The Fibonacci Quarterly

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

TABLE OF CONTENTS

VOLUME 33 AUGUST 1995 NUMBER 4

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 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. Since the Fibonacci Association has adopted $F_1 = F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$, $n \geq 2$ and $L_1 = 1$, $L_2 = 3$, $L_{n+1} = L_n + L_{n-1}$, $n \geq 2$ as the standard definitions for The Fibonacci and Lucas sequences, these definitions ***should not*** be a part of future papers. However, the notations ***must*** be used. One to three ***complete*** A.M.S. classification numbers ***must*** be given directly after references or on the bottom of the last page. Papers without classification numbers will be returned. See the new worldwide web page at:

http://www.math.uga.edu/andrew/Fibonacci/fibhome.html

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 57007-1596.**

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 $37 for Regular Membership, $42 for Library, $47 for Sustaining Membership, and $74 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

A CONGRUENCE FOR FIBONOMIAL COEFFICIENTS MODULO p^3

William A. Kimball and William A. Webb
Department of Pure and Applied Mathematics, Washington State University, Pullman, WA 99164-3113
(*Submitted June 1993*)

An interesting property of binomial coefficients is that, for primes $p > 3$,

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^k} \tag{1}$$

for $k = 1, 2, 3$.

The *Fibonomial coefficients*, defined as

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{F_n F_{n-1} \dots F_1}{(F_k F_{k-1} \dots F_1)(F_{n-k} \dots F_1)},$$

or, more generally,

$$\begin{bmatrix} n \\ k \end{bmatrix}_j = \frac{F_{nj} F_{(n-1)j} \dots F_j}{(F_{kj} F_{(k-1)j} \dots F_j)(F_{(n-k)j} \dots F_j)},$$

where F_i is the i^{th} Fibonacci number. Such expressions have been shown to possess many properties similar to binomial coefficients. In a previous paper [5] the authors investigated properties of Fibonomial coefficients similar to the property (1) of binomial coefficients for $k = 2$. The main results of that paper are:

$$\begin{bmatrix} ra \\ rb \end{bmatrix} \equiv \varepsilon^{(a-b)br} \binom{a}{b} \pmod{p^2} \tag{2}$$

and

$$\begin{bmatrix} \tau a \\ \tau b \end{bmatrix} \equiv \binom{ta}{tb} \pmod{p^2}, \tag{3}$$

where τ is the period of the Fibonacci sequence modulo an odd prime p, r is the rank of apparition of p (that is, F_r is the first nonzero F_i divisible by p), and $t = \tau / r$ is an integer. In [7] it is shown that t must assume the value 1, 2, or 4. The number ε is defined by $\varepsilon = 1$ if $\tau = r$, $\varepsilon = -1$ if $\tau = 2r$, and $\varepsilon^2 \equiv -1 \pmod{p^2}$ if $\tau = 4r$.

Unlike the ordinary binomial coefficients, these results are not true in general for higher powers of p. However, in some cases they can be extended to congruences modulo p^3.

In order to prove these results, we will first examine some congruences involving certain products of consecutive Fibonacci numbers. Throughout the paper, L_i represents the i^{th} Lucas number, and $p > 3$ is prime.

We first consider $\prod_{k=1}^{r-1} F_{mr+k}$ modulo p^3. From the identity $2F_{a+b} = L_a F_b + L_b F_a$, we obtain $2F_{mr+k} = L_{mr} F_k + L_k F_{mr}$ so that, upon expanding the product and using the facts $p \mid F_r$ and $F_r \mid F_{mr}$, we have $p \mid F_{mr}$ and

$$2^{r-1} \prod_{k=1}^{r-1} F_{mr+k} \equiv (L_{mr}^{r-1} + L_{mr}^{r-2} F_{mr} \Sigma_1 + L_{mr}^{r-3} F_{mr}^2 \Sigma_2) \left(\prod_{k=1}^{r-1} F_k \right) \pmod{p^3}, \tag{4}$$

where

$$\Sigma_1 = \sum_{k=1}^{r-1} \frac{L_k}{F_k} \quad \text{and} \quad \Sigma_2 = \sum_{\substack{n,k=1 \\ k<n}}^{r-1} \frac{L_k}{F_k}\frac{L_n}{F_n}.$$

Then, upon dividing both sides of (4) by $(2^{r-1})\prod_{k=1}^{r-1} F_k$,

$$\frac{\prod_{k=1}^{r-1} F_{mr+k}}{\prod_{k=1}^{r-1} F_k} \equiv \left(\frac{L_{mr}}{2}\right)^{r-1} + \frac{1}{2}\left(\frac{L_{mr}}{2}\right)^{r-2} F_{mr}\Sigma_1 + \frac{1}{4}\left(\frac{L_{mr}}{2}\right)^{r-3} F_{mr}^2\Sigma_2$$
$$\equiv \frac{1}{4}\left(\frac{L_{mr}}{2}\right)^{r-3} [L_{mr}^2 + L_{mr}F_{mr}\Sigma_1 + F_{mr}^2\Sigma_2] \pmod{p^3}. \tag{5}$$

We will next work toward simplifying the right-hand side of (5), specifically we will eliminate Σ_2 by writing it in terms of Σ_1.

Now, because $\Sigma_1 = \Sigma_{k=1}^{r-1}(L_k / F_k)$, we see that

$$\Sigma_1^2 = \left(\sum_{k=1}^{r-1} \frac{L_k}{F_k}\right)^2 = \sum_{k=1}^{r-1}\left(\frac{L_k}{F_k}\right)^2 + 2\sum_{\substack{n,k=1 \\ k<n}}^{r-1} \frac{L_k}{F_k}\frac{L_n}{F_n} = \sum_{k=1}^{r-1}\left(\frac{L_k}{F_k}\right)^2 + 2\Sigma_2,$$

thus

$$\Sigma_2 = \frac{1}{2}\left[\Sigma_1^2 - \sum_{k=1}^{r-1}\left(\frac{L_k}{F_k}\right)^2\right]. \tag{6}$$

Now $\Sigma_1 \equiv 0 \pmod{p}$ [5] so that, from (6), we obtain

$$F_{mr}^2\Sigma_2 \equiv -\frac{1}{2}F_{mr}^2\sum_{k=1}^{r-1}\left(\frac{L_k}{F_k}\right)^2 \pmod{p^4}. \tag{7}$$

We look at $\Sigma_{k=1}^{r-1}(L_k / F_k)^2$ modulo p^2. Clearly,

$$2\sum_{k=1}^{r-1}\left(\frac{L_k}{F_k}\right)^2 = \sum_{k=1}^{r-1}\left[\left(\frac{L_k}{F_k}\right)^2 + \left(\frac{L_{r-k}}{F_{r-k}}\right)^2\right] = \sum_{k=1}^{r-1}\left[\frac{(L_kF_{r-k})^2 + (L_{r-k}F_k)^2}{(F_kF_{r-k})^2}\right],$$

and, from an identity already mentioned,

$$(2F_r)^2 = (L_kF_{r-k} + L_{r-k}F_k)^2 = (L_kF_{r-k})^2 + (L_{r-k}F_k)^2 + 2(L_kF_{r-k}L_{r-k}F_k),$$

which implies

$$(L_kF_{r-k})^2 + (L_{r-k}F_r)^2 \equiv -2(L_kF_{r-k}L_{r-k}F_k) \pmod{p^2}.$$

Then, substituting in the equality just above,

$$2\sum_{k=1}^{r-1}\left(\frac{L_k}{F_k}\right)^2 = \sum_{k=1}^{r-1}\left[\frac{(L_kF_{r-k})^2 + (L_{r-k}F_k)^2}{(F_kF_{r-k})^2}\right] \equiv \sum_{k=1}^{r-1}\frac{-2(L_kF_{r-k}L_{r-k}F_k)}{(F_kF_{r-k})^2} \equiv -2\sum_{k=1}^{r-1}\frac{L_k}{F_k}\frac{L_{r-k}}{F_{r-k}} \pmod{p^2}$$

or

$$\sum_{k=1}^{r-1}\left(\frac{L_k}{F_k}\right)^2 \equiv -\sum_{k=1}^{r-1}\frac{L_k}{F_k}\frac{L_{r-k}}{F_{r-k}} \pmod{p^2}.$$

We now use the identity $2L_{a+b} = L_aL_b + 5F_aF_b$ to note that $2L_r = L_kL_{r-k} + 5F_kF_{r-k}$; hence,

$$5 + \frac{L_kL_{r-k}}{F_kF_{r-k}} = \frac{2L_r}{F_kF_{r-k}}.$$

Thus,

$$-\sum_{k=1}^{r-1}\frac{L_k}{F_k}\frac{L_{r-k}}{F_{r-k}} = \sum_{k=1}^{r-1}\left(5 - \frac{2L_r}{F_kF_{r-k}}\right) = 5(r-1) - \sum_{k=1}^{r-1}\frac{2L_r}{F_kF_{r-k}}$$

or

$$\sum_{k=1}^{r-1}\left(\frac{L_k}{F_k}\right)^2 \equiv 5(r-1) - \sum_{k=1}^{r-1}\frac{2L_r}{F_kF_{r-k}} \pmod{p^2}. \tag{8}$$

Then, from (7) and (8), we have

$$F_{mr}^2\Sigma_2 \equiv \frac{-5}{2}F_{mr}^2(r-1) + F_{mr}^2\sum_{k=1}^{r-1}\frac{L_r}{F_kF_{r-k}} \pmod{p^4}$$

or

$$F_{mr}^2\Sigma_2 \equiv \frac{-5}{2}F_{mr}^2(r-1) + L_r\frac{F_{mr}^2}{F_r}\sum_{k=1}^{r-1}\frac{F_r}{F_kF_{r-k}} \pmod{p^4}.$$

However,

$$2\Sigma_1 = \sum_{k=1}^{r-1}\left(\frac{L_k}{F_k} + \frac{L_{r-k}}{F_{r-k}}\right) = \sum_{k=1}^{r-1}\frac{L_kF_{r-k} + L_{r-k}F_k}{F_kF_{r-k}} = \sum_{k=1}^{r-1}\frac{2F_r}{F_kF_{r-k}}$$

so that

$$\Sigma_1 = \sum_{k=1}^{r-1}\frac{F_r}{F_kF_{r-k}}. \tag{9}$$

Hence, from the last congruence,

$$F_{mr}^2\Sigma_2 \equiv \frac{-5}{2}F_{mr}^2(r-1) + L_r\frac{F_{mr}^2}{F_r}\Sigma_1 \pmod{p^4},$$

and so, substituting into (5),

$$\frac{\prod_{k=1}^{r-1}F_{mr+k}}{\prod_{k=1}^{r-1}F_k} \equiv \left(\frac{L_{mr}}{2}\right)^{r-1} - \frac{5}{8}F_{mr}^2\left(\frac{L_{mr}}{2}\right)^{r-3}(r-1) + \left(\frac{L_{mr}}{2}\right)^{r-2}\frac{1}{2}\left(F_{mr} + \frac{L_r}{L_{mr}}\frac{F_{mr}^2}{F_r}\right)\Sigma_1 \pmod{p^3}. \tag{10}$$

It is known that, for $p \neq 5$, r divides either $p-1$ or $p+1$, so we will look at the two special cases where $r = p \pm 1$ and prove a proposition that is interesting in its own right.

Proposition 1: For $r = p \pm 1$,

$$\sum_{k=1}^{r-1} \frac{L_k}{F_k} = \Sigma_1 \equiv 0 \pmod{p^2}$$

for any odd prime p.

Proof: In order to show that $\Sigma_1 \equiv 0 \pmod{p^2}$, we need only show that $\Sigma_{k=1}^{r-1}(1/F_kF_{r-k}) \equiv 0 \pmod{p}$ since, from (9), $\Sigma_1 = \Sigma_{k=1}^{r-1}(F_r/F_kF_{r-k})$ and $p|F_r$. In [5], it was proved that $L_{kr} \equiv 2\varepsilon^k \pmod{p^2}$, where ε was as previously defined.

Thus, $L_r \equiv 2\varepsilon \not\equiv 0 \pmod{p}$, and therefore, $\Sigma_{k=1}^{r-1}(1/F_kF_{r-k}) \equiv 0 \pmod{p}$ if and only if $\Sigma_{k=1}^{r-1}(-2L_r/F_kF_{r-k}) \equiv 0 \pmod{p}$. We have, from (8), that

$$\sum_{k=1}^{r-1} \frac{-2L_r}{F_kF_{r-k}} \equiv -5(r-1) + \sum_{k=1}^{r-1}\left(\frac{L_k}{F_k}\right)^2 \pmod{p}.$$

We will show that, for $r = p \pm 1$, the right-hand side of the above congruence is congruent to 0 modulo p. We first prove a few simple lemmas.

Lemma 1: The numbers L_k / F_k are all incongruent modulo p for $k = 1, \ldots, r-1$.

Proof: Assume that $L_k/F_k \equiv L_j/F_j \pmod{p}$ for some $1 \le j < k \le r-1$. Then $L_kF_j \equiv L_jF_k \pmod{p}$, and from the identity $2F_{k-j} = F_kL_{-j} + F_{-j}L_k$ together with the facts $F_{-j} = (-1)^{j+1}F_j$ and $L_{-j} = (-1)^jL_j$, we obtain $2F_{k-j} = (-1)^j[F_kL_j - F_jL_k] \equiv 0 \pmod{p}$. However, this is impossible because $1 \le k-j \le (r-2)$.

Lemma 2: $(L_k/F_k)^2 \not\equiv 5 \pmod{p}$ for all k and all odd primes p.

Proof: Assume that $(L_k/F_k)^2 \equiv 5 \pmod{p}$, then $L_k^2 \equiv 5F_k^2 \pmod{p}$ so that $2L_k^2 \equiv L_k^2 + 5F_k^2 \pmod{p}$. But, from $2L_{a+b} = L_aL_b + 5F_aF_b$, we have $2L_{2k} = L_k^2 + 5F_k^2$ so that $L_k^2 \equiv L_{2k} \pmod{p}$. However, from the identity $L_{a+b} = L_aL_b - (-1)^bL_{a-b}$, we obtain $L_{2k} = L_k^2 \pm 2$, and combining this with $L_k^2 \equiv L_{2k} \pmod{p}$ we conclude that $0 \equiv \pm 2 \pmod{p}$ for the odd prime p.

We are now in a position to complete the proof of Proposition 1. We have seen that we need to show that $-5(r-1) + \Sigma_{k=1}^{r-1}(L_k/F_k)^2 \equiv 0 \pmod{p}$ for $r = p \pm 1$. We consider the two cases separately.

Case 1. $r = p+1$

$$-5(r-1) + \sum_{k=1}^{r-1}\left(\frac{L_k}{F_k}\right)^2 \equiv -5p + \sum_{k=1}^{p}\left(\frac{L_k}{F_k}\right)^2 \equiv \sum_{k=1}^{p}\left(\frac{L_k}{F_k}\right)^2 \pmod{p}.$$

But from Lemma 1 we have that, for $k = 1, \ldots, p = r-1$, the numbers L_k/F_k are all incongruent modulo p; thus, the set of p numbers $\{L_k/F_k : k = 1, \ldots, p\}$ forms a complete residue system modulo p. Then

$$\sum_{k=1}^{p}\left(\frac{L_k}{F_k}\right)^2 \equiv \sum_{k=1}^{p} k^2 \equiv 0 \pmod{p}.$$

Case 2. $r = p-1$

$$-5(r-1)+\sum_{k=1}^{r-1}\left(\frac{L_k}{F_k}\right)^2 = -5(p-2)+\sum_{k=1}^{p-2}\left(\frac{L_k}{F_k}\right)^2 \equiv 10+\sum_{k=1}^{p-2}\left(\frac{L_k}{F_k}\right)^2 \pmod p.$$

Now all of the L_k / F_k for $k = 1, \dots, p-2$ are incongruent modulo p by Lemma 1 and, from Lemma 2, $(L_k / F_k)^2 \not\equiv 5 \pmod p$ for each k. However, 5 is a quadratic residue modulo p [8], and we have

$$10+\sum_{k=1}^{p-2}\left(\frac{L_k}{F_k}\right)^2 \equiv \sum_{k=1}^{p} k^2 \equiv 0 \pmod p.$$

Thus, Proposition 1 is proved.

Since $p \nmid L_{mr}$, but $p|F_r$ and $F_r|F_{mr}$, an immediate consequence of Proposition 1 is the following corollary concerning the last term in equation 10.

Corollary 1:

$$\left(\frac{L_{mr}}{2}\right)^{r-2}\frac{1}{2}\left(F_{mr}+\frac{L_r}{L_{mr}}\frac{F_{mr}^2}{F_r}\right)\Sigma_1 \equiv 0 \pmod{p^3}.$$

Before proving our main theorem, we need the following result about the specific Fibonomial coefficient

$$\begin{bmatrix}(m+1)r-1\\ r-1\end{bmatrix} = \frac{\prod_{k=1}^{r-1} F_{mr+k}}{\prod_{k=1}^{r-1} F_k}$$

modulo p^3.

Lemma 3: If $p>3$ and $r = p \pm 1$, then $\left[{(m+1)r-1 \atop r-1}\right] \equiv (\mp 1)^m \pmod{p^3}$, respectively.

Proof: We again deal with the two cases separately.

Case 1. $r = p-1$

If $r = p-1$, then r is even and $\tau = p-1$. From (10) and Corollary 1,

$$\frac{\prod_{k=1}^{r-1} F_{mr+k}}{\prod_{k=1}^{r-1} F_k} \equiv \left(\frac{L_{mr}}{2}\right)^{p-2} - \frac{5}{8}F_{mr}^2\left(\frac{L_{mr}}{2}\right)^{p-4}(p-2) \equiv \frac{1}{4}\left(\frac{L_{mr}}{2}\right)^{p-4}[L_{mr}^2+5F_{mr}^2] \pmod{p^3}.$$

But $L_{mr}^2+5F_{mr}^2 = 2L_{2mr}$. Furthermore, $L_{2mr} = L_{mr}L_{mr}-(-1)^{mr}L_{mr-mr} = L_{mr}^2-2$, so $L_{mr}^2+5F_{mr}^2 = 2(L_{mr}^2-2)$. Therefore,

$$\frac{1}{4}\left(\frac{L_{mr}}{2}\right)^{p-4}[L_{mr}^2+5F_{mr}^2] = 2\left(\frac{L_{mr}}{2}\right)^{p-2} - \left(\frac{L_{mr}}{2}\right)^{p-4}.$$

However, from $L_{kr} \equiv 2\varepsilon^k \pmod{p^2}$, we obtain $L_{mr}/2 \equiv 1 \pmod{p^2}$, so $L_{mr}/2 = 1+p^2q$ for some q. Then

$$\left(\frac{L_{mr}}{2}\right)^{p-k} = (1+p^2q)^{p-k} \equiv 1+(p-k)p^2q \equiv 1-kp^2q \pmod{p^3},$$

and so

$$2\left(\frac{L_{mr}}{2}\right)^{p-2} - \left(\frac{L_{mr}}{2}\right)^{p-4} \equiv 2(1-2p^2q)-(1-4p^2q) \equiv 1 \pmod{p^3}$$

or

$$\frac{\prod_{k=1}^{r-1} F_{mr+k}}{\prod_{k=1}^{r-1} F_k} \equiv 1 \equiv (1)^m \pmod{p^3}.$$

Case 2. $r = p+1$

If $r = p+1$, then $\tau = 2r$ and r is even. From (10) and Corollary 1,

$$\frac{\prod_{k=1}^{r-1} F_{mr+k}}{\prod_{k=1}^{r-1} F_k} \equiv \left(\frac{L_{mr}}{2}\right)^p - \frac{5}{8}F_{mr}^2\left(\frac{L_{mr}}{2}\right)^{p-2}(p) \equiv \left(\frac{L_{mr}}{2}\right)^p \pmod{p^3}.$$

Now, $L_{kr} \equiv 2\varepsilon^k \pmod{p^2}$ yields $L_{mr}/2 \equiv (-1)^m \pmod{p^2}$ or $L_{mr}/2 = (-1)^m + p^2q$ for some q. Then,

$$2\left(\frac{L_{mr}}{2}\right)^p \equiv (-1)^{mp} + (-1)^{m(p-1)}(p)(p^2q) \pmod{p^3}$$

or

$$\frac{\prod_{k=1}^{r-1} F_{mr+k}}{\prod_{k=1}^{r-1} F_k} \equiv (-1)^m \pmod{p^3}.$$

Thus, Lemma 3 is proved.

Proposition 2: For any $n \geq 0$ and $m \geq 0$, if $r = p \pm 1$, then

$$\prod_{k=nr+1}^{nr+r-1} F_{mr+k} \equiv (\mp 1)^m \prod_{k=nr+1}^{nr+r-1} F_k \pmod{p^3}, \text{ respectively.}$$

Proof: From Lemma 3,

$$\prod_{k=nr+1}^{nr+r-1} F_{mr+k} = \prod_{k=1}^{r-1} F_{(m+n)r+k} \equiv (\mp 1)^{m+n} \prod_{k=1}^{r-1} F_k \pmod{p^3}$$

and

$$\prod_{k=nr+1}^{nr+r-1} F_k = \prod_{k=1}^{r-1} F_{nr+k} \equiv (\mp 1)^n \prod_{k=1}^{r-1} F_k \pmod{p^3}$$

so that

$$\frac{\prod_{k=nr+1}^{nr+r-1} F_{mr+k}}{\prod_{k=nr+1}^{nr+r-1} F_k} \equiv \frac{(\mp 1)^{m+n}\prod_{k=1}^{r-1} F_k}{(\mp 1)^n \prod_{k=1}^{r-1} F_k} \equiv (\mp 1)^m \pmod{p^3}.$$

Recalling that

$$\begin{bmatrix} a \\ b \end{bmatrix}_r = \frac{F_{ar}F_{(a-1)r}\cdots F_r}{(F_{br}F_{(b-1)r}\cdots F_r)(F_{(a-b)r}\cdots F_r)},$$

we can now prove our main theorem.

Theorem: For any prime $p>3$ and any $a \ge b \ge 0$, if $r = p \pm 1$, then

$$\begin{bmatrix} ra \\ rb \end{bmatrix} \equiv (\mp 1)^{(a-b)b} \begin{bmatrix} a \\ b \end{bmatrix}_r \pmod{p^3}, \text{ respectively.}$$

Proof: Separating the factors divisible by p from those relatively prime to p, we obtain

$$\begin{bmatrix} ar \\ br \end{bmatrix} = \frac{F_{ar}F_{ar-1}\cdots F_{(a-b)r+1}}{F_{br}F_{br-1}\cdots F_1} = \left(\frac{F_{ar}F_{(a-1)r}}{F_{br}F_{(b-1)r}}\cdots\frac{F_{(a-b+1)r}}{F_r}\right)\left(\frac{\prod_{k=(a-1)r+1}^{(a-1)r+r-1} F_k \cdots \prod_{k=(a-b)r+1}^{(a-b)r+r-1} F_k}{\prod_{k=(b-1)r+1}^{(b-1)r+r-1} F_k \cdots \prod_{k=1}^{r-1} F_k}\right).$$

By Proposition 2, the right factor above is congruent to $(\mp 1)^{a-b}\cdots(\mp 1)^{a-b} \equiv (\mp 1)^{(a-b)b} \pmod{p^3}$ and the left factor is $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]_r$. Hence,

$$\begin{bmatrix} ar \\ br \end{bmatrix} \equiv (\mp 1)^{(a-b)b} \begin{bmatrix} a \\ b \end{bmatrix}_r \pmod{p^3}.$$

Corollary: For $a \ge b \ge 0$,

$$\begin{bmatrix} a\tau \\ b\tau \end{bmatrix} \equiv \begin{cases} \begin{bmatrix} a \\ b \end{bmatrix}_r & \text{if } r = p-1 \\ \begin{bmatrix} 2a \\ 2b \end{bmatrix}_r & \text{if } r = p+1 \end{cases} \pmod{p^3}.$$

Proof: These follow immediately from the Theorem and the facts: $\tau = p-1$ if $r = p-1$ and $\tau = 2(p+1)$ if $r = p+1$. If $\tau = tr$, then

$$\begin{bmatrix} a\tau \\ b\tau \end{bmatrix} = \begin{bmatrix} atr \\ btr \end{bmatrix} \equiv (\mp 1)^{(a-b)bt} \begin{bmatrix} at \\ bt \end{bmatrix}_r \equiv \begin{bmatrix} ta \\ tb \end{bmatrix}_r \pmod{p^3}.$$

As was shown in [5], if the modulus is only p^2 instead of p^3, the expression $\left[\begin{smallmatrix} ta \\ tb \end{smallmatrix}\right]_r$ can also be written in terms of ordinary binomial coefficients. Can this be done mod p^3 as well? It might also be noted that in [5] this reduction was possible because

$$\frac{F_{kr}}{F_{p^s r}} = \frac{k}{p^s}\left(\frac{L_r}{2}\right)^{k-p^s} \pmod{p^2}$$

if $p^s | k$. (Proposition 2 was the case $s = 0$, but the general case is essentially the same and somewhat more useful.) The same congruence is, in general, false mod p^3.

REFERENCES

1. H. W. Gould. "The Bracket Function and Fontené-Ward Generalized Binomial Coefficients with Application to Fibonacci Coefficients." *The Fibonacci Quarterly* **7.1** (1969):23-40.
2. H. W. Gould. "Equal Products of Generalized Binomial Coefficients." *The Fibonacci Quarterly* **9.4** (1971):337-46.
3. V. E. Hoggatt, Jr. "Fibonacci Numbers and Generalized Binomial Coefficients." *The Fibonacci Quarterly* **5.4** (1967):383-400.
4. S. K. Jerbic. "Fibonomial Coefficients—A Few Summation Properties." Master's Thesis, San Jose State College, San Jose, California, 1968.
5. W. A. Kimball & W. A. Webb. "Congruence Properties of Fibonacci Numbers and Fibonacci Coefficients." In *Applications of Fibonacci Numbers*, Vol. 5. Dordrecht: Kluwer, 1993.
6. D. A. Lind. "A Determinant Involving Generalized Binomial Coefficients." *The Fibonacci Quarterly* **9.2** (1971):113-19, 162.
7. R. F. Torretoo & J. A. Fuchs. "Generalized Binomial Coefficients." *The Fibonacci Quarterly* **2.3** (1964):296-302.
8. J. Vinson. "The Relation of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence." *The Fibonacci Quarterly* **1.1** (1963):37-45.

AMS Classification Numbers: 11B39, 11B65, 11B50

VISUALIZING GOLDEN RATIO SUMS WITH TILING PATTERNS

Marjorie Bicknell-Johnson
665 Fairlane Avenue, Santa Clara, CA 95051

Duane DeTemple
Department of Pure and Applied Math., Washington State University, Pullman, WA 99164-3113

(*Submitted September 1993*)

Several sums involving the Golden Ratio $\Phi = (1+\sqrt{5})/2$ can be illustrated by tiling either squares or golden rectangles with squares, rectangles, gnomons, or other shapes formed from rectangles. This visually-pleasing approach complements an early paper, "Fibonacci Numbers and Geometry," by Brother Alfred Brousseau [1].

The basic golden rectangle, with ratio length to width Φ, is the basis for all figures that follow. In Figure 1, the length is 1 and the width is $1/\Phi$.

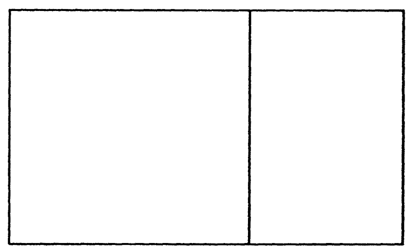


FIGURE 1: The Golden Rectangle

Divide the sides of a square and a golden rectangle in powers of $1/\Phi$ to form the templates of Figure 2.

In Figure 3 a square of side 1 tiled with golden rectangles shows that

$$1/\Phi + 1/\Phi^3 + 1/\Phi^5 + \cdots + 1/\Phi^{2n-1} + \cdots = 1$$

while a golden rectangle of length 1 tiled with squares (Figure 4) shows that

$$1/\Phi^2 + 1/\Phi^4 + 1/\Phi^6 + \cdots + 1/\Phi^{2n} + \cdots = 1/\Phi.$$

Divide a square of side Φ into powers of $1/\Phi$ and tile the rectangles that lie on falling diagonals to form Figure 5. Then each successive diagonal has n rectangles each of area $1/\Phi^{n+1}$, so that

$$1/\Phi^2 + 2/\Phi^3 + 3/\Phi^4 + \cdots + n/\Phi^{n+1} + \cdots = \Phi^2.$$

Also, the length of each side is $1/\Phi + 1/\Phi^2 + 1/\Phi^3 + \cdots + 1/\Phi^n + \cdots = \Phi$.

In Figure 6 we again divide a square of side Φ into powers of $1/\Phi$ and tile with L-shaped tiles, each formed from two rectangles having area $1/\Phi^{2n-1}$ There are F_n L-shaped tiles, each of area $2/\Phi^{2n-1}$, so that

$$1/\Phi + 1/\Phi^3 + 2/\Phi^5 + \cdots + F_n/\Phi^{2n-1} + \cdots = \Phi^2/2,$$

where F_n is the n^{th} Fibonacci number.

Figure 7 uses gnomons as tiles, where the largest has area $1/\Phi$ and the n^{th} gnomon has area $1/\Phi^{2n-1}$, making a visualization of the formula

$$1/\Phi+1/\Phi^3+1/\Phi^5+\cdots+1/\Phi^{2n-1}+\cdots=1.$$

Figure 8 is similar to Figure 5, but the tiling distinguishes squares, rectangles of area $1/\Phi^{2n}$, and rectangles of area $1/\Phi^{2n+1}$. The $(2n-1)^{\text{st}}$ diagonal contains one square of area $1/\Phi^{2n}$ and $(2n-2)$ rectangles each of area $1/\Phi^{2n}$, while the $(2n)^{\text{th}}$ diagonal contains $2n$ rectangles each of area $1/\Phi^{2n+1}$. Figure 8 provides a visualization of the sums:

$$1/\Phi^2+1/\Phi^4+1/\Phi^6+\cdots+1/\Phi^{2n}+\cdots=1/\Phi;$$
$$1/\Phi^4+2/\Phi^6+3/\Phi^8+\cdots+n/\Phi^{2n+2}+\cdots=1/\Phi^2;$$
$$1/\Phi^3+2/\Phi^5+3/\Phi^7+\cdots+n/\Phi^{2n+1}+\cdots=1/\Phi.$$

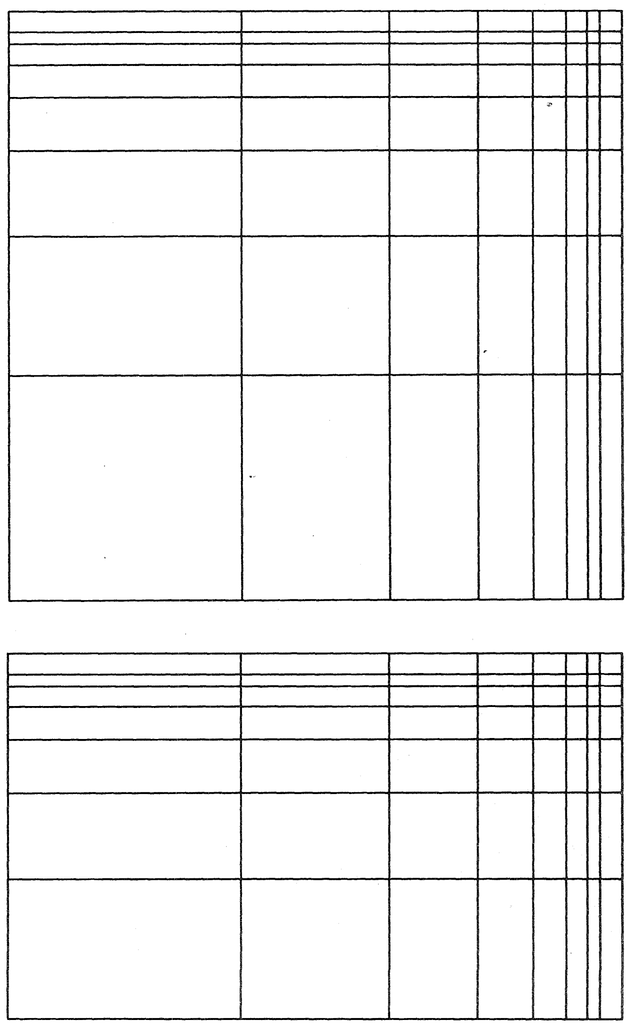


FIGURE 2: Templates for Visualizing Fibonacci and Golden Ratio Summation Formulas with Tiling Patterns

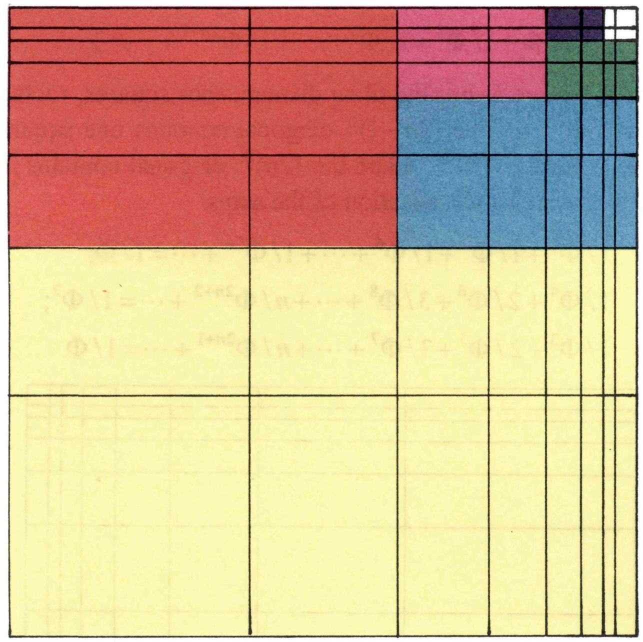


FIGURE 3: $1/\Phi + 1/\Phi^3 + 1/\Phi^5 + \cdots + 1/\Phi^{2n-1} + \cdots = 1$

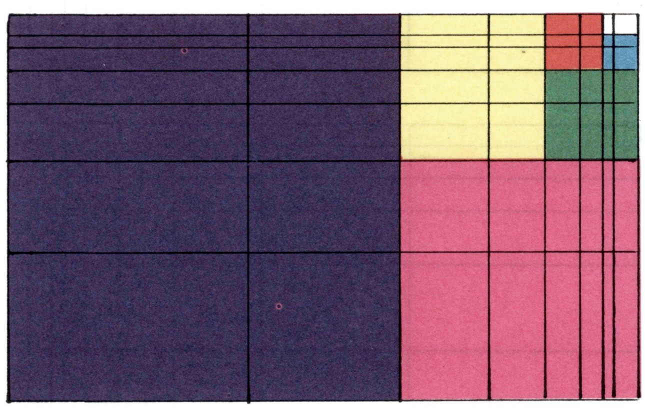


FIGURE 4: $1/\Phi^2 + 1/\Phi^4 + 1/\Phi^6 + \cdots + 1/\Phi^{2n} + \cdots = 1/\Phi$

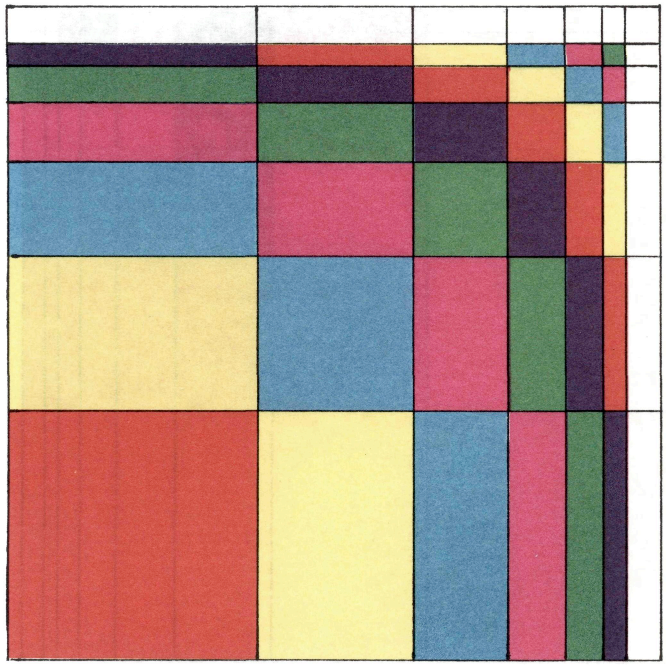


FIGURE 5: $1/\Phi^2 + 2/\Phi^3 + 3/\Phi^4 + \cdots + n/\Phi^{n+1} + \cdots = \Phi^2$
$1/\Phi + 1/\Phi^2 + 1/\Phi^3 + \cdots + 1/\Phi^n + \cdots = \Phi$

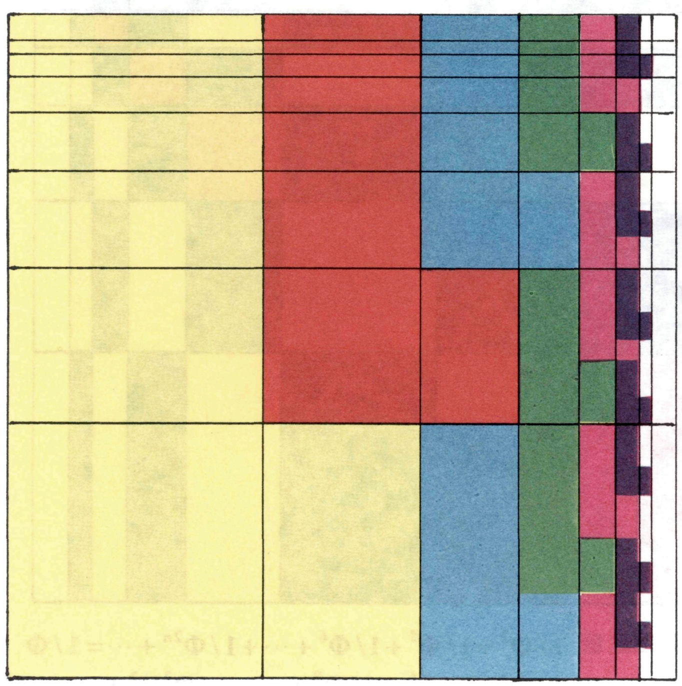


FIGURE 6: $1/\Phi + 1/\Phi^3 + 2/\Phi^5 + \cdots + F_n/\Phi^{2n-1} + \cdots = \Phi^2/2$

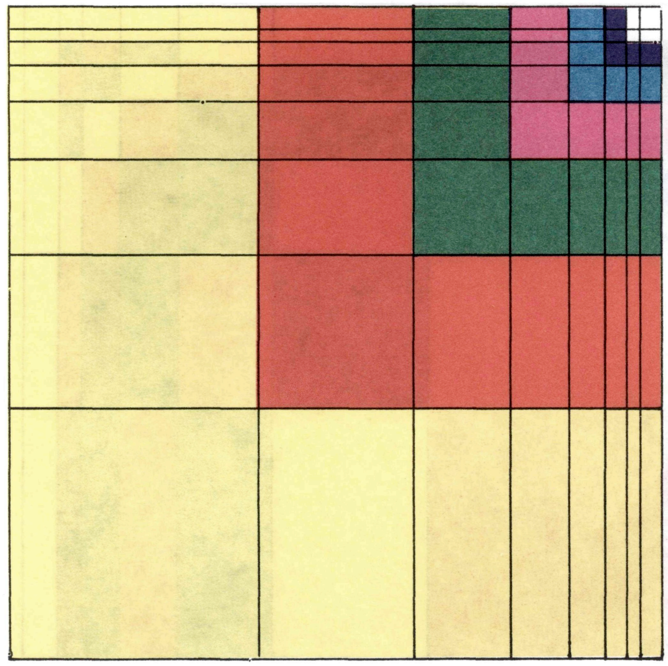


FIGURE 7: $1/\Phi + 1/\Phi^3 + 1/\Phi^5 + \cdots + 1/\Phi^{2n-1} + \cdots = 1$

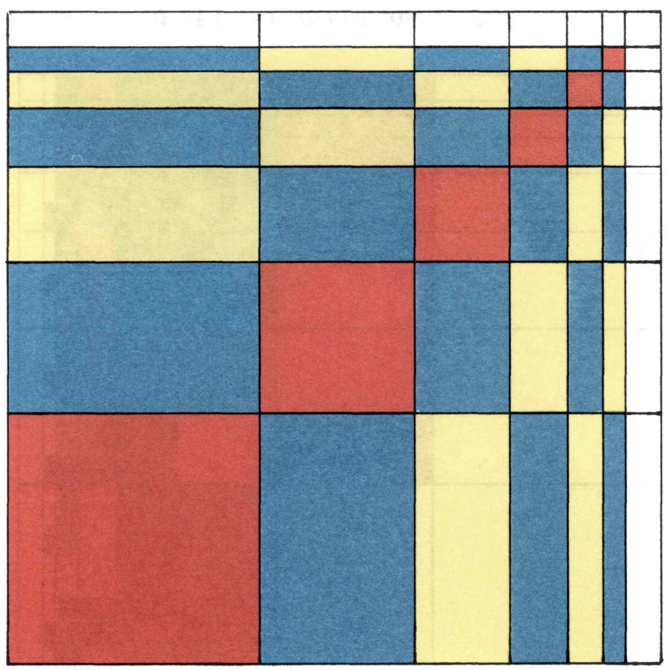


FIGURE 8: $1/\Phi^2 + 1/\Phi^4 + 1/\Phi^6 + \cdots + 1/\Phi^{2n} + \cdots = 1/\Phi$

$1/\Phi^4 + 2/\Phi^6 + 3/\Phi^8 + \cdots + n/\Phi^{2n+2} + \cdots = 1/\Phi^2$

$1/\Phi^3 + 2/\Phi^5 + 3/\Phi^7 + \cdots + n/\Phi^{2n+1} + \cdots = 1/\Phi$

REFERENCES

1. Brother Alfred Brousseau. "Fibonacci Numbers and Geometry." *The Fibonacci Quarterly* **10.3** (1972):303-18.
2. Marjorie Bicknell & Verner E. Hoggatt, Jr. "Golden Triangles, Rectangles, and Cuboids." *The Fibonacci Quarterly* **7.1** (1969):73-91.
3. Verner E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*, Chs.3 and 4. Boston: Houghton-Mifflin, 1969; rpt. Santa Clara, Calif.: The Fibonacci Association, 1980.

AMS Classification Numbers: 51M04, 11B39

❖❖❖

Announcement

SEVENTH INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS

July 14-July 19, 1996

INSTITUT FÜR MATHEMATIK
TECHNISCHE UNIVERSITÄT GRAZ
STEYRERGASSE 30
A-8010 GRAZ, AUSTRIA

LOCAL COMMITTEE

Robert Tichy, Chairman
Helmut Prodinger, Co-chairman
Peter Grabner
Peter Kirschenhofer

INTERNATIONAL COMMITTEE

A. F. Horadam (Australia), Co-chair
A. N. Philippou (Cyprus), Co-chair
G. E. Bergum (U.S.A.)
P. Filipponi (Italy)
H. Harborth (Germany)
Y. Horibe (Japan)
M. Johnson (U.S.A.)
P. Kiss (Hungary)
G. M. Phillips (Scotland)
J. Turner (New Zealand)
M. E. Waddill (U.S.A.)

LOCAL INFORMATION

For information on local housing, food, tours, etc., please contact:

PROFESSOR DR. ROBERT F. TICHY
INSTITUT FÜR MATHEMATIK
TECHNISCHE UNIVERSITÄT GRAZ
STEYRERGASSE 30
A-8010 GRAZ, AUSTRIA

Call for Papers

The SEVENTH INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS will take place at Technische Universität Graz from July 14 to July 19, 1996. This conference will be sponsored jointly by the Fibonacci Association and Technische Universität Graz.

Papers on all branches of mathematics and science related to the Fibonacci numbers as well as recurrences and their generalizations are welcome. 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
COMPUTER SCIENCE DEPARTMENT
BOX 2201
SOUTH DAKOTA STATE UNIVERSITY
BROOKINGS, SD 57007-1596

or

PROFESSOR F. T. HOWARD
DEPARTMENT OF MATH. & COMP. SCI.
BOX 7388 REYNOLDA STATION
WAKE FOREST UNIVERSITY
WINSTON-SALEM, NC 27109

PROOF OF A RESULT BY JARDEN BY GENERALIZING A PROOF BY CARLITZ

Curtis Cooper and Robert E. Kennedy
Department of Mathematics, Central Missouri State University, Warrensburg, MO 64093
(*Submitted November 1993*)

1. INTRODUCTION

Let $u_0 = 0, u_1 = 1$, and $u_n = au_{n-1} + bu_{n-2}$ for any positive integer $n \geq 2$. Also, for any nonnegative integer *m*, define

$$\binom{m}{j}_u = \begin{cases} 1, & \text{if } j = 0, \\ \frac{u_m \cdots u_{m-j+1}}{u_j \cdots u_1}, & \text{if } j = 1, \ldots, m. \end{cases}$$

In [1] Jarden showed that, for any positive integer *k*,

$$\sum_{i=0}^{k+1} (-1)^{i(i+1)/2} b^{(i-1)i/2} \binom{k+1}{i}_u u_{n-i}^k = 0.$$

In this paper we will prove Jarden's result by generalizing a proof by Carlitz [2]. In addition, we will present a new like-power recurrence relation identity. Detailed proofs of the lemmas and the theorem will be supplied at the end of the paper.

2. SEQUENTIAL RESULTS

Let

$$\alpha, \beta = \frac{a \pm \sqrt{a^2 + 4b}}{2}.$$

Lemma 2.1: Let *n* be a nonnegative integer. Then

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Lemma 2.2: Let $n \geq -1$ be an integer. Then

$$u_{n+1} = \sum_r \binom{r}{n-r} a^{2r-n} b^{n-r}.$$

Lemma 2.3: Let $n \geq 2$ be an integer. Then

(a) $u_n + bu_{n-2} = \alpha^{n-1} + \beta^{n-1}$.

(b) $bu_n u_{n-2} - bu_{n-1}^2 = \alpha^{n-1}\beta^{n-1}$.

Lemma 2.4: Let *k* be a positive integer and $0 \leq r \leq n$ be integers. Then

$$(u_k x + bu_{k-1})^r (u_{k+1} x + bu_k)^{n-r} = \sum_{r_1, \ldots, r_k} \binom{n-r}{r_1}\binom{n-r_1}{r_2} \cdots \binom{n-r_{k-1}}{r_k} a^{kn-r-2r_1-\cdots-2r_{k-1}-r_k} b^{r_1+\cdots+r_k} x^{n-r_k}.$$

3. MATRIX RESULTS

Let

$$A_{n+1}=\left[\binom{r}{n-c}a^{r+c-n}b^{n-c}\right],\quad 0\le r,c\le n,$$

be a matrix of order $n+1$. For example, for $n=3$,

$$A_4=\begin{bmatrix}0&0&0&1\\0&0&b&a\\0&b^2&2ab&a^2\\b^3&3ab^2&3a^2b&a^3\end{bmatrix}.$$

Lemma 3.1: $\operatorname{tr}(A_{n+1}^k)=\frac{u_{kn+k}}{u_k}$ for any positive integer k.

It is worth noting that the case $k=1$ is exactly Lemma 2.2, so that Lemma 3.1 is in some sense a generalization of Lemma 2.2.

Lemma 3.2: The eigenvalues of A_{n+1} are $\alpha^n,\alpha^{n-1}\beta,\dots,\alpha\beta^{n-1},\beta^n$.

Lemma 3.3:

$$\prod_{j=0}^{n}(x-\alpha^j\beta^{n-j})=\sum_{i=0}^{n+1}(-1)^{i(i+1)/2}b^{(i-1)i/2}\binom{n+1}{i}_u x^{n+1-i}.$$

The next lemma is similar to a result of Hoggatt and Bicknell [3].

Lemma 3.4: $(A_{k+1}^n)_{k,i}=\binom{k}{i}u_{n+1}^i(bu_n)^{k-i}$.

4. JARDEN'S RESULT

Theorem 4.1:

$$\sum_{i=0}^{k+1}(-1)^{i(i+1)/2}b^{(i-1)i/2}\binom{k+1}{i}_u u_{n-i}^k=0.$$

5. MORE RESULTS AND OPEN QUESTIONS

More identities, like the one just derived, need to be studied. For example, it can be shown, using the computer algebra system DERIVE that, if x_0, x_1, and x_2 are arbitrary and

$$x_n=ax_{n-1}+bx_{n-2}+cx_{n-3},$$

then

$$\begin{aligned}x_n^2&=(a^2+b)x_{n-1}^2+(a^2b+b^2+ac)x_{n-2}^2+(a^3c+4abc-b^3+2c^2)x_{n-3}^2\\&\quad+(-ab^2c+a^2c^2-bc^2)x_{n-4}^2+(b^2c^2-ac^3)x_{n-5}^2-c^4x_{n-6}^2.\end{aligned}$$

Is there a similar formula for third powers? Also, what about formulas for

$$x_n=ax_{n-1}+bx_{n-2}+cx_{n-3}+dx_{n-4}\ ?$$

6. PROOFS

Proof of Lemma 2.1: Let

$$G(z) = u_0 + u_1 z + u_2 z^2 + \cdots.$$

Then

$$azG(z) = au_0 z + au_1 z^2 + \cdots \quad \text{and} \quad bz^2 G(z) = bu_0 z^2 + \cdots.$$

Subtracting the last two equations from the first and using the definition of u_n,

$$(1 - az - bz^2)G(z) = z$$

so

$$G(z) = \frac{z}{1 - az - bz^2} = \frac{1}{\alpha - \beta}\left(\frac{1}{1 - \alpha z} - \frac{1}{1 - \beta z}\right).$$

Thus,

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Proof of Lemma 2.2: By induction on n. First, the result is true for $n = -1$ and $n = 0$. Now assume that $n \geq 0$ and that the result is true for n and $n-1$. Then

$$\begin{aligned}
u_{n+1} &= au_n + bu_{n-1} \\
&= a\sum_r \binom{r}{n-1-r} a^{2r-n+1} b^{n-1-r} + b\sum_r \binom{r}{n-2-r} a^{2r-n+2} b^{n-2-r} \\
&= \sum_r \left[\binom{r}{n-1-r} + \binom{r}{n-2-r}\right] a^{2r-n+2} b^{n-1-r} \\
&= \sum_r \binom{r+1}{n-1-r} a^{2r-n+2} b^{n-1-r} = \sum_r \binom{r}{n-r} a^{2r-n} b^{n-r}.
\end{aligned}$$

Proof of Lemma 2.3:

(a) By the definition of u_n and Lemma 2.1,

$$\begin{aligned}
u_n + bu_{n-2} &= u_n + u_n - au_{n-1} \\
&= 2\frac{\alpha^n - \beta^n}{\alpha - \beta} - (\alpha + \beta)\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} \\
&= \frac{2\alpha^n - 2\beta^n - \alpha^n + \alpha\beta^{n-1} - \beta\alpha^{n-1} + \beta^n}{\alpha - \beta} \\
&= \frac{\alpha^n - \beta^n + \alpha\beta^{n-1} - \beta\alpha^{n-1}}{\alpha - \beta} = \frac{\alpha(\alpha^{n-1} + \beta^{n-1}) - \beta(\alpha^{n-1} + \beta^{n-1})}{\alpha - \beta} \\
&= \frac{(\alpha - \beta)(\alpha^{n-1} + \beta^{n-1})}{\alpha - \beta} = \alpha^{n-1} + \beta^{n-1}.
\end{aligned}$$

(b) By the definition of u_n and Lemma 2.1,

$$\begin{aligned}
bu_nu_{n-2}-bu_{n-1}^2 &= u_n(u_n-au_{n-1})-bu_{n-1}^2 = u_n^2-au_nu_{n-1}-bu_{n-1}^2\\
&= u_n^2-u_{n-1}(au_n+bu_{n-1}) = u_n^2-u_{n-1}u_{n+1}\\
&= \left(\frac{\alpha^n-\beta^n}{\alpha-\beta}\right)^2-\frac{\alpha^{n-1}-\beta^{n-1}}{\alpha-\beta}\cdot\frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}\\
&= \frac{1}{(\alpha-\beta)^2}(\alpha^{2n}-2\alpha^n\beta^n+\beta^{2n}-\alpha^{2n}-\beta^{2n}+\alpha^{n+1}\beta^{n-1}+\alpha^{n-1}\beta^{n+1})\\
&= \frac{1}{(\alpha-\beta)^2}(\alpha^{n+1}\beta^{n-1}-2\alpha^n\beta^n+\alpha^{n-1}\beta^{n+1})\\
&= \frac{\alpha^{n-1}\beta^{n-1}}{(\alpha-\beta)^2}(\alpha^2-2\alpha\beta+\beta^2) = \alpha^{n-1}\beta^{n-1}.
\end{aligned}$$

Proof of Lemma 2.4: By induction on k. The result is true for $k=1$, since

$$x^r(ax+b)^{n-r} = \sum_s \binom{n-r}{s} a^{n-r-s}b^s x^{n-s}.$$

Now assume the result is true for some positive integer k. In this result, substitute $a+bx^{-1}$ for x and multiply by x^n. The left side of this equation is

$$(au_kx+bu_{k-1}x+bu_k)^r(au_{k+1}x+bu_kx+bu_{k+1})^{n-r}$$

which is equal to

$$(u_{k+1}x+bu_k)^r(u_{k+2}x+bu_{k+1})^{n-r}.$$

Expanding the right side of this equation and simplifying, we obtain

$$\sum_{r_1,\dots,r_{k+1}} \binom{n-r}{r_1}\binom{n-r_1}{r_2}\cdots\binom{n-r_k}{r_{k+1}} a^{(k+1)n-r-2r_1-\cdots-2r_k-r_{k+1}} b^{r_1+\cdots+r_{k+1}} x^{n-r_{k+1}}.$$

Therefore, the result is proved.

Proof of Lemma 3.1: We first recall Lemma 2.4, that is, for any positive integer k,

$$(u_kx+bu_{k-1})^r(u_{k+1}x+bu_k)^{n-r} = \sum_{r_1,\dots,r_k}\binom{n-r}{r_1}\binom{n-r_1}{r_2}\cdots\binom{n-r_{k-1}}{r_k} a^{kn-r-2r_1-\cdots-2r_{k-1}-r_k} b^{r_1+\cdots+r_k} x^{n-r_k}.$$

Multiplying both sides of this equation by x^r and summing over r, we have

$$\begin{aligned}
&\sum_{r=0}^{n} x^r(u_kx+bu_{k-1})^r(u_{k+1}x+bu_k)^{n-r}\\
&= \sum_{r,r_1,\dots,r_k}\binom{n-r}{r_1}\binom{n-r_1}{r_2}\cdots\binom{n-r_{k-1}}{r_k} a^{kn-r-2r_1-\cdots-2r_{k-1}-r_k} b^{r_1+\cdots+r_k} x^{n+r-r_k}.
\end{aligned}$$

The coefficient of x^n on the right side of this equation is $\operatorname{tr}(A_{n+1}^k)$. The coefficient of x^n on the left side of this equation is

$$\sum_{r+s+t=n}\binom{r}{s}\binom{n-r}{t}u_k^s(bu_{k-1})^{r-s}u_{k+1}^t(bu_k)^{n-r-t}$$
$$=\sum_{r+s\le n}\binom{r}{s}\binom{n-r}{s}(bu_{k-1})^{r-s}u_k^s u_{k+1}^{n-r-s}(bu_k)^s.$$

Let v_n be this last term. Thus,

$$\sum_{n=0}^{\infty}v_nx^n=\sum_{r,s=0}^{\infty}\binom{r}{s}b^ru_{k-1}^{r-s}u_k^{2s}x^{r+s}\sum_{n=r+s}^{\infty}\binom{n-r}{s}(u_{k+1}x)^{n-r-s}$$
$$=\sum_{r,s=0}^{\infty}\binom{r}{s}b^ru_{k-1}^{r-s}u_k^{2s}x^{r+s}(1-u_{k+1}x)^{-s-1}$$
$$=\sum_{s=0}^{\infty}b^su_k^{2s}x^{2s}(1-u_{k+1}x)^{-s-1}\sum_{r\ge s}\binom{r}{s}(bu_{k-1}x)^{r-s}$$
$$=\sum_{s=0}^{\infty}b^su_k^{2s}x^{2s}(1-u_{k+1}x)^{-s-1}(1-bu_{k-1}x)^{-s-1}$$
$$=\frac{1}{(1-u_{k+1}x)(1-bu_{k-1}x)}\;\frac{1}{1-\frac{bu_k^2x^2}{(1-u_{k+1}x)(1-bu_{k-1}x)}}$$
$$=\frac{1}{(1-u_{k+1}x)(1-bu_{k-1}x)-bu_k^2x^2}$$
$$=\frac{1}{1-(u_{k+1}+bu_{k-1})x+(bu_{k+1}u_{k-1}-bu_k^2)x^2}.$$

Next, by Lemma 2.3, the last expression is equal to

$$\frac{1}{1-(\alpha^k+\beta^k)x+\alpha^k\beta^kx^2}=\frac{1}{\alpha^k-\beta^k}\left(\frac{\alpha^k}{1-\alpha^kx}-\frac{\beta^k}{1-\beta^kx}\right).$$

Thus, $v_n=\frac{u_{kn+k}}{u_k}$. Therefore,

$$\operatorname{tr}(A_{n+1}^k)=\frac{u_{kn+k}}{u_k}.$$

Proof of Lemma 3.2: Let $f_{n+1}(x)=\det(xI-A_{n+1})$. If the eigenvalues of A_{n+1} are $\lambda_0, \lambda_1, \ldots, \lambda_n$, then by Lemmas 3.1 and 2.1,

$$\frac{f'_{n+1}(x)}{f_{n+1}(x)}=\sum_{j=0}^{n}\frac{1}{x-\lambda_j}=\sum_{k=0}^{\infty}x^{-k-1}\sum_{j=0}^{n}\lambda_j^k$$
$$=\sum_{k=0}^{\infty}x^{-k-1}\operatorname{tr}(A_{n+1}^k)=\sum_{k=0}^{\infty}x^{-k-1}\frac{\alpha^{nk+k}-\beta^{nk+k}}{\alpha^k-\beta^k}$$
$$=\sum_{k=0}^{\infty}x^{-k-1}\sum_{j=0}^{n}\alpha^{jk}\beta^{(n-j)k}=\sum_{j=0}^{n}\frac{1}{x-\alpha^j\beta^{n-j}}.$$

Thus,

$$f_{n+1}(x)=\prod_{j=0}^{n}(x-\alpha^j\beta^{n-j}),$$

so the eigenvalues of A_{n+1} are $\alpha^n, \alpha^{n-1}\beta, \ldots, \alpha\beta^{n-1}, \beta^n$.

Proof of Lemma 3.3: To begin the proof of Lemma 3.3, we need the identity

$$\prod_{j=0}^{n-1}(1-q^jx)=\sum_{i=0}^{n}(-1)^i q^{(i-1)i/2}\begin{bmatrix} n \\ i \end{bmatrix} x^i,$$

where

$$\begin{bmatrix} n \\ i \end{bmatrix}=\frac{(1-q^n)\cdots(1-q^{n-i+1})}{(1-q^i)\cdots(1-q)}. \tag{1}$$

Replacing q in (1) by β/α and using Lemma 2.1, we find that $\left[\begin{smallmatrix} n \\ i \end{smallmatrix}\right]$ is

$$\alpha^{i^2-ni}\binom{n}{i}_u.$$

Thus, (1) becomes

$$\prod_{j=0}^{n-1}(1-\alpha^{-j}\beta^jx)=\sum_{i=0}^{n}(-1)^i\alpha^{i(i+1)/2-ni}\beta^{(i-1)i/2}\binom{n}{i}_u x^i.$$

Substituting $\alpha^{n-1}x$ for x and using the fact that $\alpha\beta=-b$, we have

$$\begin{aligned}\prod_{j=0}^{n-1}(1-\alpha^{n-j-1}\beta^jx)&=\sum_{i=0}^{n}(-1)^i(\alpha\beta)^{(i-1)i/2}\binom{n}{i}_u x^i\\ &=\sum_{i=0}^{n}(-1)^{i(i+1)/2}b^{(i-1)i/2}\binom{n}{i}_u x^i.\end{aligned}$$

Replacing x by x^{-1} gives

$$\prod_{j=0}^{n-1}(x-\alpha^{n-j-1}\beta^j)=\sum_{i=0}^{n}(-1)^{i(i+1)/2}b^{(i-1)i/2}\binom{n}{i}_u x^{n-i},$$

which is what we wanted to prove.

Proof of Lemma 3.4: Let k be a fixed nonnegative integer. We will prove the result by induction on n. The above equality is true for $n=0$. Now assume the result is true for some $n\geq 0$. Then, since $A_{k+1}^{n+1}=A_{k+1}^n\cdot A_{k+1}$,

$$(A_{k+1}^{n+1})_{k,i}=\sum_{j=0}^{k}(A_{k+1}^n)_{k,j}(A_{k+1})_{j,i}=\sum_{j=0}^{k}\binom{k}{j}u_{n+1}^j(bu_n)^{k-j}\binom{j}{k-i}a^{j+i-k}b^{k-i}.$$

To continue the equalities, we use the identity

$$\binom{r}{m}\binom{m}{k}=\binom{r}{k}\binom{r-k}{m-k}$$

to obtain

$$\sum_{j=0}^{k}\binom{k}{k-i}\binom{i}{i+j-k}(bu_{n+1})^{k-i}(au_{n+1})^{i+j-k}(bu_n)^{k-j}$$
$$=\binom{k}{i}(bu_{n+1})^{k-i}\sum_{j=0}^{k}\binom{i}{i+j-k}(au_{n+1})^{i+j-k}(bu_n)^{k-j}$$
$$=\binom{k}{i}(bu_{n+1})^{k-i}\sum_{m=0}^{i}\binom{i}{m}(au_{n+1})^{m}(bu_n)^{i-m}$$
$$=\binom{k}{i}(bu_{n+1})^{k-i}(au_{n+1}+bu_n)^{i}=\binom{k}{i}u_{n+2}^{i}(bu_{n+1})^{k-i}.$$

Thus, the result is true by induction on n.

Proof of Theorem 4.1 By Lemma 3.3, the characteristic polynomial of A_{k+1} is

$$\sum_{i=0}^{k+1}(-1)^{i(i+1)/2}b^{(i-1)i/2}\binom{k+1}{i}_u x^{k+1-i}.$$

But, by the Cayley-Hamilton theorem, every matrix satisfies its characteristic polynomial. Thus, for $n-1\geq k+1$,

$$\sum_{i=0}^{k+1}(-1)^{i(i+1)/2}b^{(i-1)i/2}\binom{k+1}{i}_u A_{k+1}^{n-1-i}=O, \tag{2}$$

where O denotes the $(k+1)\times(k+1)$ zero matrix. Now, taking the result of Lemma 3.4 (with $i=k$ and $n=n-1-i$) and substituting this result into (2), we obtain Jarden's result.

REFERENCES

1. D. Jarden. *Recurring Sequences*. 2nd ed. Jerusalem: Riveon Lematika, 1966.
2. L. Carlitz. "The Characteristic Polynomial of a Certain Matrix of Binomial Coefficients." *The Fibonacci Quarterly* **3.1** (1965):81-89.
3. V. Hoggatt, Jr., & M. Bicknell. "Fourth Power Fibonacci Identities from Pascal's Triangle." *The Fibonacci Quarterly* **2.3** (1964):261-66.

AMS Classification Numbers: 11B37, 11B65

❖❖❖

A NOTE REGARDING CONTINUED FRACTIONS

Neville Robbins
Mathematics Department, San Francisco State University, San Francisco, CA 94132
(Submitted November 1993)

In this note we develop some properties of purely periodic infinite continued fractions. The parameters k, n, a_k, a_n, p_n, and q_n will denote positive integers, and $q_0 = 0$. Let

$$y_n = [a_1, a_2, a_3, \ldots, a_n] = p_n / q_n,$$

that is, y_n is the finite continued fraction whose partial quotients are the a_k. (The initial term of y_n is denoted a_1, not a_0.) Let

$$x_n = [\overline{a_1, a_2, a_3, \ldots, a_n}],$$

that is, x_n is the corresponding purely periodic infinite continued fraction.

Theorem 1: Let n, x_n, y_n, p_n, and q_n be as above. Then

$$x_n = \left(p_n - q_{n-1} + \sqrt{(p_n + q_{n-1})^2 - 4(-1)^n}\right) / 2q_n.$$

Proof: This follows from elementary considerations (see Hardy & Wright [1], Ch. 10). □

Remark: S. Rabinowitz [3] has asked for a formula for $[\overline{1, 2, 3, \ldots, n}]$.

Theorem 2: Let n, x_n, y_n, p_n, and q_n be as above. Let

$$\lim_{n\to\infty} y_n = A = [a_1, a_2, a_3, \ldots].$$

Then also

$$\lim_{n\to\infty} x_n = A.$$

Proof: It suffices to show that $y_n - x_n$ tends to 0 as n tends to infinity. By Theorem 1, we have

$$y_n - x_n = \frac{1}{2q_n(p_n + q_{n-1})}\left(1 - \left(1 - \frac{4(-1)^n}{(p_n + q_{n-1})^2}\right)^{1/2}\right).$$

As n tends to infinity, the factor $\frac{1}{2q_n}(p_n + q_{n-1})$ is bounded from above, since p_n / q_n tends to A and $q_{n-1} / q_n < 1$. On the other hand, p_n and q_{n-1} tend to infinity with n, so that

$$1 - \left(1 - \frac{4(-1)^n}{(p_n + q_{n-1})^2}\right)^{1/2} \quad \text{tends to } 0.$$

Thus, $y_n - x_n$ tends to 0 as n tends to infinity. □

Corollary: Let $I_k(t)$ be the modified Bessel function of the first kind of order k, that is,

$$I_k(t) = \sum_{j=0}^{\infty} (\tfrac{1}{2}t)^{2j+k} / \Gamma(j+1)\Gamma(j+k+1).$$

Let $w_n = [\overline{1, 2, 3, \ldots, n}]$. Then

$$\lim_{n\to\infty} w_n = I_0(2) / I_1(2) = 1.433127427.$$

Proof: This follows from hypothesis, Theorem 2, and ([2], Th. 1). □

Theorem 3: Let x_n, y_n, and A be as in the hypothesis of Theorem 2. Then, for all n, we have $x_{2n} < A < x_{2n-1}$.

Proof: Applying Theorem 1, we have $x_{2n} < p_{2n} / q_{2n}$, that is, $x_{2n} < y_{2n}$. Similarly, $x_{2n-1} > p_{2n-1} / q_{2n-1}$, that is, $x_{2n-1} > y_{2n-1}$. But $y_{2n} < A < y_{2n-1}$ for all n, so $x_{2n} < A < x_{2n-1}$ for all n. □

REFERENCES

1. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*. 6th ed. Oxford: Oxford University Press, 1972.
2. D. H. Lehmer. "Continued Fractions Containing Arithmetic Progressions." *Scripta Math.* **39** (1971):17-23.
3. S. Rabinowitz. Problem posed at the Fourth International Conference on Fibonacci Numbers and Their Applications, Wake Forest University, 1990.

❖❖❖

DUCCI-SEQUENCES AND PASCAL'S TRIANGLE

Herbert Glaser

Mathematisches Institut (Didaktik), Universität Würzburg, Germany

Gerd Schöffl

Korngasse 1, 97070 Würzburg, Germany

(*Submitted November 1993*)

INTRODUCTION

The so-called *Ducci-sequences* (or *n-number-game*) have recently been studied by several authors in this review (see [1] , [5], [6], [12], [17], and others). A Ducci-sequence is a sequence of n-tuples $A_i = (a_1, a_2, \ldots, a_n)$; the first n-tuple A_0 is any given n-tuple with nonnegative integer entries, $A_{i+1} := \mathcal{T}A_i$, where $\mathcal{T}$ is defined as follows:

$$\mathcal{T}A_i := (|a_1 - a_2|, |a_2 - a_3|, \ldots, |a_n - a_1|).$$

The n-tuple A_{i+1} is called the (direct) *successor* of A_i, whereas A_i is the *predecessor* of A_{i+1}. As the maximum entry of the n-tuples cannot increase under the application of $\mathcal{T}$ and therefore the number of successors of any A_0 is bounded, the sequence always leads to a cycle of repeating n-tuples or to the n-tuple $(0, \ldots, 0)$. If an n-tuple A_0 gives rise to the latter, it is usually called *vanishing*.

First, it will be shown in this article that the Ducci-sequences are closely related to *Pascal's triangle* and many properties of their cyclic structures can be found and proved considering Pascal's triangle modulo 2. In the second part we will examine whether, for a given $n \in \mathbb{N}$ there is such an M that $2^M \equiv -1 \bmod n$, which is crucial for some properties of the Ducci-sequences.

We would like to thank the referee for a number of valuable suggestions.

SOME BASIC PROPERTIES AND DEFINITIONS

It is a well-known fact that every n-tuple with integer entries vanishes if and only if n is a power of 2 (e.g., [4]). On the other hand, the n-tuples in the cycles of the Ducci-sequences are constant multiples of binary n-tuples ([6], [3]). As $\mathcal{T}(\lambda A) = \lambda \mathcal{T} A$ for every $\lambda \in \mathbb{N}_0$, we can limit any investigation of cycles to n-tuples over $\mathbb{Z}_2$. Since $|a-b| \equiv (a+b) \bmod 2$ for all integers a and b, we can use the linear operator $\mathcal{D}$ instead of $\mathcal{T}$, where $\mathcal{D}A := (a_1 + a_2, a_2 + a_3, \ldots, a_n + a_1) \bmod 2$ and A is a binary n-tuple. The operator $\mathcal{D}$ can be written as the sum of two linear operators over $\mathbb{Z}_2$: $\mathcal{D} = \mathcal{I} + \mathcal{H}$, where $\mathcal{I}$ is the identity and $\mathcal{H}A := (a_2, \ldots, a_n, a_1)$. Obviously, we get $\mathcal{H}^n = \mathcal{I}$ and $\mathcal{H}^{-1} = \mathcal{H}^{n-1}$, where $\mathcal{H}^{-1}$ is the inverse operator of $\mathcal{H}$.

We denote the k^{th} successor $\mathcal{D}^k A_0$ of a given binary n-tuple A_0 as A_k. If it is necessary to describe the entries of a certain successor A_k, we will use two indices and write $A_k = (a_{k,1}, \ldots, a_{k,n})$. Then we get:

$$A_{k+1,i} = a_{k,i} + a_{k,i+1}.$$

The subscripts denoting the place in the n-tuple are always reduced modulo n, using n instead of 0.

Ehrlich proved in [6] that the n-tuple $A_0 = (0, \dots, 0, 1)$ (and every cyclic permutation of A_0) produces a cycle of maximum length. The length of all other cycles of n-tuples of a given n divide this maximum. The sequence $\{A_k\}$ is called the *basic-Ducci-sequence* (*of n-tuples*) and the length of its periodic cycle is denoted as $\mathcal{P}(n)$. For every odd n, the first n-tuple in a cycle is $\mathcal{D}A_0 = A_1 = (0, \dots, 0, 1, 1)$. Further, Ehrlich stated the following theorems:

- If $2^m \equiv 1 \bmod n$, then $\mathcal{P}(n)$ divides $2^m - 1$. (1)
- If $2^M \equiv -1 \bmod n$, then $\mathcal{P}(n)$ divides $n(2^M - 1)$. (2)
- If n is not a power of 2, then n divides $\mathcal{P}(n)$. (3)
- If $n = 2^r \ell$, where ℓ is odd, then $\mathcal{P}(n) = 2^r \mathcal{P}(\ell)$. (4)

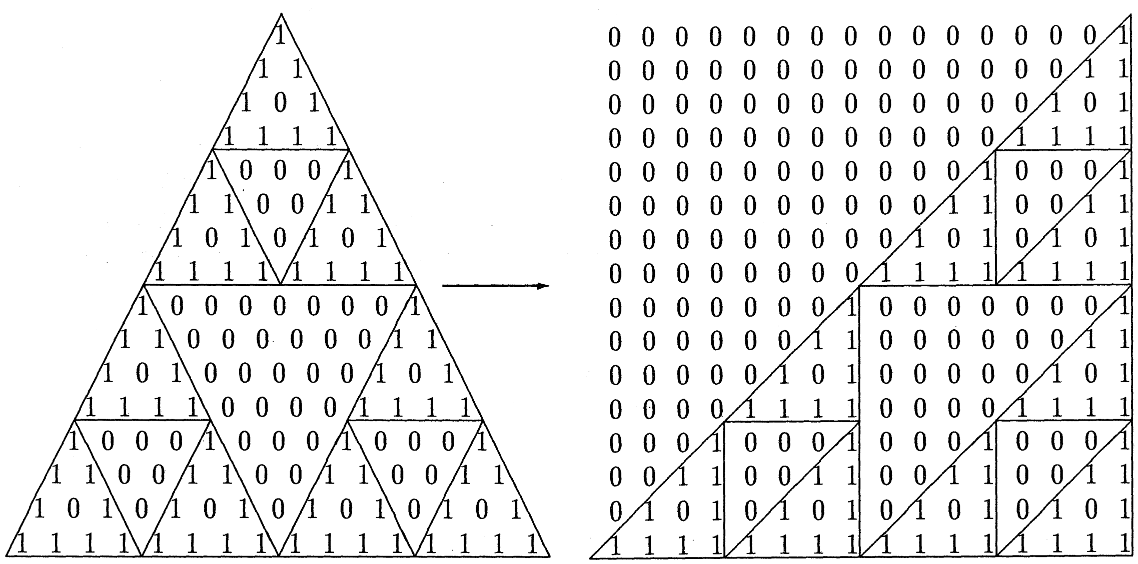
Before we take a closer look at the properties of Pascal's triangle, we will state a theorem that allows a new approach to our problem.

A NEW APPROACH TO AN OLD PROBLEM

In Pascal's triangle, we find the binomial coefficient $\binom{k}{i}$ of the i^{th} place in the k^{th} row. The 0^{th} row consists of a single one. When we place zeros left and right of the triangle, we can obtain any element by adding the two elements to the left and right above its place. This is easy to see, knowing the formula for adding the binomial coefficients:

$$\binom{k}{i} + \binom{k}{i+1} = \binom{k+1}{i+1}.$$

We will limit our investigation to $\mathbb{Z}_2$, and thus every binomial coefficient shall be considered modulo 2. Pascal's triangle modulo 2 with n rows (i.e., row 0 to row $n-1$) will be denoted as PT_n. The number of a chosen row shall be denoted as k. We fill up every k^{th} row of a PT_n with $n-k-1$ zeros on the left side. By shifting to the right and considering the rows as n-tuples, we obtain a square of n different n-tuples.



The i^{th} entry in the k^{th} row will be denoted as $a_{k,i}$. We obtain:

$$a_{k,i} = \begin{cases} 0 & : 1 \le i \le n-k-1, \\ \binom{k}{i-n+k} & : n-k \le i \le n. \end{cases}$$

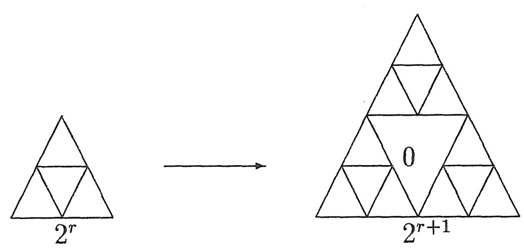
Adopting the above formula for the binomial coefficients, we get $a_{k+1,i} = a_{k,i} + a_{k,i+1}$:

- $1 \le i \le n-k-2 : a_{k+1,i} = 0 = a_{k,i} + a_{k,i+1}$.
- $i = n-k-1 : a_{k+1,i} = 1 = 0 + 1 = a_{k,i} + \binom{k+1}{0} = a_{k,i} + a_{k,i+1}$.
- $n-k \le i \le n : a_{k+1,i} = \binom{k+1}{i-n+k+1} = \binom{k}{i-n+k} + \binom{k}{i-n+k+1} = a_{k,i} + a_{k,i+1}$.

Considering that the n-tuple in the 0^{th} row is $(0, \dots, 0, 1) = A_0$, the first n-tuple of the *basic-Ducci-sequence*, we have shown

Theorem 1: The n rows in the modified Pascal triangle (as shown above) are the n-tuples A_0, A_1, ..., A_{n-1} of the *basic-Ducci-sequence*.

We will now take a closer look at Pascal's triangle. This triangle shows an interesting geometry which is closely related to that of the Sierpinski gasket (cf. [14]). Therefore, the PT_{2^r} for $r \in \mathbb{N}$ can be constructed recursively. For a given PT_{2^r}, $r \in \mathbb{N}$, we get $PT_{2^{r+1}}$ by placing two PT_{2^r}'s at the corners of the base of the first PT_{2^r} and filling up the empty triangle with zeros:



This construction can be proved using a lemma of Hinz ([8], p. 541).

Lemma 1: For $0 \le k, i < 2^r$, and $r \in \mathbb{N}_0$, it follows that

$$\binom{2^r + k}{i} \equiv \binom{k}{i} \mod 2.$$

In [8] we can find some additional facts that have been stated by Lucas [10] and Glaisher (reference can be found in Stolarsky [16]) and can be proved with the help of the above lemma ([8], p. 539):

- For $0 \le i \le k$, the binomial coefficients $\binom{k}{i}$ are all odd if and only if $k = 2^r - 1$ for some $r \in \mathbb{N}_0$. (5)
- For $0 < i < k$, the binomial coefficients $\binom{k}{i}$ are all even if and only if k is a power of 2 (the outer elements are 1). (6)
- Let $\beta(k)$ be the number of ones in the 2-adic expansion of $k \in \mathbb{N}_0$. Then the number of odd binomial coefficients $\binom{k}{i}$ for $0 \le i \le k$ is $2^{\beta(k)}$. (7)

The advantage of using PT_n for examining the Ducci-sequences is the fact that many properties of the cycles can easily be seen. Regarding the fractal geometry of the triangle, the results can be observed for small n and generalized for higher ones. For example, if we take a look at the PT_{2^r}, we see that the row $2^r - 1$ contains only ones. This leads us to an easy proof of the well-known fact that every 2^r-tuple with integer entries vanishes (see [4], [7], [3], et al.).

In the same way, we can prove all the following new results. As some of the proofs are quite long when using exclusively Pascal's triangle, we will adopt other techniques as well.

CYCLES OF SOME DUCCI-SEQUENCES

Following Ehrlich [6], we say n **is with a** -1 if $n \in \mathbb{N}$ is odd and there exists an $M \in \mathbb{N}$ with $2^M \equiv -1 \bmod n$; otherwise, we call n **without a** -1. We will now give a lower bound for $\mathcal{P}(n)$ for every n with a -1 [for an upper bound, see (2)]. First, we have to state the following lemma.

Lemma 2: Let n be with a -1 and $k \in \mathbb{N}, k \geq 1$. Then

$$\mathcal{D}^{k(2^M-1)+1} = \mathcal{H}^{-k}\mathcal{D}.$$

Proof: We proceed by induction using Ehrlich's Lemma 1 ([6], p. 302):

$$2^m \equiv t \bmod n \Rightarrow \mathcal{D}^{2^m} = \mathcal{I} + \mathcal{H}^t.$$

Let $k = 1$. Then we get

$$\mathcal{D}^{(2^m-1)+1} = \mathcal{D}^{2^M} = \mathcal{I} + \mathcal{H}^{-1} = \mathcal{H}^{-1}\mathcal{D}.$$

Assume now that the statement is true for $k \in \mathbb{N}$. It follows by computation that

$$\begin{aligned}\mathcal{D}^{(k+1)(2^M-1)+1} &= \mathcal{D}^{k(2^M-1)+1}\mathcal{D}^{2^M-1} = \mathcal{H}^{-k}\mathcal{D}\mathcal{D}^{2^M-1} \\ &= \mathcal{H}^{-k}\mathcal{D}^{2^M} \qquad = \mathcal{H}^{-k}\,\mathcal{H}^{-1}\,\mathcal{D} \\ &= \mathcal{H}^{-(k+1)}\mathcal{D}. \quad \square\end{aligned}$$

This lemma leads to

Theorem 2: For n with a -1, every cyclic permutation of $A_1 = (0, \ldots, 0, 1, 1)$ can be found in the *basic-Ducci-sequence*.

Proof: As n is odd, the n-tuple A_1 is the first n-tuple in the cycle of the *basic-Ducci-sequence* and $A_1 = \mathcal{D}(0, \ldots, 0, 1)$. Using Lemma 2 above, we obtain $\mathcal{D}^{k(2^M-1)+1}A_0 = \mathcal{H}^{-k}\mathcal{D}A_0$ and therefore $\mathcal{D}^{k(2^M-1)}A_1 = \mathcal{H}^{-k}A_1$ for every $k \in \mathbb{N}$. $\square$

Obviously this result implies that, for every n with a -1, the cyclic permutations of $(0, \ldots, 0, 1)$ give rise to the same cycle, and so there exists only one cycle of maximum length.

Theorem 3: For n with a -1, we get $\mathcal{P}(n) \geq n(n-2)$.

Proof: We have to determine the minimum number of applications of $\mathcal{D}$ for obtaining the first cyclic permutation of A_1 in the *basic-Ducci-cycle*. We use Pascal's triangle. A permutation of A_1 consists of two adjacent ones (where $a_{1,1}$ and $a_{1,n}$ are considered as being adjacent as well). Since the last and the first entry of Pascal's triangle are always ones, the number of ones in every row is at least 2. Thus, we can (possibly) find a cyclic permutation of A_1 for the first time when the first and the last entry of Pascal's triangle can be considered as adjacent ones in an n-tuple, which is to say that $a_{k,1} = 1$. Regarding the construction of n-tuples from Pascal's triangle, it follows that $k = n-1$, that means after $n-2$ applications of $\mathcal{D}$ on A_1. We use the same argument for the successors of the first permutation of A_1, and the proof is complete. □

This theorem gives rise to an important result.

Theorem 4: For n with a -1, it follows that

$$\mathcal{P}(n) = n(n-2) \Leftrightarrow n = 2^r + 1, \ r \in \mathbb{N}.$$

Proof:

"$\Leftarrow$" If $n = 2^r + 1$, then $2^r = n - 1 \equiv -1 \bmod n$ and from Theorem 3 we get $\mathcal{P}(n) \geq n(n-2)$. On the other hand, $\mathcal{P}(n)$ divides $n(2^r - 1) = n(n-2)$ [see property (2)], and so $n(2^r - 1) = n(n-2)$.

"$\Rightarrow$" As n is with a -1, the proof of Theorem 3 shows that $\mathcal{P}(n) = n(n-2)$ if and only if the n-tuple A_{n-1} is a permutation of A_1. According to properties (6) and (7), we obtain exactly two ones in a row of Pascal's triangle if and only if the number of the row is of the form $2^r + 1$. Considering that the ones are adjacent if and only if the n-tuple that is formed from the row $2^r + 1$ of Pascal's triangle is not filled up by zeros, i.e., $n = 2^r + 1$, we have shown our statement. □

Furthermore, we can extend Theorem 4 for every even n with $n = 2^r + 2^s$.

Theorem 5: If $n = 2^r + 2^s$ for $r > s \geq 0$, then $\mathcal{P}(n) = \frac{n(n-2^{s+1})}{2^s}$.

Proof: By using Theorem 4 and Ehrlich's formula (4), we obtain

$$\begin{aligned}\mathcal{P}(2^r + 2^s) &= 2^s \mathcal{P}(2^{r-s} + 1) \\ &= 2^s(2^{r-s} + 1)(2^{r-s} - 1) \\ &= \frac{(2^r + 2^s)(2^r - 2^s)}{2^s} \\ &= \frac{n(n - 2^{s+1})}{2^s}. \quad \square\end{aligned}$$

As mentioned above, Ehrlich [6] was able to describe the first n-tuple in the cycle of the *basic-Ducci-sequence* if n is odd. Nothing is yet known about the case in which n is even. We will be able to give a partial solution at this time.

Theorem 6: For $n = 2^r + 2^s$, $r > s \geq 0$, the n-tuple

$$A_{2^s} = (\underbrace{0, \ldots, 0}_{n-2^s-1}, \underbrace{1, 0, \ldots, 0, 1}_{2^s+1})$$

is the first n-tuple in the cycle of the *basic-Ducci-sequence.*

Proof:

1. The n-tuple is contained in the cycle.

Pascal's triangle PT_n shows us that

$$A_{2^r} = (\underbrace{0, \ldots, 0}_{2^2-1}, 1, \underbrace{0, \ldots, 0}_{2^r+1}, 1)$$

is a successor of

$$A_{2^s} = (\underbrace{0, \ldots, 0}_{2^{r-1}}, 1, \underbrace{0, \ldots, 0}_{2^s-1}, 1).$$

Obviously, A_{2^r} is a cyclic permutation of A_{2^s}: $A_{2^r} = \mathcal{H}^{-2^s} A_{2^s}$. On the other hand, we have $A_{2^r} = \mathcal{D}^{2^r-2^s} A_{2^s}$. We can conclude that

$$\mathcal{D}^{\frac{(2^r-2^s)n}{2^s}} A_{2^s} = \mathcal{H}^{-n} A_{2^s} = A_{2^s}$$

and, therefore, A_{2^s} is contained in the cycle. Keeping in mind that the first and the last entry of PT_n are always 1, and counting the consecutive zero-entries, we obtain that A_{2^r} is the only cyclic permutation of A_{2^s} among its successors $A_{2^s+1}, \ldots, A_n$, which are contained in the (modified) PT_n. Therefore, we have even shown that A_{2^r} is the first of the cyclic permutations of A_{2^s} that appears in the cycle.

2. A_{2^s} is the first n-tuple in the cycle.

The n-tuple A_{2^s-1} is the predecessor of A_{2^s}. We suppose that A_{2^s-1} is contained in the cycle. It follows from above that the predecessor A_{2^r}, i.e., A_{2^r-1}, is in the cycle. Therefore, A_{2^r-1} must be a cyclic permutation of A_{2^s-1}. A look at PT_n shows that A_{2^s-1} contains 2^s ones, and in A_{2^r-1} we can find 2^r ones [see property (7)]. This is a contradiction to the assertion, as $r > s$. □

Corollary 1: If $n = 2^r + 2^s$, $r > s \geq 0$, then there are 2^s different cycles of maximum length that are produced by the cyclic permutations of the n-tuple A_0.

Proof: The operators $\mathcal{D}$ and $\mathcal{H}$ commute, so

$$\begin{aligned} \mathcal{D}^{2^r-2^s} A_{2^r} &= \mathcal{D}^{2^r-2^s} \mathcal{H}^{-2^s} A_{2^s} \\ &= \mathcal{H}^{-2^s} \mathcal{D}^{2^r-2^s} A_{2^s} = \mathcal{H}^{-2\cdot 2^s} A_{2^s}. \end{aligned}$$

By induction, every n-tuple $\mathcal{H}^{-\ell 2^s} A_{2^s}$, $\ell \in \mathbb{N}$, appears in the cycle of the successors of $(0, \ldots, 0, 1)$.

Using the same argument as in the proof of Theorem 6, we conclude that for every ℓ the n-tuple $\mathcal{H}^{-(\ell+1)2^s} A_{2^s}$ is the first cyclic permutation of $\mathcal{H}^{-\ell 2^s} A_{2^s}$ among the successors of the latter. As $2^s \mid \mathcal{P}(n)$, no other cyclic permutation than the ones described above can be found in the cycle produced by $(0, \ldots, 1)$.

We use the same technique for the successors of $\mathcal{H}^{-1} A_0$, $\mathcal{H}^{-2} A_0, \ldots, \mathcal{H}^{-2^s+1} A_0$. □

We will now consider $2^r - 1$-tuples. Using Pascal's triangle, we can determine $\mathcal{P}(n)$ for $n = 2^r - 1$.

Theorem 7: If $r \in \mathbb{N}$ and $n = 2^r - 1$, then $\mathcal{P}(n) = n$.

Proof: Using the proof of Theorem 3, we see that no cyclic permutation of A_1 can be found in fewer than $(n-2)$ steps. Pascal's triangle shows that

$$A_{n-1} = \mathcal{D}^{n-2} A_1 = (1, 0, 1, 0, \dots, 1, 0, 1).$$

Then $A_n = (1, 1, \dots, 1, 0)$ and $A_{n+1} = (0, 0, \dots, 1, 1) = A_1$. □

Corollary 2: For $r \geq 2$ and $n = 2^r - 1$, no cyclic permutation of A_1 can be found in the *basic-Ducci-sequence*, and there are n different cycles of maximum length.

Again, we can extend the last theorem.

Theorem 8: If $n = 2^r - 2^s$, $r > s \geq 0$, then $\mathcal{P}(n) = n$.

Proof: We prove this theorem using Ehrlich's formulas:

$$\mathcal{P}(2^r - 2^s) = 2^s \mathcal{P}(2^{r-s} - 1) = 2^s(2^{r-s} - 1) = n. \quad \square$$

It can be shown that only for such an n does the length of the cycle of the *basic-Ducci-sequence* equal n.

Theorem 9: If $\mathcal{P}(n) = n$, then $n = 2^r - 2^s$, where $n \geq 2$ and $r > s \geq 0$.

Proof: Using properties (3) and (4), we can limit our investigation to odd numbers. Then the first n-tuple in the cycle is $A_1 = (0, \dots, 0, 1, 1)$. There are only two different (possible) predecessors of A_1: the n-tuple $(0, \dots, 0, 1)$ or the n-tuple $B := (1, \dots, 1, 0)$ (see [11]). As the first n-tuple is not in the cycle, the predecessor of A_1 in the cycle must be B. As $\mathcal{P}(n) = n$, it follows that $B = A_n$. Since every binary n-tuple has exactly two predecessors, the predecessor of B is either $C := (1, 0, 1, 0, \dots, 1, 0, 1)$ or $D := (0, 1, 0, 1, \dots, 0, 1, 0)$. We consider PT_n. The last row represents A_{n-1}, i.e., C or D. It follows from Theorem 1 that the first entry of A_{n-1} must be 1; thus, the predecessor of B in the cycle is C. If we consider PT_{n+1}, then its last row must consist entirely of ones because C is the second to last row of PT_{n+1}. Property (5) shows that all the entries are ones if and only if $n+1$ is a power of 2 and $n = 2^r - 1$ for some $r \geq 2$. (For $n = 2^1 - 1$, the Ducci-problem makes no sense). □

As above, we can answer the question: Which n-tuple is the first one in the cycle?

Theorem 10: The $2^r - 2^s$-tuple A_2, where $n \geq 2$ and $r > s \geq 0$, is the first one in the cycle of the *basic-Ducci-sequence*.

Proof:

1. The n-tuple is contained in the cycle.

From Pascal's triangle, we can conclude (using the recursive construction given above):

$$A_{n-1} = (\underbrace{1, \dots, 1}_{2^s}, \underbrace{0, \dots, 0}_{2^s}, \dots, \underbrace{1, \dots, 1}_{2^s}).$$

We obtain alternating blocks of 2^s ones and 2^s zeros, the first and the last block consisting of ones. For A_n, we conclude:

$$A_n = (\underbrace{0, \dots, 0, 1}_{2^s}, \dots, \underbrace{0, \dots, 0, 1}_{2^s}, \underbrace{0, \dots, 0}_{2^s}).$$

As the first $n/2^2-1$ blocks can be considered as the first elements of a *basic-Ducci-sequence* of 2^s-tuples, the next successors are easy to determine. After 2^s-1 applications of $\mathcal{D}$, we find

$$A_{n+2^s-1}=(\underbrace{1,1,\ldots,1,1}_{n-2^s},\underbrace{0,\ldots,0}_{2^s}).$$

It follows that

$$A_{n+2^s}=(\underbrace{0,\ldots,0}_{n-2^s-1},\underbrace{1,0,\ldots,0,1}_{2^s+1})=A_{2^s},$$

and the n-tuple A_{2^s} is contained in the cycle.

2. A_{2^s} is the first n-tuple in the cycle.

Using $\mathcal{P}(n)=n$, we can conclude: If A_{2^s-1} is contained in the cycle, then $A_{2^s-1}=A_{n+2^s-1}$. The first entry of A_{2^s-1} must be 0 (see construction of n-tuples from Pascal's triangle). On the other hand, we have shown above that $a_{n+2^s-1,1}=1$, which is a contradiction. □

THE PROBLEM "WITH" OR "WITHOUT" A –1

The question whether a given n is with or without a -1 is important for different theorems and properties of Ducci-sequences [see Theorem 4, properties (1) and (2)].

As every integer n can be considered as a product of prime numbers p, the problem can be divided into two separate questions:

- Which prime numbers are with a -1, which are without? and
- If $m,n\in\mathbb{N}$ and with (-out) a -1, is the product with (-out) a -1?

Prime numbers will be treated first. In the following, p shall denote an odd prime number and $O_p(2)$ shall denote the order of 2 in a cyclic group of unities of the Galois-field $\mathbb{Z}_p$. We keep in mind that $O_p(2)$ is a divisor of $\varphi(p)$—Euler's φ-function—and $\varphi(p)=p-1$.

The case $p\equiv-1 \bmod 4$ is easier to examine.

Lemma 3: Let $p\equiv-1 \bmod 4$, then $O_p(2)$ is odd if and only if $\frac{p+1}{4}$ is even.

Proof: We consider $p\equiv-1 \bmod 4$ first and show the equivalence of three statements:

1. $O_p(2)$ is odd if and only if 2 is a square number in $\mathbb{Z}_p$.

"$\Rightarrow$" Since, by assertion, $O_p(2)$ is odd, we obtain

$$2^{O_p(2)+1}=2=\left(2^{\frac{O_p(2)+1}{2}}\right)^2,$$

and 2 is a square number in $\mathbb{Z}_p$.

"$\Leftarrow$" $2\equiv a^2 \bmod p$ for some $a\in\mathbb{Z}_p$. By Fermat's theorem, $a^{p-1}\equiv 1 \bmod p$ and, as $2|p-1$ (p odd!), we conclude:

$$a^{p-1}=(\underbrace{a^2}_{=2})^{\frac{p-1}{2}}\equiv 1 \bmod p$$

and, further, $2^{\frac{p-1}{2}}\equiv 1 \bmod p$.

Using $p \equiv -1 \bmod 4$, we get $p-1 \equiv -2 \bmod 4$, and $\frac{p-1}{2}$ must be odd.

2. 2 is a square number in $\mathbb{Z}_p$ if and only if $(\frac{2}{p}) = 1$ (Legendre-symbol), which is equivalent to

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1.$$

3. $\frac{p+1}{4}$ is even if and only if $\frac{p^2-1}{8}$ is even. We can write p as $p = -1+4k, k \in \mathbb{N}$. Then it follows that $p^2 = 16k^2 - 8k + 1$ or $\frac{p^2-1}{8} = 2k^2 - k$.

As $2k^2$ is always even, we conclude that $\frac{p^2-1}{8}$ is even if and only if k is even. □

Theorem 11: Let $p \equiv -1 \bmod 4$. Then p is with a -1 if and only if $\frac{p+1}{4}$ is odd.

Proof:

"$\Leftarrow$" We consider the equation $x^2 \equiv 1 \bmod p$. As $\mathbb{Z}_p$ is a Galois-field, the equation has exactly two solutions: $x \equiv 1 \bmod p$ and $x \equiv -1 \bmod p$. $2^{\frac{O_p(2)}{2}}$ is an integer solution of this equation if and only if $O_p(2)$ is even, i.e., $\frac{p+1}{4}$ is odd for $p \equiv -1 \bmod 4$ (Lemma 3). As, by definition, $2^{\frac{O_p(2)}{2}}$ cannot be congruent to 1 mod p, we have $2^{\frac{O_p(2)}{2}} \equiv -1 \bmod p$ and p is with a -1.

"$\Rightarrow$" If $2^M \equiv -1 \bmod p$, then it follows that $2M | O_p(2)$, and so the order of 2 is even. From Lemma 3, it follows that $\frac{p+1}{4}$ is odd. □

Let p be with a -1 and M be the least integer number with $2^M \equiv -1 \bmod p$, $M = 2^k \ell$ where $k \geq 0$ and ℓ is odd. For our further examination, we need to know that $k = 0$. We will use a well-known theorem from number theory.

Theorem 12: The congruence $x^2 \equiv -1 \bmod p$ has a solution in $\mathbb{Z}_p$ if and only if $p \equiv 1 \bmod 4$.

This theorem leads us at once to the following corollary.

Corollary 3: M is odd for every $p \equiv -1 \bmod 4$.

Proof: We assume that M is even. Then $a = 2^{\frac{M}{2}}$ satisfies the equation $x^2 \equiv -1$ in contradiction to the above theorem. □

The case $p \equiv 1 \bmod 4$ is harder to treat because the above argument cannot be used in this case. We will give only a partial solution.

Theorem 13: Let $p \equiv 1 \bmod 4$ and $\frac{p+1}{4}$ be odd. Then p is with a -1.

Proof: We again use

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1.$$

Since $\frac{p+1}{4}$ is odd ($p \equiv 1 \bmod 4$) as well as $\frac{p+1}{4}$ (by assumption), we conclude that 2 is not a square number in $\mathbb{Z}_p$. Using $2^{O_p(2)+1} \equiv 2 \bmod p$, we see that $O_p(2)+1$ must be odd and $O_p(2)$ is even. By definition, $2^{\frac{O_p(2)}{2}}$ cannot be congruent to 1, so p must be with a -1. □

If $\frac{p+1}{4}$ is even, both cases are possible:

- 17, 41, 97, 113 are with a –1;
- 73, 89, 233 are without a –1.

As the problem is linked to the still unsolved *Artin's Problem* (see [2], p. 113), the complete solution seems to be very difficult but interesting.

We also cannot determine whether M is even or odd. In most cases, M is even; however, for 281, we obtain $M = 35$. This question will be important in our further examination.

We will now treat products of prime numbers.

Lemma 4: Let p be with a –1. Then p^n is with a –1 for every $n \in \mathbb{N}$.

Proof: By induction. Let p^n be with a –1 for some n and $2^M \equiv -1 \bmod p^n$. Then $2^M = -1 + kp^n$ for some k. We compute:

$$2^{pM} = (2^M)^p = (-1+kp^n)^p = -1+kp^{n+1} + \sum_{i=2}^{p-1}(-1)^{i+1}\binom{p}{i}k^i p^{ni} + p^{np}k^p.$$

As $\binom{p}{i}$ is divisible by p for $2 \le i \le p-1$, we obtain $2^{pM} \equiv -1 \bmod p^{n+1}$. As the lemma holds for $n = 1$, the proof is complete. □

(For a similar problem, see [13], pp. 364 ff.)

Theorem 14: Let $n = p_1 p_2 \dots p_\ell$, the product of odd prime numbers p_i (not necessarily different from each other) and (at least) one of the p_i without a –1, Then the product n is without a –1.

Proof: Without loss of generality, let p_1 be without a –1. We assume that n is with a –1, which means that there exists an $M \in \mathbb{N}$ with $2^M \equiv -1 \bmod n$. This implies that $2^M \equiv -1 \bmod p_1$ in contradiction to the choice of p_1. □

Theorem 15: Let ℓ and m be odd integers with a –1, $(\ell, m) = 1$, $2^L \equiv -1 \bmod \ell$ and $2^M \equiv -1 \bmod m$ (L and M minimal). Then $n = \ell m$ is with a –1 if and only if, for some $k \in \mathbb{N}_0$, 2^k divides L and M, and 2^{k+1} divides neither of them.

Proof:

"$\Leftarrow$" Obviously $L/2^k$ and $M/2^k$ are odd numbers. We compute:

$$(2^L)^{\frac{M}{2^k}} \equiv (-1)^{\frac{M}{2^k}} \bmod \ell \equiv -1 \bmod \ell;$$
$$(2^M)^{\frac{L}{2^k}} \equiv (-1)^{\frac{L}{2^k}} \bmod m \equiv -1 \bmod m.$$

It follows that $2^{\frac{LM}{2^k}} \equiv -1 \bmod n$ as $n = \ell m$.

"$\Rightarrow$" By contradiction:

Assume, without loss of generality, that $2^N \equiv -1 \bmod n$, $2^k | L$, $2^{k+1} \nmid L$, and $2^{k+1} | M$ and N is minimal. This implies that $2^N \equiv -1 \bmod m$, $2^N \equiv -1 \bmod \ell$, and that N is the least common multiple of L and M. Therefore, N is divisible by 2^{k+1} and $N = 2LR$ for some $R \in \mathbb{N}$. It follows by computation that

$$\begin{aligned} 2^N = 2^{2LR} &= (2^L)^{2R} \\ &\equiv (-1)^{2R} \bmod \ell \equiv 1 \bmod \ell, \end{aligned}$$

which is a contradiction to $2^N \equiv -1 \bmod \ell$ as $\ell \neq 2$. □

Corollary 4: If $p_1, \ldots, p_\ell$ are prime numbers, $p_i \equiv -1$ mod 4, and $\frac{p_i+1}{4}$ is odd for every $1 \le i \le \ell$, then $n = p_1^{k_1} \ldots p_\ell^{k_\ell}$ is with a -1.

Proof: Since $\frac{p+1}{4}$ is odd, p is with a -1 by Theorem 11. By Lemma 4, p^k is with a -1. By Corollary 3, M is odd, where $2^M \equiv -1 \bmod p$. By the proof of Lemma 4, $2^{p^{k-1}M} \equiv -1 \bmod p^k$; of course, the exponent $p^{k-1}M$ is odd. This is true for each prime p. The result now follows by Theorem 15. □

(For a similar result, see [13], p. 364.)

REMAINING QUESTIONS

During our investigation, we have seen that the Ducci-problem is closely linked to the problem of finding the order of 2 in a given field $\mathbb{Z}_p$. It seems that this problem is not yet completely solved.

Going back to the Ducci-sequences, it is interesting to ask how many different orbits the operator $\mathcal{D}$ (and therefore $\mathcal{T}$) produces if *all* Ducci-sequences are considered. If n is not a power of 2, let k be the number of divisors m of n (where $m < n$). Then we can find at least $k+2$ different cycles: the cycle that contains only the n-tuple $(0, \ldots, 0)$, the cycle of the *basic-Ducci-sequence* of n-tuples and the cycle of n-tuples that are formed of the n/m-fold repetition by the m-tuples of the corresponding *basic-Ducci-sequence*.

A whole range of new problems can be obtained using a variation of the process of forming the Ducci-sequence (first done by Wong [17]), for example:

$$\mathcal{T}(a_1, \ldots, a_n) := ((a_1 + a_2) \bmod k, \ldots, (a_n + a_1) \bmod k), \quad k \in \mathbb{N}.$$

Many interesting results on that topic can be found in [17], but the length of cycles of so-called *Ducci-processes* has not been treated yet (except the above variation in [15]).

REFERENCES

1. K. D. Boklan. "The n-Number Game." *The Fibonacci Quarterly* **22.2** (1984):152-55.
2. P. Bundschuh. *Einführung in die Zahlentheorie*. 2. Auflage. Berlin, Heidelberg, New York: Springer-Verlag, 1992.
3. M. Burmester, R. Forcade, & E. Jacobs. "Circles of Numbers." *Glasgow Mathematical Journal* **19** (1978):115-19.
4. C. Ciamberlini & A. Marengoni. "Su una interessante curiosità numerica." *Periodiche di Matematiche* **17** (1937):25-30.
5. J. W. Creely. "The Length of a Three-Number Game." *The Fibonacci Quarterly* **26.2** (1988):141-43.
6. A. Ehrlich. "Periods in Ducci's N-Number Game of Differences." *The Fibonacci Quarterly* **28.4** (1990):302-05.
7. B. Freedman. "The Four Number Game." *Scripta Mathematica* **14** (1948):35-47.

8. A. Hinz. "Pascal's Triangle and the Tower of Hanoi." *Amer. Math. Monthly* **99** (1992):538-44.
9. M. Lotan. "A Problem in Difference Sets." *Amer. Math. Monthly* **56** (1949):535-41.
10. E. Lucas. *Théeorie des nombres*. 1891, p. 420.
11. A. Ludington Furno. "Cycles of Differences of Integers." *J. Number Theory* **13** (1981):255-61.
12. A. Ludington-Young. "Length of the *n*-Number Game." *The Fibonacci Quarterly* **28.3** (1990):259-65.
13. D. P. Parent. *Exercises in Number Theory.* New York: Springer-Verlag, 1984.
14. H.-O. Peitgen, et al. *Fractale: Selbstähnlichkeit, Chaosspiel, Dimension; ein Arbeitsbuch.*, Ernst Klett Schulbuchverlag, Stuttgart. Berlin, Heidelberg, New York: Springer-Verlag, 1992.
15. G. Schöffl. "Duccifolgen und ihre Behandlung im Unterricht, Zulassungsarbeit zur Wissenschaftlichen Prüfung für das Lehramt an den Gymnasien in Bayern." Unpublished thesis, Mathematisches Institut der Universität Würzburg, 1993.
16. K. B. Stolarsky. "Power and Exponential Sums of Digital Sums Related to Binomial Coefficient Parity." *SIAM J. Appl. Math.* **32** (1977):717-30.
17. F.-B. Wong. "Ducci Processes." *The Fibonacci Quarterly* **20.2** (1982):97-105.

AMS Classification Numbers: 00A08, 11B37, 11B65

❖❖❖

SOME PROBABILISTIC ASPECTS OF THE TERMINAL DIGITS OF FIBONACCI NUMBERS

Piero Filipponi and Renato Menicocci
Fondazione Ugo Bordoni, Via B. Castiglione 59, I-00142 Rome, Italy
(*Submitted January 1994*)

1. INTRODUCTION

By *terminal* digits of an integer N, we mean both the *initial* (leftmost) digit and the *final* (rightmost) digit of N. The following notation is used throughout the paper.

Notation

(i) RFN (Random Fibonacci Number: An ℓ-digit ($\ell \geq 2$) Fibonacci number whose subscript has been randomly chosen within the interval $[K_1, K_2]$, where $K_1 \geq 7$ and K_2 is *much* greater than K_1.
(ii) $B(d)$: the probability that the initial digit of a RFN is d.
(iii) $E(d)$: the probability that the final digit of a RFN is d.
(iv) $\langle a \rangle_b$: the integer a reduced modulo the integer b.
(v) $b \mid a$: the integer b divides the integer a ($\langle a \rangle_b = 0$).
(vi) $\lg x$: the logarithm to the base 10 of x.
(vii) (a, b): the greatest common divisor of a and b.

Moreover, F_k and L_k will denote the k^{th} Fibonacci and Lucas number, respectively, whereas $\alpha = (1+\sqrt{5})/2$ is the golden section, and we assume that $K_2 \to \infty$.

The principal aim of this paper is to study some probabilistic aspects of the terminal digits of RFN's. In particular, we shall answer questions such as:

"What is the probability that the initial digit of a RFN is greater than its final digit?"
"What is the probability that a RFN is divisible by its initial digit?"

The paper is set out as follows. After establishing some preliminary results in Section 2, in Section 3 some simple properties of RFN's which are related to their terminal digits are discussed. A glimpse of possible further investigations along this avenue is caught in Section 4.

All the results established in this paper have been thoroughly checked from the numerical point of view by means of suitable computer experiments. Nothing but a negligible difference between theoretical and experimental results has been observed even for comparatively small values of $K_2 - K_1$.

2. PRELIMINARY RESULTS

For an infinite set of real numbers (expressed in base 10) $\mathcal{S} = \{s_i\}_{i=0}^{\infty}$, let $p(d)$ be the probability that the initial digit of a randomly chosen (in a *large* interval) s_i is d. If

$$p(d) = \lg\left(1 - \frac{1}{d}\right), \tag{2.1}$$

then $\mathcal{S}$ is said to obey *Benford's law* (e.g., see [1], [4], and [5]).

In [2], [8], and [10] it was conjectured that the Fibonacci sequence obeys Benford's law. This fact has been proved in [9]; thus, we can state the following

Proposition 1:

$$B(d) = \lg\left(1+\frac{1}{d}\right). \tag{2.2}$$

Since our proof of Proposition 1 is very short, we report it because its argument will be used in the proof of Proposition 3.

Proof of Proposition 1: It is known [6] that the sets

$$\{s_k(x,y)\} = \{xy^k\}_{k=0}^{\infty} \text{ (x and y arbitrary real quantities)} \tag{2.3}$$

obey Benford's law, provided y is not a rational power of 10. Furthermore, it can be readily proved that the initial digit of F_k and that of $s_k[(\sqrt{5})^{-1}, \alpha]$ coincide for all $k \geq 6$, so that it remains to prove that α is not a rational power of 10. To do this, write the following equivalent relations,

$$\begin{aligned}
&\alpha = 10^{n/m} \quad (n \geq 0, m > 0 \text{ integers}),\\
&\alpha^m = 10^n,\\
&L_m + \sqrt{5}F_m = 2\cdot 10^n,
\end{aligned}$$

the last of which is clearly impossible because an irrational cannot equal an integer. Hence, the first relation cannot be true. Q.E.D.

Proposition 2:

$$E(d) = \begin{cases} \frac{1}{15} & \text{if } d \text{ is even,}\\ \frac{2}{15} & \text{if } d \text{ is odd.}\end{cases} \tag{2.4}$$

Proof: Inspection of the periodic sequence $\{\langle F_k\rangle_{10}\}_{k=0}^{59}$, whose repetition period is 60, shows us that

$$F_k \equiv d \pmod{10} \text{ iff } k = 60n + h_t(d) \quad (n = 0, 1, 2, \dots) \tag{2.5}$$

with $h_t(d)$ depending on d and $1 \leq t \leq 4$ (8) if d is even (odd).

More precisely, we have

$$\begin{array}{ll}
h(0) = 0, 15, 30, \text{ or } 45 & h(1) = 1, 2, 8, 19, 22, 28, 41, \text{ or } 59\\
h(2) = 3, 36, 54, \text{ or } 57 & h(3) = 4, 7, 13, 26, 44, 46, 47, \text{ or } 53\\
h(4) = 9, 12, 18, \text{ or } 51 & h(5) = 5, 10, 20, 25, 35, 40, 50, \text{ or } 55\\
h(6) = 21, 39, 42, \text{ or } 48 & h(7) = 14, 16, 17, 23, 34, 37, 43, \text{ or } 56\\
h(8) = 6, 24, 27, \text{ or } 33 & h(9) = 11, 29, 31, 32, 38, 49, 52, \text{ or } 58.
\end{array} \tag{2.6}$$

Q.E.D.

Proposition 3 (main result): The terminal digits of a RFN are statistically independent.

Proof: It is sufficient to prove that the value of the final digit has no statistical influence on that of the initial digit. In other words, it is sufficient to prove that the set of all Fibonacci numbers whose final digit is a given d obeys Benford's law.

If we replace [see (2.5)] y by α^{60}, x by $\alpha^{h_t(d)}/\sqrt{5}$, and k by n in (2.3), and observe that:

(i) α^{60} is not a rational power of 10,

(ii) the initial digit of $F_{60n+h_t(d)}$ and that of $s_n[\alpha^{h_t(d)}/\sqrt{5}, \alpha^{60}]$ coincide for all $n \geq 1$, then we see that, for given d and t, the sequence $F_{60n+h_t(d)}$ obeys Benford's law. The set

$$\bigcup_{t=1}^{T}\{F_{60n+h_t(d)}\} \quad \left(T = 4\frac{3-(-1)^d}{2},\ n = 1, 2, 3, \ldots\right) \tag{2.7}$$

given by the union of the disjoint sets $F_{60n+h_t(d)}$ for all admissible values of t, obeys Benford's law as well. Q.E.D.

Proposition 3 allows us to establish most of the results presented in the next section.

3. SOME STATISTICAL PROPERTIES OF RFN'S

From this point onward, the symbols i and j will denote the initial digit and the final digit of a RFN, respectively.

Proposition 4: $\text{Prob}(i = c, j = d) = \begin{cases} \lg(1+1/c)/15 & \text{if } d \text{ is even,} \\ 2\lg(1+1/c)/15 & \text{if } d \text{ is odd.} \end{cases}$

Proof: By Proposition 3 we can write

$$\text{Prob}(i = c, j = d) = B(c)E(d), \tag{3.1}$$

so that Proposition 4 follows by Propositions 1 and 2. Q.E.D.

Proposition 5: $\text{Prob}(i = j) = \dfrac{1}{15}\left(1 + \lg\dfrac{256}{63}\right) \approx 0.107.$

Proof: By Proposition 4 we can write

$$\begin{aligned}\text{Prob}(i = j) &= \frac{1}{15}\sum_{d=1}^{4}\lg\left(1+\frac{1}{2d}\right) + \frac{2}{15}\sum_{d=1}^{5}\lg\left(1+\frac{1}{2d-1}\right) \\ &= \frac{1}{15}\left(1+\lg\frac{256}{63}\right).\ \text{Q.E.D.}\end{aligned}$$

Proposition 6: $\text{Prob}(i > j) = \dfrac{1}{15}\lg\dfrac{5^{12}}{3402} \approx 0.324.$

Proof: Put

$$S_h = \sum_{d=0}^{h} E(d) \quad (0 \leq h \leq 9) \tag{3.2}$$

and write

$$\text{Prob}(i > j) = \sum_{c=1}^{9} B(c)S_{c-1} = \sum_{c=1}^{5} B(2c-1)S_{2c-2} + \sum_{c=1}^{4} B(2c)S_{2c-1}. \tag{3.3}$$

By (2.4), it can be readily proved (e.g., by induction on h) that

$$S_h = \begin{cases} (3h+2)/30 & \text{if } h \text{ is even,} \\ (h+1)/10 & \text{if } h \text{ is odd.} \end{cases} \tag{3.4}$$

Hence, by (3.3), (2.2), and (3.4), we get

$$\begin{aligned} \text{Prob}(i > j) &= \frac{1}{15}\sum_{c=1}^{5}(3c-2)\lg\left(1+\frac{1}{2c-1}\right)+\frac{1}{5}\sum_{c=1}^{4}c\lg\left(1+\frac{1}{2c}\right) \\ &= \frac{1}{15}\lg\frac{2^{15}3^{25}5^{15}7^2}{2^{16}3^{30}5^3 7^3} = \frac{1}{15}\lg\frac{5^{12}}{2\cdot 3^5\cdot 7}. \quad \text{Q.E.D.} \end{aligned}$$

Proposition 4 allows us to obtain the probability $D(a) = \text{Prob}(i+j=a)$ $(1 \le a \le 18)$. After a good deal of calculation, we obtained $15D(a) = \lg r(a)$, where

$$\begin{aligned} &r(1) = 2,\ r(2) = r(3) = 6,\ r(4) = \frac{40}{3},\ r(5) = \frac{45}{4},\ r(6) = \frac{112}{5},\ r(7) = \frac{35}{2}, \\ &r(8) = \frac{1152}{35},\ r(9) = \frac{1575}{64},\ r(10) = \frac{2560}{63},\ r(11) = \frac{1575}{128},\ r(12) = \frac{1280}{189}, \\ &r(13) = \frac{525}{128},\ r(14) = \frac{64}{21},\ r(15) = \frac{35}{16},\ r(16) = \frac{800}{441},\ r(17) = \frac{90}{64},\ r(18) = \frac{100}{81}. \end{aligned} \tag{3.5}$$

Proposition 7: The probability that a RFN is divisible by its initial digit is

$$\text{Prob}(i\,|\,\text{RFN}) = \frac{1}{120}\lg\frac{2^{109}3^{44}5^6}{7^5} \approx 0.448. \tag{3.6}$$

Proof: An integer d $(1 \le d \le 9)$ divides F_k iff $k = hn_d$ $(h = 0, 1, 2, \ldots)$ with n_d depending on d. By inspection of the periodic sequences $\{\langle F_k\rangle_d\}$, we get

$$n_1 = 1,\ n_2 = 3,\ n_3 = 4,\ n_4 = n_8 = 6,\ n_5 = 5,\ n_6 = n_9 = 12,\ n_7 = 8. \tag{3.7}$$

Since it can be readily proved that the sequence $\{F_{hn_d}\}$ obeys Benford's law (i.e., the events "$d\,|\,\text{RFN}$" and "$i = d$" are independent), by (3.7) we can write

$$\begin{aligned} \text{Prob}(i\,|\,\text{RFN}) &= \sum_{d=1}^{9} B(d)\,\text{Prob}(d\,|\,\text{RFN}) = \sum_{d=1}^{9}\lg\left(\frac{d+1}{d}\right)\frac{1}{n_d} \\ &= \frac{1}{120}\lg\prod_{d=1}^{9}\left(\frac{d+1}{d}\right)^{120/n_d} = \frac{1}{120}\lg\frac{2^{109}3^{44}5^6}{7^5}. \quad \text{Q.E.D.} \end{aligned}$$

Proposition 8: The probability that a RFN is divisible by its final digit is

$$\text{Prob}(j\,|\,\text{RFN}) = \frac{7}{15}. \tag{3.8}$$

The complete proof of Proposition 8 is rather lengthy so, for the sake of brevity, only a partial proof is given.

Proof: Put

$$Z(d) = \text{Prob}(j = d, d\,|\,\text{RFN}), \tag{3.9}$$

whence

$$\text{Prob}(j|\text{RFN}) = \sum_{d=0}^{9} Z(d). \tag{3.10}$$

Each $Z(d)$ $(0 \le d \le 9)$ must be calculated separately. In some cases this calculation is readily carried out. For instance, we immediately obtain

$$Z(0) = 0, \tag{3.11}$$

and

$$Z(d) = E(d) \text{ for } d = 1, 2, \text{ and } 5. \tag{3.12}$$

In some cases the calculation is slightly more complicated. Getting the equality

$$Z(9) = 0 \tag{3.13}$$

is an example. In some other cases the calculation is rather tedious. Getting the equality

$$Z(8) = \frac{1}{30} \tag{3.14}$$

is an example. Let us prove (3.13) and (3.14) in full detail.

Proof of (3.13): It is known that $F_k \equiv 0 \pmod 9$ iff $k \equiv 0$ (mod 12), that is, iff $k = 12n$ ($n =$ 0, 1, 2, ...). Since $12n$ is a multiple of 3, F_{12n} is even; thus, its last digit cannot be 9. Consequently, if $9|\text{RFN}$, then $j \ne 9$ and $Z(9) = 0$. □

Proof of (3.14): It is known that

$$F_k \equiv 0 \pmod 8 \text{ iff } k \equiv 0 \pmod 6. \tag{3.15}$$

Moreover, by (2.5) and (2.6) we have

$$F_k \equiv 8 \pmod{10} \text{ iff } k \equiv 6, 24, 27, \text{ or } 33 \pmod{60}. \tag{3.16}$$

For (3.15) and (3.16) to be fulfilled simultaneously, we must have $k = 60n+6$ or $60n+24$ ($n = 0$, 1, 2, ...). It follows that $Z(8) = 2/60 = 1/30$. □

By means of similar arguments, we obtained

$$Z(3) = Z(4) = \frac{1}{30} \text{ and } Z(6) = Z(7) = \frac{1}{60}. \tag{3.17}$$

Proposition 8 is proved by (3.9)-(3.14) and (3.17). Q.E.D.

Proposition 9: The probability $G(a)$ that $(i, j) = a$ $(1 \le a \le 9)$ is:

$$G(1) = \frac{1}{15}\lg\frac{2^{24}3^9 5^7}{7^6} \approx 0.756, \quad G(2) = \frac{1}{15}\lg\frac{3^6 5^2 7^3}{2^{18}} \approx 0.092, \quad G(3) = \frac{1}{15}\lg\frac{2^{11}5^3 7^4}{3^{16}} \approx 0.077,$$

$$G(4) = \frac{1}{15}\lg\frac{3^2 5^3}{2^9} \approx 0.023, \quad G(5) = \frac{1}{5}\lg\frac{6}{5} \approx 0{,}016, \quad G(6) = \frac{2}{15}\lg\frac{7}{6} \approx 0.009,$$

$$G(7) = \frac{1}{5}\lg\frac{8}{7} \approx 0.011, \quad G(8) = \frac{2}{15}\lg\frac{9}{8} \approx 0.007, \quad G(9) = \frac{1}{5}\lg\frac{10}{9} \approx 0.009.$$

Proof: By virtue of Proposition 3 we can write

$$G(a) = \sum_{c=1}^{9} B(c) \sum_{\substack{d=0 \\ (d,c)=a}}^{9} E(d). \tag{3.18}$$

Then we use (3.18) along with (2.2) and (2.4) to obtain the above results. Q.E.D.

Let us conclude this section by giving the expected values V_i and V_j of the initial and final digit of a RFN.

Proposition 10: $\begin{cases} V_i = 9 - \lg(9!) \approx 3.44, \\ V_j = 14/3 = 4.\overline{6}. \end{cases}$

The proof of Proposition 10 is left as an exercise for the interested reader.

4. FURTHER WORK

The theory developed in this paper also applies *mutatis mutandis* to recurring sequences other than the Fibonacci sequence. For example, considering the Lucas sequence would add much to the completeness of our results. Just to taste the flavor, we offer the following to the curiosity of the reader.

The probability A that a RFN and a RLN (Random Lucas Number) have the same final digit is

$$A = 1/9, \tag{4.1}$$

whereas the probability B that, once n is randomly chosen within a sufficiently large interval, F_n and L_n have the same final digit is

$$B = 1/5. \tag{4.2}$$

Question 1: "What is the probability R that a RFN and a RLN have the same initial digit?"

The answer is:

$$R = \sum_{c=1}^{9} B^2(c) \approx 0.165. \tag{4.3}$$

Observe that the answer to the following related question is completely different.

Question 2: "Choose a positive integer n at random within a sufficiently large interval. What is the probability S that F_n and L_n have the same initial digit?"

The answer is:

$$S = 0. \tag{4.4}$$

In fact, the following curious property can be stated [3].

Proposition 11: F_n and L_n cannot have the same initial digit for $n \geq 2$.

Denoting the initial digit of the number x by $f(x)$, we can also prove the inequality:

$$3 \leq f(F_n) + f(L_n) \leq 13 \quad (n \geq 2). \tag{4.5}$$

It is obvious that the statement of Proposition 11 does not exclude the possibility that the initial digits of F_n and L_n have the same parity [i.e., $f(F_n)+f(L_n)$ is even]. The problem of determining the probability of this occurrence remains an open problem. A computer experiment showed that the event $f(F_n)+f(L_n)\equiv 0 \pmod 2$ occurs 4232 times for $1\le n\le 10{,}000$.

Finally, it can be proved that the probability T that the sum $i+f(\text{RLN})$ is even is

$$T=U^2+(1-U)^2\approx 0.524, \tag{4.6}$$

where

$$U=\sum_{c=1}^{4}B(2c)=\lg\frac{315}{128}. \tag{4.7}$$

Because of the numerical value of $T\,(\approx 1/2)$, it seems worthwhile to investigate (e.g., by means of the autocorrelation-, run-, poker-test, etc.) the statistical properties of the binary sequences $\{\langle i+f(\text{RLN})\rangle_2\}$ for cryptographic purposes (stream ciphering [7]).

The proofs of (4.1)-(4.3) and (4.5)-(4.7) are left to the perseverance of the reader.

ACKNOWLEDGMENTS

This work has been carried out in the framework of an agreement between the Italian PT Administration (Istituto Superiore PT) and the Fondazione Ugo Bordoni. The authors wish to thank A. F. Horadam and A. G. Shannon, and the editor of this journal for bringing to their attention references [2], [8], [10], and [9], respectively. The valuable suggestions of the anonymous referee were deeply appreciated.

REFERENCES

1. F. Benford. "The Law of Anomalous Numbers." *Proc. Amer. Philos. Soc.* **78** (1938):551-72.
2. W. G. Brady. "More on Benford's Law." *The Fibonacci Quarterly* **16.1** (1978):51-52.
3. P. Filipponi. "F_n and L_n Cannot Have the Same Initial Digit." *Pi Mu Epsilon Journal* **10.1** (1994):5-6.
4. B. J. Flehinger. "On the Probability that a Random Integer Has Initial Digit A." *Amer. Math. Monthly* **73** (1966):1056-61.
5. R. S. Pinkham. "On the Distribution of First Significant Digits." *Ann. Math. Stat.* **32** (1961): 1223-30.
6. R. A. Raimi. "La Particolare Distribuzione delle Prime Cifre." *Le Scienze, Quaderni* **45** (1988):33-38. (Translated into Italian from *Scientific American*.)
7. D. E. Robling-Denning. *Cryptography and Data Security*. Reading, Mass.: Addison Wesley, 1982.
8. W. A. Sentance. "A Further Analysis of Benford's Law." *The Fibonacci Quarterly* **11.5** (1973):490-94.
9. L. C. Washington. "Benford's Law for Fibonacci and Lucas Numbers." *The Fibonacci Quarterly* **19.2** (1981):175-77.
10. J. Wlodarski. "Fibonacci and Lucas Numbers Tend To Obey Benford's Law." *The Fibonacci Quarterly* **9.1** (1971):87-88.

AMS Classification Numbers: 11B39, 11A07, 11N37

❖❖❖

ON AN ARITHMETICAL FUNCTION RELATED TO EULER'S TOTIENT AND THE DISCRIMINATOR

Pieter Moree
Freesiastraat 13, 2651 XL Berkel en Rodenrijs, The Netherlands

Hans Roskam
Wilhelminapark 4, 2342 AG Oegstgeest, The Netherlands
(*Submitted January 1994*)

1. INTRODUCTION

The discriminator, $D(j, n)$, is defined to be the smallest positive integer k for which the first n j^{th} powers are distinct modulo k. It was introduced by Arnold, Benkoski, and McCabe [1] in order to determine the complexity of an algorithm they had developed. Results on the discriminator can be found in [1, 3, 4, 12, 13, 16, 17]. We show that, under certain conditions, the discriminator takes on values that are also assumed by the function $E(n) := \min\{k : n|\varphi(k)\}$. Here φ denotes Euler's totient. We call E the *Euler minimum function*. The sequence $\{a_k\}_{k=1}^{\infty}$, with $a_k = \operatorname{lcm}(\varphi(1), \ldots, \varphi(k))$ is used to link the discriminator and the Euler minimum function. As an application we show that, for several values of n and primes p, there exist unbounded sequences $\{j_k\}_{k=1}^{\infty}$ and $\{e_k\}_{k=1}^{\infty}$, such that $D(j_k, n) = p^{e_k}$ for every natural number k. The prime powers p^{e_k} are exceptional values of the discriminator, since it is known that $D(j, n)$ is squarefree for every fixed $j > 1$ and every n large enough [4]. For example, if $j > 1$ and j is odd, one has, for every n sufficiently large, $D(j, n) = \min\{k \geq n | \gcd(j, \varphi(k)) = 1$ and k is squarefree$\}$. In the literature so far only the case where j is fixed has been considered. In this paper we focus on the case where n is fixed. The behavior of $D(j, n)$ turns out to be very different in these cases. (For a table of values of the discriminator, see [17].)

Since we think that the Euler minimum function and the sequence $\{a_k\}_{k=1}^{\infty}$ are of interest in themselves, we also prove some results on them which are possibly not related to discriminators.

2. RESULTS ON THE EULER MINIMUM FUNCTION

There seems to be no literature on $E(n)$. The related set $\{k : n|\varphi(k)\}$, however, does occur in the literature. It is denoted by C_n [we will use the notation $C(n)$] and occurs in a series of papers on the equidistribution of the integers coprime with n ("the totatives") in intervals of length n/k written in the 1950s [6, 7, 10, 11]. In particular, it is shown there that $A(n) = C(n)$ if and only if n is prime, where $A(n)$ is the set $\{k \in \mathbb{N} : n^2 | k$ or there exists a p with $p \equiv 1 \pmod{n}$ and $p|k\}$. A result on $C(n)$ of a different kind (and time) is that of Dressler [5], who proved that the set $\mathbb{N} \setminus C(n)$ has natural density zero for every n.

Recall that if $\prod p_i^{\alpha_i}$ is the canonical prime factorization of n, then $\varphi(n) = \prod p_i^{\alpha_i - 1}(p_i - 1)$. So, in particular, $n|\varphi(n^2)$ and, therefore, $E(n) \leq n^2$, and so $E(n)$ exists. In the proofs, we repeatedly use the following simple principle to show that a certain number does not equal the $E(n)$: we exhibit a smaller number in the collection $C(n)$. We study only the case where n equals a prime power.

The symbol p is used exclusively for primes.

Theorem 1: Let q be a prime. Let m be the smallest squarefree number of the form $\prod_{i=1}^{k}(1+a_iq^{e_i})$ with $1+a_iq^{e_i}$ prime for $i=1,\ldots,k$ and $\sum_{i=1}^{k}e_i=n$. Then

$$E(q^n)=\min\{m, q^{n+1}\}.$$

In case $E(q^n)=m$, we have

$$\prod_{i=1}^{k}a_i<q \quad\text{and}\quad \prod_{i=1}^{k}a_i=\varphi(m)/q^n.$$

Remark: By Dirichlet's theorem on arithmetical progressions, m exists.

Proof: Assume that $p\neq q$ and $p|E(q^n)$. If $p^2|E(q^n)$, then the integer $E(q^n)/p$ is also in $C(q^n)$. Since this contradicts the definition of $E(q^n)$, it follows that $p^2\nmid E(q^n)$. Since the integer $E(q^n)/p$ is not in $C(q^n)$, we have $p\equiv 1 \pmod q$. Therefore, $p=1+aq^e$ for some positive integers a and e. Also, if $q|E(q^n)$, then the integer $E(q^n)q^e/p$, which is less than $E(q^n)$, is in $C(q^n)$. Put $g=\mathrm{ord}_q(\varphi(E(q^n)))$. Obviously, $g\geq n$. If $g>n$, then the integer $E(q^n)q^e/p$, which is less than $E(q^n)$, is in $C(q^n)$. This contradiction shows that $g=n$. Up to this point we have shown that $E(q^n)$ is a squarefree number of the form $\prod_{i=1}^{k}(1+a_iq^{e_i})$ with $1+a_iq^{e_i}$ prime for $i=1$, ..., k and $\sum_{i=1}^{k}e_i=n$. Clearly, $E(q^n)$ has to be the smallest number of this form, that is, $E(q^n)=m$. In the remaining case where $E(q^n)$ does not have a prime divisor p with $p\neq q$, we have $E(q^n)=q^{n+1}$. It follows that $E(q^n)=\min\{m,q^{n+1}\}$. In the case $m<q^{n+1}$, we have $\varphi(m)=\prod_{i=1}^{k}a_iq^{e_i}=q^n\prod_{i=1}^{k}a_i<m<q^{n+1}$ and the remaining part of the assertion follows. □

In order to compute $E(q^n)$, the following variant of Theorem 1 is more convenient to work with. We denote by $S(q)$ the set of squarefree numbers composed of only primes p satisfying $p\equiv 1 \pmod q$. For convenience, we define the minimum of the empty set to be ∞.

Theorem 1': $E(q^n)=\min\{m,q^{n+1}\}$, where $m=\min\{s\in S(q): q^n \text{ divides } \varphi(s)/q^n<q\}$.

For given positive integers a and d with $\gcd(a,d)=1$, we denote by $p(d,a)$ the smallest prime p satisfying $p\equiv a \pmod d$ and more in general by $p_i(d,a)$, $i\geq 2$, the i^{th} smallest such prime. We denote by $\omega(n)$ the number of distinct prime factors of n.

Corollary 1:

(i) The largest prime divisor of $\varphi(E(q^n))$ is q.
(ii) The smallest prime divisor of $E(q^n)$ is not less than q.
(iii) If q is odd, then $\omega(E(q^n))<\min\{n+1,\log q/\log 2\}$.
(iv) $E(q)=\min\{q^2,p(q,1)\}$.
(v) $E(q^2)=\min\{q^3,p(q^2,1),p(q,1)p_2(q,1)\}$.

Theorem 1 and in particular parts (iv) and (v) of Corollary 1 show that the behavior of the Euler minimum function is intimately tied up with the distribution of prime numbers. Theorem 1 gives rise to questions on the behavior of $p(q,1)$ and, if we delve deeper, on $p_i(q,1)$ for $i\geq 2$. Corollary 1(v), for example, gives rise to the following question: Is it true that infinitely often $p(q,1)p_2(q,1)<p(q^2,1)$? Unfortunately, problems involving $p(d,a)$ are generally very difficult (see, e.g., [14, p. 217] for an overview). However, there is a guiding principle in these difficult matters: probabilistic reasoning. The basic assumptions made in probabilistic reasoning are that

the probability that n is a prime is about $1/\log n$ and that the events n is a prime and m is a prime are independent. Using probabilistic reasoning, we arrive, for example, at the conjecture that $p(q, 1) < q^2$ for every sufficiently large prime q. Indeed, this conjecture was made by several mathematicians (see, e.g., [9] [15]). Very recently, Bach and Sorenson [2] proved that $p(q, 1) < 2(q\log q)^2$, assuming the Extended Riemann Hypothesis holds true. By Corollary 1(iv), the conjecture is equivalent to $E(q) = p(q, 1)$ for every prime q large enough. Unconditionally, we can only prove the following result.

Lemma 1: $|\{q \le x : E(q) = p(q, 1)\}| \gg x^{.6687}/\log x$.

Proof: Put $A_a(x, \delta) = |\{p : a+2 \le p \le x,\ P(p-a) \ge x^\delta\}|$, where $P(n)$ denotes the greatest prime divisor function. Put $\delta = .6687$. Then by Théorème 1 of Fouvry [8]. $A_a(x, \delta) \gg x/\log x$, where the implied constant depends only on a. Let p be a prime contributing to $A_a(x, \delta)$. Put $P(p-a) = q$. Then $p(q, a) \le p \le x \le q^{1/\delta}$. Since there are at most $x^{1-\delta}$ primes p such that $P(p-a) = q$ and $q \ge x^\delta$ (a fixed), it follows that

$$|\{q \le x : p(q, a) \le q^{1/\delta}\}| \ge \frac{A_a(x, \delta)}{x^{1-\delta}} \gg x^\delta/\log x.$$

In particular, we have $|\{q \le x : p(q, 1) < q^2\}| \gg x^{.6687}/\log x$. □

Remark: Let a be an arbitrary fixed positive integer. The result implicit in the proof of Lemma 1 that

$$|\{q \le x : p(q, a) < q^{1.496}\}| \gg x^{.6687}/\log x,$$

supersedes the record result of Motohashi mentioned in *The Book of Prime Number Records* [14, p. 218], who proved in 1970 that $|\{q \le x : p(q, a) < q^{1.6378}\}|$ tends to infinity with x.

The following lemma is a straightforward consequence of Theorem 1.

Lemma 2:

(i) $E(p^a) \ne E(q^b)$ if $p \ne q$.

(ii) $E(p^a) \ne E(p^b)$ if $a \ne b$.

Proof:

(i) If $E(p^a) = E(q^b)$, then $P(\varphi(E(p^a))) = P(\varphi(E(q^b)))$. If $p \ne q$, this is impossible by Corollary 1(i).

(ii) Since, by Theorem 1, $p^a \| \varphi(E(p^a))$ and $p^b \| \varphi(E(p^b))$, clearly $E(p^a) \ne E(p^b)$ if $a \ne b$. □

If $q = 2$, Theorem 1 can be improved. For $j \ge 0$ put $\mathcal{F}_j = 1 + 2^{2^j}$. The primes of this form are called *Fermat primes*. Let I be the set of i such that $\mathcal{F}_i$ is prime. Notice that 0, 1, 2, 3, and 4 are in I. These numbers correspond with the primes 3, 5, 17, 257 and 65537. These primes are the only known Fermat primes.

Lemma 3: Let $\sum_{j\in J} 2^j$ be the representation to the base 2 of n. Then

$$E(2^n) = \begin{cases} \prod_{j\in J} \mathcal{F}_j & \text{if } J \text{ is a subset of } I; \\ 2^{n+1} & \text{otherwise.} \end{cases}$$

Proof: Notice that the number m (in the notation of Theorem 1′) equals $\min\{s \in S(2): \varphi(s) = 2^n\}$. The prime factors of m must all be Fermat primes (for a number of the form $1+2^b$ to be prime, it is necessary that b is a power of two). On using the uniqueness of the representation to the base 2, it follows that $m = \prod_{j \in J} \mathcal{F}_j$ if J is a subset of I and ∞ otherwise. Multiplying out $\prod_{j \in J}(2^{2^j}+1)$ gives a sum of powers of 2 with unequal exponents and largest exponent n. So $\prod_{j \in J} \mathcal{F}_j < 2^{n+1}$ (using the uniqueness of the representation to the base 2 again). The lemma then follows from Theorem 1′. □

Example: $E(2^{31}) = 4294967295$.

Corollary: If there are only finitely many Fermat primes, then $E(2^a) = 2^{a+1}$ for every sufficiently large a.

Remark: The prime 2 seems to be the only one for which such an explicit result can be derived. This is in agreement with the saying of H. Zassenhaus that two is the oddest of primes.

The next lemma demonstrates that, for some odd primes, Theorem 1′ can also be sharpened, although to a lesser extent.

Lemma 4: $E(q^n) = \min\{q^{n+1}, p(q^n, 1)\}$ for $q = 3, 7, 13$, and 31. $E(q^n) = \min\{q^{n+1}, p(q^n, 1)\}$ if n is odd for $q = 5$ and 19.

Proof: We only work out the case where $q = 19$, the other cases being similar. Notice that $3 | 1+2.19^a$, so $1+2.19^a$ is not a prime. Then $\{s \in S(19): 19^n | \varphi(s), \varphi(s) < 19^{n+1}$ and $\omega(s) \geq 2\} = \{(1+4.19^a)(1+4.19^b): a+b = n$ and both $1+4.19^a$ and $1+4.19^b$ are prime$\}$. Now, since n is odd, we can assume without loss of generality that a is even. But then $5 | 1+4.19^a$, so this collection is empty. Therefore, by Theorem 1′, we find that $E(19^n) = \min\{19^{n+1}, p(19^n, 1)\}$. □

In the next section it is shown that primes p such that $E(p^n) = p^{n+1}$ for infinitely many n are related to special values of this discriminator. Let E denote the collection of primes having this property.

Lemma 5: $2 \in E$.

Proof: Since $F_5 = 641 \cdot 6700417$ is composite (Euler), it follows from Lemma 3 that $E(2^n) = 2^{n+1}$ for every n that has 2^5 in its representation to the base 2. Since there are obviously infinitely many such n, the lemma follows. □

Lemma 6: Let q be an odd prime. Suppose there are integers a, d, and n_0 such that $E(q^n) = \min\{q^{n+1}, p(q^n, 1)\}$ for every $n \geq n_0$ and $n \equiv a \pmod d$. Then q is in E.

Proof: Let k be an arbitrary integer such that $k \geq n_0$ and $k \equiv a \pmod d$. For every j in $\{1, \ldots, (q-1)/2\}$, choose some prime divisor p_j of $1+2jq^k$. Notice that $\gcd(p_j, q) = 1$. Then, by Fermat's little theorem, $p_j | 1+2jq^{k+m(p_j-1)}$ for every j in $\{1, \ldots, (q-1)/2\}$, so $1+2jq^{k+m(p_j-1)}$ is composite for every m in $\mathbb{N}$ and j in $\{1, \ldots, (q-1)/2\}$. Put $\ell = \operatorname{lcm}(p_1 - 1, \ldots, p_{(q-1)/2} - 1)$. Then $1+2jq^{k+m\ell d}$ is composite for every m in $\mathbb{N}$ and j in $\{1, \ldots, (q-1)/2\}$. Since $k + m\ell d \equiv a \pmod d$ and $k + m\ell d \geq n_0$, it follows from the hypothesis of the lemma that $E(q^{k+m\ell d}) = q^{k+1+m\ell d}$ for every m in $\mathbb{N}$; therefore, q is in E. □

Finally, using Lemmas 4, 5, and 6, we find

Lemma 7: $\{2,3,5,7,13,19,31\} \subseteq E$.

We conjecture that in fact every prime is in E and challenge the reader to prove this or, at least, to exhibit other primes in E.

3. THE LOWEST COMMON MULTIPLE OF THE SUCCESSIVE TOTIENTS

In this section we study the sequence $\{a_k\}_{k=1}^{\infty}$, with $a_k = \text{lcm}(\varphi(1), \ldots, \varphi(k))$; in plain English, a_k is the lowest common multiple of the first k totients. In the next paragraph it will transpire that this strange sequence provides a link between discriminators and the Euler minimum function. The purpose of this section is to give the reader some feeling for the behavior of this sequence.

Put $c_k = a_k / a_{k-1}$ for $k \geq 2$. We say k (≥ 2) is a *jumping point* if c_k exceeds one.

Lemma 8: The number k is a jumping point if and only if $k = E(p^r)$ for some prime p and exponent $r > 1$.

Proof: If k is a jumping point, then there is a prime p such that $p \mid c_k$. Put $r = \text{ord}_p(\varphi(k))$. Then $p^r \nmid \varphi(\ell)$ for every $\ell < k$ (otherwise $p \neq c_k$), so $k = E(p^r)$. On the other hand, if $k = E(p^r)$ for some prime p and exponent r, then $c_k \geq p$, so k is a jumping point. □

Lemma 9: For $k \geq 2$, c_k is a prime or equals 1.

Proof: If $c_k > 1$, then $k = E(p^r)$ by the previous lemma. Now p is the only prime dividing c_k because if another prime, say q, would divide c_k, then it would follow that $E(p^r) = E(q^a)$, where $q^a \| \varphi(k)$. By Lemma 2(i), this is impossible. If $p^2 \mid c_k$, then $p^{r-1} \nmid \varphi(\ell)$ for every $\ell < k$, and it follows that $E(p^{r-1}) = E(p^r)$. By Lemma 2(ii), this is impossible. □

The following lemma gives an idea of the growth of the sequence $\{a_k\}_{k=1}^{\infty}$ as k tends to infinity. A trivial lower bound for a_k is given by $\exp(c\sqrt{k})$ for some $c > 0$. To see this, note that $\prod_{p \leq \sqrt{k}} p$ divides a_k (since $p \mid \varphi(p^2)$). On using the result $\sum_{p \leq x} \log p \sim x$ of prime number theory, the bound is easily established.

Lemma 10: Let ε be an arbitrary fixed positive real number. Then

$$\exp(k^{.6687}) \ll a_k \ll \exp((1+\varepsilon)k).$$

Proof: Recall that $\Lambda(n)$, the Von Mangoldt function, is defined by $\log p$ if n is of the form p^k, and 0 otherwise. Notice that

$$\log(a_k) \leq \log(\text{lcm}(1, \ldots, k)) = \sum_{n \leq k} \Lambda(n) \leq (1+\varepsilon)k$$

for every k sufficiently large. The latter estimate follows from the well-known result

$$\sum_{n \leq x} \Lambda(n) \sim x$$

of prime number theory. This gives the upper bound.

The primes contributing to $A_1(k,\delta)$ (cf. the proof of Lemma 1) yield $\gg k^{\delta}/\log k$ distinct primes not less than k^{δ} that occur as prime factors of numbers of the form $p-1$ with p not exceeding k. The product of these primes is a divisor of a_k exceeding $\exp(ck^{\delta})$ for some $c>0$ and all $k\ge 1$. □

Remark: In case $A_a(x,\delta)\gg x/\log x$ holds for a number larger than .6687, this automatically gives rise to a corresponding improvement in Lemmas 1 and 10.

4. THE EULER MINIMUM FUNCTION AND THE DISCRIMINATOR

For $n=1, 2$, and 3, the behavior of the discriminator is not very interesting; it is easy to show that $D(j,1)=1$, $D(j,2)=2$, $D(2j-1,3)=3$, and $D(2j,3)=6$ for every j in $\mathbb{N}$. From now on we assume that n is an arbitrary fixed integer ≥ 4. We establish a connection between the Euler minimum function and discriminators.

First, we prove a lemma ("the push-up lemma") that can be used, given an arbitrary k, to find a j such that $D(j,n)\ge k$. In the proof, the following result on $e(k)$, the maximum of the exponents in the canonical prime factorization of k, is needed.

Lemma 11: $e(k)\le\varphi(k)$.

Proof: For $k=1$ there is nothing to prove. If $k>1$, there is a prime p and an exponent $e(k)\ge 1$ such that $p^{e(k)}\| k$. Then $e(k)\le 2^{e(k)-1}\le p^{e(k)-1}(p-1)\le\varphi(k)$. □

For convenience, we call a pair of integers r, s with $1<r\le s\le n$ an *n-pair*. When both r and s are coprime with k, the n-pair (r, s) is said to be coprime with k.

Lemma 12 ("push-up lemma"): For $n\ge 4$ and arbitrary k, we have $D(\varphi(k),n)\ne k$.

Proof: It suffices to exhibit an n-pair (r, s) such that $r^{\varphi(k)}\equiv s^{\varphi(k)} \pmod{k}$. We show that (2, 4) meets this requirement. Let $f=\mathrm{ord}_2 k$, then $2^{\varphi(k)}\equiv 1 \pmod{k/2^f}$. By Lemma 11 and the definition of $e(k)$, it follows that $f\le e(k)\le\varphi(k)$, so $2^{\varphi(k)}\equiv 4^{\varphi(k)} \pmod{k}$. □

We will now use the push-up lemma to prove that there is a connection between the Euler minimum function and discriminators.

Theorem 2: If $n\ge 4$ and $p>n/2$ and p^{a} is a power of p for which $E(p^{\alpha})\ge n$, and if $p^{\alpha}\,|\,\mathrm{ord}_{E(p^{\alpha})}(r/s)$ for every n-pair (r, s) coprime with $E(p^{\alpha})$, then $D(a_{e(p^{\alpha})-1},n)=E(p^{\alpha})$.

Proof: Put $k=E(p^{\alpha})$. By the push-up lemma $D(a_{k-1},n)\ge k$. We claim that $D(a_{k-1},n)=k$. Put $j=a_{k-1}$. Notice that it suffices to show that there does not exist an n-pair (r, s) such that $r^j\equiv s^j \pmod{k}$. To this end, assume that such integers do exist. Since the smallest prime divisor of k is not less than p by Corollary 1(ii), it follows from $p>n/2$ that at least one of gcd(r, k) and gcd(s, k) equals one, but then both gcd(r, k) and gcd(s, k) equal one [so the n-pair (r, s) is coprime with k]; thus, $(r/s)^j\equiv 1 \pmod{k}$ and, therefore, j is a multiple of $\mathrm{ord}_{E(p^{\alpha})}(r/s)$. Since this order is divisible by p^{α} by assumption, it follows by the definition of a_{k-1} that there is an $\ell<k$ [$=E(p^{a})$], so the theorem is proved. □

Corollary: Suppose that n, p, and α satisfy the hypothesis of Theorem 2. Then $E(p^{\alpha})$ is in $D(\mathbb{N}, m)$ for m in $\{4, \ldots, n\}$.

Remark: In Table 1, some triples $(k, E(k), n_{\max})$ are recorded with k of the form p^{α}, with p^{α} and $n_{\max}$ satisfying the hypothesis of Theorem 2. Furthermore, $n_{\max}$ is the smallest integer ≥ 4 such that p^{α} and $n_{\max}+1$ do not satisfy the hypothesis of Theorem 2.

TABLE 1. Numerical Material Related to Theorem 2

k	$E(k)$	$n_{\max}$	k	$E(k)$	$n_{\max}$	k	$E(k)$	$n_{\max}$	k	$E(k)$	$n_{\max}$
7	29	4	13	53	6	17	103	8	19	191	4
25	101	4	27	81	4	31	311	5	37	149	9
43	173	12	47	283	12	49	197	5	59	709	18
61	367	12	67	269	12	71	569	14	73	293	16
79	317	13	97	389	16	101	607	22	103	619	21
107	643	17	127	509	21	137	823	18	139	557	18
151	907	25	163	653	21	169	677	9	193	773	21

If $(E(k), n_{\max})$ is a pair in the table, then $E(k) \in D(\mathbb{N}, m)$ for every $m \in \{4, \ldots, n_{\max}\}$.

The next theorem can be regarded as a special case of Theorem 2. It shows that the hypothesis of Theorem 2 can be weakened at the cost of generality.

Theorem 3: Let $n \geq 4$ and $p \geq n$ be such that $2p+1$ is prime. Then $D(a_{2p}, n) = 2p+1$.

Proof: Notice that $\{p : 2p+1 \text{ is prime}, \ p \geq 3\} = \{p : E(p) = 2p+1\}$. Let (r, s) be an n-pair. Since $2p+1 \nmid r-s$ and $2p+1 \nmid r+s, r^2 \not\equiv s^2 \pmod{2p+1}$. Therefore, $p \mid \operatorname{ord}_{E(p)}(r/s)$ for every n-pair (r, s) and so the result follows from Theorem 2. □

Remark: The primes in the set $\{p : 2p+1 \text{ is prime}, \ p \geq 3\}$ are called *Sophie Germain* primes. They were first considered in the study of Fermat's last theorem.

From the results in [4], it follows that $D(j, n)$ is squarefree for every fixed $j \geq 2$ and every n sufficiently large. We proceed to show that there are values of n and primes p such that p^e is in $D(\mathbb{N}, n)$ for infinitely many n. For convenience, we call these primes *n-discriminator primes*. Notice that p^e with e large is far from being squarefree. So, if p^e is in $D(\mathbb{N}, n)$ for some large e, the number p^e can be regarded as an exceptional value of the discriminator.

Lemma 13: Suppose p is odd. If $a^g \equiv 1+kp \pmod{p^2}$, then $a^{p^{m-1}g} \equiv 1+kp^m \pmod{p^{1+m}}$.

Proof: The proof is left as an exercise for the interested reader. □

When $\gcd(r, p) = 1$, we have $r^{p-1} = 1 + q_r(p)p$, with $q_r(p)$ an integer. This integer is called the *Fermat quotient* of p, with base r.

Theorem 4: If $n \geq 4, p \in E, p > n/2, q_2(p) \not\equiv 0 \pmod{p}$ and $q_r(p) \not\equiv q_s(p) \pmod{p}$ for every n-pair (r, s) coprime with p, then p is an n-discriminator prime.

Proof: By the hypothesis on p and Lemma 13, it follows that $r^{p^{e-1}(p-1)} \not\equiv s^{p^{e-1}(p-1)} \pmod{p^{e+1}}$ for every positive integer e and for every n-pair (r, s) coprime with p. Since $p > n/2$, it even holds true for every n-pair (r, s). Notice that this incongruence implies $p^e \mid \text{ord}_{p^{e+1}}(r/s)$ for every $e \geq 1$. Since p is in E, there are infinitely many exponents f such that $E(p^f) = p^{f+1}$. Then, for all sufficiently large of these f, there exists a j_f such that $D(j_f, n) = p^{f+1}$, by Theorem 2. So p is an n-discriminator prime. □

Corollary: If p is an n-discriminator prime satisfying the hypothesis of Theorem 4, p is an m-discriminator prime for m in $\{4, \ldots, n\}$.

Remark: Fix some p. Suppose there is an n such that n and p satisfy the hypothesis of Theorem 4. Then define $n_{\max}$ to be the largest n such that $n_{\max}$ and p satisfy the hypothesis of Theorem 4. Notice that $n_{\max}$ exists ($n_{\max} < 2p$). The entries in Table 2 result, after some easy computations, on using Theorem 4 and Lemma 4.

TABLE 2. Numerical Material Related to Theorem 4

n	n-Discriminator Primes
4	3, 7, 13, 19, 31
5	13, 19, 31
6	13, 19, 31
7	13, 19, 31
8	19, 31
9	19, 31
10	19, 31
11	31
12	31
13	31
14	31

If p is in the row headed n, then there are infinitely many e such that $p^e \in D(\mathbb{N}, n)$.

Our final theorem shows that the condition $p > n/2$ in Theorem 4 is necessary for p to be an n-discriminator prime.

Theorem 5: If $p \leq n/2$, then p is not an n-discriminator prime.

To prove this, we need some preparatory lemmas. They give upper bounds for $D(j, n)$ that, with harder work, are not too difficult to improve upon. For our purposes, the given bounds will do, however.

Let $p_1, p_2, p_3, \ldots$ denote the sequence of rational primes and $[x]$ the greatest integer $\leq x$.

Lemma 14: $D(j, n) \leq p_{[jn^2 \log n/\log 4]+1}$ for all positive integers j and n.

Proof: For $n = 1$ the assertion is obviously correct. So assume $n > 1$. Let Diff(j, n) denote the set $\{s^j - r^j \mid 1 \leq r < s \leq n\}$. If p is a prime such that p divides none of the members of Diff(j, n), then $1^j, \ldots, n^j$ are pairwise incongruent modulo p and so $D(j, n) \leq p$. Since a number m has at most $[\log m/\log 2]$ different prime factors, the numbers in the set Diff(j, n) contain at most $[jn^2 \log n/\log 4]$ different prime factors. Therefore, there is a prime $q \leq p_{[jn^2 \log n/\log 4]+1}$ such that $1^j, \ldots, n^j$ are pairwise incongruent modulo q. Thus, $D(j, n) \leq q \leq p_{[jn^2 \log n/\log 4]+1}$. □

Lemma 15: $D(j,n) \ll_n j\log(j+1)$.

Proof: The proof is immediate from Lemma 14 and the estimate $p_n = O(n\log n)$, which follows from the Prime Number Theorem. □

Proof of Theorem 5: Suppose $p \le n/2$. Now in case $D(j,n) = p^e$ for some integers j and e, it follows that $e > j$, for if $e \le j$, then $p^j \equiv (2p)^j \pmod{p^e}$. So if p is an n-discriminator prime, there exist infinitely many j such that $D(j,n) \ge p^{j+1}$. However, this contradicts Lemma 15. □

ACKNOWLEDGMENT

We thank Prof. R. Tijdeman for proofreading early versions of this paper and Prof. M. N. Huxley for suggesting a method for obtaining a nontrivial lower bound for $\operatorname{lcm}(\varphi(1), \ldots, \varphi(k))$ as a function of k.

REFERENCES

1. L. K. Arnold, S. J. Benkoski, & B. J. McCabe. "The Discriminator (A Simple Application of Bertrand's Postulate)." *Amer. Math. Monthly* **92** (1985):275-77.
2. E. Bach & J. Sorenson. "Explicit Bounds for Primes in Residue Classes." To appear in *Math. Comp.*
3. M. Barcau. "A Sharp Estimate of the Discriminator." *Nieuw Arch. Wisk.* **6** (1988):247-50.
4. P. S. Bremser, P. Schumer, & L. C. Washington. "A Note on the Incongruence of Consecutive Integers to a Fixed Power." *J. Number Theory* **35** (1990):105-08.
5. R. E. Dressler. "A Property of the φ and σ_j Functions." *Compositio Math.* **31** (1975):115-18.
6. P. Erdös. "Some Remarks on a Paper of McCarthy." *Canad. Math. Bull.* **1** (1958):71-75.
7. P. Erdös. "Remarks and Corrections to My Paper 'Some Remarks on a Paper of McCarthy.'" *Canad. Math. Bull.* **3** (1960):127-29.
8. E. Fouvry. "Théorème de Brun-Titchmarsh: Application au Théorème de Fermat." *Invent. Math.* **79** (1985):383-407.
9. H. J. Kanold. "Elementare Bertrachtungen zur Primzahltheorie." *Arch. Math.* **14** (1963): 147-51.
10. D. H. Lehmer. "The Distribution of Totatives." *Canad. J. Math.* **7** (1955):347-57.
11. P. J. McCarthy. "Note on the Distribution of Totatives." *Amer. Math. Monthly* **64** (1957): 585-86.
12. P. Moree. "On the Incongruence of Consecutive Polynomial Values." Preprint.
13. P. Moree & G. L. Mullen. "Dickson Polynomial Discriminators." Preprint.
14. P. Ribenboim. *The Book of Prime Number Records.* New York: Springer-Verlag, 1989 (2nd ed., 1990).
15. A. Schinzel & W. Sierpinski. "Sur certain hypothèses concernant les nombres premiers." *Acta Arith.* **4** (1958):185-208.
16. P. Schumer. "On the Incongruence of Consecutive Cubes." *Math. Student* **58** (1990):42-48.
17. P. Schumer & J. Steinig. "On the Incongruence of Consecutive Fourth Powers." *Elem. Math.* **43** (1988):145-49.

AMS Classification Numbers: 11A25, 11A07

❖❖❖

A NOTE ON A GENERAL CLASS OF POLYNOMIALS, PART II

Richard André-Jeannin
IUT GEA, Route de Romain, 54400 Longwy, France
(*Submitted February 1994*)

1. INTRODUCTION

In an earlier article [1] the author has discussed the properties of a set of polynomials $\{U_n(p,q;x)\}$ defined by

$$U_n(p,q;x)=(x+p)U_{n-1}(p,q;x)-qU_{n-2}(p,q;x),\ n\geq 2, \tag{1.1}$$

with $U_0(p,q;x)=0$ and $U_1(p,q;x)=1$.

Here and in the sequel the parameters p and q are arbitrary real numbers, and we denote by α,β the numbers such that $\alpha+\beta=p$ and $\alpha\beta=q$.

The aim of the present paper is to investigate the companion sequence of polynomials $\{V_n(p,q;x)\}$ defined by

$$V_n(p,q;x)=(x+p)V_{n-1}(p,q;x)-qV_{n-2}(p,q;x),\ n\geq 2, \tag{1.2}$$

with $V_0(p,q;x)=2$ and $V_1(p,q;x)=x+p$.

The first few terms of the sequence $\{V_n(p,q;x)\}$ are

$$\begin{aligned}
&V_2(p,q;x)=(p^2-2q)+2px+x^2,\\
&V_3(p,q;x)=(p^3-3pq)+(3p^2-3q)x+3px^2+x^3,\\
&V_4(p,q;x)=(p^4-4p^2q+2q^2)+(4p^3-8pq)x+(6p^2-4q)x^2+4px^3+x^4.
\end{aligned}$$

We see by induction that there exists a sequence $\{d_{n,k}(p,q)\}_{\substack{n\geq 1\\ k\geq 0}}$ of numbers such that

$$V_n(p,q;x)=\sum_{k\geq 0}d_{n,k}(p,q)x^k,\ \underline{n\geq 1}, \tag{1.3}$$

with $d_{n,k}(p,q)=0$ if $k\geq n+1$ and $d_{n,k}(p,q)=1$ if $k=n$. For the sake of convenience, we define the sequence $\{d_{0,k}(p,q)\}$ by

$$d_{0,0}(p,q)=1 \quad\text{and}\quad d_{0,k}(p,q)=0 \text{ if } k\geq 1. \tag{1.4}$$

Notice that $V_0(p,q;x)=2=2d_{0,0}(p,q)$.

Special cases of $\{V_n(p,q;x)\}$ which interest us are the Lucas polynomials $L_n(x)$ [2], the Pell-Lucas polynomials $Q_n(x)$ [7], the second Fermat polynomial sequence $\theta_n(x)$ [8], and the Chebyschev polynomials of the first kind $T_n(x)$ given by

$$\begin{aligned}
V_n(0,-1;x)&=L_n(x),\\
V_n(0,-1;2x)&=Q_n(x),\\
V_n(0,2;x)&=\theta_n(x),\\
V_n(0,1;2x)&=2T_n(x).
\end{aligned} \tag{1.5}$$

Another interesting case is the Morgan-Voyce recurrence ([1], [5], [9], [10]. and [11]) given by $p=2$ and $q=1$ (or $\alpha=\beta=1$). In the sequel, we shall denote by $C_n(x)=V_n(2,1;x)$ this new kind of Morgan-Voyce polynomials, defined by

$$C_0(x)=2,\ C_1(x)=x+2,\ \text{and}\ C_n(x)=(x+2)C_{n-1}(x)-C_{n-2}(x),\ n\geq 2. \tag{1.6}$$

Remark 1.1: One can notice that $C_n(x^2)=L_{2n}(x)$. Actually, it is well known and readily proven that the sequence $\{L_{2n}(x)\}$ satisfies the recurrence relation $L_{2n}(x)=(x^2+2)L_{2n-2}(x)-L_{2n-4}(x)$, where $L_0(x)=2$ and $L_2(x)=x^2+2$. The result follows by this and (1.6).

It is clear that the sequence $\{V_n(p,q;0)\}$ is the generalized Lucas sequence defined by

$$V_n(p,q;0)=pV_{n-1}(p,q;0)-qV_{n-2}(p,q;0),\ n\geq 2,$$

with $V_0(p,q;0)=2$ and $V_1(p,q;0)=p$. Therefore, $V_n(p,q;0)=\alpha^n+\beta^n$. By (1.3), notice that

$$d_{n,0}(p,q)=V_n(p,q;0)=\alpha^n+\beta^n,\quad \text{for } n\geq 1. \tag{1.8}$$

More generally, our aim is to express the coefficient $d_{n,k}(p,q)$ as a polynomial in (α,β) and as a polynomial in (p,q).

2. PRELIMINARIES

In this section we shall gather the results about polynomials $\{U_n(p,p;x)\}$ (1.1) which will be needed in the sequel. The reader may wish to consult [1].

Define the sequence $\{c_{n,k}(p,q)\}_{\substack{n\geq 0\\ k\geq 0}}$ by

$$U_{n+1}(p,q;x)=\sum_{k\geq 0}c_{n,k}(p,q)x^k, \tag{2.1}$$

where $c_{n,k}(p,q)=0$, for $k>n$. It was shown in [1] that

For every $n\geq 2$ and $k\geq 1$,

$$c_{n,k}(p,q)=pc_{n-1,k}(p,q)-qc_{n-2,k}(p,q)+c_{n-1,k-1}(p,q). \tag{2.2}$$

For every $n\geq 0$ and $k\geq 0$,

$$c_{n,k}(p,q)=\sum_{i+j=n-k}\binom{k+i}{k}\binom{k+j}{k}\alpha^i\beta^j. \tag{2.3}$$

If $p^2=4q$, then $\alpha=\beta=p/2$ and (2.3) becomes

$$c_{n,k}(p,q)=\binom{n+k+1}{2k+1}(p/2)^{n-k}. \tag{2.4}$$

If $p=0$, then $\alpha=-\beta=p$, $\alpha^2=-q$, and (2.3) becomes

$$\begin{cases} c_{n,n-2k}(0,q)=(-1)^k\binom{n-k}{k}q^k, & n-2k\geq 0,\\ c_{n,n-2k-1}(0,q)=0, & n-2k-1\geq 0. \end{cases} \tag{2.5}$$

For every $n \geq 0$ and $k \geq 0$,

$$c_{n,k}(p,q) = \sum_{r=0}^{[(n-k)/2]} (-1)^r \binom{n-r}{r} \binom{n-2r}{k} q^r p^{n-2r-k}. \tag{2.6}$$

The generating function of the sequence $\{U_n(p,q;x)\}$ is given by

$$f(p,q;x,t) = \sum_{n\geq 0} U_{n+1}(p,q;x)t^n = \frac{1}{1-(x+p)t+qt^2}. \tag{2.7}$$

The generating function $F_k(p,q;t)$ of the k^{th} column of coefficients $c_{n,k}(p,q)$ is given by

$$F_k(p,q;t) = \sum_{n\geq 0} c_{n+k,k} t^n = \frac{1}{(1-pt+qt^2)^{k+1}}. \tag{2.8}$$

For every $n \geq 0$, we have

$$U_{n+1}(p,q;0) = \sum_{r=0}^{[n/2]} (-1)^r \binom{n-r}{r} q^r p^{n-2r}. \tag{2.9}$$

3. THE TRIANGLE OF COEFFICIENTS

One can display the sequence $\{d_{n,k}(p,q)\}_{\substack{n\geq 0\\ k\geq 0}}$ (1.3) in a triangle, thus,

TABLE 3.1

$n \backslash k$	0	1	2	3	4
0	1	0	0	0	0
1	p	1	0	0	0
2	p^2-2q	$2p$	1	0	0
3	p^3-3pq	$3p^2-3q$	$3p$	1	0
4	$p^4-4p^2q+2q^2$	$4p^3-8pq$	$6p^2-4q$	$4p$	1

For instance, the triangle of coefficients of the sequence $\{C_n(x)\}$ (1.6) is

TABLE 3.2

$n \backslash k$	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	2	1	0	0	0	0	0
2	2	4	1	0	0	0	0
3	2	9	6	1	0	0	0
4	2	16	20	8	1	0	0
5	2	25	50	35	10	1	0
6	2	36	105	112	54	12	1

Theorem 3.1: For every $n \geq 0$ and $k \geq 0$ we have

$$d_{n,k+1}(p,q) = \frac{1}{k+1}\frac{\partial d_{n,k}}{\partial p}.$$

Proof: One can suppose that $n \geq 1$ and it is clear by (1.2) that $V_n(p,q;x) = V_n(0,q;x+p)$. From this, we see that $V_n^{(k)}(p,q;x) = V_n^{(k)}(0,q;x+p)$, where the superscript in parentheses denotes the k^{th} derivative with respect to x. Thus, by Taylor's formula and (1.3),

$$d_{n,k}(p,q) = \frac{V_n^{(k)}(p,q;0)}{k!} = \frac{V_n^{(k)}(0,q;p)}{k!}. \tag{3.1}$$

Notice that these equalities are valid for every value of p. Now let us differentiate the first and the last member of (3.1) with respect to p (q being fixed) to get

$$\frac{\partial d_{n,k}}{\partial p} = \frac{V_n^{(k+1)}(0,q;p)}{k!} = (k+1)d_{n,k+1}(p,q).$$

The result can be checked against Table 3.1.

Remark 3.1: One can get the same result for the coefficient $c_{n,k}(p,q)$ (2.1), namely,

$$\frac{\partial c_{n,k}}{\partial p} = (k+1)c_{n,k+1}(p,q).$$

Comparing the coefficients of x^k in the two members of (1.3), we see by (1.2) that, for $n \geq 2$ and $k \geq 1$,

$$d_{n,k}(p,q) = d_{n-1,k-1}(p,q) + p d_{n-1,k}(p,q) - q d_{n-2,k}(p,q), \tag{3.2}$$

which is a relation similar to (2.2). From this, one can obtain another recurrence relation.

Theorem 3.2: For every $n \geq 1$ and $k \geq 1$, we have

$$\begin{aligned} d_{n,k}(p,q) &= \beta d_{n-1,k}(p,q) + \sum_{i=0}^{n-1} \alpha^{n-i-1} d_{i,k-1}(p,q) \\ &= \alpha d_{n-1,k}(p,q) + \sum_{i=0}^{n-1} \beta^{n-1-i} d_{i,k-1}(p,q). \end{aligned} \tag{3.3}$$

Proof: In fact, (3.3) is clear by direct computation for $n \leq 2$ [recall that $d_{0,0}(p,q) = 1$ and that $\alpha + \beta = p$]. Using (3.2), we see that the end of the proof is analogous to the proof of Theorem 1 in [1].

For instance, in the case of the Morgan-Voyce polynomial $C_n(x)$ (1.6) we have $\alpha = \beta = 1$, and (3.2) becomes (see Table 3.2)

$$d_{n,k}(2,1) = d_{n-1,k}(2,1) + \sum_{i=0}^{n-1} d_{i,k+1}(2,1),$$

which is the recursive definition of the DFF and DFFz triangles (see [3], [4], [5]) known to be the triangle of coefficients of the usual Morgan-Voyce polynomials.

4. DETERMINATION OF $d_{n,k}(p,q)$ AS A POLYNOMIAL IN (α, β)

The determination of $d_{n,k}(p,q)$ will proceed easily from the following lemmas. The first of these is a well-known result on second-order recurring sequences that can be proven by induction using (1.1) and (1.2).

Lemma 4.1: For every $n \geq 1$, we have

$$V_n(p,q;x) = U_{n+1}(p,q;x) - qU_{n-1}(p,q;x). \tag{4.1}$$

Lemma 4.2: For every $n \geq 0$, we have

$$V_n'(p,q;x) = nU_n(p,q;x), \tag{4.2}$$

where the prime represents the first derivative w.r.t. x.

Proof: By (1.1) and (1.2), the result is clear if $n = 0$ or $n = 1$. Assuming the result is true for $n \geq 1$, we obtain by (1.2),

$$\begin{aligned} V_{n+1}'(p,q;x) &= (x+p)V_n'(p,q;x) - qV_{n-1}'(p,q;x) + V_n(p,q;x) \\ &= n[(x+p)U_n(p,q;x) - qU_{n-1}(p,q;x)] + V_n(p,q;x) + qU_{n-1}(p,q;x) \\ &= nU_{n+1}(p,q;x) + U_{n+1}(p,q;x) \quad \text{by (1.1) and (4.1),} \\ &= (n+1)U_{n+1}(p,q;x). \end{aligned}$$

This concludes the proof of Lemma 4.2.

Lemma 4.3: For every $n \geq 1$ and $k \geq 1$, we have

$$d_{n,k}(p,q) = \frac{n}{k} c_{n-1,k-1}(p,q). \tag{4.3}$$

Proof: Comparing the coefficients of x^{k-1} in the two members of (4.2) we see by (1.3) and (2.1) that

$$kd_{n,k}(p,q) = nc_{n-1,k-1}(p,q), \; n \geq 1, k \geq 1.$$

Lemma 4.3 and (2.3) yield

Theorem 4.1: For every $n \geq 1$ and $k \geq 1$, we have

$$d_{n,k}(p,q) = \frac{n}{k} \sum_{i+j=n-k} \binom{k+i-1}{k-1}\binom{k+j-1}{k-1} \alpha^i \beta^j. \tag{4.4}$$

Remark 4.1: Recall from (1.8) that $d_{n,0}(p,q) = \alpha^n + \beta^n$ (for $n > 0$), an expression which can be compared with (4.4).

Let us examine two particular cases.

(i) Firstly, supposing that $p^2 = 4q$ (or $\alpha = \beta = p/2$), then by (2.4) we see that equation (4.3) becomes

$$\begin{aligned} d_{n,k}(p,q) &= \frac{n}{k}\binom{n+k-1}{2k-1}(p/2)^{n-k},\ n \geq 1, k \geq 1, \\ &= \frac{2n}{n+k}\binom{n+k}{2k}(p/2)^{n-k}. \end{aligned} \tag{4.5}$$

Notice that this last expression is again valid if $k = 0$, since $d_{n,0}(p,q) = \alpha^n + \beta^n = 2(p/2)^n$. We also see that $d_{n,1}(p,q) = n^2(p/2)^{n-1}$ (see Table 3.2, where $p = 2$). For instance, the decomposition of the polynomial $C_n(x)$ (1.6) is given by

$$\begin{aligned} C_n(x) &= 2 + \sum_{k=1}^{n} \frac{n}{k}\binom{n+k-1}{2k-1}x^k, \text{ for } n \geq 1, \\ &= 2\sum_{k=0}^{n} \frac{n}{n+k}\binom{n+k}{2k}x^k. \end{aligned}$$

(ii) Secondly, supposing that $p = 0$, we have $\alpha = -\beta$, $q = -\alpha^2$, and by (2.5) we see that equation (4.3) becomes, for $n \geq 1$,

$$\begin{aligned} d_{n,n-2k}(0,q) &= \frac{n}{n-2k}(-1)^k\binom{n-1-k}{k}q^k \\ &= \frac{n}{n-k}(-1)^k\binom{n-k}{k}q^k, \text{ for } n-2k \geq 1. \end{aligned} \tag{4.6}$$

Notice that the last member is again defined for $n-2k = 0$ $(k \geq 1)$ with value $2(-1)^k q^k$. Now, by Remark 4.1, we get that

$$d_{2k,0}(0,q) = \alpha^{2k} + \beta^{2k} = 2(-1)^k q^k, \text{ for } k \geq 1.$$

We deduce from these remarks that (4.6) is again true if $n = 2k$ $(k \geq 1)$. On the other hand, we see by (2.5) that equation (4.3) becomes

$$d_{n,n-2k-1}(0,q) = 0, \text{ for } n-2k-1 \geq 1. \tag{4.7}$$

Now by Remark 4.1 we have

$$d_{2k+1,0}(0,q) = \alpha^{2k+1} + \beta^{2k+1} = 0, \text{ for } k \geq 0.$$

We deduce from these remarks that (4.7) is again true if $n-2k-1 = 0$ $(k \geq 0)$. Now, by (1.3),

$$\begin{aligned} V_n(0,q;x) &= \sum_{k=0}^{n} d_{n,k}(0,q)x^k = \sum_{k=0}^{n} d_{n,n-k}(0,q)x^{n-k} \\ &= \sum_{k=0}^{[n/2]} d_{n,n-2k}(0,q)x^{n-2k}. \end{aligned}$$

Thus, by (4.6) and (4.7) we get

$$V_n(0,q;x) = \sum_{k=0}^{[n/2]} (-1)^k \frac{n}{n-k}\binom{n-k}{k}q^k x^{n-2k}, \text{ for } n \geq 1. \tag{4.8}$$

If $p = 0$ and $q = -1$, we obtain the known decomposition of Lucas polynomials $L_n(x)$ and of Pell-Lucas polynomials $Q_n(x) = L_n(2x)$ (see [7]), namely,

$$L_n(x) = \sum_{k=0}^{[n/2]} \frac{n}{n-k}\binom{n-k}{k} x^{n-2k}, \text{ for } n \geq 1.$$

The reader can also obtain similar formulas for the Chebyschev polynomials of the first kind ($p = 0, q = 1$), and for the second Fermat polynomial sequence ($p = 0, q = 2$).

5. DETERMINATION OF $d_{n,k}(p, q)$ AS A POLYNOMIAL IN (p, q)

Theorem 5.1: For every $n \geq 1$ and $k \geq 0$, we have

$$d_{n,k}(p, q) = \sum_{r=0}^{[(n-k)/2]} (-1)^r \frac{n}{n-r}\binom{n-r}{r}\binom{n-2r}{k} q^r p^{n-2r-k}. \tag{5.1}$$

Proof: By (3.1) we know that

$$d_{n,k}(p,q) = \frac{V_n^{(k)}(0,q;\, p)}{k!},$$

and by (4.8) one can express the right member as

$$\sum_{r=0}^{[n/2]} (-1)^r \frac{n}{n-r}\binom{n-r}{r} q^r \frac{(n-2r)\cdots(n-2r-k+1)}{k!} p^{n-2r-k}$$

$$= \sum_{r=0}^{[(n-k)/2]} (-1)^r \frac{n}{n-r}\binom{n-r}{r}\binom{n-2r}{k} q^r p^{n-2r-k}.$$

This completes the proof of Theorem 5.1.

Remark 5.1: If $k = 0$, we get by (1.8) the known Waring formula, namely,

$$\alpha^n + \beta^n = \sum_{r=0}^{[n/2]} (-1)^r \frac{n}{n-r}\binom{n-r}{r} (\alpha\beta)^r (\alpha+\beta)^{n-2r}, \text{ for } n \geq 1.$$

6. GENERATING FUNCTIONS

Define the generating function of the sequence $\{V_n(p, q;\, x)\}$ by

$$g(p, q;\, x, t) = V_0(p, q;\, x)/2 + \sum_{n\geq 1} V_n(p, q;\, x) t^n. \tag{6.1}$$

For brevity, we put $g(p, q;\, x, t) = g(x, t)$ and $V_n(p, q;\, x) = V_n(x)$. By (6.1) and (1.2) we get, since $V_0(x) = 2$ and $V_1(x) = x + p$,

$$g(x, t) = 1 + (x+p)t + (x+p)t\sum_{n\geq 2} V_{n-1}(x)t^{n-1} - qt^2 \sum_{n\geq 2} V_{n-2}(x)t^{n-2}$$

$$= 1 + (x+p)t + (x+p)t[g(x, t) - 1] - qt^2[g(x, t) + 1],$$

and from this we deduce easily that

$$g(x, t) = \frac{1 - qt^2}{1 - (x+p)t + qt^2}. \tag{6.2}$$

Let us define now the generating function of the k^{th} column of the triangle $d_{n,k}(p,q)$ in Table 3.1 by

$$G_k(p,q;t) = \sum_{n\ge 0} d_{n+k,k}(p,q)t^n, \; k \ge 0. \tag{6.3}$$

From (6.2), one can obtain a closed expression for the function G_k, namely,

Theorem 6.1: For every $k \ge 0$, we have

$$G_k(p,q;t) = \frac{1-qt^2}{(1-pt+qt^2)^{k+1}}. \tag{6.4}$$

Proof: For brevity, we omit parameters p and q in expressions for $g(p,q;x,t)$, $V_n(p,q;x)$, $d_{n,k}(p,q)$, and $G_k(p,q;t)$. If $k = 0$, we have by (6.3), (1.3), and (1.4)

$$\begin{aligned} G_0(t) &= \sum_{n\ge 0} d_{n,0}t^n = 1 + \sum_{n\ge 1} V_n(0)t^n \\ &= g(0,t) = \frac{1-qt^2}{1-pt+qt^2}, \text{ by (6.2).} \end{aligned}$$

Assuming now that $k \ge 1$, (6.1) and (6.2) yield

$$\frac{k!\,t^k(1-qt^2)}{(1-(x+p)t+qt^2)^{k+1}} = \frac{\partial^k}{\partial x^k} g(x,t) = \sum_{n\ge 1} V_n^{(k)}(x)t^n = \sum_{n\ge 0} V_{n+k}^{(k)}(x)t^{n+k},$$

since $V_n(x)$ is a polynomial of degree n.

Put $x = 0$ in the last formula and recall that $d_{n+k,k} = \frac{V_{n+k}^{(k)}(0)}{k!}$ by (1.3) and Taylor's formula, to obtain

$$\frac{1-qt^2}{(1-pt+qt^2)^{k+1}} = \sum_{n\ge 0} d_{n+k,k}t^n = G_k(t).$$

Hence, the theorem.

Formulas (6.2) and (6.4) can be compared with (2.7) and (2.8).

7. RISING DIAGONAL FUNCTIONS

Define the rising diagonal functions $\Pi_n(p,q;x)$ of the sequence $\{d_{n,k}(p,q)\}$ by

$$\Pi_n(p,q;x) = \sum_{k=0}^{n} d_{n-k,k}(p,q)x^k = \sum_{k=0}^{[n/2]} d_{n-k,k}(p,q)x^k, \; n \ge 1. \tag{7.1}$$

From Table 3.1, notice that

$$\Pi_1(x) = p,\; \Pi_2(x) = (p^2-2q)+x, \text{ and } \Pi_3(x) = (p^3-3pq)+2px, \tag{7.2}$$

where, for brevity, we put $\Pi_n(x)$ for $\Pi_n(p,q;x)$.

Theorem 7.1: For every $n \ge 3$, we have

$$\Pi_n(x) = p\Pi_{n-1}(x) + (x-q)\Pi_{n-2}(x). \tag{7.3}$$

Proof: By (7.2), the statement holds for $n = 3$. Supposing the result is true for $n \geq 3$, we get by (7.1),

$$\Pi_{n+1}(x) = d_{n+1,0} + \sum_{k=1}^{[(n+1)/2]} d_{n+1-k,k}x^k.$$

Recall from (1.2) and (1.8) that $d_{n+1,0} = V_{n+1}(0) = pd_{n,0} - qd_{n-1,0}$ and notice that $n+1-k \geq n+1-[(n+1)/2] \geq 2$, since $n \geq 3$. By these remarks and (3.2), one can see that

$$\begin{aligned}\Pi_{n+1}(x) &= pd_{n,0} - qd_{n-1,0} + \sum_{k=1}^{[(n+1)/2]} (d_{n-k,k-1} + pd_{n-k,k} - qd_{n-1-k,k})x^k \\ &= p\sum_{k=0}^{[(n+1)/2]} d_{n-k,k}x^k - q\sum_{k=0}^{[(n+1)/2]} d_{n-1-k,k}x^k + x\sum_{k=0}^{[(n+1)/2]-1} d_{n-1-k,k}x^k \\ &= p\Pi_n(x) + (x-q)\Pi_{n-1}(x),\end{aligned}$$

since $[(n+1)/2] - 1 = [(n-1)/2]$. Hence, the theorem.

Corollary 7.1: For every $n \geq 1$, we have

$$\Pi_n(p,q;x) = U_{n+1}(p,q-x;0) - qU_{n-1}(p,q-x;0). \tag{7.4}$$

Proof: By (1.1) the sequence $\{U_n(p,q-x;0)\}$ satisfies the recurrence (7.3) with

$$U_0(p,q-x;0) = 0,\ U_1(p,q-x;0) = 1,\ U_2(p,q-x;0) = p,\ U_3(p,q-x;0) = (p^2-q) + x.$$

From this and (7.2), it is readily verified that (7.4) holds for $n = 1$ and $n = 2$, and the conclusion follows since the two members of (7.4) satisfy recurrence (7.3).

Corollary 7.2: For every $n \geq 1$, we have

$$\Pi_n(x) = \binom{n-[n/2]}{[n/2]}p^{n-2[n/2]}(x-q)^{[n/2]} + \sum_{r=0}^{[(n-2)/2]} p^{n-2-2r}(x-q)^r\left[\binom{n-r}{r}p^2 - \binom{n-2-r}{r}q\right].$$

Proof: From (2.9), we get that

$$U_{n+1}(p,q-x;0) = \sum_{r=0}^{[n/2]}\binom{n-r}{r}(x-q)^r p^{n-2r},$$

and the result follows by this and Corollary 7.1.

Let us examine two particular cases.

(i) If $x = q$, then by (7.1)

$$\Pi_n(p,q;q) = \sum_{k=0}^{[n/2]} d_{n-k,k}(p,q)q^k = p^{n-2}(p^2-q), \text{ for } n \geq 2.$$

For instance, if $p = 2$ and $q = 1$ [Morgan-Voyce polynomial $C_n(x)$ (1.6)], we get

$$\sum_{k=0}^{[n/2]} d_{n-k,k}(2,1) = 3\cdot 2^{n-2},\ n \geq 2.$$

(ii) If $p = 0$, then

$$\Pi_{2m}(0,q;x) = \sum_{k=0}^{m} d_{2m-k,k}(0,q)x^k = (x-q)^{m-1}(x-2q), \text{ for } m \geq 1.$$

For instance, if $p = 0$ and $q = 1$ (Chebyschev polynomials of the first kind), or if $p = 0$ and $q = 2$ (second Fermat polynomials), this identity, with slightly different notations, was noticed by Horadam [8].

8. ORTHOGONALITY OF THE SEQUENCE $\{V_n(p,q;x)\}$

In this section we shall suppose that $q > 0$. Consider the sequence $\{W_n(p,q;x)\}$ defined by

$$W_n(p,q;x) = 2q^{n/2}T_n\left(\frac{x+p}{2\sqrt{q}}\right), \tag{8.1}$$

where $T_n(x)$ is the n^{th} Chebyschev polynomial of the first kind. Notice that

$$\begin{cases} W_0(p,q;x) = 2, \\ W_1(p,q;x) = x+p. \end{cases} \tag{8.2}$$

The recurrence relation of Chebyschev polynomials yields, for $n \geq 2$,

$$\begin{aligned} W_n(p,q;x) &= 2q^{n/2}\left[\left(\frac{x+p}{\sqrt{q}}\right)T_{n-1}\left(\frac{x+p}{2\sqrt{q}}\right) - T_{n-2}\left(\frac{x+p}{2\sqrt{q}}\right)\right] \\ &= (x+p)\left[2q^{(n-1)/2}T_{n-1}\left(\frac{x+p}{2\sqrt{q}}\right)\right] - q\left[2q^{(n-2)/2}T_{n-2}\left(\frac{x+p}{2\sqrt{q}}\right)\right] \\ &= (x+p)W_{n-1}(p,q;x) - qW_{n-2}(p,q;x). \end{aligned} \tag{8.3}$$

From (8.2) and (8.3), we get that

$$W_n(p,q;x) = V_n(p,q;x), \text{ for } n \geq 0. \tag{8.4}$$

Recalling that the sequence $\{T_n(x)\}$ is orthogonal over $[-1,+1]$ with respect to the weight $(1-x^2)^{-1/2}$, we deduce from this that the sequence $\{V_n(p,q;x)\}$ is orthogonal over $[-p-2\sqrt{q}, -p+2\sqrt{q}]$ with respect to the weight $w(x) = (-x^2-2px-\Delta)^{-1/2}$, where $\Delta = p^2-4q$. The proof is similar to that in [1], Section 7.

If $\omega = \cos t$ $(0 \leq t \leq \pi)$, it is well known that $T_n(\omega) = \cos nt$. Thus, by (8.1) and (8.4) we have

$$V_n(p,q;-p+2\omega\sqrt{q}) = 2q^{n/2}T_n(\omega) = 2q^{n/2}\cos nt.$$

Hence, we see that the roots of $V_n(p,q;x)$ are given by

$$x_k = -p+2\sqrt{q}\cos\left(\frac{(2k+1)\pi}{2n}\right), \; n \geq 1; \; k = 0, \ldots, (n-1).$$

For instance, the roots of the Morgan-Voyce polynomial $C_n(x)$ (1.6) are

$$x_k = -2+2\cos\left(\frac{(2k+1)\pi}{2n}\right) = -4\sin^2\left(\frac{(2k+1)\pi}{4n}\right), \; k = 0, \ldots, (n-1).$$

By Remark 1.1 we know that $C_n(x^2) = L_{2n}(x)$. Thus, the roots of $L_{2n}(x)$ are given by (see [6])

$$x'_k = \pm 2i \sin\left(\frac{(2k+1)\pi}{4n}\right),\ k = 0, \ldots, (n-1),$$

where $i = \sqrt{-1}$. On the other hand, the roots of the second Fermat polynomial $\theta_n(x) = V_n(0,2;\, x)$ are

$$x_k = 2\sqrt{2} \cos\left(\frac{(2k+1)\pi}{2n}\right),\ k = 0, \ldots, (n-1).$$

9. CONCLUDING REMARK

In a future paper we shall investigate the differential properties of the sequences $\{U_n(p,q;\, x)\}$ and $\{V_n(p,q;\, x)\}$.

ACKNOWLEDGMENT

The author would like to thank the referee for helpful and detailed comments.

REFERENCES

1. R. André-Jeannin. "A Note on a General Class of Polynomials." *The Fibonacci Quarterly* **32.5** (1994):445-55.
2. M. Bicknell. "A Primer for the Fibonacci Numbers: Part VII." *The Fibonacci Quarterly* **8.4** (1970):407-20.
3. G. Ferri, M. Faccio, & A. D'Amico. "A New Numerical Triangle Showing Links with Fibonacci Numbers." *The Fibonacci Quarterly* **29.4** (1991):316-21.
4. G. Ferri, M. Faccio, & A. D'Amico. "Fibonacci Numbers and Ladder Network Impedance." *The Fibonacci Quarterly* **30.1** (1992):62-67.
5. G. Ferri, M. Faccio, & A. D'Amico. "The DFF and DFFz Triangles and Their Mathematical Properties." In *Applications of Fibonacci Numbers* **5**. Ed. A. N. Philippou, G. E. Bergum, & A. F. Horadam. Dordrecht: Kluwer, 1994.
6. V. E. Hoggatt, Jr., & Marjorie Bicknell. "Roots of Fibonacci Polynomials." *The Fibonacci Quarterly* **11.3** (1973):271-74.
7. A. F. Horadam & Br. J. M. Mahon. "Pell and Pell-Lucas Polynomials." *The Fibonacci Quarterly* **23.1** (1985):7-20.
8. A. F. Horadam. "Chebyschev and Fermat Polynomials for Diagonal Functions." *The Fibonacci Quarterly* **19.4** (1979):328-33.
9. J. Lahr. "Fibonacci and Lucas Numbers and the Morgan-Voyce Polynomials in Ladder Networks and in Electrical Line Theory." In *Fibonacci Numbers and Their Applications* **1:**141-61. Ed. A. N. Philippou, G. E. Bergum, & A. F. Horadam. Dordrecht: Kluwer, 1986.
10. M. N. S. Swamy. "Properties of the Polynomials Defined by Morgan-Voyce." *The Fibonacci Quarterly* **4.1** (1966):73-81.
11. M. N. S. Swamy. "Further Properties of Morgan-Voyce Polynomials." *The Fibonacci Quarterly* **6.2** (1968):165-75.

AMS Classification Numbers: 11B39, 33C25

SQUARES OF SECOND-ORDER LINEAR RECURRENCE SEQUENCES

Tom C. Brown
Department of Mathematics and Statistics, Simon Fraser University, Burnaby, B.C., Canada V5A1S6
tbrown@sfu.ca

Peter Jau-shyong Shiue
Department of Mathematical Sciences, University of Nevada, Las Vegas, NV 89154-4020
shiue@nevada.edu

(*Submitted February 1994*)

INTRODUCTION

Let us call a sequence $\{T_n\}$ $(n \geq 0)$ an "m^{th}-order sequence" if $\{T_n\}$ $(n \geq 0)$ satisfies an m^{th}-order linear recurrence relation with constant integer coefficients. (We allow constant terms to appear in our recurrence relations.) From now on we shall generally write simply $\{T_n\}$ rather than $\{T_n\}$ $(n \geq 0)$. It is well known ([2], [3]) that if $\{T_n\}$ is a second-order sequence then the sequence of squares $\{T_n^2\}$ is a third-order sequence. (It is also easy to show this directly.) It would be of interest to be able to describe all second-order sequences $\{T_n\}$ such that $\{T_n^2\}$ is a *second*-order sequence.

In this note we do this for certain *homogeneous* sequences $\{T_n\}$. That is, we assume that $\{T_n\}$ satisfies a recurrence of the form $T_0 = a, T_1 = b, T_{n+1} = cT_n - dT_{n-1}, n \geq 1$, where $a, b, c \neq 0$, $d \neq 0$ are integers, $ab \neq 0$, and $x^2 - cx + d = 0$ has distinct roots. It then turns out that $\{T_n^2\}$ satisfies a second-order linear recurrence (which we describe in Theorem 6) if and only if $d = 1$.

As an illustration of this, consider the sequence 1, 2, 7, 26, 97, 362, ... which satisfies the second-order recurrence $B_0 = 1, B_1 = 2, B_{n+1} = 4B_n - B_{n-1}, n \geq 1$. The sequence of squares $1^2, 2^2, 7^2, 26^2, 97^2, 362^2$, ... satisfies the second-order recurrence $S_0 = 1, S_1 = 4, S_{n+2} = 14S_{n+1} - S_n - 6$.

We also consider second-order sequences $\{T_n\}$ such that a slight perturbation of the sequence of squares $\{T_n^2\}$ is a second-order sequence. For example, the sequence 1, 1, 3, 7, 17, 41, 99, ... satisfies the second-order recurrence $B_0 = B_1 = 1, B_{n+2} = 2B_{n+1} + B_n$, and the "perturbed" sequence of squares $1^2, 1^2+1, 3^2, 7^2+1, 17^2, 41^2+1, 99^2$, ... satisfies the second-order recurrence $S_0 = 1$, $S_1 = 2$, $S_{n+2} = 6S_{n+1} - S_n - 2$.

We begin with some special cases using elementary techniques. Then, in the last section, we handle the general case using an old result of E. S. Selmer [3] which states: if $T_{n+1} = AT_n + BT_{n-1}$, $n \geq 1$, and $x^2 - Ax - B = (x-\alpha)(x-\beta), \alpha \neq \beta$, then $T_{n+1}^2 = CT_n^2 + DT_{n-1}^2 + ET_{n-2}^2, n \geq 2$, where $x^3 - Cx^2 - Dx - E = (x-\alpha^2)(x-\beta^2)(x-\alpha\beta)$.

MAIN RESULTS

We begin with some special cases for which we will use the following Lemma.

Lemma: Let $p \geq 4$ be any integer, let $\delta = \sqrt{\frac{p}{4}} + \sqrt{\frac{p}{4} - 1}$, and let $S_n = (\delta^n + \frac{1}{\delta^n})^2$, $n \geq 0$. Then these numbers S_n satisfy the following identities.

(a) For all $0 \le m \le n$, $(S_n - 2)(S_m - 2) = S_{n+m} + S_{n-m} - 4$.
[In particular, $(S_n - 2)^2 = S_{2n}$, so that S_{2n} is always a perfect square.]

(b) For all $0 \le m \le n$, $m \equiv n \pmod 2$, $S_n S_m = \left(S_{(n+m)/2} + S_{(n-m)/2} - 4\right)^2$.

[In particular, $S_{n+k}S_{n-k} = (S_n + S_k - 4)^2$ and $pS_{2n+1} = S_1 S_{2n+1} = (S_n + S_{n+1} - 4)^2$, so that S_{2n+1} is always a perfect square provided p is a perfect square.]

(c) For all $0 \le m \le n$, $m \equiv n \pmod 2$, $(S_n - 4)(S_m - 4) = \left(S_{(n+m)/2} - S_{(n-m)/2}\right)^2$.

[In particular, $(p-4)(S_{2n+2} - 4) = (S_1 - 4)(S_{2n+1} - 4) = (S_{n+1} - S_n)^2$, so that $S_{2n+1} - 4$ is always a perfect square provided $p - 4$ is a perfect square.]

(d) $S_{n+2} = (p-2)S_{n+1} - S_n - 2(p-4), n \ge 0$.

Proof: We prove part (d) in detail. The proofs of parts (a), (b), and (c) are very similar, and are omitted.

Note that $\frac{1}{\delta} = \sqrt{\frac{p}{4}} - \sqrt{\frac{p}{4} - 1}$, so that $(\delta + \frac{1}{\delta})^2 = p$. Then

$$
\begin{aligned}
pS_{n+1} = \left(\delta + \frac{1}{\delta}\right)^2 S_{n+1} &= \left[\left(\delta + \frac{1}{d}\right)\left(\delta^{n+1} + \frac{1}{\delta^{n+1}}\right)\right]^2 = \left[\left(\delta^{n+2} + \frac{1}{\delta^{n+2}}\right) + \left(\delta^n + \frac{1}{\delta^n}\right)\right]^2 \\
&= S_{n+2} + S_n + 2\left[\delta^{2n+2} + \frac{1}{\delta^{2n+2}} + \delta^2 + \frac{1}{\delta^2}\right] \\
&= S_{n+2} + S_n + 2\left[\left(\delta^{n+1} + \frac{1}{\delta^{n+1}}\right)^2 - 2 + \left(\delta + \frac{1}{\delta}\right)^2 - 2\right] \\
&= S_{n+2} + S_n + 2S_{n+1} + 2(p-4),
\end{aligned}
$$

that is, $S_{n+2} = (p-2)S_{n+1} - S_n - 2(p-4), n \ge 0$.

Theorem 1: Let $d \ge 3$ be an integer. Define the sequence $\{B_n\}$ $(n \ge 0)$ by $B_0 = 2, B_1 = d$, $B_{n+2} = dB_{n+1} - B_n$, $n \ge 0$. Then the sequence of squares $\{B_n^2\}$ $(n \ge 0)$ satisfies the second-order recurrence

$$B_{n+2}^2 = (d^2 - 2)B_{n+1}^2 - B_n^2 - 2(d^2 - 4), \ n \ge 0.$$

Proof: Solving the recurrence $B_0 = 2, B_1 = d, B_{n+2} = dB_{n+1} - B_n$ in the usual way gives

$$B_n = \delta^n + \frac{1}{\delta^n}, n \ge 0, \text{ where } \delta = \sqrt{\frac{d^2}{4}} + \sqrt{\frac{d^2}{4} - 1}, \ \ \frac{1}{\delta} = \sqrt{\frac{d^2}{4}} - \sqrt{\frac{d^2}{4} - 1}.$$

Let us now simplify the notation by setting $S_n = B_n^2, n \ge 0$. Then $S_n = (\delta^n + \frac{1}{\delta^n})^2$, $n \ge 0$, and by part (d) of the Lemma (with $p = d^2$), $S_{n+2} = (d^2 - 2)S_{n+1} - S_n - 2(d^2 - 4)$, $n \ge 0$.

Now we give a second-order sequence whose squares, when slightly perturbed, form a second-order sequence.

Theorem 2: Let $d \geq 1$ be an integer. Define the sequence $\{C_n\}$ $(n \geq 0)$ by $C_0 = 2, C_1 = d,$ $C_{n+2} = dC_{n+1} + C_n,$ $n \geq 0$. Let $S_{2n} = C_{2n}^2, S_{2n+1} = C_{2n+1}^2 + 4,$ $n \geq 0$. Then

$$S_{n+2} = (d^2+2)S_{n+1} - S_n - 2d^2, \; n \geq 0.$$

Proof: Solving the recurrence $C_0 = 2, C_1 = d, C_{n+2} = dC_{n+1} + C_n$ $(n \geq 0)$ in the usual way gives

$$C_n = \delta^n + \left(\frac{-1}{n}\right)^n, \text{ where } \delta = \sqrt{\frac{d^2}{4}+1} + \sqrt{\frac{d^2}{4}}, \; \frac{1}{\delta} = \sqrt{\frac{d^2}{4}+1} - \sqrt{\frac{d^2}{4}}.$$

Then $S_{2n} = C_{2n}^2 = (\delta^{2n} + \frac{1}{\delta^{2n}})^2$, $S_{2n+1} = C_{2n+1}^2 + 4 = (\delta^{2n+1} + \frac{1}{\delta^{2n+1}})^2$, $n \geq 0$.

Since $(\delta + \frac{1}{\delta})^2 = d^2 + 4$, we obtain

$$(d^2+4)S_{n+1} = \left[\left(\delta + \frac{1}{\delta}\right)\left(\delta^{n+1} + \frac{1}{\delta^{n+1}}\right)\right]^2,$$

and the calculations used in the proof of part (d) of the Lemma now give

$$S_{n+2} = (d^2+2)S_{n+1} - S_n - 2d^2, \; n \geq 0.$$

Corollary 1: Let $S_{2n} = L_{2n}^2, S_{2n+1} = L_{2n+1}^2 + 4,$ $n \geq 0$, where $\{L_n\}$ is the Lucas sequence. Then $S_{n+2} = 3S_{n+1} - S_n - 2$.

Proof: This is the case $d = 1$ of Theorem 2.

Corollary 2: Let $T_{2n} = F_{2n}^2 + \frac{4}{5}, T_{2n+1} = F_{2n+1}^2,$ $n \geq 0$, where $\{F_n\}$ is the Fibonacci sequence. Then $T_{n+2} = 3T_{n+1} - T_n - 2$, $n \geq 0$.

Proof: This follows from Corollary 1 and the identity $5F_n^2 = L_n^2 - 4(-1)^n$ (see [1], p. 56).

If we now write $\delta = \sqrt{s} - \sqrt{s-1}, S_n = \frac{1}{4}(\delta^n + \frac{1}{\delta^n})^2$, $n \geq 0$, we obtain, just as in the Lemma, $S_0 = 1,$ $S_1 = s,$ $S_{n+2} = 4(s-2)S_{n+1} - S_n - 2(s-1)$, $n \geq 0$.

The following two results can now be proved in essentially the same way as Theorems 1 and 2.

Theorem 3: Let $d \geq 2$ be an integer. Define the sequence $\{B_n\}$ $(n \geq 0)$ by $B_0 = 1, B_1 = d,$ $B_{n+2} = 2dB_{n+1} - B_n,$ $n \geq 0$. Then the sequence of squares $\{B_n^2\}$ $(n \geq 0)$ satisfies the second-order recurrence $B_{n+2}^2 = (4d^2-2)B_{n+1}^2 - B_n^2 - 2(d^2-1)$, $n \geq 0$.

Theorem 4: Let $d \geq 1$ be an integer. Define the sequence $\{C_n\}$ $(n \geq 0)$ by $C_0 = 1, C_1 = d,$ $C_{n+2} = 2dC_{n+1} + C_n,$ $n \geq 0$. Assume $S_{2n} = C_{2n}^2, S_{2n+1} = C_{2n+1}^2,$ $n \geq 0$, then $S_{n+2} = (4D^2+2)S_{n+1} - S_n - 2d^2$, $n \geq 0$.

We now turn to the more general homogeneous case.

Theorem 5: Let $a, b, c \neq 0, d \neq 0$ be integers, with $ab \neq 0$ and $c^2 \neq 4d$. Let $B_0 = a, B_1 = b$, $B_{n+1} = cB_n - dB_{n-1}$, $n \geq 1$. Then $B_{n+1}^2 = (c^2 - 2d)B_n^2 - d^2 B_{n-1}^2 + 2(b^2 + a^2 d - abc)d^n$, $n \geq 1$.

Proof: Let α, β be the roots of $x^2 - cx + d = 0$. Then $\alpha, \beta = \frac{1}{2}(c \pm \sqrt{c^2 - 4d})$, $\alpha \neq \pm\beta$, $\alpha^2, \beta^2 = \frac{1}{2}(c^2 - 2d \pm c\sqrt{c^2 - 4d}), \alpha\beta = d$. Also $\alpha^2 \neq \beta^2 \neq d$, since $c \neq 0, d \neq 0, c^2 \neq 4d$.

According to the result of Selmer stated in the Introduction, there are constants A, B, C such that $B_n^2 = A\alpha^{2n} + B\beta^{2n} + Cd^n$, $n \geq 0$.

Solving the system

$$\begin{cases} a^2 = B_0^2 = A + B + C \\ b^2 = B_1^2 = A\alpha^2 + B\beta^2 + Cd \\ (bc - ad)^2 = B_2^2 = A\alpha^4 + B\beta^4 + Cd^2 \end{cases}$$

for C gives

$$C = \frac{2(b^2 + a^2 d - abc)}{4d - c^2}.$$

Using $(c^2 - 2d)\alpha^{2n} - d^2\alpha^{2n-2} = \alpha^{2n+2}$ and $(c^2 - 2d)\beta^{2n} - d^2\beta^{2n-2} = \beta^{2n+2}$ gives

$$(c^2 - 2d)B_n^2 - d^2 B_{n-1}^2 + ed^n = A\alpha^{2n+2} + B\beta^{2n+2} + C[(c^2 - 2d)d^n - d^{n+1}] + ed^n.$$

Now choosing e so that $C[(c^2 - 2d)d^n - d^{n+1}] + ed^n = Cd^{n+1}$ [namely, $e = C(4d - c^2) = 2(b^2 + a^2 d - abc)$] finally gives

$$(c^2 - 2d)B_n^2 - d^2 B_{n-1}^2 + ed^n = A\alpha^{2n+2} + B\beta^{2n+2} + Cd^{n+1} = B_{n+1}^2,$$

which completes the proof.

Remark: The result of Theorem 5 appears in [4].

Applying Theorem 5 to the question raised in the Introduction, we immediately get the following result.

Theorem 6: Let $a, b, c \neq 0, d \neq 0$ be integers, with $ab \neq 0$ and $c^2 \neq 4d$. Let $B_0 = a, B_1 = b, B_{n+1} = cB_n - dB_{n-1}$, $n \geq 1$. Then the sequence of squares $\{B_n^2\}$ $(n \geq 0)$ satisfies a second-order linear recurrence (with constant coefficients) if and only if $d = 1$, in which case

$$B_{n+1}^2 = (c^2 - 2)B_n^2 - B_{n-1}^2 + 2(b^2 + a^2 - abc), \; n \geq 1.$$

Our final result is the general version of Theorem 2, in which we consider a perturbation of the sequence of squares.

Theorem 7: Let $a, b, c \neq 0, d \neq 0$ be integers, with $ab \neq 0$ and $c^2 \neq 4d$, such that $e = \frac{4(a^2 + abc - b^2)}{c^2 + 4}$ is an integer. Define the sequence $\{B_n\}$ $(n \geq 0)$ by $B_0 = a, B_1 = b, B_{n+1} = cB_n + B_{n-1}$, $n \geq 1$. Let

$S_{2n} = B_{2n}^2$, $S_{2n+1} = B_{2n+1}^2 + e$, $n \geq 0$. Then $\{S_n\}$ $(n \geq 0)$ satisfies the second-order recurrence

$$S_{n+1} = (c^2+2)S_n - S_{n-1} + 2e + 2(b^2 - a^2 - abc), \; n \geq 1.$$

Proof: This is a direct application of Theorem 5 with $d = -1$, according to which

$$B_{n+1}^2 = (c^2+2)B_n^2 - B_{n-1}^2 + 2(b^2 - a - abc)(-1)^n.$$

REFERENCES

1. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers.* Boston: Houghton Mifflin, 1969; rpt. Santa Clara, Calif.: The Fibonacci Association, 1980.
2. A. J. van der Poorten. "A Note on Recurrence Sequences." *J. and Proc., Royal Soc. of New South Wales* **106** (1973):115-17.
3. E. S. Selmer. "Linear Recurrence Relations over Finite Fields." Mimeographed notes, University of Bergen, Bergen, 1966.
4. H. S. Wilf. Problem 10211. *Amer. Math. Monthly* **99** (1992):361.

AMS Classification Numbers: 11B37, 11B39

❖❖❖

DYNAMICS OF THE MAPPING $f(x) = (x+1)^{-1}$

Paul Bracken
Department of Applied Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
(*Submitted February 1994*)

A concise presentation of the dynamics of the sequences $x_{n+1} = f(x_n)$ generated by the function $f(x) = (x+1)^{-1}$ is given. This sequence has a limit for almost all real initial x_0.

To prove this, notice that the interval $(-\infty, 0]$ is eventually mapped onto the positive real axis with the exception of a negative fixed point in $[-2, -1)$, as well as a countable set of points in this interval which are mapped to -1 after n iterations. To obtain this discrete set of initial x_0, one solves the simple equation $f(x_0) = -1$ then inductively, using the fundamental recursion for the Fibonacci sequence, this set of x_0 is given by $S = \{v_n\}$, where

$$v_n = -\frac{F_{n+2}}{F_{n+1}}, \quad n \geq 1.$$

Since $(F_n / F_{n-1}) \to r$, where $r = (1+\sqrt{5})/2$ as $n \to \infty$ (see [1]), it is interesting to note that the sequence $v_n \to -r$ as $n \to \infty$, where $-r$ is the negative fixed point of f.

The behavior of the sequence v_n on each side of $-r$ is somewhat more complicated, but interesting. If $-\infty < x_0 < -2$, then $0^- > (x_0+1)^{-1} > -1$, and if $0 > x > -1$, then $1 < (x+1)^{-1} < \infty$ so that $(-\infty, -2) \to (-1, 0) \to [1, \infty)$.

The most complicated dynamics is on the set $(-2, -1)$ which contains S as a subset. In general, for $n > 2$ such that $v_n > v_{n+2} > -r$, then under the action of f,

$$\left(-\frac{F_{n+4}}{F_{n+3}}, -\frac{F_{n+2}}{F_{n+1}}\right) \to \left(-\frac{F_{n+1}}{F_n}, -\frac{F_{n+3}}{F_{n+2}}\right)$$

and for $n > 2$ such that $-r > v_{n+2} > v_n$, the order of the endpoints is reversed. Therefore, each interval of this form is mapped onto a corresponding interval which is on the opposite side of the fixed point $-r$. and for any $x_0 \in (-2, -1)$ such that $x_0 \neq -r$ or $x_n \notin S$, there is an N such that x_N leaves $(-2, -1)$ and is contained in an interval which has been considered. Convergence can be forced on $x_0 \in S$ if we set $f(\pm\infty) = 0$, then there remains only the unstable fixed point $-r$ which remains invariant.

To finish the study of the convergence of f under iteration, this shows that it suffices to consider $x_N = x_0 \in (0, \infty)$, and since $[1, \infty)$ is mapped onto $(0, 1]$, suppose $x_0 \in (0, 1]$. An expression which generates the x_n and which converges to the positive stable fixed point of the mapping can be written as

$$x_n = \frac{F_{n-1}x_0 + F_n}{F_n x_0 + F_{n+1}}, \quad x_0 \in (0, 1].$$

By induction on n, one obtains

$$x_{n+1}=f(x_n)=\frac{F_nx_0+F_{n+1}}{F_{n-1}x_0+F_n+F_nx_0+F_{n+1}}=\frac{F_nx_0+F_{n+1}}{F_{n+1}x_0+F_{n+2}},$$

and then letting $n\to\infty$ one obtains

$$x_\infty=\frac{1}{r}=\frac{\sqrt{5}-1}{2}.$$

REFERENCE

1. I. Niven & H. Zuckermann. *An Introduction to the Theory of Numbers*, 1972.

AMS Classification Numbers: 11B39, 11A99

❖❖❖

RECURRENCE SEQUENCES AND BERNOULLI POLYNOMIALS OF HIGHER ORDER

Zhang Zhizheng and Guo Lizhou
Department of Mathematics, Luoyang Teachers' College,
Luoyang, Henan, 471022, People's Republic of China
(*Submitted February 1994*)

1. It is well known that a general, linear sequence $S_n(p,q)$ $(n=0,1,2,\dots)$ of order 2 is defined by the recurrence relation

$$S_n(p,q)=pS_{n-1}(p,q)-qS_{n-2}(p,q)$$

with S_0, S_1, p, q arbitrary and $\Delta=p^2-4q>0$ [5].

In particular, if $S_0=0, S_1=1$ or $S_0=2, S_1=p$, we have the generalized Fibonacci (Lucas) sequences $S_n(p,q)=U_n(p,q)$ or $S_n(p,q)=V_n(p,q)$.

If x_1, x_2 $(x_1>x_2)$ designate the roots of $x^2-px+1=0$, it is easy to prove that

$$U_n(p,q)=\frac{x_1^n-x_2^n}{x_1-x_2},\quad V_n(p,q)=x_1^n+x_2^n \tag{1}$$

and, moreover, the general term of the sequence $S_n(p,q)$ may be expressed as a linear combination of the general terms of the Fibonacci and Lucas sequences by the formula

$$S_n(p,q)=\left(S_1-\tfrac{1}{2}pS_0\right)U_n(p,q)+\tfrac{1}{2}S_0V_n(p,q). \tag{2}$$

We assume $S_0=k, S_1=\frac{1}{2}pk+\left(x-\frac{1}{2}k\right)\Delta^{\frac{1}{2}}$, and according to equations (1) and (2), we deduce

$$S_n(x;p,q)=\left(x-\tfrac{1}{2}k\right)\Delta^{\frac{1}{2}}U_n(p,q)+\tfrac{1}{2}kV_n(p,q), \tag{3}$$

$$S_n(x;p,q)=xx_1^n+(k-x)x_2^n. \tag{4}$$

For the sake of brevity, from here on we write U_n, V_n, and $S_n(x)$ for $U_n(p,q), V_n(p,q)$, and $S_n(x;p,q)$.

2. From equation (3) we have

$$S_n(x)+S_n(k-x)=\frac{1}{2^{m-1}}\sum_{r=0}^{[m/2]}\binom{m}{2r}\Delta^r U_n^{2r}V_n^{m-2r}k^{m-2r}(2x-k)^{2r}, \tag{5}$$

and from (4) we get

$$S_n^m(x)+S_n^m(k-x)=\sum_{r=0}^{m}\binom{m}{2r}q^{nr}(x_1^{n(m-2r)}+x_2^{n(m-2r)})x^r(k-x)^{m-r}.$$

Then we have

$$S_n^{2m}(x)+S_n^{2m}(k-x)=\sum_{r=0}^{2m}\binom{2m}{r}q^{nr}(x_1^{2n(m-r)}+x_2^{2n(m-r)})x^r(k-x)^{2m-r}=\sum_{r=0}^{m}+\sum_{r=m+1}^{2m}$$

$$=\sum_{r=0}^{2m}\binom{2m}{r}q^{nr}(x_1^{2n(m-r)}+x_2^{2n(m-r)})x^r(k-x)^{2m-r}+\sum_{s=0}^{m-1}\binom{2m}{s}q^{ns}(x_1^{2n(m-s)}+x_2^{2n(m-s)})x^{2m-s}(k-x)^s$$

$$\begin{aligned}&=2\binom{2m}{m}q^{mn}x^m(k-x)^m+\sum_{r=0}^{m-1}\binom{2m}{r}q^{nr}\left(x_1^{2n(m-r)}+x_2^{2n(m-r)}\right)\left(x^r(k-x)^{2m-r}+x^{2m-r}(k-x)^r\right)\\&=2\binom{2m}{m}q^{mn}x^m(k-x)^m+\sum_{r=0}^{m-1}\binom{2m}{r}q^{nr}V_{2n(m-1)}\left(x^r(k-x)^{2m-r}+x^{2m-r}(k-x)^r\right).\end{aligned}\tag{6}$$

We can similarly find the analogous formula

$$S_n^{2m+1}(x)+S_n^{2m+1}(k-x)=\sum_{r=0}^{m}\binom{2m+1}{r}q^{nr}V_{n(2m-2r+1)}\left(x^r(k-x)^{2m-r+1}+x^{2m-r+1}(k-x)^r\right).\tag{7}$$

We also give the difference formulas

$$S_n^m(x)-S_n^m(k-x)=\frac{\Delta^{\frac{1}{2}}}{2^{m-1}}\sum_{r=0}^{[(m-1)/2]}\binom{m}{2r+1}\Delta^rU_n^{2r+1}V_n^{m-2r-1}k^{m-2r-1}(2x-k)^{2r+1},\tag{8}$$

$$S_n^m(x)+S_n^m(k-x)=\Delta^{\frac{1}{2}}\sum_{r=0}^{[(m-1)/2]}\binom{m}{r}q^{nr}U_{n(m-2r)}[x^{m-r}(k-x)^r-x^r(k-x)^{m-r}].\tag{9}$$

We end this section with the generating functions

$$\sum_{r=0}^{\infty}\frac{t^r}{r!}U_{nr}=\frac{1}{\Delta^{\frac{1}{2}}}(\exp(tx_1^n)-\exp(tx_2^n)),\tag{10}$$

and

$$\sum_{r=0}^{\infty}\frac{t^r}{r!}V_{nr}=\exp(tx_1^n)+\exp(tx_2^n).\tag{11}$$

3. We recall that Bernoulli polynomials of higher order $B_n^{(k)}(x)$ are defined by the generating expansion (see [2])

$$\sum_{r=0}^{\infty}\frac{t^r}{r!}B_r^{(k)}(x)=\left(\frac{t}{e^t-1}\right)^k e^{tx},\ |t|<2\pi,\tag{12}.$$

the usual Bernoulli polynomials by $B_n(x)=B^{(1)}(x)$, and the Bernoulli numbers by $B_n=B_n(0)$. We also recall that

$$B_{2n+1}=0\ \ (n>0)\quad\text{and}\quad B_n^{(k)}(k-x)=(-1)^nB_n^k(x),\tag{13}$$

are usually called the complementary argument theorem (see [3]).

From (12), replacing t with $\Delta^{\frac{1}{2}}U_nt$, we have

$$\begin{aligned}\sum_{r=0}^{\infty}\frac{\left(\Delta^{\frac{1}{2}}U_nt\right)^r}{r!}B_r^{(k)}(x)&=\frac{\left(\Delta^{\frac{1}{2}}U_nt\right)^k}{\left(\exp(t(x_1^n-x_2^n))\right)^k}\exp\left(tx(x_1^n-x_2^n)\right)\\&=\frac{(\Delta^{\frac{1}{2}}U_nt)^k}{\left(\exp(tx_1^n)-\exp(x_2^n)\right)^k}\exp\left(t(xx_1^n+(k-x)x_2^n)\right)=\frac{(\Delta^{\frac{1}{2}}U_nt)^k}{(\exp(tx_1^n)-\exp(x_2^n))^k}\exp(tS_n(x)).\end{aligned}$$

Therefore,

$$(\exp(tx_1^n)-\exp(tx_2^n))^k\sum_{r=0}^{\infty}\frac{(\Delta^{\frac{1}{2}}U_nt)^r}{r!}B_r^{(k)}(x)=(\Delta^{\frac{1}{2}}U_nt)^k\exp(tS_n(x))$$

and using (10) it follows that

$$\left(\sum_{r=0}^{\infty}\frac{t^r}{r!}U_{nr}\right)^k\sum_{r=0}^{\infty}\frac{(\Delta^{\frac{1}{2}}U_nt)^r}{r!}B_r^{(k)}(x)=U_n^kt^k\exp(tS_n(x)),$$

and we have

$$\left[\sum_{r=0}^{\infty}\left(\sum_{r_1+r_2+\cdots+r_k=r}\frac{U_{nr_1}}{r_1!}\cdots\frac{U_{nr_k}}{r_k!}\right)t^r\right]\sum_{r=0}^{\infty}\frac{(\Delta^{\frac{1}{2}}U_nt)^r}{r!}B_r^{(k)}(x)=U_r^{(k)}t^k\exp(tS_n(x)).$$

Expanding the product in the left-hand side and comparing powers of t, we find

$$\sum_{r=0}^{m-1}\binom{m}{r}\Delta^{\frac{r}{2}}U_n^rB_r^{(k)}(x)(m-r)!\sum_{r_1+r_2+\cdots+r_k=m-r}\frac{U_{nr_1}}{r_1!}\cdots\frac{U_{nr_k}}{r_k!}=(m)_kU_n^kS_n^{m-k}(x),\quad (m\geq k). \tag{14}$$

Now replace x with $k-x$ in equation (14) and make use of (13) to obtain

$$\sum_{r=0}^{m-1}(-1)^r\binom{m}{r}\Delta^{\frac{r}{2}}U_n^rB_r^{(k)}(x)(m-r)!\sum_{r_1+r_2+\cdots+r_k=m-r}\frac{U_{nr_1}}{r_1!}\cdots\frac{U_{nr_k}}{r_k!}=(m)_kU_n^kS_n^{m-k}(k-x),\quad (m\geq k). \tag{15}$$

Adding equations (14) and (15) and using (5), (6), and (7) we find

$$\sum_{r=0}^{[(m-1)/2]}\binom{m}{2r}\Delta^rU_n^{2r}B_{2r}^k(x)(m-2r)!\sum_{r_1+r_2+\cdots+r_k=m-2r}\frac{U_{nr_1}}{r_1!}\cdots\frac{U_{nr_k}}{r_k!}$$

$$=\frac{1}{2^{m-k}}(m)_kU_n^k\sum_{r=0}^{[(m-k)/2]}\binom{m-k}{2r}\Delta^rU_n^{2r}k^{m-2r-k}U_n^{m-2r-k}(2x-k)^{2r} \tag{16}$$

$$=\frac{1+(-1)^{m-k}}{2}(m)_kU_n^k\binom{m-k}{[(m-k)/2]}q^{[(m-k)/2]}(x(k-x))^{[(m-k)/2]}+$$

$$+\frac{1}{2}(m)_kU_n^k\sum_{r=0}^{[(m-k-1)/2]}\binom{m-k}{r}q^{nr}V_{n(m-k-2r)}[x(k-x)^{m-k-r}+x^{m-k-r}(k-x)^r]. \tag{17}$$

Subtracting equations (14) and (15) and using (8) and (9) gives

$$\sum_{r=0}^{[(m-2)/2]}\binom{m}{2r+1}\Delta^rU_n^{2r+1}B_{2r+1}^{(k)}(x)(m-2r-1)!\sum_{r_1+r_2+\cdots+r_k=m-2r-1}\frac{U_{nr_1}}{r_1!}\cdots\frac{U_{nr_k}}{r_k!}$$

$$=\frac{1}{2^{m-k}}(m)_kU_n^k\sum_{r=0}^{[(m-k-1)/2]}\binom{m-k}{r}q^{nr}U_{n(m-2r-k)}[x^{m-r-k}(k-x)^r-x^r(k-x)^{m-r-k}]. \tag{18}$$

4. If we take $x = \frac{k}{2}$ in equation (16), we get

$$\sum_{r=0}^{[(m-1)/2]} \binom{m}{2r} \Delta^r U_n^{2r} B_{2r}^{(k)}\left(\frac{k}{2}\right)(m-2r)! \sum_{r_1+r_2+\cdots r_k=m-2r} \frac{U_{nr_1}}{r_1!} \cdots \frac{U_{nr_k}}{r_k!} = \frac{1}{2^{m-k}}(m)_k U_n^k k^{m-k} V_n^{m-k}. \quad (19)$$

Taking $k = 1$ in equation (19) and recalling that $B_{2n}(\frac{1}{2}) = \left(\frac{1}{2^{2n-1}} - 1\right) B_{2n}$ (see [5]), we have

$$\sum_{r=0}^{[(m-1)/2]} \binom{m}{2r} \Delta^r U^{2r}\left(\frac{1}{2^{2r-1}} - 1\right) B_{2r} U_{n(m-2r)} = \frac{m}{2^{m-1}} U_n V_n^{m-1}. \quad (20)$$

If we make $x = 0$ in equation (17), we get

$$\sum_{r=0}^{[(m-1)/2]} \binom{m}{2r} \Delta^r U_n^{2r} B_{2r}^{(k)}(m-2r)! \sum_{r_1+r_2+\cdots+r_k=m-2r} \frac{U_{nr_1}}{r_1!} \cdots \frac{U_{nr_k}}{r_k!} = \frac{1}{2}(m)_k U_n^k V_{(m-k)}. \quad (21)$$

From expression (21), recalling that $B_k^{(n+1)} = \left(1 - \frac{k}{n}\right) B_k^{(n)} - k B_{k-1}^{(n)}$ (see [4]) and taking $k = 1, 2, 3$, we get, successively,

$$\sum_{r=0}^{[(m-1)/2]} \binom{m}{2r} \Delta^r U_n^{2r} B_{2r} U_{n(m-2r)} = \frac{1}{2} m U_n V_{n(m-1)}, \quad (22)$$

$$\sum_{r=0}^{[(m-1)/2]} \binom{m}{2r} \Delta^r U_n^{2r} (B_{2r} - 2rB_{2r} - 2rB_{2r-1}) \sum_{i=0}^{m-2r} \binom{m-2r}{i} U_{ni} U_{n(m-2r-1)} = \frac{1}{2} m(m-1) U_n^2 V_{n(m-2)}, \quad (23)$$

$$\sum_{r=0}^{[(m-1)/2]} \binom{m}{2r} \Delta^r U_n^{2r} ((2r-1)(r-1)B_{2r} + r(4r-5)B_{2r-1} + 2r(2r-1)B_{2r-2}) \sum_{i+j+k=m-2r} \binom{m-2r}{i,\, j,\, k} U_{ni} U_{nj} U_{nk}$$
$$= \frac{1}{2} m(m-1)(m-2) U_n^3 V_{n(m-3)}, \quad (24)$$

where $\binom{m-2r}{i,\, j,\, k}$ is the multinomial coefficient (see [1]).

With $p = 1$, $q = -1$, we get the Fibonacci and Lucas sequences $U_0 = 0, U_1 = 1, \ldots, U_n(1,-1) = F_n, \ldots$ and $V_0 = 2, V_1 = 1, \ldots, V_n(1,-1) = L_n, \ldots$, and from equation (19) we get Kelisky's formula (see [2])

$$\sum_{r=0}^{[m/2]} 5^r \binom{m}{2r} B_{2r} F_n^{2r} F_{n(m-2r)} = \frac{m}{2} F_n L_{n(m-1)}. \quad (25)$$

REFERENCES

1. M. Aiger. *Combinatorial Theory*. New York: Springer-Verlag, 1979.
2. R. P. Kelisky. "On Formulas Involving Both the Bernoulli and Fibonacci Numbers." *Scripta Math.* **23** (1957):27-35.
3. G. A. Ken & T. A. Ken. *Mathematical Tables* (in Chinese). Beijing, 1987.
4. P. J. McCarthy. "Some Irreducibility Theorems for Bernoulli Polynomials of Higher Order." *Duke Math. J.* **27** (1960):313-18.
5. L. Toscano. "Recurring Sequences and Bernoulli-Euler Polynomials." *Journ. Comb. Inf. & Syst. Sci.* **4** (1979):303-08.

AMS Classification Number: 11B68

A DISJOINT COVERING OF THE SET OF NATURAL NUMBERS CONSISTING OF SEQUENCES DEFINED BY A RECURRENCE WHOSE CHARACTERISTIC EQUATION HAS A PISOT NUMBER ROOT

Shiro Ando
College of Engineering, Hosei University, Koganei-shi, Tokyo 184, Japan

Teluhiko Hilano
Kanagawa Institute of Technology, Atsugi-shi, Kanagawa 243-02, Japan
(*Submitted February 1994*)

1. INTRODUCTION

Burke and Bergum [1] called a family of sequences defined by a linear recurrence "a disjoint covering" if every natural number was contained in exactly one of the given sequences. They gave arithmetic progressions and geometric progressions as simple examples of finite and infinite disjoint coverings. Although they also constructed n^{th}-order recurrences that were disjoint coverings, the resulting sequences were not essentially n^{th} ordered since they were the same as the ones listed above and could be defined by first-order recurrences. Zöllner [4] proved that there is an infinite disjoint covering generated by the Fibonacci recurrence

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

answering the question proposed in [1] affirmatively. This is the first paper establishing the existence of a disjoint covering consisting of sequences essentially defined by a second-order recurrence.

In this paper we will show the existence of disjoint coverings essentially generated by linear recurrences of any order.

2. A TYPE OF PISOT NUMBER

A Pisot number is a real algebraic integer greater than 1 such that the absolute value of every conjugate is less than 1 (see [2]). We consider a special type of Pisot number that satisfies a monic irreducible equation with integral coefficients

$$f(x) = x^m - a_1x^{m-1} - \cdots - a_{m-1}x - a_m = 0, \tag{2}$$

where $m \ge 2$, $a_1 > 0$, $a_i \ge 0$ (for $i = 2, \ldots, m-1$), and $a_m > 0$.

Since $f(1) < 0$, equation (2) has a real number solution $\alpha > 1$. Let β_i $(i = 1, 2, \ldots, m-1)$ be the other roots of (2).

Example: We will show that if

$$a_1 > 1 + a_2 + \cdots + a_m, \tag{3}$$

then $|\beta_i| < 1$ for $i = 1, 2, \ldots, m-1$, and α is a Pisot number.

Let $g(x) = x^m - a_1x^{m-1} - a_2x^{m-2} = x^{m-2}(x^2 - a_1x - a_2)$ and let $h(x) = a_3x^{m-3} + \cdots + a_{m-1}x + a_m$. Then we have

$$|g(x)| \geq a_1 - 1 - a_2 > a_3 + a_4 + \cdots + a_m \geq |h(x)|$$

for any complex value of x on the unit circle $|x| = 1$ by (3). Therefore, by Rouché's theorem (see [3]), the number of roots of equation (2), or $g(x) = h(x)$, in the unit circle is equal to one of $g(x) = 0$, which is $m-1$, since the equation $x^2 - a_1x - a_2 = 0$ has two real roots x_1 and x_2, where $x_1 > 1$, $-1 < x_2 < 0$.

Now we will show that $f(x)$ in (2) is irreducible when (3) is satisfied. If it is reducible, then it must be decomposed into monic polynomials with integral coefficients, and each factor must have at least one root of modulus greater than or equal to 1, since the product of its roots is an integer. This contradicts the fact we have just proved above. Thus, we have shown that there are equations of type (2) that have a Pisot number root for each $m \geq 2$.

Remark: It should be noticed that, if (2) has a Pisot number root, all roots of (2) are simple, since any irreducible polynomial with rational coefficients has no multiple root.

3. SEQUENCES DEFINED BY A LINEAR RECURRENCE

We consider the recurrence

$$u_n = a_1u_{n-1} + a_2u_{n-2} + \cdots + a_mu_{n-m} \tag{4}$$

that has $f(x)$ in (2) as its characteristic polynomial. Let S be the set of all the positive integer sequences $\{u_n\}$ defined by recurrence (4). In the following we will establish that the existence of a disjoint covering of the set of natural numbers consists of the sequences in S.

According to the Remark in the previous section, the general term of $\{u_n\}$ is expressed as

$$u_n = c_0\alpha^n + c_1\beta_1^n + \cdots + c_{m-1}\beta_{m-1}^n, \tag{5}$$

where $c_0 > 0$ because $\alpha^n \to \infty$ and $\beta_i^n \to 0$ for $i = 1, 2, \ldots, m-1$ as n tends to ∞.

Let us define m integer sequences $\{t_n^{(i)}\}$ (for $i = 1, 2, \ldots, m$) satisfying (4) with the initial conditions $t_j^{(i)} = \delta_{ij}$ $(i, j = 1, 2, \ldots, m)$, where the right-hand side is Kroneker's delta.

These sequences have zero or positive integer terms, and their general terms are expressed as

$$t_n^{(i)} = b_{i,0}\alpha^n + b_{i,1}\beta_1^n + \cdots + b_{i,m-1}\beta_{m-1}^n, \tag{6}$$

where $b_{i,0} > 0$ as c_0 in (5). The n^{th} term u_n of the sequence defined by recurrence (2) is expressed as a linear combination of leading m terms as

$$u_n = t_n^{(1)}u_1 + t_n^{(2)}u_2 + \cdots + t_n^{(m)}u_m, \tag{7}$$

where the coefficients consist of n^{th} terms of these sequences.

4. THE CONSTRUCTION OF A DISJOINT COVERING

Now we show that there exists a disjoint covering of the set of all natural numbers consisting of sequences in S following the method used in [4].

Notice that the set cannot be covered with a finite number of such sequences. In fact, as $c_0 > 0$ in (5), $u_n \sim c_0\alpha^n$ so that $u_{n+1} - u_n \to \infty$ as n tends to ∞.

First, we define the sequence $\{u_n^{(1)}\}$ in S with initial conditions $u_n^{(1)} = n$ (for $n = 1, 2, \ldots, m$). Then assuming that, for $i = 1, 2, \ldots, k-1$, we have determined mutually disjoint increasing sequences $\{u_n^{(i)}\}$ in S that satisfy the conditions

$$u_1^{(i)} = \min \overline{V}_{i-1}, \tag{8}$$

where $\overline{V_i}$ denotes the complement of the set $V_i = \{u_n^{(j)} \mid j = 1, 2, \ldots, i;\ n = 1, 2, 3, \ldots\}$ in the set of all natural numbers, and

$$u_n^{(i)} < u_n^{(j)} \text{ for } i < j, \tag{9}$$

we will show that we can choose the next sequence $\{u_n^{(k)}\}$ in S so that these k sequences are mutually disjoint and satisfy conditions (8) and (9).

We can see that $\overline{V_i}$ is always nonempty by using the statement made at the beginning of this section. Thus, we can put $u_1^{(k)} = \min \overline{V}_{k-1}$ and $u_r^{(k)} = \min \overline{V}_{k-1} - \{u_1^{(k)}, u_2^{(k)}, \ldots, u_{r-1}^{(k)}\}$ for $r = 2, 3, \ldots, m-1$.

Let $M_k = \max\{u_m^{(k-1)}, u_{m-1}^{(k)}\}$ and let L_k be an integer larger than M_k. If we take any integer in the interval $(M_k, L_k]$ as the value of $u_m^{(k)}$, the resulting sequence $\{u_n^{(k)}\}$ in S will satisfy the inequality $u_n^{(k-1)} < u_n^{(k)}$ for all n, but it will possibly have a common term with one of the sequences $\{u_n^{(i)}\}$ $(i = 1, 2, \ldots, k-1)$ already built. We will evaluate the number N of such integers to show that we can find an integer value of $u_m^{(k)}$ in the interval $(M_k, L_k]$ so that the resulting sequence $\{u_n^{(k)}\}$ does not overlap with any of the $k-1$ sequences already built if we take a large enough value for L_k.

Suppose that $u_p^{(k)} = u_q^{(i)}$ for some $i < k$. Then $m \le p < q$. Using the expression shown in (7) for $u_p^{(k)}$ and $u_q^{(i)}$, we have

$$t_p^{(1)} u_1^{(k)} + \cdots + t_p^{(m)} u_m^{(k)} = t_q^{(1)} u_1^{(i)} + \cdots + t_q^{(m)} u_m^{(i)}. \tag{10}$$

If $u_{p+r}^{(k)} = u_{q+r}^{(i)}$ for $r = 1, 2, \ldots, m-1$, then, using recurrence (4) to the opposite direction, we have $u_1^{(k)} = u_{q-p+1}^{(i)}$, which contradicts the choice of $u_1^{(k)}$. Thus, there is an r such that

$$0 \le r < m-1,\ u_{p+r}^{(k)} = u_{q+r}^{(i)}, \text{ and } u_{p+r+1}^{(k)} \ne u_{q+r+1}^{(i)}. \tag{11}$$

As we are going to find the largest p such that $u_p^{(k)}$ is equal to an element of V_{k-1}, replacing $p+r$ with p if necessary, we can assume that $r = 0$. Then, using expression (6), we have

$$u_{p+1}^{(k)} - \alpha u_p^{(k)} = -\sum \left\{ b_{j,1} \beta_1^p (\alpha - \beta_1) + \cdots + b_{j,m-1} \beta_{m-1}^p (\alpha - \beta_{m-1}) \right\} u_j^{(k)},$$

where summation runs from $j = 1$ to $j = m$. For $u_{q+1}^{(i)} - \alpha u_q^{(i)}$, we have a similar expression. Since we can see that

$$\left| (u_{p+1}^{(k)} - \alpha u_p^{(k)}) - (u_{q+1}^{(i)} - \alpha u_q^{(i)}) \right| = \left| u_{p+1}^{(k)} - u_{q+1}^{(i)} \right| \ge 1,$$

from (11), we have

$$\Big|\Sigma\{b_{j,1}\beta_1^p(\alpha-\beta_1)+\cdots+b_{j,m-1}\beta_{m-1}^p(\alpha-\beta_{m-1})\}u_j^{(k)} \\ -\Sigma\{b_{j,1}\beta_1^q(\alpha-\beta_1)+\cdots+b_{j,m-1}\beta_{m-1}^q(\alpha-\beta_{m-1})\}u_n^{(i)}\Big|\geq 1.$$

Here, let us put $\beta=\max\{|\beta_1|,\ldots,|\beta_{m-1}|\}$, $A=\max\{|\alpha-\beta_i||i=1,2,\ldots,m-1\}$, and $B=\max\{|b_{i,j}||i=1,2,\ldots,m;\ j=0,1,\ldots,m-1\}$. These values are independent of $u_m^{(k)}$, and $0<\beta<1$. Then we have $(m-1)AB\beta^p\{(2m-1)M_k+L_k\}\geq 1$, from which we can evaluate p as

$$\begin{aligned} p &\leq -[\log\{(2m-1)M_k+L_k\}+\log\{(m-1)AB\}]/\log\beta \\ &\leq C_1\log(L_k+C_2)+C_3 \end{aligned} \tag{12}$$

for some constants C_1, C_2, and C_3 independent of L_k and $u_m^{(k)}$.

On the other hand, from expression (6), we have

$$\begin{aligned} \left|t_q^{(1)}u_1^{(i)}+\cdots+t_q^{(m)}u_m^{(i)}\right| &\geq (b_{1,0}u_1^{(i)}+\cdots+b_{m,0}u_m^{(i)})\,\alpha^q-\Sigma\big(|b_{j,1}|+\cdots+|b_{j,m-1}|\big)u_j^{(i)} \\ &\geq (b_{1,0}u_1^{(1)}+\cdots+b_{m,0}u_m^{(1)})\,\alpha^q-m(m-1)M_k. \end{aligned}$$

We can find here a constant T depending only on the coefficients of (2) such that $t_n^{(i)}\leq T\alpha^n$ for $1\leq i\leq m$. We can also find an integer ν for which $t_n^{(m)}\geq(b_{m,0}/2)\,\alpha^n$ if $n\geq\nu$. Putting $U=\min\{b_{m,0}/2,\ \alpha^{-\nu}\}$, we have $t_n^{(m)}\geq U\alpha^n$ for $n\geq m$.

Using these inequalities and $t_p^{(m)}\geq 1$, we have the following evaluation, from (10),

$$\begin{aligned} L_k\geq u_m^{(k)} &\geq \left(t_q^{(1)}u_1^{(i)}+\cdots+t_q^{(m)}u_m^{(i)}\right)\Big/t_p^{(m)}-\left(t_p^{(1)}+\cdots+t_p^{(m-1)}\right)M_k\Big/t_p^{(m)} \\ &\geq \left(b_{1,0}u_1^{(i)}+\cdots+b_{m,0}u_m^{(i)}\right)\alpha^{q-p}\Big/T-(m-1)(mB+U^{-1}T)\,M_k. \end{aligned}$$

Taking the logarithms, we have

$$\begin{aligned} q-p &\leq \left[\log\{L_k+(m-1)(mB+U^{-1}T)M_k\}+\log T-\log\Sigma b_{j,0}u_j^{(i)}\right]\Big/\log\alpha \\ &= C_4\log(L_k+C_5)+C_6, \end{aligned}$$

which gives an evaluation of q together with inequality (12) as

$$q\geq C_1\log(L_k+C_2)+C_4\log(L_k+C_5)+C_7. \tag{13}$$

The constants C_4, C_5, C_6, and C_7 are independent of the choice of $u_m^{(k)}$ as well as the value of L_k.

Since we have already determined the $m-1$ initial terms of the k^{th} sequence, two different values of $u_m^{(k)}$ give different p^{th} terms that cannot coincide with the same $u_q^{(i)}$. Hence, the number N of the values of $u_m^{(k)}$ for which the resulting sequence $\{u_n^{(k)}\}$ has a common term with some of the first $k-1$ sequences will not exceed the number of triples (p,q,i) satisfying $u_p^{(k)}=u_q^{(i)}$. Evaluating the latter number using (12) and (13), we can obtain the inequality

$$N\leq(k-1)\{C_1\log(L_k+C_2)+C_3\}\{C_1\log(L_k+C_2)+C_4\log(L_k+C_5)+C_7\}\ll L_k-M_k$$

for large L_k.

Therefore, there must be a desired sequence $\{u_n^{(k)}\}$ in S disjoint with the $k-1$ sequences already built, and the proof can be completed by induction, since every natural number is contained in a sequence by the choice of $u_1^{(k)}$ determined in (8).

REFERENCES

1. J. R. Burke & G. E. Bergum. "Covering the Integers with Linear Recurrences." In *Applications of Fibonacci Numbers* **2:**143-47. Ed. A. N. Philippou, G. E. Bergum, & A. F. Horadam. Dordrecht: Kluwer, 1988.
2. Y. Meyer. *Algebraic Numbers and Harmonic Analysis.* The Hague: North Holland, 1972.
3. E. C. Titchmarsh. *The Theory of Functions*. 2nd. ed. London: Oxford University Press, 1939.
4. J. Zöllner. "A Disjoint System of Linear Recurring Sequences Generated by $u_{n+2} = u_{n+1} + u_n$ which Contains Every Natural Number." *The Fibonacci Quarterly* **31.2** (1993):162-65.

AMS Classification Numbers: 11B37, 11B39

ANTISOCIAL DINNER PARTIES

Richard Lewis
Mathematics Subject Group, University of Sussex, Brighton, BN1 9QH, U.K.
(*Submitted March 1994*)

1. INTRODUCTION

Take a circular dining table with n chairs arranged at equal intervals around it. In how many ways can ($n/2$ or fewer) people be seated on these chairs in such a way that no two people are seated on adjacent chairs, where two such seating patterns are to be regarded as the same if one can be got from the other by rotation? Let T_n denote the number of such seating patterns (including the case when nobody has come to dinner). The first five values of T_n are $T_1 = 1$, $T_2 = 2$, $T_3 = 2$, $T_4 = 3$, $T_5 = 3$.

I show here that, for $n \geq 2$,

$$T_n = \frac{1}{n}\sum_{d|n} L_d \phi\left(\frac{n}{d}\right) \tag{1}$$

(where the sum is over all positive divisors of n). In this expression, L_d is the d^{th} Lucas number, defined by the recurrence

$$L_0 = 2, L_1 = 1 \quad \text{and} \quad L_n = L_{n-1} + L_{n-2} \text{ thereafter,}$$

and ϕ is Euler's totient, i.e.,

$$\phi(n) = \#\{m : 0 \leq m < n, m \text{ and } n \text{ coprime}\}.$$

I was asked this question (i.e., the value of T_n) by my colleague Peter Bushell who, in connection with his work on Shapiro's inequality, was interested in the number of cyclically distinct components of the "regular boundary" of $K = \{\underline{x} \in \mathbf{R}^n : x_i \geq 0, 1 \leq i \leq n\}$. (The regular boundary of K is the set of points $\underline{x}$ in K having at least one component x_i equal to zero, but no two adjacent components both zero and not having x_1 and x_n both zero. See [1] for details and motivation.) So the number he was looking for is $T_n - 1$.

2. THE NUMBER OF CYCLICALLY DISTINCT PATTERNS

Suppose that $n \geq 2$ and let V_n denote the set of all strings $a_1 a_2 \ldots a_n$ on $\{0, 1\}$ of length n such that

V1: a_1 and a_{i+1} are not both 1 (for $1 \leq i < n$),
V2: a_1 and a_n are not both 1.

Such strings correspond to antisocial seating arrangements as described in the introduction (with $a_i = 1$ meaning that chair i is occupied). The cyclic group Z_n acts on V_n by rotations and the number T_n is the number of orbits of this action. Now Burnside's lemma ([2], 10.1.4) tells us that, if G is a finite group acting on a finite set S and if Fix(g) denotes the set of members of S fixed by $g \in C$, then

$$\#\{\text{orbits of G}\} = \frac{1}{\#\mathrm{G}} \sum_{g \in \mathrm{G}} \#\mathrm{Fix}(g).$$

So we need to find #Fix(g) for each element g of Z_n. Suppose that Z_n is generated by σ and that σ acts on V_n by $a_1 a_2 \dots a_n \sigma = a_n a_1 \dots a_{n-1}$. It is not difficult to see that, for any integer m, $\mathrm{Fix}(\sigma^m) = \mathrm{Fix}(\sigma^d)$, where $\gcd(m, n) = d$. Now, if d divides n, there are $\phi(n/d)$ integers m with $0 \le m < n$ and $\gcd(m, n) = d$, and it follows that

$$\mathrm{T}_n = \#\{\text{orbits of } \mathrm{Z}_n\} = \frac{1}{n} \sum_{d|n} \#\mathrm{Fix}(\sigma^d)\phi(n/d).$$

It is plain that

$$\mathrm{Fix}(\sigma^d) = \{\overbrace{vv \dots v}^{n/d} : v \in \mathrm{V}_d\}$$

and so $\#\mathrm{Fix}(\sigma^d) = \#\mathrm{V}_d$ and it remains for us to show that

$$\#\mathrm{V}_d = \mathrm{L}_d. \tag{2}$$

To deal with (2), consider the sets U_n of strings of 0's and 1's that satisfy V1 above but not necessarily V2. Then it is well known (and easily proved) that

$$\#\mathrm{U}_n = \mathrm{F}_{n+2} \tag{3}$$

(where F_n denotes the n^{th} Fibonacci number) and that

$$\mathrm{L}_n = \mathrm{F}_{n+1} + \mathrm{F}_{n-1}. \tag{4}$$

Let u_n denote a general element of U_n. Now (2) is true when $d = 1$ (V_1 contains only the string 0) and when $d = 2$, so suppose $d \ge 3$ and consider a string v in V_d. Either v ends in 1, in which case it looks like $0u_{d-3}01$, or v ends with 0 and looks like $u_{d-1}0$. By (3), there are F_{d-1} strings of the first kind and F_{d+1} strings of the second kind. Equation (4) now completes the proof of (2) and therefore of (1).

3. A GENERALIZATION

I now consider the obvious extension of the question answered in section 2, that is, what is S_n, the number of seating arrangements that are distinct not only under rotations but also under reflections? Now the group acting on V_n is the dihedral group, D_n, which is generated by σ and the reflection τ, which acts on a string in V_n by writing it backwards (so that $\sigma^n = \tau^2 = 1$ and $\sigma^{-1}\tau = \tau\sigma$).

Let W_k denote the set of palindromic strings w_k in U_k and, for $\eta = 0$ or 1, let $\mathrm{W}_{k,\eta}$ denote the subset of W_k of strings that begin (or end) with η. Now $\mathrm{D}_n = \{\sigma^m \tau^\varepsilon : 0 \le m < n, \varepsilon = 0, 1\}$, $\mathrm{Fix}(\sigma^m)$ is as in section 1, and (as is easy to see) $\mathrm{Fix}(\sigma^m \tau)$ is made up of strings $w_{n-m} w_m$, where w_{n-m} and w_m do not both have 1's at each end. So

$$\#\mathrm{Fix}(\sigma^m \tau) = \#\mathrm{W}_{n-m,0}\#\mathrm{W}_{m,0} + \#\mathrm{W}_{n-m,1}\#\mathrm{W}_{m,0} + \#\mathrm{W}_{n-m,0}\#\mathrm{W}_{m,1}. \tag{5}$$

Using (3), we have, for even k,

$$\#W_{k,1} = \#U_{k/2-3} = F_{k/2-1},$$
$$\#W_{k,0} = \#U_{k/2-2} = F_{k/2},$$

and, if k is odd,

$$\begin{aligned} \#W_{k,1} &= \#U_{(k-5)/2} + \#U_{(k-7)/2} = F_{(k+1)/2}, \\ \#W_{k,0} &= \#U_{(k-3)/2} + \#U_{(k-5)/2} = F_{(k+3)/2}. \end{aligned} \tag{6}$$

With the help of the well-known identity, $F_{r-1}F_s + F_rF_{s+1} = F_{r+s}$, it follows from (5) and (6) that

$$\#\mathrm{Fix}(\sigma^m\tau) = \begin{cases} F_{n/2} & \text{if } n \text{ and } m \text{ are even,} \\ F_{n/2+3} & \text{if } n \text{ is even and } m \text{ is odd,} \\ F_{(n+3)/2} & \text{if } n \text{ is odd,} \end{cases}$$

and Burnside's lemma gives

$$S_n = \begin{cases} \dfrac{1}{2n}\sum_{d|n} L_d\phi(n/d) + \dfrac{1}{2}F_{n/2+2} & \text{if } n \text{ is even,} \\ \dfrac{1}{2n}\sum_{d|n} L_d\phi(n/d) + \dfrac{1}{2}F_{(n+3)/2} & \text{if } n \text{ is odd.} \end{cases}$$

REFERENCES

1. P. J. Bushell. "Shapiro's Cyclic Sum." *Bull. London Math. Soc.* **26** (1994):569-74.
2. W. R. Scott. *Group Theory.* Englewood Cliffs, N.J.: Prentice Hall, 1964.

AMS Classification Number: 11B39

❖❖❖

ELEMENTARY PROBLEMS AND SOLUTIONS

Edited by
Stanley Rabinowitz

Please send all material for ELEMENTARY PROBLEMS AND SOLUTIONS to Dr. STANLEY RABINOWITZ; 12 VINE BROOK RD; WESTFORD, MA 01886-4212 USA. Correspondence may also be sent to the problem editor by electronic mail to Fibonacci@MathPro.com *on Internet. All correspondence will be acknowledged.*

Each solution should be on a separate sheet (or sheets) and must be received within six months of publication of the problem. Solutions typed in the format used below will be given preference. Proposers of problems should normally include solutions. Proposers should inform us of the history of the problem, if it is not original. A problem should not be submitted elsewhere while it is under consideration for publication in this column.

BASIC FORMULAS

The Fibonacci numbers F_n and the Lucas numbers L_n satisfy

$$F_{n+2} = F_{n+1} + F_n, \ F_0 = 0, \ F_1 = 1;$$
$$L_{n+2} = L_{n+1} + L_n, \ L_0 = 2, \ L_1 = 1.$$

Also, $\alpha = (1+\sqrt{5})/2$, $\beta = (1-\sqrt{5})/2$, $F_n = (\alpha^n - \beta^n)/\sqrt{5}$, and $L_n = \alpha^n + \beta^n$.

PROBLEMS PROPOSED IN THIS ISSUE

B-790 ***Proposed by H.-J. Seiffert, Berlin, Germany***

Find the largest constant c such that $F_{n+1}^2 > cF_{2n}$ for all even positive integers n.

B-791 ***Proposed by Andrew Cusumano, Great Neck, NY***

Prove that, for all n, $F_{n+11} + F_{n+7} + 8F_{n+5} + F_{n+3} + 2F_n$ is divisible by 18.

B-792 ***Proposed by Paul S. Bruckman, Edmonds, WA***

Let the sequence $\langle a_n \rangle$ be defined by the recurrence $a_{n+1} = a_n^2 - a_n + 1$, $n > 0$, where the initial term, a_1, is an arbitrary real number larger than 1. Express $\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \cdots$ in terms of a_1.

B-793 ***Proposed by Wray Brady, Jalisco, Mexico***

Show that $2^n L_n \equiv 2 \pmod 5$ for all positive integers n.

B-794 ***Proposed by Zdravko F. Starc, Vršac, Yugoslavia***

For x a real number and n a positive integer, prove that

$$\left(\frac{F_2}{F_1}\right)^x + \left(\frac{F_3}{F_2}\right)^x + \cdots + \left(\frac{F_{n+1}}{F_n}\right)^x \geq n + x \ln F_{n+1}.$$

B-795 ***Proposed by Wray Brady, Jalisco, Mexico***

Evaluate
$$\sum_{n=0}^{\infty} (-1)^n \frac{\pi^{2n}}{(2n)!} L_{2n}.$$

SOLUTIONS

A Cauchy Convolution

B-759 ***Proposed by H.-J. Seiffert, Berlin, Germany (Vol. 32, no. 1, February 1994)***

Show that for all positive integers k and all nonnegative integers n,

$$\sum_{j=0}^{n} F_{k(j+1)}P_{k(n-j+1)} = \frac{F_k P_{k(n+2)} - P_k F_{k(n+2)}}{2Q_k - L_k}.$$

Solution by Paul S. Bruckman, Edmonds, WA

Let $S_{n,k}$ denote the given sum. Treating k as fixed, make the following substitutions, for brevity: $s = \alpha^k, t = \beta^k, u = p^k$, and $v = q^k$. Then,

$$\begin{aligned}
S_{n,k}\sqrt{40} &= \sum_{j=0}^{n}(s^{j+1} - t^{j+1})(u^{n-j+1} - v^{n-j+1}) \\
&= \sum_{j=0}^{n}[su^{n+1}(s/u)^j - tu^{n+1}(t/u)^j - sv^{n+1}(s/v)^j + tu^{n+1}(t/v)^j] \\
&= \frac{su}{s-u}(s^{n+1} - u^{n+1}) - \frac{tu}{t-u}(t^{n+1} - u^{n+1}) - \frac{sv}{s-v}(s^{n+1} - v^{n+1}) + \frac{tv}{t-v}(t^{n+1} - v^{n+1}) \\
&= \frac{u}{(s-u)(t-u)}[(s^{n+2} - su^{n+1})(t-u) - (t^{n+2} - tu^{n+1})(s-u)] \\
&\quad - \frac{v}{(s-v)(t-v)}[(s^{n+2} - sv^{n+1})(t-v) - (t^{n+2} - tv^{n+1})(s-v)] \\
&= [(-1)^k p^{-k} + p^k - L_k]^{-1}[s^{n+2}t - stu^{n+1} - s^{n+2}u + su^{n+2} - st^{n+2} + stu^{n+1} + t^{n+2}u - tu^{n+2}] \\
&\quad - [(-1)^k q^{-k} + q^k - L_k]^{-1}[s^{n+2}t - stv^{n+1} - s^{n+2}v + sv^{n+2} - st^{n+2} + stv^{n+1} + t^{n+2}v - tv^{n+2}] \\
&= (2Q_k - L_k)^{-1}[s^{n+2}(t-u) + t^{n+2}(u-s) + u^{n+2}(s-t) - s^{n+2}(t-v) - t^{n+2}(v-s) - v^{n+2}(s-t)] \\
&= (2Q_k - L_k)^{-1}[(u^{n+2} - v^{n+2})(s-t) - (s^{n+2} - t^{n+2})(u-v)].
\end{aligned}$$

The result follows.

Also solved by Glenn Bookhout, C. Georghiou, Pentti Haukkanen, and the proposer.

A Simple Inequality

B-760 ***Proposed by Russell Euler, Northwest Missouri State University, Maryville, MO (Vol. 32, no. 2, May 1994)***

Prove that $F_{n+1}^2 \geq F_{2n}$ for all $n \geq 0$.

Solution by many readers

This inequality follows from Hoggatt's Identity (I_{10}) from [1]:

$$F_{2n} = F_{n+1}^2 - F_{n-1}^2.$$

The inequality is true for all n, not just $n \geq 0$. Equality holds if and only if $F_{n-1} = 0$, i.e., if and only if $n = 1$.

Reference

1. Verner E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin, 1969; rpt. Santa Clara, Calif.: The Fibonacci Association, 1979.

Lord pointed out the stronger inequality, $F_{n+p}^2 \geq F_{2n}F_{2p}$, which follows from Hoggatt's Identity (I_{25}). Prielipp mentions that the result $F_{m+n} \geq F_m F_n$, if $m, n > 0$, which comes from The American Mathematical Monthly, 1960, p. 876, implies that we can extend the given inequality to $F_{n+1}^2 \geq F_{2n} \geq F_n^2$ if $n \geq 0$. Seiffert generalized in another direction, and we present his result as problem B-790 in this issue.

Generalization by Richard André-Jeannin, Longwy, France

Consider the sequences $\langle U_n \rangle$ and $\langle V_n \rangle$ satisfying the recurrence $W_n = PW_{n-1} - QW_{n-2}$, $n \geq 2$, with initial conditions $U_0 = 0, U_1 = 1$ and $V_0 = 2, V_1 = P$. It is known and readily verified that $V_n = U_{n+1} - QU_{n-1}$ and $U_{2n} = U_n V_n$. Thus, $U_{n+1}^2 - Q^2 U_{n-1}^2 = (U_{n+1} + QU_{n-1})(U_{n+1} - QU_{n-1}) = PU_n V_n$ $= PU_{2n}$. Hence, $U_{n+1}^2 = Q^2 U_{n-1}^2 + PU_{2n}$. This gives us the desired generalization: $U_{n+1}^2 \geq PU_{2n}$.

Also solved by Charles Ashbacher, Michel A. Ballieu, Brian D. Beasley, Glenn Bookhout, Paul S. Bruckman, Charles K. Cook., Bill Correll, Jr., M. N. Deshpande, Steve Edwards, Piero Filipponi, Russell Jay Hendel, Norbert Jensen, Joseph J. Kostal, Harris Kwong, Carl Libis, Graham Lord, Bob Prielipp, H.-J. Seiffert, Sahib Singh, Lawrence Somer, M. N. S. Swamy, David C. Terr, and the proposer.

L Determinants

B-761 ***Proposed by Richard André-Jeannin, Longwy, France (Vol. 32, no. 2, May 1994)***

Evaluate the determinants

$$\begin{vmatrix} L_0 & L_1 & L_2 & L_3 & L_4 \\ L_1 & L_0 & L_1 & L_2 & L_3 \\ L_2 & L_1 & L_0 & L_1 & L_2 \\ L_3 & L_2 & L_1 & L_0 & L_1 \\ L_4 & L_3 & L_2 & L_1 & L_0 \end{vmatrix} \quad \text{and} \quad \begin{vmatrix} L_0^2 & L_1^2 & L_2^2 & L_3^2 & L_4^2 \\ L_1^2 & L_0^2 & L_1^2 & L_2^2 & L_3^2 \\ L_2^2 & L_1^2 & L_0^2 & L_1^2 & L_2^2 \\ L_3^2 & L_2^2 & L_1^2 & L_0^2 & L_1^2 \\ L_4^2 & L_3^2 & L_2^2 & L_1^2 & L_0^2 \end{vmatrix}.$$

Solution by Harris Kwong, SUNY College at Fredonia, Fredonia, NY

Let $A_n = (a_{ij})$ and $B_n = (b_{ij})$ be $n \times n$ matrices such that $a_{ij} = L_{|i-j|}$ and $b_{ij} = L_{|i-j|}^2$. The values of $\det(A_n)$ and $\det(B_n)$ can be derived as follows.

For small n, we have $\det(A_1) = 2$ and $\det(A_2) = 3$. For $n \geq 3$, subtract the sum of the second and third rows of A_n from the first row, then subtract the difference of the first and third columns from the second column. In the modified matrix, the first row is $(-2, 0, \ldots)$, and the second column is $(0, 2, 0, \ldots)^{\mathrm{T}}$. Hence, for $n \geq 3$, $\det(A_n) = -4\det(A_{n-2})$. Consequently, $\det(A_{2n-1}) = 2(-4)^{n-1}$ and $\det(A_{2n}) = 3(-4)^{n-1}$.

It is straightforward to check that $\det(B_1) = 4$, $\det(B_2) = 15$, and $\det(B_3) = -250$. For $n \geq 4$, add the fourth row of B_n to the first row, then add the third row to the second row. Since

$$L_n^2 + L_{n+3}^2 = (L_{n+2} - L_{n+1})^2 + (L_{n+2} + L_{n+1})^2 = 2(L_{n+2}^2 + L_{n+1}^2),$$

the first and second rows of the modified matrix are proportional, namely, in the ratio of $2:1$. Thus, $\det(B_n) = 0$ for $n \geq 4$.

In particular, the given determinants are $\det(A_5) = 32$ and $\det(B_5) = 0$, respectively.

Also solved by Charles Ashbacher, Paul S. Bruckman, Charles K. Cook, Bill Correll, Jr., Russell Jay Hendel, Norbert Jensen, Carl Libis, H.-J. Seiffert, and the proposer.

Taylor's Series

B-762 ***Proposed by Larry Taylor, Rego Park, NY (Vol. 32, no. 2, May 1994)***

Let n be an integer.

(a) Generalize the numbers (2, 2, 2) to form three three-term arithmetic progressions of integral multiples of Fibonacci and/or Lucas numbers with common differences $3F_n$, $5F_n$, and $3F_n$.

(b) Generalize the numbers (4, 4, 4) to form two such arithmetic progressions with common differences F_n and F_n.

(c) Generalize the numbers (6, 6, 6) to form four such arithmetic progressions with common differences F_n, $5F_n$, $7F_n$, and F_n.

Solution by H.-J. Seiffert, Berlin, Germany

The proofs of the statements presented in the following table are all easy and thus will be omitted.

Arithmetic Progression	Common Difference	Generalizes ($n = 0$)
$(-2F_{n-2}, L_n, 2F_{n+2})$	$3F_n$	$(2, 2, 2)$
$(-2L_{n-1}, L_n, 2L_{n+1})$	$5F_n$	$(2, 2, 2)$
$(2F_{n-1}, F_{n+3}, 2L_{n+1})$	$3F_n$	$(2, 2, 2)$
$(2F_{n+3}, L_{n+3}, 4F_{n+2})$	F_n	$(4, 4, 4)$
$(-4F_{n-2}, -L_{n-3}, 2F_{n-3})$	F_n	$(4, 4, 4)$
$(2L_{n+2}, 3F_{n+3}, 2F_{n+4})$	F_n	$(6, 6, 6)$
$(2L_{n-2}, 3L_n, 2L_{n+2})$	$5F_n$	$(6, 6, 6)$
$(-2F_{n-4}, 3L_n, 2F_{n+4})$	$7F_n$	$(6, 6, 6)$
$(-2F_{n-4}, 3F_{n-3}, 2L_{n-2})$	F_n	$(6, 6, 6)$

Editorial Comment: Larry Taylor asked about three-term arithmetic progressions such that

(1) each term is an integral multiple of either F_{n+a} or L_{n+a} for some integer a;

(2) the common difference is a positive integral multiple of F_n;

(3) the values assumed by the terms when $n = 0$ are positive, equal, and do not exceed 6.

He conjectured that all such arithmetic progressions are given by the solutions of problems B-762 and H-422 (*The Fibonacci Quarterly* **28.3** [1990]:285-87).

Bruckman investigated this problem and came up with the following table of arithmetic progressions of the form $(a_1H_{n+b_1}, a_2J_{n+b_2}, a_3K_{n+b_3})$ with common difference cF_n and where H, J, and K are each either "F" or "L". When $n = 0$, these progressions reduce to (e, e, e).

a_1	H	b_1	a_2	J	b_2	a_3	K	b_3	c	e
−1	L	−1	−1	F	−2	1	F	−1	1	1
−1	F	−2	+1	F	−1	1	F	+1	1	1
+1	F	−1	+1	F	+1	1	F	+2	1	1
+1	F	+1	+1	F	+2	1	L	+1	1	1
−1	L	−1	+1	F	−1	1	F	+2	2	1
−1	F	−2	+1	F	+1	1	L	+1	2	1
−2	F	−2	+1	F	−3	2	F	−1	1	2
+1	F	−3	+2	F	−1	1	L	0	1	2
+2	F	−1	+1	L	0	2	F	+1	1	2
+1	L	0	+2	F	+1	1	F	+3	1	2
+2	F	+1	+1	F	+3	2	F	+2	1	2
+1	F	−3	+1	L	0	1	F	+3	2	2
−2	L	−1	+1	F	−3	2	F	+1	3	2
−2	F	−2	+1	L	0	2	F	+2	3	2
+2	F	−1	+1	F	+3	2	L	+1	3	2
−2	L	−1	+1	L	0	2	L	+1	5	2
−3	F	−2	−1	F	−4	1	L	−2	1	3
−1	F	−4	+1	L	−2	3	F	−1	1	3
+3	F	+1	+1	L	+2	1	F	+4	1	3
+1	L	+2	+1	F	+4	3	F	+2	1	3
−3	L	−1	+1	L	−2	1	L	+2	5	3
+1	L	−2	+1	L	+2	3	L	+1	5	3
−4	F	−2	−1	L	−3	2	F	−3	1	4
+2	F	+3	+1	L	+3	4	F	+2	1	4
−4	L	−1	−1	L	−3	2	L	0	5	4
−1	L	−3	+2	L	0	1	L	+3	5	4
+2	L	0	+1	L	+3	4	L	+1	5	4
−2	F	−4	+3	F	−3	2	L	−2	1	6
+2	L	+2	+3	F	+3	2	F	+4	1	6
+2	L	−2	+3	L	0	2	L	+2	5	6
−2	F	−4	+3	L	0	2	F	+4	7	6

He believes the list is exhaustive [for $e \le 6$ and $\gcd(a_1, a_2, a_3) = 1$] but does not have a proof. The editor did a computer search and did not find any additional examples even if condition (2) is dropped.

Also solved by Paul S. Bruckman and the proposer.

Matrix Power

B-763 ***Proposed by Juan Pla, Paris, France***
(Vol. 32, no. 2, May 1994)

Let

$$A = \begin{pmatrix} e^{i\pi/3} & \sqrt{2} \\ \sqrt{2} & e^{-i\pi/3} \end{pmatrix}.$$

Express A^n in terms of Fibonacci and/or Lucas numbers.

Solution by H.-J. Seiffert, Berlin, Germany

The answer is

$$A^n = F_n A + F_{n-1} I, \tag{1}$$

where I denotes the identity matrix.

We prove this result for any matrix A of the form

$$A = \begin{pmatrix} a & c \\ b & 1-a \end{pmatrix}$$

with determinant -1 (which is true of our present proposal).

By direct calculation, we have $A^2 = A + I$ since $\det A = -1$, so equation (1) is true for $n = 2$. It is also clearly true for $n = 1$. We proceed by induction. Assume that equation (1) holds for some n. Then $A^{n+1} = A^n A = (F_n A + F_{n-1} I)A = F_n A^2 + F_{n-1} A = F_n(A + I) + F_{n-1} A = (F_n + F_{n-1})A + F_n I = F_{n+1} A + F_n I$ and equation (1) holds for $n+1$. Thus it is true for all positive integral n.

Seiffert also showed that equation (1) is true for all negative n as well. We omit the proof.

Also solved by Brian D. Beasley, Paul S. Bruckman, Charles K. Cook, Steve Edwards, Piero Filipponi, Russell Jay Hendel, Norbert Jensen, Hans Kappus, Murray S. Klamkin, Joseph J. Kostal, Bob Prielipp, M. N. S. Swamy, and the proposer.

Secret Treasures Hidden in Pascal's Triangle

B-764 ***Proposed by Mark Bowron, Tucson, AZ***
(Vol. 32, no. 2, May 1994)

Consider row n of Pascal's triangle, where n is a fixed positive integer. Let S_k denote the sum of every fifth entry, beginning with the k^{th} entry, $\binom{n}{k}$. If $0 \le i < j < 5$, show that $|S_i - S_j|$ is always a Fibonacci number.

Solution by the proposer, Channelview, TX

For $n \ge 1$, let $s_k(n)$ be the sum of every fifth entry in row n (including entries outside Pascal's triangle, which by convention are all zero) that includes $\binom{n}{\lfloor n/2 \rfloor - 2 - k}$ as a summand $(0 \le k < 5)$. The following hold by symmetry of Pascal's triangle:

n even	n odd
$s_0(n) = s_4(n)$	$s_1(n) = s_4(n)$
$s_1(n) = s_3(n)$	$s_2(n) = s_3(n)$

Define $D_0(n) = s_1(n) - s_0(n)$, $D_1(n) = s_2(n) - s_1(n)$, and $D_2(n) = s_2(n) - s_0(n)$. By the above, it suffices to show that $D_0(n)$, $D_1(n)$, and $D_2(n)$ are Fibonacci numbers for each $n \ge 1$. Claim:

n even	n odd
$D_0(n) = F_n$	$D_0(n) = F_{n-1}$
$D_1(n) = F_{n-1}$	$D_1(n) = F_n$
$D_2(n) = F_{n+1}$	$D_2(n) = F_{n+1}$

The proof is by induction on n. The claim is easily seen to hold for $n = 1$. Let $n > 1$ and assume that the claim holds for all positive integers less than n.

Suppose n is even. By the recursion that defines Pascal's triangle, we have

$$s_0(n) = s_0(n-1) + s_1(n-1),$$
$$s_1(n) = s_1(n-1) + s_2(n-1),$$
$$s_2(n) = s_2(n-1) + s_3(n-1) = 2s_2(n-1).$$

Thus, by the induction hypothesis and previous results,

$$\begin{aligned} D_0(n) &= s_1(n) - s_0(n) = s_1(n-1) + s_2(n-1) - s_0(n-1) - s_1(n-1) \\ &= D_0(n-1) + D_1(n-1) = F_{n-2} + F_{n-1} = F_n; \\ D_1(n) &= s_2(n) - s_1(n) = 2s_2(n-1) - s_1(n-1) - s_2(n-1) \\ &= D_1(n-1) = F_{n-1}; \\ D_2(n) &= s_2(n) - s_0(n) = 2s_2(n-1) - s_0(n-1) - s_1(n-1) \\ &= D_2(n-1) + D_1(n-1) = F_n + F_{n-1} = F_{n+1}. \end{aligned}$$

The equations for odd n are similar. This completes the proof.

Also solved by Paul S. Bruckman, Norbert Jensen, and H.-J. Seiffert.

An Expansion of e

B-765 ***Proposed by Mohammad K. Azarian, University of Evansville, Evansville, IN (Vol. 32, no. 2, May 1994)***

Let m and n be positive integers greater than 1, and let $x = F_{mn}/(F_mF_n)$. What famous constant is represented by

$$\left[\sum_{i=0}^{\infty}\left(\sum_{j=0}^{i}\frac{1}{j!}\right)\left(\frac{1}{x^i}-\frac{1}{x^{i+1}}\right)\right]^x?$$

Solution by Norbert Jensen, Kiel, Germany

For $m, n > 1$, we have $F_{mn} \ge F_{m+n} = F_mF_{n+1} + F_{m-1}F_n > F_mF_n$. Thus $x > 1$ and all the terms of the series are positive. We may thus rearrange the order of summation.

We find that for any $x > 1$,

$$\begin{aligned} \left[\sum_{i=0}^{\infty}\left(\sum_{j=0}^{i}\frac{1}{j!}\right)\left(\frac{1}{x^i}-\frac{1}{x^{i+1}}\right)\right]^x &= \left[\sum_{i=0}^{\infty}\left(\sum_{j=0}^{i}\frac{1}{j!}\right)\frac{1}{x^i}\left(1-\frac{1}{x}\right)\right]^x = \left(\frac{x-1}{x}\right)^x\left[\sum_{i=0}^{\infty}\left(\sum_{j=0}^{i}\frac{1}{j!}\right)\frac{1}{x^i}\right]^x \\ &= \left(\frac{x-1}{x}\right)^x\left[\sum_{j=0}^{\infty}\frac{1}{j!}\sum_{i=j}^{\infty}\frac{1}{x^i}\right]^x = \left(\frac{x-1}{x}\right)^x\left[\sum_{j=0}^{\infty}\frac{x^{-j}}{j!}\,\frac{x}{x-1}\right]^x \\ &= \left(\frac{x-1}{x}\right)^x\left[\frac{x}{x-1}e^{1/x}\right]^x = e. \end{aligned}$$

Thus the magic constant is e.

Also solved by O. Brugia and P. Filipponi (jointly), Paul S. Bruckman, Bill Correll, Jr., Steve Edwards, Russell Jay Hendel, Hans Kappus, Carl Libis, H.-J. Seiffert, and the proposer.

ADVANCED PROBLEMS AND SOLUTIONS

Edited by
Raymond E. Whitney

Please send all communications concerning ADVANCED PROBLEMS AND SOLUTIONS to RAYMOND E. WHITNEY, MATHEMATICS DEPARTMENT, LOCK HAVEN UNIVERSITY, LOCK HAVEN, PA 17745. This department especially welcomes problems believed to be new or extending old results. Proposers should submit solutions or other information that will assist the editor. To facilitate their consideration, all solutions should be submitted on separate signed sheets within two months after publication of the problems.

PROBLEMS PROPOSED IN THIS ISSUE

H-499 ***Proposed by Paul S. Bruckman, Edmonds, WA***

Given n a natural number, n is a *Lucas pseudoprime* (LPP) if it is composite and satisfies the following congruence:

$$L_n \equiv 1 \pmod{n}. \tag{1}$$

If $\gcd(n, 10) = 1$, the *Jacobi symbol* $(5/n) = \varepsilon_n$ is given by the following:

$$\varepsilon_n = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{10}, \\ -1 & \text{if } n \equiv \pm 3 \pmod{10}. \end{cases}$$

Given $\gcd(n, 10) = 1$, n is a *Fibonacci pseudoprime* (FPP) if it is composite and satisfies the following congruence:

$$F_{n-\varepsilon_n} \equiv 0 \pmod{n}. \tag{2}$$

Define the following sequences for $e = 1, 2, \ldots$:

$$u = u_e = F_{3^{e+1}} / F_{3^e}; \tag{3}$$

$$v = v_e = L_{3^{e+1}} / L_{3^e}; \tag{4}$$

$$w = w_e = F_{2\cdot 3^{e+1}} / F_{2\cdot 3^e} = uv. \tag{5}$$

Prove the following for all $e \ge 1$:

(i) u is a FPP and a LPP, provided it is composite;

(ii) same statement for v;

(iii) w is a FPP but not a LPP.

H-500 ***Proposed by H.-J. Seiffert, Berlin, Germany***

Define the Fibonacci polynomials by $F_0(x) = 0$, $F_1(x) = 1$, $F_n(x) = xF_{n-1}(x) + F_{n-2}(x)$, for $n \ge 2$. Show that for all complex numbers x and all nonnegative integers n,

$$\sum_{k=0}^{[n/2]}\binom{2n+2}{n-2k}F_{2k+1}(x)=x^nF_{n+1}(4/x), \tag{1}$$

where [ ] denotes the greatest integer function.

As special cases of (1), obtain the following identities:

$$\sum_{k=0}^{[n/2]}\binom{2n+2}{n-2k}F_{2k+1}=\frac{1}{2}F_{3n+3}; \tag{2}$$

$$\sum_{k=0}^{[n/2]}\binom{2n+2}{n-2k}F_{6k+3}=2^{2n+1}F_{n+1}; \tag{3}$$

$$\sum_{k=0}^{[n/2]}\binom{2n+2}{n-2k}L_{4k+2}=\frac{1}{2}(5^{n+1}-(-1)^{n+1}). \tag{4}$$

H-501 ***Proposed by Paul S. Bruckman, Edmonds, WA***

Define the following sequences for $e = 1, 2, \ldots$:

(i) $u = u_e = F_{5^{e+1}} / 5F_{5^e}$;

(ii) $v = v_e = L_{5^{e+1}} / L_{5^e}$;

(iii) $w = w_e = F_{2\cdot 5^{e+1}} / 5F_{2\cdot 5^e} = uv$.

Prove the following:

(a) If u is composite, it is both a Fibonacci pseudoprime (FPP) and a Lucas pseudoprime (LPP); see Problems H-496 and H-498 for definitions of FPP's and LPP's.

(b) Same problem for v.

(c) Show that w is a FPP but not a LPP.

H-502 ***Proposed by Zdzislaw W. Trzaska, Warsaw, Poland***

Given two sequences of polynomials in complex variable $z \in C$ defined recursively as

$$T_k(z)=\sum_{m=0}^{k}a_{km}z^m,\ k=0,1,2,\ldots, \tag{1}$$

with $T_0(z)=1$ and $T_1(z)=(1+z)T_0$, and

$$P_k(z)=\sum_{m=0}^{k}b_{km}z^m,\ k=0,1,2,\ldots, \tag{2}$$

with $P_0(z)=0$ and $P_1(z)=1$.

Prove that for all $z \in C$ and $k=0,1,2,\ldots$, the equality

$$P_k(z)T_{k-1}(z)-T_k(z)P_{k-1}(z)=1 \tag{3}$$

holds.

SOLUTIONS

Eventually

H-485 ***Proposed by Paul S. Bruckman, Edmonds, WA***
(Vol. 32, no. 1, February 1994)

If x is an unspecified large positive real number, obtain an asymptotic evaluation for the sum $S(x)$, where

$$S(x) = \sum_{p \le x} (-1)^{Z(p)}; \tag{1}$$

here, the p's are prime and $Z(p)$ is the Fibonacci entry-point of p (the smallest positive n such that $p | F_n$).

Solution by the proposer

Let $\mathscr{L} = \{L_n\}_{n \ge 0}$ denote the Lucas sequence. It is well known that $Z(p)$ is even iff $p \in \rho(\mathscr{L})$, where $\rho(\mathscr{L})$ denotes the set of primes p such that p divides an element of $\mathscr{L}$. Let $\pi_{\mathscr{L}}(x)$ denote the number of primes $p \in \rho(\mathscr{L})$ with $p \le x$; also, $\pi(x)$ denotes the number of $p \le x$. The density of $\rho(\mathscr{L})$ is defined as $\lim_{x \to \infty} \pi_{\mathscr{L}}(x) / \pi(x) \equiv \theta_{\mathscr{L}}$, assuming such a limit exists.

In 1985, Lagarias showed [1], among other things, that $\theta_{\mathscr{L}} = 2/3$. We see that this result is equivalent to the following:

$$\lim_{x \to \infty} A(x) / \pi(x) = \theta_{\mathscr{L}} = 2/3, \tag{2}$$

where

$$A(x) \equiv \sum_{\substack{p \le x \\ Z(p) \text{ even}}} 1; \text{ also, } B(x) \equiv \sum_{\substack{p \le x \\ Z(p) \text{ odd}}} 1. \tag{3}$$

Also note that $A(x) - B(x) = S(x)$ and $A(x) + B(x) = \pi(x)$. Moreover, we recall the famous Prime Number Theorem, namely,

$$\pi(x) \sim \frac{x}{\log x} \quad (\text{as } x \to \infty). \tag{4}$$

Consequently, we see that

$$A(x) \sim \frac{2x}{3 \log x}, \quad B(x) \sim \frac{x}{3 \log x}, \quad \text{and} \quad S(x) \sim B(x),$$

or:

$$S(x) \sim \frac{x}{3 \log x}. \tag{5}$$

Reference

1. J. C. Lagarias. "The Set of Primes Dividing the Lucas Numbers Has Density 2/3." *Pacific J. Math.* **118** (1985):19-23.

Long Range PI

H-486 ***Proposed by Piero Filipponi, Rome, Italy***
(Vol. 32, no. 2, May 1994)

Let the terms of the sequence $\{Q_k\}$ be defined by the second-order recurrence relation $Q_k = 2Q_{k-1}+Q_{k-2}$ with initial conditions $Q_0 = Q_1 = 1$. Find restrictions on the positive integers n and m for

$$T(n,m)=\sum_{k=1}^{\infty}\frac{k^2n^kQ_k}{m^k}$$

to converge, and, under these restrictions, evaluate this sum. Moreover, find the set of all couples (n_i, m_i) for which $T(n_i, m_i)$ is an integer.

Solution by Charles K. Cook, University of South Carolina at Sumter, Sumter, SC

The ratio test shows that the series will converge if

$$\frac{n}{m}<\sqrt{2}-1\approx .4142. \text{ Thus, } \left|\frac{n}{m}(1\pm\sqrt{2})\right|<1.$$

Since $Q_k=\frac{1}{2}[(1+\sqrt{2})^k+(1-\sqrt{2})^k]$, it follows from the summation formula

$$\sum_{k=1}^{\infty}k^2x^k=\frac{x(1+x)}{(1-x)^3},\ |x|<1,$$

that

$$T=\sum_{k=1}^{\infty}k^2\left(\frac{n}{m}\right)^kQ_k=\frac{1}{2}\left(\sum_{k=1}^{\infty}k^2\left[\frac{n}{m}(1+\sqrt{2})\right]^k+\sum_{k=1}^{\infty}k^2\left[\frac{n}{m}(1-\sqrt{2})\right]^k\right)$$

simplifies to

$$T(n,m)=\frac{nm(m^2+n^2)(m^2+6mn-n^2)}{(m^2-2mn-n^2)}.$$

The only values of (n, m) for which T will be integral are those satisfying $m^2-2mn-n^2=1$ or $(n-m)^2=1+2n^2$. The equation

$$x^2-2n^2=1$$

is a Pell equation with the fundamental solution $x_1=3$ and $n_1=2$. Thus, the solution set $\{(x_k, n_k)\}$ is generated from

$$x_k+y_k\sqrt{2}=(3+2\sqrt{2})^k.$$

Since $m = x + n$ all pairs (n, m) leading to the integral values of $T(n, m)$ are determined. The first four are $(2, 5)$, $(12, 29)$, $(70, 169)$, and $(408, 985)$. The first three integral values of T are 23490, 954642300, and 37463036986830.

Also solved by P. Bruckman, H.-J. Seiffert, and the proposer (partial solution).

Nice Couples

H-487 ***Proposed by Stanley Rabinowitz, MathPro Press, Westford, MA (Vol. 32, no. 2, May 1994)***

Suppose H_n satisfies a second-order linear recurrence with constant coefficients. Let $\{a_i\}$ and $\{b_i\}$, $i = 1, 2, \ldots, r$, be integer constants and let $f(x_0, x_1, x_2, \ldots, x_r)$ be a polynomial with integer coefficients. If the expression

$$f((-1)^n, H_{a_1n+b_1}, H_{a_2n+b_2}, \ldots, H_{a_rn+b_r})$$

vanishes for all integers $n > N$, prove that the expression vanishes for all integral n.

[As a special case, if an identity involving Fibonacci and Lucas numbers is true for all positive subscripts, then it must also be true for all negative subscripts as well.]

Solution by Paul S. Bruckman, Edmonds, WA

Let $\underline{H}_n = \{(-1)^n, H_{a_1n+b_1}, H_{a_2n+b_2}, \ldots, H_{a_rn+b_r}\}$ and $f_n \equiv f(\underline{H}_n)$. Also, let Π_n denote any product of the form $(-1)^{ne_0}H^{e_1}_{a_1n+b_1} \cdots H^{e_r}_{a_rn+b_r}$, $e_i \geq 0$ and integers. Since H_n has a nullifying (i.e., characteristic) polynomial satisfying the recurrence relation $P(E)(H_n) = 0$ (here E is the unit "right-shift" operator, with n the operand, and P is a polynomial with constant coefficients, of second degree), it follows that $H_{a_in+b_i}$ also has a nullifying polynomial; then so does $H^{e_i}_{a_in+b_i}$, where the integers e_i are nonnegative. The same is true for $(-1)^{ne_0}$, for which the nullifying polynomial is $E-(-1)^{e_0}$. Then any product Π_n has a nullifying polynomial; since f_n is a sum of products of the form Π_n, it follows that f_n itself has a nullifying polynomial, say $G(x)$. Thus, $G(E)(f_n) = 0$ *for all n*. We may suppose that $G(x) = \sum_{j=m}^{M} c_j x^j$, where $M \geq m \geq 0$, $c_m \neq 0$, $c_M \neq 0$. We consider two possibilities:

(a) $m = M$—then $G(E)(f_n) = c_m f_{m+n} = 0$ for all n, which implies $f_n = 0$ for all n;

(b) $M > m \geq 0$. Then $G(E)(f_{N-m}) = \sum_{j=m}^{M} c_j f_{N-m+j} = c_m f_N = 0$, since $f_{N+1} = f_{N+2} = \cdots = 0$, by hypothesis. Thus, $f_N = 0$.

We may repeat the process (i.e., setting $n = N-1-m,\ N-2-m$, etc.), and conclude that $f_n = 0$ for all n. Q.E.D.

Pseudo Nim

H-488 ***Proposed by Paul S. Bruckman, Edmonds, WA (Vol. 32, no. 4, August 1994)***

The *Fibonacci pseudoprimes* (FPP's) are those composite integers n with $\gcd(n, 10) = 1$ and satisfying the following congruence:

$$F_{n-\varepsilon_n} \equiv 0 \pmod{n}, \tag{i}$$

where

$$\varepsilon_n = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{10}, \\ -1 & \text{if } n \equiv \pm 3 \pmod{10}. \end{cases}$$

$$\left[\text{Thus, } \varepsilon_n = (\tfrac{5}{n}), \text{ a Jacobi symbol.}\right]$$

Given a prime $p > 5$, prove that $u = \frac{1}{3}L_{2_p}$ is a FPP if u is composite.

The *Lucas pseudoprimes* (LPP's) are those composite positive integers n satisfying the following congruence:

$$L_n \equiv 1 \pmod{n}. \tag{ii}$$

Given a prime $p > 5$, prove that $u = \frac{1}{3}L_{2_p}$ is a LPP if u is composite.

Solution by Norbert Jensen, Kiel, Germany

Step 0: 3 divides L_{2p}; hence, u is always an integer.

Proof: Consider the Lucas numbers modulo 3: $L_0 = 2$, $L_1 = 1$, $L_2 \equiv 0$, $L_3 \equiv 1$, $L_4 \equiv 1$, $L_5 \equiv 2$, $L_6 \equiv 0$, $L_7 \equiv 2$, $L_8 \equiv 2 = L_0$, $L_9 \equiv 1 = L_1 \pmod 3$. Hence, $(L_n)_{n\in\mathbb{N}_0}$ has period length 8 modulo 3 and $L_n \equiv 0 \pmod 3$ if and only if $n \equiv 2$ or $n \equiv 6 \pmod 8$. But as $p \equiv 1$ or $\equiv 3 \pmod 4$, it is clear that $2p \equiv 2$ or $2p \equiv 6 \pmod 8$. Q.E.D. (Step 0)

Suppose that u is composite. We have to show that u is a FPP and a LPP.

Step 1: We show that $u \equiv 1 \pmod{10}$. Hence, $\gcd(u, 10) = 1$.

Proof: Consider the residues of $(L_n)_{n\in\mathbb{N}_0}$ mod 10: $L_0 = 2$, $L_1 = 1$, $L_2 = 3$, $L_3 = 4$, $L_4 \equiv -3$, $L_5 \equiv 1$, $L_6 \equiv -2$, $L_7 \equiv -1$, $L_8 \equiv -3$, $L_9 \equiv -4$, $L_{10} \equiv 3$, $L_{11} \equiv -1$, $L_{12} \equiv 2 = L_0$, $L_{13} \equiv 1 = L_1$. Hence, the sequence $(L_n)_{n\in\mathbb{N}_0}$ has period length 12 mod 10. As p is either $\equiv 1$ or $\equiv -1$ mod 6, it follows that $2p$ is either $\equiv 2$ or $\equiv -2$ mod 12. Hence, $L_{2p} \equiv L_2 = 3$ or $L_{2p} \equiv L_{10} \equiv 3$ mod 10. Cancelling 3 in the above congruences shows that $u \equiv 1 \pmod{10}$. Q.E.D. (Step 1)

In particular, we have $\varepsilon_u = 1$. So to prove that u is a FPP and a LPP, we have to demonstrate that $F_{u-1} \equiv 0$, $L_u \equiv 1 \pmod u$.

Step 2: We show that $L_{8p} \equiv 2$, $L_{8p+1} \equiv 1$, $F_{8p} \equiv 0$, $F_{8p+1} \equiv 1 \pmod u$. Hence, $8p$ is a common period of the Lucas and the Fibonacci sequence modulo u.

(Actually, it can be shown that—in terms of algebraic number theory—the order of α modulo the ideal $u\mathbb{Z}[\alpha]$ in $\mathbb{Z}[\alpha]$ is $8p$.)

Proof: From the definition of u, it follows that $\alpha^{2p} + \beta^{2p} = L_{2p} = 3u$ or $\alpha^{2p} = -\beta^{2p} + 3u$. By multiplication with $(1/\beta)^{2p} = (-\alpha)^{2p} = \alpha^{2p}$, we obtain $\alpha^{4p} = -1 + 3u\alpha^{2p}$. Squaring both sides, we arrive at

$$\alpha^{8p} = 1 - 6u\alpha^{2p} + 9u^2\alpha^{4p}. \tag{2.1}$$

Exchanging α and β in these operations leads to

$$\beta^{8p} = 1 - 6u\beta^{2p} + 9u^2\beta^{4p}. \tag{2.2}$$

Multiplying (2.1) and (2.2) by α and β, respectively, we obtain

$$\alpha^{8p+1} = \alpha - 6u\alpha^{2p+1} + 9u^2\alpha^{4p+1}. \tag{2.3}$$

$$\beta^{8p+1} = \beta - 6u\beta^{2p+1} + 9u^2\beta^{4p+1}. \tag{2.4}$$

Summing up (2.1), (2.2) and (2.3), (2.4) gives $L_{8p} \equiv 2 \pmod{u}$, $L_{8p+1} \equiv 1 \pmod{u}$. Now, subtracting (2.2) from (2.1) and (2.4) from (2.3) and multiplying with $\alpha - \beta = \sqrt{5}$ gives $5F_{8p} \equiv 0$ (mod u), $5F_{8p+1} \equiv 5 \pmod{u}$. By Step 1, 5 does not divide u; hence, we cancel 5 in the above congruences. Thus, $F_{8p} \equiv 0$, $F_{8p+1} \equiv 1 \pmod{u}$. Q.E.D. (Step 2)

It remains to show that $u \equiv 1 \pmod{8p}$.

Splitting up into congruences modulo prime powers, we obtain the following results (i.e., Steps 3 and 4).

Step 3: We show that $L_{2p} \equiv 3 \pmod{8}$.

Proof: First, we determine the period length of $(L_n)_{n\in\mathbb{N}_0}$ mod 8. We have $L_0 = 2$, $L_1 = 1$, $L_2 = 3$, $L_3 = 4$, $L_4 \equiv -1$, $L_5 \equiv 3$, $L_6 \equiv 2$, $L_7 \equiv -3$, $L_8 \equiv -1$, $L_9 \equiv 4$, $L_{10} \equiv 3$, $L_{11} \equiv -1$, $L_{12} \equiv 2 = L_0$, $L_{13} \equiv 1 = L_1 \pmod{8}$. Hence, 12 is the period length of $(L_n)_{n\in\mathbb{N}_0}$. Since $p > 5$, we just have to consider the following two cases:

Case 1: $p \equiv 1 \pmod{6}$. Then $2p \equiv 2 \pmod{12}$ and $L_{2p} \equiv L_2 = 3 \pmod{8}$.

Case 2: $p \equiv -1 \pmod{6}$. Then $2p \equiv 10 \pmod{12}$ and $L_{2p} \equiv L_{10} = 3 \pmod{8}$.

Q.E.D. (Step 3)

Step 4: We show that $L_{2p} \equiv 3 \pmod{p}$.

Proof: We need the following two facts:

$$L_{2p} = 2^{1-2p} \sum_{\substack{j=0 \\ j\equiv 0 \,(\mathrm{mod}\, 2)}}^{2p} \binom{2p}{j} 5^{j/2}; \tag{4.1}$$

$$\binom{2p}{j} \equiv 0 \pmod{p} \text{ if either } o < j < p \text{ or } p < j < 2p. \tag{4.2}$$

From these facts, it follows (using Fermat's theorem) that

$$4 \cdot L_{2p} \equiv 2^{2p} L_{2p} \equiv 2 \cdot (1 + 5^p) \equiv 2 \cdot 6 \pmod{p}.$$

Since p and 4 are coprime, we can cancel 4 on both sides of the congruence; whence the assertion follows. Q.E.D. (Step 4)

Step 5: Using Steps 3 and 4, we obtain $L_{2p} \equiv 3 \pmod{8p}$. Now, by Step 0, and since 3 and $8p$ are coprime, it follows that $u \equiv 1 \pmod{8p}$.

Step 6: Applying Steps 2 and 5, we see that $L_u \equiv L_1 = 1 \pmod{u}$ and $F_{u-1} \equiv 0 \pmod{u}$. Q.E.D.

Also solved by H.-J. Seiffert and the proposer.

❖❖❖

SUSTAINING MEMBERS

*H.L. Alder	J. De Kerf	R.E. Kennedy	J.A. Schumaker
G.L. Alexanderson	L.A.G. Dresel	C.H. Kimberling	A.G. Shannon
S. Ando	U. Dudley	Y.H.H. Kwong	L.W. Shapiro
R. Andre-Jeannin	M. Faccio	J. Lahr	J.R. Siler
*J. Arkin	D.R. Farmer	J.C. Lagarias	D. Singmaster
C. Ashbacher	D.C. Fielder	B. Landman	J. Sjoberg
M.K. Azarian	P. Filipponi	L.H. Lange	L. Somer
N. Balasubramania	Fondazione Ugo Bordoni	K.W. Lok	P. Spears
L. Bankoff	Emerson Frost	*C.T. Long	W.R. Spickerman
J.G. Bergart	Anthony Gioia	G. Lord	Paul K. Stockmeyer
G. Bergum	*H.W. Gould	*J. Maxwell	J. Suck
G. Berzsenyi	P. Hagis, Jr.	F.U. Mendizabal	M.N.S. Swamy
*M. Bicknell-Johnson	H. Harborth	J.L. Miller	*D. Thoro
P.S. Bruckman	P. Haukkanen	M.G. Monzingo	J.C. Turner
M.F. Bryn	*A.P. Hillman	J.F. Morrison	T.P. Vaughan
G.D. Chakerian	*A.F. Horadam	K. Nagasaka	J.N. Vitale
W.V. Chappelow	Y. Horibe	S.A. Obaid	M. Waddill
C. Chouteau	F.T. Howard	S. Palsson	*L.A. Walker
C.K. Cook	R.J. Howell	J. Pla	J.E. Walton
R.L. Creech	S. Howell	A. Prince	W.A. Webb
J.W. Creely	J.P. Jones	S. Rabinowitz	G.E. Weekly
M.G. DeBruin	R.N. Joyner	I. Sadoveanu	R.E. Whitney
M.J. DeLeon		S. Sato	B.E. Williams

*Charter Members

INSTITUTIONAL MEMBERS

CALIFORNIA STATE UNIVERSITY SACRAMENTO
Sacramento, California

CAREY VIGOR-ZIERK, M.D.
Santa Ana, California

ETH-BIBLIOTHEK
Zurich, Switzerland

GONZAGA UNIVERSITY
Spokane, Washington

HOLY NAME COLLEGE
Oakland, California

HOWELL ENGINEERING COMPANY
Bryn Mawr, California

INDIANA UNIVERSITY
Bloomington, Indiana

KLEPCO, INC.
Sparks, Nevada

LAURENTIAN UNIVERSITY
Sudbury, Ontario, Canada

MISSOURI SOUTHERN STATE COLLEGE
Joplin, Missouri

NATIONAL LIBRARY OF EDUCATION
Copenhagen, Denmark

SAN JOSE STATE UNIVERSITY
San Jose, California

SANTA CLARA UNIVERSITY
Santa Clara, California

UNIVERSITY OF NEW ENGLAND
Armidale, N.S.W. Australia

UNIVERSITY OF TECHNOLOGY
Sydney, N.S.W. Australia

WAKE FOREST UNIVERSITY
Winston-Salem, North Carolina

WASHINGTON STATE UNIVERSITY
Pullman, Washington

YESHIVA UNIVERSITY
New York, New York

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.

Applications of Fibonacci Numbers, Volumes 1-5. Edited by G.E. Bergum, A.F. Horadam and A.N. Philippou

Generalized Pascal Triangles and Pyramids Their Fractals, Graphs and Applications by Boris A. Bondarenko. Translated from the Russian and edited by Richard C. Bollinger, FA, 1993.

Please write to the Fibonacci Association, Santa Clara University, Santa Clara CA 95053, U.S.A., for more information and current prices.