The Fibonacci Quarterly

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

TABLE OF CONTENTS

VOLUME 27 JUNE-JULY 1989 NUMBER 3

PURPOSE

The primary function 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, challenging problems, and innovative proofs of old ideas.

EDITORIAL POLICY

THE FIBONACCI 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 new ideas that develop enthusiasm for number sequences or the exploration of number facts. Illustrations and tables should be wisely used to clarify the ideas of the manuscript. Unanswered questions are encouraged, and a complete list of references is absolutely necessary.

SUBMITTING AN ARTICLE

Articles should be submitted in the format of the current issues of the **THE FIBONACCI QUARTERLY.** They should be typewritten or reproduced typewritten copies, that are clearly readable, double spaced with wide margins and on only one side of the paper. 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 print.

Two copies of the manuscript should be submitted to: **GERALD E. BERGUM, EDITOR, THE FIBONACCI QUARTERLY, DEPARTMENT OF COMPUTER SCIENCE, SOUTH DAKOTA STATE UNIVERSITY, BOX 2201, BROOKINGS, SD 57007-0194.**

Authors are encouraged to keep a copy of their manuscripts for their own files as protection against loss. The editor will give immediate acknowledgment of all manuscripts received.

SUBSCRIPTIONS, ADDRESS CHANGE, AND REPRINT INFORMATION

Address all subscription correspondence, including notification of address change, to: **RICHARD VINE, SUBSCRIPTION MANAGER, THE FIBONACCI ASSOCIATION, SANTA CLARA UNIVERSITY, SANTA CLARA, CA 95053.**

Requests for reprint permission should be directed to the editor. However, general permission is granted to members of The Fibonacci Association for noncommercial reproduction of a limited quantity of individual articles (in whole or in part) provided complete reference is made to the source.

Annual domestic Fibonacci Association membership dues, which include a subscription to **THE FIBONACCI QUARTERLY,** are $30 for Regular Membership, $40 for Sustain Membership, and $67 for Institutional Membership; foreign rates, which are based on international mailing rates, are somewhat higher than domestic rates; please write for details. **THE FIBONACCI 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.** Reprints can also be purchased from **UMI CLEARING HOUSE** at the same address.

The Fibonacci Quarterly

Founded in 1963 by Verner E. Hoggatt, Jr. (1921-1980)
and Br. Alfred Brousseau (1907-1988)

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

SOME NEW RESULTS ON QUASI-ORTHOGONAL NUMBERS

Selmo Tauber
Portland State University, Portland, OR 97201
(Submitted April 1987)

1. Introduction

As far as is known to this author, the term "Quasi-Orthogonality" was first introduced by K. S. Miller in [1]:

Given two sets of numbers $A(m, n)$ and $B(m, n)$ such that $m, n, s \in Z$, and $A(m, n)$, $B(m, n) = 0$ for $n < 0$, $m < 0$, and $n < m$, they are said to be quasi-orthogonal to each other if

$$\sum_{s=m}^{n} A(s, n)B(m, s) = \delta(m, n) \tag{1}$$

where $\delta(m, n)$ is the Kronecker delta.

Equivalently, we can say that if $A(n)$ is the square, and triangular matrix of elements $A(m, n)$ of n rows, and $B(n)$ the square and triangular matrix of elements $B(m, n)$ of n rows, then

$$A(n)B(n) = I, \tag{2}$$

i.e., the two matrices are inverse of each other.

H. W. Gould has compared the different aspects of quasi-orthogonality and studied some of its properties [2].

In this paper we shall be concerned with the so-called BILINEARLY RECURRENT orthogonal numbers, i.e., numbers satisfying recurrence relations of the form:

$$A(m, n) = f_1(m, n)A(m - 1, n - 1) + f_2(m, n)A(m, n - 1); \tag{3}$$

$$B(m, n) = f_3(m, n)B(m - 1, n - 1) + f_4(m, n)B(m, n - 1). \tag{4}$$

The problem to solve is the following: knowing f_1 and f_2, find f_3 and f_4, or, since the problem is symmetric, knowing f_3 and f_4, find f_1 and f_2.

So far, only the following cases have been studied:

Case 1: $f_1 = N(n)$, $f_2 = M(n)$,

$f_3 = 1/[N(m + 1)]$, $f_4 = -M(m + 1)/[N(m + 1)]$. Cf. [3].

Case 2: $f_1 = P(m)$, $f_2 = K(n) + M(m + 1)$,

$f_3 = 1/P(n)$, $f_4 = -[K(m + 1) + M(n)]/P(n)$. Cf. [3].

Other cases of quasi-orthogonal numbers have been studied but they are not of the bilinearly recurrent kind.

The final aim is to obtain a general case where the functions f_i are all of the form $f_i(m, n)$. This result has thus far been impossible to reach.

In this paper we study

Case 3: $f_1(m, n) = \alpha(m)\beta(n)$, $f_2(m, n) = \eta(n)$,

$f_3(m, n) = 1/\alpha(n)\beta(m)$, $f_4(m, n) = -\eta(m + 1)/\alpha(n)\beta(m + 1)$.

2. P-Polynomials and A-Numbers

Let J be the set of positive numbers and zero, i.e., $J = [0, Z^+]$. We assume that $m, n, k, s \in J$, and that $a(m, n)$, $b(m)$, and $c(m)$ are defined, and not equal to zero, also that $x > 0$.

Consider the polynomial

$$P(n, x) = \sum_{m=0}^{n} a(m, n)A(m, n)x^m = \prod_{k=1}^{n} [b(k) + c(k)x], \tag{5}$$

so that

$$\begin{aligned} P(n+1, x) &= \sum_{m=0}^{n+1} a(m, n+1)A(m, n+1)x^m \\ &= \prod_{k=1}^{n+1} [b(k) + c(k)x] = [b(n+1) + c(n+1)x]P(n, x) \\ &= [b(n+1) + c(n+1)x] \sum_{m=0}^{n} a(m, n)A(m, n)x^n. \end{aligned} \tag{6}$$

By comparing the coefficients of x^{m+1}, we obtain

$$\begin{aligned} a(m+1, n+1)A(m+1, n+1) &= c(n+1)a(m, n)A(m, n) \\ &\quad + b(n+1)a(m+1, n)A(m+1, n) \end{aligned}$$

or, since $a(m+1, n+1) \neq 0$,

$$\begin{aligned} A(m+1, n+1) &= c(n+1)\frac{a(m, n)}{a(m+1, n+1)} A(m, n) \\ &\quad + b(n+1)\frac{a(m+1, n)}{a(m+1, n+1)} A(m+1, n), \end{aligned}$$

or again,

$$\begin{aligned} A(m, n) &= c(n)\frac{a(m-1, n-1)}{a(m, n)} A(m-1, n-1) \\ &\quad + b(n)\frac{a(m, n-1)}{a(m, n)} A(m, n-1). \end{aligned} \tag{7}$$

This is the recurrence relation for the numbers $A(m, n)$.

3. B-Numbers

We express x^n in terms of P-polynomials as defined in Section 2, thus

$$\begin{aligned} x^n &= \sum_{s=0}^{n} \lambda(s, n)B(s, n)P(s, x) \\ &= \sum_{s=0}^{n} \lambda(s, n)B(s, n)\left[\sum_{m=0}^{n} a(m, s)A(m, s)x^m\right], \end{aligned} \tag{8}$$

where the numbers $\lambda(s, n)$ are defined, and different from zero, for $s, n \in J$, and $B(s, n)$ satisfy the conditions of Section 1.

It follows that

$$\begin{aligned} x^n &= \sum_{s=0}^{n} \sum_{m=0}^{s} \lambda(s, n)a(m, s)B(s, n)A(m, s)x^m \\ &= \sum_{m=0}^{n} x^m\left[\sum_{s=m}^{n} \lambda(s, n)a(m, s)B(s, n)A(m, s)\right], \end{aligned} \tag{9}$$

which shows that the quantity in brackets, i.e., the coefficient of x^m must be equal to δ_m^n.

To assure the quasi-orthogonality of the numbers $A(m, s)$ and $B(s, n)$ it is necessary to assume that

$$\lambda(s, n)a(m, s) = 1. \tag{10}$$

This result can be obtained in the following way:

For $m = n$, we take $\lambda(s, n)a(n, s) = 1$, i.e., $\lambda(s, n) = 1/a(n, s)$.

For $m \neq n$, i.e., for $m < n$, it is necessary to write

$$a(m, s) = a_1(m)a_2(s), \ \lambda(s, n) = \lambda_1(s)\lambda_2(n),$$

with $\lambda_1(s) = 1/a_2(s)$, so that

$$\lambda(s, n)a(m, s) = \lambda_2(n)a_1(m),$$

which, substituted into (9), gives

$$\begin{aligned} x^n &= \sum_{m=0}^{n} \lambda_2(n)a_1(m)x^m \left[\sum_{s=m}^{n} B(s, n)A(m, s)\right] \\ &= \sum_{m=0}^{n} \lambda_2(n)a_1(m)x^m\delta_m^n, \end{aligned} \tag{9a}$$

which is satisfied if $\lambda_2(n) = 1/a_1(n)$.

We summarize this result by writing

$$\lambda(s, n) = [1/a_2(s)]\lambda_2(n),$$

or

$$\lambda(s, n) = 1/a(n, s) = 1/a_1(n)a_2(s).$$

Under these conditions, clearly (9) can be written as

$$x^n = \sum_{m=0}^{n} x^m\delta_n^m \tag{11}$$

and

$$\sum_{s=m}^{n} B(s, n)A(m, s) = \delta_n^m. \tag{12}$$

On the other hand,

$$x^{n+1} = x^n \cdot x = \left[\sum_{s=0}^{n} \lambda(s, n)B(s, n)P(s, x)\right]x. \tag{12a}$$

Since, according to (6),

$$P(s + 1, x) = [b(s + 1 + c(s + 1)x]P(s, n), \tag{13}$$

it follows that

$$xP(s, x) = [P(s + 1, x) - b(s + 1)P(s, x)]/c(s + 1) \tag{14}$$

so that, substituting into (12a), we obtain

$$\begin{aligned} x^{n+1} &= \sum_{s=0}^{n} \lambda(s, n)B(s, n)\left[\frac{P(s + 1, x)}{c(s + 1)} - \frac{b(s + 1)}{c(s + 1)} P(s, x)\right] \\ &= \sum_{s=0}^{n+1} \lambda(s, n + 1)B(s, n + 1)P(s, x). \end{aligned} \tag{15}$$

Comparing the coefficients of $P(s + 1, x)$, we see that

$$\lambda(s + 1, n + 1)B(s + 1, n + 1) = \frac{\lambda(s, n)}{c(s + 1)} B(s, n) - \frac{\lambda(s + 1, n)b(s + 2)}{c(s + 2)} B(s + 1, n) \tag{16}$$

or

$$B(s + 1, n + 1) = \frac{\lambda(s, n)}{\lambda(s + 1, n + 1)c(s + 1)} B(s, n) - \frac{\lambda(s + 1, n)b(s + 2)}{\lambda(s + 1, n + 1)c(s + 2)} B(s + 1, n), \tag{17}$$

or again,

$$B(s, n) = \frac{\lambda(s - 1, n - 1)}{\lambda(s, n)c(s)} B(s - 1, n - 1) - \frac{\lambda(s, n - 1)b(s + 1)}{\lambda(s, n)c(s + 1)} B(s, n - 1). \tag{18}$$

Equation (18) is a first form of the recurrence relation for the B-numbers.

4. Evaluation of $a(m, n)$

According to (4) and (7), we can write:

$$c(n)\frac{a(m - 1, n - 1)}{a(m, n)} = f_1(m, n); \tag{19}$$

$$b(n)\frac{a(m, n - 1)}{a(m, n)} = f_2(m, n). \tag{20}$$

From (20), we deduce

$$\begin{aligned} b(n)a(m, n - 1) &= f_2(m, n)a(m, n) \\ b(n - 1)a(m, n - 2) &= f_2(m, n - 1)a(m, n - 1) \\ b(n - 2)a(m, n - 3) &= f_2(m, n - 2)a(m, n - 2) \\ &\vdots \\ b(2)a(m, 1) &= f_2(m, 2)a(m, 2) \end{aligned}$$

and multiplying through and simplifying,

$$\left[\prod_{k=2}^{n} b(k)\right] a(m, 1) = a(m, n)\left[\prod_{k=2}^{n} f_2(m, k)\right]$$

or

$$a(m, n) = a(m, 1)\left[\prod_{k=2}^{n} \frac{b(k)}{f_2(m, k)}\right] \tag{21}$$

and

$$a(m - 1, n - 1) = a(m - 1, 1)\left[\prod_{k=2}^{n-1} b(k)/f_2(m - 1, k)\right]. \tag{22}$$

Substituting (21) and (22) into (19), we obtain

$$c(n)a(m - 1, 1)\left[\prod_{k=2}^{n-1} b(k)/f_2(m - 1, k)\right]$$

$$= a(m, 1)\left[\prod_{k=2}^{n} b(k)/f_2(m, k)\right] f_1(m, n)$$

which, after simplification, gives

$$a(m, 1) = a(m - 1, 1)[c(n)/b(n)]$$

$$\cdot \left[\prod_{k=2}^{n-1} f_2(m, k)/f_2(m - 1, k)\right][f_2(m, n)/f_1(m, n)] \tag{23}$$

or

$$a(m, 1) = a(m - 1, 1)\Omega(m), \tag{24}$$

since the left-hand member of (23) is independent of n, i.e.,

$$\Omega(m) = [c(n)/b(n)]\left[\prod_{k=2}^{n-1} f_2(m, k)/f_2(m - 1, k)\right][f_2(m, n)/f_1(m, n)]. \tag{25}$$

To eliminate n in the right-hand member of (25), we assume that

$$f_1(m, n) = \alpha(m)\beta(n), \text{ and } f_2(m, n) = \delta(m)\eta(n).$$

Equation (25) can then be written as

$$\Omega(m) = [c(n)/b(n)][\delta(m)/\delta(m - 1)]^{n-2}[\delta(m)\eta(n)/\alpha(m)\beta(n)].$$

In order to have the right-hand side independent of n, it is necessary to assume that

$$[c(n)/b(n)][\eta(n)/\beta(n)] = A = \text{Const.}, \tag{26}$$

and

$$\delta(m)/\delta(m - 1) = 1, \tag{27}$$

i.e., $\delta(m) = B =$ Const. We may also assume that $A = B = 1$, i.e.,

$$f_2(m, n) = f_2(n) = \eta(n), \tag{28}$$

$$[c(n)/b(n)][\eta(n)/\beta(n)] = 1. \tag{29}$$

It follows that $\Omega(m) = 1/\alpha(m)$ and, returning to (24), we can write

$$\begin{aligned} a(m, 1) &= a(m - 1)/\alpha(m) \\ a(m - 1, 1) &= a(m - 2)/\alpha(m - 1) \\ a(m - 2, 1) &= a(m - 3)/\alpha(m - 2) \\ &\vdots \\ a(2, 1) &= a(1, 1)/\alpha(2), \end{aligned}$$

and multiplying through, we obtain

$$a(m, 1) = a(1, 1)\left[\prod_{j=2}^{m} 1/\alpha(j)\right]. \tag{30}$$

Substituting (30) into (21), we obtain

$$a(m, n) = a(m, 1)\prod_{k=2}^{n} b(k)/f_2(m, k) = a(1, 1)\prod_{j=2}^{m}\frac{1}{\alpha(j)}\prod_{k=2}^{n}\frac{b(k)}{\eta(k)}. \tag{31}$$

In the following examples we shall show how the results so obtained can be used to solve the proposed problem.

5. Example I

Given $A(m+1, n+1) = mnA(m, n) + A(m+1, n)$, which we rewrite in the form of (4),

$$A(m, n) = (m-1)(n-1)A(n-1, n-1) + A(m, n-1),$$

so that $f_1 = (m-1)(n-1)$, i.e., $\alpha(m) = m-1$, $\beta(n) = n-1$, $f_2 = \eta(n) = 1$.

Equation (26) gives

$$c(n)/b(n) = \beta(n)/\eta(n) = n-1,$$

and from (31) we obtain, with $a(1, 1) = 1$,

$$a(m, n) = \prod_{j=2}^{m} \frac{1}{j-1} \prod_{k=2}^{n} b(k) = X(n)/(m-1)!, \quad X(n) = \prod_{k=2}^{n} b(k).$$

From (10), it follows that, since $\lambda(s, n)a(m, s) = 1$,

$$\lambda(s, n) = (n-1)!/X(s).$$

From (18), we obtain

$$\begin{aligned} f_3 &= \lambda(s-1, n-1)/\lambda(s, n)c(s) \\ &= [(n-2)!/X(s-1)][X(s)/(n-1)!c(s)]. \end{aligned}$$

As we have shown in this example, $c(n)/b(n) = n-1$, so $c(n) = (n-1)b(n)$ and $f_3 = 1/(n-1)(s-1)$. Again, from (18), we obtain $f_4 = -1/s(n-1)$. It follows that the B-numbers satisfy the relation

$$B(s, n) = [1/(n-1)(s-1)]B(s-1, n-1) - [1/(n-1)s]B(s, n-1).$$

For $A(1, 1) = B(1, 1) = 1$, we present a table of the A- and B-numbers:

	$A(m, n)$					$B(m, n)$				
$n \backslash m$	1	2	3	4	5	1	2	3	4	5
1	1					1				
2	1	1				-1	1			
3	1	3	4			$\frac{1}{2}$	$-\frac{3}{4}$	$\frac{1}{4}$		
4	1	6	22	36		$-\frac{1}{6}$	$\frac{7}{24}$	$-\frac{11}{72}$	$\frac{1}{36}$	
5	1	10	70	300	576	$\frac{1}{24}$	$-\frac{5}{64}$	$\frac{85}{1728}$	$\frac{-25}{1728}$	$\frac{1}{576}$

6. Evaluation of f_3 and f_4

As we have seen in Section 4, it is necessary to assume that

$$f_1(m, n) = \alpha(m)\beta(n) \quad \text{and} \quad f_2(m, n) = \eta(n).$$

From (31), $a(m, n)$, and (10) and its consequences, it follows that $\lambda(s, n) = 1/a(n, s)$. Thus

$$\lambda(s, n) = \left[\prod_{j=2}^{n} \alpha(j)\right]\left[\prod_{k=2}^{n} \eta(k)/b(k)\right]. \tag{32}$$

Then it follows from (18) that

$$f_3(s, n) = \lambda(s - 1, n - 1)/\lambda(s, n)c(s) = 1/\alpha(n)\beta(s) \tag{33}$$

and

$$f_4(s, n) = -\lambda(s, n - 1)b(s + 1)/\lambda(s, n)c(s + 1)$$
$$= -\eta(s + 1)/\alpha(n)\beta(s + 1). \tag{34}$$

The results of Example I can be checked easily using (33) and (34).

7. Example II

Given

$$A(m + 1, n + 1) = \frac{n^2}{m} A(m, n) + A(m + 1, n).$$

We rewrite this in the form of (3), i.e.,

$$A(m, n) = [(n - 1)^2/(m - 1)]A(m - 1, n - 1) + A(m, n - 1).$$

It follows that

$$f_1(m, n) = \alpha(m)\beta(n) = (n - 1)^2/(m - 1),$$
$$f_2 = 1,$$
$$f_3(m, n) = (n - 1)/(m - 1)^2,$$

and

$$f_4(m, n) = -(n - 1)/m^2,$$

so that

$$B(m, n) = [(n - 1)/(m - 1)^2]B(m - 1, n - 1) - [(n - 1)/m^2]B(m, n - 1).$$

For $A(1, 1) = 1$, we give here the values of the A- and B-numbers for $m, n \le 5$.

	$A(m, n)$					$B(m, n)$				
$n \backslash m$	1	2	3	4	5	1	2	3	4	5
1	1					1				
2	1	1				-1	1			
3	1	5	2			2	$-\frac{5}{2}$	$\frac{1}{2}$		
4	1	14	$\frac{49}{2}$	6		-6	$\frac{63}{8}$	$-\frac{49}{24}$	$\frac{1}{6}$	
5	1	30	$\frac{273}{2}$	$\frac{410}{3}$	24	24	$-\frac{255}{8}$	$\frac{1897}{216}$	$-\frac{205}{216}$	$\frac{1}{24}$

References

1. K. S. Miller. *An Introduction to the Calculus of Finite Differences, and Difference Equations*. New York, 1960.
2. H. W. Gould. "The Construction of Orthogonal and Quasi-Orthogonal Number Sets." *Amer. Math. Monthly* 72 (1965):591-602.
3. S. Tauber. "On Quasi-Orthogonal Numbers." *Amer. Math. Monthly* 69 (1962): 365-372.

*****

PROBABILISTIC ALGORITHMS FOR TREES

Bruce E. Sagan
Michigan State University, East Lansing, MI 48824-1027

Yeong-Nan Yeh
Academica Sinica Nanking, Taipei, Taiwan, R.O.C.
(Submitted April 1987)

1. Introduction and Definitions

A *rooted tree*, τ, is a partially ordered set whose Hasse diagram is a tree (in the graph-theoretic sense of the term) having a unique minimal element called the *root*, see Figure 1a. If $|\tau| = n$, a *natural labeling* of τ is a bijection T: $\tau \to \{1, 2, \ldots, n\}$ such that $v < w$ in τ implies $T(v) < T(w)$. One such labeling is given in Figure 1b. In this case, we say T has *shape* τ. We let f_τ represent the number of natural labelings of τ.

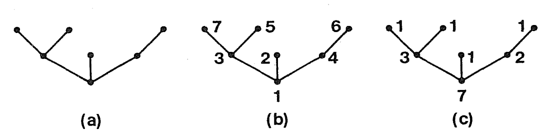
The *hook* of a node $v \in \tau$ is

$$H_v = \{w \in \tau \mid w \geq v\}$$

with corresponding *hooklength* $h_v = |H_v|$. The hooklengths of our example tree are displayed in Figure 1c. The well-known hook formula [3] for the number of natural labelings states that

$$f_\tau = n! \Big/ \prod_{v \in \tau} h_v. \tag{1.1}$$

Thus, in our example $f_\tau = 7!/(7)(3)(2)(1)^4 = 120$.



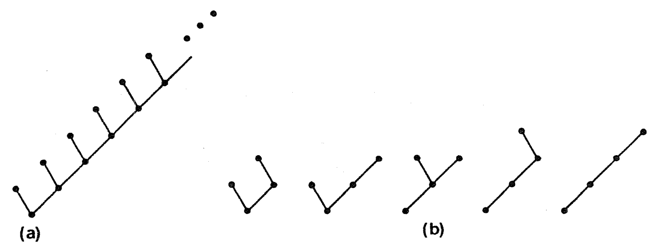
A tree, a labeling and the hooklengths

FIGURE 1

In Section 2 we will give a simple probabilistic proof of (1.1) inspired by an algorithm of Greene, Nijenhuis, and Wilf [1] for standard Young tableaux. The tree version has previously appeared in [5], but is included here for completeness. An algorithmic derivation of the hook-generating function for reverse tree partitions [which specializes to (1.1) as the variable approaches 1] can be found in [6].

A *Fibonacci tree* [9] is a finite lower-order ideal of the infinite poset in Figure 2a. The name derives from the easily proved fact that the number of Fibonacci trees with n nodes is the n^{th} Fibonacci number. For example, Figure 2b shows the five Fibonacci trees with four nodes. Let $\mathscr{F}_n$ be the set of all Fibonacci trees with n nodes, then

$$\sum_{\tau \in \mathscr{F}_n} f_\tau^2 = n! \qquad (1.2$$



Fibonacci trees

FIGURE 2

Formula (1.2) has a bijective proof due to Bender (reported in [9]). I Sections 3 and 4 below we will give two constructions that build a labeled tre $\tau \in \mathscr{F}_n$ with probability $f_\tau^2/n!$, thus proving (1.2) twice. The first algorith constructs the tree "from without" as done for tableaux in another paper o Greene et al. [2]. The second builds the tree "from within" and is based o work of Pittel [4].

2. Choosing a Labeling Uniformly

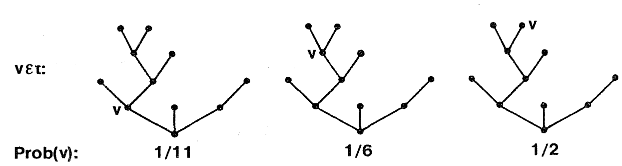
Let τ be a fixed shape with n nodes. The following algorithm can be use to choose a labeling of τ.

GNW1. Pick a node $v \in \tau$ uniformly at random, i.e., with probability $1/n$.

GNW2. If v is maximal (a leaf), then let $T(v) = n$ and return to GNW1 wit τ and n replaced by $\tau - \{v\}$ and $n - 1$, respectively (unless there are no node left, in which case the algorithm halts).

GNW3. If v is not maximal, then choose a different node $w \in H_v$ uniforml at random, i.e., with probability $1/(h_v - 1)$, and return to GNW2 with w in th role of v.

A sequence of nodes generated in the process of finding a vertex to b labeled (in this case by the loop between GNW2 and GNW3) is called a *trial*. A example of a typical trial is given in Figure 3.



A GNW trial

FIGURE 3

Theorem 1: If τ is a fixed rooted tree with n nodes, then GNW1-3 produce al labelings of τ uniformly at random. In fact, the probability of any give labeling is

$$\prod_{v \in \tau} h_v / n!$$

Proof: Let w be any maximal element of τ and let W be the set of vertices c the unique path from w to the root of τ (excluding w itself). Note that the:

are the only vertices whose hooklengths are changed if w is removed from τ during GNW2. Therefore, by induction, it suffices to show that the probability that w gets label n is

$$\begin{aligned} P(w) &= (1/n)\prod_{v \in W} h_v/(h_v - 1) \\ &= (1/n)\prod_{v \in W}\left(1 + \frac{1}{h_v - 1}\right). \end{aligned}$$

But $1/n$ is the probability of choosing an initial node and each term in the expansion of the product corresponds to the probability of a unique trial ending in w. □

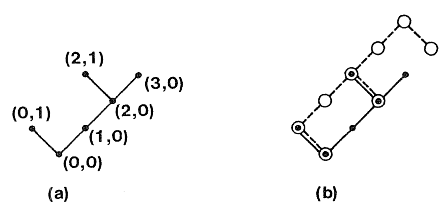
As an immediate corollary we have

Corollary 2: The number of labelings of a given tree τ with n nodes is

$$f_\tau = n! \Big/ \prod_{v \in \tau} h_v. \quad \Box$$

3. Fibonacci Trees Grown from Without

It will be convenient to introduce coordinates for the infinite tree of Figure 2a. Let the nodes of the "spine" be $(i, 0)$ for $i = 0, 1, 2, \ldots$ while the leaves are denoted by $(i, 1)$ for the same range of i. Now, any Fibonacci tree can be specified by its coordinates as is done in Figure 4a.



Coordinates and the associated tree

FIGURE 4

Given any vertex $v = (i, j)$, then v has *associate* $v' = (i, 1 - j)$. If τ is a Fibonacci tree with spine of length s, then the *associated tree* is

$$\tau' = \{v = (i, j) \mid v' \in \tau \text{ or } i = s + 1\};$$

see Figure 4b where the associated tree's nodes are the open circles. Note that τ' is "upside down" with root $r = (s + 1, 1)$.

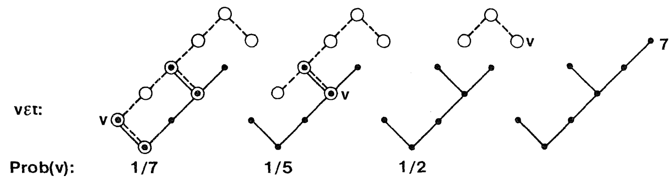
Now suppose we wish to build a labeled Fibonacci tree, T. Assume that the first $m - 1$ vertices of T have already been constructed and given the labels $1, \ldots, m - 1$. Let τ be the current shape of T with associate τ' whose root is r. To add a node labeled m to T we proceed as follows:

WNG1. Choose a $v \in \tau' - \{r\}$ uniformly at random.

WNG2. If $v \notin \tau$, then add v to τ with label m and halt.

WNG3. If $v \in \tau$, say $v = (i, j)$, then return to WNG1 with τ' replaced by $\tau' - \{(i', j')\ i' \le i\}$.

Figure 5 presents an example of a trial generated by WGN1-3.



A WNG trial

FIGURE 5

If this procedure is used iteratively for $m = 1, 2, \ldots, n$ to produce a labeled Fibonacci tree, then let $P(T)$ be the probability that labeling T is created. Thus, the total probability of producing a given shape τ is $P(\tau) = \Sigma P(T)$, where the sum is over all labelings T of τ.

Theorem 3: If τ is a Fibonacci shape with n nodes, then iteration of WNG1-3 produces all labelings of τ with total probability

$$P(\tau) = f_\tau^2/n!$$

Note: It is not true that WNG1-3 produces each labeling of τ with probability $P(T) = f_\tau/n!$.

Proof: Let τ have leaves $w_1, w_2, \ldots, w_k$ and define the subtrees $\tau_i = \tau - \{w_i\}$ for all i. Let $P(w_i|\tau_i)$ denote the probability that w_i gets labeled n after the algorithm constructs some labeling of τ_i. Hence, by the definitions above and induction,

$$P(\tau) = \sum_i P(\tau_i)P(w_i|\tau_i) = \sum_i (f_{\tau_i}^2/(n-1)!)P(w_i|\tau_i). \tag{3.1}$$

Let the w_i be arranged in order of increasing first coordinate, i.e.,

$$w_1 = (a_1, 1), \ldots, w_{k-1} = (a_{k-1}, 1), w_k = (a_k, j),$$

where $a_1 < \cdots < a_k$ and j may be 0 or 1. We need a couple of lemmas to help compute the quantities in (3.1).

Lemma 4: Let τ and the w_i be as above, then

$$f_\tau = \prod_{i=1}^{k-1}(n - a_i - i).$$

Proof: Using the hook formula (Corollary 2), we see that every term in the $n!$ is canceled by a hook of τ except those in the product above. □

Lemma 5: Let τ and the w_i be as above, then

$$P(w_i|\tau_i) = (1/n)\prod_{j=1}^{i-1}\left(1 + \frac{2}{n - a_j - j - 1}\right).$$

Proof: Initially we can pick any one of the n nodes in $\tau_i' - \{r\}$. Any trial ending at w_i can only pass through those w_j with $j < i$ and their associates w_j'. Landing on either of these two reduces the number of available nodes in $\tau_i' - \{r\}$ to $n - a_j - j - 1$, accounting for the second term of the binomial above. □

For notational convenience, let $b_i = n - a_i - i$. Hence, by Lemma 4,

$$f_\tau = b_1 b_2 \ldots b_{k-1}$$

and

$$f_{\tau_i} = (b_1 - 1) \ldots (b_{i-1} - 1) b_{i+1} \ldots b_{k-1}.$$

Also, from Lemma 5,

$$P(w_i | \tau_i) = (1/n)\left(1 + \frac{2}{b_1 - 1}\right) \ldots \left(1 + \frac{2}{b_{i-1} - 1}\right).$$

Thus,

$$f_{\tau_i}^2 P(w_i | \tau_i)/(n - 1)! = (1/n!)\left\{\prod_{1 \le j < i} (b_j^2 - 1)\right\}\left\{\prod_{i < j < k} b_j^2\right\}.$$

Plugging this expression into (3.1), we see that the sum of products telescopes (from the right-hand end) so that

$$P(t) = b_1^2 \ldots b_{k-1}^2/n! = f_\tau^2/n!$$

as desired. □

The obvious corollary is

Corollary 6: $\sum_{\tau \in \mathscr{F}_n} f_\tau^2 = n!$ □

We should also note that this algorithm has a "zone effect" similar to the original one for Young tableaux. Specifically, if $v = (a, 1)$ and $w = (b, 1)$ with $a_i < a$, $b < a_{i+1}$, then by Lemma 5 we have $P(v|\tau) = P(w|\tau)$. This observation will be useful in the next section.

4. Fibonacci Trees Grown from Within

Given $v \in \tau$, then v is a *singleton* if $v' \notin \tau$ and a *doubleton* otherwise. In Figure 6a, the singletons are (0, 0), (3, 0), (4, 0), and (6, 0), with the rest of the vertices being doubletons. If τ has a spine of length s, then the corresponding *extended tree* is

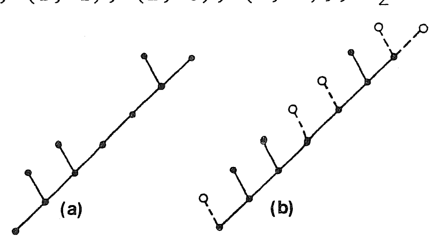
$$\tau'' = \tau \cup \{v' | v \in \tau \text{ is a singleton}\} \cup \{(s + 1, 0)\},$$

see Figure 6b. The elements of $\tau'' - \tau$ are organized into *zones*, which are maximal strings of vertices with consecutive first coordinates. Zones are numbered from the bottom up starting with zone 0, e.g., in Figure 6,

$$Z_0 = \{(0, 1)\},\ Z_1 = \{(3, 1), (4, 1)\},\ Z_2 = \{(6, 1), (7, 0)\}.$$

In the same way, the doubletons of τ are grouped into *bands* with band i directly below zone i. In our example, the bands are

$$B_0 = \emptyset,\ B_1 = \{(1, 0), (1, 1), (2, 0), (2, 1)\},\ B_2 = \{(5, 0), (5, 1)\}.$$



A tree and the extended tree

FIGURE 6

Finally, it will be convenient to have a total order on the vertices. If $v = (i, j)$ and $w = (x, y)$, then we will write $v \leq_t w$ if $i < x$ or $i = x$ and $j \leq y$.

Now, given a labeled Figonacci tree T of shape τ on $m - 1$ nodes, we find a node of $w \in \tau'' - \tau$ to label m by constructing a trial as follows. As usual, ":=" is the Pascal assignment symbol.

P1. Let $v := (0, 0)$ with probability 1. Let the set of predecessors of v be $P := \emptyset$.

P2. Set $P := P \cup \{v\}$.

P3. Pick w uniformly at random from among the set, D, of possible direct successors of $v = (i, j)$ defined by:

(a) if v is a doubleton, then $D = \{w \in \tau'' - P | w \geq_t v\}$.

(b) if v is a singleton, then let B be the band of largest index containing an element of P and let b be the maximum node of B (with respect to $\leq_t$). In this case

$$D = \{w \in \tau'' - P | w >_t b\} - \{w \text{ a singleton} | w \leq v\}.$$

If B does not exist, i.e., P consists only of singletons up to this point, then we take $b = (0, 0)$.

P4. If $w \in \tau'' - \tau$, then halt, else return to P2 with $w := v$.

Note that the trials generated by P1-4 do not necessarily respect the partial order in τ and the sequence of D's computed in P3 is not ordered by containment. For example, if a trial in the tree of Figure 6 has begun (0, 0), (4, 0), then the next node could be any one in τ'' except the two initial nodes and (3, 0). If the trial continues to (1, 1), then any nontrial vertex (i, j) with $i > 1$ is available for the next choice, including (3, 0). However, if the trial begins (0, 0), (1, 1), (4, 0), then the only possible successors are vertices (3, 1), (4, 1), (5, 0), (5, 1), (6, 0), (6, 1), and (7, 0).

Nevertheless, these rules do provide the desired distribution.

Theorem 7: If τ is a Fibonacci shape with n nodes, then iteration of P1-4 produces all labelings of τ with total probability

$$P(\tau) = f_\tau^2/n!$$

Proof: It suffices to show that Lemma 5 is still true when using P1-4. It will be convenient to reformulate the Lemma slightly for this setting. Let λ be a Fibonacci tree with $n - 1$ nodes and leaves $w_1, w_2, \ldots$ with first coordinates $a_1 < a_2 < \ldots$.

Lemma 8: With λ as above and $w \in \lambda'' - \lambda$ in the k^{th} zone, then the probability of terminating a P1-4 trial at w is

$$P(w) = (1/n) \prod_{w_j \in B_i,\ i \leq k} \left(1 + \frac{2}{n - a_j - j - 1}\right).$$

Proof: Induct on k. We will provide an explicit proof of the induction step, the anchor step being similar.

The trials t: $v_0 = (0, 0), v_1, \ldots, w$ are of two types, those that pass through an element of B_k and those that do not. The latter are in bijective probability preserving correspondence with trials $v_0, v_1, \ldots, w'$, where $w' \in Z_{k-1}$. In the former case, if $v_j \in B_k$ is the first such node then $v_0, \ldots, v_{j-1}, w'$ is a legal trial having the same probability as the initial segment of t. We will show below that the sum of the probabilities P of all possible final segments $v_j, v_{j+1}, \ldots, w$ is independent of both the particular node of B_k and the initial history of t. Thus, by induction, it suffices to demonstrate that

$$1 + P|B_k| = \prod_{w_j \in B_k} \left(1 + \frac{2}{n - a_j - j - 1}\right).$$

But the right side above telescopes to $(s + |B_k|)/s$, where s is the denominator corresponding to the largest leaf in B_k that has coordinates $(a, 1)$, say. It is easy to see that if we consider the subtree $\sigma = \{(i, j) \in \lambda | i > a\}$ then $s = |\sigma| + 1$. Hence, to finish the proof of the theorem, we need only show

Lemma 9: Let t, $v = v_j$, P, and σ be as above. Then P is independent of the set of nodes on t prior to v and of v itself (as long as $v \in B_k$). In fact, $P = 1/(|\sigma| + 1)$.

Proof: Let $\{v = u_1 \le_t u_2 \le_t \dots \le_t u_m\}$ be the set of all possible vertices that could appear on t from v up to (but not including) w, i.e., the set of all elements above v that are either elements of B_k or singletons not previously on t. Because of these restrictions, the set of direct successors, $D(u_i)$, does not depend on the previous u_j chosen and, in fact, we have

$$\begin{aligned} D(u_i) &= \{u_j | j > i\} \cup \{v \in \sigma'' | v \text{ is not a singleton in } \sigma\} \\ &= D(u_{i-1}) - \{u_i\}. \end{aligned}$$

Thus,

$$|D(u_m)| = |\{v \in \sigma'' | v \text{ is not a singleton in } \sigma\}| = |\sigma| + 1$$

and

$$|D(u_i)| = |D(u_{i-1})| - 1.$$

Hence,

$$P = \frac{1}{|D(u_1)|}\left(1 + \frac{1}{|D(u_1)| - 1}\right) \cdots \left(1 + \frac{1}{|\sigma| + 1}\right) = \frac{1}{|\sigma| + 1}$$

as desired. □

Of course, Theorem 7 gives another proof of Corollary 6.

5. Remarks and Open Questions

Another point of similarity between Fibonacci trees and standard tableaux is the formula

$$\sum_{\tau \in \mathscr{F}_n} f_\tau = I_n, \tag{5.1}$$

where I_n is the number of involutions in the symmetric group S_n. The correspondence of Bender [9] mentioned in the introduction also proves (5.1). Is there a probabilistic way to demonstrate this, either for trees or tableaux?

A third family of posets that displays behavior similar to that of standard tableaux and rooted trees are the shifted standard tableaux [3]. The shifted analog of the hook formula (1.1) has been proved probabilistically by one of us [7]. It would be interesting to find an aleatory proof of the "sum of squares" equation in the shifted case (see [8] for the exact formula).

Finally, tableaux and shifted tableaux are intimately connected with representations of S_n. Ordinary tableaux give the degrees of ordinary irreducible representations (using matrices in GL_n), while their shifted cousins are related to projective ones (those using PGL_n, the projective linear group). In this setting, the analog of (1.2) expresses the fact that the sum of the squares of the irreducible degrees equals the order of the group. Can (1.2) itself be recast in this light? Specifically, is there a group of matrices G such that the degrees of the irreducible representations $\rho:S_n \to G$ are given by the f_τ?

References

1. C. Greene, A. Nijenhuis, & H. S. Wilf. "A Probabilistic Proof of a Formula for the Number of Young Tableaux of a Given Shape." *Adv. in Math* 31 (1979):104-109.
2. C. Greene, A. Nijenhuis, & H. S. Wilf. "Another Probabilistic Method in the Theory of Young Tableaux." *J. Combin. Theory Ser. A* 37 (1984):127-135.
3. D. E. Knuth. *The Art of Computer Programming: Sorting and Searching*. Vol. 3. Reading, Mass.: Addison-Wesley, 1973.
4. B. Pittel. "On Growing a Random Young Tableau." *J. Combin. Theory Ser. A* 41 (1986):278-285.
5. B. Sagan. "Partially Ordered Sets with Hooklenghts: An Algorithmic Approach." Ph. D. dissertation, M.I.T., 1979.
6. B. Sagan. "Enumeration of Partitions with Hooklengths." *European J. of Combin.* 3 (1982):85-94.
7. B. Sagan. "On Selecting a Random Shifted Young Tableau." *J. Algorithms* 1 (1980):213-234.
8. B. Sagan. "Shifted Tableaux, Schur Q-Functions and a Conjecture of R. Stanley. *J. Combin. Theory Ser. A*. To appear.
9. R. P. Stanley. "The Fibonacci Lattice." *Fibonacci Quarterly* 13 (1975): 215-232.

*****

Announcement

FOURTH INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS

Monday through Friday, July 30-August 3, 1990

Department of Mathematics and Computer Science Wake Forest University Winston-Salem, North Carolina 27109

International Committee: Horadam, A.F. (Australia), *Co-Chairman;* Philippou, A.N. (Cyprus), *Co-Chairman;* Ando, S. (Japan), Bergum, G. (U.S.A.), Johnson, M. (U.S.A.), Kiss, P. (Hungary), Filipponi, Piero (Italy), Campbell, Colin (Scotland), Turner, J.C. (New Zealand).

Local Committee: Fred T. Howard, *Co-Chairman;* Marcellus E. Waddill, *Co-Chairman;* Elmer K. Hayashi, Theresa Vaughan, Deborah Harrell.

CALL FOR PAPERS

The FOURTH INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS will take place at Wake Forest University, Winston-Salem, N.C., from July 30 to August 3, 1990. This Conference is sponsored jointly by the Fibonacci Association and Wake Forest University.

Papers on all branches of mathematics and science related to the Fibonacci numbers as well as recurrences and their generalizations are welcome. Abstracts are to be submitted by March 15, 1990, while manuscripts are due by May 1, 1990. Abstracts and manuscripts should be sent in duplicate following the guidelines for submission of articles found on the inside front cover of any recent issue of *The Fibonacci Quarterly* to:

Professor Gerald E. Bergum
The Fibonacci Quarterly
Department of Computer Science
South Dakota State University
P.O. Box 2201
Brookings, South Dakota 57007-0194

CONVOLUTIONS OF FIBONACCI-TYPE POLYNOMIALS OF ORDER K AND THE NEGATIVE BINOMIAL DISTRIBUTIONS OF THE SAME ORDER

Andreas N. Philippou and Costas Georghiou
University of Patras, Patras, Greece
(Submitted April 1987)

1. Introduction and Summary

Unless otherwise explicitly stated, in this paper k is a fixed positive integer, n_i $(1 \le i \le k)$ and n are nonnegative integers as specified, p and x are real numbers in the intervals $(0, 1)$ and $(0, \infty)$, respectively, $q = 1 - p$, and $[x]$ denotes the greatest integer in x. Let

$$\{F^{(k)}(x)\}_{n=0}^{\infty}$$

be the sequence of Fibonacci-type polynomials of order k, i.e.,

$$F_0^{(k)}(x) = 0, \; F_1^{(k)}(x) = 1,$$

and

$$F^{(k)}(x) = \begin{cases} x\displaystyle\sum_{i=1}^{n} F_{n-i}^{(k)}(x) & \text{if } 2 \le n \le k+1, \\ x\displaystyle\sum_{i=1}^{n} F_{n-i}^{(k)}(x) & \text{if } n \ge k+2. \end{cases} \tag{1.1}$$

This definition is due to Philippou, Georghiou, and Philippou [11] (see also [8]), who obtained the following results:

$$\sum_{n=0}^{\infty} s^n F_{n+1}^{(k)}(x) = \frac{1}{1 - xs - \cdots - xs^k} = \frac{1 - s}{1 - (1 + x)s + xs^{k+1}}, \tag{1.2}$$

$$|s| < 1/(1 + x),$$

$$F_{n+1}^{(k)}(x) = \sum_{\substack{n_1, \ldots, n_k \ni \\ n_1 + 2n_2 + \cdots + kn_k = n}} \binom{n_1 + \cdots + n_k}{n_1, \ldots, n_k} x^{n_1 + \cdots + n_k}, \; n \ge 0, \tag{1.3}$$

and

$$F_{n+1}^{(k)}(x) = \sum_{i=0}^{1} (-1)^i (1 + x)^{n-i} \sum_{j=0}^{[(n-i)/(k+1)]} (-1)^j \binom{n - i - kj}{j} \times x^j (1 + x)^{-(k+1)j}, \; n \ge 0. \tag{1.4}$$

Now let N_k be a random variable which denotes the number of Bernoulli trials until the occurrence of the k^{th} consecutive success. Then

$$P(N_k = n) = p^n F_{n+1-k}^{(k)}(q/p), \; n \ge k, \tag{1.5}$$

$$P(N_k = n + k) = \sum_{i=0}^{1} (-1)^i p^{k+i} \sum_{j=0}^{[(n-i)/(k+1)]} (-1)^j \binom{n - i - kj}{j} (qp^k)^j, \quad n \ge 0, \tag{1.6}$$

and

$$P(N_k = n) = \begin{cases} p^k, & n = k, \\ qp^k, & k + 1 \le n \le 2k, \\ P(N_k = n - 1) - qp^k P(N_k = n - 1 - k), & n \ge 2k + 1. \end{cases} \tag{1.7}$$

The three results above are due, respectively, to Philippou, Georghiou, and Philippou [11], Uppuluri and Patil [12], and Philippou and Makri [8]. We note, however, that expression (1.6) was implicit in the work of [10], and variants of (1.7) have also been established in [1] and [6] by different methods.

In the present paper we generalize relations (1.6) and (1.7) to two types of negative binomial distributions of order k (see Propositions 3.3 and 3.4, and Theorems 3.1 and 3.2), and we illustrate the computational usefulness of Proposition 3.3. The first type of negative binomial distribution of order k was introduced and studied in [9] and [5], while the second type was considered in [4]. Although the latter was recognized as a negative binomial distribution of order k, different from the first, it was named in [4] "compound Poisson distribution of order k" as arising from the Poisson distribution of order k by compounding. The above-mentioned propositions and theorems are stated and proved in Section 3. Their proofs depend on generalizations of expressions (1.1)-(1.5) to the $(r - 1)$-fold convolution of $\{F_n^{(k)}(x)\}_{n=0}^{\infty}$ with itself, which we proceed to discuss first. Here, and in the sequel, r is a positive integer, unless otherwise explicitly stated.

2. Convolutions of Fibonacci-Type Polynomials of Order k

Let $\{F_{n,r}^{(k)}(x)\}_{n=0}^{\infty}$ be the $(r-1)$-fold convolution of the sequence $\{F_n^{(k)}(x)\}_{n=0}^{\infty}$ with itself, i.e., $F_{0,r}^{(k)}(x) = 0$, and for $n \ge 1$,

$$F_{n,r}^{(k)}(x) = \begin{cases} F_n^{(k)}(x) & \text{if } r = 1, \\ \displaystyle\sum_{j=1}^{n} F_{j,r-1}^{(k)}(x) F_{n+1-j}^{(k)}(x) & \text{if } r \ge 2. \end{cases} \tag{2.1}$$

As a consequence of (2.1), and in view of (1.2), we get

$$\sum_{n=0}^{\infty} s^n F_{n+1,r}^{(k)}(x) = \left[\sum_{n=0}^{\infty} s^n F_{n+1}^{(k)}(x)\right]^r = \frac{1}{(1 - xs - \cdots - xs^k)^r} \tag{2.2}$$

$$= \frac{(1 - s)^r}{[1 - (1 + x)s + xs^{k+1}]^r}, \quad |s| < 1/(1 + x).$$

Expanding (2.2) as a Taylor series about $s = 0$, and following procedures similar to those of [9]-[11], we readily find the following closed formulas for $\{F_{n,r}^{(k)}(x)\}_{n=0}^{\infty}$, in terms of the multinomial and binomial coefficients, respectively.

Theorem 2.1: Let $\{F_{n,r}^{(k)}(x)\}_{n=0}^{\infty}$ be the $(r - 1)$-fold convolution of the sequence $\{F_n^{(k)}(x)\}_{n=0}^{\infty}$ with itself. Then

(a) $$F_{n+1,r}^{(k)}(x) = \sum_{\substack{n_1, \ldots, n_k \ni \\ n_1 + 2n_2 + \cdots + kn_k = n}} \binom{n_1 + \cdots + n_k + r - 1}{n_1, \ldots, n_k, r - 1} x^{n_1 + \cdots + n_k}, \quad n \ge 0;$$

and

(b) $$F_{n+1,r}^{(k)}(x) = \sum_{i=0}^{r}(-1)^i\binom{r}{i}(1+x)^{n-i}\sum_{j=0}^{[(n-i)/(k+1)]}(-1)^j\binom{n-i-kj}{j}$$
$$\times\binom{n-i-kj+r-1}{r-1}x^j(1+x)^{-(k+1)j},\quad n \ge 0.$$

We also note that, if we multiply both sides of (2.2) by x^r and then differentiate them with respect to x, we obtain the following reduction formula with respect to r.

Proposition 2.1: Let $\{F_{n,r}^{(k)}(x)\}_{n=0}^{\infty}$ be the $(r-1)$-fold convolution of the sequence $\{F_n^{(k)}(x)\}_{n=0}^{\infty}$ with itself. Then
$$F_{n+1,r+1}^{(k)}(x) = \frac{d}{dx}[x^r F_{n+1,r}^{(k)}(x)]/rx^{r-1},\quad n \ge 0.$$

We proceed next to show that $\{F_{n,r}^{(k)}(x)\}_{n=0}^{\infty}$ satisfies the following linear recurrence with variable coefficients.

Theorem 2.2: Let $\{F_{n,r}^{(k)}(x)\}$ be the $(r-1)$-fold convolution of the sequence $\{F_n^{(k)}(x)\}_{n=0}^{\infty}$ with itself, and set $F_{n,r}^{(k)}(x) = 0$ for $-k+1 \le n \le -1$. Then
$$F_{0,r}^{(k)}(x) = 0,\ F_{1,r}^{(k)}(x) = 1,$$
and
$$F_{n+1,r}^{(k)}(x) = \frac{x}{n}\sum_{j=1}^{k}[n+j(r-1)]F_{n+1-j,r}^{(k)}(x),\quad n \ge 1.$$

From the definition of $\{F_{n,r}^{(k)}(x)\}_{n=0}^{\infty}$, we have
$$F_{0,r}^{(k)}(x) = 0 \quad\text{and}\quad F_{1,r}^{(k)}(x) = 1. \tag{2.3}$$
Now, let $|s| < 1/(1+x)$. Noting that
$$(1 - xs - \cdots - xs^k)^{-r} = (1 - xs - \cdots - xs^k)^{-r-1}\left(1 - x\sum_{j=1}^{k}s^j\right), \tag{2.4}$$
and
$$s^j(1 - xs - \cdots - xs^k)^{-r-1} = \sum_{n=0}^{\infty}s^n F_{n+1-j,r+1}^{(k)}(x),\ 1 \le j \le k, \quad\text{by (2.2)}, \tag{2.5}$$
we get
$$\sum_{n=0}^{\infty}s^n F_{n+1,r}^{(k)}(x) = (1 - xs - \cdots - xs^k)^{-r-1} - x\sum_{j=1}^{k}s^j(1 - xs - \cdots - xs^k)^{-r-1},\quad \text{by (2.2) and (2.4)},$$
$$= \sum_{n=0}^{\infty}s^n F_{n+1,r+1}^{(k)}(x) - x\sum_{j=1}^{k}\sum_{n=0}^{\infty}s^n F_{n+1-j,r+1}^{(k)}(x),\quad \text{by (2.2) and (2.5)},$$
$$= \sum_{n=0}^{\infty}s^n\left[F_{n+1,r+1}^{(k)}(x) - x\sum_{j=1}^{k}F_{n+1-j,r+1}^{(k)}(x)\right].$$
Therefore,
$$F_{n+1,r}^{(k)}(x) = F_{n+1,r+1}^{(k)}(x) - x\sum_{j=1}^{k}F_{n+1-j,r+1}^{(k)}(x),\quad n \ge 0. \tag{2.6}$$

Next, differentiating both sides of (2.2) with respect to s, we get
$$\sum_{n=1}^{\infty}ns^{n-1}F_{n+1,r}^{(k)}(x) = rx\sum_{j=1}^{k}js^{j-1}(1 - xs - \cdots - xs^k)^{-r-1}$$
$$= rx\sum_{j=1}^{k}j\sum_{n=0}^{\infty}s^n F_{n+2-j,r+1}^{(k)}(x),\quad \text{by (2.2) and (2.5)},$$

$$= \sum_{n=1}^{\infty} s^{n-1} rx \sum_{j=1}^{k} jF_{n+1-j,\,r+1}^{(k)}(x),$$

which implies

$$nF_{n+1,\,r}^{(k)}(x) = rx \sum_{j=1}^{k} jF_{n+1-j,\,r+1}^{(k)}(x), \; n \geq 1. \tag{2.7}$$

Combining (2.6) and (2.7), we obtain

$$F_{n+1,\,r+1}^{(k)}(x) = \frac{x}{n} \sum_{j=1}^{k} (n + jr) F_{n+1-j,\,r+1}^{(k)}(x), \; n \geq 1,$$

which, along with (1.1) and (2.3), establishes the theorem.

Remark 2.1: Results analogous to Proposition 2.1 and Theorem 2.2 have been obtained by Horadam and Mahon [3] for convolutions of the sequence of Pell polynomials (of order 2) with itself.

3. Binomial Expressions and Recurrences for the Negative Binomial Distributions of Order k

In the present section, we employ Theorems 2.1 and 2.2 to derive binomial expressions and simple recurrences for the following two distributions of order k [4], [5], [9].

Definition 3.1: A random variable X is said to be distributed as negative binomial distribution of order k, type I, with parameter vector (r, p), to be denoted by $NB_{k,\,\mathrm{I}}(r, p)$, if

$$P(X=n) = p^n \sum_{\substack{n_1, \ldots, n_k \ni \\ n_1 + 2n_2 + \cdots + kn_k = n - kr}} \binom{n_1 + \cdots + n_k + r - 1}{n_1, \ldots, n_k, r - 1} \left(\frac{q}{p}\right)^{n_1 + \cdots + n_k}, \; n \geq kr.$$

Definition 3.2: A random variable X is said to be distributed as negative binomial distribution of order k, type II, with parameter vector (r, p), to be denoted by $NB_{k,\,\mathrm{II}}(r, p)$, if

$$P(X=n) = p^r \sum_{\substack{n_1, \ldots, n_k \ni \\ n_1 + 2n_2 + \cdots + kn_k = n}} \binom{n_1 + \cdots + n_k + r - 1}{n_1, \ldots, n_k, r - 1} \left(\frac{q}{p}\right)^{n_1 + \cdots + n_k}, \; n \geq 0.$$

The negative binomial distribution of order k, type I, gives the probability that the first occurrence of r success runs of length k happens at trial n [5]. The negative binomial distribution of order k, type II, arises as a gamma compound Poisson distribution of order k. More precisely, if we use $CP_k(r, \alpha)$ to denote the (gamma) compound Poisson distribution of order k with parameter vector (r, α) [4], we note that

$$NB_{k,\,\mathrm{II}}(r, p) = CP_k(r, \alpha) \text{ for } p = \alpha/(\alpha + k).$$

The fact that $CP_k(r, \alpha)$ is a negative binomial distribution of order k, albeit different from $NB_{k,\,\mathrm{I}}(r, p)$, was already mentioned in [4] by Philippou, who named the new distribution, however, "compound Poisson distribution of order k" as arising from the Poisson distribution of order k by compounding.

As a consequence of Theorem 2.1(a) and Definitions 3.1 and 3.2, respectively, we have the following relationships.

Proposition 3.1: Let X be a random variable distributed as $NB_{k,\mathrm{I}}(r, p)$ and let $\{F_{n,r}^{(k)}(x)\}_{n=0}^{\infty}$ be the $(r-1)$-fold convolution of $\{F_n^{(k)}(x)\}_{n=0}^{\infty}$ with itself. Then

$$P(X = n) = p^n F_{n+1-kr,\, r}^{(k)}(q/p), \quad n \geq kr.$$

Proposition 3.2: Let X be a random variable distributed as $NB_{k,\mathrm{II}}(r, p)$ and let $\{F_{n,r}^{(k)}(x)\}_{n=0}^{\infty}$ be as above. Then

$$P(X = n) = p^r F_{n+1,\, r}^{(k)}(q/k), \quad n \geq 0.$$

Combining Theorem 2.1(b) with Propositions 3.1 and 3.2, respectively, we obtain the following binomial expressions for the negative binomial distributions of order k.

Proposition 3.3: Let X be a random variable distributed as $NB_{k,\mathrm{I}}(r, p)$. Then

$$P(X = n + kr) = \sum_{i=0}^{r} (-1)^i \binom{r}{i} p^{kr+i} \sum_{j=0}^{[(n-i)/(k+1)]} (-1)^j \binom{n-i-kj}{j} \times \binom{n-i-kj+r-1}{r-1} (qp^k)^j, \quad n \geq 0.$$

Proposition 3.4: Let X be a random variable distributed as $NB_{k,\mathrm{II}}(r, p)$. Then

$$P(X = n) = p^r \sum_{i=0}^{r} (-1)^i \binom{r}{i} \left(\frac{k+q}{k}\right)^{n-i} \sum_{j=0}^{[(n-i)/(k+1)]} (-1)^j \binom{n-i-kj}{j} \times \binom{n-i-kj+r-1}{r-1} \left[\left(\frac{q}{k}\right)\left(\frac{k}{k+q}\right)^{k+1}\right]^j, \quad n \geq 0.$$

Remark 3.1: Another binomial expression for the probabilities $P(X = n + kr)$ ($n \geq 0$) of $NB_{k,\mathrm{I}}(r, p)$ has been obtained by Charalambides [2], who employed for this purpose the truncated exponential Bell polynomials. Our expression appears to be more applicable.

Remark 3.2: For $r = 1$, Propositions 3.3 and 3.4 provide binomial expressions for the probabilities of

$$G_{k,\mathrm{I}}(p) \equiv NB_{k,\mathrm{I}}(1, p) \quad \text{and} \quad G_{k,\mathrm{II}}(p) \equiv NB_{k,\mathrm{II}}(1, p),$$

respectively. The first one implies (1.6), the main result of Uppuluri and Patil [12], since N_k is distributed as $G_{k,\mathrm{I}}(p)$ [7], [9]. The second is noted presently for the first time.

Theorem 2.2 and Proposition 2.1 imply

Theorem 3.1: Let X be a random variable distributed as $NB_{k,\mathrm{I}}(r, p)$, and set $P_n = P(X = n)$. Then

$$P_n = \begin{cases} 0, & n \leq kr - 1, \\ p^{kr}, & n = kr, \\ \dfrac{(q/p)}{n - kr} \displaystyle\sum_{j=1}^{k} [n - kr + j(r-1)] p^j P_{n-j}, & n \geq kr + 1. \end{cases}$$

Proof: For $n \leq kr - 1$, $(X = n) = \emptyset$, which implies $P_n = P(\emptyset) = 0$. For $n = kr$, Definition 3.1 gives $P_n = p^{kr}$. For $n \geq kr + 1$, we have

$$P_n = p^n F_{n-kr+1,\, r}^{(k)}(q/p), \text{ by Proposition 3.1,}$$

$$= p^n \frac{(q/p)}{n - kr} \sum_{j=1}^{k} [n - kr + j(r - 1)] F_{n-kr+1-j,\, r}^{(k)}(q/p), \text{ by Theorem 2.2,}$$

$$= \frac{(q/p)}{n - kr} \sum_{j=1}^{k} [n - kr + j(r - 1)] p^j P_{n-j}, \text{ by Proposition 3.1.}$$

For $r = 1$, Theorem 3.1 reduces to the following corollary, which implies recurrence (1.7), since N_k is distributed as $G_{k,\mathrm{I}}(p)$ [7], [9].

Corollary 3.1: Let X be a random variable distributed as $G_{k,\mathrm{I}}(p) \equiv NB_{k,\mathrm{I}}(1, p)$, and set $P_n = P(X = n)$. Then

$$P_n = \begin{cases} p^k, & n = k, \\ qp^k, & k + 1 \le n \le 2k, \\ P_{n-1} - qp^k P_{n-1-k}, & n \ge 2k + 1. \end{cases}$$

Theorem 2.2 and Proposition 2.2 imply

Theorem 3.2: Let X be a random variable distributed as $NB_{k,\mathrm{II}}(r, p)$, and set $P_n = P(X = n)$, $n \ge -k + 1$. Then

$$P_n = \begin{cases} 0, & -k + 1 \le n \le -1, \\ p^r, & n = 0, \\ \dfrac{q}{kn} \displaystyle\sum_{j=1}^{k} [n + j(r - 1)] P_{n-j}, & n \ge 1. \end{cases}$$

Proof: For $-k + 1 \le n \le -1$, $(X = n) = \emptyset$, which implies $P_n = P(\emptyset) = 0$. For $n = 0$, Definition 3.2 gives $P_n = p^r$. For $n \ge 1$, we have

$$P_n = p^r F_{n+1,\, r}^{(k)}(q/k), \text{ by Proposition 3.2,}$$

$$= p^r \frac{(q/k)}{n} \sum_{j=1}^{k} [n + j(r - 1)] F_{n+1-j,\, r}^{(k)}(q/k), \text{ by Theorem 2.2,}$$

$$= \frac{q}{kn} \sum_{j=1}^{k} [n + j(r - 1)] P_{n-j}, \text{ by Proposition 3.2,}$$

which completes the proof of the theorem.

For $r = 1$, Theorem 3.2 reduces to the following corollary.

Corollary 3.2: Let X be a random variable distributed as $G_{k,\mathrm{II}}(p) \equiv NB_{k,\mathrm{II}}(1, p)$, and set $P_n = P(X = n)$, $n \ge -k + 1$. Then

$$P_n = \begin{cases} p, & n = 0 \\ \left(\dfrac{k + q}{k}\right)^{n-1} \dfrac{pq}{k}, & 1 \le n \le k, \\ \left(\dfrac{k + q}{k}\right) P_{n-1} - \dfrac{q}{k} P_{n-1-k}, & n \ge k + 1. \end{cases}$$

4. Computational Examples

In this section we illustrate the computational usefulness of Propositions 3.3 and 3.4. Since both propositions are of the same nature, we restrict attention to Proposition 3.3 in comparison to Definition 3.1.

Example 4.1: Assume that a random variable X is distributed as $NB_{3,\mathrm{I}}(5, p)$ and we are interested in calculating $P(X = 18)$ and $P(X = 20)$.

Proposition 3.3 gives

$$P(X = 18) = \sum_{i=0}^{5} (-1)^i \binom{5}{i}\binom{7-i}{4} p^{15+i} = 35p^{15} - 75p^{16} + 50p^{17} - 10p^{18} \tag{4.1}$$

and

$$\begin{aligned} P(X = 20) &= \sum_{i=0}^{5} (-1)^i \binom{5}{i} p^{15+i} \sum_{j=0}^{[(5-i)/4]} (-1)^j \binom{5-i-3j}{j}\binom{9-i-3j}{4}(qp^3)^j \\ &= p^{15}\left[\binom{9}{4} - 2\binom{6}{4}qp^3\right] - 5p^{16}\left[\binom{8}{4} - \binom{5}{4}qp^3\right] + 10p^{17}\binom{7}{4} \\ &\qquad - 10p^{18}\binom{6}{4} + 5p^{19}\binom{5}{4} - p^{20}\binom{4}{4} \\ &= 126p^{15} - 350p^{16} + 350p^{17} - 150p^{18} + 25p^{19} - p^{20} \\ &\qquad - 30qp^{18} + 25qp^{19}. \end{aligned} \tag{4.2}$$

Alternatively, if we use Definition 3.1, we get

$$\begin{aligned} P(X = 18) &= p^{18} \sum_{\substack{n_1, n_2, n_3 \ni \\ n_1 + 2n_2 + 3n_3 = 3}} \binom{n_1 + n_2 + n_3 + 4}{n_1,\ n_2,\ n_3,\ 4}\left(\frac{q}{p}\right)^{n_1+n_2+n_3} \\ &= p^{18}\left[\binom{3+0+0+4}{3,\ 0,\ 0,\ 4}\left(\frac{q}{p}\right)^3 + \binom{1+1+0+4}{1,\ 1,\ 0,\ 4}\left(\frac{q}{p}\right)^2 + \binom{0+0+1+4}{0,\ 0,\ 1,\ 4}\left(\frac{q}{p}\right)^1\right] \\ &= 35q^3p^{15} + 30q^2p^{16} + 5qp^{17} \end{aligned} \tag{4.3}$$

and

$$\begin{aligned} P(X = 20) &= p^{20} \sum_{\substack{n_1, n_2, n_3 \ni \\ n_1 + 2n_2 + 3n_3 = 5}} \binom{n_1 + n_2 + n_3 + 4}{n_1,\ n_2,\ n_3,\ 4}\left(\frac{q}{p}\right)^{n_1+n_2+n_3} \\ &= p^{20}\left[\binom{5+0+0+4}{5,\ 0,\ 0,\ 4}\left(\frac{q}{p}\right)^5 + \binom{3+1+0+4}{3,\ 1,\ 0,\ 4}\left(\frac{q}{p}\right)^4 + \binom{2+0+1+4}{2,\ 0,\ 1,\ 4}\left(\frac{q}{p}\right)^3\right. \\ &\qquad \left. + \binom{1+2+0+4}{1,\ 2,\ 0,\ 4}\left(\frac{q}{p}\right)^3 + \binom{0+1+1+4}{0,\ 1,\ 1,\ 4}\left(\frac{q}{p}\right)^2\right] \\ &= 126q^5p^{15} + 280q^4p^{16} + 210q^3p^{17} + 30q^2p^{18}. \end{aligned} \tag{4.4}$$

Example 4.2: Assume that a random variable X is distributed as $NB_{20,\mathrm{I}}(3, p)$ and we are interested in calculating $P(X = 80)$ and $P(X = 100)$.

Proposition 3.3 gives

$$\begin{aligned} P(X = 80) &= \sum_{i=0}^{3} (-1)^i \binom{3}{i}\binom{22-i}{2} p^{60+i} \\ &= 231p^{60} - 630p^{61} + 570p^{62} - 171p^{63} \end{aligned} \tag{4.5}$$

and

$$\begin{aligned} &P(X = 100) \\ &= \sum_{i=0}^{3} (-1)^i \binom{3}{i} p^{60+i} \sum_{j=0}^{[(40-i)/21]} (-1)^j \binom{40-i-20j}{j}\binom{42-i-20j}{2}(qp^{20})^j \end{aligned}$$

$$= p^{60}\left[\binom{42}{2} - 20\binom{22}{2}qp^{20}\right] - 3p^{61}\left[\binom{41}{2} - 19\binom{21}{2}qp^{20}\right]$$
$$+ 3p^{62}\left[\binom{40}{2} - 18\binom{20}{2}qp^{20}\right] - p^{63}\left[\binom{39}{2} - 17\binom{19}{2}qp^{60}\right]$$
$$= 861p^{60} - 2460p^{61} + 2340p^{62} - 741p^{63} - 4620qp^{80}$$
$$+ 11970qp^{81} - 10260qp^{82} + 2907qp^{83}. \tag{4.6}$$

On the other hand, Definition 3.1 does not appear to be applicable for this task without a considerable amount of computational effort, even with the aid of the computer.

In general, when k and $n - kr$ are large, Proposition 3.3 fares much better than Definition 3.1 for calculating negative binomial probabilities of order k, type I. If all probabilities up to $P(X = m)$ are needed, for some integer m ($\geq kr$), the recurrence given in Theorem 3.1 is most appropriate for calculating them.

References

1. S. Aki, H. Kuboki, & K. Hirano. "On Discrete Distributions of Order k." *Annals of the Institute of Statistical Mathematics* *36A*, no. 3 (1984):431-440.
2. A. Ch. Charalambides. "On Discrete Distributions of Order k." *Annals of the Institute of Statistical Mathematics* *38A*, no. 3 (1986):557-568.
3. A. F. Horadam & Br. J. M. Mahon. "Convolutions for Pell Polynomials." In *Fibonacci Numbers and Their Applications: Proceedings of the First International Conference on Fibonacci Numbers and Their Applications* (Patras, 1984), ed. by A. N. Philippou, G. E. Bergum, & A. F. Horadam. Dordrecht: D. Reidel Publishing Company, 1986, pp. 55-80.
4. A. N. Philippou. "Poisson and Compound Poisson Distributions of Order k and Some of Their Properties" (in Russian, English summary). *Zapiski Nauchnykh Seminarov Liningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova An SSSR* *130* (1983):175-180.
5. A. N. Philippou. "The Negative Binomial Distribution of Order k and Some of Its Properties." *Biometrical Journal* *26* (1984):789-794.
6. A. N. Philippou. "Recursive Theorems for Success Runs and Reliability of Consecutive-k-out-of-n:F Systems." In *Applications of Fibonacci Numbers: Proceedings of the Second International Conference on Fibonacci Numbers and Their Applications* (San Jose, 1986), ed. by A. N. Philippou, G. E. Bergum, & A. F. Horadam. Dordrecht: D. Reidel Publishing Company, 1988, pp. 149-161.
7. A. N. Philippou & A. A. Muwafi. "Waiting for the k^{th} Consecutive Success and the Fibonacci Sequence of Order k." *Fibonacci Quarterly* *20*, no. 1 (1982):28-32.
8. A. N. Philippou & F. S. Makri. "Longest Success Runs and Fibonacci-type Polynomials of Order k." *Fibonacci Quarterly* *23*, no. 4 (1985):338-346.
9. A. N. Philippou, C. Georghiou, & G. N. Philippou. "A Generalized Geometric Distribution of Order k and Some of Its Properties." *Statistics & Probability Letters* *1* (1983):171-175.
10. A. N. Philippou, C. Georghiou, & G. N. Philippou. "Fibonacci Polynomials of Order k, Multinomial Expansions, and Probability." *International Journal of Mathematics and Mathematical Sciences* *6*, no. 3 (1983):545-550.
11. A. N. Philippou, C. Georghiou, & G. N. Philippou. "Fibonacci-Type Polynomials of Order k with Probability Applications." *Fibonacci Quarterly* *23*, no. 2 (1985):100-105.
12. V. R. R. Uppuluri & S. A. Patil. "Waiting times and Generalized Fibonacci Sequences." *Fibonacci Quarterly* *21*, no. 4 (1983):342-349.

*****

MINIMUM PERIODS OF $S(n, k)$ MODULO M

Y. H. Harris Kwong
SUNY College at Fredonia, Fredonia, NY 14063
(Submitted May 1987)

1. Introduction

The Stirling number of the second kind, $S(n, k)$, is defined as the number of ways to partition a set of n elements into k nonempty subsets. Obviously, $S(n, k) = 0$ if $n < k$. The sequence $\{S(n, k) \pmod{p^N}\}_{n \geq k}$ is known to be periodic. That is, there exists $N_0 \geq k$ and $\pi \geq 1$ such that

$$S(n + \pi, k) \equiv S(n, k) \pmod{p^N}, \text{ for } n > N_0.$$

Note that any period is divisible by the minimum period. Carlitz [2] showed that if $k > p > 2$ and $p^{b-1} < k \leq p^b$, where $b \geq 2$, $(p - 1)p^{N+b-2}$ is a period for $\{S(n, k) \pmod{p^N}\}_{n \geq k}$.

In this paper, we will determine the minimum period of $\{S(n, k) \pmod{M}\}_{n \geq k}$ for $k \geq 1$ and $M \geq 1$. This extends the results given in [1] and [3], and confirms that the periods in [2] are indeed the minimum periods for odd p.

2. Preliminaries

Given any sequence $\{a_n\}_{n \geq 0}$ of integers, its generating function, $A(x)$, is defined as

$$A(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Certainly, $A(x)$ is a formal power series over the ring of integers. A period of $\{a_n \pmod{M}\}_{n \geq 0}$ will also be called a period of $A(x)$ modulo M. The next theorem is obvious.

Theorem 2.1: If $\{a_n\}_{n \geq 0}$ is generated by $A(x)$, then π is a period of $\{a_n \pmod{M}\}_{n \geq 0}$ if and only if $(1 - x^{\pi})A(x)$ is a polynomial modulo M.

We will study generating functions in the forms of $1/f(x)$, where $f(x) \in \mathbb{Z}[x]$, and $f(0) = 1$. We have

Theorem 2.2: Given $f(x)$, $u(x) \in \mathbb{Z}[x]$, where $f(0) = u(0) = 1$, let μ and μ' be the minimum periods of $1/f(x)$ and $1/f(x)u(x)$ modulo M, respectively. Then μ divides μ'.

Proof: From the definition of μ', we have

$$\frac{1 - x^{\mu'}}{f(x)u(x)} \equiv h(x) \in \mathbb{Z}_M[x].$$

Therefore,

$$\frac{1 - x^{\mu'}}{f(x)} \equiv h(x)u(x) \in \mathbb{Z}_M[x].$$

This implies that μ' is a period of $1/f(x)$ modulo M. However, μ' may not be the minimum period. Thus, $\mu|\mu'$. $\square$

The next theorem is again obvious. Yet, it allows us to assume that M is a prime power.

Theorem 2.3: Let $p_1^{e_1} \ldots p_s^{e_s}$ be the prime factorization of M, and let $\mu(p_i^{e_i})$ be the minimum period of $\{a_n \pmod{p_i^{e_i}}\}_{n \geq 0}$. Then the minimum period of $\{a_n \pmod{M}\}_{n \geq 0}$ is the least common multiple of $\mu(p_i^{e_i})$, where $1 \leq i \leq s$.

Let $\mu(k; p^N)$ be the minimum period of the sequence of Stirling numbers of the second kind $\{S(n, k) \pmod{p^N}\}_{n \geq k}$. It is well known that

$$\sum_{n=0}^{\infty} S(n + k, k)x^n = \frac{1}{(1 - x)(1 - 2x) \cdots (1 - kx)}.$$

It now follows from Theorem 2.2 that $\mu(k; p^N)|\mu(k + 1; p^N)$. We would like to know when $\mu(k; p^N) = \mu(k + 1; p^N)$.

Theorem 2.4: Let $A(x)$ be a formal power series over the ring of integers, and $r \in \mathbb{Z}$, where $r \geq 1$. Let π be a period of $A(x)$ modulo p^N. Then π is not a period of $A(x)/(1 - rx)$ iff $r \not\equiv 0 \pmod{p}$ and $h(r^{-1}) \not\equiv 0 \pmod{p^N}$, where $h(x)$ is the polynomial $(1 - x^\pi)A(x)$ modulo p^N, and r^{-1} is the inverse of r modulo p^N.

Proof: If $r \equiv 0 \pmod{p}$, then $1 - rx$ is invertible $\pmod{p^N}$. Thus,

$$(1 - x^\pi)A(x)/(1 - rx)$$

is still a polynomial modulo p^N. Now assume that $r \not\equiv 0 \pmod{p}$, and let

$$h(x) = \sum_{n=0}^{D} a_n x^n.$$

Then we have

$$\begin{aligned}\frac{(1 - x^\pi)A(x)}{1 - rx} &\equiv \frac{h(x)}{1 - rx} \equiv \left(\sum_{n=0}^{D} a_n x^n\right)\left(\sum_{n=0}^{\infty} (rx)^n\right) \\ &\equiv \sum_{m=0}^{D-1}\left(\sum_{n=0}^{m} a_n r^{m-n}\right)x^m + \sum_{m=D}^{\infty}\left(\sum_{n=0}^{D} a_n r^{-n}\right)(rx)^m \pmod{p^N}\end{aligned}$$

is a polynomial modulo p^N if and only if

$$\sum_{n=0}^{D} a_n r^{-n} \equiv h(r^{-1}) \equiv 0 \pmod{p^N}. \quad \square$$

Therefore, to determine $\mu(k; p^N)$, it suffices to find the minimum period of $1/f_k(x)$ modulo p^N, where

$$f_k(x) = \prod_{\substack{i=1 \\ p \nmid i}}^{k} (1 - ix).$$

3. Stirling Numbers

First of all, we determine $\mu(k; p^N)$ for $1 < k \le p$. The following theorem is a routine exercise.

Theorem 3.1: For $1 < k \le p$, $\mu(k; p^N)$ is the least common multiple of the orders of i modulo p^N for $1 \le i \le k$.

For $k > p$, we use induction on N. The case of $N = 1$ is relatively simple.

Theorem 3.2: If $k > p$, $b \ge 2$, then $\mu(k; p) = (p - 1)p^{b-1}$, where $p^{b-1} < k \le p^b$.

Proof: If $k = p^b$, $b \ge 1$, then

$$f_{p^b}(x) = \prod_{\substack{i=1 \\ p \nmid i}}^{p^b} (1 - ix) \equiv \left\{\prod_{i=1}^{p-1} (1 - ix)\right\}^{p^{b-1}}$$
$$\equiv (1 - x^{p-1})^{p^{b-1}} \equiv 1 - x^{(p-1)p^{b-1}} \pmod{p}.$$

So, $\mu(p^b; p) = (p - 1)p^{b-1}$. Therefore, $\mu(k; p) \mid (p - 1)p^{b-1}$ for $p^{b-1} < k \le p^b$, $b \ge 1$. In particular, for a fixed $b \ge 2$,

$$h(x) = \frac{1 - x^{(p-1)p^{b-2}}}{f_{p^{b-1}}(x)} \equiv 1 \pmod{p}.$$

From Theorems 2.2 and 2.4, we know that

$$(p - 1)p^{b-2} = \mu(p^{b-1}; p) \text{ divides } \mu(p^{b-1} + 1; p) \text{ properly.}$$

Consider $p^{b-1} < k \le p^b$, $b \ge 2$. On one hand,

$$\mu(p^{b-1} + 1; p) \text{ divides } \mu(k; p),$$

so $(p - 1)p^{b-2}$ is a *proper* divisor of $\mu(k; p)$. On the other hand,

$$\mu(k; p) \text{ divides } \mu(p^b; p) = (p - 1)p^{b-1}.$$

Therefore, $\mu(k; p) = (p - 1)p^{b-1}$. □

The next lemma can be easily verified. We leave the proof to the reader.

Lemma 3.3: Let $f(x) \in \mathbb{Z}[x]$ such that $f(0) = 1$, and let π be a period of $1/f(x)$ modulo p^N. Then $p\pi$ is a period of $1/f(x)$ modulo p^{N+1}.

Corollary 3.4: For $p^{b-1} < k \le p^b$, $b \ge 1$, $\mu(k; p^N)$ always divides $(p - 1)p^{N+b-2}$.

Now we are ready to prove

Theorem 3.5: For $k > p > 2$, and $p^{b-1} < k \le p$, where $b \ge 2$,

$$\mu(k; p^N) = (p - 1)p^{N+b-2}.$$

Proof: The case of $N = 1$ is proved in Theorem 3.2. Assume it is true for some $N \ge 1$; we want to show that it is also true for $N + 1$. Because of Lemma 3.3, if $p^{b-1} < k \le p^b$, $b \ge 2$, then $\mu(k; p^{N+1})$ is either

$$(p - 1)p^{N+b-2} \quad \text{or} \quad (p - 1)p^{N+b-1}.$$

In any case, for $k = p^{b-1}$, we always have

$$h(x) = \frac{1 - x^{(p-1)p^{N+b-2}}}{f_{p^{b-1}}(x)} \in \mathbb{Z}_{p^{N+1}}[x].$$

If we are able to show that $h((p^{b-1} + 1)^{-1}) \not\equiv 0 \pmod{p^{N+1}}$, then

$(p - 1)p^{N+b-2}$ divides $\mu(p^{b-1} + 1; p^{N+1})$ properly.

This implies that $\mu(p^{b-1} + 1; p^{N+1})$ must be $(p - 1)p^{N+b-1}$. Then $\mu(k; p^{N+1})$, where $p^{b-1} < k \le p^b$, will also be $(p - 1)p^{N+b-1}$. Note that $h(x)$ can also be rewritten as

$$h(x) = \frac{1 - x^{(p-1)p^{N+b-3}}}{f_{p^{b-1}}(x)} \sum_{j=0}^{p-1} x^{j(p-1)p^{N+b-3}}.$$

From the inductive hypothesis on N, we have

$$\left.\frac{1 - x^{(p-1)p^{N+b-3}}}{f_{p^{b-1}}(x)}\right|_{x=(p^{b-1}+1)^{-1}} \not\equiv 0 \pmod{p^N}.$$

On the other hand, it is easy to check that the highest power of p that divides

$$\left. x^{j(p-1)p^{N+b-3}}\right|_{x=(p^{b-1}+1)^{-1}}$$

is exactly p. Hence, $h((p^{b-1} + 1)^{-1}) \not\equiv 0 \pmod{p^{N+1}}$. □

Theorem 3.6: If $p = 2$, then

(1) $\mu(1; 2^N) = \mu(2; 2^N) = 1$,

(2) $\mu(3; 2^N) = \mu(4; 2^N) = \begin{cases} 2 & \text{if } N = 1 \text{ or } 2 \\ 2^{N-1} & \text{if } N \ge 3 \end{cases}$,

(3) $\mu(k; 2^N) = 2^{N+b-2}$ for $2^{b-1} < k \le 2$, $b \ge 3$.

Proof: The proof is identical to that of Theorem 3.5 for $b \ge 3$. We have to determine $\mu(3; 2^N) = \mu(4; 2^N)$ separately. In this case, we study

$$\frac{1}{f_4(x)} = \frac{1}{(1 - x)(1 - 3x)} = \left(\sum_{i=0}^{\infty} x^i\right)\left(\sum_{j=0}^{\infty} 3^j x^j\right) = \sum_{n=0}^{\infty} b_n x^n,$$

where $b_n = (3^{n+1} - 1)/2$. Thus, $\mu(3; 2^N)$ is the smallest n such that

$b_n \equiv b_0 = 1 \pmod{2^N}$.

That is, it is the smallest n such that

$3^n \equiv 1 \pmod{2^{N+1}}$.

Therefore, $\mu(3; 2^N)$ satisfies (2) in the statement of the theorem. □

4. Final Remarks

It is possible to obtain the same results without invoking any induction. However, the computation is more involved. We were also able to extend the result to the generating function $1/f(x)$, where $f(x)$ is a product of linear factors of the forms $1 - rx$, $r \in \mathbb{Z}$. These approaches will appear in a forthcoming paper elsewhere.

References

1. H. W. Becker & J. Riordan. "The Arithmetic of Bell and Stirling Numbers." *Amer. J. Math.* *70* (1948):385-394.
2. L. Carlitz. "Congruences for Generalized Bell and Stirling Numbers." *Duke Math. J.* *22* (1955):193-205.
3. A. Nijenhuis & H. S. Wilf. "Periodicities of Partition Functions and Stirling Numbers Modulo p." *J. Number Theory* *25* (1987):308-312.

*****

ON r-GENERALIZED FIBONACCI NUMBERS

François Dubeau
Collège militaire royal de Saint-Jean
Saint-Jean-sur-Richelieu, Québec, Canada, J0J 1R0

(Submitted May 1987)

Introduction

Miles [5] defined the r-generalized Fibonacci numbers ($r \geq 2$) as follows:

$$u_{r,n} = 0 \quad (n = -1, -2, -3, \ldots), \tag{1a}$$

$$u_{r,0} = 1, \tag{1b}$$

$$u_{r,n} = \sum_{i=1}^{r} u_{r,n-i} \quad (n = 1, 2, 3, \ldots). \tag{1c}$$

In such a way, for $r = 2$, we get the ordinary Fibonacci numbers. The object of this paper is to present, in the first section, an elementary proof of the convergence of the sequences of ratios

$$\left\{ t_{r,n} = \frac{u_{r,n}}{u_{r,n-1}} \right\}_{n=1}^{\infty}$$

using neither the theory of difference equations nor the theory of continued fractions. In the second section, we consider a geometric interpretation of the r-generalized Fibonacci numbers that is a natural generalization of the golden rectangle. Finally, in the third section, we consider electrical schemes generating these numbers.

1. Convergence Results

For each $r \geq 2$, we consider the sequence of ratios

$$t_{r,n} = u_{r,n}/u_{r,n-1} \quad (n = 1, 2, 3, \ldots).$$

Rather than using the theory of difference equations to obtain a formula for $u_{r,n}$ and use it to prove the convergence of the sequence to the unique positive root of the polynomial

$$p_r(x) = x^r - \sum_{i=1}^{r} x^{r-i} \quad (\text{see [5]}),$$

we present here a proof based on a fixed point argument using the way the $u_{r,n}$ are generated.

Observe that $u_{r,n} > 0$ for $n \geq 0$. Hence, dividing (1c) by $u_{r,n-1}$, we get

$$t_{r,n} = 1 + \sum_{i=2}^{r} \frac{u_{r,n-i}}{u_{r,n-1}} \quad (n \geq 1)$$

and, using the definition of $t_{r,i}$, we obtain

$$t_{r,n} = 1 + \sum_{i=2}^{r} \frac{1}{\prod_{j=1}^{i-1} t_{r,n-j}} \quad (n \geq r). \tag{2}$$

From (1), we also have

$$u_{r,n} = 2u_{r,n-1} - u_{r,n-r-1} \text{ for } n \geq 2;$$

hence, dividing by $u_{r,n-1}$, we obtain

$$t_{r,n} = 2 - \frac{1}{\prod_{i=1}^{r} t_{r,n-i}} \quad (n \geq r+1). \tag{3}$$

Now, since $t_{r,n} \geq 1$ for $n = 1, \ldots, r$, using (2) we have $t_{r,n} \geq 1$ for all $n \geq 1$ and, using (3), we also have $t_{r,n} \leq 2$ for all $n \geq 1$.

Using (2) and (3) we can generate a sequence of upper bounds $\{B_{r,\ell}\}_{\ell=0}^{\infty}$ and a sequence of lower bounds $\{b_{r,\ell}\}_{\ell=0}^{\infty}$ for $t_{r,n}$ as follows. We have

$$1 = b_{r,0} \leq t_{r,n} \leq B_{r,0} = 2 \quad (n \geq 1)$$

and, assuming that $b_{r,\ell-1}$ and $B_{r,\ell-1}$ are known and such that

$$b_{r,\ell-1} \leq t_{r,n} \leq B_{r,\ell-1} \text{ for all } n \geq r(\ell-1)+1,$$

we generate $b_{r,\ell}$ and $B_{r,\ell}$ using (2) and (3) in such a way that

$$b_{r,\ell} = 1 + \sum_{i=2}^{r} \frac{1}{B_{r,\ell-1}^{i-1}} \leq t_{r,n} \leq 2 - \frac{1}{B_{r,\ell-1}^{r}} = B_{r,\ell} \tag{4}$$

for all $n \geq r\ell + 1$.

The problem is now related to the convergence of the sequences

$$\{b_{r,\ell}\}_{\ell=0}^{\infty} \quad \text{and} \quad \{B_{r,\ell}\}_{\ell=0}^{\infty}.$$

We consider the two functions

$$f_r(x) = 1 + \sum_{i=2}^{r} \frac{1}{x^{i-1}} \quad \text{and} \quad F_r(x) = 2 - \frac{1}{x^r}$$

From (4), $B_{r,\ell} = F_r(B_{r,\ell-1})$ and $b_{r,\ell} = f_r(B_{r,\ell-1})$; hence, the result we look for will be obtained from the study of the two functions $f_r(\cdot)$ and $F_r(\cdot)$.

Lemma 1: Let $r \geq 2$ and $F_r(x) = 2 - \dfrac{1}{x^r}$.

(a) The equation $x = F_r(x)$ has two solutions in the interval $(0, \infty)$. One solution is 1 and the other, noted α_r, is in the interval $(1, 2)$.

(b) Let $\{x_i\}_{i=0}^{\infty}$ be a sequence defined by $x_{i+1} = F_r(x_i)$ for $i = 0, 1, 2, \ldots$.

  (i) If $x_0 \in (1, \alpha_r)$, the sequence $\{x_i\}_{i=0}^{\infty}$ is strictly increasing and converges to α_r.

(ii) If $x_0 \in (\alpha_r, \infty)$, the sequence $\{x_i\}_{i=0}^{\infty}$ is strictly decreasing and converges to α_r.

Proof: If $x \in (0, \infty)$, then

$$F'(x) = \frac{r}{x^{r+1}} > 0 \quad \text{and} \quad F''(x) = \frac{r(r+1)}{x^{r+2}} < 0;$$

hence, $F_r(\cdot)$ is a strictly increasing continuous concave function on $(0, \infty)$. Also

$$\lim_{x \to 0^+} F_r(x) = -\infty, \quad \lim_{x \to +\infty} F_r(x) = 2,$$

$F_r(1) = 1$ and $F'(1) = r > 1$, then $F_r(x) < x$ on $(0, 1)$ and there exists a real number α_r such that $F_r(x) > x$ on $(1, \alpha_r)$ and $F_r(x) < x$ on (α_r, ∞) (see Figure 1). The results follow from these observations. □

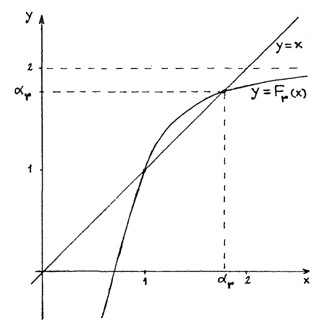


FIGURE 1. Graph of $y = F_r(x)$

Lemma 2: Let $r \geq 2$ and let

$$f_r(x) = 1 + \sum_{i=2}^{r} \frac{1}{x^{i-1}}.$$

The equation $x = f_r(x)$ has a unique solution β_r in the interval $(0, \infty)$. Also β_r is the unique positive root of the polynomial

$$p_r(x) = x^r - \sum_{i=1}^{r} x^{r-i}.$$

Proof: If $x \in (0, \infty)$, we have

$$f_r'(x) = -\sum_{i=2}^{r} \frac{(i-1)}{x^i} < 0 \quad \text{and} \quad f_r''(x) = \sum_{i=2}^{r} \frac{i(i-1)}{x^{i+1}} > 0;$$

therefore, $f_r(\cdot)$ is a strictly decreasing continuous convex function on $(0, \infty)$. Also

$$\lim_{x \to 0^+} f_r(x) = +\infty \quad \text{and} \quad \lim_{x \to +\infty} f_r(x) = 1 \text{ (see Figure 2).}$$

It follows that there exists a unique positive x such that $x = f_r(x)$. Also, for $x > 0$, $x = f_r(x)$ is equivalent to

$$x^r = \sum_{i=1}^{r} x^{r-i}$$

and the result follows. □

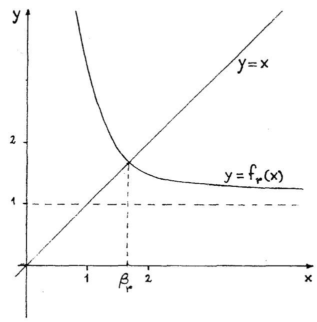


FIGURE 2. Graph of $y = f_r(x)$

Lemma 3: Let $r \geq 2$. For $x \neq 1$, $x = f_r(x)$ is equivalent to $x = F_r(x)$, and it follows that

$$\beta_r = \alpha_r \in \left(2\left(1 - \frac{1}{2^r}\right),\ 2\right).$$

Proof: $x = F_r(x)$ is equivalent to $x^r(x - 1) = x^r - 1$. For $x \neq 1$, $x = F_r(x)$ is equivalent to

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

which is also equivalent to $x = f_r(x)$. Hence,

$$\alpha_r = f_r(\alpha_r) \geq f_r(2) = 2\left(1 - \frac{1}{2^r}\right). \quad \square$$

From Lemmas 1-3 we can conclude that i) the sequence $\{B_{r,\ell}\}_{\ell=0}^{\infty}$ is strictly decreasing and converges to α_r, ii) the sequence $\{b_{r,\ell}\}_{\ell=0}^{\infty}$ is strictly increasing and converges to α_r. Then, using (4), we have the following result.

Theorem 1: Let $r \geq 2$, $u_{r,n}$ given by (1), and

$$t_{r,n} = \frac{u_{r,n}}{u_{r,n-1}} \qquad \text{for } n \geq 1.$$

The sequence $\{t_{r,n}\}_{n=1}^{\infty}$ converges to the unique positive root α_r of the polynomial

$$p_r(x) = x^r - \sum_{i=1}^{r} x^{r-i}. \quad \square$$

We could call α_r the r-generalized golden number; hence, we have the following result.

Theorem 2: The sequence of r-generalized golden numbers $\{\alpha_r\}_{r=2}^{\infty}$ is a strictly increasing sequence converging to 2.

Proof: Let $2 \le r_1 \le r_2$. We have $F_{r_1}(x) < F_{r_2}(x)$ for all $x \in (1, \infty)$; Hence,

$$\alpha_{r_1} = F_{r_1}(\alpha_{r_1}) < F_{r_2}(\alpha_{r_1}).$$

It follows that $\alpha_{r_1} \in (1, \alpha_{r_2})$. Then the sequence $\{\alpha_r\}_{r=2}^{\infty}$ is strictly increasing and upper bounded by 2. It converges and we have

$$\lim_{r \to \infty} \alpha_r = \lim_{r \to \infty}\left(2 - \frac{1}{\alpha_r^r}\right) = 2. \quad \square$$

Remark 1: Somer [8] considered the proof of Theorem 2 based on continued fractions.

Remark 2: We have shown that α_r is the unique positive root of the polynomial

$$p_r(x) = x^r - \sum_{i=1}^{r} x^{r-i}.$$

We can also easily observe that $p_r(x)$ has

(i) only one negative real root if r is even,
(ii) no negative real root if r is odd,

because $p_r(x) = 0$ is equivalent to

$$x^r = \frac{x^r - 1}{x - 1} \quad \text{for } x < 0$$

(see Miles [5] for a complete study of the polynomial $p_r(x)$).

Remark 3: We could consider that $u_{r,i}$ are given positive real numbers for $i = 0, \ldots, r - 1$ and that $u_{r,n}$ are generated using (1c) for $n \ge r$. In this way, we could show that $t_{r,n} \ge 1$ for $n \ge r$ and $t_{r,n} \le 2$ for $n \ge 2r$. More generally, it follows that we could start with any given real numbers $u_{r,i}$ ($i = 0, \ldots, r - 1$) and use the method described here to show

$$\lim_{n \to \infty} t_{r,n} = \alpha_r,$$

which is the positive root of $p_r(x)$, as soon as r successive values $u_{r,i}$ of the same sign appear.

2. A Geometric Interpretation

Let us consider the sequence of r-tuples $\{\vec{v}_{r,n}\}_{n=0}^{\infty}$ generated by induction. Let $\vec{v}_{r,0} = (u_{r,0}, u_{r,1}, \ldots, u_{r,r-1})$. Assuming that $\vec{v}_{r,j}$ is already generated for $j = 0, \ldots, n - 1$, we generate $\vec{v}_{r,n}$ as follows:

(i) determine the unique integers i and k such that $n = i + kr$, $0 < i \le r$ and $k \ge 0$ [in other words, $i = 1 + (n - 1) \bmod r$],

(ii) the coordinates of $\vec{v}_{r,n}$ are those of $\vec{v}_{r,n-1}$ except for the i^{th} coordinate of $\vec{v}_{r,n}$ which is the sum of the r coordinates of $\vec{v}_{r,n-1}$.

From this construction, we can show that the coordinates of $\vec{v}_{r,n}$ are successively $u_{r,n}, u_{r,n+1}, \ldots, u_{r,n+r-1}$ where $u_{r,n+r-1}$ is the i^{th} coordinate, and the sum of the coordinates of $\vec{v}_{r,n}$ is $u_{r,n+r}$.

To each $\vec{v}_{r,n}$ we can associate the parallelepiped rectangle in $\mathbb{R}^r$ having this point as the vertex that is not on the axis. This construction for $r > 2$ is a natural generalization of what happens in the case $r = 2$. Figures 3 and 4 illustrate the cases $r = 2$ and $r = 3$, respectively.

$$\vec{v}_{2,0} = (1,\ 1)$$
$$\vec{v}_{2,1} = (2,\ 1)$$
$$\vec{v}_{2,2} = (2,\ 3)$$
$$\vec{v}_{2,3} = (5,\ 3)$$
$$\vec{v}_{2,4} = (5,\ 8)$$
$$\vec{v}_{2,5} = (13,\ 8)$$
$$\vdots$$

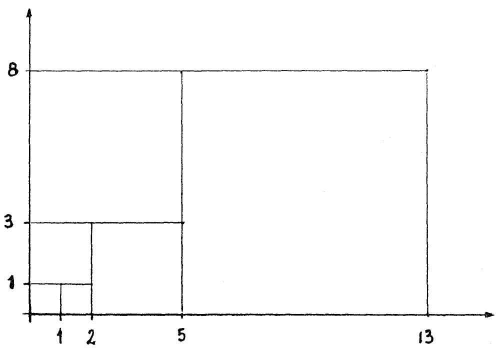


FIGURE 3. Case $r = 2$

$$\vec{v}_{3,0} = (1,\ 1,\ 2)$$
$$\vec{v}_{3,1} = (4,\ 1,\ 2)$$
$$\vec{v}_{3,2} = (4,\ 7,\ 2)$$
$$\vec{v}_{3,3} = (4,\ 7,\ 13)$$
$$\vec{v}_{3,4} = (24,\ 7,\ 13)$$
$$\vec{v}_{3,5} = (24,\ 44,\ 13)$$
$$\vdots$$

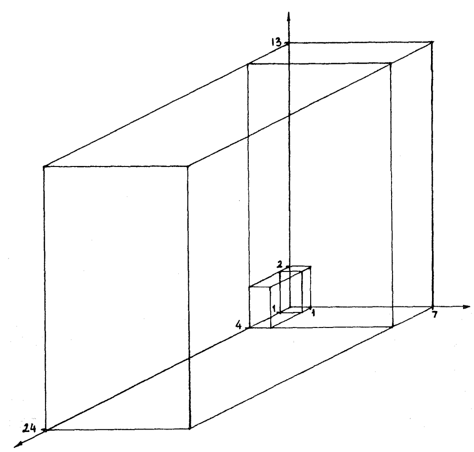


FIGURE 4. Case $r = 3$

Normalizing the vectors $\vec{v}_{r,n}$ with respect to the uniform norm $\|\cdot\|_\infty$, we observe that

$$\lim_{k\to\infty} \frac{\vec{v}_{r,\,i+kr}}{\|\vec{v}_{r,\,i+kr}\|_\infty} = \vec{d}_{r,\,i} \qquad (i = 1,\ \ldots,\ r)$$

where $\vec{d}_{r,i}$ is a unit vector, with respect to the uniform norm, having the coordinates $1/\alpha_r^{r-1}$, $1/\alpha_r^{r-2}$, ..., $1/\alpha_r^2$, $1/\alpha_r$, 1, and such that 1 is the i^{th} coordinate. Figures 5 and 6 illustrate the vectors $\vec{d}_{r,i}$ $(i = 1, \ldots, r)$ for $r = 2$ and $r = 3$, respectively.

$$\alpha_2 = 1.618034\ldots$$
$$\vec{d}_{2,1} = (1,\ 1/\alpha_2)$$
$$\vec{d}_{2,2} = (1/\alpha_2,\ 1)$$

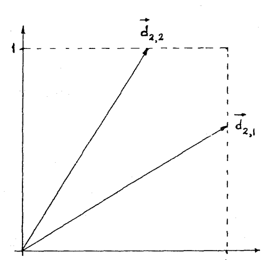


FIGURE 5. Case $r = 2$

$$\alpha_3 = 1.8392868\ldots$$
$$\vec{d}_{3,1} = (1,\ 1/\alpha_3^2,\ 1/\alpha_3)$$
$$\vec{d}_{3,2} = (1/\alpha_3,\ 1,\ 1/\alpha_3^2)$$
$$\vec{d}_{3,3} = (1/\alpha_3^2,\ 1/\alpha_3,\ 1)$$

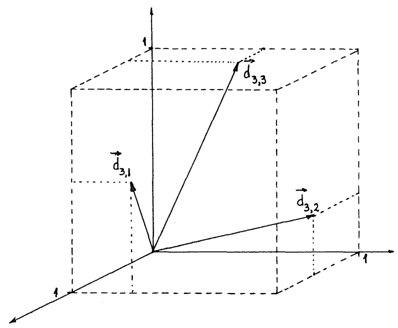


FIGURE 6. Case $r = 3$

Moreover, the volume V of the parallelepiped generated by the vectors $\vec{d}_{r,1}$, $\vec{d}_{r,2}$, ..., $\vec{d}_{r,r}$ is

$$V_r = \det(\vec{d}_{r,1}, \ldots, \vec{d}_{r,r}) = \left(1 - \frac{1}{\alpha_r^r}\right)^{r-1}.$$

Since $\lim\limits_{r \to +\infty} \alpha_r = 2$, it follows that $\lim\limits_{r \to \infty} V_r = 1$.

We can present an informal interpretation of the last result. If we consider coordinatewise convergence, we can define for the sequence $\{\vec{d}_{r,i}\}_{r=i}^{\infty}$ the limit

$$\vec{d}_{\infty,i} = \lim_{r \to \infty} \vec{d}_{r,i} = (2^{1-i},\ 2^{2-i},\ \ldots,\ 2^{-2},\ 2^{-1},\ 1,\ 0,\ 0,\ \ldots)$$

which is a vector in the infinite-dimensional euclidean space $\mathbb{R}^{\infty}$ (or the set of infinite sequences). Hence, the semi-infinite determinant

$$V_{\infty} = \det(\vec{d}_{\infty,1},\ \vec{d}_{\infty,2},\ \ldots) = \lim_{r \to \infty} V_r$$

is triangular and has 1's along the diagonal, so $V_{\infty} = 1$.

3. Electrical Schemes

It is well known that we can generate the sequence

$$\left\{\frac{u_{2,n+1}}{u_{2,n}}\right\}_{n=0}^{\infty}$$

using electrical circuits (see [1], [2], [3], [4], [6], [7]). Recently, Beran [2] wondered if it was also possible for the sequence

$$\left\{\frac{u_{3,n+1}}{u_{3,n}}\right\}_{n=0}^{\infty}.$$

We present here one method to generate the sequence

$$\left\{\frac{u_{r,n+1}}{u_{r,n}}\right\}_{n=0}^{\infty}$$

using electrical circuits.

Let us define the resistances

$$\Omega^r_{j,i} = \frac{u_{r,j+i}}{u_{r,j}}$$

for $j \geq 0$ and $i \geq -j$. Hence defined, connecting in series r successive resistances

$$\Omega^r_{j,i+k} \ (k = 0, \ldots, r-1)$$

we obtain the resistance next to the last one $\Omega^r_{j,i+r}$ because

$$\Omega^r_{j,i+r} = \sum_{k=0}^{r-1} \Omega^r_{j,i+k}.$$

Also, connecting in parallel r successive resistances

$$\Omega^r_{j+k,i} \ (k = 0, \ldots, r-1)$$

we obtain again the resistance next to the last one $\Omega^r_{j+r,i}$ because

$$\Omega^r_{j+r,i} = \frac{1}{\sum_{k=0}^{r-1} 1/\Omega^r_{j+k,i}}.$$

Using these observations, we can generate a sequence of sets $\{S^r_n\}^\infty_{n=0}$, where S^r_n is the set of resistances having values $\Omega^r_{n,i}$ for $i = -r, -r+1, \ldots, -1, 0, 1, \ldots, r-1, r$. The process is by induction.

For $n = 0$, we have:

(i) $\Omega^r_{0,i} = 0$ for $i = -r, \ldots, -1$;

(ii) $\Omega^r_{0,0} = 1$;

(iii) $\Omega^r_{0,i} = \sum_{j=1}^{i} \Omega^r_{0,i-j}$ for $i = 1, \ldots, r$.

Assuming that the resistances in the sets $S^r_0, S^r_1, S^r_2, \ldots, S^r_{n-1}$ are available, we can generate the resistances in the set S^r_n as follows:

(i) for $i = -r, \ldots, -1$, we have $\Omega^r_{n,i} = \dfrac{1}{\sum_{j=1}^{r} 1/\Omega^r_{n-j,j+i}}$

and $\Omega^r_{n-j,j+i} \in S^r_{n-j}$ for $j = 1, \ldots, r$

(in these expressions we do not consider a term for which the index j is such that $n - j < 0$). Then the resistance $\Omega^r_{n,i}$ can be constructed if we use the already constructed resistances and connect them in parallel.

(ii) $\Omega^r_{n,0} = 1$.

(iii) for $i = 1, \ldots, r$, we have $\Omega^r_{n,i} = \sum_{j=1}^{r} \Omega^r_{n,i-j}$,

where $\Omega^r_{n,i-j} \in S^r_n$ for $j = 1, \ldots, r$.

These resistances are already known and can be connected in series to obtain the desired resistance.

If we consider the rational resistances hence built, in each set S^r_n their smallest common denominator is $u_{r,n}$ if we start with $u_{r,0}, \ldots, u_{r,r-1}$ having no common factor, i.e., $(u_{r,0}, u_{r,1}, \ldots, u_{r,r-1}) = 1$. Then, if we write these rational numbers using their common denominator $u_{r,n}$, the numerators form the sequence $\{u_{r,n+i}\}_{i=-r}^{r}$.

References

1. S. L. Basin. "The Appearance of Fibonacci Numbers and the Q Matrix in Electrical Network Theory." *Math. Mag.* *36* (1963):84-97.
2. L. Beran. "Schemes Generating the Fibonacci Sequence." *Math. Gazette 70* (1986):38-40.
3. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin, 1969.
4. V. E. Hoggatt, Jr., & M. Bicknell. "A Primer for the Fibonacci Numbers: Part XIV." *Fibonacci Quarterly 12* (1974):147-156.
5. E. P. Miles. "Generalized Fibonacci Numbers and Associated Matrices." *Amer. Math. Monthly 67* (1960):745-752.
6. A. M. Morgan-Voyce. "Ladder Network Analysis Using Fibonacci Numbers." *IRE Transactions on Circuit Theory*, Vol. CT-6, September 1959, pp. 321-322.
7. W. P. Risk. "Thevenin Equivalents of Ladder Networks." *Fibonacci Quarterly 20* (1982):245-248.
8. L. Somer. Problem H-197 (and solution). *Fibonacci Quarterly 12* (1974) 110-111.

*****

NOTE ON A FAMILY OF FIBONACCI-LIKE SEQUENCES

John C. Turner

University of Waikato, Hamilton, New Zealand

(Submitted May 1987)

In [2] P. Asveld gave a solution to the recurrence relation

$$G_n = G_{n-1} + G_{n-2} + \sum_{j=0}^{k} \alpha_j n^j \text{ with } G_0 = G_1 = 1. \tag{1}$$

In [2] we showed that the solution to the recurrence relation

$$G_n = G_{n-1} + G_{n-2} + S_n,\ G_1 = S_1,\ G_2 = S_1 + S_2, \tag{2}$$

where S_n is the n^{th} term of *any* sequence $\{S_n\} \equiv S$, is given by the n^{th} term of the convolution of the Fibonacci sequence F with the sequence S. That is, the solution of (2) can be expressed as

$$G_n = (F * S)_n,$$

using $*$ to mean *convolution*.

This note shows how Asveld's family can be dealt with by the convolution technique, using generating functions. Although we do not work through the details in the note, it is clear that a comparison of the two final solutions would yield interesting identities relating Asveld's tabulated polynomials and coefficients, and the coefficients from our solution.

Solution Method

Comparing (1) and (2), we see that the sequence on the right-hand side is:

$$S \equiv \{S_n\} = \sum_{j=0}^{k} \alpha_j n^j;$$

but the initial conditions differ since G_0, G_1 both equal 1 rather than S_1 and $(S_1 + S_2)$, respectively. However, it may quickly be ascertained that with $G_0 = G_1 = 1$ Asveld's equation is satisfied by

$$G_n = F_{n+1} + (F * S')_{n-1}, \text{ where } S' = \{s_2, s_3, s_4, \ldots\}. \tag{3}$$

Now the generating function of F is $f(x) = 1/(1 - x - x^2)$. To find the generating function of S', we note that α_0 is generated by $\alpha_0/(1 - x)$, and $\alpha_j n^j$ by

$$\alpha_j \frac{d}{dx}(xg_{j-1}(x)) \text{ for } j = 1, \ldots, k,$$

where $g_i(x)$ refers to the generating function of n^i and $g_0(x) = 1/(1 - x)$. It follows that the generating function of S' is:

$$g(x) = \frac{1}{x}\left[\frac{\alpha_0}{1 - x} + \frac{\alpha_1}{(1 - x)^2} + \frac{\alpha_2(1 + x)}{(1 - x)^3} + \cdots + \alpha_k \frac{d}{dx}\left(xg_{k-1}(x)\right) - \sum_{j=0}^{k} \alpha_j\right]. \tag{4}$$

Finally, from (3) and (4), we know that the solution of (1) is, for $n \geq 2$:

$$G_n = F_{n+1} + C_{n-2}, \tag{5}$$

where C_{n-2} is the coefficient of x^{n-2} in the product of generating functions $f(x)$, $g(x)$, with $G_0 = G_1 = 1$.

Comparison of Solutions

As stated above, we do not wish in this note to go into the algebraic detail necessary to make a full comparison of the two types of solution. It will be instructive, however, to show the two solutions with a small value of k. We shall set $k = 2$, and then $S_n = \alpha_0 + \alpha_1 n + \alpha_2 n^2$. The solutions are:

Asveld's Solution:

$$G_n = (1 + a_{00}\alpha_0 + a_{01}\alpha_1 + a_{02}\alpha_2)F_{n+1} + \lambda_2 F_n - \sum_{j=0}^{2} \alpha_j p_j(n), \tag{6}$$

where

$$p_j(n) = \sum_{i=0}^{j} a_{ij} n^i \quad \text{and} \quad \lambda_2 = \alpha_1 + (1 + a_{12})\alpha_2,$$

and the coefficients a_{ij}

$$\left.\begin{aligned} a_{ii} &= 1 \\ a_{ij} &= -\sum_{m=i+1}^{j} \beta_{im} a_{mj}, \text{ if } j > i \end{aligned}\right\} \text{with } \beta_{im} = \binom{m}{i}(-1)^{m-i}(1 + 2^{m-i}).$$

Asveld [1] tabulates the coefficients of the α_j's in (6), and with these coefficients equation (6) reduces to the following:

$$G_n = (1 + \alpha_0 + 3\alpha_1 + 13\alpha_2)F_{n+1} + (\alpha_1 + 7\alpha_2)F_n - [\alpha_0 + (n+3)\alpha_1 + (n^2 + 6n + 13)\alpha_2], \tag{7}$$

where $\{F_n\}$ is the Fibonacci sequence $\{1, 1, 2, 3, 5, \ldots\}$.

Turner's Solution:

For $n \geq 2$, from (5) we see that

$$G_n = F_{n+1} + C_{n-2},$$

where C_{n-2} is the coefficient of x^{n-2} in the expansion of

$$\frac{1}{x(1 - x - x^2)}\left[\frac{\alpha_0}{1 - x} + \frac{\alpha_1}{(1 - x)^2} + \frac{\alpha_2(1 + x)}{(1 - x)^3} - (\alpha_0 + \alpha_1 + \alpha_2)\right]$$

$$= (1 - x - x^2)^{-1}(1 - x)^{-3}[(\alpha_0 + 2\alpha_1 + 4\alpha_2) - (2\alpha_0 + 3\alpha_1 + 3\alpha_2)x + (\alpha_0 + \alpha_1 + \alpha_2)x^2].$$

This gives

$$G_n = F_{n+1} + \alpha_0(a - 2b + c) + \alpha_1(2a - 3b + c) + \alpha_2(4a - 3b + c), \tag{8}$$

where $a = (F * B)_{n-1}$, $b = (F * B)_{n-2}$, and $c = (F * B)_{n-3}$, with F the Fibonacci sequence and B the sequence of binomial coefficients

$$\binom{2}{0}, \binom{3}{1}, \binom{4}{2}, \ldots, \binom{n+1}{n-1}, \ldots .$$

[N.B. the expressions $(F * B)_i$ are to be set to zero if $i \leq 0$.]

Corresponding coefficients in (7) and (8) may now be compared, and, as promised above, interesting identities result. Thus:

Coefficients of α_0: $F_{n+1} - 1 = a - 2b + c$;

Coefficients of α_1: $3F_{n+1} + F_n - (n + 3) = 2a - 3b + c$;

Coefficients of α_2: $13F_{n+1} + 7F_n - (n^2 + 6n + 13) = 4a - 3b + c$.

These in themselves are identities relating the Fibonacci terms and the convolutions with binomial coefficients.

Solving the three equations for a, b, and c, and taking the sum $a + b + c$, leads to the identity

$$\sum_{i=1}^{3} (F * B)_{n-i} \equiv 2F_{n+5} - \tfrac{1}{2}(3n^2 + 9n + 20). \tag{9}$$

Using (9) we can obtain

$$(F * B)_n - (F * B)_{n-3} \equiv 2F_{n+4} - 3(n + 2). \tag{10}$$

Then, setting $n = 3i - 2$ in (10) and summing over $i = 1, 2, 3, \ldots, N$, we obtain

$$(F * B)_{3N-2} \equiv F_{3N+4} - \tfrac{3}{2}(3N^2 + 3N + 2). \tag{11}$$

Similar identities may be obtained for $(F * B)_{3N-1}$ and $(F * B)_{3N}$.

Clearly, repeating these procedures for $k = 3, 4, \ldots$ would lead to more and more complex identities of this type.

References

1. P. R. J. Asveld. "A Family of Fibonacci-Like Sequences." *Fibonacci Quarterly* *25.1* (1987):81-83.
2. J. C. Turner. "Convolution Trees and Pascal-T Triangles." *Fibonacci Quarterly* (to appear).

*****

MORE ON THE FIBONACCI PSEUDOPRIMES

Adina Di Porto and Piero Filipponi
Fondazione Ugo Bordoni, Roma, Italy
(Submitted May 1987)

1. Generalities

The idea of writing this note was triggered by the necessity that occurred in the course of our research job, of expressing the quantity $x^n + y^n$ (x and y arbitrary quantities, n a nonnegative integer) in terms of powers of xy and $x + y$. Such expressions, commonly referred to as *Waring formulae*, are given in high school books and others (e.g., see [1]) only for the first few values of n, namely

$$\begin{cases} x^0 + y^0 = 2 \\ x^1 + y^1 = x + y \\ x^2 + y^2 = (x + y)^2 - 2xy \\ x^3 + y^3 = (x + y)^3 - 3xy(x + y) \\ x^4 + y^4 = (x + y)^4 - 4xy(x + y)^2 + 2(xy)^2. \end{cases} \tag{1.1}$$

Without claiming the novelty of the result, we found (see [2]) the following general expression

$$x^n + y^n = \sum_{k=0}^{[n/2]} (-1)^k C_{n,k} (xy)^k (x + y)^{n-2k}, \tag{1.2}$$

where

$$\begin{cases} C_{0,0} = 2 \\ C_{n,k} = \dfrac{n}{n-k}\dbinom{n-k}{k} = nB_{n,k} \quad (n \ge 1) \end{cases} \tag{1.3}$$

and $[a]$ denotes the greatest integer not exceeding a.

Several interesting combinatorial and trigonometrical identities emerge (see [2]) from certain choices of x and y in (1.2). In particular, sensing Lucas numbers L_n on the left-hand side of (1.2) is quite natural for a Fibonacci fan. In fact, replacing x and y by $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$, respectively, we get

Work carried out in the framework of the Agreement between the Fondazione "Ugo Bordoni" and the Italian PPT Administration.

$$L_n = \sum_{k=0}^{[n/2]} C_{n,k} \quad (n \geq 0), \tag{1.4}$$

that is

$$L_n = 1 + nS_n \quad (n \geq 1), \tag{1.5}$$

where

$$S_n = \sum_{k=1}^{[n/2]} \frac{1}{n-k}\binom{n-k}{k} = \sum_{k=1}^{[n/2]} B_{n,k}. \tag{1.6}$$

We point out that the equality (1.5) can also be obtained using the relationships (see [3], [4])

$$L_n = F_{n-1} + F_{n+1} \tag{1.7}$$

$$F_{n+1} = \sum_{k=0}^{[n/2]} \binom{n-k}{k}, \tag{1.8}$$

where F_n stands for the n^{th} Fibonacci number.

Observing (1.5), the following question arises spontaneously:

"When is the congruence

$$L_n \equiv 1 \pmod{n} \quad (n > 1) \tag{1.9}$$

verified?"

The obvious answer is:

"The congruence (1.9) holds iff S_n is integral."

Theorem 1: If n is relatively prime to k $(1 \leq k \leq [n/2])$, then $B_{n,k}$ is a positive integer.

Proof: The statement holds clearly for $k = 1$. Consequently, let us consider the case $2 \leq k \leq [n/2]$. Letting

$$P_{n,k} = \prod_{j=1}^{k-1}(n - k - j), \tag{1.10}$$

it suffices to prove that, if n is relatively prime to k, then $P_{n,k}/k!$ is integral. It is known [5] that

$$P_{n,k} \equiv 0 \pmod{(k-1)!},$$

that is,

$$A_{n,k} = P_{n,k}/(k-1)! \tag{1.11}$$

is an integer. Again, from [5] we have

$$(n-k)P_{n,k} \equiv 0 \pmod{k!} \tag{1.12}$$

whence, dividing both the two sides and the modulus by $(k-1)!$, we can write

$$(n-k)A_{n,k} \equiv 0 \pmod{k}, \tag{1.13}$$

see [6, Ch. 3., Sec. 3(b)]. If n is relatively prime to k, from (1.13) it follows that

$$n - k \not\equiv 0 \pmod{k}, \tag{1.14}$$

$$A_{n,k} \equiv 0 \pmod{k}. \tag{1.15}$$

From (1.15) and (1.11), it appears that, if n is relatively prime to k, then

$$P_{n,k} \equiv 0 \pmod{k!}. \quad \text{Q.E.D.}$$

From Theorem 1 it follows that, if n is prime, all addends $B_{n,k}$, cf. (1.6), are integral. Therefore, S_n is integral. This is a further proof of the well-known result (see [7])

$$L_n \equiv 1 \pmod{n} \quad \text{(if } n \text{ is a prime).} \tag{1.16}$$

2. On the Fibonacci Pseudoprimes

The sum S_n can be integral also if n is not a prime. In particular, this sum can also be integral if two or more of its addends $B_{n,k}$ are not integral. The composite numbers n which satisfy this property, i.e., for which congruence (1.9) holds, are called *Fibonacci Pseudoprimes* (see [8]), which we abbreviate *F.Psps.* and denote by Q_k ($k = 1, 2, \ldots$).

Proposition 1: A composite number n is a F.Psp. iff S_n is integral.

The smallest F.Psp. is $Q_1 = 705$. It was discovered by M. Pettet in 1966 [9] who discovered also $Q_2 = 2465$ and $Q_3 = 2737$, but we cannot forget the unbelievable misfortune of D. Lind [10] who in 1967 limited his computer experiment for disproving the converse of (1.6) to $n = 700$, thus missing the mark by a hair's breadth. In the early 1970s, J. Greener (Lawrence Livermore Lab.) discovered Q_4 and Q_5 [7]. To the best of our knowledge, the F.Psps. are known up to $Q_7 = 6721$. The discovery of Q_6 and Q_7 is due to G. Logothetis [8].

Curiosity led us to discover many more F.Psps. Using the facilities of the Istituto Superiore P.T. (the Italian Telecommunication Ministry), a weighty computer experiment was carried out to find all F.Psps. within the interval $[2, 10^6]$. They are shown in Table 1 together with their canonical factorization. The computational algorithm is outlined in Section 3, where a worked example is also appended.

Inspection of Table 1 suggests some considerations on the basis of which we state several propositions and theorems. Most of them show that certain classes of integers are not F.Psps., thus extending the results established in [8, Sec. 6]. Some conjectures can also be formulated.

Consideration 1: No even F.Psps. occur in Table 1.

Proposition 2:

(i) $L_{6n} \not\equiv 1 \pmod{6n}$

(ii) $L_{6n+2} \not\equiv 1 \pmod{6n+2}$ (n odd)

(iii) $L_{6n+4} \not\equiv 1 \pmod{6n+4}$ (n even)

Proof:

(i) The congruence $L_{6n} \equiv 0 \pmod{2}$ implies that $6n \nmid L_{6n} - 1$.

(ii) Using the identities [11, formula (11)] and I_{23}, I_{22} (from [3]), it can be proved that

$$(L_{6n+2} - 1)/2 = F_{6n+2} + \sum_{k=1}^{2n-1} F_{3k}. \tag{2.1}$$

Since $F_{3k} \equiv 0 \pmod{2}$ and $F_{6n+2} \equiv 1 \pmod{2}$, the quantity on the left-hand side of (2.1) is clearly odd, that is,

$$L_{6n+2} - 1 \not\equiv 0 \pmod{4}.$$

Since, for n odd, the congruence $6n + 2 \equiv 0 \pmod 4$ holds, it follows that

$$6n + 2 \nmid L_{6n+2} - 1 \quad (n \text{ odd}).$$

(iii) The proof is similar to that of (ii) and is omitted for brevity. Q.E.D.

TABLE 1

Q_1	705	$= 3 \cdot 5 \cdot 47$	Q_{44}	252601	$= 41 \cdot 61 \cdot 101$
Q_2	2465	$= 5 \cdot 17 \cdot 29$	Q_{45}	254321	$= 263 \cdot 967$
Q_3	2737	$= 7 \cdot 17 \cdot 23$	Q_{46}	257761	$= 7 \cdot 23 \cdot 1601$
Q_4	3745	$= 5 \cdot 7 \cdot 107$	Q_{47}	268801	$= 13 \cdot 23 \cdot 29 \cdot 31$
Q_5	4181	$= 37 \cdot 113$	Q_{48}	272611	$= 131 \cdot 2081$
Q_6	5777	$= 53 \cdot 109$	Q_{49}	283361	$= 13 \cdot 71 \cdot 307$
Q_7	6721	$= 11 \cdot 13 \cdot 47$	Q_{50}	302101	$= 317 \cdot 953$
Q_8	10877	$= 73 \cdot 149$	Q_{51}	303101	$= 101 \cdot 3001$
Q_9	13201	$= 43 \cdot 307$	Q_{52}	327313	$= 7 \cdot 19 \cdot 23 \cdot 107$
Q_{10}	15251	$= 101 \cdot 151$	Q_{53}	330929	$= 149 \cdot 2221$
Q_{11}	24465	$= 3 \cdot 5 \cdot 7 \cdot 233$	Q_{54}	399001	$= 31 \cdot 61 \cdot 211$
Q_{12}	29281	$= 7 \cdot 47 \cdot 89$	Q_{55}	430127	$= 463 \cdot 929$
Q_{13}	34561	$= 17 \cdot 19 \cdot 107$	Q_{56}	433621	$= 199 \cdot 2179$
Q_{14}	35785	$= 5 \cdot 17 \cdot 421$	Q_{57}	438751	$= 541 \cdot 811$
Q_{15}	51841	$= 47 \cdot 1103$	Q_{58}	447145	$= 5 \cdot 37 \cdot 2417$
Q_{16}	54705	$= 3 \cdot 5 \cdot 7 \cdot 521$	Q_{59}	455961	$= 3 \cdot 11 \cdot 41 \cdot 337$
Q_{17}	64079	$= 139 \cdot 461$	Q_{60}	489601	$= 7 \cdot 23 \cdot 3041$
Q_{18}	64681	$= 71 \cdot 911$	Q_{61}	490841	$= 13 \cdot 17 \cdot 2221$
Q_{19}	67861	$= 79 \cdot 859$	Q_{62}	497761	$= 11 \cdot 37 \cdot 1223$
Q_{20}	68251	$= 131 \cdot 521$	Q_{63}	512461	$= 31 \cdot 61 \cdot 271$
Q_{21}	75077	$= 193 \cdot 389$	Q_{64}	520801	$= 241 \cdot 2161$
Q_{22}	80189	$= 17 \cdot 53 \cdot 89$	Q_{65}	530611	$= 461 \cdot 1151$
Q_{23}	90061	$= 113 \cdot 797$	Q_{66}	556421	$= 431 \cdot 1291$
Q_{24}	96049	$= 139 \cdot 691$	Q_{67}	597793	$= 7 \cdot 23 \cdot 47 \cdot 79$
Q_{25}	97921	$= 181 \cdot 541$	Q_{68}	618449	$= 13 \cdot 113 \cdot 421$
Q_{26}	100065	$= 3 \cdot 5 \cdot 7 \cdot 953$	Q_{69}	635627	$= 563 \cdot 1129$
Q_{27}	100127	$= 223 \cdot 449$	Q_{70}	636641	$= 461 \cdot 1381$
Q_{28}	105281	$= 11 \cdot 17 \cdot 563$	Q_{71}	638189	$= 619 \cdot 1031$
Q_{29}	113573	$= 137 \cdot 829$	Q_{72}	639539	$= 43 \cdot 107 \cdot 139$
Q_{30}	118441	$= 83 \cdot 1427$	Q_{73}	655201	$= 23 \cdot 61 \cdot 467$
Q_{31}	146611	$= 271 \cdot 541$	Q_{74}	667589	$= 13 \cdot 89 \cdot 577$
Q_{32}	161027	$= 283 \cdot 569$	Q_{75}	687169	$= 7 \cdot 89 \cdot 1103$
Q_{33}	162133	$= 73 \cdot 2221$	Q_{76}	697137	$= 3 \cdot 7 \cdot 89 \cdot 373$
Q_{34}	163081	$= 17 \cdot 53 \cdot 181$	Q_{77}	722261	$= 491 \cdot 1471$
Q_{35}	179697	$= 3 \cdot 7 \cdot 43 \cdot 199$	Q_{78}	741751	$= 431 \cdot 1721$
Q_{36}	186961	$= 31 \cdot 37 \cdot 163$	Q_{79}	851927	$= 881 \cdot 967$
Q_{37}	194833	$= 23 \cdot 43 \cdot 197$	Q_{80}	852841	$= 11 \cdot 31 \cdot 41 \cdot 61$
Q_{38}	197209	$= 199 \cdot 991$	Q_{81}	853469	$= 239 \cdot 3571$
Q_{39}	209665	$= 5 \cdot 19 \cdot 2207$	Q_{82}	920577	$= 3 \cdot 7 \cdot 59 \cdot 743$
Q_{40}	219781	$= 271 \cdot 811$	Q_{83}	925681	$= 23 \cdot 167 \cdot 241$
Q_{41}	228241	$= 13 \cdot 97 \cdot 181$	Q_{84}	930097	$= 7 \cdot 23 \cdot 53 \cdot 109$
Q_{42}	229445	$= 5 \cdot 109 \cdot 421$	Q_{85}	993345	$= 3 \cdot 5 \cdot 47 \cdot 1409$
Q_{43}	231703	$= 263 \cdot 881$	Q_{86}	999941	$= 577 \cdot 1733$

It must be noted that the well-known result [7] $L_{2^k} \not\equiv 1 \pmod{2^k}$ $(k \geq 2)$ appears to be included in the incongruences (ii) and (iii).

Proposition 2 can be summarized by the following

Theorem 2: If n is even but $n \neq 2(6k \pm 1)$ $(k = 1, 2, \ldots)$, then n is not a F.Psp.

The set of integers of the form $2(6k \pm 1)$ contains all numbers that are twice a prime greater than 3.

Proposition 3: If $n = 2p$ is twice a prime and $1 \leq k \leq p - 1$, then the fractional part of $B_{n,k}$ is either 0 or 1/2.

The proof of Proposition 3 is based on the argument used in the proof of Theorem 1 and is omitted for brevity.

Since the last term of the sum S_{2p}, cf. (1.6), is $B_{2p,p} = 1/p$, from Proposition 3 it follows that the fractional part of this sum is either $1/p$ or $1/p + 1/2$. Noting that, in the particular case $p = 2$, the fractional part of S_4 is clearly 1/2, from Proposition 1 we have

Theorem 3: If n is twice a prime, then n is not a F.Psp.

On the other hand, the same result can be obtained using the congruence [7]

$$L_{kp} \equiv L_k \pmod{p} \quad (p \text{ a prime}) \tag{2.2}$$

whence we get $L_{2p} - 1 \equiv 2 \pmod{p}$, that is, $2p \nmid L_{2p} - 1$.

Now, let us consider the integers of the form $2(6k \pm 1)$ with $6k \pm 1$ composite and state the following

Theorem 4: If $n = 2(6k \pm 1)$ and $k \equiv \mp 1 \pmod{5}$ (i.e., if n is even, divisible by 5 and not divisible by 3 and 4), then n is not a F.Psp.

Proof: The identity I_{17} [3] can be rewritten in the form

$$L_{2(2m\pm1)} - 1 = 5F^2_{2m\pm1} - 3$$

whence we obtain the congruence

$$L_{2(2m\pm1)} - 1 \equiv 2 \pmod{5}, \tag{2.3}$$

which implies that $2(6k \pm 1) \nmid L_{2(6k\pm1)} - 1$ if $6k \pm 1 \equiv 0 \pmod{5}$, that is, if $k \equiv \mp 1 \pmod{5}$. Q.E.D.

Finally, we observe that there exist F.Psps. of the form $6k \pm 1$ with $k \not\equiv \mp 1 \pmod{5}$ (e.g., $Q_{65} = 6 \cdot 88435 + 1$ and $Q_{66} = 6 \cdot 92737 - 1$) and state the following

Theorem 5: If $n = 2k + 1$ is a F.Psp., then $2n$ is not a F.Psp.

Proof (reductio ad absurdum): Let us suppose that

$$L_{2(2k+1)} = L_{4k+2} \equiv 1 \pmod{4k+2}. \tag{2.4}$$

From identity I_{18} [3] and (2.4), we can write

$$L_{4k+2} - 2 \equiv -1 \equiv L^2_{2k+1} \pmod{4k+2},$$

whence we obtain the congruence

$$L^2_{2k+1} \equiv -1 \pmod{2k+1} \tag{2.5}$$

which contradicts the assumption. Q.E.D.

Consideration 1, together with Theorems 2, 3, 4, and 5, allows us to offer the following

Conjecture 1: F.Psps. are odd.

Consideration 2: The F.Psps. listed in Table 1 are given by the product of a certain number of distinct primes.

Using (2.2), one can readily prove the following

Theorem 6: If $p_1, p_2, \ldots, p_k$ are distinct odd primes, then $n = p_1p_2 \ldots p_k$ is a F.Psp. iff $L_{n/p_i} \equiv 1 \pmod{p_i}$ ($i = 1, 2, \ldots, k$).

For example, we see that

$$3 \cdot 5 \cdot 47 = Q_1 \Leftrightarrow \begin{cases} L_{15} \equiv 1 \pmod{47} \\ L_{141} \equiv 1 \pmod{5} \\ L_{235} \equiv 1 \pmod{3}. \end{cases}$$

On the basis of Theorem 6, we observe that, if p and q are distinct odd primes $(q > p)$, then

$$L_{pq} \equiv 1 \pmod{pq} \Leftrightarrow \begin{cases} L_p \equiv 1 \pmod{q} \\ L_q \equiv 1 \pmod{p} \end{cases} \quad (q > p). \tag{2.6}$$

Now, the upper congruence on the right-hand side of (2.6) is clearly impossible for $p = 3, 5, 7, 11, 13$. It follows that $n = pq$ is not a F.Psp. for the above values of p. The smallest p such that $n = pq$ is a F.Psp. is $p = 37$.

In [8] the authors show that, for the conjecture $L_n \not\equiv 1 \pmod{n^2}$ $(n > 1)$, it follows that p^k (p a prime, $k > 1$) is not a F.Psp. We formulate the following

Conjecture 2: F.Psps. are square-free.

Consideration 3: The rightmost digits of the F.Psps. listed in Table 1 are not uniformly distributed.

The occurrence frequency $f(c)$ of the rightmost digit c of the F.Psps. within the interval $[2, 10^6]$ is shown in Table 2.

TABLE 2

c	$f(c)$
1	45
3	6
5	11
7	13
9	11

Moreover, it can be noted that, in the same interval, only 17% of the F.Psps. are of the form $4n + 3$. Hence, the F.Psps. congruent to 3 both modulo 4 and modulo 10 are supposedly *very rare*.

Consideration 4: The density of the F.Psps. less than n *shows a comparatively slow decrease as* n *increases, within the interval* $[2, 10^6]$.

Conjecture 3: There are infinitely many F.Psps.

Let $q(n)$ denote the number of F.Psps. smaller than or equal to a given positive integer n. Numerically, the F.Psp.-counting function $q(n)$ seems asymptotically related to the prime-counting function $\pi(n)$ (cf. [4, p. 204].

Conjecture 4: $q(n)$ is asymptotic to $\pi(\sqrt{n})/\alpha$.

The behaviors of $q(n)$ and $\hat{\pi}(\sqrt{n})/\alpha$ vs n are plotted in Figure 1 for $2 \le n \le 10^6$, $\hat{\pi}(x) = x/\ln x$ being the Gauss estimate of $\pi(x)$.

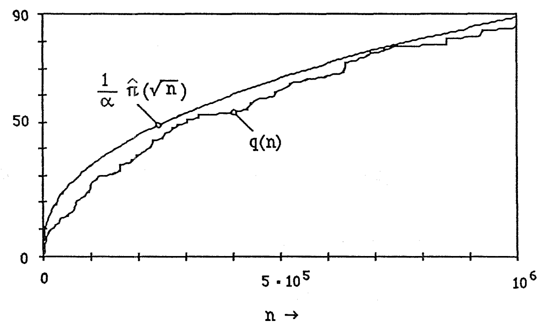


FIGURE 1

Behaviors of $q(n)$ and $\hat{\pi}(\sqrt{n})/\alpha$ vs n

We conclude this section by pointing out that, for a given odd prime p, it is possible to find out necessary (sufficient) conditions for $n = pk$ (k an integer greater than 2) to be (not to be) a F.Psp.

Hinging upon the periodicity of the Lucas sequence reduced modulo p (P being the period), we observe that

$$\begin{cases} L_n \equiv 1 \pmod 3 \text{ iff } n \equiv 1, 3, 4 \pmod 8 \\ L_n \equiv 1 \pmod 5 \text{ iff } n \equiv 1 \pmod 4 \\ L_n \equiv 1 \pmod 7 \text{ iff } n \equiv 1, 7 \pmod{16} \\ L_n \equiv 1 \pmod{11} \text{ iff } n \equiv 1 \pmod{10} \\ \vdots \\ L_n \equiv 1 \pmod p \text{ iff } n \equiv r_1, r_2, \ldots, r_s \pmod P. \end{cases} \tag{2.7}$$

It is readily seen that, if $n = pk \not\equiv r_1, r_2, \ldots, r_s \pmod P$, then $L_{pk} \not\equiv 1 \pmod p$ and *a fortiori* $L_{pk} \not\equiv 1 \pmod{pk}$, that is, $n = pk$ is not a F.Psp. As an example, solving some of the congruences (2.7) $pk \equiv r_1, r_2, \ldots, r_s \pmod P$ in k and taking into account that an even integer not of the form $2(6h \pm 1)$ (cf. Theorem 2) is not a F.Psp., lead to the statement of the following

Theorem 7: If either $n = 3k$ and $k \not\equiv 1, 3 \pmod 8$
or $n = 5k$ and $k \not\equiv 1 \pmod 4$
or $n = 7k$ and $k \not\equiv 1, 7 \pmod{16}$
or $n = 11k$ and $k \not\equiv 1 \pmod{10}$
or $n = 13k$ and $k \not\equiv 1, 13 \pmod{28}$
or $n = 17k$ and $k \not\equiv 1, 17 \pmod{36}$
or $n = 19k$ and $k \not\equiv 1 \pmod{18}$,
then n is not a F.Psp.

Denoting by $M_n = 2^n - 1$ the n^{th} *Mersenne number*, we can state the following corollary to Theorem 7.

Corollary 1: If $n = 2h$ and $h \geq 2$, then M_n is not a F.Psp.

Proof: Since $M_n = 2^{2h} - 1 \equiv 0 \pmod 3$ and $k = (2^{2h} - 1)/3 \equiv 5 \pmod 8$, the proof follows directly from the first statement of Theorem 7. Q.E.D.

Furthermore, considering the following classes of composite integers congruent to 3 modulo 10 (cf. Consideration 3 for $c = 3$):

$$n_1 = 3(10k + 1) \quad (k = 1, 2, \ldots)$$
$$n_2 = 13(10k + 1) \quad (k = 1, 2, \ldots)$$
$$n_3 = 11(10k + 3) \quad (k = 0, 1, \ldots)$$
$$n_4 = 19(10k + 7) \quad (k = 0, 1, \ldots)$$
$$n_5 = 7(10k + 9) \quad (k = 0, 1, \ldots)$$
$$n_6 = 17(10k + 9) \quad (k = 0, 1, \ldots)$$

the intersection of which is not empty, we can state the following further corollary to Theorem 7.

Corollary 2: If either $n = n_1$ and $k \not\equiv 0, 1 \pmod 4$
or $n = n_2$ and $k \not\equiv 0, 4 \pmod{14}$
or $n = n_3$
or $n = n_4$ and $k \not\equiv 3 \pmod 9$
or $n = n_5$ and $k \not\equiv 3, 4 \pmod 8$
or $n = n_6$ and $k \not\equiv 8, 10 \pmod{18}$,
then n is not a F.Psp.

3. A Computational Algorithm to Find L_n Reduced Modulo n

The algorithm described in the following finds the value of $\langle L_n \rangle_n$ (L_n reduced modulo n) after $[\log_2 n]$ recursive calculations. The values of n composite ($2 \le n \le 10^6$) for which $\langle L_n \rangle_n = 1$ correspond, obviously, to the F.Psps. Q_k shown in Table 1.

Step 1: Decompose n as a sum of powers of 2.

$$n = \sum_{i=0}^{m} a_i 2^i, \tag{3.1}$$

where $m = [\log_2 n]$ and a_i can assume either the value 0 or the value 1.

Step 2: Starting from the initial values

$$\begin{cases} L_{k_0} = L_1 = 1 \\ F_{k_0} = F_1 = 1, \end{cases} \tag{3.2}$$

calculate the pairs

$$(L_{k_i}, F_{k_i}) \quad (i = 1, 2, \ldots, m - 1) \tag{3.3}$$

where $k_0 = 1$ and

$$k_i = \begin{cases} 2k_{i-1} & \text{if } a_{m-i} = 0 \\ 2k_{i-1} + 1 & \text{if } a_{m-i} = 1. \end{cases} \tag{3.4}$$

The pairs (3.3) can be calculated, on the basis of the previously obtained values, using the identities

$$L_{2k} = L_k^2 + 2(-1)^{k-1}, \tag{3.5}$$
$$L_{2k+1} = L_k(5F_k + L_k)/2 + (-1)^{k-1}, \tag{3.6}$$
$$F_{2k} = F_k L_k, \tag{3.7}$$

and

$$F_{2k+1} = L_k(F_k + L_k)/2 + (-1)^{k-1}, \tag{3.8}$$

derived from identities I_7, I_8, I_{15}, I_{18}, and I_{32} [3].

Step 3: Calculate L_n using

$$L_n = \begin{cases} L_{2k_{m-1}} & \text{if } a_0 = 0 \\ L_{2k_{m-1}+1} & \text{if } a_0 = 1. \end{cases} \tag{3.9}$$

End.

The algorithm works modulo n throughout. We recall, cf. (3.6) and (3.8), that the multiplicative inverse of 2 modulo an odd n is $(n + 1)/2$.

As a practical example, the various steps to find $\langle L_n \rangle_n$ for $n = Q_{23} = 90061$ are shown in the following.

$$Q_{23} = 90061 = 2^{16} + 2^{14} + 2^{12} + 2^{11} + 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^3 + 2^2 + 2^0$$

$$m = 16$$

i	a_{m-i}	k_i	$\langle L_{k_i} \rangle_{Q_{23}}$	$\langle F_{k_i} \rangle_{Q_{23}}$
0	1	1	1	1
1	0	2	3	1
2	1	5	11	5
3	0	10	123	55
4	1	21	24476	10946
5	1	43	86547	30844
6	1	87	78960	73765
7	1	175	27806	89112
8	1	351	89985	90027
9	1	703	9349	4181
10	1	1407	26554	23164
11	0	2814	27349	70287
12	0	5628	11194	17179
13	1	11257	69119	26137
14	1	22515	59408	0
15	0	45030	90059	0
16	1	90061	1	-

4. Conclusions

We think that a thorough investigation of the behavior of the fractional part of the quantity $B_{n,k}$, cf. (1.6), as n and k vary could lead to the discovery of further properties of the F.Psps.

4.1. A practical application

If we could know *a priori* that an integer N is not a F.Psp., then the algorithm developed in Section 3 would ascertain the primality of N.

On the other hand, the proof of Conjecture 4 would suffice to make the above algorithm an efficient *probabilistic test* for the primality of large numbers. Besides being interesting *per se*, this algorithm could find an application in modern cryptography. Currently, probabilistic testing for the primality of large numbers (more than 100 digits) plays a relevant role in the so-called public-key cryptosystems [12]. The most widely used probabilistic test is the SS (Solovay & Strassen) test [13]. The computational complexity of a *single* step of this test is slightly greater than the complexity of our algorithm. Usually, 100 steps of the SS algorithm are required, thus assuring that N is prime with probability $p_1 = 1 - 1/2^{100} \approx 1 - 7.88 \cdot 10^{-31}$. If Conjecture 4 were proved, we could state that a sufficiently large number N satisfying the congruence $L_N \equiv 1 \pmod{N}$ is prime with probability $p_2 \approx 1 - 2/(\alpha\sqrt{N})$. It can be readily proved that, if N has more than 61 digits, $p_2 > p_1$. For example, if N is a 100-digit number, we have $p_2 \approx 1 - 3.9 \cdot 10^{-50}$.

4.2. A remark

We wish to conclude this section and the paper with a remark. It appears that $Q_5 = F_{19}$ and $Q_{17} = L_{23}$. We asked ourselves whether this fact has an intimate significance and whether there exist other F.Psps. which are either Fibonacci or Lucas numbers.

First we noted that $h = 19$ is the smallest prime such that F_h is composite: $F_{19} = 4181 = 37 \cdot 113$. Moreover, if we exclude $k = 3$ (recall that L_{3n} is even) $k = 23$ is the smallest prime such that L_k is composite: $L_{23} = 64079 = 139 \cdot 461$. The subsequent values of h and k that verify this property are $h = 31$ and $k = 29$. Using the algorithm described in Section 3, we ascertained that

$$L_{F_{31}} \equiv 1 \pmod{F_{31}} \quad (F_{31} = 1346269 = 557 \cdot 2417)$$

and

$$L_{L_{29}} \equiv 1 \pmod{L_{29}} \quad (L_{29} = 1149851 = 59 \cdot 19489).$$

The following question arises: "Are all the composite Fibonacci and Lucas numbers with prime subscript, F.Psps.?"

Furthermore, we found that

$$L_{L_{32}} \equiv 1 \pmod{L_{32}},$$

$L_{32} = 4870847 = 1087 \cdot 4481$ being the smallest composite Lucas number of which the subscript is a power of 2.

Finally, we note that $Q_6 = L_{18} - 1$. A brief search showed that the smallest F.Psp. equal to a Fibonacci number diminished by 1 is

$$F_{33} - 1 = 3524577 = 3 \cdot 7 \cdot 47 \cdot 3571.$$

References

1. *Dizionario Enciclopedico Italiano* (entry: Waring, Edward).
2. O. Brugia & P. Filipponi. "Waring Formulae and Certain Combinatorial Identities." Int. Rept. 3B5986 (1986). Fondazione Ugo Bordoni, Roma.
3. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin Co., 1969.
4. M. R. Schroeder. *Number Theory in Science and Communication*. 2nd ed. Berlin: Springer-Verlag, 1986.
5. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*. 2nd ed. Oxford: The Clarendon Press, 1945.
6. I. M. Vinogradov. *Elements of Number Theory*. New York: Dover Publ. Inc., 1954.
7. V. E. Hoggatt, Jr., & M. Bicknell. "Some Congruences of the Fibonacci Numbers Modulo a Prime P." *Mathematics Magazine* 47.5 (1974):210-214.
8. J. M. Pollin & I. J. Schoenberg. "On the Matrix Approach to Fibonacci Numbers and the Fibonacci Pseudoprimes." *Fibonacci Quarterly* 18.3 (1980): 261-268.

9. M. Pettet. Problem B-93. *Fibonacci Quarterly 4.2* (1966):191.
10. D. Lind. Solution to Problem B-93. *Fibonacci Quarterly 5.1* (1967):111-112.
11. H. T. Freitag & P. Filipponi. "On the Representation of Integral Sequences $\{F_n/d\}$ and $\{L_n/d\}$ as Sums of Fibonacci Numbers and as Sums of Lucas Numbers." *Proc. of the Second Int. Conf. on Fibonacci Numbers and Their Appl.*, San Jose, California, August 1986, pp. 97-112.
12. R. L. Rivest, A. Shamir, & L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Comm. ACM 21.2* (1978):120-126.
13. R. Solovay & V. Strassen. "A Fast Monte-Carlo Test for Primality." *SIAM J. Comput. 6.1* (1977):84-85.

*****

A REMARK ON A THEOREM OF WEINSTEIN

J. W. Sander
Institut fur Mathematik, Universitat Hannover
Welfengarten 1, 3000 Hannover 1, Fed. Rep. of Germany
(Submitted June 1987)

Let $(f_n)_{n\in\mathbb{N}_0}$ denote the Fibonacci sequence:

$$f_0 = 0,\ f_1 = 1,\ f_{n+2} = f_{n+1} + f_n \quad (n \geq 0).$$

For a positive integer m, let $\underline{m} = \{1, 2, \ldots, m\}$. In [5] L. Weinstein proves by an inductive argument the following

Theorem 1: For a positive integer m let $A \subseteq \{f_n: n \in \underline{2m}\}$ with $|A| \geq m + 1$. Then there are $f_k,\ f_j \in A,\ k \neq j$, such that $f_k | f_j$.

Proof: It is a well-known fact that $f_k | f_j$ for $k | j$ (see, e.g., [4]). Hence, it suffices to show that, for $B \subseteq \underline{2m}$ with $|B| = m + 1$, there are $k,\ j \in B,\ k \neq j$, such that $k|j$. Let $2^{e(B)}$ denote the exact power of 2 dividing the positive integer b, and define, for all $r \in \underline{2m},\ 2 \nmid r$,

$$B_r = \{b \in B: b/2^{e(B)} = r\}.$$

Obviously, $\bigcup_r B_r = B$. Since $|B| = m + 1$, the pigeon-hole principle yields a B_r containing two distinct elements $k < j$ of B. By definition of B_r, $k|j$.

Remark 1: It should be mentioned that the theorem is best possible, since for $|B| = m$ the conclusion does not hold: Choose, for example, $B = \underline{2m}\backslash\underline{m}$. It might be an interesting question to ask how many sets $B \subseteq \underline{2m}$ with $|B| = m$ have the property that any two elements $k,\ j \in B,\ k \neq j$, satisfy $k \nmid j$.

A problem similar to the one treated in Theorem 1 will be considered in

Theorem 2: For a positive integer m let $A \subseteq \{f : n \in \underline{2m}\}$ with $|A| \geq m + 1$. Then there are $f_k,\ f_j \in A,\ k \neq j$, such that $(f_k,\ f_j) = 1$.

Proof: Since $(f_k,\ f_j) = f_{(k,j)}$ (see [4]), it suffices to show that for $B \subseteq \underline{2m}$ with $|B| = m + 1$, there are $k,\ j \in B,\ k \neq j$, such that $(k,\ j) = 1$. For $r \in \underline{m}$, let

$$B_r = \{2r - 1, 2r\}.$$

Obviously, $\bigcup_r B_r = \underline{2m}$. By virtue of $|B| = m + 1$, the pigeon-hole principle implies that there is a B_r containing two distinct elements $k < j$ of B; hence, $k = 2r - 1$, $j = 2r$. Therefore, $(k, j) = 1$.

Remark 2: This theorem is best possible, too:

$$B = \{b \in \underline{2m}\colon 2|b\} \text{ satisfies } |B| = m.$$

However, all elements of B are divisible by 2. If we make the additional assumption that B contains an odd element, small examples suggest that now

$$B = \{b \in \underline{2m}\colon 3|b\}$$

is the "worst" case. Thus, one might conjecture that

$$|B| \geq \left[\frac{2m}{3}\right] + 1$$

will suffice for B to contain a pair of relatively prime elements. In the sequel, we will prove that this is not true for sufficiently large m.

Remark 3: The application of the pigeon-hole principle in the proofs of Theorems 1 and 2 is well known (see [1], Ch. 5).

Lemma 1: Let $n > 1$, $2 \nmid n$. Let

$$B(n) = \{b \leq n\colon 2|b,\ (b, n) > 1\} \cup \{n\}.$$

Then

$$|B(n)| = \frac{1}{2}(n - \varphi(n) + 1),$$

where φ denotes Euler's function.

Proof: All the tools used in this proof can be found in [3], Ch. XVI. Let μ be the Möbius function.

$$\begin{aligned}|B(n)| &= 1 + \sum_{\substack{2b \leq n \\ (b,n) > 1}} 1 = 1 + \frac{n-1}{2} - \sum_{\substack{b \leq n/2 \\ (b,n) = 1}} 1 \\ &= \frac{n+1}{2} - \sum_{b \leq n/2} \sum_{d|(b,n)} \mu(d) = \frac{n+1}{2} - \sum_{d|n} \mu(d) \sum_{\substack{b \leq n/2 \\ b \equiv 0 \bmod d}} 1 \\ &= \frac{n+1}{2} - \sum_{d|n} \mu(d)\left[\frac{n}{2d}\right] = \frac{n+1}{2} - \sum_{d|n} \mu(d)\left(\frac{n}{2d} - \frac{1}{2}\right) \\ &= \frac{n+1}{2} - \frac{n}{2}\sum_{d|n}\frac{\mu(d)}{d} + \frac{1}{2}\sum_{d|n}\mu(d) = \frac{n+1}{2} - \frac{n}{2}\,\frac{\varphi(n)}{n}.\end{aligned}$$

From now on, let p always be a prime, respectively, run through the set of primes.

Lemma 2: Let x and y be reals satisfying

$$2 \leq y \leq \frac{x}{2}. \tag{1}$$

Let

$$n = \prod_{y < p \leq x} p. \tag{2}$$

Then

$$|B(n)| = \frac{n+1}{2} - \frac{n}{2}\frac{\log y}{\log x} + O\left(\frac{n \log y}{\log^2 x}\right),$$

where $B(n)$ is defined as in Lemma 1 and the constant implied by $O(\ )$ is absolute.

Proof: We have

$$\frac{\varphi(n)}{n} = \prod_{p|n}\left(1 - \frac{1}{p}\right) = \prod_{y < p \le x}\left(1 - \frac{1}{p}\right) = \prod_{p \le x}\left(1 - \frac{1}{p}\right)\prod_{p \le y}\left(1 - \frac{1}{p}\right)^{-1}. \tag{3}$$

It is well known (see, e.g., [3], Ch. XXII) that there is a constant C_1 such that for all $z \ge 2$,

$$\prod_{p \le z}\left(1 - \frac{1}{p}\right)^{-1} = C_1 \log z + O(1). \tag{4}$$

This implies

$$\prod_{p \le z}\left(1 - \frac{1}{p}\right) = \frac{1}{C_1 \log z} + O\left(\frac{1}{\log^2 z}\right). \tag{5}$$

By (3), (4), and (5), we have

$$\frac{\varphi(n)}{n} = \frac{\log y}{\log x} + O\left(\frac{\log y}{\log^2 x}\right).$$

By Bertrand's Postulate (see [3], Th. 418) and (1), the product in (2) is not empty, thus $n > 1$. By Lemma 1, the claimed formula follows.

Theorem 3: Let x and y be reals satisfying

$$2 \le y \le \frac{x}{2}. \tag{6}$$

Let

$$n = \prod_{y < p \le x} p.$$

Then there is an x_0 such that for all $x > x_0$,

$$|B(n)| = \frac{n}{2} + O\left(\frac{n \log y}{\log \log n}\right),$$

where $B(n)$ is defined as in Lemma 1 and the constant implied by $O(\ )$ is absolute.

Proof: By Tchebychev's Theorem (see [2], Ch. 7), there are constants C_2, C_3, and x_0 satisfying

$$\frac{4}{5} < C_2 < 1 < C_3 < \frac{6}{5}, \tag{7}$$

such that for all $x > x_0$,

$$C_2 x < \theta(x) < C_3 x, \tag{8}$$

where

$$\theta(x) = \sum_{p \le x} \log p.$$

This implies

$$e^{C_2 x - C_3 y} < n < e^{C_3 x - C_2 y}. \tag{9}$$

In case $x \le y^2$, by (8), $n < e^{C_3 y^2}$; hence,

$$\log \log n < (\log C_3 + 2)\log y;$$

thus, the theorem is obvious. Therefore, we may assume $x > y^2$, i.e., there is $t > 2$ such that $x = y^t$. By (6) and (7),

$$y^{t-1} > 2 \ge \frac{4}{3}\frac{C_3}{C_2};$$

hence,

$$C_2 y^t - C_3 y > \frac{1}{4} C_2 y^t.$$

By (9),

$$\frac{1}{4} C_2 y^t < \log n < C_3 y^t.$$

Taking logarithms, we get positive constants C_4 and C_5 with

$$C_4 \frac{\log y}{\log \log n} < \frac{1}{t} < C_5 \frac{\log y}{\log \log n}.$$

By Lemma 2, this implies

$$|B(n)| = \frac{n+1}{2} + O\left(\frac{n}{t}\right) = \frac{n+1}{2} + O\left(\frac{n \log y}{\log \log n}\right).$$

Thus, the theorem is proved.

Now we are in the position to show the following: If for all $n \in \mathbb{N}$ and all $B \subseteq \underline{n}$ satisfying $|B| \ge \alpha_1 n + \alpha_0$, where α_1 and α_0 are given reals, we find b_1, $b_2 \in B$ with $(b_1, b_2) = 1$, then, necessarily, $\alpha_1 \ge 1/2$, even if we assume the existence of an element $b \in B$ free of prime divisors $p \le y$ for arbitrary y.

For this reason define, for y, α_1, $\alpha_0 \in \mathbb{R}$,

$$\mathbf{B}(y;\, \alpha_1,\, \alpha_0) = \bigcup_{n \in \mathbb{N}} \{B \subseteq \underline{n}\colon\ |B| \ge \alpha_1 n + \alpha_0,\ \underset{b \in B}{\exists}\ \underset{p \le y}{\forall}\ p \nmid b\},$$

$$M(y;\, \alpha_0) = \inf\{\alpha_1 \in \mathbb{R}\colon \underset{B \in \mathbf{B}(y;\, \alpha_1,\, \alpha_0)}{\forall}\ \underset{b_1,\, b_2 \in B}{\exists} (b_1,\, b_2) = 1\}.$$

Theorem 4: Let $\alpha_0 \ge 1$, $y \in \mathbb{R}$. Then

$$M(y;\, \alpha_0) = \frac{1}{2}.$$

Proof: By the proof of Theorem 2, we have for all $n \in \mathbb{N}$ and all $B \subseteq \underline{n}$, $|B| \ge n/2 + 1$, that there are b_1, $b_2 \in B$ such that $(b_1, b_2) = 1$. This implies, for $\alpha_0 \ge 1$ and arbitrary y, that

$$M(y;\, \alpha_0) \le \frac{1}{2}.$$

It remains to show that

$$M(y;\, \alpha_0) \ge \frac{1}{2}. \tag{10}$$

For $y < 2$, (10) is obvious by Remark 2. Hence, let $y \ge 2$ and α_0 be given, and suppose $M(y;\, \alpha_0) < 1/2$. This implies

$$\underset{\alpha < 1/2}{\exists}\ \underset{B \in \mathbf{B}(y;\, \alpha,\, \alpha_0)}{\forall}\ \underset{b_1,\, b_2 \in B}{\exists} (b_1,\, b_2) = 1. \tag{11}$$

Let x be a real satisfying $x \geq 2y$, $x > x_0$ (as in Theorem 3). Let

$$n = \prod_{y < p \leq x} p.$$

By definition of $B(n)$ as in Lemma 1 there is $b \in B$, namely n, such that $p \nmid b$ for all $p \leq y$. By Theorem 3 we have, for sufficiently large n (i.e., for sufficiently large x)

$$|B(n)| \geq \alpha n + \alpha_0.$$

Thus, there is $n \in \mathbb{N}$ with $B(n) \in \mathfrak{B}(y; \alpha, \alpha_0)$. Obviously, $(b_1, b_2) > 1$ for all $b_1, b_2 \in B(n)$, contradicting (11). Therefore, (10) is proved in any case. This finishes the proof of the theorem.

Example: Consider the original problem in Remark 2, i.e., find $n \in \mathbb{N}$ and $B \subseteq n$, $|B| > n/3$, such that there is an odd $b \in B$ and $(b_1, b_2) = 1$ for all $b_1, b_2 \in B$.

By Lemma 1, it suffices to look for the least odd n satisfying

$$\frac{n}{2}\left(1 - \frac{\varphi(n)}{n}\right) > \frac{n}{3}.$$

Since

$$\frac{\varphi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

we may suppose w.l.o.g. that n is squarefree; in fact, we would like to find x such that

$$\prod_{2 < p \leq x} \left(1 - \frac{1}{p}\right) < \frac{1}{3}.$$

The smallest solution is $x = 23$. Therefore, we may choose

$$n = \prod_{2 < p \leq 23} p = 111{,}546{,}435.$$

This is possibly not the least n having the desired properties, but it indicates that the situation for small n (Remark 2) is different from the situation for large n.

I would like to thank the referee for his helpful comments.

References

1. D. I. A. Cohen. *Basic Techniques of Combinatorial Theory*. New York: John Wiley & Sons, 1978.
2. H. Davenport. *Multiplicative Number Theory*. 2nd ed. New York-Heidelberg-Berlin: Springer-Verlag, 1980.
3. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*. 5th ed. Oxford: Clarendon Press, 1979.
4. N. N. Vorob'ev. *Fibonacci Numbers*. New York: Blaisdell, 1961.
5. L. Weinstein. "A Divisibility Property of Fibonacci Numbers." *Fibonacci Quarterly 4.1* (1966):83-84.

*****

FIBONACCI NUMBERS AND BIPYRAMIDS

A. F. Alameddine
King Fahd University of Petroleum and Minerals
KFUPM Box 206, Dhahran 31261, Saudi Arabia
(Submitted June 1987)

1. Introduction

A *bipyramid* B_n of order $n \geq 5$ with degree sequence

$$d_1 \leq d_2 \leq \cdots \leq d_n,\ d_{n-1} = d_n = n - 2$$

is a maximal planar graph consisting of a cycle of order $n - 2$ and two nonadjacent vertices u and v. Every vertex of the cycle has degree 4 and is adjacent to both u and v whose degrees are $n - 2$ as in Figure 1.

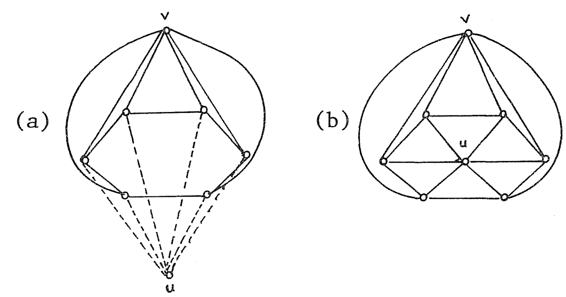


FIGURE 1. A bipyramid with $n = 8$

If B_n is redrawn as in Figure 1(b), then it is geometrically obvious that all such maximal planar graphs contain wheels as subgraphs with $n - 2$ vertices on the rim and a center u with degree $n - 2$ [3]. The graph B_n is called a *generalized bipyramid* if the restriction on d_{n-1} is relaxed while preserving maximal planarity with $3 \leq d_{n-1} \leq n - 2$. Some maximal planar graphs B_8 are shown in Figure 2.

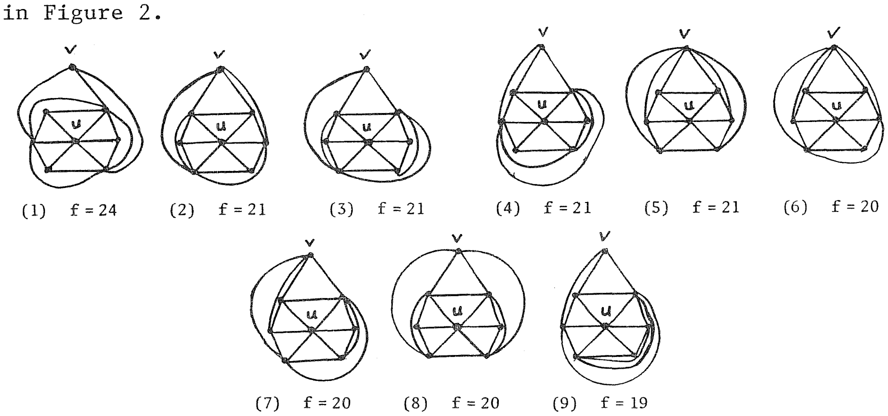


FIGURE 2. Some bipyramids B_n of order 8

The Fibonacci number $f(G)$ of a simple graph G is the number of all complete subgraphs of the complement graph of G. In this paper, our main goal is to present a structural characterization of the class of generalized bipyramids whose Fibonacci numbers are minimum. We will prove that, if G is a maximal planar graph of order n belonging to this class, then

$$f(G) \sim (0.805838\ldots)(1.465571\ldots)^n.$$

This result will be achieved via outerplanar graphs.

Prodinger and Tichy [2] gave upper and lower bounds for trees: If T is a tree on n vertices, then

$$F_{n+1} \le f(T) \le 2^{n-1} + 1,$$

where F_n is the n^{th} Fibonacci number of the sequence

$$F_n = F_{n-1} + F_{n-2},\ F_0 = F_1 = 1.$$

The upper and lower bounds are assumed by the stars S_n and paths P_n in Figure 3, where

$$f(S_n) = 2^{n-1} + 1 \quad \text{and} \quad f(P_n) = F_{n+1}.$$

The upper bound of the set of all maximal outerplanar graphs was investigated in [1]. It is shown that if G is a maximal outerplanar graph of order n and N_n is the fan shown in Figure 3, then

$$f(G) \le f(N_n) = F_n + 1.$$

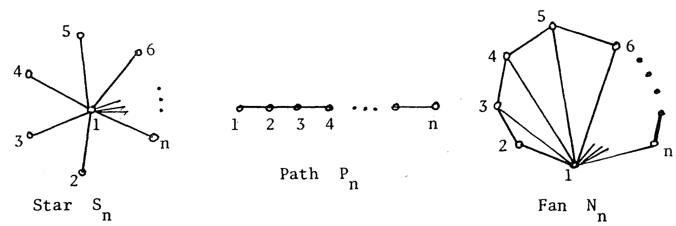


Figure 3. Stars, Paths, and Fans

2. From Maximal Planar to Maximal Outerplanar

From the definition of the Fibonacci number of a graph, we observe that the number of complete subgraphs in the complement of B_n is the same as the number of those complete subgraphs that do not contain the center u and the number of those that do contain u. That is,

$$f(B_n) = f(B_n - u) + 2.$$

The graphs $B_n - u$ for $n = 8$ are redrawn in Figure 4.

Let $C_{n-1} = B_n - u$ and consider the vertex v in C_n. We have

$$f(C_{n-1}) = f(H_{n-2}) + f(H'_{n-2}),$$

where $f(H_{n-2})$ is the number of complete subgraphs in the complement of $C_{n-1} - v$ and $f(H'_{n-2})$ is the number of those complete subgraphs of the complement of C_{n-1} that contain v. We remark that if an edge e is added to two nonadjacent vertices of any graph G without destroying maximal planarity, then

$$f(G) > f(G + e);$$

e is called a *chord* if it is not a rim edge. It suffices to show that the graph

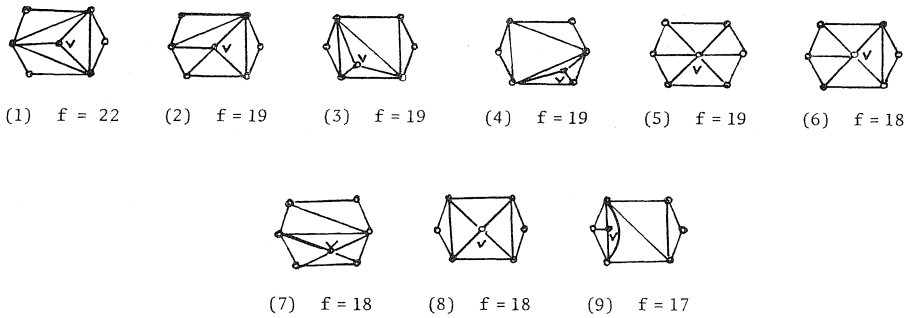


FIGURE 4. Fibonacci numbers of $B_n - u$, $n = 8$

C_{n-1} has minimum f if the remaining chords form longest paths in H_{n-2} and H'_{n-2} as in graph (9) in Figures 4 and 5. That is, $f(C_{n-1})$ is minimum if both H_{n-2} and H'_{n-2} are maximal outerplanar graphs with longest paths of chords.

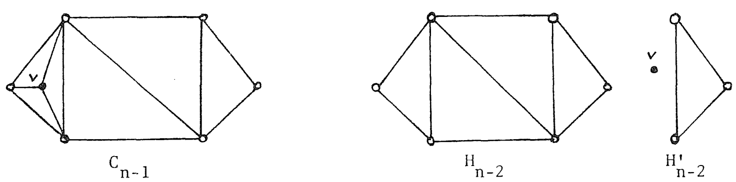


FIGURE 5. $f(C_{n-1}) = f(H_{n-2}) + f(H'_{n-2})$

Since a maximal outerplanar graph G is a triangulation of a polygon and every such graph has two vertices of degree two, there are two triangles T_1 and T_2 in G each of which has a vertex of degree 2. If the vertex v is chosen in one of these triangles, then we have the following theorem.

Theorem 1: Let H_n be a maximal outerplanar graph of order n with a longest path of chords. Let $C_{n+1} = H_n + v$, where v is inserted in any triangle of H_n and joined to the corresponding vertices, then $f(C_{n+1})$ is minimum if $v \in T_1$ or $v \in T_2$.

Proof: Consider the formula

$$f(C_{n+1}) = f(H_n) + f(H'_n).$$

$f(H_n)$ is invariant under all possible choices of triangles, whereas H'_n has the same Fibonacci number if and only if $v \in T_1$ or $v \in T_2$. For all other choices of triangles, H'_n is a disjoint subgraph and hence has a larger Fibonacci number. □

In the next theorem, we show that among all maximal outerplanar graphs of the same order $f(H_n)$ is smallest.

Theorem 2: Let G be an arbitrary maximal outerplanar graph of order n. Then $f(H_n) \le f(G)$, where H_n is maximal outerplanar with longest path of chords.

Proof: Let G and H_n have the same order n and proceed by induction on n. Assume that $f(H_k) \le f(G)$ for all maximal outerplanar graphs G of order $k < n$.

Using the same labeling of the hamiltonian circuit of G we draw the graph H_n. This means that G and H_n differ only in the arrangements of the chords. Let u and v be vertices of degree 2 in G and H_n, respectively. Define $G^* = G - u$ and $H^* = H_n - v$. That is, G^* and H^* are the maximal outerplanar graphs of order $n - 1$ obtained by deleting u and v from G and H_n, respectively. Also, let G^{**} and H^{**} be the graphs obtained by deleting the two neighbors of u from G and the two neighbors of v from H_n. [Let $v = 2k$ in Figure 6(a) and $v = k$ in Figure 6(b).] We observe that the number of complete subgraphs in the complement of G is the sum of the number of those complete subgraphs which do not contain the vertex u and the number of those which do contain u. After noting that

$$f(G^{**}) = f(G^{**} - u),$$

we have

$$f(G) = f(G^*) + f(G^{**}) \quad \text{and} \quad f(H_n) = f(H^*) + f(H^{**}). \tag{1}$$

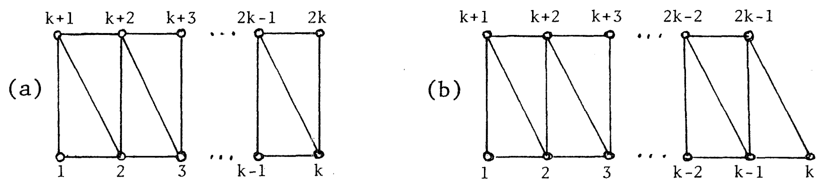


FIGURE 6. The graphs H_{2k} and H_{2k-1} with longest path of chords

Since G^* and H^* are maximal outerplanar of order $n - 1$, then, by the induction assumption,

$$f(H^*) \leq f(G^*). \tag{2}$$

As for H^{**} and G^{**}, we see that the former is maximal outerplanar after deleting v (see Figure 6) while the latter need not be. However, by arbitrarily adding edges to $G^{**} - u$, we see that at each stage the Fibonacci number is less than that at the previous stage until we construct a maximal outerplanar graph G^{***} with $2(n - 3) - 3$ edges having $G^{**} - u$ as a subgraph (see Figure 7).

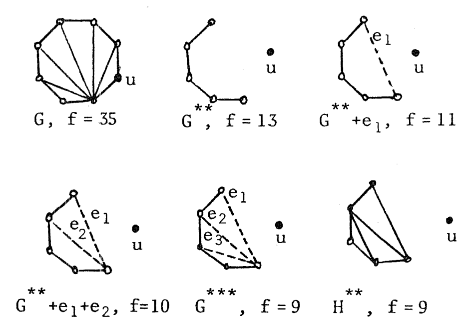


FIGURE 7. The construction of G^{***}, $n = 8$

Now, since $f(G^{**}) = f(G^{**} - u)$, we have

$$f(G^{***}) = f(G^{***} - u),$$

and since $H^{**} - u$ and G^{***} satisfy the hypotheses of the theorem and their order is less than n, we have

$$f(H^{**}) \le f(G^{***}) \le f(G^{**}). \tag{3}$$

From (1), (2), and (3), we see that $f(H_n) \le f(G)$ and the proof is complete. □

Now we show that these graphs H_n are the only ones with the relevant property.

Theorem 3: If G is a maximal outerplanar graph of order n with $f(G) = f(H_n)$, then G is isomorphic to H_n.

Proof: We argue by induction, assuming the result for small values. The argument for Theorem 2 shows that $f(G^*) = f(H_{n-1})$ and $f(G^{**}) = f(H_{n-3})$, where $f(G) = f(G^*) + f(G^{**})$. Hence, by the induction hypothesis, $G^* \simeq H_{n-1}$ and G^{**} is maximal outerplanar (by observing that an additional edge decreases the Fibonacci number) and is isomorphic to H_{n-3}. These conditions easily force the conclusion. □

3. The Fibonacci Number of H_n

The graphs H_n shown in Figure 6 satisfy the recurrence relation

$$h_n = h_{n-1} + h_{n-3}, \tag{4}$$

where $f(H_n) = h_n$, $h_0 = 1$, $h_1 = 2$, $h_2 = 3$.

The solution of (4) is

$$h_n = \left[\frac{u+v+10}{3u+3v}\right]\left[\frac{u+v+1}{3}\right]^n + \left[\frac{u+v-5}{3u+3v}\right]\left[-\frac{u+v-2}{6} + \frac{u-v}{6}\sqrt{3}\,i\right]^n + \left[\frac{u+v-5}{3u+3v}\right]\left[-\frac{u+v-2}{6} - \frac{u-v}{6}\sqrt{3}\,i\right]^n,$$

where $u = \sqrt[3]{\dfrac{29+3\sqrt{93}}{2}}$ and $v = \sqrt[3]{\dfrac{29-3\sqrt{93}}{2}}$.

Since $f(C_{n-1}) = f(H_{n-2}) + f(H'_{n-2})$, we have

$$f(C_{n-1}) = f(H_{n-2}) + f(H_{n-5}) \quad \text{and} \quad f(B_n) = f(H_{n-2}) + f(H_{n-5}) + 2,$$

from which we can prove the following result.

Theorem 4: If B_n is the generalized bipyramid with minimum Fibonacci number, then

$$f(B_n) \sim c\alpha^n, \text{ where } c \approx 0.805838\ldots \text{ and } \alpha \approx 1.465571\ldots .$$

Proof: The order of growth of $f(H_n)$ is governed by the dominant root

$$\alpha = \frac{u+v+1}{3}$$

and $f(H_n) \sim c_1\alpha^n$, where $c_1 \approx 1.3134\ldots$.

For the bipyramids B_n with minimum Fibonacci number, we have

$$f(B_n) = f(H_{n-2}) + f(H_{n-5}) + 2,$$

which implies

$$f(B_n) \sim c_1[\alpha^{n-2} + \alpha^{n-5}] \quad \text{or} \quad f(B_n) \sim c_1(\alpha^{-2} + \alpha^{-5})\alpha^n.$$

So, we can write

$$f(B_n) \sim (0.805838\ldots)\alpha^n, \text{ where } \alpha = 1.465571\ldots .$$

We summarize our results for small graphs and compare with F_n, $n \le 20$, in Table 1.

TABLE 1

Fibonacci numbers of various graphs of order ≤ 20

n	F_n	$f(N_n)$	$f(H_n)$	$f(B_n)$
0	1	1	1	
1	1	2	2	
2	2	3	3	
3	3	4	4	
4	5	6	6	
5	8	9	9	7
6	13	14	13	10
7	21	22	19	14
8	34	35	28	19
9	55	56	41	27
10	89	90	60	39
11	144	145	88	56
12	233	234	129	81
13	377	378	189	118
14	610	611	277	172
15	987	988	406	251
16	1597	1598	595	367
17	2584	2585	872	537
18	4181	4182	1278	786
19	6765	6766	1873	1151
20	10946	10947	2745	1686

Acknowledgment

The author wishes to acknowledge the support of King Fahd University of Petroleum & Minerals.

References

1. A. F. Alameddine. "An Upper Bound for the Fibonacci Number of a Maximal Outerplanar Graph." *The Arabian Journal for Science and Engineering 8* (1983):129-131.
2. H. Prodinger & R. F. Tichy. "Fibonacci Numbers of Graphs." *Fibonacci Quarterly 20.1* (1982):16-21.
3. Z. Skupien. "Locally Hamiltonian and Planar Graphs." *Fund. Math. 58* (1966):193-200.

*****

ON A CLASS OF DETERMINANTS

Andrew Granville

Queen's University, Kingston, Ontario, Canada, K7L 3N6

(Submitted June 1987)

Recently,* D. H. Lehmer posed the following problem:

> If c_n is the coefficient of x^n in $(1 + x + x^2)^n$, then show that 2^n is the determinant of the matrix
>
> $$M_n = \begin{bmatrix} c_0 c_1 & \cdots & c_n \\ c_1 c_2 & \cdots & c_{n+1} \\ \vdots & & \\ c_n & \cdots & c_{2n} \end{bmatrix}.$$

He noted that the generating function for the c_n's is

$$(1 - 2x - 3x^2)^{-1/2} = 1 + x + 3x^2 + 7x^3 + 19x^4 + \cdots .$$

One might equally ask about the value of the same determinant where the c_n's are the coefficients of x^n in $(a + bx + cx^2)^n$ [note that these c_n's have generating function $(1 - 2bx + dx^2)^{-1/2}$, where $d = b^2 - 4ac$]; or perhaps where the c_n's are the coefficients of x^{n+r} in $(a + bx + cx^2)^n$ for some fixed integer r.

As an example, consider the case where the c_n's are the coefficients of x^{n+r} in $(1 + 2x + x^2)^n = (1 + x)^{2n}$, that is,

$$c_n = \begin{bmatrix} 2n \\ n + r \end{bmatrix}.$$

There does not seem to be an immediate combinatorial argument for finding the determinant even in this case.

In this paper we will answer all of these questions in a very simple way, by easy manipulations of the defining polynomials of the c_n's. We make the following definitions:

Let S be the set of sequences of polynomials $F = [F_n(x)]_{n \geq 0}$ such that each $F_n(x)$ has degree less than or equal to $2n$, and such that $F_n(x)/x^n$ is symmetric (about x^0). [Clearly $F_n(x) = (1 + x + x^2)^n$ and $F_n(x) = (1 + x)^{2n}$ are examples of such sequences.] We define the "elementary sequence" of S to be

$$I = [I_n(x)]_{n \geq 0},$$

where $I_0(x) = 1$ and $I_n(x) = x^{2n} + 1$ for each $n \geq 1$.

Suppose F, $G \in S$ and r is a fixed integer. For each integer $n \geq 0$, let $A_n(F, G)$ be the $(n + 1)$ by $(n + 1)$ matrix with $(i, j)^{\text{th}}$ entry

$$F_i(x)/x^i \cdot G_j(x)/x^j \quad (\text{for } 0 \leq i, j \leq n).$$

For any matrix A with entries in $\mathbb{Z}[x]$, we define $c_r(A)$ to be the matrix formed from A by replacing each entry with the coefficient of x^r. We let $D_r(A)$ be the determinant of $c_r(A)$.

*At the Western Number Theory Conference in Asilomar, December, 1985.

Finally, we let $B_n(F)$ be the $(n+1)$ by $(n+1)$ matrix with $(i, j)^{\text{th}}$ entry $b_{i,j}$ $(0 \le i, j \le n)$, where

$$F_i(x)/x^i = b_{i,0} + \sum_{j=1}^{i} b_{i,j}(x^j + x^{-j}).$$

We will see that the value $D_r[A_n(F, G)]$ is easily computed in terms of the determinants of $B_n(F)$, $B_n(G)$, and $D_r[A_n(I, I)]$.

Lemma 1: Suppose that A, U, and V are $n \times n$ matrices, where A has entries from $\mathbb{C}[x]$ and U and V from $\mathbb{C}$. Then, for any integer r,

$$c_r(UAV) = Uc_r(A)V.$$

The proof of this lemma follows immediately from the observation that, if $a(x)$, $b(x) \in \mathbb{C}[x]$ and α, $\beta \in \mathbb{C}$, then α times the coefficient of x^r in $a(x)$ plus β times the coefficient of x^r in $b(x)$ equals the coefficient of x^r in $\alpha a(x) + \beta b(x)$.

We also make the following trivial observation

Lemma 2: If F, $G \in S$, then for any positive integer n,

$$A_n(F, G) = B_n(F)A_n(I, I)B_n(G)^{\top}.$$

Combining Lemmas 1 and 2, we observe

Corollary 1: If F, $G \in S$ and r is a given integer, then

$$D_r[A_n(F, G)] = D_r[A_n(I, I)] \cdot \text{Det}[B_n(F)] \cdot \text{Det}[B_n(G)].$$

Observing that, by definition, $B_n(F)$ is a lower triangular matrix with diagonal entries $F_m(0)$, $0 \le m \le n$, we have

Lemma 3: If $F \in S$, then $\text{Det}[B_n(F)] = \prod_{m=0}^{n} F_m(0)$.

We now compute the values of $D_r[A_n(I, I)]$.

Lemma 4: For integers r and n with $n \ge 0$, we have

$$D_r[A_n(I, I)] = \begin{cases} 2^n & \text{if } r = 0 \\ (-1)^{[(n+1)/2]} & \text{if } r \ne 0 \text{ and } 2r \text{ divides } n+1 \text{ or } n+r, \\ 0 & \text{otherwise.} \end{cases}$$

Proof: $c_r[A_n(I, I)]$ has $(i, j)^{\text{th}}$ entry equal to the coefficient of x^r in $(x^i + x^{-i})(x^j + x^{-j})$ for i, $j \ge 1$. Thus,

$$c_r[A_n(I, I)] = c_{-r}[A_n(I, I)],$$

so we will assume henceforth that $r \ge 0$. Now, if $r = 0$,

$$[c_0(A_n(I, I))]_{i,j} = \begin{cases} 1 & i = j = 0, \\ 2 & i = j > 0, \\ 0 & \text{otherwise,} \end{cases}$$

and so it is clear that $D_0[A_n(I, I)] = 2^n$.

Let $X = c_r[A_n(I, I)]$ and $D_n = D_r[A_n(I, I)]$. For $r \ge 0$,

$$(X)_{i,j} = \begin{cases} 1 & i + j = r, \\ 1 & |i - j| = r, \\ 0 & \text{otherwise}. \end{cases}$$

We will prove the result for fixed r by induction on n.

Now if $0 \le n \le r - 1$, then all entries of the top row of X are zero, and so $D_n = 0$. If $n = r$, then X has ones on the reverse diagonal and zeros everywhere else, so that

$$D_n = (-1)^{[(n+1)/2]}$$

For $r + 1 \le n \le 2r - 2$, observe that the $r - 1^{\text{st}}$ and $r + 1^{\text{st}}$ rows of X are both $(0, 1, 0, \ldots, 0)$ so that $D_n = 0$.

Now let K_r be the $2r$ by $2r$ matrix with $r \times r$ block structure

$$\left[\begin{array}{c|c} O_r & I_r \\ \hline I_r & O_r \end{array}\right]$$

so that Det $K_r = (-1)^r$.

If $n = 2r - 1$, then the i^{th} row of x has all zero entries except for ones in columns $r - i$ and $r + i$ if $i \le r - 1$, and in column $i - r$ if $i \ge r$. We subtract row $r + i$ from row $r - i$ for $i = 1, 2, \ldots, r - 1$, which are all determinant-preserving operations and get the matrix K_r. Thus,

$$D_n = \text{Det } K_r = (-1)^{(n+1)/2}.$$

Now suppose $n \ge 2r$. If $i \ge n - r + 1$, then row i has just one nonzero entry (in column $j = i - r$) and so we can subtract this row from all other rows with entries in the $(i - r)^{\text{th}}$ column. (This is clearly a determinant-preserving operation.) We perform the same action for each column j, with $j \ge n - r + 1$ and we are left with the matrix

$$\left[\begin{array}{c|c} Y & 0 \\ \hline 0 & K_r \end{array}\right], \text{ where } Y = c_r[A_{n-2r}(I, I)].$$

Thus,

$$D_n = D_{n-2r} \quad \text{Det } K_r = (-1)^{[(n-2r+1)/2]}(-1)^r = (-1)^{[(n+1)/2]}$$

by the induction hypothesis.

So by combining Corollary 1 with Lemmas 3 and 4, we may state the main

Theorem: If $F, G \in S$ and A is the $(n + 1)$ by $(n + 1)$ matrix whose $(i, j)^{\text{th}}$ entry is the coefficient of x^{i+j+r} in $F_i(x) \cdot G_j(x)$, then the determinant of A equals

$$\left[\prod_{n=0}^{n} F_m(0)G_m(0)\right]. \begin{cases} 2^n & \text{if } r = 0, \\ (-1)^{[(n+1)/2]} & \text{if } r \ne 0 \text{ and } 2 \text{ divides } n + 1 \text{ or } n + r, \\ 0 & \text{otherwise}. \end{cases}$$

Some consequences are

Corollary 2: The determinant of M_n with c_n equal to the coefficient of x^n in $(1 + x + x^2)^n$ is 2^n.

Proof: Take $F_m(x) = G_m(x) = (1 + x + x^2)^m$ in the Theorem.

Corollary 3: The determinant of M_n with $c_n = \begin{bmatrix} 2n \\ n + r \end{bmatrix}$ is:

$$\begin{cases} 2^n & \text{if } r = 0, \\ (-1)^{[(n+1)/2]} & \text{if } r \neq 0 \text{ and } 2r \text{ divides } n+1 \text{ or } n+r, \\ 0 & \text{otherwise.} \end{cases}$$

Proof: Take $F_m(x) = G_m(x) = (1 + x)^{2m}$ in the Theorem.

We make an interesting combinatorial observation in

Corollary 4: If c_n is the coefficient of x^n in $(1 + tx + x^2)^n$, then the value of the determinant of M_n is independent of t.

Proof: Take $F_m(x) = G_m(x) = (1 + tx + x^2)^m$ in the Theorem and observe that each $F_m(0)$ is independent of t.

Corollary 5: The determinant of M_n with c_n equal to the coefficient of x^{n+r} in $(a + bx + cx^2)^n$ (with $a, b, c \neq 0$) is:

$$(a^{n-r}c^{n+r})^{(n+1)/2} = \begin{cases} 2^n & \text{if } r = 0, \\ (-1)^{[(n+1)/2]} & \text{if } r \neq 0 \text{ and } 2^n \text{ divides } n+1 \text{ or } n+r, \\ 0 & \text{otherwise.} \end{cases}$$

Proof: Let $\theta = (ac)^{1/2}$, $x = \theta y/c$, so that c_n is the coefficient of

$$\frac{\theta^{n+r}y^{n+r}}{c^{n+r}}$$

in $a^n[1 + (b/\theta)y + y^2]^n$. Let d_n be the coefficient of y^{n+r} in $[1 + (b/\theta)y + y^2]^n$ so that $c_n = (a^{n-r}c^{n+r})^{1/2}d_n$. Then

$$\begin{bmatrix} c_0 c_1 & \cdots & c_n \\ c_1 c_2 & \cdots & c_{n+1} \\ \vdots & & \\ c_n & \cdots & c_{2n} \end{bmatrix} = (c/a)^{r/2} \begin{bmatrix} 1 & & & 0 \\ & \theta & & \\ & & \theta^2 & \\ 0 & & & \ddots \; \theta^n \end{bmatrix} \begin{bmatrix} d_0 d_1 & \cdots & d_n \\ d_1 d_2 & \cdots & d_{n+1} \\ \vdots & & \\ d_n & \cdots & d_{2n} \end{bmatrix} \begin{bmatrix} 1 & & & 0 \\ & \theta & & \\ & & \theta^2 & \\ 0 & & & \ddots \; \theta^n \end{bmatrix},$$

and so the result follows immediately from Corollaries 3 and 4.

Corollary 6: The Legendre polynomials $[P_n(t)]_{n \geq 0}$ are defined by

$$(1 - 2tx + x^2)^{-1/2} = \sum_{n \geq 0} P_n(t)x^n.$$

By taking $c_n = P_n(t)$, the determinant of M_n is

$$2^n\left(\frac{t^2 - 1}{4}\right)^{\binom{n+1}{2}}.$$

Proof: Use Corollary 5 with $b = t$ and $b^2 - 4ac = 1$.

Clearly, this technique of computing this class of determinants may be generalized to a number of different questions. The real keys to the method are that $(1, x + x^{-1}, x^2 + x^{-2}, \ldots)$ form an additive basis for $\mathbb{Z}[x + x^{-1}]$ over $\mathbb{Z}$; and that the action of taking the coefficients of x^r of the entries of a matrix of polynomials, commutes with multiplication by matrices with entries in $\mathbb{C}$ (i.e., Lemma 1).

*****

GENERATING PARTITIONS USING A MODIFIED GREEDY ALGORITHM

Joseph W. Creely
31 Chatham Place, Vincentown, NJ 08088
(Submitted June 1987)

Let A be an increasing sequence of integers with first element 1. The "greedy" algorithm for partitioning an integer n with respect to A is:

1. Choose the largest $a \in A$ such that $a \leq n$.
2. Form $n - \left[\frac{n}{a}\right]a$.
3. Repeat this process until n is reduced to 0.

This produces a partition of n and the process is called the *greedy* algorithm since n is reduced by the largest possible bites. In this paper we will deal with what we call the "modified greedy" algorithm which replaces the first step above with

1*. Choose *any* $a \in A$ such that $a \leq n$.

Note that this method allows us the flexibility of choosing which elements to remove from n, but once chosen, they must be removed as many times as possible. Therefore, there were many different partitions of n using this algorithm.

Let p_{mn} represent the number of modified greedy partitions of n with largest member m. Then

$$p_{nn} = p_{n-1,\,n} = p_{1n} = p_{2n} = 1, \quad n > 1.$$

Define

$$p_n^* = \sum_1^n p_{in} \quad \text{and} \quad p_0^* = 1. \tag{1}$$

Theorem: $p_{mn} = p_q^*$, where $q \equiv n \pmod{m}$, and $0 < q < m$.

Proof: Every partition counted in p_{mn} contains copies of m by the modified greedy algorithm. Removal of m's from each partition does not change their number but reduces their size so that $p_{mn} = p_q^*$, where $q \equiv n \pmod{m}$. □

The following two equations are corollaries.

$$p_{m,\,n+an} = p_{mn}, \quad a \geq 0. \tag{2}$$

$$p_{m+a,\,2m-1+a} = p_{m-1}^*, \quad a \geq 0. \tag{3}$$

Table 1 exhibits p_{mn} with $A = \{1, 2, 3, \ldots\}$ and $m, n = 1, 2, 3, \ldots, 15$. Equations (2) and (3) describe patterns evident in the table. Note that the n^{th} row has n positive entries, $p_{mn} = p_q^*$, in which q is a maximum corresponding to $m = (n + 1)/2$, $[(n/2) + 1]$ if n is odd [even].

The following conjectures are derived from a larger (80 × 80) table. (Define $\Delta p_n^* = p_{n+1}^* - p_n^*$.)

1. $\log p_n^*$ approximates a linear function of n if $n > 40$.
2. If n is even, $\Delta p_n^* > 0$.

3. If $\Delta p^*_{n-1} < 0$, then n is even and has at least three prime factors.

   Examples: n = 12, 18, 24, 30, 36, 40, 42, 48, 54, 56, 60, 64, 66, 70, 72, 76, and 80.

4. If $\Delta p^*_{n-1} < 0$, then $\Delta p^*_{an-1} < 0$, $a > 0$.

5. For a given n, let m_r, $r = 1, 2, 3, \ldots$ be elements of the set $\{[n/r]\}$, then $m_{r-1} \geq m_r$. Let $q_r \equiv n \pmod{m_r}$ and $m_{r-1} > m_r - j \geq m_r$, in which $j = 0, 1, 2, \ldots, m_{r-1} - m_r - 1$, then $p_{m_r - j, n} = p^*_{q_r \neq (r_j)}$.

   Example: Let $n = 29$, then $m_1 = 29$, $m_2 = 14$, $m_3 = 9$, $m_4 = 7$, ...

   We have $q_2 = 1$; thus, for $j = 0, 1, 2, 3, 4$, we have

$$p_{14-j,29} = p^*_{1+2j}.$$

TABLE 1

Number of Partitions p_{mn}

$n \backslash m$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	p^*_n
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	2
3	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	3
4	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	4
5	1	1	2	1	1	0	0	0	0	0	0	0	0	0	0	6
6	1	1	1	2	1	1	0	0	0	0	0	0	0	0	0	7
7	1	1	1	3	2	1	1	0	0	0	0	0	0	0	0	10
8	1	1	2	1	3	2	1	1	0	0	0	0	0	0	0	12
9	1	1	1	1	4	3	2	1	1	0	0	0	0	0	0	15
10	1	1	1	2	1	4	3	2	1	1	0	0	0	0	0	17
11	1	1	2	3	1	6	4	3	2	1	1	0	0	0	0	25
12	1	1	1	1	2	1	6	4	3	2	1	1	0	0	0	24
13	1	1	1	1	3	1	7	6	4	3	2	1	1	0	0	32
14	1	1	2	2	4	2	1	7	6	4	3	2	1	1	0	37
15	1	1	1	3	1	3	1	10	7	6	4	3	2	1	1	45

*****

CONCERNING THE DIVISORS OF N AND THE EXPONENTS THEY BELONG TO MODULO $(N - 1)$ or $(N + 1)$

Irving Adler
North Bennington, VT 05257
(Submitted June 1987)

1. Definition

A finite set of positive integers is said to have property A if every member of the set is a divisor of the greatest member of the set.

Example: The set of exponents to which numbers prime to m belong modulo m has property A. [The greatest exponent in the set is $\lambda(m)$, and every member of the set is a divisor of $\lambda(m)$. See the propositions listed for reference in Section 3 below.] Let N be any positive integer greater than 3. Let S be the set of exponents to which the numbers prime to $N - 1$ belong modulo $(N - 1)$. Let T be the set of exponents to which the numbers prime to $N + 1$ belong modulo $(N + 1)$. S and T have property A. Let S' and T' be the sets of exponents to which the divisors of N belong modulo $(N - 1)$ and $(N + 1)$, respectively. S' is a subset of S, and T' is a subset of T. For example, if $N = 21$, the numbers less than 20 and prime to it are 1, 3, 7, 9, 11, 13, 17, and 19. The exponents they belong to modulo (20) are, respectively, 1, 4, 4, 2, 2, 4, 4, and 2. Then $S = \{1, 2, 4\}$. The divisors of 21 are 1, 3, 7, and 21. The exponents they belong to modulo (20) are, respectively, 1, 4, 4, and 1. Then $S' = \{1, 4\}$. The numbers less than 22 and prime to it are 1, 3, 5, 7, 9, 13, 15, 17, 19, and 21. The exponents they belong to modulo (22) are, respectively, 1, 5, 5, 10, 5, 10, 5, 10, 10, and 2. Then $T = \{1, 2, 5, 10\}$. The exponents that the divisors of 21 (1, 3, 7, 21) belong to modulo (22) are, respectively, 1, 5, 10, and 2. Then $T' = \{1, 2, 5, 10\}$. The propositions proved in this paper grew out of a search for values of N for which S' and T' also have property A.

2. Origin of the Problem

This problem grew out of the following permutation problem. Let a be any proper divisor of N. N cards in a deck are numbered from 1 to N from the top down and are permuted as follows: Divide the deck into a equal piles and place them side by side in the order of their positions in the deck from the top down. Then pick up the top card from each pile in rotation, starting with the pile that came from the top, until all the cards have been picked up. Question: What is the order of the permutation? That is, how many repetitions of this procedure will restore all the cards to their original positions in the deck? It is not hard to prove that the answer is e repetitions, where e is the exponent that a belongs to modulo $(N - 1)$. (The proof is given in the Appendix.) (For example, for an ordinary deck of playing cards, $N = 52$. If the permutation is done with two piles, $a = 2$. Then $e = 8$, since 8 is the least exponent for which $2^e \equiv 1$ modulo 51.) This fact led to an examination of the set S' defined above. Since the set T' is also well defined for any N, it is natural to examine this set as well. It is immediate that S' or T' has property A if N has a divisor that is a primitive λ-root of $(N - 1)$ or $(N + 1)$, respectively. Calculation for many values of N shows that there are many cases where S' or T' has property A even when N does not have a divisor that is a primitive λ-root of $(N - 1)$ or $(N + 1)$, respectively. However, there are also values of N for which S' does not have property A. For $N < 26{,}720$, there are 130 values of N for which S' does not have property A. The first ten of these are 572, 1182, 1463, 1953, 2004, 2010, 2338, 2343, 2405, and 3002. (For example, for $N = 572$, $S' = \{1, 57, 114, 190, 285\}$. Since neither 114 nor 190 is a divisor of 285, S' does not have property A.) All 130 of these numbers have the property that they are divisible by three or more different prime numbers. Also, for $N < 5254$, there are 25 values of N for which T' does not have property A. The first ten of these are 1085, 1434, 2354, 2409, 2849, 2975, 3069, 3130, 3138, and 3154. (For example, for $N = 1085$, $T' = \{1, 2, 12, 20, 30\}$. Since neither 12 nor 20 is a divisor of 30, T' does not have property A.) All 25 of these numbers also have the property that they are divisible by three or more different primes. These observations led to the conjecture that if N has at most two different prime divisors, then S' and T' have property A. The purpose of this paper is to prove the conjecture.

3. Definitions and Propositions

For handy reference, we list below the definitions and propositions of elementary number theory that are relevant to this paper.

Definition: If a and m are relatively prime positive integers, and e is the least positive integer such that $a^e \equiv 1 \bmod (m)$, then e is said to be the exponent to which a belongs mod (m).

Definition (Euler's ϕ-function)*:* For any positive integer m, $\phi(m)$ is the number of positive integers not greater than m and prime to it.

Proposition 3.0: If $p_1, p_2, \ldots, p_n$ are the different prime divisors of m, then

$$\phi(m) = m(1 - 1/p_1)(1 - 1/p_2) \ldots (1 - 1/p_n). \quad \text{(see [1], p. 32).}$$

Definition: For any positive integer m, $\lambda(m)$ is defined as follows:

$\lambda(2^a) = \phi(2^a)$ if $a = 0, 1, 2$.

$\lambda(2^a) = (1/2)\phi(2^a)$ if $a > 2$.

$\lambda(p^a) = \phi(p^a)$ if p is an odd prime.

$\lambda(2^a p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}) = M$, where M is the least common multiple of $\lambda(2^a), \lambda(p_1^{a_1}), \lambda(p_2^{a_2}), \ldots, \lambda(p_n^{a_n})$.

Definition: If a belongs to $\lambda(m)$ modulo m, then a is said to be a primitive λ-root modulo m.

Proposition 3.1: If $(a, b) = 1$, there exist positive integers x, y such that $xa - yb = \pm 1$.

Proposition 3.2: If a and m are any two relatively prime positive integers, the congruence $a^{\lambda(m)} \equiv 1 \bmod m$ is satisfied (see [1], p. 54).

Proposition 3.3: If a belongs to d mod m, and $a^n \equiv 1 \bmod m$, then d is a divisor of n (see [1], p. 62).

Proposition 3.4: Every modulus m has primitive λ-roots (see [1], p. 72).

Proposition 3.5: If x belongs to the exponent ab modulo m, then x^a belongs to the exponent b (see [2], p. 106).

Proposition 3.6: If x belongs to the exponent a and y belongs to the exponent b modulo m, where $(a, b) = 1$, then xy belongs to the exponent ab (see [2], p. 106).

4. Propositions I and II

Proposition I: If N has the form p^a, where p is a prime number, then S' and T' have property A.

Proof: The following argument is valid for congruences modulo $(N-1)$ or $(N+1)$: Let p belong to e, and let p^r belong to d for any $r \le a$. Since $p^e \equiv 1$, it follows that $(p^r)^e \equiv 1$. Therefore, by Proposition 3.3, d divides e. Then S' and T' have property A.

Proposition IIA: If N has the form $p^a q^b$, where p and q are different primes, then S' has property A.

Proposition IIB: If N has the form $p^a q^b$, where p and q are different primes, then T' has property A.

The proofs for Propositions IIA and IIB are carried through separately below.

5. Proofs of Some Preliminary Propositions

Before proving Proposition IIA, we prove some preliminary propositions. We consider first the special case where $(a, b) = 1$. Since a and b are relatively prime, then (with appropriate choice of notation, interchanging a and b if necessary) there exist positive integers x and y such that $xa - yb = 1$.

Proposition 5.1: If $(a, b) = 1$, there exist integers x, y such that $0 < x \le b$ and $0 \le y < a$ and $xa - yb = 1$.

(1) Can we have $x \le b$ and $y > a$? If we did, then $b = x + s$ for some $s \ge 0$, and $y = a + r$ for some $r > 0$. Then $ax - (a + r)(x + s) = 1$ yields $-as - rx - rs = 1$, which is impossible.

(2) Can we have $y \le a$ and $x > b$? If we did, then $a = y + s$ for some $s \ge 0$, and $x = b + r$ for some $r > 0$. Then $(b + r)(y + s) - yb = 1$, and $bs + ry + rs = 1$. This is impossible if $s > 0$. If $s = 0$, $ry = 1$, and hence $r = 1$ and $y = 1$. Then $x = b + 1$, $y = a = 1$. Then this case is possible only if $N = pq^b$. However, with a change of notation, writing p for q and vice versa, and a for b and vice versa, we could have written $N = p^a q$, and use $x = 1$, $y = a - 1$, so that we have $x = b$, $y < a$ [see case (4) below]. Note that y is positive unless $a = 1$, in which case $y = 0$.

(3) If $x > b$ and $y > a$, we can replace x by $x - b$ and y by $y - a$, since

$$(x - b)a - (y - a)b = xa - yb = 1.$$

By repeated application of this procedure, we would ultimately get either case (2) above or case (4) below.

(4) $0 < x \le b$, and $0 \le y \le a$. We can include case (2) in the changed notation ($N = p^a q$, with $x = 1$, $y < a$, and $y = 0$ only if $a = 1$) by permitting y to be 0 if $a = 1$. We cannot have $y = a$, because if $y = a$,

$xa - ba = 1$, $a(x - b) = 1$; thus $a = 1$, $x = b + 1$, contradicting $x \le b$. If $x = b$, $ba - by = 1$, $b(a - y) = 1$. Then $b = 1$, $y = a - 1$. Consequently, we may always assume x and y such that $0 < x \le b$ and $0 \le y < a$.

Proposition 5.2: If $(a, b) = 1$, then S' has property A.

Proof: By Proposition 5.1, $p^y q^x$ is a proper divisor of N. Let e be the exponent to which $p^y q^x$ belongs modulo $(N - 1)$. We now show that if $p^m q^n$ is any proper divisor of N, and it belongs to f modulo $(N - 1)$, then f divides e. We show first that the ordered pairs $(0, 1)$ and $(1, 0)$ are linear combinations (with integral coefficients) of (a, b) and (y, x):

$$a(y, x) - y(a, b) = (0, ax - by) = (0, 1).$$

$$x(a, b) - b(y, x) = (xa - by, 0) = (1, 0).$$

$$\begin{aligned}(m, n) = m(1, 0) + n(0, 1) &= mx(a, b) - mb(y, x) + na(y, x) - ny(a, b)\\ &= (mx - ny)(a, b) - (mb - na)(y, x).\end{aligned}$$

We know that $p^a q^b \equiv 1$ modulo $(N - 1)$ and $(p^y q^x)^e \equiv 1$ modulo $(N - 1)$. Then

$$(p^a q^b)^{e(mx - ny)} \equiv 1 \quad \text{and} \quad (p^y q^x)^{e(mb - na)} \equiv 1.$$

Therefore,

$$(p^a q^b)^{e(mx - ny)} \equiv (p^y q^x)^{e(mb - na)} \bmod (N - 1).$$

Since p and q are prime to $N - 1$, we may divide by the right-hand member. This yields

$$(p^m q^n)^e \equiv 1 \text{ modulo } (N - 1).$$

Therefore, f divides e.

6. Proof of Proposition IIA

We consider now the general case, $N = p^{ga} q^{gb}$, where $(a, b) = 1$ and $g \ge 1$. Let (x, y) be determined such that $xa - yb = 1$, $0 < x \le b$ and $0 \le y < a$. Let e be the exponent that $p^y q^x$ belongs to modulo $(N - 1)$. Let $p^r q^s$ be any divisor of N.

$$p = (p^a q^b)^x (p^y q^x)^{-b}. \qquad q = (p^a q^b)^{-y} (p^y q^x)^a.$$

$$p^r = (p^a q^b)^{rx} (p^y q^x)^{-br}. \qquad q^s = (p^a q^b)^{-sy} (p^y q^x)^{as}.$$

Then $p^r q^s = (p^a q^b)^{rx - sy} (p^y q^x)^{as - br}$.

Let f be the least common multiple of g and e. Then

$$(p^r q^s)^f \equiv (p^a q^b)^{f(rx - sy)} (p^y q^x)^{f(as - br)} \equiv 1.$$

If $p^r q^s$ belongs to h modulo $(N - 1)$, it follows that h divides f. To complete the proof, we now show that there exists a divisor of N that belongs to f. In the special case where g is a divisor of e, the result is immediate, since then $f = e$, and $p^y q^x$ belongs to e.

For the completely general situation, we express g and e as products of powers of primes.

$$g = p_1^{a_1} \ldots p_k^{a_k} \quad \text{and} \quad e = p_1^{b_1} \ldots p_k^{b_k},$$

where the set $W = \{p_1, \ldots, p_k\}$ includes all the primes that occur in either g or e. (Some of the a_i and some of the b_i may be zero.) Partition W into two disjoint sets U and V as follows:

$$p_i \in U \text{ if } a_i > b_i, \quad p_i \in V \text{ if } a_i \le b_i.$$

Let $m = \prod_{p_i \in U} p_i^{a_i}$, $\quad n = \prod_{p_i \in V} p_i^{a_i}$. $\quad g = mn$.

Let $w = \prod_{p_i \in U} p_i^{b_i}$, $\quad z = \prod_{p_i \in V} p_i^{b_i}$. $\quad e = wz$.

Let $m = w = 1$ if U is empty. Let $n = z = 1$ if V is empty.

$p^a q^b$ belongs to mn. Therefore, $(p^a q^b)^n$ belongs to m, by Proposition 3.5.

$p^y q^x$ belongs to wz. Therefore, $(p^y q^x)^w$ belongs to z.

But m and z are relatively prime. Therefore, by Proposition 3.6,

$(p^a q^b)^n (p^y q^x)^w$ belongs to $mz = f$.

Let $J = (p^a q^b)^n (p^y q^x)^w = p^{na+wy} q^{nb+wx}$.

If $w = m = 1$, then $f = e$, which is an element of S'; otherwise, $w < m$, $y < a$, and $x \le b$. Then

$$na + wy < (n + m)a \quad \text{and} \quad nb + wx < (n + m)b.$$

$m = n$ only if $m = n = 1$, in which case $g = 1$, a case already disposed of.

Assume now that $m \ne n$.

A. If $m > n$, $m = n + d$, $d > 0$. Then $m + n = 2n + d$ and $mn = n^2 + nd$.

If $n > 1$, $mn > m + n$. Then

$$(n + m)a < mna = ga \quad \text{and} \quad (n + m)b < mnb = gb.$$

Then J is a divisor of N.

If $n = 1$, $m = g$ and $w < g$. Then

$$na + wy = a + wy \le a + wa = a(1 + w) \le ga.$$

$$nb + wx = b + wx \le b + wb = b(1 + w) \le gb.$$

Then J is a divisor of N.

B. If $n > m$, $n = m + d$, $d > 0$. $m + n = 2m + d$, $mn = m^2 + md$.

If $m > 1$, $mn > m + n$. Then, as in A above, J is a divisor of N.

If $m = 1$, then $g = n$, and g divides e, a case dealt with above.

Since J is a divisor of N, and J belongs to f modulo $(N - 1)$, S' has property A.

7. Proofs of Some Preliminary Propositions

Here we prove some preliminary propositions that will be used in the proof of Proposition IIB.

Proposition 7.1: Let $N = p^{ga} q^{gb}$, where $(a, b) = 1$. Then $p^a q^b$ belongs to $2g$ modulo $(N + 1)$.

Proof: $N^2 \equiv 1$ modulo $(N + 1)$. Let $p^a q^b$ belong to m. Then, since $(p^a q^b)^{2g} = 1$, $m = 2g/k$ for some positive integer k. If $k \ge 2$, then $m \le g$ and $p^{ma} q^{mb} \le N$, while $(p^a q^b)^m \equiv 1$. This is impossible, since all the numbers $0, 1, 2, \ldots, N$ are noncongruent modulo $(N + 1)$. Therefore, $k = 1$ and $m = 2g$.

Proposition 7.2: If $JJ' = N$, and J belongs to m modulo $(N + 1)$, and J' belongs to n modulo $(N + 1)$, then either both m and n are even and $m = n$ or m is odd and $n = 2m$ or n is odd and $m = 2n$.

Proof: $(JJ')^2 \equiv 1$ modulo $(N + 1)$. Therefore, $[J^m(J')^m]^2 \equiv 1$. Hence, $(J')^{2m} \equiv 1$. Consequently, $2m = kn$ for some positive integer k. Similarly, $2n = mh$ for some positive integer h. Therefore, $hk = 4$. Consequently, $k = 1$, 2, or 4. If $k = 1$, $n = 2m$. If $k = 2$, $m = n$. If $k = 4$, $m = 2n$. If m is even, we have both J^m and $J^m(J')^m$ congruent to 1 modulo $(N + 1)$. Then $(J')^m \equiv 1$ and n divides m. Similarly, if n is even, m divides n. Therefore, if both m and n are even, $m = n$. If m is odd and n is even, then $n = 2m$; if n is odd and m is even, then $m = 2n$. Moreover, m and n cannot both be odd, for if they were it would be necessary that $m = n$. It would follow that $(JJ')^m \equiv 1$, and 2 would be a divisor of m, which is impossible.

Proposition 7.3: If J is a divisor of N and $J'' = NJ$, and J belongs to m modulo $(N + 1)$ and J'' belongs to n, then either both m and n are even and $m = n$, or m is odd and $n = 2m$, or n is odd and $m = 2n$. The proof is similar to the proof of Proposition 7.2.

Proposition 7.4: (Corollary of Propositions 7.2 and 7.3) If J is a divisor of N and $J' = N/J$ and $J'' = NJ$, and the exponent that either J or J' or J'' belongs to is divisible by 4, then all three belong to the same exponent.

8. Proof of Proposition IIB

We consider first the special case where $(a, b) = 1$. By Proposition 5.1, there exist integers x and y such that $xa - yb = 1$, with $0 < x \le b$ and $0 \le y < a$, so that $p^y q^x$ is a divisor of N. Let $p^y q^x$ belong to e modulo $(N + 1)$. $p^a q^b$ belongs to 2. Let $p^{a-y} q^{b-x}$ belong to g. Let $p^r q^s$ be any divisor of N. Then, as shown in Section 6,

$$p^r q^s = (p^a q^b)^{rx - sy}(p^y q^x)^{as - br}.$$

Let f be the least common multiple of e and 2. Then $(p^r q^s)^f \equiv 1$. Consequently, the exponent that every divisor of N belongs to is a divisor of f. If e is even, $f = e$. If e is odd, $g = 2e$ by Proposition 7.2. Then $f = g$. In either case, f is an element of T'. Therefore, T' has property A.

If $N = p^{ga} q^{gb}$, where $(a, b) = 1$ and $g > 1$, let (x, y) be determined as before such that $xa - yb = 1$, with $0 < x \le b$ and $0 \le y < a$. Again, let $p^y q^x$ belong to e modulo $(N + 1)$. By Proposition 7.1, $p^a q^b$ belongs to $2g$. As shown above, if $p^r q^s$ is any divisor of N,

$$p^r q^s = (p^a q^b)^{rx - sy}(p^y q^x)^{as - br}.$$

Let f be the least common multiple of e and $2g$. Then $(p^r q^s)^f \equiv 1$ modulo $(N + 1)$, and the exponent that each divisor of N belongs to is a divisor of f. To complete the proof, we must show that there exists a divisor of N that belongs to f, so that f would be an element of T'. Express $2g$ and e as products of powers of primes.

$$2g = p_1^{a_1} \dots p_k^{a_k}, \quad e = p_1^{b_1} \dots p_k^{b_k},$$

where, as in Section 6, $W = \{p_1, \dots, p_k\}$ includes all the primes that occur in either $2g$ or e. Define U, V, m, n, w, and z as in Section 6. Then $p^a q^b$ belongs to $mn = 2g$, and $p^y q^x$ belongs to $wz = e$. $(p^a q^b)^n$ belongs to m, and $(p^y q^x)^w$ belongs to z. Then $(p^a q^b)^n (p^y q^x)^w$ belongs to $mz = f$. Let

$$J = (p^a q^b)^n (p^y q^x)^w = p^{na + wy} q^{nb + wx}.$$

If $m = 1$, then $w = 1$, and $f = e$, which is an element of T'. If $m \ne 1$, then $w < m$. Thus,

$$na + wy < (n + m)a \quad \text{and} \quad nb + wx < (n + m)b.$$

(a) Consider first n, $m > 3$. If $n = m = 4$, then $n + m \leq (1/2)mn = g$. By induction on m and n separately, it follows that, for all m, $n > 3$,

$$na + wy < ga \quad \text{and} \quad nb + wx < gb.$$

Consequently, J is a divisor of N, and f is an element of T'.

(b) If $m = 3$, then n is even, since $mn = 2g$. Suppose $n \geq 6$. Then, by induction on n, $m + n \leq (1/2)mn$, and J is a divisor of N. Similarly, if $n = 3$, then m is even, and if $m \geq 6$, $m + n \leq (1/2)mn$, and J is a divisor of N. Therefore, for m or $n = 3$, we have left for consideration only $m = 3$ and $n = 2$, or $m = 3$ and $n = 4$, or $m = 2$ and $n = 3$, or $m = 4$ and $n = 3$. The cases where m or $n = 2$ are considered in (c) and (d) below. If $m = 3$ and $n = 4$, $2g = 12$, and $g = 6$. It follows that $w = 3^0 = 1$. Then

$$na + wy = 4a + y < 5a < ga \quad \text{and} \quad nb + wx = 4b + x \leq 5b < gb.$$

Then J is a divisor of N. If $n = 3$ and $m = 4$, $2g = 12$, and $g = 6$. Then $w = 2$ or 1. If $w = 1$,

$$na + wy = 3a + y < 4a < ga \quad \text{and} \quad nb + wx = 3b + x \leq 4b < gb.$$

If $w = 2$,

$$na + wy = 3a + 2y < 5a < ga \quad \text{and} \quad nb + wx = 3b + 2x \leq 5b < gb.$$

In both cases, then, J is a divisor of N.

(c) If $m = 2$, then $w = 1$, $2g = 2n$, $g = n$, and $e = z$, which is odd. $f = mz = 2e$, which is the exponent that $p^{ga-y}q^{gb-x}$ belongs to. Therefore, f is an element of T'.

(d) If $n = 2$, $m = g$, and m is odd. Therefore, g is odd.

$$w \leq (1/3)m = (1/3)g.$$

$$na + wy < 2a + (1/3)ga = (2 + g/3)a.$$

Since $3 \leq g$ (because $g > 1$ and is odd), $2 \leq 2g/3$. Then

$$na + wy < (2g/3 + g/3)a = ga.$$

Similarly, $nb + wx \leq gb$. Consequently, J is a divisor of N.

(e) If $n = 1$, $m = 2g$, and $w \leq (1/2)m$. Consider first $w < (1/2)m$. Then

$$w \leq (1/4)m = (1/2)g.$$

$$na + wy < a + (1/2)ga = (1 + g/2)a.$$

Since $2 \leq g$, $1 \leq g/2$. Then

$$na + wy < (g/2 + g/2)a = ga.$$

Similarly, $nb + wx \leq gb$. Then J is a divisor of N.

(f) If $w = (1/2)m$, $w = g$ and the only element of U is 2. Consequently, g is a power of 2. Then f, which equals $2gz$, is divisible by 4. $e = wz = gz$. $f = mz = 2gz$, and z is odd. $J = p^{a+gy}q^{b+gx}$. $a + gy < 2ga$ and $b + gx < 2gb$. If

$$a + gy \leq ga \quad \text{and} \quad b + gx \leq gb,$$

J is a divisor of N. Still to be dealt with is the case where either $a + gy > ga$, or $b + gx > gb$. If $a + gy > ga$, $y > a(g - 1)/g$. Since $xa = by + 1$,

$$xa > ab(g - 1)/g + 1.$$

Thus, $gx > (g - 1)b + g/a$; $b + gx > gb + g/a > gb$. Then $J' = J/N$ is well defined and is a divisor of N. Now, by Proposition 7.4, since $J = J'N$ and f is divisible by 4, J' belongs to f. Therefore, f is an element of T'. Suppose $b + gx > gb$. Then $x > b(g - 1)/g$. Since $by = xa - 1$,

$$by > ab(g - 1)/g - 1.$$

Then $gy > (g - 1)a - g/b$ and $a + gy > ga - g/b$. If $g \le b$, $a + gy \ge ga$. Then $J' = J/N$ is well defined, is a divisor of N, and belongs to f. If $g > b$,

$$b + gx < g + gx = g(1 + x) \le gb \text{ if } x < b.$$

This contradicts the assumption that $b + gx > gb$. Thus, the case $x < b$ cannot occur in this context. If $x = b$, since $ax - by = 1$, $b(a - y) = 1$. Then $b = 1$ and $y = a - 1$. $b + gx = g + 1 > bg$.

$$a + gy = a + g(a - 1) = ga + (a - g) \ge ga \text{ if } a \ge g.$$

Then, as above, $J' = J/N$ is well defined, is a divisor of N, and belongs to f. Now suppose that $g > a$. Recall that $x = b = 1$, and $y = a - 1$. $N = p^{ga}q^g$. p^aq belongs to $2g$, which is divisible by 4. Therefore, $p^{ga-a}q^{g-1}$ belongs to $2g$, which is a power of 2. $p^yq^x = p^{a-1}q$ belongs to gz. Then $p^{ga-g}q^g$ belongs to z, which is odd. Thus, $p^{2ga-g-a}q^{2g-1}$ belongs to $2gz$. Let

$$J'' = p^{2ga-g-a}q^{2g-1}$$

and let

$$J' = J''/N = p^{ga-g-a}q^{g-1}.$$

Assume $a \ge 2$. Then $g(a - 1) - a < 0$ only if $g < a/(a - 1) < 2$. But $g > a \ge 2$. Therefore, for $a \ge 2$, $0 \le ga - g - a < ga$. Moreover, $0 < g - 1 < g$. Then J' is a divisor of N. Since J'' belongs to $2gz$ which is divisible by 4, J' belongs to $2gz$, which equals f. Then f is an element of T'. What remains to be dealt with now is the case where $a = 1$, $g > 1$. Then we have $N = p^gq^g$. $g = 2^c$ for some $c > 0$. $a = b = 1$, $x = 1$, $y = a - 1 = 0$. $p^aq^b = pq$ belongs to $2g$, and $p^yq^x = q$ belongs to gz. Therefore, q^g belongs to z which is odd. Thus, p^g belongs to $2z$. Let p belong to e'. Then e' divides $2gz$, so that $2gz = e'h$ for some positive integer h. Since $(p^g)^{e'} \equiv 1$, $2z$ divides e', so that $e' = 2zk$ for some positive integer k. Then $2gz = e'h = 2zkh$. Thus, $kh = g$. Consequently, k is a power of 2 such that $1 \le k \le g$. Then possible values of e' are $2z$, $4z$, $8z$, ..., gz, $2gz$. If $e' = 2gz$, then $f = e'$, which is an element of T'. If $e' = gz$, then p^g belongs to z, contradicting the fact that p^g belongs to $2z$. So this case cannot arise. If $e' = gz/t$ with $t > 1$, then we would have $p^{gz/t} \equiv 1$, from which it follows that $(p^{gz/t})^t \equiv 1$, which implies that $(p^g)^z \equiv 1$, which implies that $2z$ divides z. Hence, this case too cannot arise.

References

1. R. D. Carmichael. *The Theory of Numbers*. New York: Wiley & Sons, 1914.
2. I. M. Vinogradov. *Elements of Number Theory*. New York: Dover, 1954.

Appendix

Let $b = N/a$. The cards are in a piles, with b cards in each pile. This is equivalent to a rectangular array with a columns and b rows. Consider the card in row h, column k ($h = 1, 2, \ldots, b$; $k = 1, 2, \ldots, a$). Let x designate its original position in the deck. Let $f(x)$ be its new position as a result of the permutation. $x = (k - 1)b + h$. $f(x) = (h - 1)a + k$. Direct calculation shows that

$$f(x) = ax - (a - 1) - (k - 1)(N - 1).$$

Therefore, $f(x) \equiv ax - (a - 1)$ modulo $(N - 1)$. Designate by $f_i(x)$ the position of the card after i repetitions of the permutation. Then, by induction,

$$f^i(x) \equiv a^i x - (a^i - 1) \text{ modulo } (N - 1).$$

It follows that $f^i(x) = x$ if and only if $a^i \equiv 1$ modulo $(N - 1)$.

*****

A GENERAL RECURRENCE RELATION FOR REFLECTIONS IN MULTIPLE GLASS PLATES

Jeffrey A. Brooks
(student)
West Virginia University, Morgantown, WV 26506
(Submitted June 1987)

The number of possible light paths in a stack of two glass plates can be expressed in terms of Fibonacci numbers, as was first pointed out by Moser [1]. If two glass plates are placed together in such a way that each surface can either reflect or transmit light, then the number of distinct paths through the two plates with exactly n internal reflections is F_{n+2}.

Junge and Hoggatt [2] used matrix methods to count reflections in larger numbers of plates. Hoggatt and Bicknell-Johnson [3] used geometric and matrix techniques to count specific sets of reflections. However, these authors did not present a general recurrence relation for the number of distinct light paths with a fixed number of reflections in an arbitrary number of glass plates. Here we shall present such a recurrence relation.

Consider a single ray of light directed into a stack of r glass plates. Let $T_r(n)$ be the number of distinct paths that can be taken by a light ray entering through the top plate, leaving through either the top plate or the bottom plate, and having exactly n internal reflections. Figure 1 illustrates the distinct light paths in two plates with zero, one, two, and three reflections.

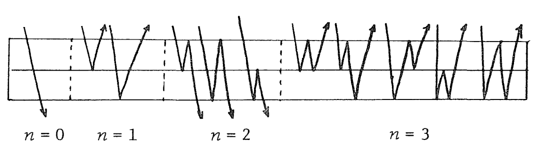


FIGURE 1

As a light ray passes through the stack of plates in a fixed direction, there are a total of r internal surfaces from which it could be reflected. (The surface crossed by the light ray as it enters the stack of plates cannot cause an internal reflection.) Number the reflecting surfaces from 1 to r along the direction of the ray. Figure 2 illustrates this numbering scheme; the path shown consists of reflections from surfaces 2-3-3-2-2.

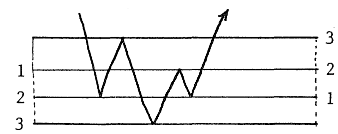


FIGURE 2

Let $G_r(m, n)$ be the number of distinct light paths with exactly n internal reflections such that the n^{th} internal reflection occurs at reflecting surface m. Then, for $n \geq 1$,

$$T_r(n) = \sum_{k=1}^{r} G\ (k, n). \tag{1}$$

A light path of length $n + 1$ whose last reflection was from surface m could have undergone its n^{th} reflection at any one of the reflecting surfaces $r - m + 1$ through r. So

$$G_r(m, n + 1) = \sum_{k=r-m+1}^{r} G_r(k, n). \tag{2}$$

Combining (1) and (2), we see that

$$G_r(m, n + 1) = T_r(n) - \sum_{k=1}^{r-m} G_r(k, n). \tag{3}$$

Let σ represent the permutation of $\{1, 2, \ldots, r\}$ that maps $1, 2, 3, 4, \ldots$ onto $r, 1, r - 1, 2, \ldots,$ and let

$$G_r'(m, n) = G_r(\sigma_m, n).$$

The functions $\{G_r'(m, n): 1 \leq m \leq r\}$ form a reordering of the $\{G_r'(m, n): 1 \leq m \leq r\}$ which can be expanded recursively in terms of $T_r(n)$.

Let $1 \leq i \leq \lfloor k/2 \rfloor$, where $\lfloor x \rfloor$ is the floor function of Donald Knuth and represents the greatest integer less than or equal to x. Then, applying (2), (3), and the definition of $G_r'(m, n)$, we see that:

$$G_r'(1, n) = G_r(r, n) = T_r(n - 1); \tag{4}$$

$$G_r'(2i, n) = G_r(i, n) = \sum_{k=r-i+1}^{r} G_r(k, n - 1) \tag{5}$$

$$= \sum_{k=1}^{i} G_r'(2k - 1, n - 1);$$

$$G_r'(2i + 1, n) = G_r(r - i, n) = T_r(n - 1) - \sum_{k=1}^{i} G_r(k, n - 1) \tag{6}$$

$$= T_r(n - 1) - \sum_{k=1}^{i} G_r'(2k, n - 1).$$

By repeatedly applying (4), (5), (6), we can obtain an expansion for $G_r'(m, n)$ in terms of $\{T_r(n - k): 1 \leq k \leq m\}$. Furthermore, the coefficients in the expansion of $G_r'(m, n)$ are independent of r. So, for any system of r plates and any $m \leq r$, the coefficients of the expansion of $G_r'(m, n)$ in terms of $\{T_r(n - k)\}$, are the same.

Let H_k^j denote the coefficient of $T_r(n - k)$ in the expansion of $G_r'(j, n)$. Figure 3 gives the values of H_k^j for $1 \leq k \leq j \leq 8$.

H_k^j	$k=1$	2	3	4	5	6	7	8	9	10
$j=1$	1									
2	0	1								
3	1	0	-1							
4	0	2	0	-1						
5	1	0	-3	0	1					
6	0	3	0	-4	0	1				
7	1	0	-6	0	5	0	-1			
8	0	4	0	-10	0	6	0	-1		
9	1	0	-10	0	15	0	-7	0	1	
10	0	5	0	-20	0	21	0	-8	0	1

FIGURE 3

Before proceeding, we must introduce a notation for iterated sums of integers. For $m,\ n \geq 1$, define the n^{th}-iterated sum from 1 to n, denoted $S(m, n)$, by

$$S(m, n) = \sum_{i_1=1}^{n} \sum_{i_2=1}^{i_1} \sum_{i_3=1}^{i_2} \cdots \sum_{i_n=1}^{i_{n-1}} 1.$$

By convention, we let $S(0, n) = 1$ for all n. Note that $S(m, n)$ obeys the following identity:

$$\sum_{i=1}^{m} S(n, i) = S(n + 1, m).$$

Theorem 1: If $j \equiv k \pmod 2$, then

$$H_k^j = (-1)^{\lfloor (k-1)/2 \rfloor} S(k - 1, \lfloor (j - k)/2 \rfloor + 1).$$

Otherwise, $H_k^j = 0$.

Proof: By induction on k.

Suppose $k = 1$. Then H_k^j is the coefficient of $T_r(n - 1)$ in the expansion of $G_r'(j, n)$. If j is odd, then $H_k^j = 1$, since none of the terms in the summation in (6) can depend on $T_r(n - 1)$. If j is even, then $H_k^j = 0$, since none of the terms in the summation in (5) can depend on $T\ (n - 1)$. In either case, the statement of the theorem is satisfied.

Suppose $k > 1$. Assume the statement of the theorem is true for $k' \leq k$. Four cases must be considered:

1. Suppose j and k are both even. Let $j = 2i$ where $1 \leq i \leq \lfloor j/2 \rfloor$. Then

$$\begin{aligned} H_k^j = \sum_{m=1}^{i} H_{k-1}^{2m-1} &= \sum_{m=1}^{i} (-1)^{\left\lfloor \frac{(k-1)-1}{2} \right\rfloor} S\left(k - 2, \left\lfloor \frac{(2m - 1) - (k - 1)}{2} \right\rfloor + 1\right) \\ &= (-1)^{\left\lfloor \frac{k-2}{2} \right\rfloor} \sum_{m=1}^{i} S\left(k - 2, \left\lfloor \frac{2m - k}{2} \right\rfloor + 1\right) \\ &= (-1)^{\left\lfloor \frac{k-2}{2} \right\rfloor} S\left(k - 1, \left\lfloor \frac{2i - k}{2} \right\rfloor + 1\right) \\ &= (-1)^{\left\lfloor \frac{k-1}{2} \right\rfloor} S\left(k - 1, \left\lfloor \frac{j - k}{2} \right\rfloor + 1\right) \end{aligned}$$

where in the last step we used the fact that k even implies $\left\lfloor\frac{k-2}{2}\right\rfloor = \left\lfloor\frac{k-1}{2}\right\rfloor$.

2. Suppose j and k are both odd. Let $j = 2i + 1$ where $1 \le i \le \lfloor j/2 \rfloor$. Then

$$\begin{aligned}
H_k^j &= -\sum_{m=1}^{i} H_{k-1}^{2m} = -\sum_{m=1}^{i} (-1)^{\left\lfloor\frac{(k-1)-1}{2}\right\rfloor} S\left(k-2, \left\lfloor\frac{2m-(k-1)}{2}\right\rfloor + 1\right) \\
&= (-1)^{\left\lfloor\frac{k}{2}\right\rfloor} \sum_{m=1}^{i} S\left(k-2, \left\lfloor\frac{(2m+1)-k}{2}\right\rfloor + 1\right) \\
&= (-1)^{\left\lfloor\frac{k}{2}\right\rfloor} S\left(k-1, \left\lfloor\frac{(2i+1)-k}{2}\right\rfloor + 1\right) \\
&= (-1)^{\left\lfloor\frac{k-1}{2}\right\rfloor} S\left(k-1, \left\lfloor\frac{j-k}{2}\right\rfloor + 1\right)
\end{aligned}$$

where in the last step we used the fact that k odd implies $\left\lfloor\frac{k}{2}\right\rfloor = \left\lfloor\frac{k-1}{2}\right\rfloor$.

3. Suppose j is even and k is odd. Let $j = 2i$ where $1 \le i \le \lfloor j/2 \rfloor$. Then

$$H_k^j = \sum_{m=1}^{i} H_{k-1}^{2m-1} = 0.$$

4. Suppose j is odd and k is even. Let $j = 2i + 1$ where $1 \le i \le \lfloor j/2 \rfloor$. Then

$$H_k^j = \sum_{m=1}^{i} H_{k-1}^{2m} = 0.$$

This completes the proof of Theorem 1.

Theorem 2: $T_r(n) = \sum_{k=1}^{r} (-1)^{\lfloor (k-1)/2 \rfloor} S(k, \lfloor (r-k)/2 \rfloor + 1) T_r(n-k)$.

Proof:

$$\begin{aligned}
T_r(n) &= \sum_{m=1}^{r} G_r(m, n) = \sum_{m=1}^{r} G_r'(m, n) = \sum_{m=1}^{r} \left(\sum_{k=1}^{m} H_k^m T_r(n-k)\right) \\
&= \sum_{k=1}^{r} \left(\sum_{m=k}^{r} H_k^m\right) T_r(n-k) \\
&= \sum_{k=1}^{r} \left(\sum_{m=k}^{r} (-1)^{\lfloor (k-1)/2 \rfloor} S(k-1, \lfloor (m-k)/2 \rfloor + 1)\ T_r(n-k)\right) \\
&= \sum_{k=1}^{r} (-1)^{\lfloor (k-1)/2 \rfloor} S(k, \lfloor (r-k)/2 \rfloor + 1) T_r(n-k).
\end{aligned}$$

Figure 4 illustrates the coefficients of this recurrence for $1 \le r \le 10$.

$T_r(n)$	$k=1$	2	3	4	5	6	7	8	9	10
$r=1$	1									
2	1	1								
3	2	1	−1							
4	2	3	−1	−1						
5	3	3	−4	−1	1					
6	3	6	−4	−5	1	1				
7	4	6	−10	−5	6	1	−1			
8	4	10	−10	−15	6	7	−1	−1		
9	5	10	−10	−15	21	7	−8	−1	1	
10	5	15	−20	−35	21	28	−8	−9	1	1

FIGURE 4

For r = 1, 2, 3, 4, and 5, these expansions for $T_r(n)$ are the same as those derived by matrix methods in [2]; however, the matrix methods required a separate set of computations for each value of r.

The recurrence in Theorem 2 has an even simpler statement involving binomial coefficients. Noting that

$$S(m, n) = \sum_{1 \le i_1 \le i_2 \le \cdots \le i_m \le n} 1 = \binom{n + k - 1}{k},$$

it follows that

$$T\;(n) = \sum_{k=1}^{r} (-1)^{\lfloor (k-1)/2 \rfloor} \binom{\left\lfloor \frac{r-k}{2} \right\rfloor + k}{k} T_r(n - k).$$

Remark: This problem was proposed in a graduate combinatorics class taught by H. W. Gould at West Virginia University.

References

1. L. Moser & M. Wyman. Problem B-6. *Fibonacci Quarterly 1.1* (1963):74.
2. Bjarne Junge & V. E. Hoggatt, Jr. "Polynomials Arising from Reflections Across Multiple Plates." *Fibonacci Quarterly 11.3* (1973):285-291.
3. V. E. Hoggatt, Jr., & Marjorie Bicknell-Johnson. "Reflections Across Two and Three Glass Plates." *Fibonacci Quarterly 17.2* (1979):118-142.

*****

THE MANN-SHANKS PRIMALITY CRITERION IN THE PASCAL-T TRIANGLE T_3

Richard C. Bollinger
The Pennsylvania State University at Erie,
The Behrend College, Erie, PA 16563
(Submitted June 1987)

1. Introduction

In [1] H. B. Mann and D. Shanks gave a novel criterion for primality in terms of the displaced entries in the Pascal triangle (T_2); the simple description is as follows. Consider the left-justified form of the Pascal triangle and displace the entries in each row two places to the right from the previous row (so that the $n + 1$ entries in row n occupy columns $2n$ to $3n$, inclusive); also, circle the entries in row n which are divisible by n. Then the column number k is a prime if and only if all the entries in column k are circled.

A little experimentation suggests that the result is also true for the Pascal-T triangle T_3 (see the portion of T_3 below), and in what follows we show that this is the case. [T_m here is the Pascal-T triangle of order m, as defined in Section 2, and the n^{th}-row, k^{th}-column entry is denoted by $C_m(n, k)$; T_2 is *the* Pascal triangle, and

$$C_2(n, k) = \binom{n}{k}.]$$

That is, the same displacement by two is applied to successive rows of T_3, the entries to be circled are chosen in the same way, and it is still true that the column number k is a prime if and only if all the entries in column k are circled.

$n \backslash k$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	1																	
1			1	1	1													
2					1	2	3	2	1									
3							1	3	6	7	6	3	1					
4									1	4	10	16	19	16	10	4	1	
5											1	5	15	30	45	51	45	30
6													1	6	21	50	90	126
7															1	7	28	77
8																	1	8

The Displaced Array for T_3

In addition to the original paper of Mann and Shanks, the result for T_2 is also given in Honsberger [2, p. 3] with a slightly different proof. Gould [3] gives yet another version using a theorem of Hermite [and also extends the result to certain arbitrary rectangular arrays, e.g., Fibonomial coefficients, in which the entries satisfy a relation analogous to

$$\binom{n}{k} = n(n-1)\cdots(n-k+1)/k!$$

for the binomial coefficients]. All three proofs are straightforward and essentially depend only on the facts that

$$C_2(n,\ k) = \binom{n}{k}$$

has an explicit formula, and the simple property that

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1},$$

so that if n and k are relatively prime, n divides $\binom{n}{k}$.

These simplifications, however, are not available for $C_m(n,\ k)$ with $m > 2$, and so, at least for the present, we show only that T_3 has the property claimed, since in this case the reduction formula given in Section 2 allows us to use only ordinary binomial coefficients.

2. Preliminaries

To keep the exposition here self-contained, we will briefly recall the definition of the Pascal-T triangle T_m (as used e.g., in Bollinger [4]), and state two theorems which are used in the sequel.

Definition: For any $m \geq 0$, T_m is the array whose rows are indexed by $n = 0, 1, 2, \ldots$, and columns by $k = 0, 1, 2, \ldots$, and whose entries are obtained as follows:

(a) T_0 is the all-zero array;

(b) T_1 is the array all of whose rows consist of a one followed by zeros;

(c) T_m, $m \geq 2$, is the array whose $n = 0$ row is a one followed by zeros, whose $n = 1$ row is m ones followed by zeros, and any of whose entries in subsequent rows is the sum of the m entries just above and to the left in the preceding row.

The entry in row n and column k is denoted by $C_m(n,\ k)$, although we note that

$$C_2(n,\ k) = \binom{n}{k},$$

since T_2 is *the* Pascal triangle. There are $(m - 1)n + 1$ nonzero entries in row n, and these are the coefficients in the expansion

$$(1 + x + x^2 + \cdots + x^{m-1})^n = \sum_{k=0}^{(m-1)n} C_m(n,\ k)x^k.$$

The reduction formula referred to earlier is also from [4, Th. 2.2], and its statement is as follows.

Theorem I: $C_m(n,\ k) = \sum_{j=0}^{n} \binom{n}{j} C_{m-1}(j,\ k - j)$.

Lastly, we will also need a theorem of Ricci [5]; since this is of some interest in its own right, and the source may not be widely available, we include the short proof.

Theorem II (Ricci): If $a, b, \ldots, c$ are nonnegative integers, and

$$n = a + b + \cdots + c,$$

then

$$\frac{n!}{a!b!\ \dots\ c!} \equiv 0, \quad \operatorname{mod}\left(\frac{n}{D(a,\ b,\ \dots,\ c)}\right),$$

where $D(a,\ b,\ \dots,\ c)$ denotes the greatest common divisor of $a,\ b,\ \dots,\ c$.

Proof: We first note that for any $k \geq 1$ it follows from $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$ that

$$\binom{n}{k} \equiv 0, \quad \operatorname{mod}\left(\frac{n}{D(n,\ k)}\right).$$

If we now write the left side of the main congruence as

$$\frac{n!}{a!(n-a)!} \cdot \frac{(n-a)!}{b!\ \dots\ c!}$$

and use the fact just noted, we conclude that the first factor here is divisible by $n/D(n,\ a)$. Considering a similar decomposition for $b,\ \dots,\ c$, we conclude that the multinomial coefficient is divisible by the least common multiple of the numbers

$$\frac{n}{D(n,\ a)},\ \frac{n}{D(n,\ b)},\ \dots,\ \frac{n}{D(n,\ c)}.$$

And then by known divisibility properties this least common multiple is

$$\frac{n}{D(D(n,\ a),\ D(n,\ b),\ \dots,\ D(n,\ c))},$$

which is the modulus used in the statement of the theorem.

3. Proof of the Criterion for T_3

In the displaced array for T_3, constructed as described previously, we can of course dispose of the even (composite) column numbers exceeding 2 by noting that the construction puts an uncircled 1 (the first entry in any row) in every such column in the same manner as that for T_2. When k is odd, then, we need to show that, if k is a prime, every entry in column k is circled, and if k is composite, at least one entry in column k is uncircled.

We should also note at the outset that by the construction for the displaced array, the $2n + 1$ entries in row n will now occur in columns $2n$ to $4n$ ($2n \leq k \leq 4n$, or $k/4 \leq n \leq k/2$), and the general entry in position $(n,\ k)$ will be $C_3(n,\ k - 2n)$. Then, if $k = p$, p a prime > 3, the entries in column p are the numbers $C_3(n,\ p - 2n)$ for $p/4 \leq n \leq p/2$, and for these values of n, n and $p - 2n$ are relatively prime.

We now show that for *any* relatively prime n and k, $C_3(n,\ k)$ is divisible by n [which means that the entries $C_3(n,\ p - 2n)$ referred to in the previous paragraph will all be circled]. From Theorem I with $m = 3$, we have that

$$\begin{aligned} C_3(n,\ k) &= \sum_{j=0}^{n}\binom{n}{j}C_2(j,\ k-j) = \sum_{j=0}^{n}\binom{n}{j}\binom{j}{k-j} \\ &= \sum_{j=0}^{n}\binom{n}{j}\binom{j}{2j-k} = \sum_{\begin{cases} j = \frac{k+1}{2},\ k \text{ odd} \\ j = \frac{k}{2}\ \ ,\ k \text{ even}\end{cases}}^{k} \frac{n!}{(n-j)!(k-j)!(2j-k)!}. \end{aligned}$$

But from the facts that the arguments of the denominator factorials must add up to n, and that twice the second argument plus the third must add up to k, it follows that the assumption that the arguments have a common divisor $d > 1$ implies that d also divides n and k, contrary to the hypothesis. Theorem II now implies that every term in the sum is therefore divisible by n, and then so is $C_3(n, k)$. Thus, all the entries $C_3(n, p - 2n)$ in column p will be circled in the displaced array.

Finally, for k odd and composite, we let p be an odd prime divisor of k and let $k = p(2r + 1)$. In this case, the row $n = pr$ contributes the entry $C_3(pr, p)$ to column k, where, again from Theorem I,

$$C_3(pr, p) = \sum_{j=\frac{p+1}{2}}^{p} \frac{(pr)!}{(pr - j)!(p - j)!(2j - p)!}.$$

Here, for each term except the last, the assumption that the arguments of the denominator factorials have a common divisor $d > 1$ leads to the conclusion that the prime p is composite; thus, their gcd is 1, and from Ricci's Theorem we again conclude each of these terms is divisible by pr. The last term ($j = p$), however, is just the binomial $\binom{pr}{p}$, which is not divisible by pr [2, p. 8]. Thus, $C_3(pr, p)$ is not divisible by pr, and so there will be an uncircled entry in column k. This completes the proof.

Theorem: In the displaced array for T_3, the column number is a prime if and only if all entries in the column are circled.

Lastly, we note that, as with T_3, a little experimentation suggests the conjecture that the criterion is true in all triangles T_m, but the nature of various formulas for $C_m(n, k)$ (see [4], [6], and [7]) appears to require an approach different from that used here.

References

1. H. B. Mann & D. Shanks. "A Necessary and Sufficient Condition for Primality, and Its Source." *J. Combinatorial Theory (A)* *13* (1972):131-134.
2. Ross Honsberger. *Mathematical Gems II*. Washington, D.C.: Mathematical Association of America, 1976.
3. H. W. Gould. "A New Primality Criterion of Mann and Shanks and Its Relation to a Theorem of Hermite With Extension to Fibonomials." *Fibonacci Quarterly* *10.4* (1972):355-364, 372.
4. R. C. Bollinger. "A Note on Pascal-T Triangles, Multinomial Coefficients, and Pascal Pyramids." *Fibonacci Quarterly* *24.2* (1986):140-144.
5. G. Ricci. "Sui Coefficienti Binomiale E Polinomali." *Giornale di Matematiche (Battaglini)* *69* (1931):9-12.
6. J. E. Freund. "Restricted Occupancy Theory—A Generalization of Pascal's Triangle." *Amer. Math. Monthly* *63.1* (1956):20-27.
7. R. C. Bollinger. "Fibonacci k-Sequences, Pascal-T Triangles, and k-in-a-Row Problems." *Fibonacci Quarterly* *22.2* (1984):146-151.

*****

ON THE F-REPRESENTATION OF INTEGRAL SEQUENCES $\{F_n^2/d\}$ AND $\{L_n^2/d\}$ WHERE d IS EITHER A FIBONACCI OR A LUCAS NUMBER

Herta T. Freitag
B40 Friendship Manor, Roanoke, VA 24012

Piero Filipponi
Fondazione Ugo Bordoni, Roma, Italy
(Submitted June 1987)

1. Introduction

A new look at Zeckendorf's theorem [1] has led to several seemingly unexpected results [2], [3], [4], [5], [6]. It is the purpose of this paper to extend previous findings [4] by involving squares of Fibonacci numbers (F_n) and Lucas numbers (L_n).

The Fibonacci representation of a positive integer N (F-representation of N) [1] is defined to be the representation of N as a sum of positive, distinct, nonconsecutive Fibonacci numbers. It is unique [7]. The number of terms in this representation is symbolized by $f(N)$.

Consider the sequences

$$\{F_n^2/F_m\},\quad \{F_n^2/L_m\},\quad \{L_n^2/L_m\},\quad \{L_n^2/F_m\}.$$

Necessary interrelationships between n and m need to be stipulated to assure integral elements in these sequences. We will predict the number of terms (F-addends) necessary in these representations, and will also exhibit the representations themselves.

Beyond the identities I_7, I_{14} - I_{18}, and I_{21} - I_{24} available in [7], the following further identities are used in the proofs of theorems:

$$\sum_{i=1}^{r} F_{ai+b} = \frac{F_{a(r+1)+b} + (-1)^{a-1}F_{ar+b} - F_{a+b} + (-1)^a F_b}{L_a + (-1)^{a-1} - 1}; \tag{1.1}$$

$$L_{n+k} - (-1)^k L_{n-k} = 5F_nF_k; \tag{1.2}$$

$$L_{n+k} + (-1)L_{n-k} = L_nL_k. \tag{1.3}$$

Their validity can be readily proved with the aid of the Binet form for F_n and L_n. In particular, (1.1) plays a prominent role throughout the proofs.

2. The F-Representation of F_{sk}^2/F_s

If s is an odd positive integer and k is a natural number, then

$$f(F_{sk}^2/F_s) = \begin{cases} sk/2 & \text{if } k \text{ is even} \\ s(k-1)/2 + 1 & \text{if } k \text{ is odd} \end{cases} \tag{2.1}$$

and

$$F_{sk}^2/F_s = \begin{cases} \sum_{i=1}^{k/2}\sum_{j=1}^{s} F_{4si+2j-3s-1} & \text{if } k \text{ is even,} \quad (2.2) \\ F_s + \sum_{i=1}^{(k-1)/2}\sum_{j=1}^{s} F_{4si+2j-s-1} & \text{if } k \text{ is odd.} \quad (2.3) \end{cases}$$

Proof of (2.2) (k is even): Using (1.1), I_{23}, I_{24}, I_{16}, and I_7, the right-hand side of (2.2) can be rewritten as

$$\begin{aligned} &\sum_{i=1}^{k/2}(F_{4si-s+1} - F_{4si-s-1} - F_{4si-3s+1} + F_{4si-3s-1}) \\ &= \sum_{i=1}^{k/2}(F_{4si-s} - F_{4si-3s}) = L_s\sum_{i=1}^{k/2}F_{4si-2s} \\ &= L_s(F_{2sk+2s} - F_{2sk-2s} - 2F_{2s})/(L_{4s} - 2) \\ &= L_s(L_{2sk}F_{2s} - 2F_{2s})/(L_{4s} - 2) = L_sF_{2s}(L_{2sk} - 2)/(L_{4s} - 2) \\ &= 5L_sF_{2s}F_{sk}^2/(5F_{2s}^2) = L_sF_{sk}^2/F_{2s} = F_{sk}^2/F_s. \end{aligned}$$

Proof of (2.3) (k is odd): Using (1.1), I_{23}, I_{24}, I_{16}, I_7, and I_{17}, the right-hand side of (2.3) can be rewritten as

$$\begin{aligned} &F_s + \sum_{i=1}^{(k-1)/2}(F_{4si+s+1} - F_{4si+s-1} - F_{4si-s+1} + F_{4si-s-1}) \\ &= F_s + \sum_{i=1}^{(k-1)/2}(F_{4si+s} - F_{4si-s}) = F_s + L_s\sum_{i=1}^{(k-1)/2}F_{4si} \\ &= F_s + L_s(F_{2sk+2s} - F_{2sk-2s} - F_{4s})/(L_{4s} - 2) \\ &= F_s + L_s(L_{2sk}F_{2s} - F_{4s})/(L_{4s} - 2) \\ &= F_s + F_{2s}L_s(L_{2sk} - L_{2s})/(5F_{2s}^2) = F_s + L_s(L_{2sk} - L_{2s})/(5F_{2s}) \\ &= (5F_sF_{2s} + L_s(L_{2sk} - L_{2s}))/(5F_{2s}) = L_s(5F_s^2 + L_{2sk} - L_{2s})/(5F_{2s}) \\ &= (5F_s^2 + L_{2sk} - L_{2s})/(5F_s) = (L_{2sk} + 2)/(5F_s) \\ &= 5F_{sk}^2/(5F_s) = F_{sk}^2/F_s. \end{aligned}$$

(2.1) follows readily from (2.2) and (2.3).

As a particular case, letting $s = 1$ in (2.1), (2.2), and (2.3), we have (see also [3])

$$f(F_k^2) = [(k+1)/2], \tag{2.4}$$

where $[x]$ denotes the greatest integer not exceeding x, and

$$F_k^2 = \begin{cases} \sum_{j=1}^{k/2} F_{4j-2} & \text{if } k \text{ is even,} \\ F_2 + \sum_{j=1}^{(k-1)/2} F_{4j} & \text{if } k \text{ is odd.} \end{cases} \tag{2.5}$$

Theorem 2: If s is an even positive integer and k is a natural number, then

$$f(F_{sk}^2/F_s) = k \tag{2.6}$$

and

$$F_{sk}^2 / F_s = \sum_{j=1}^{k} F_{2sj-s}. \tag{2.7}$$

Proof of (2.7): Using (1.1), I_{24}, and I_{16}, the right-hand side of (2.7) can be rewritten as

$$\begin{aligned}(F_{2sk+s} - F_{2sk-s} - 2F_s)/(L_{2s} - 2) &= (L_{2sk}F_s - 2F_s)/L_{2s} - 2)\\ &= (F_s(L_{2sk} - 2))/(L_{2s} - 2) = (5F_sF_{sk}^2)/(5F_s^2) = F_{sk}^2/F_s.\end{aligned}$$

(2.6) is an immediate consequence of (2.7).

As a particular case, letting $s = 2$ in (2.6) and (2.7), we have [cf. (2.4) and (2.5)]

$$f(F_{2k}^2) = k \tag{2.8}$$

and

$$F_{2k}^2 = \sum_{j=1}^{k} F_{4j-2}. \tag{2.9}$$

3. The F-Representation of F_{tk}^2/L_s

Theorem 3: ($t = 2s$) If s is an odd positive integer and k is a natural number, then

$$f(F_{2sk}^2/L_s) = (s+1)k/2 \tag{3.1}$$

and

$$F_{2sk}^2/L_s = \sum_{i=1}^{k}\left(F_{4si-3s+1} + \sum_{j=1}^{(s-1)/2} F_{4si+4j-3s}\right). \tag{3.2}$$

Proof of (3.2): Using (1.1), I_{14}, (1.2), I_{24}, I_{16}, and I_7, the right-hand side of (3.2) can be rewritten as

$$\begin{aligned}&\sum_{i=1}^{k}(F_{4si-3s+1} + (F_{4si-s+2} - F_{4si-s-2} - F_{4si-3s+4} + F_{4si-3s})/5)\\ &= \sum_{i=1}^{k}(L_{4si-s} - F_{4si-3s+4} + F_{4si-3s} + 5F_{4si-3s+1})/5\\ &= \sum_{i=1}^{k}(L_{4si-s} + L_{4si-3s})/5 = F_s\sum_{i=1}^{k}F_{4si-2s}\\ &= F_s(F_{4sk+2s} - F_{4sk-2s} - 2F_{2s})/(L_{4s} - 2)\\ &= F_s(L_{4sk}F_{2s} - 2F_{2s})/(L_{4s} - 2) = F_sF_{2s}(L_{4sk} - 2)/(L_{4s} - 2)\\ &= 5F_sF_{2s}F_{2sk}^2/(5F_{2s}^2) = F_sF_{2sk}^2/F_{2s} = F_{2sk}^2/L_s.\end{aligned}$$

(3.1) follows.

Theorem 4: ($t = 2s$) If s is an even positive integer and k is a natural number, then

$$f(F_{2sk}^2/L_s) = sk/2 \tag{3.3}$$

and

$$F_{2sk}^2/L_s = \sum_{i=1}^{k}\sum_{j=1}^{s/2} F_{4si+4j-3s-2}. \tag{3.4}$$

Proof of (3.4): As in the proof of Theorem 3, using (1.1), I_{14}, (1.2), I_{24}, I_{16}, and I_7, the right-hand side of (3.4) can be rewritten as

$$\sum_{i=1}^{k} (F_{4si-s+2} - F_{4si-s-2} - F_{4si-3s+2} + F_{4si-3s-2})/5$$
$$= \sum_{i=1}^{k} (L_{4si-s} - L_{4si-3s})/5 = F_s \sum_{i=1}^{k} F_{4si-2s} = F_{2sk}^2/L_s.$$

(3.3) follows.

It can be noted that, by letting $s = 2$ in (3.3) and (3.4), we obtain the same identities as those resulting from $s = 4$ in (2.6) and (2.7).

Theorem 5: ($t = s = 3$) If k is an odd positive integer, then

$$f(F_{3k}^2/L_3) = k \tag{3.5}$$

and

$$F_{3k}/4 = F_2 + \sum_{j=1}^{(k-1)/2} (F_{12j-2} + F_{12j+1}). \tag{3.6}$$

Proof of (3.6): Using (1.1), I_{24}, and I_{17}, the right-hand side of (3.6) can be rewritten as

$$F_2 + 2\sum_{j=1}^{(k-1)/2} F_{12j} = F_2 + 2(F_{6k+6} - F_{6k-6} - F_{12})/(L_{12} - 2)$$
$$= 1 + (8L_{6k} - 144)/160 = (L_{6k} + 2)/20 = 5F_{3k}^2/20 = F_{3k}^2/4.$$

(3.5) results from (3.6).

4. The F-Representation of L_{sk}^2/L_s

Theorem 6: ($s = 1$) If k is a natural number, then

$$f(L_k^2/L_1) = f(L_k^2) = \begin{cases} k & \text{if } k = 1, 2 \\ 3 & \text{if } k \geq 4 \text{ is even} \\ k - 1 & \text{if } k \geq 3 \text{ is odd} \end{cases} \tag{4.1}$$

and

$$L_k^2/L_1 = L_k^2 = \begin{cases} F_3 + F_{2k-1} + F_{2k+1} & \text{if } k \geq 4 \text{ is even}, \quad (4.2) \\ F_{2k+1} + \sum_{j=1}^{k-2} F_{2j+2} & \text{if } k \geq 3 \text{ is odd}. \quad (4.3) \end{cases}$$

Proof of (4.2): ($k \geq 4$ is even) Using I_{15}, the right-hand side of (4.2), which is given by the sum of three F-addends, can be rewritten as

$$F_3 + L_{2k} = L_{2k} + 2 = L_k^2.$$

Proof of (4.3): ($k \geq 3$ is odd) Using (1.1) and I_{18}, the right-hand side of (4.3) can be rewritten as

$$F_{2k+1} + F_{2k} - F_{2k-2} - 2 = L_{2k} - 2 = L_k^2.$$

(4.1) follows as it is trivial for $k = 1$ or 2.

Theorem 7: If s and k are odd positive integers ($s > 1$), then

$$f(L_{sk}^2/L_s) = 2k \tag{4.4}$$

and

$$L_{sk}^2/L_s = \sum_{j=1}^{k} (F_{2sj-s-1} + F_{2sj-s+1}). \tag{4.5}$$

Proof of (4.5): Using (1.1), (1.3), and I_{18}, the right-hand side of (4.5) can be rewritten as

$$\begin{aligned}(L_{2sk+s} &- L_{2sk-s} - 2L_s)/(L_{2s} - 2) = (L_s L_{2sk} - 2L_s)/(L_{2s} - 2)\\ &= L_s(L_{2sk} - 2)/(L_{2s} - 2) = L_s L_{sk}^2/L_s^2 = L_{sk}^2/L_s.\end{aligned}$$

(4.4) follows.

Theorem 8: If s is an even positive integer and k is an odd positive integer, then

$$f(L_{sk}^2/L_s) = \begin{cases} 1 & \text{if } k = 1 \\ k + 1 & \text{if } k \geq 3 \\ (s+1)(k-1)/2 + 2 & \text{if } s \geq 4 \end{cases} \quad \begin{matrix}\\ \left.\begin{matrix} \\ \\ \end{matrix}\right\} \text{and } s = 2 \\ \\ \end{matrix} \tag{4.6}$$

and (for $s = 2$):

$$L_{2k}^2/3 = \begin{cases} F_4 & \text{if } k = 1 \\ F_2 + F_{4k-1} + \displaystyle\sum_{j=1}^{(k-1)/2} (F_{8j-3} + F_{8j-1}) & \text{if } k \geq 3; \end{cases} \tag{4.7}$$

(for $s \geq 4$):

$$\begin{aligned}L_{sk}^2/L_s = F_{s-1} + F_{s+1} + \sum_{i=1}^{(k-1)/2} \Bigg(&F_{4si-s-2} + F_{4si-s+1}\\ &+ F_{4si+s+1} + \sum_{j=1}^{s-2} F_{4si+2j-s+2}\Bigg).\end{aligned} \tag{4.8}$$

Proof of (4.7): ($s = 2$) The statement clearly holds for $k = 1$. For $k \geq 3$, using (1.1), (1.2), and I_{15}, the right-hand side of (4.7) can be rewritten as

$$\begin{aligned}&F_{2k} + F_{4k-1} + (L_{4k+2} - L_{4k-6} - 15)/(L_8 - 2)\\ &= 1 + F_{4k-1} + (5F_4 F_{4k-2} - 15)/45 = 1 + F_{4k-1} + (F_{4k-2} - 1)/3\\ &= 3F_{4k-1} + F_{4k-2} + 2)/3 = (L_{4k} + 2)/3 = L_{2k}^2/3.\end{aligned}$$

Proof of (4.8): ($s \geq 4$) Using (1.1), I_{14}, (1.2), I_{24}, I_7, I_{16}, and I_{15}, the right-hand side of (4.8) can be rewritten as

$$\begin{aligned}&L_s + \sum_{i=1}^{(k-1)/2} (F_{4si-s-2} + F_{4si-s+1} + F_{4si+s+1} + F_{4si+s}\\ &\qquad\qquad - F_{4si+s-2} - F_{4si-s+4} + F_{4si-s+2})\\ &= L_s + \sum_{i=1}^{(k-1)/2} (F_{4si-s-2} - F_{4si-s+2} + F_{4si+s+2} - F_{4si+s-2})\\ &= L_s + \sum_{i=1}^{(k-1)/2} (L_{4si+s} - L_{4si-s}) = L_s + 5F_s \sum_{i=1}^{(k-1)/2} F_{4si}\\ &= L_s + 5F_s(F_{2sk+2s} - F_{2sk-2s} - F_{4s})/(L_{4s} - 2)\\ &= L_s + 5F_s F_{2s}(L_{2sk} - L_{2s})/(5F_{2s}^2) = L_s + F_s(L_{2sk} - L_{2s})/F_{2s}\\ &= L_s + (L_{2sk} - L_{2s})/L_s = (L_s^2 + L_{2sk} - L_{2s})/L_s\\ &= (L_{2sk} + 2)/L_s = L_{sk}^2/L_s.\end{aligned}$$

(4.6) follows from (4.7) and (4.8).

5. The F-Representation of L_n^2/F_m for Certain Values of n and m

Theorem 9: ($n = 3k$, $m = 3$) If k is a natural number, then

$$f(L_{3k}^2/F_3) = 2k - 1 \tag{5.1}$$

and

$$L_{3k}^2/2 = \begin{cases} F_5 + F_{6k} + \sum_{j=1}^{2k-3} F_{3j+4} & \text{if } k \text{ is even} \quad (5.2) \\ F_{6k} + \sum_{j=1}^{2k-2} F_{3j+1} & \text{if } k \text{ is odd.} \quad (5.3) \end{cases}$$

Proof of (5.2) (k is even): Using (1.1), I_{23}, I_{22}, and I_{15}, the right-hand side of (5.2) can be rewritten as

$$\begin{aligned} &F_5 + F_{6k} + (F_{6k-2} + F_{6k-5} - F_7 - F_4)/L_3 \\ &= 5 + (4F_{6k} + F_{6k-2} + F_{6k-5} - 16)/14 \\ &= 1 + (F_{6k+3} - F_{6k-3} + F_{6k-2} + F_{6k-5})/4 \\ &= 1 + (F_{6k+3} + F_{6k-3})/4 \\ &= 1 + L_{6k}F_3/4 = 1 + L_{6k}/2 = (L_{6k} + 2)/2 = L_{3k}^2/2. \end{aligned}$$

Proof of (5.3) (k is odd): As before, using I_{18} instead of I_{15}, the right-hand side of (5.3) becomes

$$\begin{aligned} &F_{6k} + (F_{6k-2} + F_{6k-s} - F_4 - F_1)/L_3 \\ &= (4F_{6k} + F_{6k-2} + F_{6k-s})/4 - 1 \\ &= L_{6k}/2 - 1 = (L_{6k} - 2)/2 = L_{3k}/2. \end{aligned}$$

(5.1) follows from (5.2) and (5.3), regardless of the parity of k.

Theorem 10: ($n = 6k - 3$, $m = 6$) If k is a natural number, then

$$f(L_{6k-3}^2/F_6) = 3k - 2 \tag{5.4}$$

and

$$L_{6k-3}^2/8 = F_3 + \sum_{j=1}^{k-1} (F_{12j-4} + F_{12j-1} + F_{12j+3}). \tag{5.5}$$

Proof of (5.5): Using I_{21}, (1.1), I_{24}, I_{22}, and I_{18}, the right-hand side of (5.5) can be rewritten as

$$\begin{aligned} &F_3 + \sum_{j=1}^{k-1} (F_{12j-4} + 3F_{12j+1}) \\ &= F_3 + (F_{12k-4} - F_{12k-16} + 3(F_{12k+1} - F_{12k-11}) - 720)/320 \\ &= (F_6 L_{12k-10} + 3F_6 L_{12k-5} - 80)/320 = (3L_{12k-5} + L_{12k-10} - 10)/40 \\ &= (F_{12k-1} + F_{12k-11} - 10)/40 = (5L_{12k-6} - 10)/40 \\ &= (L_{6(2k-1)} - 2)/8 = L_{3(2k-1)}^2/8. \end{aligned}$$

(5.4) follows.

Note that the case ($n = 2k$, $m = 4$) is nothing but the case (4.7) of Theorem 8.

6. Concluding Remarks

F-representations of the sequences

$$\{F_{sk}^2/F_s\},\ \{F_{2sk}^2/L_s\},\ \{F_{3k}^2/L_3\},\ \{L_{sk}^2/L_s\},\ \text{and } \{L_n^2/F_m\}$$

have been investigated and their f-functions, as well as the specific summation expressions, have been given. The authors believe that the results presented in this paper are new. Many further analogous sequences could be analyzed. Possibly, some of the work above could be extended to simple cases of the sequences $\{F_n^k/d\}$ and $\{L_n^k/d\}$, where $k \geq 1$, and d is a power of certain Fibonacci or Lucas numbers. The authors hope to continue their investigations in this area. As an example, we offer the sequences:

$$\text{(i)}\quad \{F_{sk}^2/F_s^2\} \quad \text{and} \quad \text{(ii)}\quad \{F_{skF_s}^2/F_s^2\}.$$

Example (i): $(s = 4)$

$$f(F_{4k}^2/F_4^2) = \begin{cases} (4k-1)/3 & \text{if } k \equiv 1 \pmod 3 \\ (4k+1)/3 & \text{if } k \equiv 2 \pmod 3 \\ 4k/3 & \text{if } k \equiv 0 \pmod 3 \end{cases} \tag{6.1}$$

and

$$F_{4k}^2/9 = \begin{cases} F_2 + \displaystyle\sum_{i=1}^{(k-1)/3} (F_{24i-10} + F_{24i-5} + F_{24i-1} + F_{24i+1}) & \text{if } k \equiv 1 \pmod 3, \\ F_3 + F_7 + F_9 + \displaystyle\sum_{i=1}^{(k-2)/3} (F_{24i-2} + F_{24i+3} + F_{24i+7} + F_{24i+9}) & \text{if } k \equiv 2 \pmod 3, \\ \displaystyle\sum_{i=1}^{k/3} (F_{24i-18} + F_{24i-13} + F_{24i-9} + F_{24i-7}) & \text{if } k \equiv 0 \pmod 3. \end{cases} \tag{6.2}$$

Example (ii): $(s = 4)$ It can be proved that, for $s > 2$, $F_s^2 | F_m$ if and only if $m = ksF_s$ $(k = 0, 1, \ldots)$. In this particular case, we have (cf. [4], Th. 5).

$$f(F_{4kF_4}/F_4^2) = f(F_{12k}/9) = \begin{cases} 3k & \text{if } k \text{ is even} \\ 3k-1 & \text{if } k \text{ is odd} \end{cases} \tag{6.3}$$

and

$$F_{12k}/9 = \begin{cases} \displaystyle\sum_{i=1}^{k/2} \Big(F_{24i-19} + F_{24i-5} + \sum_{j=1}^{4} F_{24i+2j-17}\Big) & \text{if } k \text{ is even} \\ F_4 + F_7 + \displaystyle\sum_{i=1}^{(k-1)/2} \Big(F_{24i-7} + F_{24i+7} + \sum_{j=1}^{4} F_{24i+2j-5}\Big) & \text{if } k \text{ is odd.} \end{cases} \tag{6.4}$$

We leave the proofs of these illustrative examples to the enjoyment of the reader.

References

1. J. L. Brown, Jr. "Zeckendorf's Theorem and Some Applications." *Fibonacci Quarterly 2.3* (1964):163-168.
2. P. Filipponi. "Sulle Proprietà dei Rapporti fra Particolari Numeri di Fibonacci e di Lucas." *Note Recensioni Notizie 33.3-4* (1984):91-96.
3. P. Filipponi. "The Representation of Certain Integers as a Sum of Distinct Fibonacci Numbers." Int. Rept. 2B0985, Fondazione Ugo Bordoni, Roma, 1985.

(Please turn to page 286)

THE CONVOLVED FIBONACCI EQUATION

H. W. Corley
The University of Texas at Arlington, Arlington, TX 76019
(Submitted July 1987)

In this note we consider the recurrence relation

$$f_{n+1} = \sum_{k=0}^{n} f_k a_{n-k} + b_n, \; n = 0, 1, 2, \ldots, \tag{1}$$

where $f \;\; = 1$ and $\langle a_n \rangle$ and $\langle b_n \rangle$ are sequences of parameters. Equation (1) is termed the convolved Fibonacci equation because of the occurrence on the right side of the convolution of the sequences $\langle f_n \rangle$ and $\langle a_n \rangle$. Special cases of (1) include the following:

When $a_0 = a_1 = 1$, $a_n = 0$ for $n \geq 2$, and $b_n = 0$ for $n = 0, 1, 2, \ldots$, the f_n are the usual Fibonacci numbers.

When $a_0 = a_1 = \cdots = a_{r-1} = 1$, $a_n = 0$ for $n \geq r$, and $b_n = 0$ for $n = 1, 2, \ldots$, the f_n are r^{th}-order Fibonacci numbers (see, e.g., [2] and [3]).

When $a_0 = a_1 = 1$, $a_n = 0$ for $n \geq 2$, $b_0 = 0$, and

$$b_1 = \sum_{j=1}^{k} \alpha_j (n+1)^j \text{ for } n = 1, 2, 3, \ldots,$$

(1) becomes the recent recurrence studied by Asveld [1].

We first take the generating function of (1) to obtain the generating function

$$F(z) = \sum_{n=0}^{\infty} f_n z^n$$

of $\langle f_n \rangle$ in terms of the generating functions $A(z)$ of $\langle a_n \rangle$ and $B(z)$ of $\langle b_n \rangle$. Using standard results (see, e.g., [4]), we immediately get

$$F(z) = \frac{1 + zB(z)}{1 - zA(z)} \tag{2}$$

for all z for which $F(z)$, $A(z)$, $B(z)$ exist and $1 - zA(z) \neq 0$.

Two examples of (1) and their solution via (2) are now presented. The a_n and b_n are integers in the first example, while they are not in the second.

Let a_n and b_n be the usual Fibonacci numbers. In this case, the f_n are called the convolved Fibonacci numbers. Since

$$A(z) = B(z) = \frac{z}{1 - z - z^2},$$

it follows from (2) *that*

$$F(z) = 1 + \frac{-\sqrt{2}/2}{1 - (\sqrt{2} - 1)z} + \frac{\sqrt{2}/2}{1 + (\sqrt{2} + 1)z}$$

and hence $f_0 = 1$,

$$f_n = \frac{\sqrt{2}}{2}(\sqrt{2} - 1)^n + \frac{\sqrt{2}}{2}(\sqrt{2} + 1)^n, \ n = 1, 2, 3, \ldots .$$

Example 2: A standard six-sided fair die has three sides painted red, two sides painted black, and one side painted white. A series of throws of the die is made. We will determine the probability f_n that nowhere in the first n throws of the die is a throw of black followed by a throw of white.

Let E_n denote the event that nowhere in the first n throws of the die is a throw of black followed by a throw of white, W_n be the event that a white is thrown on throw n, and R_n that a red is thrown on throw n. $\overline{W}_n$ will denote complementation, i.e., the event that a white is not thrown on throw n. We may thus write

$$P(E_n) = P(E_n|W_n)P(W_n) + P(E_n|\overline{W}_n)P(\overline{W}_n)$$

from which

$$f_n = 5/6\ f_{n-1} + 1/6\ P(E_n|W_n), \ n = 2, 3, \ldots, \tag{3}$$

where $f_1 = 1$. But

$$\begin{aligned} P(E_k|W_k) &= P(R_{k-1};\ E_{k-2}) + P(W_{k-1};\ E_{k-1}) \\ &= 1/2\ f_{k-2} + P(E_{k-1}|W_{k-1})P(W_{k-1}), \ k = 2, 3, \ldots . \end{aligned}$$

Hence,

$$P(E_k|W_k) = 1/2\ f_{k-2} + 1/6\ P(E_{k-1}|W_{k-1}), \ k = 2, 3, \ldots, \tag{4}$$

where $f_0 = 1$ and $P(E_1|W_1) = 1$. Substitution of (4) into (3) for $k = n$ yields

$$f_n = 5/6\ f_{n-1} + 1/6[1/2\ f_{n-2} + 1/6\ P(E_{n-1}|W_{n-1})], \ n = 2, 3, \ldots, \tag{5}$$

for which $P(E_{n-1}|W_{n-1})$ may be found from (4).

Successive substitution of $P(E_k|W_k)$ into (3) for $k = n - 1, \ldots, 1$ yields

$$f_n = 5/6\ f_{n-1} + 1/2 \sum_{j=0}^{n-2} (1/6)^{n-1-j} f_j + (1/6)^n, \ n = 2, 3, \ldots . \tag{6}$$

Equation (6) and the initial conditions can be expressed in the form of (1) with

$$a_0 = 5/6,$$
$$a_n = 1/2\ (1/6)^n, \ n = 1, 2, 3, \ldots,$$
$$b_n = 1/6\ (1/6)^n, \ n = 0, 1, 2, \ldots .$$

References

1. P. J. Asveld. "A Family of Fibonacci-Like Sequences." *Fibonacci Quarterly 25.1* (1987):81-83.
2. P. S. Fisher & E. E. Kohlbecker. "A Generalized Fibonacci Sequence." *Fibonacci Quarterly 10.4* (1972):337-344.
3. H. Gabai. "Generalized Fibonacci k-Sequences." *Fibonacci Quarterly 8.1* (1970):31-38.
4. L. G. Mitten, G. L. Nemhauser, & C. Beightler. "A Short Table of z-Transforms and Generating Functions." *Operations Research* 9 (1961):574-578.

*****

A NOTE CONCERNING THOSE n FOR WHICH $\phi(n) + 1$ DIVIDES n

G. L. Cohen
The New South Wales Institute of Technology, Sydney, Australia

S. L. Segal
The University of Rochester, Rochester, NY 14627

(Submitted July 1987)

In [3, p. 52], Richard Guy gives the following problem of Schinzel: If p is an odd prime and $n = 2$ or p or $2p$, then $(\phi(n) + 1)|n$, where ϕ is Euler's totient function. Is this true for any other n?

We shall show that this question is closely related to a much older problem due to Lehmer [4]: whether or not there exist composite n such that $\phi(n)|(n-1)$. It will turn out that if there are no such composite n, then Schinzel's are the only solutions of his problem; if there are other solutions of Schinzel's problem, then they have at least 15 distinct prime factors. Let $\omega(n)$ denote the number of distinct prime factors of n. More specifically, we shall prove the following.

Theorem: Let n be a natural number and suppose $(\phi(n) + 1)|n$. Then one of the following is true.

(i) $n = 2$ or p or $2p$, where p is an odd prime.

(ii) $n = mt$, where $m = 3$, 4, or 6, $\gcd(m, t) = 1$, and $t - 1 = 2\phi(t)$ [so that $\omega(t) \geq 14$].

(iii) $n = mt$, where $\gcd(m, t) = 1$, $\phi(m) = j \geq 4$, and $t - 1 = j\phi(t)$ [so that $\omega(t) \geq 140$].

Proof: Since $(\phi(n) + 1)|n$, we have

$$m(\phi(n) + 1) = n \tag{1}$$

for some natural number m. Let $t = \phi(n) + 1$ and $d = \gcd(m, t)$. Then, using (1) and an easy and well-known result (Apostol [1, p. 28]),

$$\phi(n) = \phi(mt) = \frac{\phi(m)\phi(t)d}{\phi(d)}. \tag{2}$$

Since $d|m$, we have $\phi(d)|\phi(m)$ so that $\phi(m)/\phi(d)$ is an integer. Then, from (2), $d|\phi(n)$; but, by definition, $d|(\phi(n) + 1)$. Hence $d = 1$. Thus, we have $n = mt$, where

$$t = \phi(n) + 1 = \phi(mt) + 1 = \phi(m)\phi(t) + 1.$$

We cannot have $t = 1$. Also, t is prime if and only if $\phi(m) = 1$. In this case, $m = 1$ or 2, and we have Schinzel's solutions, in (i).

Suppose now that t is composite. If $\phi(m) = 2$, then $m = 3$, 4, or 6 and $t - 1 = 2\phi(t)$. Cohen and Hagis [2] showed in this case that $\omega(t) \geq 14$. These are the solutions in (ii). It is impossible to have $\phi(m) = 3$, so the only remaining possibility is that $\phi(m) \geq 4$, so $t - 1 = j\phi(t)$, say, with $j \geq 4$. For this equation to hold, Lehmer [4] pointed out that t must be odd and squarefree, and Lieuwens [5] showed that $\omega(t) \geq 212$ if $3|t$. (This latter remark applies also to the solution $n = 4t$ in (ii).] Suppose $3 \nmid t$, and write

$$t = \prod_{i=1}^{u} p_i, \quad 5 \le p_1 < p_2 < \cdots < p_u,$$

where $p_1, p_2, \ldots, p_u$ are primes. Then $p_2 \ge 7$, $p_3 \ge 11$, ... If $u \le 139$,

$$4 \le j = \frac{t-1}{\phi(t)} < \frac{t}{\phi(t)} = \prod_{i=1}^{u} \frac{p_i}{p_i - 1} \le \frac{5}{4}\,\frac{7}{6}\,\frac{11}{10} \cdots \frac{811}{810} < 4.$$

(There are 139 primes from 5 to 811, inclusive.) This contradiction shows that $u = \omega(t) \ge 140$ in this case, giving (iii) and completing the proof.

Using the above and results of Pomerance [6, esp. the Remark] and [7], it is not difficult to show that the number of natural numbers n such that $n \le x$, $(\phi(n) + 1) | n$ and n is not a prime or twice a prime, is

$$O\left(x^{1/2} (\log x)^{3\,4} (\log \log x)^{-5/6}\right).$$

References

1. T. A. Apostol. *Introduction to Analytic Number Theory*. New York: Springer-Verlag, 1980.
2. G. L. Cohen & P. Hagis, Jr. "On the Number of Prime Factors of n if $\phi(n) | (n - 1)$." *Nieuw Archief voor Wiskunde* (3) *28* (1980):177-185.
3. R. K. Guy. *Unsolved Problems in Number Theory*. New York: Springer-Verlag, 1981.
4. D. H. Lehmer. "On Euler's Totient Function." *Bull. Amer. Math. Soc. 38* (1932):745-751.
5. E. Lieuwens. "Do There Exist Composite Numbers M for Which $k\phi(M) = M - 1$ Holds?" *Nieuw Archief voor Wiskunde* (3) *18* (1970):165-169.
6. C. Pomerance. "On Composite n for which $\phi(n) | n - 1$, II." *Pacific J. Math. 69* (1977):177-186.
7. C. Pomerance. "Popular Values of Euler's Function." *Mathematika 27* (1980):84-89.

*****

(Continued from page 282)

4. H. T. Freitag P. Filipponi. "On the Representation of Integral Sequences $\{F_n/d\}$ and $\{L_n/d\}$ as Sums of Fibonacci Numbers and as Sums of Lucas Numbers." Presented at the Second International Conference on Fibonacci Numbers and Their Applications, August 13-16, San Jose, California, U.S.A.
5. P. Filipponi. "A Note on the Representation of Integers as a Sum of Distinct Fibonacci Numbers." *Fibonacci Quarterly 24.4* (1986):336-343.
6. P. Filipponi & O. Brugia. "On the F-Representation of Integral Sequences Involving Ratios between Fibonacci and Lucas Numbers." Int. Rept. 3B1586, Fondazione Ugo Bordoni, Roma, 1986.
7. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin Co., 1969.

*****

CHARACTERIZATIONS AND EXTENDIBILITY OF P_t-SETS

Vamsi Krishna Mootha
(student)
Msgr. Kelly High School, Beaumont, TX 77707

George Berzsenyi
Rose-Hulman Institute of Technology, Terre Haute, IN 47803

(Submitted December 1988)

Let t be a nonzero integer and S be a set of three or more integers. We will say that S is a P_t-set if, for any two distinct elements x and y of S, the integer $xy + t$ is a perfect square. A P_t-set S will be termed extendible if, for some integer d, $d \notin S$, the set $S \cup \{d\}$ is a P_t-set.

The purpose of this paper is to characterize certain families of P_t-sets, and to show that some of these are not extendible. In particular, the result of Thamotherampillai [1], that the P_2-set $\{1, 2, 7\}$ is not extendible, will be obtained as an easy corollary.

To simplify the exposition, throughout this paper statements of congruences are to be interpreted modulo 4; i.e., $x \equiv y$ will mean $x \equiv y \pmod 4$.

Lemma: If S is a P_t-set and $a, b, c \in S$, then none of the numbers

$$a(c - b), \quad b(c - a), \quad c(b - a)$$

is congruent to 2, modulo 4.

Proof: By the definition of P_t-sets, we have

$$ab + t = x^2, \quad ac + t = y^2, \quad bc + t = z^2$$

for some integers x, y, and z. Upon eliminating t among the equations above, the result follows from the fact that perfect squares are congruent to 0 or 1, modulo 4.

Theorem 1: If all of the elements of a P_t-set are odd, then they are congruent to one another, modulo 4.

Proof: Let S be a P_t-set, and $a, b, c \in S$. Observe that, if $a \equiv b \equiv 1$ and $c \equiv 3$, then $a(c - b) \equiv 2$; while if $a \equiv 1$ and $b \equiv c \equiv 3$, then $b(c - a) \equiv 2$. Both of these conclusions are impossible in view of the Lemma; hence, either $a \equiv b \equiv c \equiv 1$ or $a \equiv b \equiv c \equiv 3$.

Theorem 2: If only one of the elements of a P_t-set is odd, then all of the others are congruent to 0, modulo 4.

Proof: Let S be a P_t-set, and $a, b, c \in S$. Observe that, if $a \equiv 1$, $b \equiv 2$, and $c \equiv 0$ or if $a \equiv 3$, $b \equiv 2$, $c \equiv 0$, then $a(c - b) \equiv 2$; while if $a \equiv 1$ and $b \equiv c \equiv 2$ or if $a \equiv 3$ and $b \equiv c \equiv 2$, then $c(b - a) \equiv 2$. Both of these conclusions are impossible in view of the Lemma; hence, if $a \equiv 1$ or 3, then $b \equiv c \equiv 0$.

Theorem 3: P_t-sets of the form $\{4k + 1, 4m + 2, 4n + 3\}$ are not extendible.

Proof: Assume that $\{4k + 1, 4m + 2, 4n + 3, d\}$ is a P_t-set. If d is odd, then $\{4k + 1, 4n + 3, d\}$ is a P_t-set all of whose elements are odd. However, $4k + 1 \not\equiv 4n + 3$, contrary to Theorem 1. If d is even, then $\{4k + 1, 4m + 2, d\}$ is a P_t-set with only one odd element, $4k + 1$. But $4m + 2 \not\equiv 0$, contrary to Theorem 2. Consequently, such d cannot exist.

Corollary: The P_2-set $\{1, 2, 7\}$ is not extendible.

At this point, the authors wish to express their appreciation to Bud Brown, who sent them a copy of [2] upon reading [3], and hence called their attention to [1]. It may also be noted that Thamotherampillai's proof of the corollary is much more complicated, and its method does not allow for generalizations.

In conclusion, we provide a table of examples which shows that all of the cases not disallowed by Theorems 1 and 2 are indeed possible. In the "congruence type" column, the members of S are reduced modulo 4 to allow for a quick review; thus, for example, the P_{97}-set $\{3, 8, 24\}$ is type [3,0,0] since $3 \equiv 3$ and $8 \equiv 24 \equiv 0$. In this terminology, P_t-sets of types [1,1,3] and [1,3,3] do not exist in view of Theorem 1, P_t-sets of types [1,2,2], [1,2,0], [3,2,2], and [3,2,0] do not exist in view of Theorem 2; and P_t-sets of type [1,2,3] are not extendible in view of Theorem 3.

Table of Examples

Congruence type	S	t	Congruence type	S	t
[1,1,1]	{1,5,33}	31	[2,2,2]	{2,10,22}	5
[3,3,3]	{7,11,23}	323	[1,1,0]	{1,9,20}	16
[1,0,0]	{5,8,16}	41	[1,1,2]	{1,5,10}	-1
[3,0,0]	{3,8,24}	97	[1,3,0]	{1,7,16}	9
[0,0,0]	{4,12,32}	16	[1,3,2]	{1,79,98}	2
[2,0,0]	{2,12,420}	1	[3,3,0]	{3,27,60}	144
[2,2,0]	{2,6,16}	4	[3,3,2]	{3,7,2}	-5

References

1. N. Thamotherampillai. "The Set of Numbers {1, 2, 7}." *Bull. Calcutta Math. Society* 72 (1980):195-197.
2. Ezra Brown. "Sets in Which $xy + k$ is Always Square." *Math. Comp.* 45.172 (1985):613-620.
3. G. Berzsenyi. "Problems, Puzzles and Paradoxes: Discoveries." *Consortium* No. 25 (March 1988):5.

*****

SUSTAINING MEMBERS

*Charter Members

A.F. Alameddine
*A.L. Alder
G.L. Alexanderson
S. Ando
R. Andre-Jeannin
*J. Arkin
M.K. Azarian
L. Bankoff
F. Bell
M. Berg
J.G. Bergart
G. Bergum
G. Berzsenyi
*M. Bicknell-Johnson
M.F. Bryn
P.F. Byrd
G.D. Chakerian
J.W. Creely
P.A. DeCaux
M.J. DeLeon
J. Desmond
H. Diehl
T.H. Engel
D.R. Farmer
P. Flanagan
F.F. Frey, Jr.
Emerson Frost
Anthony Gioia
R.M. Giuli
I.J. Good
*H.W. Gould
M. Guild
H. Harborth
H.E. Heatherly
A.P. Hollman
*A.F. Horadam
F.T. Howard
R.J. Howell
H. Ibstedt
R.P. Kelisky
C.H. Kimberling
J. Lahr
J. C. Lagarias
N. Levine
C.T. Long
Br. J. M. Mahon
*J. Maxwell
F.U. Mendizabal
L. Miller
M.G. Monzingo
S.D. Moore, Jr.
J.F. Morrison
K. Nagasaka
F.G. Ossiander
A. Prince
S. Rabinowitz
E.D. Robinson
S.E. Schloth
J. A. Schumaker
A.G. Shannon
D. Singmaster
J. Sjoberg
B. Sohmer
L. Somer
M.N.S. Swamy
*D. Thoro
J.C. Turner
R. Vogel
J.N. Vitale
M. Waddill
J.E. Walton
G. Weekly
R.E. Whitney
B.E. Williams
A.C. Yanoviak

INSTITUTIONAL MEMBERS

THE BAKER STORE EQUIPMENT COMPANY
Cleveland, Ohio

BOSTON COLLEGE
Chestnut Hill, Massachusetts

BUCKNELL UNIVERSITY
Lewisburg, Pennsylvania

CALIFORNIA STATE UNIVERSITY SACRAMENTO
Sacramento, California

THE COLLEGE OF IDAHO
Caldwell, Idaho

EMERGING TECHNOLOGIES GROUP, INC.
Dix Hills, New York

ETH-BIBLIOTHEK
Zurich, Switzerland

FERNUNIVERSITAET HAGEN
Hagen, West Germany

HOWELL ENGINEERING COMPANY
Bryn Mawr, California

NEW YORK PUBLIC LIBRARY GRAND CENTRAL STATION
New York, New York

NORTHWESTERN UNIVERSITY
Evanston, Illinois

PRINCETON UNIVERSITY
Princeton, New Jersey

SAN JOSE STATE UNIVERSITY
San Jose, California

SANTA CLARA UNIVERSITY
Santa Clara, California

KLEPKO, INC.
Sparks, Nevada

TECHNOLOGICAL EDUCATION INSTITUTE
Larissa, Greece

UNIVERSITY OF SALERNO
Salerno, Italy

UNIVERSITY OF CALIFORNIA, SANTA CRUZ
Santa Cruz, California

UNIVERSITY OF GEORGIA
Athens, Georgia

UNIVERSITY OF NEW ENGLAND
Armidale, N.S.W. Australia

WAKE FOREST UNIVERSITY
Winston-Salem, North Carolina

WASHINGTON STATE UNIVERSITY
Pullman, Washington

JOVE STATISTICAL TYPING SERVICE
2088 Orestes Way
Campbell, California 95008

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.

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.

Fibonacci Numbers and Their Applications. Edited by A.N. Philippou, G.E. Bergum and A.F. Horadam.

Please write to the Fibonacci Association, Santa Clara University, Santa Clara, CA 95053, U.S.A., for current prices.