b, p) = p - 1.$$

(ii) *If s is a prime and $p = 2s - 1$ is a prime such that $(D/p) = 1$ and $-b$ is a primitive root* modulo p, *then*

$$\mu(a, b, p) = p^2 - 1.$$

PROOF: (i) By the corollary to Lemma 2, $\mu(a, b, p)$ is at most $p - 1$ and the result now follows.

(ii) By Lemma 2,

$$u_p \equiv (D/p) \equiv -1 \pmod{p}$$

and

$$u_{p-(D/p)} = u_{p+1} \equiv 0 \pmod{p}.$$

Now, by the recursion relation,

$$\begin{aligned} s(a, b, p) &= u_{\alpha(a,b,p)+1} = u_{p+2} = bu_p + au_{p+1} \\ &\equiv -b + 0 \equiv -b \pmod{p}. \end{aligned}$$

Further,

$$\operatorname{ord}_p(s(a, b, p)) = \operatorname{ord}_p(-b) = p - 1$$

by hypothesis. Thus,

$$\mu(a,\ b,\ p) = \ (a,\ b,\ p) \cdot \mathrm{ord}_p(s(a,\ b,\ p))$$
$$= (p + 1)(p - 1) = p^2 - 1.$$

Unfortunately, it is not known if there exist an infinite number of pairs of primes of the form $(r,\ 2r + 1)$ or $(s,\ 2s - 1)$. Two other classic sets of primes, the Mersenne primes, $M_q = 2^q - 1$, where q is a prime, and the Fermat primes, $F_n = 2^{2^n} + 1$, can have maximal periods. We have the following theorems.

<u>THEOREM 2</u>: *Consider the* PFLS $u(a,\ b)$. *Let* $p = M_q = 2^q - 1$ *be a Mersenne prime.*

(i) *If* $(-b/p) = (D/p) = -1$, *then*

$$\alpha(a,\ b,\ p) = p + 1.$$

(ii) *If* $(D/p) = -1$ *and* $-b$ *is a primitive root* modulo p, *then*

$$\mu(a,\ b,\ p) = p^2 - 1.$$

<u>PROOF</u>: (i) By Lemma 2, $u_{p+1} \equiv 0 \pmod{p}$. Now by Lemma 1, if $u_k \equiv 0 \pmod{p}$, then $\alpha(a,\ b,\ p)|k$. Moreover, by Lemma 3, $p \nmid u_{(p+1)/2}$. The only divisors of $p + 1$ are 2^n, where $0 \leqslant n \leqslant q$. Thus,

$$\alpha(a,\ b,\ p) = p + 1,$$

since this is the only divisor of $p + 1$ not dividing $(p + 1)/2$.

(ii) This follows from the same argument used in the proof of assertion (ii) of the corollary to Theorem 1.

<u>THEOREM 3</u>: *Consider the* PFLS $u(a, b)$. *Let* $p = F_n = 2^{2^n} + 1$ *be a Fermat prime. If* $(-b/p) = -1$ *and* $(D/p) = 1$, *then*

$$\alpha(a,\ b,\ p) = \mu(a,\ b,\ p) = p - 1.$$

<u>PROOF</u>: By Lemma 2 and its corollary, $\alpha(a,\ b,\ p)|p_n - 1$ and $\mu(a,\ b,\ p)|p - 1$. The only divisors of $p - 1$ are 2^k, where $0 \leqslant k \leqslant 2$. But by Lemma 3, we have $p \nmid u_{(p-1)/2}$. Therefore,

$$\alpha(a,\ b,\ p) = \mu(a,\ b,\ p) = p - 1,$$

since this is the only divisor of $p - 1$ not dividing $(p - 1)/2$.

Unfortunately, again, it is not known if there are an infinite number of Mersenne or Fermat primes.

4. PRELIMINARY LEMMAS FOR THE GENERAL CASE

Theorems 1, 2, and 3 and the corollary to Theorem 1 are limited in that, for a specific PFLS, we do not know if there are an infinite number of primes having the required form to assure that these primes have maximal ranks of apparition or periods. What we intend to do is, instead of fixing the PFLS $u(a, b)$, we will fix the prime and ask if there are PFLS's for which the rank of apparition or period is a maximum. The answer is "yes" for both the cases $(D/p) = 1$ and $(D/p) = -1$, and there are an infinite number of PFLS's which satisfy this condition. More generally, given an odd prime p, we will vary over all PFLS's and investigate the possible values for the period, rank of apparition, exponent of the multiplier, and multiplier modulo p. In the first three cases, we shall see that there exist PFLS's reduced modulo p for which the function takes on a maximal value. Clearly, if we let the parameters a and b vary over all the integers rather than just the integers between 0 and $p - 1$, we will obtain an infinite number of PFLS's $u(a, b)$ with this property. We will now need the following four lemmas.

LEMMA 4: *Let p be an odd prime. Suppose that $p \nmid bD$. Let P be a prime ideal in $K = Q(\sqrt{D})$ dividing p. Consider the* PFLS $u(a, b)$.

(i) $\mu(a, b, p)$ *is the least common multiple of the exponents of* r_1 *and* r_2 modulo P.

(ii) $\alpha(a, b, p)$ *is the exponent of* r_1/r_2 modulo P. *This is also the least positive integer n such that* $r_1^n \equiv r_2^n \pmod{P}$. *If* $(D/p) = -1$, *then $\alpha(a, b, p)$ is also the least positive integer n such that r_1^n is congruent to a rational integer* modulo P.

(iii) *If* $k = \alpha(a, b, p)$, *then*

$$s(a, b, p) \equiv r_1^k \pmod{P}.$$

PROOF: Let R denote the integers of K. Since $b \not\equiv 0 \pmod{p}$, neither r_1 nor $r_2 \equiv 0 \pmod{P}$. Since R/P is a field of p or p^2 elements, $r_1/r_2 \pmod{P}$ is well-defined.

(i) Let $n = \mu(a, b, p)$. Then

$$u_n \equiv 0 \pmod{p} \equiv 0 \pmod{P}$$

and

$$u_{n+1} \equiv 1 \pmod{p} \equiv 1 \pmod{P}$$

by definition of $\mu(a, b, p)$. Since $D = (r_1 - r_2)^2 \not\equiv 0 \pmod{p}$,

$$u_n = (r_1^n - r_2^n)/(r_1 - r_2)$$

is well-defined modulo P. Since

$$(r_1^n - r_2^n)/(r_1 - r_2) \equiv 0 \pmod{P}, \ r_1^n \equiv r_2^n \pmod{P}.$$

Hence,

$$u_{n+1} \equiv (r_1^n(r_1) - r_1^n(r_2))/(r_1 - r_2) \equiv r_1^n \equiv 1 \pmod{P}.$$

Thus,

$$r_1^n \equiv r_2^n \equiv 1 \pmod{P}.$$

Conversely, if

$$r_1^k \equiv r_2^k \equiv 1 \pmod{P},$$

then it easily follows that $u_k \equiv 0 \pmod{p}$ and $u_{k+1} \equiv 1 \pmod{p}$. Assertion (i) now follows.

(ii) Now let $n = \alpha(a, b, p)$. Then

$$u_n = (r_1^n - r_2^n)/(r_1 - r_2) \equiv 0 \pmod{P}.$$

This occurs only if $r_1^n \equiv r_2^n \pmod{P}$. Dividing through by r_2^n, we obtain

$$(r_1/r_2)^n \equiv 1 \pmod{P},$$

and hence $\alpha(a, b, p)$ is the exponent of $r_1/r_2 \pmod{P}$. Further, if $(D/p) = -1$, let σ be the automorphism of the Galois field R/P of p^2 elements. Then

$$\sigma(r_1) = r_1^p \equiv r_2 \pmod{P}$$

and

$$\sigma(r_1^n) = (r_1^p)^n \equiv r_2^n \pmod{P}.$$

Thus, if $r_1^n \equiv r_2^n \pmod{P}$, we obtain $(r_1^n)^p \equiv r_1^n \pmod{P}$. Now, $R/P = Z_p[\sqrt{D}]$, where Z_p is the field with p elements. In $Z_p[\sqrt{D}]$, the only solutions of the equation

$$x^p - x = 0$$

are those in Z_p by Fermat's theorem. Consequently, the rest of assertion (ii) now follows.

(iii) Let $k = \alpha(a, b, p)$. Then

$$u_{k+1} \equiv s(a, b, p) \pmod{p} \equiv s(a, b, p) \pmod{P}.$$

By the proof of (ii), $r_1^k \equiv r_2^k \pmod{P}$. Thus,

$$u_{k+1} = (r_1^{k+1} - r_2^{k+1})/(r_1 - r_2) \equiv (r_1^k(r_1) - r_1^k(r_2))/(r_1 - r_2)$$
$$\equiv r_1^k \equiv s(a, b, p) \pmod{P}.$$

The proof is now complete.

<u>LEMMA 5</u>: *Let p be an odd prime. Let m be a residue* modulo p. *Then, given a fixed integer a, there exists a unique residue b* (mod p) *such that in the* PFLS $u(a, b)$, $(D/p) = 0$ *or* 1 *and* $r_1 \equiv m \pmod{p}$.

<u>PROOF</u>: We want

$$m \equiv (a + \sqrt{a^2 + 4b})/2 \pmod{p}.$$

Then

$$(2m - a)^2 \equiv a^2 + 4b \pmod{p}.$$

Solving for b, we see that $b \equiv m^2 - am \pmod{p}$ suffices. Note that if $m \equiv a/2 \pmod{p}$, then $r_1 \equiv r_2 \pmod{p}$ and $(D/p) = 0$.

<u>LEMMA 6</u>: *Let* $m \not\equiv 0$ (mod p) *be some residue* modulo p, *where p is an odd prime. Then, given a fixed integer b, where* $b \not\equiv 0$ (mod p), *there exists a unique residue a* (mod p) *such that in the* PFLS $u(a, b)$, $(D/p) = 0$ *or* 1 *and* $r_1 \equiv m \pmod{p}$.

<u>PROOF</u>: By the proof of Lemma 5, if such a residue a exists,

$$b \equiv m^2 - am \pmod{p}.$$

Solving for a, we obtain

$$a \equiv (m^2 - b)/m \pmod{p}.$$

Thus, such a residue a does exist. Note that if $m^2 \equiv -b \pmod{p}$, then

$$r_2 \equiv -b/m \equiv m \equiv r_1 \pmod{p}$$

and $(D/p) = 0$.

<u>LEMMA 7</u>: *Let m and n be a fixed pair of residues* modulo p *where p is an odd prime. Then there exists a unique* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 0$ *or* 1 *and* $r_1 \equiv m$, $r_2 \equiv n \pmod{p}$.

<u>PROOF</u>: Suppose that such a PFLS $u(a, b)$ does exist. Then $r_1 \equiv m$ and $r_2 \equiv n \pmod{p}$. Further, $r_1 + r_2 = a$. Moreover, $r_1 r_2 = -b$. Thus,

$$a \equiv m + n,\ b \equiv -mn \pmod{p}$$

suffice as the parameters of the PFLS $u(a, b)$. Note that if $m \equiv n \pmod{p}$, then $r_1 \equiv r_2 \pmod{p}$ and $(D/p) = 0$.

5. THE CASE $(D/p) = 1$

We are now ready to present our main results.

THEOREM 4: Let p be an odd prime and let $d \neq 1$ be a divisor of $p - 1$. Let $t(d)$ be the number of ways of expressing d as the least common multiple of the exponents of the nonzero residues m and n (mod p), *where* $m \not\equiv n$ (mod p). *Then there exist $t(d)$* PFLS's $u(a, b)$, *where* $0 \leqslant a \leqslant p - 1$ *and* $1 \leqslant b \leqslant p - 1$, *reduced* modulo p, *such that* $(D/p) = 1$ *and* $\mu(a, b, p) = d$. *In particular there exist $t(p - 1)$ reduced* PFLS's $u(a, b)$ *with a maximal period of* $p - 1$.

PROOF: First, by the corollary to Lemma 2, $\mu(a, b, p)$ is at most $p - 1$. By Lemma 4(i), $\mu(a, b, p)$ is the least common multiple of the exponents of r_1 and r_2 modulo p. By Lemma 7, for any pair of residues m and n, where $m \not\equiv n$ (mod p), we can find a PFLS $u(a, b)$ such that $r_1 \equiv m$ (mod p), $r_2 \equiv n$ (mod p), and $(D/p) = 1$. Since for any positive divisor d of $p - 1$ there exists a residue m such that $\text{ord}_p(m) = d$, the theorem follows.

THEOREM 5: Let p be an odd prime and let $d \neq 1$ be any positive divisor of $p - 1$. Then there exist exactly $(p - 1)/2 \cdot \phi(d)$ PFLS's $u(a, b)$ *reduced* modulo p *such that* $b \not\equiv 0$ (mod p), $(D/p) = 1$, *and* $\alpha(a, b, p) = d$. *In particular there exist $(p - 1)/2 \cdot \phi(p - 1)$ such* PFLS's *with a maximal rank of apparition of* $p - 1$.

PROOF: $\alpha(a, b, p) = d$ if and only if

$$u_d = (r_1^d - r_2^d)/(r_1 - r_2) \equiv 0 \pmod{p}$$

and $u_n \not\equiv 0$ (mod p) for any positive integer $n < d$. Let $r_2 \equiv gr_1$, where $g \not\equiv 1$ (mod p). Then $r_2^d \equiv g^d r_1^d$. Hence, $\alpha(a, b, p) = d$ if and only if g belongs to the exponent d modulo p. Note that neither r_1 nor $r_2 \equiv 0$ (mod p), since $b \not\equiv 0$ (mod p). Now there exist $\phi(d)$ residues belonging to the exponent d modulo p. Since r_1 can be any one of the $p - 1$ nonzero residues by Lemma 7, we have $(p - 1) \cdot \phi(d)$ ordered pairs of residues, $(r_1, r_2) \equiv (r_1, gr_1)$, such that the corresponding PFLS $u(a, b)$ has a rank of apparition of p equal to d.

We are really interested in the unordered pairs of solutions for r_1 and r_2, since r_1 and r_2 considered in any order determine the same PFLS. The ordered pairs (r_1, r_2) and (r_2, r_1) are equal as unordered pairs. Now, if $r_2 \equiv gr_1$, then $r_1 \equiv r_2/g$, where $g \not\equiv 0$ (mod p), since neither r_1 nor $r_2 \equiv 0$ (mod p). But if g belongs to the exponent d, so does $1/g$. Further, $r_1 \not\equiv r_2$ (mod p), since $(D/p) \neq 0$. Thus, exactly half of the $(p - 1) \cdot \phi(d)$ ordered pairs are equal as unordered pairs. The theorem now follows.

THEOREM 6: Let p be an odd prime. If $d | p - 1$ and $d \neq p - 1$, then there exists a PFLS $u(a, b)$ *reduced* modulo p *such that* $b \not\equiv 0$ (mod p), $(D/p) = 1$, *and* $\beta(a, b, p) = d$. *Further, if* $s \not\equiv 0$ (mod p) *is a fixed integer, then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $s(a, b, p) \equiv s$ (mod p).

PROOF: By Lemma 7, simply pick residues r_1 and r_2 modulo p such that

$$\text{ord}_p(r_1) = p - 1 \quad \text{and} \quad r_2 \equiv gr_1 \pmod{p},$$

where $\text{ord}_p(g) = (p - 1)/d$ and $g \not\equiv 1 \pmod{p}$. Hence, for the corresponding PFLS $u(a, b)$,

$$\mu(a, b, p) = [\text{ord}_p(r_1), \text{ord}_p(r_2)] = p - 1$$

by Lemma 4(i), where $[m, n]$ is the least common multiple of m and n. By the proof of Theorem 5,

$$\alpha(a, b, p) = (p - 1)/d.$$

Then

$$\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p) = d.$$

Now suppose that s is a fixed integer and the exponent of s modulo p is d. Then, by elementary number theory, there is a primitive root r_1 of p such that $r_1^{(p-1)/d} \equiv s \pmod{p}$. By the above proof, we can find an integer r_2 such that r_1 and r_2 are the characteristic roots of the PFLS $u(a, b)$ with

$$\mu(a, b, p) = p - 1 \quad \text{and} \quad \alpha(a, b, p) = (p - 1)/d = k.$$

Then

$$s(a, b, p) \equiv r^k \equiv s \pmod{p}$$

and we are done.

6. THE CASE $(D/p) = -1$

Theorems 7, 8, and 9 below will deal with those PFLS's $u(a, b)$ for which $(D/p) = -1$.

THEOREM 7: Let p be an odd prime. Suppose that $d \mid p^2 - 1$ but $d \nmid p - 1$. Then there exist exactly $(1/2)\phi(d)$ PFLS's $u(a, b)$ reduced modulo p *such that*

$$(D/p) = -1 \quad \text{and} \quad \mu(a, b, p) = d.$$

In particular, there exist exactly $(1/2)\phi(p^2 - 1)$ reduced PFLS's $u(a, b)$ *with a maximal period of $p^2 - 1$.*

PROOF: Look at $\text{GF}(p^2)$, the finite field of p^2 elements. Since the nonzero elements form a cyclic multiplicative group, there exist exactly $\phi(d)$ elements in this field belonging to the exponent d. Let r_1 be one of these elements. Let Z_p represent the field of p elements. Now, $r_1 \in \text{GF}(p^2)$ but $r_1 \notin Z_p$ by Fermat's Little Theorem, since the exponent of r_1 does not divide $p - 1$. So $Z_p[r_1] = \text{GF}(p^2)$. Thus, r_1 satisifes an irreducible polynomial of degree 2 over Z_p:

$$x^2 - ax - b = 0, \tag{5}$$

where $0 \leqslant a \leqslant p - 1$ and $1 \leqslant b \leqslant p - 1$. The other root of this polynomial is $\sigma(r_1) = r_1^p = r_2$. Then

$$r_1 = (a + \sqrt{a^2 + 4b})/2 \quad \text{and} \quad r_2 = (a - \sqrt{a^2 + 4b})/2$$

can be considered elements of $K = Q(\sqrt{a^2 + 4b})$. Let P denote a prime ideal of K dividing p. By assumption, both r_1 and r_2 belong to the exponent d in the field R/P of p^2 elements, since r_1 does and r_2 is automorphic to r_1. Hence, by Lemma 4(i), $\mu(a, b, p) = d$. Finally, it is clear that there exist exactly $(1/2)\phi(d)$ such PFLS's reduced modulo p, since each PFLS $u(a, b)$ is determined by r_1 and r_2.

<u>THEOREM 8:</u> *Let p be an odd prime. Suppose $d|p + 1$ and $d \neq 1$. Then, there exist* PFLS's *reduced* modulo p, *such that $(D/p) = -1$ and $\alpha(a, b, p) = d$. In particular, there exist* PFLS's *$u(a, b)$ with a maximal rank of apparition of p of $p + 1$.*

<u>PROOF:</u> First, find an element r_1 of $GF(p^2)$ such that r_1 belongs to the exponent $(p - 1)d$. Then r_1 is not a $(p - 1)$st root of unity and, hence, r_1 is not a member of the prime field Z_p. Thus, $GF(p^2) = Z_p[r_1]$. As in the proof of Theorem 7, we can consider r_1 an element of K. Let P be a prime ideal in K dividing p. Then

$$r_1^{(p-1)d} \equiv 1 \pmod{P}$$

and r_1^d is a $(p - 1)$st root of unity in R/P. Hence,

$$r_1^d \equiv z \pmod{P},$$

where z is a rational integer and $z \not\equiv 0 \pmod{p}$, since these are the only residue classes (mod P) that are $(p - 1)$st roots of unity.

Now, suppose that $r_1^n \equiv z' \pmod{p}$, where $0 < n < d$ and z' is a rational integer. Then

$$r_1^{n(p-1)} \equiv 1 \pmod{P}$$

and $n(p - 1) < (p - 1)d$. But this is a contradiction. Thus, d is the least positive integer such that $r_1^d \equiv z \pmod{P}$, where z is a rational integer. Hence, by Lemma 4(ii), $\alpha(a, b, p) = d$.

<u>THEOREM 9:</u> *Let p be an odd prime; also let $d|p - 1$. If p is not a Mersenne prime, then there exists a* PFLS *$u(a, b)$ reduced* modulo p *such that $(D/p) = -1$ and $\beta(a, b, p) = d$. If p is a Mersenne prime then there exists at least one* PFLS *$u(a, b)$ reduced* modulo p *such that $(D/p) = -1$ and $\beta(a, b, p) = d$ if and only if d is even. In any case, there exists a* PFLS *$u(a, b)$ with a maximal exponent of the multiplier* modulo p *of $p - 1$. Further, if $d|p - 1$ and there exists a* PFLS *$u(a, b)$ such that $\beta(a, b, p) = d$ and s is any integer whose exponent* modulo p *is d, then there exists a* PFLS *$u(a, b)$ such that $s(a, b, p) \equiv s \pmod{p}$.*

<u>PROOF:</u> Suppose that the period modulo p of a PFLS $u(a, b)$ is k, where

$$k \nmid p - 1,\ k|p^2 - 1, \text{ and } (D/p) = -1.$$

By the proof of Theorem 8, both r_1 and r_2 belong to the exponent k modulo P. It is clear that we can express k uniquely as the product of m and n, where m and n are positive integers, $m|p-1$, $n|p+1$, $n > 1$, and $(mn, p-1) = m$. We shall show that $n = \alpha(a, b, p)$ and $m = \beta(a, b, p)$.

By Lemma 4(ii), $\alpha(a, b, p)$ is the least positive integer c such that r_1^c is congruent to a rational integer modulo P. Now, n is such an integer, because r_1^n is an mth root of 1 in R/P and $m|p-1$. I claim that no smaller positive integer j suffices. If this were true, then

$$\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p) = mn/j$$

and mn/j must divide $p - 1$. Clearly,

$$mn/j \mid mn$$

also. But, since $j < n$, $mn/j > m$. However, m is the largest integer dividing both m and $p - 1$, so we have a contradiction. Thus, $\alpha(a, b, p) = n$ and $\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p) = m$.

Now suppose that p is not a Mersenne prime. Clearly, $(p-1, p+1) = 2$. Since p is not a Mersenne prime, $p + 1$ has a prime factor $h > 2$ such that $(h, p-1) = 1$. Let r_1 be any integer in R whose exponent (mod P) is dh. By the proof of Theorem 7, we can find a PFLS $u(a, b)$ such that $(D/p) = -1$, the characteristic roots r_1 and r_2 have exponent dh (mod P), and $\mu(a, b, p) = dh$. It is apparent that $(dh, p-1) = d$. By our above arguments in this proof, $\beta(a, b, p) = d$. Furthermore, among the $\phi(dh)$, such possibilities for r_1, r_1^h must be one of the $\phi(d)$ residues (mod P) whose expopent is d. Since $(d, h) = 1$, $\phi(dh) = \phi(d)\phi(h)$. Thus, it follows that for any fixed integer s with exponent d (mod p), there exist $\phi(h)$ residues r_1 (mod P) such that $r_1^h \equiv s$ (mod P). Then r_1 and $\sigma(r_1) = r_2$ are the characteristic roots of a unique PFLS $u(a, b)$ modulo p, where σ is the Frobenius automorphism of R/P. By Lemma 4-(iii),

$$r_1^h \equiv s(a, b, p) \equiv s \pmod{p}.$$

Now assume that p is a Mersenne prime. Then $p + 1$ is a power of 2 and $2|p-1$ but $4\nmid p-1$. If d is an even number, then by Theorem 7 we can find a PFLS $u(a, b)$ such that $(D/p) = -1$ and $\mu(a, b, p) = 2d$. It is easily seen that $(2d, p-1) = d$. By our above arguments, $\beta(a, b, p) = d$. Further, by using our arguments above, if s is a residue (mod p) whose exponent is d, then there exists a PFLS $u(a, b)$ such that $s(a, b, p) \equiv s$ (mod p). If d is an odd number, it is impossible to find positive integers h and k such that $dh = k$, $d|p-1$, $h|p+1$, $h > 1$, and $(dh, p-1) = d$. This is so because h must be a power of 2 greater than 1 and thus $(dh, p-1) = 2d$, not d. The theorem now follows.

7. THE CASE $(D/p) = 0$

Theorem 10 will explore the case in which $(D/p) = 0$. But first, we will need Lemma 8, which discusses the possibilities for $\mu(a, b, p)$, $\alpha(a, b, p)$, $\beta(a, b, p)$, and $s(a, b, p)$ for such PFLS's $u(a, b)$.

<u>*LEMMA 8:*</u> *In the* PFLS $u(a, b)$, *suppose* $p \nmid ab$, *but* $p \mid D$. *Let* $a' = a/2$. *Then*

$$\alpha(a, b, p) = p,$$
$$\mu(a, b, p) = p \cdot \mathrm{ord}_p(a'),$$
$$s(a, b, p) \equiv a' \pmod{p},$$

and

$$\beta(a, b, p) = \mathrm{ord}_p(a').$$

<u>*PROOF:*</u> The fact that $\alpha(a, b, p) = p$ follows from Lemma 2. The rest of the theorem follows from definition of the terms and the fact that

$$s(a, b, p) \equiv r_1^p \equiv (a/2)^p \equiv (a/2) \pmod{p}.$$

<u>*THEOREM 10:*</u> *Let* p *be an odd prime.*

(i) *There exist exactly* $p - 1$ PFLS's $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 0$, $b \not\equiv 0 \pmod{p}$, *and* $\alpha(a, b, p) = p$.

(ii) *If* $d \mid p - 1$, *then there exist exactly* $\phi(d)$ PFLS's $u(a, b)$ *reduced* modulo p *such that* $\beta(a, b, p) = d$ *and* $\mu(a, b, p) = dp$. *If* s *is any integer such that the exponent of* $s \pmod{p}$ *is* d, *then there exists exactly one of these* $\phi(d)$ PFLS's $u(a, b)$ *reduced* modulo p *such that* $s(a, b, p) \equiv s \pmod{p}$.

<u>*PROOF:*</u> (i) $\alpha(a, b, p) = p$ if and only if $a^2 + 4b \equiv 0 \pmod{p}$. Given a nonzero residue a, there is a unique nonzero residue b such that $a^2 + 4b \equiv 0 \pmod{p}$. Assertion (i) now easily follows from Lemma 8 and Lemma 7.

(ii) By Lemma 8, $s(a, b, p) \equiv a/2 \pmod{p}$. The result now easily follows from Lemma 7.

8. THE CASE FOR WHICH b IS A FIXED INTEGER

By Lemma 3, one might suspect that the parameter b might play a large part in determining the divisibility properties of the PFLS $u(a, b)$. The following two well-known identities add further credence to this suspicion, since they depend only on the parameter b.

$$u_n^2 - u_{n-1}u_{n+1} = (-b)^{n-1}. \tag{6}$$

$$u_{m+n} = bu_m u_{n-1} + u_n u_{m+1}. \tag{7}$$

Both (6) and (7) can be proved from the Binet formulas or by induction. So, given a fixed value of b, we should be able to develop some conclusions concerning the possible periods and ranks of apparition of PFLS's $u(a, b)$ with respect to a given odd prime p. In particular, we have the following three theorems.

THEOREM 11: Suppose that p is an odd prime and b is any integer such that $b \not\equiv 0 \pmod{p}$. If $\mu(a, b, p) = d$, then $\mathrm{ord}_p(-b) | d$ for any PFLS $u(a, b)$ *such that $(D/p) = 1$. Let $d \neq 1$ be any integer such that $d | p - 1$ and $\mathrm{ord}_p(-b) | d$. Further, suppose that it is not the case that both $b \equiv 1 \pmod{p}$ and $d = 4$ or both $b \equiv -1 \pmod{p}$ and $d = 2$. Then there exists at least one* PFLS $u(a, b)$ *reduced* modulo p *such that $\mu(a, b, p) = d$ and $(D/p) = 1$. If $b \equiv 1 \pmod{p}$ and $d = 4$ or $b \equiv -1 \pmod{p}$ and $d = 2$, then no such* PFLS $u(a, b)$ *exists. In particular, if $\mathrm{ord}_p(-b) = p - 1$, then there exists at least one* PFLS $u(a, b)$ *with a maximal period* modulo p.

PROOF: Firstly, we shall show that if $u(a, b)$ is a PFLS such that $(D/p) = 1$ and $\mu(a, b, p) = d$, then $\mathrm{ord}_p(-b) | d$. Note that $-b = r_1 r_2$ and $d = [\mathrm{ord}_p(r_1), \mathrm{ord}_p(r_2)]$ by Lemma 4(i). Thus, it follows that

$$(-b)^d = r_1^d r_2^d \equiv 1 \cdot 1 \equiv 1 \pmod{p}.$$

Thus, $\mathrm{ord}_p(-b) | d$. Next, note that if $(D/p) = 1$, then $r_1 \not\equiv r_2 \pmod{p}$. Since $r_2 = -b/r_1$, $r_1 \equiv r_2 \pmod{p}$ if and only if $r_1^2 \equiv -b \pmod{p}$.

If $d \neq 2, 3, 4$, or 6, then $\phi(d) \geqslant 4$. Consequently, we can then choose a residue r_1 modulo p such that $\mathrm{ord}_p(r_1) = d$ and $r_1^2 \not\equiv -b \pmod{p}$, since there are $\phi(d)$ residues $n \pmod{p}$ such that $\mathrm{ord}_p(n) = d$ and at most two residues $m \pmod{p}$ such that $m^2 \equiv -b \pmod{p}$. Then

$$r_2^d \equiv (-b/r_1)^d \equiv 1 \pmod{p},$$

since $\mathrm{ord}_p(-b) | d$. Hence, $\mathrm{ord}_p(r_2) | \mathrm{ord}_p(r_1)$ and

$$[\mathrm{ord}_p(r_1), \mathrm{ord}_p(r_2)] = d.$$

By Lemma 4(i), $\mu(a, b, p) = d$ for the PFLS $u(a, b)$ corresponding to r_1 and $r_2 \pmod{p}$. By Lemma 6, we can find a PFLS $u(a, b)$ such that its characteristic root r_1 indeed satisfies the conditions that $\mathrm{ord}_p(r_1) = d$ and $r_1^2 \not\equiv -b \pmod{p}$.

Now suppose that $d = 2, 3, 4$, or 6 and we can choose a residue $r_1 \pmod{p}$ such that $\mathrm{ord}_p(r_1) = d$ and $r_1^2 \not\equiv -b \pmod{p}$. Then, by our previous argument, $\mu(a, b, p) = d$.

If $d = 2$ and $r_1^2 \equiv -b \pmod{p}$ for all choices of r_1 such that $\mathrm{ord}_p(r_1) = 2$, then $-b \equiv 1 \pmod{p}$. However, this case is excluded by hypothesis.

If $d = 3$ and $r_1^2 \equiv -b \pmod{p}$ for all choices of r_1 such that $\mathrm{ord}_p(r_1) = 3$, then $\mathrm{ord}_p(-b) = 3$. Now, choose $r_1 \equiv 1 \pmod{p}$. Then

$$r_2 \equiv -b/r_1 \equiv -b \pmod{p}.$$

By Lemma 4(i), $\mu(a, b, p) = 3$.

If $d = 4$ and $r_1^2 \equiv -b \pmod{p}$ for all choices of r_1 such that $\mathrm{ord}_p(r_1) = 4$, then $-b \equiv -1 \pmod{p}$. But this case is excluded by hypothesis.

If $d = 6$ and $r_1 \equiv -b \pmod{p}$ for all choices of r_1 such that $\text{ord}_p(r_1) = 6$, then $\text{ord}_p(-b) = 3$. In this case, choose $r_1 \equiv -1 \pmod{p}$. Then $r_2 \equiv -b/-1 \equiv b \pmod{p}$. Clearly then, $\text{ord}_p(b) = 6$. By Lemma 4(i), $\mu(a, b, p) = 6$.

Now suppose that $b \equiv 1 \pmod{p}$ and $d = 4$. Then $\{u_n\}$ modulo p is of the form

$$u_0 \equiv 0,\ u_1 \equiv 1,\ u_2 \equiv a,\ u_3 \equiv a^2 + 1,$$

$$u_4 \equiv a^3 + 2a \equiv 0,\ u_5 \equiv a^2 + 1,\ \ldots .$$

Since $a^2 + 1 \equiv 1 \pmod{p}$, then $a \equiv 0 \pmod{p}$. But then, $\mu(a, b, p) = 2$ and not 4. Thus, $\mu(a, 1, p)$ can never be 4.

If $b \equiv -1 \pmod{p}$ and $d = 2$, then $\{u_n\}$ modulo p is of the form

$$u_0 \equiv 0,\ u_1 \equiv 1,\ u_2 \equiv 0,\ u_3 \equiv -u_1 \equiv 1,\ \ldots .$$

But it is clearly impossible for u_3 to be both congruent to -1 and 1 if p is an odd prime. Thus, $\mu(a, -1, p)$ never equals 2.

<u>*THEOREM 12:*</u> *Let p be an odd prime, and let b be any integer such that $b \not\equiv 0 \pmod{p}$.*

(i) *If $(-b/p) = 1$, then there exists a* PFLS *$u(a, b)$ reduced* modulo *p such that $(D/p) = 1$ and $\alpha(a, b, p) = d$ if and only if $d \mid (p - 1)/2$, where $d \neq 1$.*

(ii) *If $(-b/p) = -1$, then there exists a* PFLS *$u(a, b)$ reduced* modulo *p such that $(D/p) = 1$ and $\alpha(a, b, p) = d$ if and only if $d \mid p - 1$ and $d \nmid (p - 1)/2$.*

<u>*PROOF:*</u> (i) Firstly, $\alpha(a, b, p)$ can never equal 1, since $u_1 = 1$. Now, suppose that we have found a PFLS $u(a, b)$ such that $\alpha(a, b, p) = d$, where $d \neq 1$ is a positive integer dividing $p - 1$ and $(-b/p) = 1$. Then

$$r_2 = -b/r_1 \equiv gr_1 \pmod{p}$$

for some nonzero residue $g \not\equiv 1 \pmod{p}$. This leads to the congruence

$$r_1^2 \equiv -b/g \pmod{p}. \tag{8}$$

If $\alpha(a, b, p) = d$, then by Lemma 4(ii), d is the least positive integer such that $r_1^d \equiv r_2^d \pmod{p}$. Consequently, $\text{ord}_p(g) = d$. Since $(-b/p) = 1$, congruence (8) is solvable if and only if $(g/p) = 1$. But since $\text{ord}_p(g) = d$, $(g/p) = 1$ if and only if

$$d \mid (p - 1)/2.$$

By Lemma 6, we can now choose r_1 such that

$$r_1^2 \equiv -b/g \pmod{p},$$

where $\operatorname{ord}_p(g) = d$. Assertion (i) now follows.

(ii) This proof is similar to the proof of (i).

Before presenting Theorem 13, we will need Lemma 9, which is due to Wyler [8].

<u>*LEMMA 9 (Wyler):*</u> *Consider the* PFLS $u(a, b)$. *Suppose* $b \not\equiv 0 \pmod{p}$, *and let* $h = \operatorname{ord}_p(-b)$. *Suppose* $h = 2^c h'$, *where* h' *is an odd integer. Let*

$$k = \alpha(a, b, p) = 2^j k',$$

where k' *is an odd integer. Let* H *be the least common multiple of* h *and* k.

(i) $\mu(a, b, p) = H$ *or* $2H$; $\beta(a, b, p) = H/k$ *or* $2H/k$.

(ii) *If* $c \neq j$, *then* $\mu(a, b, p) = 2H$.
If $c = j > 0$, *then* $\mu(a, b, p) = H$.

<u>*THEOREM 13:*</u> *Let* p *be an odd prime of the form* $2^m q + 1$, *where* q *is an odd integer. Let* b *be a fixed integer such that* $b \not\equiv 0 \pmod{p}$. *Let* $h = \operatorname{ord}_p(-b) = 2^c h'$, *where* h' *is an odd integer.*

(i) *If* a *is an integer, then* $\beta(a, b, p) \mid 2h$ *for the* PFLS $u(a, b)$.

(ii) *If* $(-b/p) = -1$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d \mid h'$.

(iii) *If* $(-b/p) = 1$, $h' \neq q$, *and either* $c = 0$ *or* $c < m - 1$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $B(a, b, p) = d$ *if and only if* $d \mid 2h$.

(iv) *If* $(-b/p) = 1$, $m \geq 2$, $c = m - 1$, *and* $h' \neq q$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d \mid 2h$ *and* $d \not\equiv 2 \pmod{4}$.

(v) *If* $(-b/p) = 1$, $m = 1$, *and* $h = q$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d \mid 2h$ *and* $h \nmid d$.

(vi) *If* $(-b/p) = 1$, $m \geq 2$, *and* $h = q$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d \mid 2h$ *and* $d \neq h$.

(vii) *If* $(-b/p) = 1$, $m = 2$, *and* $h = 2q$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d \mid 2h$, $d \not\equiv 2 \pmod{4}$, *and* $h \nmid d$.

(viii) *If* $(-b/p) = 1$, $m \geqslant 3$, $1 \leqslant c < m - 1$, *and* $h' = q$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d|2h$ *and* $d \neq 2h$.

(ix) *If* $(-b/p) = 1$, $m \geqslant 3$, $c = m - 1$, *and* $h' = q$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d|2h$, $d \not\equiv 2 \pmod 4$, *and* $d \neq 2h$.

(x) *If there exists a* PFLS $u(a, b)$ *such that* $\beta(a, b, p) = d$ *and* s *is an integer such that* $\text{ord}_p(s) = d$, *then there exists a* PFLS $u(a, b)$ *such that* $s(a, b, p) \equiv s \pmod p$.

<u>*PROOF:*</u> (i) Let $k = \alpha(a, b, p)$. By the definition of $s(a, b, p)$ and (6),

$$s^2 = u_{k+1}^2 = u_{k+1}^2 - 0 \equiv u_{k+1}^2 - u_k u_{k+2} \equiv (-b)^k \pmod p.$$

Thus,

$$s^{2h} \equiv (-b)^{kh} \equiv ((-b)^h)^k \equiv 1 \equiv 1 \pmod p$$

and $\text{ord}_p(s)$, which is equal to $\beta(a, b, p)$, divides $2h$.

(ii) Note that $(-b/p) = -1$ implies that $c = m$. Since $(-b/p) = -1$, it follows from Theorem 12(ii) that for any PFLS $u(a, b)$ such that $(D/p) = 1$, $\alpha(a, b, p) \nmid (p - 1)/2$, but $\alpha(a, b, p)|p - 1$. Thus,

$$2^m|\alpha(a, b, p).$$

By Theorem 11, $h = 2^c h' | \mu(a, b, p)$. Since $\alpha(a, b, p)|\mu(a, b, p)$, $\mu(a, b, p)|p - 1$, and $\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p)$, it follows that $\beta(a, b, p)$ is an odd integer. By part (i),

$$\beta(a, b, p)|2h.$$

Thus,

$$\beta(a, b, p)|h'.$$

Now suppose that $d|h'$. We wish to choose a residue r_1 such that

$$r_1^2 \equiv (-b)^{d+1} \pmod p. \tag{9}$$

One solution for r_1 is $(-b)^{(d+1)/2}$, since $d + 1$ is even. By Lemma 6, we can find a PFLS $u(a, b)$ whose characteristic root r_1 satisfies congruence (9). Now,

$$r_2 = -b/r_1 \equiv (-b)^{(1-d)/2} \pmod p.$$

Since $(d + 1)/2$ and $(1 - d)/2$ are relatively prime to each other and to h',

$$[\text{ord}_p(r_1), \text{ord}_p(r_2)] = \text{ord}_p(-b) = 2^c h'.$$

Thus, by Lemma 4(i), $\mu(a, b, p) = 2^c h'$. By Lemma 4(ii),

$$\alpha(a, b, p) = \mathrm{ord}_p(r_1/r_2) = \mathrm{ord}_p\big((-b)^{(d+1)/2}/(-b)^{(1-d)/2}\big)$$
$$= \mathrm{ord}_p\big((-b)^d\big) = 2^c h'/d.$$

Thus

$$\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p) = d.$$

(iii) It follows from part (i) that if $\beta(a, b, p) = d$, then $d|2h$. If $d|2h$ and d is odd, then by the same argument as in the proof of part (ii), one can find a PFLS $u(a, b)$ such that $(D/p) = 1$,

$$\mu(a, b, p) = \mathrm{ord}_p(-b),\ \alpha(a, b, p) = \mathrm{ord}_p(-b)/d,$$

and

$$\beta(a, b, p) = d.$$

Now suppose that $c = 0$, $d|2h$, and $d \equiv 2 \pmod 4$. By what was stated above in this proof, we can find a PFLS $u(a, b)$ such that $(D/p) = 1$,

$$\mu(a, b, p) = h,\ \alpha(a, b, p) = h/(\tfrac{1}{2}d),$$

and

$$\beta(a, b, p) = d/2,$$

since $d/2$ is odd. Note that

$$\mu(a, b, p),\ \alpha(a, b, p),\ \text{and}\ \beta(a, b, p)$$

are all odd. Since $\mu(a, b, p)$ is odd, $\mathrm{ord}_p\big(s(a, b, p)\big)$ is odd, and no power of $s(a, b, p)$ is congruent to -1 modulo p. Let $k = \alpha(a, b, p)$ and $s \equiv s(a, b, p) \pmod p$. Note that $u_{k+1} \equiv s \pmod p$ and $u_{gk+1} \equiv s^g \pmod p$, where g is a positive integer. One can easily verify that for the PFLS $u(a, b)$,

$$u_n(-a, b) = (-1)^{n-1}u_n(a, b).$$

It is clear that $\alpha(a, b, p) = \alpha(-a, b, p)$. Let $k' = \alpha(-a, b, p) = k$ and $s' = s(-a, b, p)$. Then $\mu(-a, b, p) = gk'$ for some positive integer g and

$$u_{gk'+1}(-a, b) \equiv (s')^g \equiv (-1)^{gk'}u_{gk'+1}(a, b)$$
$$\equiv (-1)^{gk}s^g \equiv 1 \pmod p.$$

Since $s^g \not\equiv -1 \pmod p$ and $\mathrm{ord}_p(s) = d/2$, it follows that

$$g = \mathrm{ord}_p(s') = d$$

and that $\beta(-a, b, p) = d$.

Now suppose that $c > 0$, $4|d$, and $d|2h$. Choose a residue n such that $n^2 \equiv -b \pmod{p}$. This is possible because $m > c$ and $h'|q$ imply that

$$(-b)^{(p-1)/2} \equiv (-b)^{2^{m-1}q} \equiv 1 \pmod{p}.$$

By Lemma 6, we can find a PFLS $u(a, b)$ whose characteristic root r_1 satisfies

$$r_1^2 \equiv n^{d+2} \pmod{p}.$$

One solution for r_1 is $n^{(d/2)+1}$, since d is even. Then

$$r_2 \equiv -b/r_1 \equiv n^{2-((d/2)+1)} \equiv n^{1-(d/2)} \pmod{p}.$$

Since $1 + (d/2) = -(1 - (d/2)) + 2$, the greatest common divisor of $1 + (d/2)$ and $1 - (d/2)$ must divide 2. Since $d/2$ is even, it follows that $1 + (d/2)$ and $1 - (d/2)$ are both odd, and thus relatively prime. Furthermore, $1 + (d/2)$ and $1 - (d/2)$ are both relatively prime to $\text{ord}_p(n)$, which is equal to $2h$. Thus,

$$\mu(a, b, p) = [\text{ord}_p(r_1), \text{ord}_p(r_2)] = \text{ord}_p(n) = 2h.$$

Further,

$$\alpha(a, b, p) = \text{ord}_p(r_1/r_2) = \text{ord}_p(n^{1+(d/2)}/n^{1-(d/2)})$$
$$= \text{ord}_p(n^d) = 2h/d.$$

Thus,

$$\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p) = d.$$

Finally, suppose that $c > 0$, $d|2h$, and $d \equiv 2 \pmod{4}$. Choose a residue f such that $f^4 \equiv -b \pmod{p}$. This is possible, since $c < m - 1$ and $h'|q$ imply that

$$(-b)^{(p-1)/4} \equiv (-b)^{2^{m-2}q} \equiv 1 \pmod{p}.$$

Note that $\text{ord}_p(f)|4h$. By Lemma 6, we can find a PFLS $u(a, b)$ whose characteristic root r_1 satisfies

$$r_1^2 \equiv f^{d+4} \pmod{p}.$$

One solution for r_1 is $f^{(d/2)+2}$, since d is even. Then

$$r_1 = -b/r_1 \equiv f^{4-((d/2)+2)} \equiv f^{2-(d/2)} \pmod{p}.$$

Since $2 + (d/2) = -(2 - (d/2)) + 4$, the greatest common divisor of $2 + (d/2)$ and $2 - (d/2)$ must divide 4. Since $d \equiv 2 \pmod{4}$, $d/2$ is odd. Consequently, $2 - (d/2)$ and $2 + (d/2)$ are both odd and therefore both are relatively prime to $4h$, since $d|2h$. Thus,

$$\mu(a,\, b,\, p) = [\mathrm{ord}_p(r_1),\, \mathrm{ord}_p(r_2)] = \mathrm{ord}_p(f).$$

Further,

$$\alpha(a,\, b,\, p) = \mathrm{ord}_p(r_1/r_2) = \mathrm{ord}_p(f^{2+(d/2)}/f^{2-(d/2)})$$
$$= \mathrm{ord}_p(f^d) = 4 \cdot \mathrm{ord}_p(f)/d.$$

Hence,

$$\beta(a,\, b,\, p) = \mu(a,\, b,\, p)/\alpha(a,\, b,\, p) = d.$$

(iv) Suppose that there exists a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\beta(a, b, p) = d$, where $d \mid 2h$ and $d \equiv 2 \pmod 4$. Further, suppose $2^{m-1} \| \alpha(a, b, p)$, where $2^k \| n$ means that $2^k \mid n$ but $2^{k+1} \nmid n$. Then, by Lemma 9, $\mu(a, b, p) = H$, where

$$H = [\mathrm{ord}_p(-b),\, \alpha(a,\, b,\, p)].$$

Thus,

$$2^{m-1} \| \mu(a,\, b,\, p) \quad \text{and} \quad 2^0 \| \beta(a,\, b,\, p),$$

which is a contradiction. Now suppose that $2^e \| \alpha(a, b, p)$ where $e \leqslant m - 2$. Then by Lemma 9, $\mu(a, b, p) = 2H$ and $4 \mid \beta(a, b, p)$, which again is a contradiction. Now suppose that $2^m \| \alpha(a, b, p)$. Then by Lemma 9, $\mu(a, b, p) = 2H$ and $2^{m+1} \| \mu(a, b, p)$. This contradicts the fact that $(D/p) = 1$, which implies $\mu(a, b, p) \mid p - 1$. Therefore, $\beta(a, b, p) \not\equiv 2 \pmod 4$ for any PFLS $u(a, b)$ such that $(D/p) = 1$. The rest of this proof is similar to the proofs of parts (ii) and (iii).

(v) Suppose that there exists a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\beta(a, b, p) = q$ or $\beta(a, b, p) = 2q$. If $f \mid \alpha(a, b, p)$, where $f \mid q$ and $f > 1$, then by Lemma 9, $\mu(a, b, p) = H$ or $2H$, and q/f is the largest odd divisor of $\beta(a, b, p)$. This contradicts the fact that $q \mid \beta(a, b, p)$. Further, $\alpha(a, b, p) \neq 1$. Thus, $\alpha(a, b, p) = 2$. In this case, $\mu(a, b, p) = 2H$ by Lemma 9, and $4 \mid \mu(a, b, p)$. However, this contradicts the fact that $(D/p) = 1$, which implies $\mu(a, b, p) \mid p - 1$. Thus, $q \nmid \beta(a, b, p)$. The rest of the proof is similar to the proofs of parts (ii) and (iii).

(vi) We shall exhibit a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\beta(a, b, p) = 2q$. By Theorem 12(i), we can find a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\alpha(a, b, p) = 2$, since $m \geqslant 2$ and thus $2 \mid (p - 1)/2$. By Lemma 9, $\mu(a, b, p) = 2H = 4q$, which divides $p - 1$. Hence, $\beta(a, b, p) = 2q$. The rest of the proof is similar to proofs of parts (ii), (iii), and (iv).

(vii) We shall exhibit a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\beta(a, b, p) = q$. By Theorem 12(i), we can find a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\alpha(a, b, p) = 2$. By Lemma 9, $\mu(a, b, p) = H = 2q$

$\beta(a, b, p) = q$. The rest of the proof is similar to proofs of parts (ii)-(v).

(viii) We shall exhibit a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\beta(a, b, p) = 2^e q$, where $0 \leqslant e \leqslant c$. If $1 < e \leqslant c$, then by Theorem 12(i) we can find a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\alpha(a, b, p) = 2^{c-e+1}$, since $2^{c-e+1} | (p - 1)/2$. By Lemma 9, $\mu(a, b, p) = 2H = 2^{c+1}q$ and $\beta(a, b, p) = 2^e q$. If $e = 1$, then by Theorem 12(i) we can find a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\alpha(a, b, p) = 2^{c+1}$, since $2^{c+1} | (p-1)/2$. By Lemma 9, $\mu(a, b, p) = 2H = 2^{c+2}q$ and $\mu(a, b, p) | p - 1$, which is consistent with $(D/p) = 1$. It follows that $\beta(a, b, p) = 2q$. If $e = 0$, then by Theorem 12(i) we can find a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\alpha(a, b, p) = 2^c$. By Lemma 9, $\mu(a, b, p) = H = 2^c q$ and $\beta(a, b, p) = q$. The rest of the proof is similar to proofs of parts (ii), (iii), and (v).

(ix) This proof is similar to proofs of parts (ii)-(v) and (viii).

(x) This proof is similar to that of Theorem 6.

9. THE CASE FOR WHICH a IS A FIXED INTEGER

I am unable to obtain such definitive results given the parameter a as were obtained given the parameter b. The reason is that $r_1 r_2 = -b$, while $r_1 + r_2 = a$, and it is frequently easier to obtain multiplicative results in number theory than additive results. We now present two theorems, Theorems 14 and 15. Theorem 14 is complete, while Theorem 15 is not as comprehensive as the corresponding result in the preceding section.

<u>*THEOREM 14:*</u> *Let p be an odd prime and let a be any fixed integer. If $a \equiv 0 \pmod p$, then for any integer b such that $b \not\equiv 0 \pmod p$, $\alpha(a, b, p) = 2$. If $a \not\equiv 0 \pmod p$, $d | p - 1$, and $d \nmid 2$, then there exists a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\alpha(a, b, p) = d$.*

<u>*PROOF:*</u> If $a \equiv 0 \pmod p$ and $b \not\equiv 0 \pmod p$, it is obvious that $\alpha(a, b, p) = 2$. Suppose that $a \not\equiv 0 \pmod p$, $d | p - 1$, and $d \nmid 2$. Let s be an integer such that $\text{ord}_p(s) = d$. We wish to find residues r_1 and r_2 that satisfy the simultaneous congruences

$$\begin{aligned} r_1 + r_2 &\equiv a \pmod p \\ r_1/r_2 &\equiv s \pmod p \end{aligned} \tag{10}$$

which lead to the simultaneous congruences

$$\begin{aligned} r_1 + r_2 &\equiv a \pmod p \\ r_1 - r_2 s &\equiv 0 \pmod p. \end{aligned} \tag{11}$$

By Cramer's rule, if $a \not\equiv 0 \pmod{p}$, then (11) is solvable if and only if

$$-r_1r_2s - r_1r_2 \not\equiv 0 \pmod{p}.$$

Now, $-r_1r_2s - r_1r_2 \equiv 0 \pmod{p}$ if and only if $s \equiv -1 \pmod{p}$, which implies that $d = 2$. However, this case is ruled out by hypothesis. Thus, (10) is solvable. Now, by Lemma 7, we can find a PFLS $u(a, b)$ such that $r_1 + r_2 \equiv a \pmod{p}$ and $r_1/r_2 \equiv s \pmod{p}$. Then

$$\alpha(a, b, p) = \text{ord}_p(r_1/r_2) = \text{ord}_p(s) = d$$

and we are done.

<u>*THEOREM 15:*</u> *Let p be an odd prime and a be any integer. Look at the collection*

$$a - 1,\ a - 2,\ a - 3,\ \ldots,\ a - (p - 1).$$

Then there exists a PFLS $u(a, b)$ *such that* $b \not\equiv 0 \pmod{p}$, $(D/p) = 1$, *and* $\mu(a, b, p) = m$, *where m is any of the numbers*

$$[\text{ord}_p(a - r_i),\ \text{ord}_p(r_i)],\quad 1 \leqslant r_i \leqslant p - 1,\ r_i \not\equiv a/2 \pmod{p}.$$

In particular, if $p > 3$, then, given any integer a, there exist at least $(\phi(p-1))/2$ PFLS's $u(a, b)$ *reduced* modulo p *such that* $b \not\equiv 0 \pmod{p}$, $(D/p) = 1$, *and $u(a, b)$ has a maximal period* modulo p *of* $p - 1$.

<u>*PROOF:*</u> This follows from the fact that $r_1 + r_2 = a$ and from Lemmas 4(i) and 7. Note that by hypothesis, $r_1 \not\equiv r_2 \pmod{p}$, which is satisfied if and only if $r_1 \not\equiv a/2 \pmod{p}$. The last assertion follows from the fact that there are $\phi(p - 1)$ residues modulo p belonging to the exponent $p - 1$. Excluding the residue $a/2$ modulo p leaves at least $\phi(p - 1) - 1$ residues remaining with a maximal exponent of $p - 1$. Since $p > 3$, $\phi(p - 1) - 1$ is a positive odd integer. Since a PFLS $u(a, b)$ might have both its characteristic roots r_1 and r_2 with exponents of $p - 1$, these residues correspond to at least

$$(\phi(p - 1) - 2)/2 + 1$$

distinct PFLS's $u(a, b)$ modulo p. The result now follows.

The reason I was not able to obtain a more definitive result for Theorem 15 was that for a PFLS $u(a, b)$, $\mu(a, b, p)$ is determined by

$$[\text{ord}_p(r_1),\ \text{ord}_p(r_2)],\ \text{where } r_1 + r_2 = a.$$

However, I was not able to find any clear relationship between the exponents of r_1 and $a - r_1$ modulo p, which limited the scope of the theorem.

ACKNOWLEDGMENT

I wish to express my appreciation to Professor Harald Niederreiter for suggestions leading to the improvement of Theorem 14.

REFERENCES

1. Robert P. Backstrom. "On the Determination of the Zeros of the Fibonacci Sequence." *The Fibonacci Quarterly* 4, No. 4 (Dec. 1966):313-322.
2. R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n + \beta^n$." *Ann. Math.* Second Series, 15 (1913):30-70.
3. Marshall Hall. "Divisors of Second-Order Sequences." *Bull. Amer. Math. Soc.* 43 (1937):78-80.
4. John H. Halton. "On the Divisibility Properties of Fibonacci Numbers." *The Fibonacci Quarterly* 4, No. 3 (Oct. 1966):217-240.
5. D. H. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. Math.* Second Series, 31 (1930):419-488.
6. Lawrence Somer. "Fibonacci-Like Groups and Periods of Fibonacci-Like Sequences." *The Fibonacci Quarterly* 15, No. 1 (Feb. 1977):35-41.
7. Morgan Ward. "Note on the Period of a Mark in a Finite Field." *Bull. Amer. Math. Soc.* 40 (1934):279-281.
8. Oswald Wyler. "On Second-Order Recurrences." *Amer. Math. Monthly* 72 (1965):500-506.

*****

ON A CONVOLUTION PRODUCT FOR THE TRANSFORM WHICH MAPS DERIVATIVES INTO DIFFERENCES

MIOMIR S. STANKOVIĆ
Braće Taskovića 17/29, 18 000 NIŠ, Yugoslavija

INTRODUCTION

In [1] we defined a linear transform with the property that derivatives are mapped into differences in the following way:

$$V\{f(x)\} = (v_n) = \left(\frac{d^n}{dx^n} e^x f(x)\Big|_{x=0}\right), \text{ i.e., } v_n = \sum_{i=0}^{n} \binom{n}{i} f^{(i)}(0). \tag{1}$$

Its inverse E transform considered in [2] is defined by:

$$E(e_n) = f(x) = \sum_{i=0}^{+\infty} \frac{\Delta^i e_0}{i!} x^i, \text{ i.e., } f(x) = e^{-x} \sum_{i=0}^{+\infty} \frac{e_i}{i!} x^i, \tag{2}$$

where $\Delta e_n = e_{n+1} - e_n$, $\Delta^k e_n = \Delta(\Delta^{k-1} e_n)$ $(k = 0, 1, \ldots)$.

The linear two-dimensional R transform and its inverse, the I transform, with the property that the partial derivatives are mapped into partial differences are defined in [3] by:

$$R\{f(x, y)\} = (r_{m,n}) = \left(\frac{\partial^{m+n}}{\partial x^m \partial y^n} e^{x+y} f(x, y)\Big|_{\substack{x=0\\y=0}}\right), \tag{3}$$

$$I(i_{m,n}) = f(x, y) = \sum_{i=0}^{+\infty} \sum_{j=0}^{+\infty} \frac{\Delta_m^i \Delta_n^j i_{0,0}}{i!j!} x^i y^j, \tag{4}$$

where

$$\Delta_m i_{m,n} = i_{m+1,n} - i_{m,n}, \ \Delta_m^k i_{m,n} = \Delta_m(\Delta_m^{k-1} i_{m,n}),$$

$$\Delta_n i_{m,n} = i_{m,n+1} - i_{m,n}, \ \Delta_n^k i_{m,n} = \Delta_n(\Delta_n^{k-1} i_{m,n}) \ (k = 0, 1, \ldots).$$

In this paper, we give an extension of the results obtained in [1], [2], and [3]. Having the transform at hand, we proceed to determine a convolution for E and I transforms. Also, we will apply this product to solve some discrete equations by establishing analogies between these equations and corresponding continuous equations. At the end of this paper, we will show the practical use of the described transform for obtaining some combinatorial identities. We use the notation introduced in [1].

1. A CONVOLUTION PRODUCT FOR E AND I TRANSFORMS

Let $C^\infty(R)$ be the set of real functions having continuous derivatives of all orders. Furthermore, let $S_f \subset C^\infty(R)$ be the set where $f \in S_f$ if and only if there exist constants α, $M > 0$ such that $|f^{(k)}(0)| < \alpha M^k$, for every $k \in N_0$, and let S_v be the set of all real sequences where $(v_n) \in S_v$ if and only if there exist constants β, $N > 0$ and $|\Delta^k v_0| < \beta N^k$ for every $k \in N_0$.

DEFINITION 1: Let (v_n), $(w_n) \in S_v$. The convolution product of sequences (v_n) and (w_n) is given by

$$v_n * w_n = \sum_{i=0}^{n} \sum_{j=0}^{i} (-1)^{n-i} \binom{n}{i} \binom{i}{j} v_j w_{i-j}. \tag{5}$$

It is easy to see that the convolution product can be defined by

$$v_n * w_n = \sum_{i=0}^{n} \sum_{j=0}^{i} \binom{n}{i} \binom{i}{j} \Delta^j v_0 \Delta^{i-j} w_0. \tag{6}$$

If (u_n), (v_n), $(w_n) \in S_v$, then the following properties of convolution product can readily be established:

(a) $c * v_n = cv_n$ (c constant),

(b) $u_n * v_n = v_n * u_n$,

(c) $u_n * (v_n + w_n) = u_n * v_n + u_n * w_n$,

(d) $\Delta^k u_n * v_n = \sum_{i=0}^{k} \binom{k}{i} \Delta^i u_n * \Delta^{k-i} v_n$.

THEOREM 1: (a) *If $f(x) \in S_f$, then $Vf \in S_v$,*

(b) *If $(e_n) \in S_v$, then $E(e_n) \in S_f$,*

(c) *If (u_n), $(v_n) \in S_v$, then $(u_n * v_n) \in S_v$.*

PROOF: (a) By (1), we conclude that

$$|\Delta^k v_0| = |f^{(k)}(0)| < \alpha M^k,$$

and we have that $Vf \in S_v$.

(b) By (2), we conclude that

$$|f^{(k)}(0)| = |\Delta^k e_0| < \beta N^k,$$

and we have that $E(e_n) \in S_f$.

(c) Since (u_n), $(v_n) \in S_v$, it follows that there exist β_1, β_2, N_1, $N_2 > 0$ such that

$$|\Delta^k u_0| < \beta_1 N_1^k \quad \text{and} \quad |\Delta^k v_0| < \beta_2 N_2^k.$$

Using (6), we conclude that

$$\left|\Delta^k (u_n * v_n)\big|_{n=0}\right| < \beta_1\beta_2(N_1 + N_2)^k,$$

which means that $u_n * v_n$ given by (5) or (6) belongs to S_v.

<u>THEOREM 2</u>: *Let* (v_n), $(w_n) \in S_v$. *The relation*

$$E(v_n * w_n) = E(v_n)E(w_n) \tag{7}$$

is satisfied if and only if $v_n * w_n$ *is defined by* (6).

<u>PROOF</u>: If (7) is satisfied, then we will have

$$\Delta^i (v_n * w_n)\Big|_{n=0} = \sum_{j=0}^{i} \binom{i}{j} \Delta^j v_0 \Delta^{i-j} w_0,$$

and hence follows (6). Conversely, if (6) is satisfied, then (7) will follow by elementary series manipulations.

Let $Vf = (v_n)$ and $Vg = (u_n)$. Then by (7) we easily conclude that

$$V\{f(x)g(x)\} = \sum_{i=0}^{n} \sum_{j=0}^{i} (-1)^{n-i} \binom{n}{i}\binom{i}{j} u_j v_{i-j},$$
$$\text{i.e., } V\{f(x)g(x)\} = (u_n * v_n). \tag{8}$$

Now we consider an extension of the result obtained for V and E transforms to two-dimensional R and I transforms defined by (3) and (4). Theorems for R and I transforms are proved analogously and we omit the proofs here.

Let $C^\infty(R^2)$ be the set of real functions having continuous partial derivatives of all orders with respect to both variables. Also, let $S_f^2 \subset C^\infty(R^2)$ be the set where $f \in S_f^2$ if and only if there exist constants $\alpha, M, N > 0$ such that

$$\left|\frac{\partial^{i+j}}{\partial x^i \partial y^j} f(0, 0)\right| < \alpha M^i N^j,$$

and S_v^2 be the set of real sequences where $(v_{m,n}) \in S_v^2$ if and only if there exist constants β, P, Q and $|\Delta_m^i \Delta_n^j v_{0,0}| < \beta P^i Q^j$ for every i, $j \in N_0$.

<u>DEFINITION 2</u>: Let $(v_{m,n})$, $(w_{m,n}) \in S_v^2$. The convolution product of the sequences $(v_{m,n})$ and $(w_{m,n})$ is given by

$$v_{m,n} * w_{m,n} = \sum_{i=0}^{m} \sum_{j=0}^{n} \sum_{p=0}^{i} \sum_{q=0}^{j} (-1)^{m+n-i-j} \binom{m}{i}\binom{n}{j}\binom{i}{p}\binom{j}{q} v_{p,q} w_{i-p,j-q}.$$

It is easy to see that the convolution product can be defined by

$$v_{m,n} * w_{m,n} = \sum_{i=0}^{m} \sum_{j=0}^{n} \sum_{p=0}^{i} \sum_{q=0}^{j} \binom{m}{i}\binom{n}{j}\binom{i}{p}\binom{j}{q} \Delta_m^p \Delta_n^q v_{0,0} \Delta_m^{i-p} \Delta_n^{j-q} w_{0,0}. \tag{9}$$

THEOREM 3: (a) *If* $f(x, y) \in S_f^2$, *then* $R\{f(x, y)\} \in S_v^2$,

(b) *If* $(i_{m,n}) \in S_v^2$, *then* $I(i_{m,n}) \in S_f^2$,

(c) *If* $(i_{m,n}), (r_{m,n}) \in S_v^2$, *then* $(i_{m,n} * r_{m,n}) \in S_v^2$.

THEOREM 4: *Let* $(i_{m,n}), (r_{m,n}) \in S_v^2$. *The relation*

$$I(i_{m,n} * r_{m,n}) = I(i_{m,n}) I(r_{m,n}) \tag{10}$$

is satisfied if and only if $i_{m,n} * r_{m,n}$ *is defined by* (9).

Let $R\{f(x, y)\} = (r_{m,n})$ and $Rf(x, y) = (s_{m,n})$. Then by (10) we easily conclude that

$$R\{f(x, y)g(x, y)\} = (r_{m,n} * s_{m,n}). \tag{11}$$

2. SOME APPLICATIONS

2.1 Difference Equations

In this section, we will give some applications of the V, R and its inverse transform in solving some difference and partial difference equations.

From (8) and (11), using the orthogonality relation of the binomial coefficients, we obtain the following relations:

$$V\left\{x^k \frac{d^p f(x)}{dx^p}\right\} = (n^{(k)} \Delta^p v_{n-k})$$

and

$$R\left\{x^k y^k \frac{\partial^{i+j} f(x, y)}{\partial x^i \partial y^j}\right\} = (m^{(k)} n^{(p)} \Delta_m^i \Delta_n^j r_{m-k,n-p}).$$

These relations show that the V and R transform maps linear differential equations with polynomial coefficients to linear difference equations with polynomial coefficients, too. The above correspondence may provide a useful method for solving difference equations with polynomial coefficients because the resulting differential equation is often easier to solve.

2.1.1. By an application of the V transform we conclude that the difference equation which corresponds to the following differential equation

$$(a_1x^2 + b_1x + c_1)y'' + (a_2x^2 + b_2x + c_2)y' + (a_3x^2 + b_3x + c_3)y = 0 \quad (12)$$

is given by

$$\begin{aligned} c_1v_{n+2} + (b_1n - 2c_1 + c_2)v_{n+1} + (a_1n(n-1) + (b_2 - 2b_1)n + c_1 - c_2 + c_3)v_n \\ + n((a_2 - 2a_1)(n-1) + b_1 - b_2 + b_3)v_{n-1} \\ + n(n-1)(a_1 - a_2 + a_3)v_{n-2} = 0. \quad (13) \end{aligned}$$

Equation (13) is a second-order difference equation in one of the following three cases:

1. $b_1 = 0$, $c_1 = c_2 = 0$;
2. $a_1 = a_3$, $a_2 = 2a_1$, $b_1 + b_3 = b_2$;
3. $c_1 = 0$, $a_1 + a_3 = a_2$.

Notice that Equation (12) contains some differential equations of special functions as Legendre's, Laguerre's, Chebyshev's, Hermite's, etc. For example, by an application of V and E transforms to Laguerre and Bessel differential equations and their solutions, we find that the solutions of difference equations

$$(n+1)v_{n+1} + (m - 3n - 1)v_n + 2nv_{n-1} = 0$$

and

$$(n^2 - m^2)v_n - n(2n-1)v_{n-1} + n(n-1)v_{n-2} = 0$$

are given by

$$v_n = m!\sum_{k=0}^{m}(-1)^k\binom{m}{k}\binom{n}{k},$$

and

$$v_n = \sum_{k=0}^{n}\binom{n}{k}\frac{(-1)^k}{\pi}\int_0^{\pi}\cos\left(mt + \frac{k\pi}{2}\right)\sin^k t\, dt.$$

2.1.2. By an application of the V transform to the equation

$$(e^x + 1)y' + e^x y = 2ae^{ax} \quad (a \in R) \quad (14)$$

we get the equation

$$v_{n+1} - v_n + \sum_{i=0}^{n}\binom{n}{i}v_{i+1} = 2a(1+a)^n. \quad (15)$$

Since a particular solution of (14), given by

$$y = \frac{2e^{ax}}{e^x + 1}$$

belongs to S_f, we have that a particular solution of (15) is given by

$$v_n = E_n(a+1),$$

where $E_n(a+1)$ are Euler's polynomials.

2.1.3. By an application of the V transform to the equation

$$y'' - y' = 2 \sin x,\ y(0) = 2,\ y'(0) = 0 \tag{16}$$

we get the equation

$$v_{n+2} - 3v_{n+1} + 2v_n = 2^{(n/2)+1} \sin\left(n \frac{\pi}{4}\right),\ v_0 = 2,\ v_1 = 2. \tag{17}$$

Since the solution of (16), given by

$$y = e^x + \cos x - \sin x$$

belongs to S_f, we have that the solution of (17) is given by

$$v_n = 2^n + 2^{n/2} \cos\left(n \frac{\pi}{4}\right) - 2^{n/2} \sin\left(n \frac{\pi}{4}\right).$$

2.1.4. The transforms V_1 and E_1, defined by

$$V_1\{f(x)\} = (v_n) = \left(\frac{d^n}{dx^n} e^{x-x_0} f(x)\bigg|_{x=x_0}\right)$$

and

$$E_1(e_n) = f(x) = \sum_{k=0}^{+\infty} \frac{\Delta^k v_0}{k!}(x - x_0)^k$$

have analogous properties to the V and E transforms.

By an application of the E_1 transform to

$$\Delta^m v_n + a_1 \Delta^{m-1} v_n + \cdots + a_m v_n = e_n \quad (a_i \in R,\ i = 1, 2, \ldots, m) \tag{18}$$

we get the equation

$$y^{(m)}(x) + a_1 y^{(m-1)}(x) + \cdots + a_m y(x) = f(x), \tag{19}$$

where $f(x) = E(e_n)$.

In paper [4] (see also [5]), Cauchy obtained that the general solution of Equation (19) is given by

$$y = \sum \operatorname{Res}\left(\frac{f(z)}{g(z)} e^{zx}\right) + \sum \operatorname{Res}\left(\frac{e^{zx}}{g(z)} \int_{x_0}^{x} e^{-zt} f(t)\,dt\right),$$

where $f(z)$ is an arbitrary regular function whose zeros do not coincide with zeros of the polynomial $g(z) = z^m + a_1 z^{m-1} + \cdots + a_m$. The summation is taken over all the singularities of the function

$$\frac{f(z)}{g(z)} e^{zx},$$

i.e., over all the zeros of the polynomial $g(z)$.

Since $y(x) \in S_f$, then by an application of the V_1 transform and using the convolution product, i.e., using (8), we have that the solution of linear difference equations (18) is given by

$$v_n = \sum \operatorname{Res} \frac{f(z)}{g(z)}(1 + z)^n + \sum \operatorname{Res}\left((1 + z)^{n-1} \sum_{k=0}^{n-1}(1 + z)^{-k} f_k\right).$$

Notice that B. Tortolini [6] (see also [5]) obtained this result in another way.

2.1.5. By an application of the V transform to the following recurrence relations for Laguerre and Gegenbauer polynomials

$$(m + 1)L_{m+1}^{(\alpha)}(x) - (x - 2m - \alpha - 1)L_m^{(\alpha)}(x) + (m + \alpha)L_{m-1}^{(\alpha)}(x) = 0$$

and

$$(m + 1)G_{m+1}^{(\alpha)}(x) - 2(m + \alpha)xG_m^{(\alpha)}(x) + (m + 2\alpha - 1)G_{m-1}^{(\alpha)}(x) = 0$$

we get that particular solutions of equations

$$(m + 1)v_{m+1,n} - (2m + \alpha - 1)v_{m,n} + (m + \alpha)v_{m-1,n} + nv_{m,n-1} = 0$$

and

$$(m + 1)v_{m+1,n} + (m + 2\alpha - 1)v_{m-1,n} - 2(m + \alpha)nv_{m,n-1} = 0$$

are given, respectively, by

$$v_{m,n} = \sum_{i=0}^{\min(m,n)} (-1)^i \binom{m + \alpha}{m - i}\binom{n}{i} \qquad (\alpha > -1)$$

and

$$v_{m,n} = \frac{1}{\Gamma(\alpha)} \sum_{i=0}^{[m/2]} (-1)^i \frac{2^{m-2i}\Gamma(m + \alpha - i)}{i!}\binom{n}{m - 2i} \quad \left(\alpha > -\frac{1}{2}, \alpha \neq 0\right).$$

2.1.6. By an application of the I transform to the equation

$$Ar_{m+1,n} + Br_{m,n+1} + (C - A - B)r_{m,n} = 0 \quad (A, B, C \in R) \tag{20}$$

we get the equation

$$Af_x + Bf_y + Cf = 0. \tag{21}$$

Since the general solution of Equation (21), given by

$$f = e^{-(C/A)x} f(Bx - Ay),\ A \neq 0;\ f = e^{-(C/B)y} f(x),\ A = 0,\ B \neq 0,$$

where f is an arbitrary function, belongs to S_f^2, we have, by application of the R transform and the convolution product, i.e., using (11), that the general solution of (20) is given by

$$r_{m,n} = \left(1 - \frac{C}{A}\right)^m \sum_{i=0}^{m} \sum_{j=0}^{n} (-1)^j A^j \binom{m}{i} \binom{n}{j} \left(\frac{AB}{A - C}\right)^i a_{i+j} \qquad (A \neq 0,\ A \neq C)$$

$$r_{m,n} = B^m \sum_{i=0}^{n} (-1)^i A^i \binom{n}{i} a_{m+i} \qquad (A \neq 0,\ A = C)$$

$$r_{m,n} = \left(1 - \frac{C}{B}\right)^n a_m \qquad (A = 0,\ B \neq 0)$$

where in all cases a_m is an arbitrary sequence. Compare this with the solutions given by Kečkić [7].

2.1.7. By an application of the I transform to the equation

$$r_{m+1,\,n+1} - 3r_{m+1,\,n} - 4r_{m,\,n+1} + 12r_{m,\,n} = 2^{m+n+1}, \tag{22}$$

we get the equation

$$f_{xy} - 2f_x - 3f_y + 6f = 2e^{x+y}. \tag{23}$$

Since the general solution of Equation (23), given by

$$f(x,\ y) = (a(x) + b(y))e^{3x+2y} + e^{x+y},$$

where $a(x)$ and $b(y)$ are arbitrary functions, belongs to S_f^2, we have, by an application of the R transform, that the general solution of (22) is given by

$$r_{m,\,n} = (a_m + b_n) * 4^m 3^n + 2^{m+n},$$

where a_m and b_n are arbitrary sequences.

2.2 Combinatorial Identities

Now we will show that the described transform is very useful for obtaining some combinatorial identities.

Applying the V transform to both sides of relations

$$\sum_{i=0}^{k} L_i^{\alpha}(x) = L_k^{\alpha+1}(x)$$

and

$$\sum_{i=0}^{k} (-1)^i \binom{k}{i} L_i(x) = \frac{x^k}{k!},$$

where $L_i^{\alpha}(x)$ are Laguerre polynomials defined by

$$L_i^\alpha(x) = \sum_{j=0}^{i} (-1)^j \binom{i+\alpha}{i-j}\frac{x^j}{j!},$$

we can easily obtain the following combinatorial identities:

$$\sum_{i=0}^{k} \sum_{j=0}^{\min(n,i)} (-1)^j \binom{i+\alpha}{i-j}\binom{n}{j} = \sum_{j=0}^{\min(n,k)} (-1)^j \binom{n}{j}\binom{k+\alpha+1}{k-j};$$

$$\sum_{i=0}^{k} \sum_{j=0}^{\min(n,i)} (-1)^{i+j} \binom{k}{i}\binom{i}{j}\binom{n}{j} = \binom{n}{k}.$$

Similarly, by application of the R transform to the relations

$$\sum_{i=0}^{k} (-1)^i \binom{k}{i}(x+y)^{k-i}y^i = x^k$$

and

$$\sum_{i=0}^{k} \binom{k}{i}(2y)^i H_{k-i}(x) = H_k(x+y),$$

where $H_i(x)$ are Hermite polynomials defined by

$$H_i(x) = \sum_{j=0}^{[i/2]} \frac{(-1)^j i!}{j!(i-2j)!}(2x)^{i-2j},$$

we have the following combinatorial identities:

$$\sum_{i=0}^{\min(n,k)} (-1)^i \binom{n}{i}\binom{m+n-1}{k-i} = \binom{m}{n};$$

$$\sum_{i=0}^{\min(n,k)} \sum_{j=0}^{\left[\frac{k-i}{2}\right]} \frac{(-1)^j}{4^j j!}\binom{n}{i}\binom{m}{k-i-2j} = \sum_{j=0}^{[k/2]} \frac{(-1)^j}{4^j j!}\binom{m+n}{k-2j}$$

REFERENCES

1. B. Danković & M. Stanković. "A Transformation Which Maps Derivatives into Differences." *Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz.* No. 634-677 (1979):214-220.
2. M. Stanković. "A Transform Which Maps Differences into Derivatives." *Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz.* (1980):132-134.
3. B. Danković & M. Stanković. "A Transformation Which Maps Partial Derivatives into Partial Differences." *Publ. Inst. Math. Beograd.* (in press).
4. A. Cauchy. "Application du calcul des résidus a l'intégration des équations differentialles linéaires et a coefficients constants: Exercises de mathématiques. Paris, 1826. *Oeuvres* (2) 6 (1887):252-255.
5. D. Mitrinović & J. Kečkić. *Cauchyjev račun ostataka sa primenama.* Beograd, 1978.

6. B. Tortolini. "Trattato del calcolo dei residui." *Giornale Arcad.* 63 (1834-1835):86-138.
7. J. Kečkić. "Analogies between Differential and Difference Equations with Constant Coefficients." *Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz.* No. 634-677 (1979):192-196.

*****

LETTER TO THE EDITOR

A NOTE ON THE GEOMETRY OF THE GREAT PYRAMID

The information in James M. Suttenfield, Jr., "A New Series," *The Fibonacci Quarterly* 16, no. 4 (August 1978):335-343, may be misleading to those who have never studied the geometry of the Great Pyramid.

Mr. Suttenfield apparently used information in recent literature to suggest geometry for the Great Pyramid which is different from well-known theories. Mr. Suttenfield's dimensions yield an angle between a face plane and the base plane:

$$\beta = \arctan \frac{\pi}{2\sqrt{\phi}} = 50°59'58.9'' \quad (\phi = \text{golden number})$$

An error analysis using eight sets of angle data from W. M. F. Petrie, *The Pyramids and Temples of Gizeh* (Longon: Field & Tauer, 1883), yields an average of his mean angles of 51°50'03.25". Considering his uncertainties, the standard deviation (1σ) about the mean is ±02'59.155". A more narrow window of ±01'29.375" can be found by taking the averages of his minimum and maximum angles due to the uncertainties.

The theory that the perimeter of the pyramid divided by twice its vertical height is the value of π gives an angle of 51°51'14.3" which is just inside the upper limit of the more narrow range of uncertainty. The theory that the slant height divided by one-half the basewidth gives the golden number yields an angle of 51°49'38.25", and this is just short of the average mean angle from Petrie's data. Mr. Suttenfield's theory yields an angle that is short of the mean by 50'04.35", and this is far outside the range of uncertainties in the survey data.

Elmer D. Robinson
JHU Applied Physics Laboratory
Laurel, MD 20180

*****

EULERIAN NUMBERS AND THE UNIT CUBE

DOUGLAS HENSLEY
Texas A & M University, College Station, TX 77843
(Submitted April 1981)

1. INTRODUCTION

There is an excellent expository paper [3] on Eulerian numbers and polynomials, and we begin with a quotation from it: "Following Euler [5] we may put

$$\frac{1-\lambda}{e^x-\lambda} = \sum_{n=0}^{\infty} H_n \frac{x^n}{n!} \qquad (\lambda \neq 1), \tag{1.1}$$

where $H_n = H_n(\lambda)$ is a rational function of λ; indeed

$$R_n = R_n(\lambda) = (\lambda - 1)^n H_n(\lambda) \tag{1.2}$$

is a polynomial in λ of degree $n - 1$ with integral coefficients. If we put

$$R_n = \sum_{k=1}^{n} A_{nk}\lambda^{k-1} \qquad (n \geqslant 1), \tag{1.3}$$

then the first few values of A_{nk} are given by the following table, where n denotes the row and k the column;

$$\begin{array}{cccccc} 1 & & & & & \\ 1 & 1 & & & & \\ 1 & 4 & 1 & & & \\ 1 & 11 & 11 & 1 & & \\ 1 & 26 & 66 & 26 & 1 & \\ 1 & 57 & 302 & 302 & 57 & 1 \end{array} \tag{1.4}$$

Alternatively, Worpitzky showed that the A_{nk} may be defined by means of

$$x_n = \sum_{k=1}^{n} A_{nk}\binom{x+k-1}{n}." \tag{1.5}$$

The numbers A_{nk} occur in connection with Bernoulli numbers and polynomials [11], and splines [10], and as the number of permutations of $(1, 2, \ldots, n)$ with k *rises*. [A permutation $(a_1, \ldots, a_n)$ has a rise at a_i if $a_i < a_{i+1}$; by convention, there is a rise to the left of a_1.] The A_{nk} satisfy a recursion and are symmetric:

$$A_{n+1,k} = kA_{n,k} + (n-k+1)A_{n,k-1} \tag{1.6}$$

and

$$A_{n,k} = A_{n,n-k+1} \qquad (1 \leqslant k \leqslant n).$$

From (1.6), it follows that

$$\sum_{k=1}^{n} A_k = n! \qquad (n \geqslant 1).$$

We now consider the unit cube $Q_n : 0 \leqslant x_i \leqslant 1$ $(1 \leqslant i \leqslant n)$, with the usual measure. It is evident from elementary calculations and from observation of (1.4) that, for $n = 2, 3$, or 4 and $1 \leqslant k \leqslant n$, the volume V_{nk} of the section

$$k - 1 \leqslant \sum_{i=1}^{n} x_i \leqslant k$$

of the unit cube is given by $V_{nk} = A_{nk}/n!$. This observation led Hillman (in a private communication with this author) to conjecture that, generally,

$$V_{nk} = A_{nk}/n!$$

He was right.

2. APPLICATIONS

In the notation of Section 1, we have

THEOREM 1: *For $1 \leqslant k \leqslant n$, we have $V_{nk} = A_{nk}/n!$* (2.1)

The proof is not difficult, but we defer that to the last. What is nice about this is that the unit cube is the natural probability space for a sum of n independent random variables X_i $(1 \leqslant i \leqslant n)$ identically and uniformly distributed on $[0, 1]$. Thus, we may reinterpret (2.1) to read:

$$\text{For } 1 \leqslant k \leqslant n, \ \text{Prob}\left(k - 1 \leqslant \sum_{1}^{n} X_i \leqslant k\right) = A_{nk}/n! \tag{2.2}$$

Through this interpretation, the central limit theorem and related results can be brought to bear on the asymptotic behavior of the Eulerian numbers.

For instance, the variance of each X_i is

$$\int_0^1 (x - 1/2)^2 dx = 1/12.$$

Thus the variance of $\sum_{1}^{n} X_i$ is $n/12$. Now, by the central limit theorem, if x is fixed and

$$\omega_n = (n/12)^{1/2}x + \frac{1}{2}n,$$

then

$$\lim_{n\to\infty} \text{Prob}\left(\sum_1^n X_i \leqslant \omega_n\right) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt. \tag{2.3}$$

Since the probability density function $f_n(t)$ of $\sum_1^n X_i$ tends to zero uniformly in t as $n \to \infty$, we can replace ω_n with $[\omega_n]$ in (2.3). Then, from (2.2), we have

$$\lim_{n\to\infty} \sum_{k=1}^{[\omega_n]} A_{nk}/n! = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt. \tag{2.4}$$

This is equivalent to Theorem 1 of [4]. It may be that this approach permits a simpler proof or an improvement in the error term in the other theorem of [4], which states that

$$(1/n!)A_{n,[\omega_n]} = (6/n\pi)^{1/2}\exp\left(-\frac{1}{2}x^2\right) + 0(n^{-3/4}). \tag{2.5}$$

From a geometric point of view, one important property of the cube is that it is convex. The Brunn-Minkowski theorem states that the area $A(t)$ of the intersection of a hyperplane $H(t)$ with equation

$$\sum_1^n c_i x_i = t$$

with a convex body Q in real n-space has a concave nth root on the interval where it is positive. Thus, if $H_n(t)$ has equation

$$\sum_1^n x_i = t$$

and $A_n(t)$ is the area of $H_n(t) \cap Q_n$ (where Q_n is still the unit cube $0 \leqslant x_i \leqslant 1$, $1 \leqslant i \leqslant n$), then $(A_n(t))^{1/n}$ is concave on $(0, n)$. Consequently,

$$\log A_n(t) \text{ is concave on } (0, n). \tag{2.6}$$

There is a simple relation between $A_n(t)$ and the probability density function $f_n(t)$ of $\sum_1^n X_i$:

$$A_n(t) = \sqrt{n}f_n(t).$$

(See, e.g., [6].)

Now let V_{nk} be the volume of Q_n between $H(k - 1)$ and $H(k)$. Then,

$$V_{nk} = n^{-1/2}\int_{k-1}^{k} A_n(t)dt = \int_{k-1}^{k} f_n(t)dt. \tag{2.7}$$

There is a considerable literature on logarithmic concavity. A function $g(t)$ is called *log-concave* if $g(t) \geqslant 0$ on $\mathbf{R}$ and is positive on just one interval, and if $\log g(t)$ is concave on that interval. A very special case of a theorem due to Prekopa says that if $f(t)$ is log-concave, then

$$F(x) = \int_{x-c}^{x} f(t)\,dt$$

is also log-concave [2, 8, 9]. In particular,

$$V(x) = n^{-1/2}\int_{x-c}^{x} A(t)\,dt$$

is log-concave, and in most particular,

$$V_{n,\,k-1}V_{n,\,k+1} \leqslant V_{n,\,k}^2, \tag{2.8}$$

or what is the same thing,

$$A_{n,\,k-1}A_{n,\,k+1} \leqslant A_{n,\,k}^2. \tag{2.9}$$

This is due to Kurtz, who proved strict inequality in (2.9) when $1 \leqslant k \leqslant n$.

3. PROOF OF THEOREM 1

The probability density functions $f_n(t)$ for $\sum_1^n X_i$ can be generated recursively starting with

$$f_1(t) = \begin{cases} 1 & \text{if } 0 \leqslant t \leqslant 1 \\ 0 & \text{otherwise} \end{cases}$$

and using

$$f_{n+1}(t) = f_n(t) * f_1(t) = \int_0^t f_n(u)f_1(t-u)\,du = \int_{t-1}^{t} f_n(u)\,du. \tag{3.1}$$

Thus,

$$V_{nk} = \int_{k-1}^{k} f_n(t)\,dt = f_{n+1}(k). \tag{3.2}$$

It follows from (1.5) (but not trivially) that

$$A_{nk} = \sum_{j=0}^{k-1} (-1)^j \binom{n+1}{j} (k-j)^n. \tag{3.3}$$

This is (2.15) of [3] and is due to Euler. Thus, we can prove Theorem 1 by showing that

$$f_{n+1}(k) = \frac{1}{n!}\sum_{j=0}^{k-1} (-1)^j \binom{n+1}{j} (k-j)^n. \tag{3.4}$$

Now, $f_{n+1}(t)$ is the convolution of $n+1$ copies of $f_1(t)$, so its Laplace transform is

$$F(s) = \left(\frac{1}{s}(1-e^{-s})\right)^{n+1}. \tag{3.5}$$

(See, e.g., [1].) Expanding (3.5) by the binomial theorem gives

$$F(s) = (1/s)^{n+1}\sum_{j=0}^{n+1}(-1)^j\binom{n+1}{j}e^{-sj},$$

and the inverse Laplace transform of the sum of these $n+2$ terms computes to

$$f_{n+1}(t) = \sum_{j=0}^{n+1}\frac{1}{n!}(-1)^j\binom{n+1}{j}(t-j)_+^n, \tag{3.6}$$

where $(t-j)_+$ is 0 for $t < j$ and $t - j$ for $t \geqslant j$. With $t = k$, (3.6) reduces to (3.4). □

REFERENCES

1. W. Boyce & R. DiPrima. *Elementary Differential Equations and Boundary Value Problems*, Chap. 6. New York: John Wiley & Sons, 1977.
2. H. Brascamp & E. Lieb. "On Extensions of the Brunn-Minkowski and Prekopa-Leindler Theorems, Including Inequalities for Log Concave Functions, and With an Application to the Diffusion Equation." *J. Func. Anal.* 22 (1976):366-389.
3. L. Carlitz. "Eulerian Numbers and Polynomials." *Math. Mag.* 33 (1959): 247-260.
4. L. Carlitz, D. Kurtz, R. Scoville, & O. Stackelberg. "Asymptotic Properties of Eulerian Numbers." *Z. Wahrscheinlichkeitstheorie verw. Geb.* 23 (1972):47-54.
5. L. Euler. "Institutiones Calculi Differentialis." *Omnia Opera* (1), 10 (1913).
6. D. Hensley. "Slicing the Cube in $\mathbf{R}^n$ and Probability (Bounds for the Measure of a Central Cube Slice in $\mathbf{R}^n$ by Probability Methods)." *Proc. Am. Math. Soc.* 73, No. 1 (1979):95-100.
7. A. Hillman, P. Mana, & C. McAbee. "A Symmetric Substitute for Stirling Numbers." *The Fibonacci Quarterly* 9, no. 1 (1979):51-60, 73.
8. A. Prekopa. "On Logarithmic Concave Measures and Functions." *Acta Sci. Math.* (Szeged) 34 (1973):335-343.
9. Y. Rinott. "On Convexity of Measures." *The Annals of Probability* 4, No. 6 (1976):1020-1026.
10. I. Schoenberg. "Cardinal Spline Interpolation and the Exponential Euler Splines." *Lecture Notes in Math.*, No. 399 (New York: Springer, 1973): 477-489.
11. H. Vandiver. "An Arithmetical Theory of the Bernoulli Numbers." *Trans. Am. Math. Soc.* 51:502-531.

★★★★★

ON A SYSTEM OF DIOPHANTINE EQUATIONS CONCERNING THE POLYGONAL NUMBERS

SHIRO ANDO
Hosei University, Koganei, Tokyo 184 Japan
(Submitted May 1981)

1. INTRODUCTION

For the integer k ($k \geqslant 3$) and the natural number n, we call the integer

$$P_{n,k} = \frac{1}{2}\{(k-2)n^2 - (k-4)n\}$$

the nth polygonal number of order k. If $k = 3$, this number is called the nth triangular number and is denoted by t_n.

Wieckowski [1] showed that the system of Diophantine equations

$$\begin{aligned} t_x + t_y &= t_u \\ t_x + t_z &= t_v \\ t_y + t_z &= t_w \end{aligned}$$

has infinitely many solutions. It seems difficult to establish the counterpart of this theorem for general polygonal numbers.

In this paper it will be shown that the system of Diophantine equations

$$\begin{aligned} P_{x,k} + P_{y,k} &= P_{u,k} \\ P_{x,k} + P_{z,k} &= P_{v,k} \end{aligned}$$

has infinitely many solutions for any integer k ($k \geqslant 3$). In other words, there are infinitely many polygonal numbers of order k which can be represented in two different ways as the difference of polygonal numbers of order k.

To show this, we establish a stronger theorem in a manner similar to that used earlier in [2].

THEOREM: Let a and b be integers such that $a > 0$ and $a \equiv b \pmod 2$, and let

$$A_n = \frac{1}{2}(an^2 + bn) \qquad (n = 1, 2, 3, \ldots).$$

There are an infinite number of A_n's which can be expressed in two different ways as the difference of numbers of the same type.

2. PROOF OF THE THEOREM

First, we prove the following lemma.

LEMMA: The equation

$$A_\ell = A_m - A_n \tag{1}$$

is satisfied by the positive integers

$$\ell = (ra + 1)s \tag{2}$$

$$m = n + s = \frac{1}{2}\{(r^2a^2 + 2ra + 2)s + rb\} \tag{3}$$

$$n = \frac{1}{2}\{ra(ra + 2)s + rb\} \tag{4}$$

where r is any positive integer and s is any sufficiently large positive integer that is odd if both a and r are odd.

PROOF: From (1), we have

$$\ell(a\ell + b) = (m - n)(am + an + b).$$

Therefore, the integers ℓ, m, and n which satisfy the relations

$$\ell = c(m - n),$$

and

$$a\ell + b = \frac{1}{c}(am + an + b),$$

for any possible constant c, give a solution of (1). Solving for m and n, we have

$$m = \frac{1}{2}\left\{\frac{\ell}{c} + c\ell + \frac{b}{a}(c - 1)\right\} = \frac{1}{2}\{(ra + 1)^2 s + s + rb\}$$

$$n = \frac{1}{2}\left\{-\frac{\ell}{c} + c\ell + \frac{b}{a}(c - 1)\right\} = \frac{1}{2}\{(ra + 1)^2 s - s + rb\},$$

where $\ell = cs$, and $c = ra + 1$ are the defining equations for r and s. Equations (2), (3), and (4) follow immediately.

By observing Equation (4) and recalling that $a \equiv b \pmod 2$, we see that if r is any positive integer and s is any integer that is odd if both a and r are odd, which also satisfies

$$s > \max\left\{0, -\frac{b}{a(ra + 2)}\right\},$$

then ℓ, m, and n are positive integers, and the lemma is proved.

To prove the theorem, we first observe that for any t that satisfies the same condition as s in the lemma,

$$\ell' = \frac{1}{2}\{ra(ra + 2)t + rb\},$$

$$m' = \frac{1}{2}\{(r^2a^2 + 2ra + 2)t + rb\},$$

$$n' = (ra + 1)t,$$

satisfy the equation

$$A_{\ell'} = A_{m'} - A_{n'}. \tag{5}$$

Now we shall determine values of s and t so that we have $\ell = \ell'$. For these values, (1) and (5) will yield the required representations.

Let

$$s = \frac{1}{2}\{ra(ra + 2)x + r(ra + 1)b\}, \tag{6}$$

$$t = (ra + 1)x + rb, \tag{7}$$

where x is an integer that makes s odd if ra is odd. Then we have

$$\ell = (ra + 1)s = \frac{1}{2}\{ra(ra + 2)t + rb\} = \ell'$$

and thus, for x sufficiently large, s and t given by (6) and (7) will satisfy our requirement. Substituting (6) and (7) into ℓ, m, n, m', and n', we get the following proposition, which establishes the theorem.

PROPOSITION: *If x is a sufficiently large integer that makes s in* (6) *odd whenever ra is odd, then*

$$\ell = \frac{1}{2}\{ra(ra + 1)(ra + 2)x + r(ra + 1)^2b\}$$

$$m = \frac{1}{4}\{ra(ra + 2)(r^2a^2 + 2ra + 2)x + r(r^3a^3 + 3r^2a^2 + 4ra + 4)b\}$$

$$n = \frac{1}{4}\{r^2a^2(ra + 2)^2x + r(r^3a^3 + 3r^2a^2 + 2ra + 2)b\}$$

$$m' = \frac{1}{2}\{(ra + 1)(r^2a^2 + 2ra + 2)x + r(r^2a^2 + 2ra + 3)b\}$$

$$n' = (ra + 1)^2x + r(ra + 1)b$$

are positive integers, with $m \neq m'$, which satisfy the relation

$$A_\ell = A_m - A_n = A_{m'} - A_{n'}.$$

Note that for any r, a, and b, the equation $m = m'$ has at most one solution x, because it can be reduced to the equation

$$(r^2a^2 - 2)x = -r(ra - 1)b.$$

3. THE CASE OF POLYGONAL NUMBERS

If we put

$$a = k - 2,\ b = -(k - 4),\ \text{for } k \geqslant 3,$$

in ℓ, m, n, m', and n' in the proposition, we get formulas for polygonal numbers which satisfy the equation

$$P_{\ell,k} = P_{m,k} - P_{n,k} = P_{m',k} - P_{n',k}. \tag{8}$$

If $r = 1$, for instance, then we have

$$\ell = \frac{1}{2}\{k(k - 1)(k - 2)x - (k - 1)^2(k - 4)\}$$

$$m = \frac{1}{4}\{k(k - 2)(k^2 - 2k + 2)x - k(k - 4)(k^2 - 3k + 4)\}$$

$$n = \frac{1}{4}\{k^2(k - 2)^2x - (k - 4)(k^3 - 3k^2 + 2k + 2)\}$$

$$m' = \frac{1}{2}\{(k - 1)(k^2 - 2k + 2)x - (k - 4)(k^2 - 2k + 3)\}$$

$$n' = (k - 1)^2x - (k - 1)(k - 4).$$

For every positive integer x, if k is even, and for positive x such that $x \equiv k + 1 \pmod 4$, if k is odd, these values are positive integers with $m \neq m'$, which satisfy Equation (8).

In the case of $r = 2$ we have, for every positive integer x,

$$\ell = 2(k - 1)(k - 2)(2k - 3)x - (k - 4)(2k - 3)^2$$

$$m = 2(k - 1)(k - 2)(2k^2 - 6k + 5)x - 2(k - 4)(2k^3 - 9k^2 + 14k - 7)$$

$$n = 4(k - 1)^2(k - 2)^2x - (k - 4)(4k^3 - 18k^2 + 26k - 11)$$

$$m' = (2k - 3)(2k^2 - 6k + 5)x - (k - 4)(4k^2 - 12k + 11)$$

$$n' = (2k - 3)^2x - 2(k - 4)(2k - 3),$$

which are positive integers with $m \neq m'$, which satisfy Equation (8).

For $k = 3$ and 5, these values are as follows. In the case of $r = 1$, we use $4x$ for $k = 3$ and $4x - 2$ for $k = 5$ instead of x, so that we can get positive integral values for every positive integer x.

	$r = 1$	$r = 2$
$k = 3$	$\ell = 12x + 2$ $m = 15x + 3$ $n = 9x + 2$ $m' = 20x + 3$ $n' = 16x + 2$	$\ell = 12x + 9$ $m = 20x + 16$ $n = 16x + 13$ $m' = 15x + 11$ $n' = 9x + 6$
$k = 5$	$\ell = 120x - 68$ $m = 255x - 145$ $n = 225x - 128$ $m' = 136x - 77$ $n' = 64x - 36$	$\ell = 168x - 49$ $m = 600x - 176$ $n = 576x - 169$ $m' = 175x - 51$ $n' = 49x - 14$

ACKNOWLEDGMENT

This note was written during my stay at the University of Santa Clara. I would like to thank Professor G. L. Alexanderson there for correcting it.

REFERENCES

1. A. Wieckowski. "On Some Systems of Diophantine Equations Including the Algebraic Sum of Triangular Numbers." *The Fibonacci Quarterly* 18, No. 2 (1980):165-170.
2. S. Ando. "A Note on the Polygonal Numbers." *The Fibonacci Quarterly* 19, No. 2 (1981):180-183.

*****

SOME PROPERTIES OF DIVISIBILITY OF HIGHER-ORDERED LINEAR RECURSIVE SEQUENCES

GERÖCS LÁSZLÓ
Balzac U. 35, Budapest, 1136, V.3. Hungary
(Submitted August 1981)

In this paper we consider the Fibonacci sequence defined by

$$F_0 = 0,\ F_1 = 1, \text{ and } F_n = F_{n-1} + F_{n-2},\ n \geqslant 2,$$

the k-ordered Fibonacci sequence $\{G_n^{(k)}\}$, and the generalized k-ordered linear recursive sequence $\{R_n^{(k)}\}$, both of which will be defined.

First a new relation on the Fibonacci sequence will be proved and a well-known relation on the Fibonacci sequence will be generalized for the k-ordered Fibonacci sequence. Then an infinite set of positive integers will be found such that no integer in this set is a divisor of any term in the sequence $\{R_n^{(k)}\}$. Finally, a result of Lieuwens [1] will be generalized for k-ordered linear recursive sequences.

DEFINITION 1: For every $k > 1$, the k-ordered Fibonacci sequence $\{G_n^{(k)}\}$ is defined by $G_0^{(k)} = G_1^{(k)} = \cdots = G_{k-1}^{(k)} = 1$, and

$$G_n^{(k)} = \sum_{i=1}^{k} G_{n-i}^{(k)},\ n \geqslant k.$$

(When $k = 2$, this sequence is essentially the Fibonacci sequence.)

DEFINITION 2: For every $k > 1$, the generalized k-ordered linear recursive sequence $\{R_n^{(k)}\}$ is defined by $R_0^{(k)} = R_1^{(k)} = \cdots = R_{k-1}^{(k)} = 1$, and

$$R_n^{(k)} = \sum_{i=1}^{k} a_i R_{n-i}^{(k)},\ n \geqslant k,$$

where the a_i are integers not all equal to 0.

DEFINITION 3: If $m \neq 0$ is an integer, then for every $k > 1$, the length of the period modulo m of $\{R_n^{(k)}\}$ is the least natural number $p(m)$ such that there exists an index n_0, and for $n > n_0$,

$$R_{n+p}^{(k)} \equiv R_n^{(k)} \pmod{m}.$$

A sequence is called absolutely periodic modulo m if $n_0 = 0$.

REMARK: Every sequence $\{R_n^{(k)}\}$ is clearly periodic.

DEFINITION 4: The occurrence order of the natural number $m > 1$ in the sequence $\{R_n^{(k)}\}$ is the number $r(m)$, for which $m \mid R_r^{(k)}$, but $m \nmid R_n^{(k)}$ if $0 < n < r$.

EXAMPLE 1: Let the $a_i = 1$ and $k = 3$. Then we have the sequence

$$\{R_n^{(3)}\} \equiv 1, 1, 1, 3, 5, 9, 17, 31, 57, 105, 193, \ldots .$$

If $m = 5$, this sequence reduced modulo 5 becomes

$$1, 1, 1, 3, 0, 4, 2, 1, 2, 0, 3, 0, 3, 1, 4, 3, 3, 0, 1, 4,$$
$$0, 0, 4, 4, 3, 1, 3, 2, 1, 1, 4, 1, 1, 1, 3, \ldots,$$

and we have

$$p(5) = 31,\ n_0 = 0,\ r(5) = 4.$$

THEOREM 1: If $\{R_n\}$ is the sequence defined by

$$R_0 = 1,\ R_n = \sum_{j=1}^{n} jR_{n-j},\ n > 0,$$

then for $n \geqslant 2$,

(a) $R_n = F_{2n}$;

(b) $\sum_{j=0}^{n} R_j = F_{2n+1}$.

PROOF: (a) For $n = 2$, 3, and 4, the theorem is easily established. Using finite induction, and assuming that for $i > 4$,

$$R_i = F_{2i},$$

then

$$\begin{aligned} F_{2(i+1)} &= F_{2i+2} = F_{2i+1} + F_{2i} = F_{2i} + F_{2i-1} + F_{2i} \\ &= 2F_{2i} + F_{2i} - F_{2i-2} = 3F_{2i} - F_{2(i-1)} = 3R_i - R_{i-1} \\ &= 3\sum_{j=1}^{i} jR_{i-j} - \sum_{j=1}^{i-1} jR_{i-j-1} = \sum_{j=1}^{i} (2j+1)R_{i-j} \\ &= \sum_{j=1}^{i} jR_{i-j} + \sum_{j=2}^{i+1} jR_{i+1-j} = R_i + \sum_{j=2}^{i+1} jR_{i+1-j} \end{aligned}$$

$$= \sum_{j=1}^{i+1} jR_{i+1-j} = R_{i+1},$$

as required.

(b) Applying (a) above, we have

$$\begin{aligned} F_{2n+1} &= F_{2(n+1)} - F_{2n} = R_{n+1} - R_n \\ &= \sum_{j=1}^{n+1} jR_{n+1-j} - \sum_{j=1}^{n} jR_{n-j} = \sum_{j=0}^{n} R_j. \end{aligned}$$

A well-known identity for Fibonacci numbers is

$$F_n = \sum_{i=2}^{n} F_{n-i} + 1, \; n \geqslant 2. \tag{1}$$

An alternate form of (1), which we obtain by renaming $F_0 = 1$, $F_1 = 1$, $F_2 = 2$, and generalize as Theorem 2, is

$$F_n = \sum_{i=2}^{n-2} F_{n-i} + 3, \; n \geqslant 4. \tag{2}$$

<u>THEOREM 2</u>: *If $G_n^{(k)}$ is as in Definition 1, then for all $n \geqslant 2k$,*

$$G_n^{(k)} = \sum_{i=1}^{k-2} iG_{n-i-1}^{(k)} + (k-1)\sum_{i=k}^{n-k} G_{n-i}^{(k)} + \frac{k(k+1)}{2}. \tag{3}$$

Note that $G_n^{(2)} = F_n$ as defined in (2) and hence (2) is a special case of (3).

<u>PROOF</u>: Let $k \geqslant 2$ be fixed. If $n = 2k$, then using the definition of $G_{2k}^{(k)}$ twice and performing the indicated sums, we have

$$\begin{aligned} G_{2k}^{(k)} &= \sum_{i=1}^{k} G_{2k-i}^{(k)} = \sum_{i=1}^{k} \sum_{j=1}^{k} G_{2k-i-j}^{(k)} \\ &= G_{2k-2}^{(k)} + 2G_{2k-3}^{(k)} + \cdots + (k-2)G_{k+1}^{(k)} + (k-1)G_k^{(k)} + \frac{k(k+1)}{2} \\ &= \sum_{i=1}^{k-2} iG_{2k-i-1}^{(k)} + (k-1)G_k^{(k)} + \frac{k(k+1)}{2}. \end{aligned}$$

(Recall that $G_0^{(k)} = G_1^{(k)} = \cdots = G_{k-1}^{(k)} = 1$.)

Now suppose that (3) is true for $m > 2k$. Then

$$\begin{aligned} G_{m+1}^{(k)} &= \sum_{i=1}^{k} G_{m-i+1}^{(k)} = \sum_{i=0}^{k-1} G_{m-i}^{(k)} = G_m^{(k)} + \sum_{i=1}^{k-1} G_{m-i}^{(k)} \\ &= \sum_{i=1}^{k-2} iG_{m-i-1}^{(k)} + (k-1)\sum_{i=k}^{m-k} G_{m-i}^{(k)} + \frac{k(k+1)}{2} + \sum_{i=1}^{k-1} G_{m-i}^{(k)} \end{aligned}$$

$$= \left[\sum_{i=1}^{k-3} iG_{m-i-1}^{(k)} + \sum_{i=1}^{k-2} G_{m-i}^{(k)}\right] + \left[(k-2)G_{m-(k-1)}^{(k)} + G_{m-(k-1)}^{(k)} + (k-1)\sum_{i=k}^{m-k} G_{m-i}^{(k)}\right] + \frac{k(k+1)}{2}$$

$$= \sum_{i=1}^{k-2} iG_{(m+1)-i-1}^{(k)} + (k-1)\sum_{i=k}^{m+1-k} G_{(m+1)-i}^{(k)} + \frac{k(k+1)}{2},$$

which proves that (3) is true for $n = m + 1$ and hence for all n.

We now turn to the question of divisibiltiy of the terms of the sequence $\{R_n^{(k)}\}$ by the natural number m and state the following theorem.

THEOREM 3: If $\{R_n^{(k)}\}$ is as in Definition 2, *and if m if a natural number such that*

$$\left(\sum_{i=1}^{k} a_i\right) - 1 \neq 0$$

and

$$\text{g.c.d.}\left(m, \left(\sum_{i=1}^{k} a_i - 1\right)\right) = d > 1,$$

then $m \nmid R_n^{(k)}$ for any n. That is, $r(m)$ does not exist.

PROOF: Let

$$M = \left(\sum_{i=1}^{k} a_i\right) - 1.$$

If g.c.d. $(m, M) = d > 1$, we show that for every n,

$$R_n^{(k)} \equiv 1 \pmod{M}.$$

If $n < k$, then $R_n^{(k)} = 1$ and $M \nmid R_n^{(k)}$, since $M > 1$.

Now, if we assume that the theorem is true for any k successive terms of the sequence, we have

$$R_n^{(k)} = j_0 M + 1$$

$$R_{n+1}^{(k)} = j_1 M + 1$$

$$\cdots\cdots\cdots$$

$$R_{n+k-1}^{(k)} = j_{k-1} M + 1.$$

Multiplying each of these equations successively by $a_k, a_{k-1}, \ldots, a_1$, we obtain

$$\begin{aligned} a_k R_n^{(k)} &= a_k j_0 M + a_k \\ a_{k-1} R_{n+1}^{(k)} &= a_{k-1} j_1 M + a_{k-1} \\ \cdots & \cdots \\ a_1 R_{n+k-1}^{(k)} &= a_1 j_{k-1} M + a_1, \end{aligned}$$

and then adding, we have

$$\begin{aligned} R_{n+k}^{(k)} = \sum_{i=1}^{k} a_i R_{n+k-i}^{(k)} &= M \sum_{i=1}^{k} a_i j_{k-i} + \left(\sum_{i=1}^{k} a_i\right) - 1 + 1 \\ &= M\left(\sum_{i=1}^{k} a_i j_{k-i} + 1\right) + 1, \end{aligned}$$

which establishes that $R_{n+k}^{(k)} \equiv 1 \pmod{M}$.

Now we assume that for some s,

$$m | R_s^{(k)}.$$

Then $d | R_s^{(k)}$ and $d | M$ and hence there exist integers j, r_1, and r_2 such that

$$R_s^{(k)} = r_1 d = jM + 1 = r_2 d + 1,$$

which implies $d | 1$, a contradiction, and the proof is complete.

If g.c.d. $(m, M) = 1$, then it is not known whether, in general, there exists n such that $m | R_n^{(k)}$.

Finally, we examine $p(m)$, the length of the period of $\{R_n^{(k)}\}$ modulo m.

Waddill[2] has shown that in the special case where $R_0 = 0$, $R_1 = R_2 = 1$, $k = 3$, $a_1 = a_2 = a_3 = 1$, and $m = q_1^{\alpha_1}, q_2^{\alpha_2}, \ldots, q_r^{\alpha_r}$, q_i prime, then

$$p(m) = \text{l.c.m.}\ [p(q_1^{\alpha_1}), p(q_2^{\alpha_2}), \ldots, p(q_r^{\alpha_r})]. \tag{4}$$

Lieuwens [1] has shown that (4) holds for an arbitrary 2-ordered sequence. We show that (4) is true for every k-ordered sequence.

<u>*THEOREM 4:*</u> *Let* $\{R_n^{(k)}\}$ *be as in Definition* 2 *and let* $m > 1$ *be an arbitrary integer, where*

$$m = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_r^{\alpha_r},\ q_i \text{ prime},$$

then

$$p(m) = \text{l.c.m.}\ [p(q_1^{\alpha_1}), p(q_2^{\alpha_2}), \ldots, p(q_r^{\alpha_r})].$$

PROOF: For every integer $q_i^{\alpha_i}$, there exists an index n_{0_i} such that for $n > n_{0_i}$,

$$R_{n+jp(q_i^{\alpha_i})}^{(k)} \equiv R_n^{(k)} \pmod{q_i^{\alpha_i}},\ j = 0, 1, 2, \ldots .$$

Let $n^* = \max(n_{0_1}, n_{0_2}, \ldots, n_{0_r})$. Then for every integer $t > 0$, $j \geqslant 0$,

$$R_{n^*+jp(q_i^{\alpha_i})+t}^{(k)} \equiv R_{n^*+t}^{(k)} \pmod{q_i^{\alpha_i}}$$

for all i. Hence, for $i = 1, 2$, say,

$$R_{n^*+jp(q_1^{\alpha_1})+t}^{(k)} \equiv R_{n^*+t}^{(k)} \pmod{q_1^{\alpha_1}}$$

$$R_{n^*+jp(q_2^{\alpha_2})+t}^{(k)} \equiv R_{n^*+t}^{(k)} \pmod{q_2^{\alpha_2}},$$

Since g.c.d. $(q_1, q_2) = 1$, then the smallest integer, p, such that

$$R_{n^*+p+t}^{(k)} \equiv R_{n^*+t}^{(k)} \pmod{q_1^{\alpha_1} q_2^{\alpha_2}}$$

occurs when

$$p = \text{l.c.m.}\ [p(q_1^{\alpha_1}),\ p(q_2^{\alpha_2})],$$

since p must be a multiple of both $p(q_1^{\alpha_1})$ and $p(q_2^{\alpha_2})$. The general case follows similarly.

ACKNOWLEDGMENT

The author acknowledges the assistance of Professor Marcellus E. Waddill in editing this manuscript for publication.

REFERENCES

1. E. Lieuwens. *Fermat Pseudo Primes*. Drukkerij, Hoogland, Delft, 1971.
2. Marcellus E. Waddill. "Some Properties of a Generalized Fibonacci Sequence Modulo m." *The Fibonacci Quarterly* 16, No. 4 (August 1978):344-353.

*****

THE EXISTENCE OF K ORTHOGONAL LATIN K-CUBES OF ORDER 6

JOHN KERR
National University of Singapore, Singapore 1025
(Submitted September 1981)

INTRODUCTION

A Latin cube of order n is an n^3 ($n \times n \times n$) array in which each of the numbers 1, 2, ..., n appears exactly once in each line of the array. Similarly, a Latin k-cube of order n is an n^k array where each of the numbers 1, 2, ..., n appears exactly once in each line. A set of k Latin k-cubes is orthogonal if, when superimposed, each ordered k-tuple of the numbers 1, 2, ..., n appears once.

Orthogonal Latin k-cubes of order n can be constructed from 2 orthogonal Latin squares of order λ [1]. However, there are no orthogonal Latin squares of order 6 [3] and it has been conjectured that there are thus no orthogonal Latin k-cubes or order 6 [4].

We now show how orthogonal Latin k-cubes can be constructed from three orthogonal Latin cubes.

THEOREM: If there exist three orthogonal Latin cubes and k orthogonal Latin k-cubes or order n, then there exist orthogonal Latin $(k + 2)$-cubes of order n.

PROOF: Let $A = (a_{ijk})$, $B = (b_{ijk})$, and $C = (c_{ijk})$ be orthogonal Latin cubes and $A^1, A^2, \ldots, A^k$ be orthogonal Latin k-cubes of order n. Write the entries of A^j as $a^j_{i_1, \ldots, i_k}$.

Then we can define $(k+2)$ orthogonal Latin $(k+2)$-cubes $B^1, B^2, \ldots, B^{k+2}$ by

$$b^1_{i_1, \ldots, i_{k+2}} = a_{a^1_{i_1, \ldots, i_k}, i_{k+1}, i_{k+2}}$$

$$\vdots$$

$$b^k_{i_1, \ldots, i_{k+2}} = a_{a^1_{i_1, \ldots, i_k}, i_{k+1}, i_{k+2}}$$

$$b^{k+1}_{i_1, \ldots, i_{k+2}} = b_{a^1_{i_1, \ldots, i_k}, i_{k+1}, i_{k+2}}$$

$$b^{k+2}_{i_1, \ldots, i_{k+2}} = c_{a^1_{i_1, \ldots, i_k}, i_{k+1}, i_{k+2}}$$

The $(k + 2)$-cubes thus defined are orthogonal, since there is a unique position $(i_1, i_2, \ldots, i_{k+2})$ in each Latin $(k + 2)$-cube for every $(k + 2)$-tuple of the numbers $(1, 2, \ldots, n)$ (see [1]).

Examples of 3 orthogonal Latin 3-cubes and 4 orthogonal Latin 4-cubes of order 6 are presented in Table 1 below. Hence, we have shown the existence of k orthogonal Latin k-cubes of order 6.

TABLE 1

(a) 3 Orthogonal Latin Cubes of Order 6

661	433	526	242	354	115
435	522	663	356	111	244
524	665	431	113	246	352
212	344	155	421	563	636
346	151	214	565	632	423
153	216	342	634	425	561

Other layers are obtained by the cyclic permutation (1 2 3 4 5 6).

(b) 4 Orthogonal Latin 4-Cubes of Order 6

I						II					
3554	2241	1115	5663	4332	6426	1131	3516	2263	6442	5625	4354
1135	3514	2261	6446	5623	4352	2223	1151	3536	4314	6462	5645
2221	1155	3534	4312	6466	5643	3556	2243	1111	5665	4334	6422
4413	5662	6346	3524	1251	2135	6362	4435	5624	2151	3546	1213
6366	4433	5622	2155	3544	1211	5644	6322	4455	1233	2111	3566
5642	6326	4453	1231	2115	3564	4415	5664	6342	3526	1253	2131

III						IV					
2225	1153	3532	4316	6464	5641	6443	5322	4656	2534	3211	1165
3552	2245	1113	5661	4336	6424	4616	6463	5342	1125	2554	3231
1133	3512	2265	6444	5621	4356	5362	4636	6423	3251	1145	2514
5646	6324	4451	1235	2113	3562	1254	3141	2515	6363	5432	4626
4411	5666	6344	3522	1255	2133	2535	1214	3161	4646	6323	5452
6364	4431	5626	2153	3542	1215	3121	2555	1234	5412	4666	6343

V						VI					
4612	6465	5344	1121	2556	3233	5366	4634	6421	3255	1143	2512
5364	4632	6425	3253	1141	2516	6441	5326	4654	2532	3215	1163
6445	5324	4652	2536	3213	1161	4614	6461	5346	1123	2552	3235
2531	1216	3163	4642	6325	5454	3125	2553	1232	5416	4664	6341
3123	2551	1236	5414	4662	6345	1252	3145	2513	6361	5436	4624
1256	3143	2511	6365	5434	4622	2533	1212	3165	4644	6321	5456

Other layers are obtained by the cyclic permutation (1 2 3 4 5 6).

REFERENCES

1. J. Arkin & E. G. Straus. "Latin k-Cubes." *The Fibonacci Quarterly* 12, No. 3 (Oct. 1974):288-292.
2. J. Arkin & E. G. Straus. "Orthogonal Latin Systems." *The Fibonacci Quarterly* 19, No. 3 (Oct. 1981):289-293.
3. G. Tarry. "Le problem de 36 officiers." *Comptes Rendu de l'Association Francaise pour L'Advancement de Science Natural* 2 (1901):170-203.
4. P. D. Warrington. "Graeco-Latin Cubes." *J. Recreat. Math.* 6 (1973):47-53.

*****

A TRINOMIAL DISCRIMINANT FORMULA

PHYLLIS LEFTON
Manhattanville College, Purchase, NY 10577

The expression $b^2 - 4ac$ is well known to algebra students as the discriminant of the quadratic $ax^2 + bx + c$, with $a \neq 0$. However, how many students are aware of the existence of discriminant formulas for higher-degree polynomials? The purpose of this paper is to develop such a formula for the trinomial

$$ax^n + bx^k + c, \tag{1}$$

with $n > k > 0$ and $a \neq 0$. The formula has appeared in the literature in various forms ([1, p. 130], [2], [3], [4], [5, p. 41], and [6]). It can be written as

$$\Delta_{n,k} = (-1)^{\frac{1}{2}n(n-1)}a^{n-k-1}c^{k-1}(n^N a^K c^{N-K} + (-1)^{N-1}(n-k)^{N-K}k^K b^N)^d, \tag{2}$$

where d is the greatest common divisor of n and k and N and K are given by $n = Nd$ and $k = Kd$. Notice that the case $n = 2$ and $k = 1$ gives the quadratic discriminant

$$\Delta_{2,1} = b^2 - 4ac.$$

In this paper we derive (2) by standard algebraic techniques that involve some elementary calculus and roots of unity. As a generalization of the quadratic case, the trinomial discriminant formula can provide an interesting enrichment topic for advanced-level algebra students.

To appreciate what is involved in deriving (2), consider the usual definition of the discriminant D_n of the general nth-degree polynomial

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n. \tag{3}$$

Van der Waerden [7, p. 101], for example, defines D_n as

$$D_n = a_0^{2n-2}\prod_{i<j}(\alpha_i - \alpha_j)^2, \tag{4}$$

where the α's are the roots of $f(x)$.

As examples, let us compute D_n for $n = 2$ and $n = 3$. In these cases, (3) is more commonly written as $f(x) = ax^2 + bx + c$ and $f(x) = ax^3 + bx^2 + cx + d$, respectively. Using (4) together with the well-known expressions that relate the coefficients of each polynomial to the elementary symmetric functions of their roots, we get

$$D_2 = b^2 - 4ac$$

and

$$D_3 = b^2c^2 - 27a^2d^2 - 4b^3d - 4ac^3 + 18abcd.$$

We note that for $n \geqslant 3$, D_n becomes more difficult to compute directly from the roots of $f(x)$.

There are other expressions for D_n that involve the derivative f' of (3). A straightforward manipulation of the product (4), for example, gives:

$$D_n = (-1)^{\frac{1}{2}n(n-1)} a_0^{n-2} \prod_{i=1}^{n} f'(\alpha_i). \tag{5}$$

Still another expression for D_n is the one we will use to derive (2), namely:

$$D_n = (-1)^{\frac{1}{2}n(n-1)} a_0^{n-1} n^n \prod_{j=1}^{n-1} f(\beta_j), \tag{6}$$

where the β's are the roots of $f'(x)$. It is not hard to compute the discriminant of (1) from (6) because the derivative of a trinomial is a binomial whose roots are easy to find.

The expression (6) is obtained by considering the double product

$$(a_0 n)^n \prod_{i=1}^{n} \prod_{j=1}^{n-1} (\alpha_i - \beta_j),$$

where the α_i's and the β_j's are the roots of $f(x)$ and $f'(x)$, respectively. By rearranging this double product, as described in [7], it is easy to show that it is equal to each of the following single products, which are hence equal to each other:

$$a_0 n^n \prod_{j=1}^{n-1} f(\beta_j) = \prod_{i=1}^{n} f'(\alpha_i). \tag{7}$$

A comparison of (7) with (5) then gives (6).

We now derive the discriminant formula. We first obtain the formula for $f(x) = ax^n - bx^k + c$ and then replace b by $-b$. Write

$$f(x) = ax^n - bx^k + c = c - (b - ax^{n-k})x^k \tag{8}$$

and

$$f'(x) = nax^{n-1} - kbx^{k-1} = x^{k-1}(nax^{n-k} - kb).$$

Clearly, the roots of the binomial $f'(x)$ are $(k - 1)$ zeros and the solutions of $x^{n-k} = kb/na$. Therefore, by (8),

$$\prod_{j=1}^{n-1} f(\beta_j) = c^{k-1} \prod_{\zeta} \Big(c - (b - a(\zeta\beta)^{n-k})(\zeta\beta)^k\Big),$$

where ζ runs through all of the $(n - k)$th roots of unity and $\beta^{n-k} = kb/na$. For further information about roots of unity, see [7, Sec. 36]. Simplifying, we have

$$\prod_{j=1}^{n-1} f(\beta_j) = c^{k-1} \prod_{\zeta}\left(c - \left(\frac{n-k}{n}\right)b\ \beta^k\zeta^k\right).$$

Now, as ζ runs through the $(n - k)$th roots of unity, ζ^k runs d times through the $(N - K)$th roots of unity. Therefore, after further simplification with roots of unity, we get

$$\prod_{j=1}^{n-1} f(\beta_j) = c^{k-1}\left(c^{N-K} - (n - k)^{N-K} k^K n^{-N} a^{-K} b^N\right)^d.$$

Here we are using the fact that, if ω is a primitive mth root of unity, then

$$u^m - v^m = \prod_{i=0}^{m-1} (u - v\omega^i).$$

Using (6) and substituting $-b$ for b, we obtain the desired formula given in (2).

ACKNOWLEDGMENT

Thanks is given to Professor P. X. Gallagher for his help and to Professor K. S. Williams for referring the author to the articles by Masser, Heading, and Goodstein.

REFERENCES

1. E. Artin. *Theory of Algebraic Numbers*. Göttingen, 1959.
2. R. L. Goodstein. "The Discriminant of a Certain Polynomial." *Math. Gaz.* 53 (1969):60-61.
3. J. Heading. "The Discriminant of an Equation of nth Degree." *Math. Gaz.* 51 (1967):324-326.
4. D. W. Masser. "The Discriminants of Special Equations." *Math. Gaz.* 50 (1966):158-160.
5. P. Samuel. *Algebraic Theory of Numbers*. Paris: Hermann, 1970.
6. R. Swan. "Factorization of Polynomials Over Finite Fields." *Pacific J. Math.* 12 (1962):1099-1106.
7. B. L. van der Waerden. *Algebra*. Vol. I. New York: Ungar, 1970.

*****

ELEMENTARY PROBLEMS AND SOLUTIONS

Edited by
A. P. HILLMAN
University of New Mexico, Albuquerque, NM 87131

Send all communications regarding ELEMENTARY PROBLEMS AND SOLUTIONS to PROFESSOR A. P. HILLMAN, 709 SOLANO DR., S.E.; ALBUQUERQUE, NM 87108. Each problem or solution should be on a separate sheet (or sheets). Preference will be given to those that are typed with double spacing in the format used below. Solutions should be received within 4 months of the publication date.

DEFINITIONS

The Fibonacci numbers F_n and Lucas numbers L_n satisfy

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

and

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

Also, a and b designate the roots $(1 + \sqrt{5})/2$ and $(1 - \sqrt{5})/2$, respectively, of $x^2 - x - 1 = 0$.

PROBLEMS PROPOSED IN THIS ISSUE

B-484 Proposed by Philip L. Mana, Albuquerque, NM

For a given x, what is the least number of multiplications needed to calculate x^{98}? (Assume that storage is unlimited for intermediate products.)

B-485 Proposed by Gregory Wulczyn, Bucknell University, Lewisburg, PA

Find the complete solution u_n to the difference equation

$$u_{n+2} - 5u_{n+1} + 6u_n = 11F_n - 4F_{n+2}.$$

B-486 Proposed by Valentina Bakinova, Rondout Valley, NY

Prove or disprove that, for every positive integer k,

$$\frac{F_{k+1}}{F_1} < \frac{F_{k+3}}{F_3} < \frac{F_{k+5}}{F_5} < \cdots < a^k < \cdots < \frac{F_{k+6}}{F_6} < \frac{F_{k+4}}{F_4} < \frac{F_{k+2}}{F_2}.$$

B-487 Proposed by Herta T. Freitag, Roanoke, VA

Prove or disprove that, for all positive integers n,

$$5L_{4n} - L_{2n}^2 + 6 - 6(-1)^n L_{2n} \equiv 0 \pmod{10F_n^2}.$$

B-488 Proposed by Herta T. Freitag, Roanoke, VA

Let a and d be positive integers with d odd. Prove or disprove that for all positive integers h and k,

$$L_{a+hd} + L_{a+hd+d} \equiv L_{a+kd} + L_{a+kd+d} \pmod{L_d}.$$

B-489 Proposed by Herta T. Freitag, Roanoke, VA

Is there a Fibonacci analogue (or semianalogue) of B-488?

SOLUTIONS

Pythagorean Triples

B-457 Proposed by Herta T. Freitag, Roanoke, VA

Prove or disprove that there exists a positive integer b such that the Pythagorean-type relationship $(5F_n^2)^2 + b^2 \equiv (L_n^2)^2 \pmod{5m^2}$ holds for all m and n with $m|F_n$.

Solution by Bob Prielipp, University of Wisconsin-Oshkosh, WI

We will show that the specified Pythagorean-type relationship holds with $b = 4$. Since

$$L_n^2 = 5F_n^2 + 4(-1)^n,\ (L_n^2)^2 = (5F_n^2)^2 + 8(-1)^n(5F_n^2) + 4^2,$$

we have

$$(5F_n^2)^2 + 4^2 \equiv (L_n^2)^2 \pmod{5F_n^2}.$$

Hence, for all m such that m divides F_n,

$$(5F_n^2)^2 + 4^2 \equiv (L_n^2)^2 \pmod{5m^2}.$$

Also solved by Paul S. Bruckman, Frank Higgins, Sahib Singh, Lawrence Somer, and the proposer.

Prime Difference of Triangular Numbers

B-458 Proposed by H. Klauser, Zurich, Switzerland

Let T_n be the triangular number $n(n+1)/2$. For which positive integers k do there exist positive integers n such that $T_{n+k} - T_n$ is a prime?

Solution by Lawrence Somer, Washington, D.C.

The answer is $k = 1$ or $k = 2$. Note that

$$T_{n+k} - T_n = (n + k)(n + k + 1)/2 - n(n + 1)/2$$
$$= (k^2 + k + 2nk)/2 = k(k + 2n + 1)/2.$$

If $T_{n+k} - T_n$ is prime, then $k = 1$ or $k/2 = 1$ since $k + 2n + 1 > k$. If $k = 1$, then $n = p - 1$, where p is prime, suffices to make $T_{n+k} - T_n$ prime. If $k = 2$, then $n = (p - 3)/2$, where p is prime, suffices to make $T_{n+k} - T_n$ prime.

Also solved by Paul Bruckman, Herta Freitag, Frank Higgins, Walther Janous, Peter Lindstrom, Bob Prielipp, Sahib Singh, J. Suck, Gregory Wulczyn, and the proposer.

Incongruent Differences

B-459 Proposed by E. E. McDonnell, Palo Alto, CA and J. O. Shallit, Berkeley, CA

Let g be a primitive root of the odd prime p. For $1 \leqslant i \leqslant p - 1$, let a_i be the integer in $S = \{0, 1, \ldots, p - 2\}$ with $g^{a_i} \equiv i \pmod{p}$. Show that

$$a_2 - a_1,\ a_3 - a_2,\ \ldots,\ a_{p-1} - a_{p-2}$$

(differences taken mod $p - 1$ to be in S), is a permutation of $1, 2, \ldots, p - 2$.

Solution by Lawrence Somer, Washington, D.C.

Suppose that $a_{i+1} - a_i \equiv a_{j+1} - a_j \pmod{p - 1}$, where $1 \leqslant i < j \leqslant p - 2$. Then

$$g^{a_{i+1} - a_i} \equiv g^{a_{j+1} - a_j} \pmod{p}$$

or

$$g^{a_{i+1}}/g^{a_i} \equiv (i + 1)/i \equiv g^{a_{j+1}}/g^{a_j} \equiv (j + 1)/j \pmod{p}.$$

Since neither i nor $j \equiv 0 \pmod{p}$, this implies that

$$(i + 1)j = ij + j \equiv i(j + 1) = ij + i \pmod{p}.$$

However, this is a contradiction, since $i \not\equiv j \pmod{p}$.

Also solved by Paul S. Bruckman, Frank Higgins, Walther Janous, Bob Prielipp, Sahib Singh, and the proposer.

First of a Pair

B-460 Proposed by Larry Taylor, Rego Park, NY

For all integers j, k, n, prove that

$$F_k F_{n+j} - F_j F_{n+k} = (-1)^j F_{k-j} F_n.$$

Solution by A. G. Shannon, New South Wales I.T., Australia

$$\begin{aligned} F_k F_{n+j} - F_j F_{n+k} &= (a^k - b^k)(a^{n+j} - b^{n+j})/5 - (a^j - b^j)(a^{n+k} - b^{n+k}) \\ &= (ab)^j (a^{k-j} - b^{k-j})(a^n - b^n)/5 \\ &= (-1)^j F_{k-j} F_n. \end{aligned}$$

Also solved by Clyde Bridger, Paul Bruckman, D. K. Chang, Herta Freitag, John Ivie, Walther Janous, John Milsom, Bob Prielipp, Heinz-Jurgen Seiffert, Sahib Singh, Gregory Wulczyn, and the proposer.

Companion Identity

B-461 Proposed by Larry Taylor, Rego Park, NY

For all integers j, k, n, prove or disprove that

$$F_k L_{n+j} - F_j L_{n+k} = (-1)^j F_{k-j} L_n.$$

Solution by Paul S. Bruckman, Sacramento, CA

The following relation follows readily from the Binet definitions:

$$F_u L_v = F_{v+u} - (-1)^u F_{v-u}. \tag{1}$$

Therefore,

$$\begin{aligned} F_k L_{n+j} - F_j L_{n+k} &= F_{n+j+k} - (-1)^k F_{n+j-k} - F_{n+k+j} + (-1)^j F_{n+k-j} \\ &= (-1)^j (F_{n+k-j} - (-1)^{k-j} F_{n-(k-j)}) \\ &= (-1)^j F_{k-j} L_n \end{aligned}$$

[using (1) again, with $u = k - j$, $v = n$].

Also solved by Clyde Bridger, Herta Freitag, John Ivie, Walther Janous, John Milsom, Bob Prielipp, A. G. Shannon, Sahib Singh, Gregory Wulczyn, and the proposer.

Typographical Monstrosity

B-462 Proposed by Herta T. Freitag, Roanoke, VA

Let $L(n)$ denote L_n and $T_n = n(n+1)/2$. Prove or disprove:

$$L(n) = (-1)^{T_{n-1}}[L(T_{n-1})L(T_n) - L(n^2)].$$

Solution by John W. Milsom, Butler County Community College, Butler, PA

Using $L(n) = L_n = a^n + b^n$, $ab = -1$, and $T_n = n(n+1)/2$, it follows that

$$(-1)^{T_{n-1}}[L(T_{n-1})L(T_n) - L(n^2)] = (ab)^{n(n-1)}(a^n + b^n) = (-1)^{n(n-1)} L_n.$$

The number $n(n - 1)$ is always even, so that $(-1)^{n(n-1)} = 1$. Thus

$$L(n) = (-1)^{T_{n-1}}[L(T_{n-1})L(T_n) - L(n^2)].$$

Also solved by Clyde Bridger, Paul Bruckman, Walther Janous, Bob Prielipp, Sahib Singh, Gregory Wulczyn, and the proposer.

Casting Out Fives

B-463 Proposed by Herta T. Freitag, Roanoke, VA

Using the notations of B-462, prove or disprove:

$$L(n) \equiv (-1)^{T_{n-1}}L(n^2) \pmod 5.$$

Solution by Bob Prielipp, University of Wisconsin-Oshkosh, WI

We shall prove that the given congruence holds. Let $F(n)$ denote F_n. It is known that

$$L(a + b) - (-1)^b L(a - b) = 5F(a)F(b)$$

[see (10) and (12) on p. 115 of the April 1975 issue of this journal.] Hence,

$$L(T_n + T_{n-1}) - (-1)^{T_{n-1}}L(T_n - T_{n-1}) = 5F(T_n)F(T_{n-1})$$

so

$$L(n^2) - (-1)^{T_{n-1}}L(n) \equiv 0 \pmod 5.$$

The desired result follows almost immediately.

Also solved by Clyde Bridger, Paul Bruckman, Walther Janous, Sahib Singh, Gregory Wulczyn, and the proposer.

Consequence of a Hoggatt Identity

B-464 Proposed by Gregory Wulczyn, Bucknell University, Lewisburg, PA

Let n and w be integers with w odd. Prove or disprove:

$$F_{n+2w}F_{n+w} - 2L_wF_{n+w}F_{n-w} - F_{n-w}F_{n-2w} = (L_{3w} - 2L_w)F_n^2.$$

Solution by Sahib Singh, Clarion State College, Clarion, PA

The given equation is equivalent to:

$$F_{n+2w}F_{n+w} - F_{n-w}F_{n-2w} - L_{3w}F_n^2 = 2L_w(F_{n+w}F_{n-w} - F_n^2).$$

Using I_{19} (*Fibonacci and Lucas Numbers* by Hoggatt), the right side

$$= 2(-1)^n L_wF_w^2.$$

Expressing the left side of the above equation in a and b, it simplifies to

$$\frac{2(-1)^n}{5}(L_{3w} + L_w) = 2(-1)^n L_w F_w^2.$$

Also solved by Paul Bruckman, Herta Freitag, Walther Janous, Bob Prielipp, M. Wachtel, and the proposer.

Evenly Proportioned

B-465 Proposed by Gregory Wulczyn, Bucknell University, Lewisburg, PA

For positive integers n and k, prove or disprove:

$$\frac{F_{2k} + F_{6k} + F_{10k} + \cdots + F_{(4n-2)k}}{L_{2k} + L_{6k} + L_{10k} + \cdots + L_{(4n-2)k}} = \frac{F_{2nk}}{L_{2nk}}.$$

Solution by Sahib Singh, Clarion State College, Clarion, PA

Expressing

$$F_{2k} = \frac{a^{2k} - b^{2k}}{\sqrt{5}} \quad \text{and} \quad L_{2k} = a^{2k} + b^{2k},$$

the left side of the equation simplifies to

$$\frac{F_{(4n+2)k} - F_{(4n-2)k} - 2F_{2k}}{L_{(4n+2)k} - L_{(4n-2)k}}$$

Using I_{24} and I_{16} (*Fibonacci and Lucas Numbers* by Hoggatt) successively, the above becomes

$$\frac{5F_{2k}F_{2nk}^2}{L_{(4n+2)k} - L_{(4n-2)k}}.$$

Since $L_{(4n+2)k} - L_{(4n-2)k} = 5F_{2k}F_{2nk}L_{2nk}$, we are done.

Also solved by Clyde Bridger, Paul Bruckman, Herta Freitag, Bob Prielipp, and the proposer.

*****

ADVANCED PROBLEMS AND SOLUTIONS

Edited by
RAYMOND E. WHITNEY
Lock Haven State College, Lock Haven, PA 17745

Send all communications concerning ADVANCED PROBLEMS AND SOLUTIONS to RAYMOND E. WHITNEY, MATHEMATICS DEPARTMENT, LOCK HAVEN STATE COLLEGE, LOCK HAVEN, PA 17745. This department especially welcomes problems believed to be true or extending old results. Proposers should submit solutions or other information that will assist the editor. To facilitate their consideration, solutions should be submitted on separate, signed sheets within two months after publication of the problems.

PROBLEMS PROPOSED IN THIS ISSUE

H-345 Proposed by Albert A. Mullin, Huntsville, AL

Prove or disprove: No four consecutive Fibonacci numbers can be products of two distinct primes.

H-346 Proposed by Verner E. Hoggatt, Jr., deceased

Prove or disprove: Let

$$P_1 = 1,\ P_2 = 2,\ P_{n+2} = 2P_{n+1} + P_n \text{ for } n = 1, 2, 3, \ldots,$$

then $P_7 = 169$ is the largest Pell number which is a square, and there are no Pell numbers of the form $2s^2$ for $s > 1$.

H-347 Proposed by Paul S. Bruckman, Sacramento, CA

Prove the identity:

$$\left\{\sum_{n=-\infty}^{\infty} \frac{x^n}{1 + x^{2n}}\right\}^2 = \sum_{n=-\infty}^{\infty} \frac{x^n}{(1 + (-x)^n)^2} \tag{1}$$

valid for all real $x \neq 0, \pm 1$. In particular, prove the identity:

$$\left\{\sum_{n=-\infty}^{\infty} \frac{1}{L_{2n}}\right\}^2 = \sum_{n=-\infty}^{\infty} \frac{1}{L_n^2}. \tag{2}$$

H-348 Proposed by Andreas N. Philippou, Patras, Greece

For each fixed integer $k \geqslant 2$, define the sequence of polynomials $a_n^{(k)}(p)$ by

$$a_n^{(k)}(p) = p^{n+k} \sum_{n_1, \ldots, n_k} \binom{n_1 + \cdots + n_k}{n_1, \ldots, n_k} \left(\frac{1-p}{p}\right)^{n_1 + \cdots + n_k} \quad (n \geqslant 0,\ -\infty < p < \infty),$$

where the summation is over all nonnegative integers $n_1, \ldots, n_k$ such that $n_1 + 2n_2 + \cdots + kn_k = n$. Show that

$$\sum_{n=0}^{\infty} a_n^{(k)}(p) = 1 \quad (0 < p < 1).$$

SOLUTIONS

Are You Curious?

H-327 Proposed by James F. Peters, St. John's University, Collegeville, MN (Vol. 19, No. 2, April 1981)

The sequence

$$1,\ 3,\ 4,\ 6,\ 8,\ 9,\ 11,\ 12,\ 14,\ 16,\ 17,$$
$$19,\ 21,\ 22,\ 24,\ 25,\ 27,\ 29,\ 30,\ 32,\ 34,\ 35,\ \ldots$$

was introduced by D. E. Thoro [Advanced Problem H-12, *The Fibonacci Quarterly* 1, no. 1 (April 1963):54]. Dubbed "A curious sequence," the following is a slightly modified version of the defining relation for this sequence suggested by the Editor [*The Fibonacci Quarterly* 1, no. 1 (Dec. 1963):50]: If

$$T_0 = 1,\ T_1 = 3,\ T_2 = 4,\ T_3 = 6,\ T_4 = 8,\ T_5 = 9,\ T_6 = 11,\ T_7 = 12,$$

then

$$T_{8m+k} = 13m + T_k, \text{ where } k \geqslant 0,\ m = 1, 2, 3, \ldots .$$

Assume

$$F_0 = 1,\ F_1 = 1,\ F_{n+1} = F_n + F_{n-1}$$

and

$$L_0 = 2,\ L_1 = 1,\ L_{n+1} = L_n + L_{n-1}$$

and verify the following identities:

$$T_{F_n - 2} = F_{n+1} - 2, \text{ where } n \geqslant 6. \tag{1}$$

For example,

$$T_{F_6 - 2} = T_6 = 11 = F_7 - 2$$
$$T_{F_7 - 2} = T_{11} = 19 = F_8 - 2$$
etc.

$$T_{F_n - 2} - T_{F_{n-2} - 2} = F_n, \text{ where } n \geqslant 6. \tag{2}$$

$$T_{F_n - 2} = F_{n+1} - 2 + L_{n-12}, \text{ where } n \geqslant 15. \tag{3}$$

Solution by Paul S. Bruckman, Concord, CA

We first prove the following explicit formula for T_n:

$$T_n = \left[\frac{13n + 12}{8}\right], \; n = 0, 1, 2, \ldots . \tag{1}$$

Let $U_n = \left[\frac{13n + 12}{8}\right]$. We readily verify that $U_n = T_n$ for $0 \leqslant n \leqslant 7$. Also,

$$U_{8m+k} = \left[\frac{13(8m + k) + 12}{8}\right] = 13m + \left[\frac{13k + 12}{8}\right] = 13m + U_k.$$

Since T_n and U_n satisfy the same recursion and have the same initial values, thereby determining each sequence uniquely, they must coincide. This proves (1).

Next, we will prove the following formula:

$$T_{F_n - 2} = F_{n+1} - 2 + \sum_{k=1}^{m} L_{n-12k}, \; 3 + 12m \leqslant n \leqslant 11 + 12m \tag{2}$$

(if $m = 0$, the sum involving Lucas numbers is considered to vanish). Let

$$G_n = T_{F_n - 2}.$$

Then

$$G_n = \left[\frac{13(F_n - 2) + 12}{8}\right] = \left[\frac{13F_n - 14}{8}\right],$$

or

$$G_n = \left[\frac{13F_n + 2}{8}\right] - 2. \tag{3}$$

Now, using well-known Fibonacci and Lucas identities, it is easy to verify that, for all n,

$$13F_n - 8F_{n+1} = F_7F_n - F_6F_{n+1} = F_{n-6};$$

$$13F_n - 8F_{n+1} - 8L_{n-12} = F_{n-6} - 8L_{n-12} = F_{n-18};$$

$$13F_n - 8F_{n+1} - 8L_{n-12} - 8L_{n-24} = F_{n-18} - 8L_{n-24} = F_{n-30};$$

and, in general,

$$13F_n = 8F_{n+1} + 8\sum_{k=1}^{m} L_{n-12k} + F_{n-6-12m} \text{ (the sum vanishing for } m = 0). \tag{4}$$

Substituting this expression into (3) yields:

$$G_n = F_{n+1} - 2 + \sum_{k=1}^{m} L_{n-12k} + \left[\frac{F_{n-6-12m} + 2}{8}\right], \text{ for all } m, n \geqslant 0. \tag{5}$$

Let $N = n - 6 - 12m$. If $3 + 12m \leqslant n \leqslant 11 + 12m$, then $-3 \leqslant N \leqslant 5$. Hence,

$$-1 = F_{-2} \leqslant F_N \leqslant F_5 = 5 \Rightarrow 1 \leqslant F_N + 2 \leqslant 7 \Rightarrow \left[\frac{F_N + 2}{8}\right] = 0.$$

Thus, for the range $3 + 12m \leqslant n \leqslant 11 + 12m$, the greatest integer term in (5) vanishes, and we are left with (2). It may further be shown that (2) is also valid for $n = 12m + 1$ while, if $n = 12m$ or $12m + 2$, the formula should be reduced by 1 [i.e., the "2" should be replaced by "3" in (2)]. We may therefore obtain an expression which works for *all* values of n:

$$G_n = F_{n+1} - 2 - \chi_n + \sum_{k=1}^{m} L_{n-12k}, \text{ for all } n \geqslant 3 \tag{6}$$

(to avoid negative indices for T_n)

where

$$\chi_n = \begin{cases} 1, & \text{if } n \equiv 0 \text{ or } 2 \pmod{12}; \\ 0, & \text{otherwise}; \end{cases} \quad \text{and } m = [n/12].$$

As a matter of passing interest, we may observe that χ_n may be expressed in terms of familiar functions of n:

$$\chi_n = [n/12] - [(n - 1)/12] + [(n - 2)/12] - [(n - 3)/12]. \tag{7}$$

Furthermore, the sum in (6) may be simplified to the following expression:

$$\sum_{k=1}^{m} L_{n-12k} = \frac{F_{6m}L_{n-6-6m}}{8} \tag{8}$$

The formula in (6) corrects the misstatement of the problem's parts (1) and (3). Thus, part (1) is valid only for $3 \leqslant n \leqslant 11$ and part (3) only for $15 \leqslant n \leqslant 23$ and $n = 13$.

Part (2) of the problem is also false in general. The correct statement of part (2) is as follows:

$$G_n - G_{n-2} = F_n - \theta_n + \sum_{k=1}^{m'} L_{n-1-12k}, \tag{9}$$

where

$$n \geqslant 5;\ \theta_n = \begin{cases} 1, & \text{if } n \equiv 1 \text{ or } 4 \pmod{12}; \\ -1, & \text{if } n \equiv 0 \pmod{12}; \\ 0, & \text{otherwise}; \end{cases} \quad \text{and } m' = [(n - 1)/12].$$

The derivation of (9) is a straightforward consequence of applying (6) and considering the possible residues of (mod 12). Remarks similar to those made after (6) may be made in conjunction with (9). Thus, we see that part (2) of the problem yields the correct formula only for $5 \leqslant n \leqslant 11$.

Also solved by C. Wall and the proposer.

Irrationality

H-328 Proposed by Verner E. Hoggatt, Jr., deceased
(Vol. 19, no. 2, April 1981)

Let θ be a positive irrational number such that $1/\theta + 1/\theta^{j+1} = 1$ ($j \geqslant 1$ and integer). Further, let $A_n = [n\theta]$ and $B_n = [n\theta^{j+1}]$ and $C_n = [n\theta^j]$.

Prove: (a) $A_{C_n} + 1 = B_n$

(b) $A_{C_n+1} - A_{C_n} = 2$

$A_{m+1} - A_m = 1$ ($m \neq C_k$ for any $k > 0$)

(c) $B_n - n$ is the number of A_j's less than B_n.

Solution by Charles R. Wall, Trident Technical College, Charleston, SC

Since $1/\theta + 1/\theta^{j+1} = 1$, $1 = \theta^j(\theta - 1)$ and $1 < \theta < 2$ from elementary considerations.

Now, $n\theta^j - 1 < [n\theta^j] \leqslant n\theta^j$, but the second inequality must be strict, for if $n\theta^j = N$, an integer, then

$$\theta = 1 + 1/\theta^j = 1 + n/N$$

and the left side is irrational but the right side is rational, a contradiction. Thus, $n\theta^j - 1 < [n\theta^j] < n\theta^j$, and multiplying through by $\theta - 1$ yields

$$\begin{aligned} n - 1 < n + 1 - \theta &= n\theta^j(\theta - 1) - (\theta - 1) \\ &< [n\theta^j](\theta - 1) < n\theta^j(\theta - 1) = n. \end{aligned} \tag{$*$}$$

(a) Note that

$$B_n = [n\theta^{j+1}] = [n(\theta^j + 1)] = [n\theta^j + n] = [n\theta^j] + n.$$

Since $C_n = [n\theta^j]$, we have

$$A_{C_n} = [[n\theta^j]\theta] = [[n\theta^j] + [n\theta^j](\theta - 1)] = [n\theta^j] + n - 1$$

by ($*$). Therefore, $1 + A_{C_n} = B_n$ as asserted.

(b) Since $A_1 = 1$, the claim that

$$A_{m+1} - A_m = \begin{cases} 2, & \text{if } m = C_k \\ 1, & \text{otherwise} \end{cases}$$

is equivalent to

$$C_k < m \leqslant C_{k+1} \text{ iff } A_m = m + k,$$

a version we shall prove. Now,

$$A_m - m = [m\theta] - m = [m(\theta - 1)] = [m/\theta^j].$$

Let $k = [m/\theta^j]$:

$$m = k\theta^j + r \text{ with } 0 \leqslant r < \theta^j$$

iff
$$m - \theta^j < [m/\theta^j]\theta^j = k\theta^j \leqslant m$$
iff
$$k\theta^j \leqslant m < (k + 1)\theta^j.$$

Taking integral parts, the last inequality is equivalent to

$$C_k = [k\theta^j] < k\theta^j \leqslant m \leqslant [(k + 1)\theta^j] = C_{k+1},$$

which is to say $C_k < m \leqslant C_{k+1}$.

(c) In (a) we noted that $B_n - n = [n\theta^j] = C_n$. From (a), $1 + A_{C_n} = B_n$, so $C_n = B_n - n$ is the number of A's less than B_n.

Also solved by P. Bruckman and the proposer.

E Gads

H-329 Proposed by Leonard Carlitz, Duke University, Durham, NC (Vol. 19, No. 2, April 1981)

Show that, for s, t nonnegative integers,

$$(1)\quad e^{-x}\sum_k \frac{x^k}{k!}\binom{k}{s}\binom{k}{t} = \sum_k \frac{x^{s+t-k}}{k!(s-k)!(t-k)!}.$$

More generally, show that

$$(2)\quad e^{-x}\sum_k \frac{x^k}{k!}\binom{k+\alpha}{s}\binom{k}{t} = \sum_k \frac{x^{s+t-k}}{(s-k)!t!}\binom{\alpha+t}{k},$$

and

$$(3)\quad e^{-x}\sum_k \frac{x^k}{k!}\binom{k}{s}\binom{k+\beta}{t} = \sum_k \frac{x^{s+t-k}}{s!(t-k)!}\binom{\beta+s}{k}.$$

Solution by the proposer.

$$e^{-x}\sum_{s,t=0} y^s z^t \sum_k \frac{x}{k!}\binom{k}{s}\binom{k}{t} = e^{-x}\sum_{k=0}^{\infty}\frac{x^k}{k!}(1+y)^k(1+z)^k = e^{xy+xz+xyz}$$
$$= \sum_{k,s,t=0}^{\infty}\frac{(xyz)^k y^s z^t}{k!s!t!}$$
$$= \sum_{s,t=0}^{\infty} y^s z^t \sum_k \frac{x^{s+t-k}}{k!(s-k)!(t-k)!}$$

Equating coefficients of $y^s z^t$, we get (1).

To prove (2), we take

$$e^{-x}\sum_k \frac{x^k}{k!}\binom{k+\alpha}{s}\binom{k}{t} = e^{-x}\sum_k \frac{x^k}{k!}\sum_{i=0}^{s}\binom{\alpha}{i}\binom{k}{s-i}\binom{k}{t}$$
$$= \sum_i \binom{\alpha}{i} e^{-x}\sum_k \frac{x^k}{k!}\binom{k}{s-i}\binom{k}{t}$$

$$= \sum_i \binom{\alpha}{i} \sum_k \frac{x^{s+t-k-i}}{k!(s-k-i)!(t-k)!} \qquad \text{[by (1)]}$$

$$= \sum_k \frac{x^{s+t-k}}{(s-k)!} \sum_i \binom{\alpha}{i} \frac{1}{(k-i)!(t-k+i)!}. \qquad (*)$$

The inner sum is equal to

$$\frac{1}{k!(t-k)!} \sum_i \frac{(-k)_i(-\alpha)_i}{i!(t-k+1)_i}$$

$$= \frac{1}{k!(t-k)!} \frac{(\alpha+t-k+1)_k}{(t-k+1)_k} \quad \text{(by Vandermonde's theorem)}$$

$$= \frac{1}{t!}\binom{\alpha+t}{k}.$$

Thus (*) becomes

$$\sum_k \frac{x^{s+t-k}}{(s-k)!t!}\binom{\alpha+t}{k},$$

which proves (2).

The proof of (3) is exactly the same.

REMARK: It does not seem possible to get a simple result for

$$e^{-x} \sum_k \frac{x^k}{k!}\binom{k+\alpha}{s}\binom{k+\beta}{t}.$$

It can be proved that this is equal to the triple sum

$$\sum_{i,j,k} \frac{x^{s+t-k}}{(k-i-j)!(s-k+j)!(t-k+i)!}\binom{\alpha}{i}\binom{\beta}{j}$$

Also solved by P. Bruckman.

O Rats

H-330 Proposed by Verner E. Hoggatt, Jr., deceased (Vol. 19, No. 4, October 1981)

If θ is a positive irrational number and $1/\theta + 1/\theta^3 = 1$, $A_n = [n\theta]$, $B_n = [n\theta^3]$, $C_n = [n\theta^2]$, then prove or disprove:

$$A_n + B_n + C_n = C_{B_n}.$$

Solution by Paul S. Bruckman, Sacramento, CA

The assertion is false, the first counterexample occurring for $n = 13$. The equation defining θ is equivalent to the cubic: $\theta^3 = \theta^2 + 1$, which has only one real solution:

(1) $\theta = \frac{1}{3}(U + V + 1)$, where $U = \left(\frac{1}{2}(29 + 3\sqrt{93})\right)^{1/3}$, $V = \left(\frac{1}{2}(29 - 3\sqrt{93})\right)^{1/3}$;

thus,

(2) $\theta \doteq 1.4655712,\ \theta^2 \doteq 2.1478989,\ \theta^3 \doteq 3.1478989.$

We find readily that $A_{13} = 19$, $B_{13} = 40$, $C_{13} = 27$, $C_{B_{13}} = C_{40} = 85$; thus

$$A_{13} + B_{13} + C_{13} = 86 \neq 85 = C_{B_{13}}.$$

It is conjectured that the assertion is true for infinitely many n, however. It is further conjectured that $C_{B_n} - (A_n + B_n + C_n) = 0$ or 1 for all n, each occurrence occurring infinitely often, but with "zero" predominating. A proof of this conjecture was not attempted, since it was not required in the solution of the problem; it will probably depend upon the property that $(A_n)_{n=1}^{\infty}$ and $(B_n)_{n=1}^{\infty}$ partition the natural numbers, and moreover, $B_n = C_n + n$ (both properties readily proved). It is easy to show that

$$|C_{B_n} - (A_n + B_n + C_n)| \leqslant 2 \text{ for all } n,$$

the proof of which depends solely on the properties of the greatest integer function.

Barely There

H-331 Proposed by Andreas N. Philippou, American Univ. of Beirut, Lebanon (Vol. 19, No. 4, October 1981)

For each fixed integer $k \geqslant 2$, define the k-Fibonacci sequence $\left\{f_n^{(k)}\right\}_{n=0}^{\infty}$ by $f_0^{(k)} = 0$, $f_1^{(k)} = 1$, and

$$f_n^{(k)} = \begin{cases} f_{n-1}^{(k)} + \cdots + f_0^{(k)} & \text{if } 2 \leqslant n \leqslant k \\ f_{n-1}^{(k)} + \cdots + f_{n-k}^{(k)} & \text{if } n \geqslant k+1. \end{cases}$$

Letting $\alpha = (1 + \sqrt{5})/2$, show:

(a) $f^{(k)} > \alpha^{n-2}$ if $n \geqslant 3$;

(b) $\left\{f^{(k)}\right\}_{n=2}^{\infty}$ has Schnirelmann density 0.

Solution by Paul S. Bruckman, Sacramento, CA

We see that $f_3^{(k)} = 2$ for all $k \geqslant 2$, and $f_n^{(k)} \geqslant F_n + 1$ for all $k \geqslant 3$ and $n \geqslant 4$. Since $2 > \alpha$ and $4 > \alpha$, we see that (a) holds for $n = 3$ and $n = 4$. Also,

$$45 < 49 \Rightarrow 3\sqrt{5} < 7 \Rightarrow 3\sqrt{5} - 5 < 2 \Rightarrow 5^{-1/2} > \tfrac{1}{2}(3 - \sqrt{5}) = 1 + \beta = \beta^2.$$

Therefore, if $n \geqslant 5$,

$$f_n^{(k)} \geqslant F_n + 1 = 5^{-1/2}(\alpha^n - \beta^n) + 1 > \beta^2(\alpha^n - \beta^n) + 1$$
$$= \alpha^{n-2} + 1 - \beta^{n+2} > \alpha^{n-2}.$$

Hence (a) is true for all $n \geqslant 3$. Q.E.D.

We recall the definition of the Schnirelmann density of a set A of nonnegative integers. If $A(n)$ denotes the number of positive integers in A that are less than or equal to n, then the Schnirelmann density $d(A)$ is given by: $d(A) = \inf\limits_{n \geqslant 1} A(n)/n$.

Let $f^{(k)} = (f_n^{(k)})_{n=0}^{\infty}$ and $A_n^{(k)}$ be the number of positive integers in $f^{(k)}$ that are $\leqslant n$. Since $f_n^{(k)} \geqslant f_n^{\,2}$ for all n and $k \geqslant 2$, it is clear that

$$A_n^{(k)} \leqslant A_n^{(2)};$$

hence $d(f^{(k)}) \leqslant d(f^{(2)})$. It therefore suffices to show that $d(f^{(2)}) = 0$.

Now $A_1^{(2)} = 1$ and $\frac{1}{2}A_2^{(2)} = 1$ (since $F_2 = 1$, $F_3 = 2$, and $f^{(2)}$ is an increasing sequence. Generally, it may be shown that

$$A_n^{(2)} = \left[\frac{\log(1 + n\sqrt{5})}{\log \alpha}\right] - 1.$$

Therefore,

$$d(f^{(2)}) = \inf_{n \geqslant 1}\left\{n^{-1}\left(\left[\frac{\log(1 + n\sqrt{5})}{\log \alpha}\right] - 1\right)\right\} \leqslant \inf_{n \geqslant 1}\left\{n^{-1}\left(\frac{\log(1 + n\sqrt{5})}{\log \alpha} - 1\right)\right\}$$

$$\leqslant \inf_{n \geqslant 1}\left\{n^{-1}\,\frac{\log 2n\alpha}{\log \alpha}\right\} \leqslant \inf_{n \geqslant 3}\left\{\frac{2}{\log \alpha}\cdot\frac{\log n}{n}\right\}.$$

Note that $\log z/z$ is a decreasing function for $z \geqslant 3$ and approaches zero as $z \to \infty$ (z real). Hence,

$$\inf_{z \geqslant 3}(\log z/z) = 0.$$

It follows that $d(f^{(2)}) = 0$. Q.E.D.

Also solved by the proposer.

*****

VOLUME INDEX

SUSTAINING MEMBERS

*H.L. Alder
J. Arkin
B.I. Arthur, Jr.
Leon Bankoff
Murray Berg
J.G. Bergart
G. Bergum
George Berzsenyi
*M. Bicknell-Johnson
Clyde Bridger
J.L. Brown, Jr.
P.S. Bruckman
P.F. Byrd
L. Carlitz
G.D. Chakerian
R.M Chamberlain, Jr.
P.J. Cocuzza
Commodity Advisory Corp. of Texas
J.W. Creely
P.A. DeCaux
M.J. DeLeon
James Desmond
Harvey Diehl
J.L. Ercolano
D.R. Farmer
F.F. Frey, Jr.
C.L. Gardner
R.M. Giuli
*H.W. Gould
W.E. Greig
V.C. Harris
H.E. Heatherly
A.P. Hillman
*A.F. Horadam
R.J. Howell
R.P. Kelisky
C.H. Kimberling
Joseph Lahr
*C.T. Long
*James Maxwell
R.K. McConnell, Jr.
*Sr. M. DeSales McNabb
Leslie Miller
M.G. Monzingo
F.J. Ossiander
E.D. Robinson
J.A. Schumaker
D. Singmaster
John Sjoberg
M.N.S. Swamy
L. Taylor
*D. Thoro
H.L. Umansky
R. Vogel
C.C. Volpe
Marcellus Waddill
*L.A. Walker
J.E. Walton
R.E. Whitney
B.E. Williams
E.L. Yang

*Charter Members

INSTITUTIONAL MEMBERS

THE BAKER STORE EQUIPMENT COMPANY
Cleveland, Ohio

CALIFORNIA STATE POLY UNIVERSITY, POMONA
Pomona, California

CALIFORNIA STATE UNIVERSITY, SACRAMENTO
Sacramento, California

INDIANA UNIVERSITY
Bloomington, Indiana

ORION ENTERPRISES
Cicero, Illinois

REED COLLEGE
Portland, Oregon

SAN JOSE STATE UNIVERSITY
San Jose, California

SCIENTIFIC ENGINEERING INSTRUMENTS, INC.
Sparks, Nevada

SONOMA STATE UNIVERSITY
Rohnert Park, California

TRI STATE UNIVERSITY
Angola, Indiana

UNIVERSITY OF SANTA CLARA
Santa Clara, California

UNIVERSITY OF SCRANTON
Scranton, Pennsylvania

UNIVERSITY OF TORONTO
Toronto, Canada

WASHINGTON STATE UNIVERSITY
Pullman, Washington

BOOKS AVAILABLE THROUGH THE FIBONACCI ASSOCIATION

Introduction to Fibonacci Discovery by Brother Alfred Brousseau. Fibonacci Association (FA), 1965.

Fibonacci and Lucas Numbers by Verner E. Hoggatt, Jr. FA, 1972.

A Primer For the Fibonacci Numbers. Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1972

Fibonacci's Problem Book. Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1974.

The Theory of Simply Periodic Numerical Functions by Edouard Lucas. Translated from the French by Sidney Kravitz. Edited by Douglas Lind. FA, 1969.

Linear Recursion and Fibonacci Sequences by Brother Alfred Brousseau. FA, 1971.

Fibonacci and Related Number Theoretic Tables. Edited by Brother Alfred Brousseau. FA, 1972.

Number Theory Tables. Edited by Brother Alfred Brousseau. FA, 1973.

Recurring Sequences by Dov Jarden. Third and enlarged edition. Riveon Lematematika, Israel, 1973.

Tables of Fibonacci Entry Points, Part One. Edited and annotated by Brother Alfred Brousseau. FA, 1965.

Tables of Fibonacci Entry Points, Part Two. Edited and annotated by Brother Alfred Brousseau. FA, 1965.

A Collection of Manuscripts Related to the Fibonacci Sequence — 18th Anniversary Volume. Edited by Verner E. Hoggatt, Jr. and Marjorie Bicknell-Johnson. FA, 1980.

Please write to the Fibonacci Association, University of Santa Clara, CA 95053, U.S.A., for current prices.