The Fibonacci Quarterly

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

TABLE OF CONTENTS

VOLUME 30 MAY 1992 NUMBER 2

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.

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

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

SUBSCRIPTIONS, ADDRESS CHANGE, AND REPRINT INFORMATION

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

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

Annual domestic Fibonacci Association membership dues, which include a subscription to **THE FIBONACCI QUARTERLY,** are $35 for Regular Membership, $45 for Sustaining Membership, and $70 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.

©1992 by
The Fibonacci Association
All rights reserved, including rights to this journal
issue as a whole and, except where otherwise noted,
rights to each individual contribution.

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

EDITOR

GERALD E. BERGUM, South Dakota State University, Brookings, SD 57007-0194

ASSISTANT EDITORS

MAXEY BROOKE, Sweeny, TX 77480
JOHN BURKE, Gonzaga University, Spokane, WA 99258
LEONARD CARLITZ, Duke University, Durham, NC 27706
HENRY W. GOULD, West Virginia University, Morgantown, WV 26506
A.P. HILLMAN, University of New Mexico, Albuquerque, NM 87131
A.F. HORADAM, University of New England, Armidale, N.S.W. 2351, Australia
CLARK KIMBERLING, University of Evansville, Evansville, IN 47722
DAVID A. KLARNER, University of Nebraska, Lincoln, NE 68588
RICHARD MOLLIN, University of Calgary, Calgary T2N 1N4, Alberta, Canada
GARY L. MULLEN, The Pennsylvania State University, University Park, PA 16802
SAMIH OBAID, San Jose State University, San Jose, CA 95192
JOHN RABUNG, Randolph-Macon College, Ashland, VA 23005
NEVILLE ROBBINS, San Francisco State University, San Francisco, CA 94132
DONALD W. ROBINSON, Brigham Young University, Provo, UT 84602
LAWRENCE SOMER, Catholic University of America, Washington, D.C. 20064
M.N.S. SWAMY, Concordia University, Montreal H3C 1M8, Quebec, Canada
D.E. THORO, San Jose State University, San Jose, CA 95192
ROBERT F. TICHY, Technical University, Graz, Austria
CHARLES R. WALL, Trident Technical College, Charleston, SC 29411
WILLIAM WEBB, Washington State University, Pullman, WA 99164-2930

BOARD OF DIRECTORS
THE FIBONACCI ASSOCIATION

CALVIN LONG (President)
Washington State University, Pullman, WA 99164-2930

G.L. ALEXANDERSON
Santa Clara University, Santa Clara, CA 95053

PETER HAGIS, JR.
Temple University, Philadelphia, PA 19122

FRED T. HOWARD
Wake Forest University, Winston-Salem, NC 27109

MARJORIE JOHNSON (Secretary-Treasurer)
Santa Clara Unified School District, Santa Clara, CA 95051

JEFF LAGARIAS
Bell Laboratories, Murray Hill, NJ 07974

LESTER LANGE
San Jose State University, San Jose, CA 95192

THERESA VAUGHAN
University of North Carolina, Greensboro, NC 27412

STRONG DIVISIBILITY LINEAR RECURRENCES OF THE THIRD ORDER

Pavel Horák
T. G. Masaryk University, Brno, Czechoslovakia

(Submitted April 1990)

1. Introduction

A k^{th}-order linear recurrent sequence $\mathbf{u} = \{u_n : n = 1, 2, \ldots\}$ of integers, satisfying the following property for greatest common divisors:

$$(u_i, u_j) = |u_{(i,j)}| \quad \text{for all } i, j \geq 1,$$

is called a k^{th}-order strong divisibility sequence (SDS). The notion of strong divisibility was introduced by C. Kimberling in [3] for k^{th}-order linear recurrences $\{u_n : n = 0, 1, 2, \ldots\}$.

All the second-order SDS's have been described in [2]. A characterization of all the SDS's in certain subsystems of the system T of all the third-order linear recurrences of integers was given in [1]. The purpose of this note is to extend the results of [1] and to describe all the SDS's in further subsystems of T.

Let U denote the system of all the sequences $\mathbf{u} = \{u_n : n = 1, 2, \ldots\}$ defined by

$$u_1 = 1, \; u_2 = \nu \neq 0, \; u_3 = \mu \neq 0$$

$$u_{n+3} = a \cdot u_{n+2} + b \cdot u_{n+1} + c \cdot u_n, \quad \text{for } n \geq 1,$$

where ν, μ, a, b, and c are integers. The system of all the strong divisibility sequences from U will be denoted by D.

Notice that we may take $u_1 = 1$ without loss of generality as all the third-order SDS's with $u_2 \neq 0 \neq u_3$ are exactly all the nonzero integral multiples of the sequences from D.

Lemma 1.1: Let $\mathbf{u} = \{u_n\} \in U$. Then $u_2 | u_4$ if and only if there exists an integer f such that

$$(1) \qquad c = f \cdot \nu - a \cdot \mu.$$

Proof: From the above definition we obtain $u_2 = \nu$, $u_4 = a\mu + b\nu + c$ and the assertion follows.

2. The Case $a = b = c = 1$

Let V denote the system of all the sequences from U satisfying the condition $a = b = c = 1$, i.e., $\mathbf{u} = \{u_n\} \in V$ if and only if

$$(2) \qquad \begin{aligned} &u_1 = 1, \; u_2 = \nu \neq 0, \; u_3 = \mu \neq 0 \\ &u_{n+3} = u_{n+2} + u_{n+1} + u_n, \quad \text{for } n \geq 1. \end{aligned}$$

The following theorem will show that there are no SDS's in V.

Theorem 2.1: The system of sequences V contains no strong divisibility sequences, i.e., $V \cap D = \emptyset$.

Proof: Let us suppose that $\mathbf{u} = \{u_n\} \in V \cap D$. By Lemma 1.1, there exists an integer f such that

$$(3) \qquad \mu = f \cdot \nu - 1$$

and thus

$$u_4 = \nu \cdot (f + 1).$$

Then by (2):

$$u_5 = \nu \cdot (f + 2) + \mu \quad \text{and} \quad u_6 = \nu \cdot (2f + 3) + 2\mu.$$

From $u_2 | u_6$, $u_3 | u_6$, and $(\nu, \mu) = 1$, we get $\nu | 2$ and $\mu | 2f + 3$. Then, using (3), we obtain:

$$\nu = 1,\ \mu | 5 \quad \text{or} \quad \nu = -1,\ \mu | 1 \quad \text{or} \quad \nu = 2,\ \mu | 4 \quad \text{or} \quad \nu = -2,\ \mu | 2.$$

But ν, μ are coprime, which leaves 10 possible pairs of ν and μ. For all of them it is easy to find i, j (always ≤ 9) such that $(u_i, u_j) \ne |u_{(i, j)}|$. Therefore $\mathbf{u} \notin D$, a contradiction.

3. The Case $\mu = 1$; $a = b = 1$

Let W denote the system of all the sequences from U satisfying the conditions $\mu = 1$; $a = b = 1$, i.e., $\mathbf{u} = \{u_n\} \in W$ if and only if

$$(4) \qquad \begin{aligned} &u_1 = 1,\ u_2 = \nu \ne 0,\ u_3 = 1 \\ &u_{n+3} = u_{n+2} + u_{n+1} + c \cdot u_n, \quad \text{for } n \ge 1. \end{aligned}$$

Furthermore, let W_1, W_2 denote the following subsystems of W:

$$W_1 = \{\mathbf{u} \in W : u_2 | u_4 \text{ and } f = -1\}$$

$$W_2 = \{\mathbf{u} \in W : u_2 | u_4 \text{ and } f \ne -1\}$$

where f is the integer from (1). Obviously, W_1 and W_2 are disjoint and

$$D \cap W \subseteq W_1 \cup W_2.$$

Proposition 3.1: The system of sequences W_1 contains no strong divisibility sequences, i.e., $W_1 \cap D = \emptyset$.

Proof: Let $\mathbf{u} \in W_1 \cap D$; then $b + f = 0$ and, according to Theorem 3.1 of [1], we get $\mathbf{u} = \mathbf{c}$ or $\mathbf{u} = \mathbf{d}$ where

$$\mathbf{c} = \{1, 2, 1, 0, 1, 2, 1, 0, \ldots\}, \quad \mathbf{d} = \{1, -2, 1, 0, 1, -2, 1, 0, \ldots\}.$$

But $\mathbf{c}, \mathbf{d} \notin W$ and thus $\mathbf{u} \notin W_1$, a contradiction.

Lemma 3.2: Let $\mathbf{u} = \{u_n\} \in W_2$. Then:

$$(5) \qquad c = f \cdot \nu - 1,$$

$$(6) \qquad u_4 = \nu \cdot (f + 1) \ne 0,$$

$$(7) \qquad c \equiv -\nu - 1 \pmod{|u_4|}.$$

Proof: The assertion (5) follows from (1), the assertions (6) and (7) follow from $u_4 = 1 + \nu + c$, from (5), and from the definition of W_2.

Lemma 3.3: Let $\mathbf{u} = \{u_n\} \in W_2 \cap D$, such that $f \ne 0$. Then $\nu \ne -1$.

Proof: Let us suppose that $\mathbf{u} \in W_2 \cap D$, $f \ne 0$, and $\nu = -1$. Then from (6) and (4) we get $0 \ne u_4 = c$ and consequently

$$u_{n+3} \equiv u_{n+2} + u_{n+1} \pmod{|u_4|}, \quad \text{for } n \ge 1.$$

Thus, $u_8 \equiv 3 \pmod{|u_4|}$ and from $u_4 | u_8$ we obtain $u_4 = c = \pm 1, \pm 3$. But

$c = 1 \Rightarrow \mathbf{u} \notin D$ (by Theorem 2.1), a contradiction
$c = -1 \Rightarrow f = 0$ [by (5)], a contradiction
$c = 3 \Rightarrow (u_9, u_{10}) \ne |u_1| \Rightarrow \mathbf{u} \notin D$, a contradiction
$c = -3 \Rightarrow (u_6, u_7) \ne |u_1| \Rightarrow \mathbf{u} \notin D$, a contradiction.

Lemma 3.4: Let $\mathbf{u} = \{u_n\} \in W_2$. Then $u_4 | u_8$ if and only if

$$\nu^2 \equiv \nu + 5 \pmod{|f + 1|}.$$

Proof: Using (7) and (4) we get $u_5 \equiv 1 - \nu - \nu^2 \pmod{|u_4|}$, then

(8) $\quad u_6 \equiv -\nu(\nu + 2) \pmod{|u_4|}, \quad u_7 \equiv -2\nu^2 - 3\nu + 1 \pmod{|u_4|}$

and, finally,

$$u_8 \equiv \nu(\nu^2 - \nu - 5) \pmod{|u_4|}.$$

But by (6), $u_4 = \nu \cdot (f + 1)$ and, therefore:

$$u_4 | u_8 \text{ if and only if } \nu^2 - \nu - 5 \equiv 0 \pmod{|f + 1|}.$$

Lemma 3.5: Let $\mathbf{u} = \{u_n\} \in W_2$ such that $u_4 | u_8$ and $u_4 | u_{12}$. Then

$$33\nu + 60 \equiv 0 \pmod{|f + 1|}.$$

Proof: From (7) and (6) we obtain $c \equiv -\nu - 1 \pmod{|f + 1|}$. Using this fact, (8), Lemma 3.4, (4), and the assumptions $u_4 | u_8$, $u_4 | u_{12}$, we get:

$$u_6 \equiv -3\nu - 5 \pmod{|f + 1|}, \qquad u_7 \equiv -5\nu - 9 \pmod{|f + 1|},$$
$$u_8 \equiv 0 \pmod{|f + 1|}, \qquad u_9 \equiv 6\nu + 11 \pmod{|f + 1|},$$
$$u_{10} \equiv 25\nu + 45 \pmod{|f + 1|}, \qquad u_{11} \equiv 31\nu + 56 \pmod{|f + 1|},$$

and, finally,

$$u_{12} \equiv 33\nu + 60 \equiv 0 \pmod{|f + 1|}.$$

Proposition 3.6: Let $\mathbf{u} = \{u_n\} \in W_2$ such that $u_4 | u_8$ and $u_4 | u_{12}$. Then $f + 1 | 135$.

Proof: From Lemma 3.4, we get:

(9) $\quad 1089\nu^2 \equiv 1089\nu + 5445 \pmod{|f + 1|}.$

Similarly, from Lemma 3.5, we get:

(10) $\quad 1089\nu^2 \equiv 3600 \pmod{|f + 1|};$

(11) $\quad 1089\nu \equiv -1980 \pmod{|f + 1|}.$

Now, from (9), (10), and (11) we obtain

$$3600 \equiv 3465 \pmod{|f + 1|}$$

and thus, $f + 1 | 135$.

Lemma 3.7: Let $\mathbf{u} = \{u_n\} \in W_2$. Then $u_5 \neq 0$ and

(12) $\quad u_{10} \equiv \nu \cdot (f^3 - 5f^2 - 2f + 1) + f^2 - 4f - 6 \pmod{|u_5|}.$

Proof: From (5), (6), and (4) we get:

(13) $\quad u_5 = \nu^2 f + \nu f + 1.$

If $u_5 = 0$, then $\nu f \cdot (\nu + 1) = -1$ and thus, $\nu + 1 = \pm 1$, a contradiction. Furthermore, by a direct computation from (4), using (5), we get:

(14) $\quad u_{10} = \nu^3 f^3 + 6\nu^3 f^2 + 10\nu^2 f^2 + 6\nu^2 f + 10\nu f + \nu.$

From (13) we get $\nu^2 f \equiv -\nu f - 1 \pmod{|u_5|}$; using this fact in (14), we obtain (12).

Proposition 3.8: Let $\mathbf{u} = \{u_n\} \in W_2$ such that $u_5 | u_{10}$. Then

$$u_5 | f^4 - 13f^3 + 34f^2 + 38f + 1.$$

Proof: Let us denote $\alpha = f^3 - 5f^2 - 2f + 1$; $\beta = f^2 - 4f - 6$. Obviously,

$$(15) \qquad \alpha^2 - \beta f(\alpha - \beta) = \alpha^2(\nu^2 f + \nu f + 1) - (\nu\alpha + \beta)(\alpha f \nu + f(\alpha - \beta)).$$

Then from $u_5 | u_{10}$, (12), (13), and (15), we obtain

$$u_5 | \alpha^2 - \beta f(\alpha - \beta) = f^4 - 13f^3 + 34f^2 + 38f + 1$$

which completes the proof of the proposition.

Now, let us denote by H the following subsystem of the system W:

$$H = \{\mathbf{u} \in W : c = -1\},$$

i.e., $\mathbf{u} \in H$ if and only if $\mathbf{u} = \{1, v, 1, v, \ldots\}$. It is obvious that $H \subseteq W_2$.

Proposition 3.9: Let $\mathbf{u} = \{u_n\} \in W_2$. Then $\mathbf{u} \in D$ if and only if $\mathbf{u} \in H$.

Proof: If $\mathbf{u} \in H$, then clearly $\mathbf{u} \in D$. Conversely, let $\mathbf{u} \in D$; then (by Proposition 3.6), $f + 1 | 135$. From Lemma 3.4 and from the fact that the congruence $\nu^2 \equiv \nu + 5 \pmod 9$ has no solution, we get $|f + 1| \neq 9, 27, 45, 135$. Therefore, we obtain for f the following eight possibilities: $f = 0, 2, 4, 14, -2, -4, -6, -16$. Now:

(i) let $f = 0$, then by (5), $c = -1$; thus, $\mathbf{u} = \{1, v, 1, v, \ldots\} \in H$.

(ii) let $f \neq 0$ and let us denote $\delta = f^4 - 13f^3 + 34f^2 + 38f + 1$. The possible values of f and the factorization of the corresponding δ are given in the table:

f	2	4	14	-2	-4	-6	-16
δ	5^3	11^2	9941	181	1481	5101	$181 \cdot 701$

But $u_5 | \delta$ (by Proposition 3.8), which gives us 38 possible pairs $\{f, u_5\}$. For a given pair $\{f, u_5\}$, we obtain the value ν from (13). Obviously, ν must be an integer and $\nu \neq 0, -1$ [by (4) and Lemma 3.3]. By a direct computation, we obtain the following solutions:

$$f = 2,\ \nu = 1, 3, -2, -4, \text{ and } f = 4,\ \nu = 5, -6.$$

For $f = 2$, $\nu = -4$, we get $(u_4, u_{11}) \neq |u_1|$; for $f = 4$, $\nu = 5$, we get $(u_5, u_6) \neq |u_1|$, and in the remaining cases we get $\nu^2 \not\equiv \nu + 5 \pmod{|f + 1|}$ and, therefore, by Lemma 3.4, $u_4 \nmid u_8$. Thus $\mathbf{u} \notin D$, a contradiction.

The following theorem gives a complete characterization of all the strong divisibility sequences in the system W.

Theorem 3.10: Let $\mathbf{u} \in W$. Then $\mathbf{u}$ is a strong divisibility sequence if and only if $\mathbf{u} \in H$.

Proof: The assertion follows immediately from Propositions 3.1 and 3.9 and from the inclusion $D \cap W \subseteq W_1 \cup W_2$.

Acknowledgment

The author wishes to thank the referee for suggestions that led to an improved presentation of this paper.

References

1. P. Horák. "A Note on the Third-Order Strong Divisibility Sequences." *Fibonacci Quarterly* *26.4* (1988):366-71.

2. P. Horák & L. Skula. "A Characterization of the Second-Order Strong Divisibility Sequences." *Fibonacci Quarterly 23.2* (1985):126-32.
3. C. Kimberling. "Strong Divisibility Sequences with Nonzero Initial Term." *Fibonacci Quarterly 16.6* (1978):541-44.

*****

At the request of Professor Lester Lange and with the permission of Professor Leonard Gillman, we have simply lifted Professor Gillman's delightful, melodic note, below, from page 375 of the June-July 1982 issue of *The American Mathematical Monthly*. Students need to know that the well-known limit mentioned involves the golden mean.

Gerald E. Bergum
Editor

MISCELLANEA

77.

Leonid Hambro, the well-known pianist, told me recently that he was about to enter a billiards tournament in which he would play 12 games; he knew the opposition, he said, and he estimated his odds for winning any particular game as 8 to 5. "What do you think your chances are of sweeping all 12 games?" I asked him. "They're pretty small," he said. "The probability that I'll win any one game is 8/13. To find the probability that I'll win all 12 you have to take 8/13 to the 12th power. That's a pretty small number."

He did not have a calculator in his pocket. But he had a pencil and a pad—and an inspiration. "Hey!" he said. "Those are Fibonacci numbers. The ratio of successive terms approaches a limit (about .618), and very fast: even a ratio near the beginning like 8/13 is very close to the limit." He scribbled some additions. "The 12th Fibonacci number after 8 is 2584. Therefore 8/13 to the 12th power is approximately the same as 8/13 times 13/21 and so on, twelve times; everything cancels out except the 8 in the beginning and the 2584 at the end. So the probability that I will win all 12 games is about 8/2584, or about 1/300. See, I told you it was pretty small."

—Leonard Gillman
The University of Texas at Austin

ON A GENERALIZATION OF A RECURSIVE SEQUENCE

Péter Kiss and Béla Zay*
Teacher's Training College, Leányka u. 4., 3301 Eger, Hungary
(Submitted April 1990)

1. Introduction

Let k and t be fixed positive integers and let $G_{k,t}(n)$, $n = 0, 1, 2, \ldots$, be a sequence of integers defined by

$$(1) \qquad G_{k,t}^{'}(n) = \begin{cases} n & \text{if } 0 \le n \le t-1 \\ n - G_{k,t}^{k}(n-t) & \text{if } n \ge t, \end{cases}$$

where $G_{k,t}^{k}$ denotes the k^{th} iterated composition of $G_{k,t}$, i.e.,

$$G_{k,t}^{1}(m) = G_{k,t}(m) \quad \text{and} \quad G_{k,t}^{i}(m) = G_{k,t}(G_{k,t}^{i-1}(m))$$

for $i > 1$ and for any $m \ge 0$.

This sequence is a generalization of some which have been investigated earlier. P. J. Downey & R. E. Griswold [1] (and later V. Granville & J. P. Rasson [3]) proved that the solution of recurrence (1) in the case $k = 2$, $t = 1$ is given by

$$(2) \qquad G_{2,1}(n) = [(n+1)\mu]$$

for any $n \ge 0$, where $\mu = (-1 + \sqrt{5})/2$ and [ ] denotes the integer part function. In [1] a similar formula is shown for $G_{2,t}(n)$ with arbitrary $t \ge 1$.

Recently B. Zay [6] has shown some properties of the general sequence for any k and t. Among others he proved that $G_{k,t}(n)$ is defined for each nonnegative integer n, the sequence is monotonically increasing, and that the general case can be traced back to the case $t = 1$ by

$$G_{k,t}(n) = \begin{cases} t \cdot G_{k,1}\left(\left[\frac{n}{t}\right]\right) & \text{if } G_{k,1}\left(\left[\frac{n}{t}\right]\right) = G_{k,1}\left(\left[\frac{n}{t} + 1\right]\right) \\ t \cdot G_{k,1}\left(\left[\frac{n}{t}\right]\right) + n - t \cdot \left[\frac{n}{t}\right] & \text{if } G_{k,1}\left(\left[\frac{n}{t}\right]\right) \ne G_{k,t}\left(\left[\frac{n}{t} + 1\right]\right) \end{cases}$$

for any $n \ge 0$. So it is enough to investigate the sequence with $t = 1$. Furthermore, we can suppose that $k \ge 2$ since the case $k = t = 1$ gives the sequence $G_{1,1}(n) = [(n+1)/2]$, which can be considered as a trivial case.

Throughout this paper, k will denote a fixed integer with $k \ge 2$ and, for brevity, we write $G(n)$ instead of $G_{k,1}(n)$.

In general (if $k > 2$) the terms of the sequence $G(n)$ cannot be expressed similarly as in (2). In order to see it, let us suppose that there is an integer r and a positive real number ω such that

$$(3) \qquad G(n) = [(n+r)\omega].$$

Then

$$(4) \qquad \lim_{n \to \infty} \frac{G(n)}{n} = \omega.$$

*This research was partially supported by the Hungarian National Foundation for Scientific Research grant no. 273.

On the other hand, by (1) we have

$$\frac{G(n)}{n} = 1 - \frac{G^k(n-1)}{G^{k-1}(n-1)} \cdot \frac{G^{k-1}(n-1)}{G^{k-2}(n-1)} \cdots \frac{G^2(n-1)}{G(n-1)} \cdot \frac{G(n-1)}{n-1} \cdot \frac{n-1}{n};$$

therefore, $G^i(n) = G(G^{i-1}(n))$ and (4) imply the equation

$$\omega = 1 - \omega^k.$$

So ω is the only positive real root of the equation $x^k + x - 1 = 0$. But it can be checked by numerical calculation that, in the case $k = 3$, equation (3), with any integer r, does not hold for all n. Namely, in this case, we have $\omega = 0.6823\ldots$, $G(2) = 1$, $G(18) = 13$; thus, from

$$G(2) = 1 = [(2 + r)\omega] \quad \text{and} \quad G(18) = 13 = [(18 + r)\omega],$$

$r < 1$ and $r > 1$ would follow, respectively, which is impossible.

Thus, (2) really cannot be extended for any $k \geq 2$. But we shall show that (4) holds for any k.

Theorem: For any integer $k \geq 2$,

$$\lim_{n\to\infty} \frac{G(n)}{n} = \omega,$$

where ω is the single positive real root of the equation $x^k + x - 1 = 0$.

We note that the Theorem also holds if $t > 1$ or $k = 1$, which follows from the results mentioned above.

2. Auxiliary Results

For the proof of our Theorem, we need the following lemmas.

Lemma 1: For any $n > 0$, we have

(5) $$G(n) = G(n-1) + \varepsilon_n$$

and

(6) $$G^k(n) = G^k(n-1) + \varepsilon_n',$$

where ε_n and ε_n' are 0 or 1.

Proof: Equalities (5) and (6) hold for $n = 1$ and $n = 2$ since, by the definition of the sequence,

$$G(0) = 0,\ G^k(0) = 0,\ G(1) = 1,\ G(2) = 1,\ G^k(1) = 1,\ G^k(2) = 1$$

for any $k \geq 2$. Assume that $m \geq 2$ and (5) holds for any $n \leq m$, i.e.,

$$G(n) = G(n-1) + \varepsilon_n$$

for any n with $0 < n \leq m$ and $\varepsilon_n = 0$ or 1. From this $G(n) \leq n \leq m$ also follows and so, by the assumption, we get

$$G(G(n)) = G^2(n) = \begin{cases} G^2(n-1) & \text{if } \varepsilon_n = 0 \\ G^2(n-1) + \varepsilon_n'' & \text{if } \varepsilon_n = 1, \end{cases}$$

where $\varepsilon_n'' = 0$ or 1. Continuing this process,

(7) $$G^k(n) = G^k(n-1) + \varepsilon_n' \quad (\varepsilon_n' = 0 \text{ or } 1)$$

follows for any $0 < n \leq m$. By (1) we have

$$G(m) = m - G^k(m-1) \quad \text{and} \quad G(m+1) = m + 1 - G^k(m)$$

from which, using (7), we obtain

$$G(m+1) - G(m) = 1 - (G^k(m) - G^k(m-1)) = \varepsilon_{m+1} \quad (\varepsilon_{m+1} = 0 \text{ or } 1).$$

Thus, (5), (7), and (6) also hold for $n = m + 1$.

From these, the lemma follows by mathematical induction.

Lemma 2: Let $\{n_i\}_{i=0}^{\infty}$ be a sequence of positive integers such that

$$G(n_i) = n_{i-1}$$

for any $i > 0$. Then

$$n_i = n_{i-1} + n_{i-k} - \varepsilon_i$$

for any $i \geq k$, where $\varepsilon_i = 0$ or 1.

Proof: By the assumption of the lemma, using Lemma 1 and the definition of the sequence $G(n)$, for any $i \geq k$ we have

$$\begin{aligned} n_{i-1} = G(n_i) &= n_i - G^k(n_i - 1) = n_i - G^k(n_i) + \varepsilon_i' \\ &= n_i - G^{k-1}(n_{i-1}) + \varepsilon_i' = n_i - G^{k-2}(n_{i-2}) + \varepsilon_i' = \cdots \\ &= n_i - G(n_{i-k+1}) + \varepsilon_i' = n_i - n_{i-k} + \varepsilon_i', \end{aligned}$$

where $\varepsilon_i' = 0$ or 1. The lemma follows from this assertion.

Lemma 3: Let $\{n_i\}_{i=0}^{\infty}$ be an increasing sequence of nonnegative integers satisfying the recursion

$$n_i = n_{i-1} + n_{i-k} - \varepsilon_i \quad (i \geq k),$$

where $k \geq 2$ is a fixed positive integer and $\varepsilon_i = 0$ or 1. Define a k^{th}-order linear recurrence sequence $\{u_i\}_{i=0}^{\infty}$ of integers by $u_i = n_i$ for $0 \leq i \leq k - 1$ and

$$u_i = u_{i-1} + u_{i-k}$$

for $i \geq k$. Further, let $\{F_i\}_{i=0}^{\infty}$ be a sequence of natural numbers defined by $F_0 = F_1 = \cdots = F_{k-1} = 1$ and

$$F_i = F_{i-1} + F_{i-k} \quad (i \geq k).$$

Then

$$n_i = u_i - \delta_i$$

for any $i \geq 0$, where $0 \leq \delta_i \leq F_i - 1$.

Proof: For $0 \leq i \leq k - 1$, the lemma evidently holds with $\delta_i = 0$. If $i \geq k$ and $n_j = u_j - \delta_j$ with $0 \leq \delta_j \leq F_j - 1$ for any $0 \leq j < i$, then

$$\begin{aligned} n_i &= n_{i-1} + n_{i-k} - \varepsilon_i \\ &= u_{i-1} + u_{i-k} - (\delta_{i-1} + \delta_{i-k} + \varepsilon_i) = u_i - \delta_i, \end{aligned}$$

where

$$0 \leq \delta_i = \delta_{i-1} + \delta_{i-k} + \varepsilon_i \leq F_{i-1} + F_{i-k} - 2 + \varepsilon_i \leq F_i - 1,$$

since the δ_j's are integers. The lemma follows from the above by mathematical induction on i.

Lemma 4: Let $\{v_n\}_{n=0}^{\infty}$ be a k^{th}-order linear recurrence sequence of positive rational integers defined by the nonzero initial values $v_0, v_1, \ldots, v_{k-1}$ and by the recursion

$$v_n = v_{n-1} + v_{n-k}$$

for $n \geq k$. Denote by $\alpha_1, \alpha_2, \ldots, \alpha_k$ the roots of the characteristic polynomial $x^k - x^{k-1} - 1$. Then the terms of the sequence can be expressed as

$$v_n = a_1\alpha_1^n + a_2\alpha_2^n + \cdots + a_k\alpha_k^n \quad (n \geq 0), \tag{8}$$

where the a_i's ($i = 1, 2, \ldots, k$) are elements of the number field generated by $\alpha_1, \alpha_2, \ldots, \alpha_k$ over the rationals.

Proof: This lemma is a special case of a more general well-known result, so it is not necessary to prove it here.

Lemma 5: Let $\{v_n\}_{n=0}^{\infty}$ be the linear recurrence sequence defined in Lemma 4. If

$$0 < v_0 = \min_{0 \le i < k} (v_i) \quad \text{and} \quad |\alpha_1| > |\alpha_i| \text{ for } 2 \le i \le k,$$

then there is a real number $c > 0$, depending only on the characteristic polynomial of the sequence, such that

$$|a_1| > c \cdot v_0, \tag{9}$$

where a_1 is defined by (8).

Proof: Ferguson [2] as well as Hoggatt & Alladi [4] proved that the roots of the polynomial $x^k - x^{k-1} - 1$ are distinct and that there is a dominant real root α_1 with the largest modulus; thus, we may suppose that $|\alpha_1| > |\alpha_i|$ for $i = 2, \ldots, k$.

By (8), for the a_i's, we have the system equations:

$$\begin{aligned}
&a_1 + a_2 + \cdots + a_k = v_0\\
&a_1\alpha_1 + a_2\alpha_2 + \cdots + a_k\alpha_k = v_1\\
&\vdots\\
&a_1\alpha_1^{k-1} + a_2\alpha_2^{k-1} + \cdots + a_k\alpha_k^{k-1} = v_{k-1};
\end{aligned}$$

thus,

$$a_1 = \frac{D_1}{D}, \tag{10}$$

where

$$D = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_k \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_k^2 \\ \vdots & & & \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_k^{k-1} \end{vmatrix}, \quad D_1 = \begin{vmatrix} v_0 & 1 & \ldots & 1 \\ v_1 & \alpha_2 & \ldots & \alpha_k \\ v_2 & \alpha_2^2 & \ldots & \alpha_k^2 \\ \vdots & & & \\ v_{k-1} & \alpha_2^{k-1} & \ldots & \alpha_k^{k-1} \end{vmatrix},$$

and $D \ne 0$ since the α_i's are distinct. The determinant D_1 can be written in the form

$$D_1 = \sum_{i=1}^{k} (-1)^{i-1} v_{i-1} \cdot D^{(i)}, \tag{11}$$

where

$$D^{(i)} = \begin{vmatrix} 1 & \ldots & 1 \\ \alpha_2 & \ldots & \alpha_k \\ \vdots & & \\ \alpha_2^{i-2} & \ldots & \alpha_k^{i-2} \\ \alpha_2^{i} & \ldots & \alpha_k^{i} \\ \vdots & & \\ \alpha_2^{k-1} & \ldots & \alpha_k^{k-1} \end{vmatrix}$$

is a $(k - 1) \times (k - 1)$ determinant rejecting the first column and the i^{th} row from D_1.

It was proved in the lemma of [5] that

$$D^{(i)} = D_0 \cdot S_{k-i} \text{ for any } 1 \le i \le k, \tag{12}$$

where

$$D_0 = \begin{vmatrix} 1 & \dots & 1 \\ \alpha_2 & \dots & \alpha_k \\ \vdots & & \\ \alpha_2^{k-2} & \dots & \alpha_k^{k-2} \end{vmatrix}$$

is a $(k-1) \times (k-1)$ Vandermonde determinant and S_{k-i} is the elementary symmetrical polynomial of degree $k - i$ of variables $\alpha_2, \dots, \alpha_k$ if $k - i > 0$, and $S_0 = 1$. It is known that for the coefficients of a polynomial

$$b(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n$$

we have

$$b_j = (-1)^j b_0 S_j' \quad (1 \le j \le n)$$

where

$$S_j' = \sum \beta_{i_1}\beta_{i_2} \dots \beta_{i_j}$$

is the elementary symmetrical polynomial of degree j of the roots $\beta_1, \dots, \beta_n$ of $b(x)$ (the sum runs over the distinct $i_1 < i_2 < \cdots < i_j$ combinations of 1, 2, ..., n). Since $S_1, S_2, \dots, S_{k-1}$ are the elementary symmetrical polynomials of $\alpha_2, \dots, \alpha_k$ of degree 1, 2, ..., $k - 1$, thus $S_1 + \alpha_1$, $S_2 + S_1\alpha_1$, ..., $S_{k-1} + S_{k-2}\alpha_1$, $S_{k-1}\alpha_1$ are the elementary symmetrical polynomials of $\alpha_1, \alpha_2, \dots, \alpha_k$ of degree 1, 2, ..., $k - 1$, k, respectively. So, for the coefficients of the polynomial $x^k - x^{k-1} - 1$, we have

$$\begin{aligned} -1 &= -(S_1 + \alpha_1) \\ 0 &= S_2 + S_1\alpha_1 \\ &\vdots \\ 0 &= (-1)^{k-1}(S_{k-1} + S_{k-2}\alpha_1) \\ -1 &= (-1)^k \cdot S_{k-1}\alpha_1. \end{aligned} \tag{13}$$

Since α_1 is real, $\alpha_1 > 1$, which implies that $S_1 = 1 - \alpha_1 > 0$. But, from this, $S_2 > 0$ follows, and contiuing this process, by (13), we obtain the inequalities

$$S_{2i} > 0 \quad (0 \le 2i \le k - 1) \tag{14}$$

and

$$S_{2i+1} < 0 \quad (1 \le 2i + 1 \le k - 1). \tag{15}$$

Finally, by (11) and (12) we get

$$D_1 = D_0(v_0S_{k-1} - v_1S_{k-2} + \cdots + (-1)^{k-1}v_{k-1}S_0)$$

and, by (14) and (15), using the condition $0 < v_0 \le v_i$ for $1 \le i \le k - 1$,

$$|D_1| = |D_0| \cdot \sum_{i=1}^{k} v_{i-1} \cdot |S_{k-i}| > v_0 \cdot |D_0| \cdot \sum_{i=1}^{k} |S_{k-i}|$$

follows. By (10), this implies the lemma.

3. Proof of the Theorem

Let N be a sufficiently large positive integer and define an integer m by

$$m = \left[\frac{\log N}{2 \cdot \log 3}\right]$$

([ ] is the integer part function). Let $n_0, n_1, \dots, n_m$ be a set of natural numbers defined by

$$n_m = N \quad \text{and} \quad n_{i-1} = G(n_i) \quad \text{for } 1 \le i \le m. \tag{16}$$

From Lemma 1 and its proof, it follows that $G(n) < n$ for any $n > 1$, and so

$$n_0 < n_1 < \cdots < n_m = N$$

for N sufficiently large so that $n_0 \geq 1$.

We show that there are no three consecutive equal terms in the sequence $G(n)$. For if

$$G(n) = G(n + 1) = G(n + 2),$$

then, by the definition of the sequence,

$$n - G^k(n - 1) = n + 1 - G^k(n) = n + 2 - G^k(n + 1) \tag{17}$$

would follow. But $G(n) = G(n + 1)$ implies that $G^k(n) = G^k(n + 1)$ and so, by (17), we would obtain the equality $n + 1 = n + 2$, which is impossible. Thus, $G(n + 2) \geq G(n) + 1$ for any $n \geq 0$, and so

$$G(n) \geq \frac{1}{3}n. \tag{18}$$

By (16) and (18), we get

$$N = n_m \leq 3 \cdot G(n_m) = 3 \cdot n_{m-1} \leq 3^2 \cdot G(n_{m-1}) = 3^2 \cdot n_{m-2} \leq \cdots \leq 3^m n_0,$$

which, by the definition of m, can be written in the form

$$n_0 \geq \frac{N}{3^m} \geq \sqrt{N}. \tag{19}$$

By Lemmas 2-4 and their notations, using (16), we obtain

$$\frac{G(N)}{N} = \frac{n_{m-1}}{n_m} = \frac{u_{m-1} - \delta_{m-1}}{u_m - \delta_m} = \frac{a_1\alpha_1^{m-1} + \cdots + a_k\alpha_k^{m-1} - \delta_{m-1}}{a_1\alpha_1^m + \cdots + a_k\alpha_k^m - \delta_m} \tag{20}$$

$$= \frac{1}{\alpha_1} \cdot \frac{1 + \frac{a_2}{a_1}\left(\frac{\alpha_2}{\alpha_1}\right)^{m-1} + \cdots + \frac{a_k}{a_1}\left(\frac{\alpha_k}{\alpha_1}\right)^{m-1} - \frac{1}{a_1}\ \delta_{m-1}/\alpha_1^{m-1}}{1 + \frac{a_2}{a_1}\left(\frac{\alpha_2}{\alpha_1}\right)^{m} + \cdots + \frac{a_k}{a_1}\left(\frac{\alpha_k}{\alpha_1}\right)^{m} - \frac{1}{a_1} \cdot \delta_m/\alpha_1^m}.$$

By the proof of Lemma 5, it follows that there are complex numbers $b_1, b_2, \ldots, b_k$, which depend only on the α_i's ($i = 1, 2, \ldots, k$), such that

$$a_i = \sum_{i=0}^{k-1} b_i u_i$$

and so, using that $|a_1| > c \cdot u_0$ by Lemma 5,

$$\left|\frac{a_i}{a_1}\right| < \frac{\left|\sum_{i=0}^{k-1} b_i u_i\right|}{c \cdot u_0} \tag{21}$$

follows. But $u_i = n_i$ for $i = 0, 1, 2, \ldots, k - 1$, $n_i < n_{k-1}$ for $0 \leq i < k - 1$, and by (18) $n_i/n_{i-1} \leq 3$ for any $i > 0$; thus, from (21),

$$\left|\frac{a_i}{a_1}\right| < b \cdot \frac{n_{k-1}}{n_0} = b \cdot \frac{n_1}{n_0} \cdot \frac{n_2}{n_1} \cdot \ldots \cdot \frac{n_{k-1}}{n_{k-2}} \leq b \cdot 3^{k-1} = B \tag{22}$$

follows for $2 \leq i \leq k$, where b and B are positive real numbers which do not depend on m and the n_i's. Since $|\alpha_1| > |\alpha_i|$ for $2 \leq i \leq k$, and $m \to \infty$ as $N \to \infty$, so by (22),

$$(23) \qquad \lim_{N\to\infty} \frac{a_i}{a_1}\left(\frac{\alpha_i}{\alpha_1}\right)^{m-1} = \lim_{N\to\infty} \frac{a_i}{a_1}\left(\frac{\alpha_i}{\alpha_1}\right)^{m} = 0 \quad \text{for } i = 2, 3, \ldots, k.$$

On the other hand, by Lemmas 3 and 4, we get

$$0 \le \delta_n < F_n = c_1\alpha_1^n + c_2\alpha_2^n + \cdots + c_k\alpha_k^n = c_1\alpha_1^n\left(1 + \sum_{i=2}^{k} \frac{c_i}{c_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)$$

for any $n \ge 0$, where the c_i's ($i = 1, 2, \ldots, k$) are complex numbers which are independent of n,

$$\lim_{n\to\infty}(\alpha_i/\alpha_1)^n = 0,$$

and it can be easily seen that $c_1 \neq 0$. From these, it follows that there is a real number $C > 0$, depending only on the characteristic polynomial of the sequence $\{F_i\}$, such that

$$\left|\frac{\delta_n}{\alpha_1^n}\right| < C \text{ for any } n \ge 0.$$

However, by (19) and Lemma 5,

$$|a_1| > c \cdot u_0 = c \cdot n_0 \ge c \cdot \sqrt{N}$$

and so

$$(24) \qquad \lim_{N\to\infty}\left(\frac{1}{a_1} \cdot \frac{\delta_{m-1}}{\alpha_1^{m-1}}\right) = \lim_{N\to\infty}\left(\frac{1}{a_1} \cdot \frac{\delta_m}{\alpha_1^m}\right) = 0.$$

From (20), (23), and (24),

$$\lim_{N\to\infty} \frac{G(N)}{N} = \frac{1}{\alpha_1}$$

follows, where α_1 is the single positive root of the equation $x^k - x^{k-1} - 1 = 0$. But, if α is a root of the polynomial $x^k - x^{k-1} - 1$, then $1/\alpha$ is a root of $x^k + x - 1$, thus $1/\alpha_1 = \omega$ and the theorem is proved.

Acknowledgment

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

References

1. P. J. Downey & R. E. Griswold. "On a Family of Nested Recurrences." *Fibonacci Quarterly* *22* (1984):310-17.
2. H. R. P. Ferguson. "On a Generalization of the Fibonacci Numbers Useful in Memory Allocation Schema; or All About the Zeros of $z^k - z^{k-1} - 1$, $k > 0$." *Fibonacci Quarterly* *14* (1976):233-43.
3. V. Granville & J. P. Rasson. "A Strange Recursive Relation." *J. Number Theory* *30* (1988):238-41.
4. V. E. Hoggatt, Jr. & K. Alladi. "Limiting Ratios of Convolved Recursive Sequences." *Fibonacci Quarterly* *15* (1977):211-14.
5. P. Kiss. "On Some Properties of Linear Recurrences." *Publ. Math. Debrecen* *30* (1983):273-81.
6. B. Zay. "Egy Rekurziv Sorozatról." (Hungarian) *Acta Acad. Paed. Agriensis*, to appear.

*****

ON A THEOREM OF MONZINGO CHARACTERIZING THE PRIME DIVISORS OF CERTAIN SEQUENCES OF INTEGERS

R. B. McNeill
Northern Michigan University, Marquette, MI 49855

(Submitted May 1990)

In [1], M. G. Monzingo extended a problem found in *Elementary Number Theory* by David M. Burton concerning the common divisors of two successive integers of the form $n^2 + 3$ by establishing

Theorem 1 (Monzingo): Let p be an odd prime. If p is of the form $4K + 1$, then p is the only prime that divides successive integers of the form $n^2 + K$, and p divides successive pairs precisely when n is of the form $bp + 2K$, for any integer b. If p is of the form $4K + 3$, then p is the largest prime that divides successive integers of the form $n^2 + (3K + 2)$, and p divides successive pairs precisely when n is of the form $bp + (2K + 1)$, for any integer b. Furthermore, p will be the only prime divisor if and only if $p = 3$.

The purpose of this note is to generalize these results to the general quadratic. Specifically, we prove the following

Theorem 2: Let p be an odd prime and define $P(n) \equiv a_2n^2 + a_1n + a_0$, where n and all coefficients are integers and $a_2 \neq 0$. If p divides $P(n)$ and $P(n + d)$, where d is an integer not divisible by p, then p divides $a_2^2d^2 - a_1^2 + 4a_0a_2$, and n satisfies the equation

$$(2n + d)a_2 + a_1 \equiv 0 \bmod p.$$

Proof: Suppose that p divides $P(n)$ and $P(n+d)$. Since p divides the difference of these integers, and p does not divide d, p divides $Q(n) \equiv (2n + d)a_2 + a_1$, i.e., n satisfies

$$(2n + d)a_2 + a_1 \equiv 0 \bmod p.$$

In addition, p divides $nQ(n) - 2P(n)$, i.e., p divides $R(n) \equiv n(a_2d - a_1) - 2a_0$. Finally, p divides $(a_2d - a_1)Q(n) - 2a_2R(n)$, and the result is established unless (perhaps) either $n = 0$ or $a_2d - a_1 = 0$. Since it is straightforward to verify directly that p divides $a_2^2d^2 - a_1^2 + 4a_0a_2$ in each of these cases, the theorem is established.

Remark: Theorem 1 (Monzingo) follows easily from Theorem 2 after selecting $d = 1$, $a_2 = 1$, $a_1 = 0$, and $a_0 = K$ or $a_0 = 3K + 2$, depending on whether $p = 4K + 1$ or $p = 4K + 3$, respectively.

Reference

1. M. G. Monzingo. "On Prime Divisors of Sequences of Integers Involving Squares." *Fibonacci Quarterly 26.1* (1988):31-32.

*****

ZECKENDORF REPRESENTATIONS USING NEGATIVE FIBONACCI NUMBERS

M. W. Bunder
The University of Wollongong, Wollongong, N.S.W. 2500, Australia

(Submitted May 1990)

It is well known that every positive integer can be represented uniquely as a sum of distinct, nonconsecutive Fibonacci numbers (see, e.g., Brown [1]). This representation is called the Zeckendorf representation of the positive integer. Other Zeckendorf-type representations where the Fibonacci numbers are not necessarily consecutive are possible. Brown [2] considers one where a maximal number of distinct Fibonacci numbers are used rather than a minimal number.

We show here that every integer can be represented uniquely as a sum of nonconsecutive Fibonacci numbers F_i where $i \le 0$ and we specify an algorithm that leads to this representation. We also show that no maximal representation of this form is possible.

We note that for all integers i,

$$F_{-i} = (-1)^{i+1}F_i$$

and

(1) $$F_{i+1} = F_i + F_{i-1}.$$

We note further that $F_0 = 0$, F_{-1}, F_{-3}, F_{-5}, ... are positive and F_{-2}, F_{-4}, ... are negative. Also for $i > 1$,

$$|F_{-i}| < |F_{-i-1}|.$$

The four lemmas below will show that the algorithm that follows them is effective.

Lemma 1: If n, $k > 0$ and $-F_{-2k} \le n < F_{-2k-1} - 1$ then, for some ℓ, $k > \ell > 0$,

$$-F_{-2k+2\ell-1} \le n - F_{-2k-1} < -F_{-2k+2\ell+1} < 0.$$

If $n = F_{-2k-1} - 1$, then

$$n - F_{-2k-1} = -F_{-1}.$$

Proof: If $-F_{-2k} \le n < F_{-2k-1} - 1$, then

$$1 < F_{-2k-1} - n \le F_{-2k-1} + F_{-2k},$$

i.e.,

$$1 < F_{-2k-1} - n \le F_{-2k+1} = F_{2k-1}.$$

Now every integer $p > 1$ is in a range $0 < F_{2m-3} < p \le F_{2m-1}$ where $m \ge 2$.

We must, if $p = F_{-2k-1} - n$, then have $m + \ell = k + 1$ for some $\ell > 0$ and so:

$$0 < F_{2k-2\ell-1} < F_{-2k-1} - n \le F_{2k-2\ell+1};$$

thus,

$$-F_{-2k+2\ell-1} \le n - F_{-2k-1} < -F_{-2k+2\ell+1} < 0.$$

Lemma 2: If n, $k > 0$ and $F_{-2k+1} < n \le -F_{-2k}$ then, for some ℓ, $k > \ell > 0$:

$$0 \le -F_{-2k+2\ell+2} < n - F_{-2k+1} \le -F_{-2k+2\ell}.$$

Proof: If $F_{-2k+1} < n \le -F_{-2k}$, then

$$0 < n - F_{-2k+1} \le -F_{-2k} - F_{-2k+1},$$

so

$$0 < n - F_{-2k+1} \le -F_{-2k+2} = F_{2k-2}.$$

Now every positive integer p is in the range

$$0 \le F_{2m-4} < p \le F_{2m-2}$$

where $m \ge 2$.

We must, if $p = n - F_{-2k+1}$, then have $m + \ell = k + 1$ for some ℓ, $k > \ell > 0$, and so

$$0 \le F_{2k-2\ell-2} < n - F_{-2k+1} \le F_{2k-2\ell},$$

i.e.,

$$0 \le -F_{-2k+2\ell+2} < n - F_{-2k+1} \le -F_{-2k+2\ell}.$$

Lemma 3: If $n < 0$, $k > 0$, and $1 + F_{-2k} < n \le -F_{-2k+1}$ then, for some ℓ, $k > \ell > 0$,

$$0 \le -F_{-2k+2\ell+2} < n - F_{-2k} \le -F_{-2k+2\ell}.$$

If $n = F_{-2k} + 1$,

$$n - F_{-2k} = F_{-1}.$$

Proof: If $1 + F_{-2k} < n \le -F_{-2k+1}$, then

$$1 < n - F_{-2k} \le -F_{-2k+2} = F_{2k-2}$$

and as in the proof of Lemma 2,

$$0 \le F_{2k-2\ell-2} < n - F_{-2k} \le F_{2k-2\ell} \text{ for some } \ell,\ k > \ell > 0;$$

thus,

$$0 \le -F_{-2k+2\ell+2} < n - F_{-2k} \le -F_{-2k+2\ell}.$$

Lemma 4: If $n < 0$, $k > 0$, and $-F_{-2k-1} \le n < F_{-2k} - 1$ then, for some ℓ, $k > \ell > 0$,

$$-F_{-2k+2\ell-1} \le n - F_{-2k} < -F_{-2k+2\ell+1} < 0.$$

If $n = F_{-2k} - 1$,

$$n - F_{-2k} = F_{-2}.$$

Proof: If $-F_{-2k-1} \le n < F_{-2k} - 1$, then

$$1 < F_{-2k} - n \le F_{-2k} + F_{-2k-1} = F_{-2k+1},$$

so

$$1 < F_{-2k} - n \le F_{2k-1}$$

and, as in the proof of Lemma 1,

$$0 < F_{2k-2\ell-1} < F_{-2k} - n \le F_{2k-2\ell+1} \text{ where } k > \ell \ge 1,$$

i.e.,

$$-F_{-2k+2\ell-1} \le n - F_{-2k} < -F_{-2k+2\ell+1} < 0.$$

Algorithm Z: This algorithm produces, for a given integer, the promised sum of Fibonacci numbers.

(1) If $n = F_{-i}$ for some i, then stop.

(2) If $n > 0$ and for $k > 0$, $F_{2k} < n < F_{2k+1}$, i.e., $-F_{-2k} < n < F_{-2k-1}$, write $n = F_{-2k-1} + (n - F_{-2k-1})$, and apply this algorithm to $n - F_{-2k-1}$, giving the next term in the sum.

(3) If $n > 0$ and for $k > 0$, $F_{2k-1} < n < F_{2k}$, i.e., $F_{-2k+1} < n < -F_{-2k}$, write $n = F_{-2k+1} + (n - F_{-2k+1})$, and apply this algorithm to $n - F_{-2k+1}$, giving the next term in the sum.

(4) If $n < 0$ and for $k > 0$, $F_{2k-1} < -n < F_{2k}$, i.e., $F_{-2k} < n < -F_{-2k+1}$, write $n = F_{-2k} + (n - F_{-2k})$, and apply this algorithm to $n - F_{-2k}$, giving the next term in the sum.

(5) If $n < 0$ and for $k > 0$, $-F_{2k} < -n < F_{2k+1}$, i.e., $-F_{-2k-1} < n < F_{-2k}$, write $n = F_{-2k} + (n - F_{-2k})$, and apply this algorithm to $n - F_{-2k}$, giving the next term in the sum.

The algorithm terminates when, eventually,

$$n - F_{-i_1} - F_{-i_2} \cdots - F_{-i_m} = F_{-i_{m+1}}.$$

Lemma 5: Algorithm Z produces a representation of any nonzero integer n as a sum of Fibonacci numbers F_i where $i \le 0$ and any two of the i's differ by at least 2.

Proof: If after the application of (2), $n - F_{-2k-1} \ne F_{-j}$ for any j, we have, by Lemma 1:

$$-F_{-2k+2\ell-1} < n - F_{-2k-1} < -F_{-2k+2\ell+1} < 0, \text{ where } \ell > 0.$$

By applying (4) or (5), the algorithm next considers $n - F_{-2k-1} - F_{-2k+2\ell}$. If after (3), $n - F_{-2k+1} \ne F_{-j}$, by Lemma 2:

$$0 < -F_{-2k+2\ell+2} < n - F_{-2k+1} \le -F_{-2k+2\ell}, \text{ where } \ell > 0.$$

By (2) or (3), the algorithm next considers $n - F_{-2k+1} - F_{-2k+2\ell+1}$. If after (4), $n - F_{-2k} \ne F_{-j}$, by Lemma 3:

$$0 \le -F_{-2k+2\ell+2} < n - F_{-2k} < -F_{-2k+2\ell}, \text{ where } \ell > 0.$$

By (2) or (3) the algorithm next considers $n - F_{-2k} - F_{-2k+2\ell+1}$. If after (5), $n - F_{-2k} \ne F_{-j}$, by Lemma 4:

$$-F_{-2k+2\ell-1} < n - F_{-2k} < -F_{-2k+2\ell+1} < 0, \text{ where } \ell > 0.$$

By (4) and (5), the algorithm next considers $n - F_{-2k} - F_{-2k+2\ell}$.

Thus, if the first stage of the algorithm produces $n - F_{-i}$ $(i > 0)$, the second produces $n - F_{-i} - F_{-i+p}$, where $p \ge 2$ and $-i + p < 0$.

The same applies to later stages of the algorithm which therefore produces Fibonacci numbers with subscripts at least two apart.

The next two lemmas are required to prove the uniqueness of this representation.

Lemma 6: (i) $\displaystyle\sum_{i=1}^{k} F_{-2i} = 1 - F_{-2k-1}$;

(ii) $\displaystyle\sum_{i=1}^{k} F_{-2i+1} = -F_{-2k}$;

(iii) $\displaystyle\sum_{i=1}^{k} F_{-i} = 1 - F_{-k+1}$.

Proof: The proof is simple and is therefore omitted here.

Lemma 7: If $i_1 > i_2 > \cdots > i_h > 0$ and, for $2 < j \le h$, $i_j - i_{j+1} \ge 2$,

$$-F_{-i_1+1} < \sum_{k=1}^{h} F_{-i_k} \le -F_{-i_1-1} \text{ if } i_1 \text{ is odd,}$$

and

$$-F_{-i_1-1} < \sum_{k=1}^{h} F_{-i_k} \le -F_{-i_1+1} \text{ if } i_1 \text{ is even.}$$

Proof: If i_1 is odd, by Lemma 6:

$$F_{-i_1} + F_{-i_1+3} + F_{-i_1+5} + \cdots + F_{-2} \le \sum_{k=1}^{h} F_{-i_k} \le F_{-i_1} + F_{-i_1+2} + \cdots + F_{-1}$$

$$F_{-i_1} + 1 - F_{-i_1+2} \le \sum_{k=1}^{h} F_{-i_k} \le -F_{-i_1-1},$$

so, $$-F_{-i_1+1} < 1 - F_{-i_1+1} \le \sum_{k=1}^{h} F_{-i_k} < -F_{-i_1-1}.$$

If i_1 is even, by Lemma 6:

$$F_{-i_1} + F_{-i_1+2} + \cdots + F_{-2} \le \sum_{k=1}^{h} F_{-i_k} \le F_{-i_1} + F_{-i_1+3} + \cdots + F_{-3} + F_{-1}$$

$$1 - F_{-i_1-1} \le \sum_{k=1}^{h} F_{-i_k} \le -F_{-i_1+1}.$$

Theorem 1: Algorithm Z expresses every integer n as a unique sum of a minimal number of distinct Fibonacci numbers F_i, where $i \le 0$.

Proof: If $n = 0$, $n = F_0$.

If $n \ne 0$, by Lemma 5 the algorithm produces a sum of the form

$$n = \sum_{k=1}^{h} F_{-i_k}, \text{ where } i_k \ge i_{k+1} + 2.$$

If the representation were not unique or not minimal, we would also have

$$n = \sum_{k=1}^{m} F_{-j_k}, \text{ where } j_k \ge j_{k+1} + 2, \text{ and possibly } m < h.$$

Let $-i_p$ and $-j_p$ be the first of these subscripts, if any, that are distinct and assume $i_p > j_p$. Then

$$n - F_{-i_1} - \cdots - F_{-i_{(p-1)}} = \sum_{k=p}^{h} F_{-i_k} = \sum_{k=p}^{m} F_{-j_k}.$$

If i_p and j_p are odd, then, by Lemma 7,

$$\sum_{k=p}^{h} F_{-} > -F_{-i_p+1} \quad \text{and} \quad -F_{-j_p-1} \ge \sum_{k=p}^{m} F_{-j_k}.$$

Also, $i_p - 2 \ge j_p$, and so $-F_{-i_p+1} \ge -F_{-j_p-1}$, which is impossible.

If i_p is odd and j_p is even, then

$$\sum_{k=p}^{h} F_{-i_k} \text{ is positive and } \sum_{k=p}^{m} F_{-j_k} \text{ is negative}$$

by Lemma 7.

Similarly, if i_p is even and j_p is odd, then

$$\sum_{k=p}^{h} F_{-i_k} \text{ is negative and } \sum_{k=p}^{m} F_{-j_k} \text{ is positive}$$

by Lemma 7.

If i_p and j_p are both even, then $i_p - 2 \ge j_p$, and by Lemma 7,

$$\sum_{k=p}^{h} F_{-i_k} \le -F_{i_p+1} \quad \text{and} \quad -F_{-i_p-1} < \sum_{k=p}^{m} F_{-j_k}$$

and also

$$-F_{i_p+1} \le -F_{-j_p-1},$$

which is impossible.

Thus, for $1 \le k \le m$, $i_k = j_k$.

If $m < h$, we have by the above:

$$n = \sum_{k=1}^{m} F_{-i_k} = \sum_{k=1}^{h} F_{-i_k},$$

so

$$\sum_{k=m+1}^{h} F_{-i_k} = 0.$$

If $h > m + 1$, then by Lemma 7, if i_{m+1} is odd, $-F_{-i_{m+1}+1} < 0$, and if i_{m+1} is even, then $0 \leq -F_{-i_{m+1}+1}$, both of which are impossible.

If $h = m + 1$, then $F_{-i_h} = 0$, which is impossible because $i_h \neq 0$.

Therefore, the representation of n is unique and minimal.

As any representation of a number n as a sum of Fibonacci numbers

$$\sum_{k=1}^{h} F_{-i_k}, \text{ where } i_1 > i_2 > \cdots > i_h > 0,$$

can be changed to

$$\sum_{k=1}^{h-1} F_{-i_k} + F_{-i_h-1} + F_{-i_h-2},$$

it is clear that there can be no maximal number of Fibonacci numbers in a given sum.

References

1. J. L. Brown. "Zeckendorf's Theorem and Some Applications." *Fibonacci Quarterly 2.2* (1964):163-68.
2. J. L. Brown. "A New Characterization of the Fibonacci Numbers." *Fibonacci Quarterly 3.1* (1975):1-8.

*****

Author and Title Index for *The Fibonacci Quarterly*

Currently, Dr. Charles K. Cook of the University of South Carolina at Sumter is working on an AUTHOR index, TITLE index and PROBLEM index for *The Fibonacci Quarterly.* In fact, the three indices are already completed. We hope to publish these indices in 1993 which is the 30th anniversary of *The Fibonacci Quarterly.* Dr. Cook and I feel that it would be very helpful if the publication of the indices also had AMS classification numbers for all articles published in *The Fibonacci Quarterly.* We would deeply appreciate it if all authors of articles published in *The Fibonacci Quarterly* would take a few minutes of their time and send a list of articles with primary and secondary classification numbers to

PROFESSOR CHARLES K. COOK
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SOUTH CAROLINA AT SUMTER
1 LOUISE CIRCLE
SUMTER, S.C. 29150

The Editor
Gerald E. Bergum

FIBONACCI SEQUENCES IN FINITE GROUPS

Steven W. Knox*
The College of Wooster, Wooster, OH 44691

(Submitted May 1990)

0. Introduction

The Fibonacci sequence and its related higher-order sequences (tribonacci, quatranacci, k-nacci) are generally viewed as sequences of integers. In 1960, Wall [4] considered Fibonacci sequences modulo some fixed integer m; i.e., Fibonacci sequences of elements of $\mathbb{Z}_m$. He proved that these sequences were periodic for any m. Shah [3] partially determined for which integers the Fibonacci sequence modulo m contained the complete residue system, $\mathbb{Z}_m$. The papers of Wall [4] and Shah [3] provided the motivation for Wilcox's [5] study of the Fibonacci sequence in finite abelian groups.

This paper is in the spirit of [3], [4], and [5]. It addresses not only the traditional Fibonacci (2-nacci) sequence, but also the k-nacci sequence, and does so for finite (not necessarily abelian) groups.

1. Definitions and Notation

A *k-nacci sequence in a finite group* is a sequence of group elements x_0, x_1, x_2, x_3, ..., x_n, ... for which, given an initial (seed) set x_0, ..., x_{j-1}, each element is defined by

$$x_n = \begin{Bmatrix} x_0x_1 \ldots x_{n-1} \text{ for } j \le n < k \\ \\ x_{n-k}x_{n-k+1} \ldots x_{n-1} \text{ for } n \ge k \end{Bmatrix}.$$

We also require that the initial elements of the sequence, x_0, ..., x_{j-1}, generate the group, thus forcing the k-nacci sequence to reflect the structure of the group. The k-nacci sequence of a group G seeded by x_0, ..., x_{j-1} is denoted by $F_k(G; x_0, \ldots, x_{j-1})$.

The classic Fibonacci sequence in the integers modulo m can be written as $F_2(\mathbb{Z}_m; 0, 1)$. We call a 2-nacci sequence of group elements a *Fibonacci sequence of a finite group*.

A finite group G is *k-nacci sequenceable* if there exists a k-nacci sequence of G such that every element of the group appears in the sequence.

A sequence of group elements is *periodic* if, after a certain point, it consists only of repetitions of a fixed subsequence. The number of elements in the repeating subsequence is the *period* of the sequence. The sequence a, b, c, d, b, c, d, b, c, d, ... is periodic after the initial element a and has period 3. We denote the period of a k-nacci sequence $F_k(G; x_0, \ldots, x_{j-1})$ by $P_k(G; x_0, \ldots, x_{j-1})$. A sequence is *simply periodic* with period k if the first k elements in the sequence form a repeating subsequence. For example, a, b, c, d, e, a, b, c, d, e, ... is simply periodic with period 5.

2. Theorems

Theorem 1: A k-nacci sequence in a finite group is simply periodic.

*This work was supported by NSF grant DMS-8900507.

Proof: Let n be the order of G. Since there are n^k distinct k-tuples of elements of G, at least one of the k-tuples appears twice in a k-nacci sequence of G. Therefore, the subsequence following this k-tuple repeats; hence, the k-nacci sequence is periodic.

Since the sequence is periodic, there exist natural numbers i and j, with $i > j$, such that

$$x_{i+1} = x_{j+1},\ x_{i+2} = x_{j+2},\ x_{i+3} = x_{j+3},\ \ldots,\ x_{i+k} = x_{j+k}.$$

By the defining relation of a k-nacci sequence, we know that

$$x_i = x_{i+k}(x_{i+(k-1)})^{-1}(x_{i+(k-2)})^{-1} \ldots (x_{i+1})^{-1}$$

and

$$x_j = x_{j+k}(x_{j+(k-1)})^{-1}(x_{j+(k-2)})^{-1} \ldots (x_{j+1})^{-1}.$$

Hence, $x_i = x_j$, and it then follows that

$$x_{i-1} = x_{j-1},\ x_{i-2} = x_{j-2},\ \ldots,\ x_{i-j} = x_{j-j} = x_0.$$

Therefore, the sequence is simply periodic.

This is a generalization of a theorem of Wall [4], which states that $F(\mathbb{Z}_m; 0, 1)$, the classically seeded Fibonacci sequence of the integers modulo m, is simply periodic. From the proof of Theorem 1, we have $|G|^k$ as an upper bound for the period of any k-nacci sequence in a group G.

We will now address the periods of k-nacci sequences in specific classes of groups. A Group D_n is *dihedral* if

$$D_n = \langle a, b : a^n = b^2 = e \text{ and } ba = a^{-1}b \rangle.$$

The order of the group D_n is $2n$. Note that in a dihedral group generated by a and b,

$$(ab)^2 = abab = aa^{-1}b^2 = e \text{ and } (ba)^2 = baba = baa^{-1}b = e.$$

Theorem 2: Consider the dihedral group D_n for some $n \geq 3$ with generators a, b. Then $P_k(D_n; a, b) = P_k(D_n; b, a) = 2k + 2$.

Proof: Let the orders of a and b be n and 2, respectively. If $k = 2$, the possible sequences are

$$a,\ b,\ ab,\ a^{-1},\ a^2b,\ ab,\ a,\ b,\ \ldots$$

and

$$b,\ a,\ a^{-1}b,\ b,\ a^{-1},\ ab,\ b,\ a,\ \ldots,$$

both of which have period 6. If $k \geq 3$, the first k elements of $F_k(D_n; a, b)$ are

$$x_0 = a,\ x_1 = b,\ x_2 = ab,\ x_3 = (ab)^2,\ \ldots,\ x_{k-1} = (ab)^{2^{k-3}}.$$

This sequence reduces to

$$a,\ b,\ ab,\ e,\ e,\ \ldots,\ e,\ e$$

where $x_j = e$ for $3 \leq j \leq k - 1$. Thus,

$$x_k = \prod_{i=0}^{k-1} x_i = abab = e, \qquad x_{k+1} = \prod_{i=1}^{k} x_i = bab = a^{-1},$$

$$x_{k+2} = \prod_{i=2}^{k+1} x_i = aba^{-1} = a^2b, \qquad x_{k+3} = \prod_{i=3}^{k+2} x_i = a^{-1}a^2b = ab,$$

$$x_{k+4} = \prod_{i=4}^{k+3} x_i = a^{-1}a^2bab = e.$$

It follows that $x_{k+j} = e$ for $4 \leq j \leq k$. We also have:

$$x_{k+k+1} = \prod_{i=k+1}^{k+k} x_i = a^{-1}a^2bab = e, \qquad x_{k+k+2} = \prod_{i=k+2}^{k+k+1} x_i = a^2bab = a,$$
$$x_{k+k+3} = \prod_{i=k+3}^{k+k+2} x_i = aba = b, \qquad x_{k+k+4} = \prod_{i=k+4}^{k+k+3} x_i = ab.$$

Since the elements succeeding x_{2k+2}, x_{2k+3}, x_{2k+4}, depend on a, b, and ab for their values, the cycle begins again with the $2k+2$nd element; i.e., $x_0 = x_{2k+2}$. Thus, the period of $F_k(D_n;\ a,\ b)$ is $2k+2$. If we choose to seed the sequence with the generators in the other order, we see that the sequence b, a, ba, $(ba)^2$, $(ba)^4$, $(ba)^8$, ..., $(ba)^{2^{k-3}}$ reduces to b, a, ba, e, e, ..., e, e and the proof works similarly.

If a group is generated by i elements, then it is said to be an *i-generated group*.

Theorem 3: If G is a 2-generated group with generators a and b, and the identity element appears in $F_2(G;\ a,\ b)$ or $F_2(G;\ b,\ a)$, a Fibonacci sequence of G, then G is abelian.

Proof: Without loss of generality consider the sequence $F_2(G;\ a,\ b)$ and suppose the identity, e, is the $n+1$st element of this Fibonacci sequence for some natural number n. The nth element of the sequence may be any element of the group. Thus, we have a sequence

$$a,\ b,\ \ldots,\ s,\ e,\ \ldots\ .$$

What precedes s? Only s^{-1} could satisfy the defining relation for the $n-1$st position. Similarly, s^2 must be in the $n-2$nd sequence position, s^{-3} in the $n-3$rd, and so on, forming the sequence

$$a,\ b,\ \ldots,\ s^{-8},\ s^5,\ s^{-3},\ s^2,\ s^{-1},\ s^1,\ e,\ \ldots\ .$$

Since these elements have exponents generated using the relation $u_{i-2} = -u_{i-1} + u_i$, which is equivalent to $u_i = u_{i-1} + u_{i-2}$, we find the Fibonacci sequence of integers occurring in the exponents of s, with alternating signs. Hence, a Fibonacci sequence of the group has one of two forms:

(i) n odd: The sequence is

$$s^{u_n},\ s^{-u_{n-1}},\ s^{u_{n-2}},\ \ldots,\ s^5,\ s^{-3},\ s^2,\ s^{-1},\ s^1,\ e.$$

In this case, we have

$$s^{u_n} = a,\ s^{-u_{n-1}} = b$$

(which implies $s^{u_{n-1}} = b^{-1}$), and $s^{u_{n-2}} = ab$. Since

$$s^{u_{n-1}}\, s^{u_{n-2}} = s^{u_{n-1}+u_{n-2}} = s^{u_n},$$

we have $b^{-1}ab = a$, or $ab = ba$. Therefore, the group is abelian.

(ii) n even: The sequence is

$$s^{-u_n},\ s^{u_{n-1}},\ s^{-u_{n-2}},\ \ldots,\ s^5,\ s^{-3},\ s^2,\ s^{-1},\ s^1,\ e.$$

In this case, we have

$$s^{-u_n} = a,\ s^{u_{n-1}} = b$$

(which implies $s^{-u_{n-1}} = b^{-1}$), and $s^{-u_{n-2}} = ab$. Since

$$s^{-u_{n-1}}\, s^{-u_{n-2}} = s^{-(u_{n-1}+u_{n-2})} = s^{-u_n},$$

we have $b^{-1}ab = a$, or $ab = ba$. Therefore, the group is abelian.

The converse of Theorem 3 does not hold. Consider the abelian group

$$A = \langle a,\ b\colon\ a^9 = b^2 = e \text{ and } ba = ab\rangle.$$

The Fibonacci sequences of this group are:

$$a, b, ab, a, a^2b, a^3b, a^5, a^8b, a^4b, a^3, a^7b, ab, a^8, b,$$
$$a^8b, a^8, a^7b, a^6b, a^4, ab, a^5b, a^6, a^2b, a^8b, a, b, ab, \ldots,$$

and

$$b, a, ab, a^2b, a^3, a^5b, a^8b, a^4, a^3b, a^7b, a, a^8b, b, a^8,$$
$$a^8b, a^7b, a^6, a^4b, ab, a^5, a^6b, a^2b, a^8, ab, b, a, ab, \ldots .$$

The elements e, a^2, and a^7 do not appear in either sequence.

Corollary: A 2-nacci sequenceable group is cyclic.

Proof: Let G be a 2-nacci sequenceable group. Then G is either 1- or 2-generated. If G is 2-generated, then since e appears in the 2-nacci sequence of G, we can construct the sequence in terms of an element $s \in G$ as in the proof of Theorem 3. Every element of G appears in its 2-nacci sequence, and therefore all the elements of G may be represented in terms of a single element, s. Hence, G is 1-generated, or cyclic.

For $k \geq 3$, k-nacci sequenceable groups are not, in general, abelian. The dihedral group of six elements is 3-nacci sequenceable.

Theorem 4: If the identity element appears in a Fibonacci sequence of a 2-generated group, then the collection of subscripts of the sequence elements x_i for which $x_i = e$ contains a sequence which has an arithmetic progression.

Proof: By Theorem 3 the group $G = \langle a, b \rangle$ is abelian. Hence, the n^{th} term of the sequence has the form $a^{u_{n-1}} b^{u_n}$. By a theorem of Wall [4], we know that the terms where $u_n \equiv 0 \pmod{m}$ have subscripts that form a simple arithmetic progression. Thus, the sequences of elements $a, a, a^2, \ldots, a^{u_n}$ and $b, b, b^2, b^3, \ldots, b^{u_n}$ both have e occurring in positions whose subscripts form arithmetic progressions, with the period of the occurrence of e depending on the order of a and b. The period of this induced occurrence of e in $a, b, ab, ab^2, a^2b^3, \ldots$ will be the least common multiple of the period of e in $a, a, a^2, \ldots$ and the period of e in $b, b, b^2, b^3, \ldots$. Hence, the positions of e in $a, b, ab, ab^2, a^2b^3, \ldots$ will have subscripts which contain an arithmetic progression.

3. An Open Question

It is clear that a homomorphic image of a k-nacci sequenceable group is k-nacci sequenceable. The extension of a k-nacci sequenceable group by a k-nacci sequenceable group is not necessarily k-nacci sequenceable. In fact, the direct product of k-nacci sequenceable groups is not necessarily k-nacci sequenceable.

We refer to the abelian group

$$A = \langle a, b \colon a^9 = b^2 = e \text{ and } ba = ab \rangle.$$

The group $\langle b \rangle$ has a Fibonacci sequence

$$F_2(\langle b \rangle; e, b) = e, b, b, e, \ldots,$$

and hence is 2-nacci sequenceable. The group $\langle a \rangle$ has a sequence

$$F_2(\langle a \rangle; e, a) = e, a, a, a^2, a^3, a^5, a^8, a^4, a^3, a^7, a, a^8, e, a^8, a^8,$$
$$a^7, a^6, a^4, a, a^5, a^6, a^2, a^8, a, e, a, a, \ldots$$

and hence is 2-nacci sequenceable. We have already seen that A, the direct product of $\langle a \rangle$ and $\langle b \rangle$, is not 2-nacci sequenceable.

Question: Are all nonsimple k-nacci sequenceable groups nontrivial extensions of a k-nacci sequenceable group by a k-nacci sequenceable group? That is, does a nonsimple k-nacci sequenceable group have a k-nacci sequenceable normal subgroup?

References

1. Derek K. Chang. "Higher-Order Fibonacci Sequences Modulo m." *Fibonacci Quarterly* *24.2* (1986):138-39.
2. Mark Feinberg. "Fibonacci-Tribonacci." *Fibonacci Quarterly* *1.2* (1963):71-74.
3. A. P. Shah. "Fibonacci Sequence Modulo m." *Fibonacci Quarterly* *6.2* (1968): 139-41.
4. D. D. Wall. "Fibonacci Series Modulo m." *American Math. Monthly* *67* (1960): 525-32.
5. Howard J. Wilcox. "Fibonacci Sequences of Period n in Groups." *Fibonacci Quarterly* *24.4* (1986):356-61.

*****

Applications of Fibonacci Numbers

Volume 4

New Publication

Proceedings of 'The Fourth International Conference on Fibonacci Numbers and Their Applications, Wake Forest University, July 30-August 3, 1990'

edited by **G.E. Bergum, A.N. Philippou** and **A.F. Horadam**

This volume contains a selection of papers presented at the Fourth International Conference on Fibonacci Numbers and Their Applications. The topics covered include number patterns, linear recurrences and the application of the Fibonacci Numbers to probability, statistics, differential equations, cryptography, computer science and elementary number theory. Many of the papers included contain suggestions for other avenues of research.

For those interested in applications of number theory, statistics and probability, and numerical analysis in science and engineering.

1991, 314 pp. ISBN 0—7923—1309—7
Hardbound Dfl. 180.00/£61.00/US $99.00

A.M.S. members are eligible for a 25% discount on this volume providing they order directly from the publisher. However, the bill must be prepaid by credit card, registered money order or check. A letter must also be enclosed saying "I am a member of the American Mathematical Society and am ordering the book for personal use."

KLUWER
ACADEMIC
PUBLISHERS

P.O. Box 322, 3300 AH Dordrecht, The Netherlands
P.O. Box 358, Accord Station, Hingham, MA 02018-0358, U.S.A.

MORE BINOMIAL COEFFICIENT CONGRUENCES

D. F. Bailey
Trinity University, San Antonio, TX 78212

(Submitted May 1990)

1. Introduction

In 1878 Edouard Lucas gave the following result for computing binomial coefficients modulo a prime [3], [4].

Theorem 1.1: If p is a prime, n, r, n_0, and r_0 are nonnegative integers, and n_0 and r_0 are both less than p, then

$$\binom{np + n_0}{rp + r_0} \equiv \binom{n}{r}\binom{n_0}{r_0} \pmod{p}.$$

We have recently derived the following variations of Lucas' Theorem (see [1]).

Theorem 1.2: If n and r are nonnegative integers, and p is prime, then

$$\binom{np}{rp} \equiv \binom{n}{r} \pmod{p^2}.$$

Theorem 1.3: If n and r are nonnegative integers, and p is a prime greater than 3, then

$$\binom{np}{rp} \equiv \binom{n}{r} \pmod{p^3}.$$

In [2] we have also obtained the following congruences which bear a strong resemblance to the theorem of Lucas.

Theorem 1.4: If p is prime, n and r are nonnegative integers, and i is an integer strictly between 0 and p, then

$$\binom{np}{rp + i} \equiv (r + 1)\binom{n}{r + 1}\binom{p}{i} \pmod{p^2}.$$

Theorem 1.5: If $p \geq 5$ is prime, n, m, and k are nonnegative integers, $k < p$, and i is an integer strictly between 0 and p, then

$$\binom{mp^2}{np^2 + kp + i} \equiv (n + 1)\binom{m}{n + 1}\binom{p^2}{kp + i} \pmod{p^3}.$$

In this paper we show that in fact an infinite sequence of results like those above hold. In our proofs we need the following result (see, e.g., [5]).

Theorem 1.6: If p is prime, $n = p^s$, and p^t divides k while p^{t+1} does not divide k, then p^{s-t} divides $\binom{n}{k}$ and p^{s-t+1}does not divide $\binom{n}{k}$.

2. Main Results

Our first result is as follows.

Theorem 2.1: If $p \geq 5$ is prime, n and m are nonnegative integers, s and all the a_k are integers with $s \geq 1$, $0 < a_0 < p$, and $0 \leq a_k < p$ for $k = 1, 2, \ldots, s - 1$, then

$$\binom{mp^s}{np^s + a_{s-1}p^{s-1} + \cdots + a_1p + a_0}$$

$$\equiv (n+1)\binom{m}{n+1}\binom{p^s}{a_{s-1}p^{s-1} + \cdots + a_1p + a_0} \pmod{p^{s+1}}.$$

Proof: Theorems 1.4 and 1.5 show that the conclusion of the theorem is valid for $s = 1$ and $s = 2$. We assume therefore that the theorem's conclusion holds for some $s \geq 2$ and consider the assertion

$$\binom{mp^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_1p + a_0}$$

$$\equiv (n+1)\binom{m}{n+1}\binom{p^{s+1}}{a_sp^s + \cdots + a_1p + a_0} \pmod{p^{s+2}}.$$

If $m = 0$ the assertion above is merely that $0 \equiv 0$. Likewise, if $m = 1$ one can check that our inductive assertion holds trivially. Therefore, we assume the validity of the inductive assertion for some $m \geq 1$ and consider first the case in which $n = 0$. Then we must treat

$$\binom{(m+1)p^{s+1}}{a_sp^s + \cdots + a_1p + a_0} = \sum_{j=0}^{a_sp^s + \cdots + a_1p + a_0}\binom{mp^{s+1}}{a_sp^s + \cdots + a_0 - j}\binom{p^{s+1}}{j}.$$

We first show that whenever $0 < j < a_sp^s + \cdots + a_1p + a_0$, we have

(1) $$\binom{mp^{s+1}}{a_sp^s + \cdots + a_1p + a_0 - j}\binom{p^{s+1}}{j} \equiv 0 \pmod{p^{s+2}}.$$

To this end, let $j = b_sp^s + \cdots + b_1p + b_0$ and note that, if $b_0 \neq 0$, then Theorem 1.6 shows that

$$\binom{p^{s+1}}{j} \equiv 0 \pmod{p^{s+1}}.$$

Moreover, by Theorem 1.1,

$$\binom{mp^{s+1}}{a_sp^s + \cdots + a_0 - j} = \binom{mp^{s+1}}{c_sp^s + \cdots + c_0}$$

$$\equiv \binom{m}{0}\binom{0}{c_s}\binom{0}{c_{s-1}} \cdots \binom{0}{c_0} \equiv 0 \pmod{p},$$

since not all the c_i are zero. Hence, we have the product in (1) congruent to 0 modulo p^{s+2} as desired. If, on the other hand, $b_0 = 0$, we see that

$$\binom{mp^{s+1}}{a_sp^s + \cdots + a_0 - j} = \binom{mp^{s+1}}{c_sp^s + \cdots + c_1p + a_0}$$

and that this last is congruent to zero modulo p^{s+1} since $a_0 \neq 0$ by hypothesis. Likewise, one can argue that

$$\binom{p^{s+1}}{j} \equiv 0 \pmod{p},$$

and again the product in (1) is congruent to 0 modulo p^{s+2}.

Therefore, we have established that

$$\binom{(m+1)p^{s+1}}{a_sp^s + \cdots + a_1p + a_0} \equiv \binom{mp^{s+1}}{a_sp^s + \cdots + a_0} + \binom{p^{s+1}}{a_sp^s + \cdots + a_0} \pmod{p^{s+2}}$$

and by the inductive hypothesis this is congruent modulo p^{s+2} to

$$(m+1)\binom{p^{s+1}}{a_sp^s + \cdots + a_1p + a_0}$$

which is the desired result.

Next we assume $n \neq 0$ and consider

$$\binom{(m+1)p^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_0} = \sum_{j=0}^{p^{s+1}} \binom{mp^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_0 - j}\binom{p^{s+1}}{j}.$$

As previously, one can show that all terms in the above sum are congruent to 0 modulo p^{s+2} save those where $j = 0$, $j = p^{s+1}$, or $j = a_sp^s + \cdots + a_0$. So, thus far, we have

$$\binom{(m+1)p^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_1 + a_0}$$

$$\equiv \binom{mp^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_1p + a_0} + \binom{mp^{s+1}}{np^{s+1}}\binom{p^{s+1}}{a_sp^s + \cdots + a_0}$$

$$\binom{mp^{s+1}}{(n-1)p^{s+1} + a_sp^s + \cdots + a_1p + a_0} \pmod{p^{s+2}}.$$

Now consider the terms on the right-hand side of the above congruence. By the inductive assumption

$$\binom{mp^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_1p + a_0}$$

$$\equiv (n+1)\binom{m}{n+1}\binom{p^{s+1}}{a_sp^s + \cdots + a_1p + a_0} \pmod{p^{s+2}}.$$

Moreover, since

$$\binom{mp^{s+1}}{np^{s+1}} - \binom{m}{n} \equiv 0 \pmod{p} \text{ and } \binom{p^{s+1}}{a_sp^s + \cdots + a_0} \equiv 0 \pmod{p^{s+1}},$$

$$\binom{mp^{s+1}}{np^{s+1}}\binom{p^{s+1}}{a_sp^s + \cdots + a_0} \equiv \binom{m}{n}\binom{p^{s+1}}{a_sp^s + \cdots + a_0} \pmod{p^{s+2}}.$$

And calling on the inductive assumption once again, we see that

$$\binom{mp^{s+1}}{(n-1)p^{s+1} + a_sp^s + \cdots + a_1p + a_0}$$

$$\equiv n\binom{m}{n}\binom{p^{s+1}}{a_sp^s + \cdots + a_1p + a_0} \pmod{p^{s+2}}.$$

Thus, we conclude that

$$\binom{(m+1)p^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_1p + a_0}$$

$$\equiv \left[(n+1)\binom{m}{n+1} + \binom{m}{n} + n\binom{m}{n}\right]\binom{p^{s+1}}{a_sp^s + \cdots + a_0} \pmod{p^{s+2}}.$$

But this last expression is obviously

$$(n+1)\binom{m+1}{n+1}\binom{p^{s+1}}{a_sp^s + \cdots + a_1p + a_0}.$$

This completes the induction and establishes the theorem.

Our next result generalizes that of Theorem 1.3.

Theorem 2.2: If $p \geq 5$ is prime and k, r, and s are all nonnegative integers, then

$$\binom{kp^{s+1}}{rp^{s+1}} \equiv \binom{kp^s}{rp^s} \pmod{p^{s+3}}.$$

Proof: We proceed by induction. For $s = 0$ the assertion is identical with that of Theorem 1.3. We therefore assume the result for some $s \geq 0$ and consider the assertion

$$(2) \qquad \binom{kp^{s+2}}{rp^{s+2}} \equiv \binom{kp^{s+1}}{rp^{s+1}} \pmod{p^{s+4}}.$$

Obviously assertion (2) holds for $r = 0$. Thus, we fix $r \geq 1$, assume (2) holds for all smaller r, and establish our assertion by induction on k. Assertion (2) clearly holds for $k \leq r$, so we assume its validity for some fixed $k \geq r$ and consider

$$\binom{(k+1)p^{s+2}}{rp^{s+2}} = \sum_{i=0}^{p^{s+2}} \binom{kp^{s+2}}{rp^{s+2} - i}\binom{p^{s+2}}{i} = \sum_{i=0}^{p^{s+1}} \binom{kp^{s+2}}{rp^{s+2} - lp}\binom{p^{s+2}}{lp} + B$$

where B is the sum of those terms of the form

$$\binom{kp^{s+2}}{rp^{s+2} - i}\binom{p^{s+2}}{i} \quad \text{for } i \text{ not a multiple of } p.$$

As in Theorem 2.1, it is easy to show that each summand in B is congruent to 0 modulo p^{s+4}. Therefore, we have

$$(3) \qquad \binom{(k+1)p^{s+2}}{rp^{s+2}} \equiv \sum_{l=0}^{p^{s+1}} \binom{kp^{s+2}}{rp^{s+2} - lp}\binom{p^{s+2}}{lp} \pmod{p^{s+4}}.$$

Now we consider a particular summand in (3) with $0 < l < p^{s+1}$ so that

$$l = a_s p^s + a_{s-1}p^{s-1} + \cdots + a_q p^q \text{ where } a_q \neq 0 \text{ and } 0 \leq q \leq s.$$

Then

$$\binom{p^{s+2}}{lp} = \binom{p^{s+1-q}p^{q+1}}{(a_s p^{s-q} + \cdots + a_q)p^{q+1}}$$

$$\equiv \binom{p^{s+1-q}p^q}{(a_s p^{s-q} + a_{s-1}p^{s-q-1} + \cdots + a_q)p^q} \pmod{p^{q+3}}$$

by inductive assumption. But this simply says

$$\binom{p^{s+2}}{lp} \equiv \binom{p^{s+1}}{l} \pmod{p^{q+3}}.$$

One can also show

$$\binom{p^{s+1}}{l} \equiv 0 \pmod{p^{s+1-q}},$$

$$\binom{kp^{s+2}}{rp^{s+2} - lp} \equiv \binom{kp^{s+1}}{rp^{s+1} - l} \pmod{p^{q+3}},$$

and

$$\binom{kp^{s+2}}{rp^{s+2} - lp} \equiv 0 \pmod{p^{s+1-q}}.$$

Therefore,

$$\binom{p^{s+2}}{lp}\binom{kp^{s+2}}{rp^{s+2}-lp} \equiv \binom{p^{s+1}}{l}\binom{kp^{s+2}}{rp^{s+2}-lp} \pmod{p^{s+4}}$$

and

$$\binom{p^{s+1}}{l}\binom{kp^{s+1}}{rp^{s+2}-lp} \equiv \binom{p^{s+1}}{l}\binom{kp^{s+1}}{rp^{s+1}-l} \pmod{p^{s+4}}.$$

It follows then that

$$\binom{p^{s+2}}{lp}\binom{kp^{s+2}}{rp^{s+2}-lp} \equiv \binom{p^{s+1}}{l}\binom{kp^{s+1}}{rp^{s+1}-l} \pmod{p^{s+4}}.$$

Now if we note finally that the inductive hypotheses on k and r insure that

$$\binom{kp^{s+2}}{rp^{s+2}} \equiv \binom{kp^{s+1}}{rp^{s+1}} \pmod{p^{s+4}}$$

holds, as does a similar statement with r replaced by $r-1$, we see that

$$\binom{(k+1)p^{s+2}}{rp^{s+2}} \equiv \sum_{l=0}^{p^{s+1}} \binom{kp^{s+1}}{rp^{s+1}-l}\binom{p^{s+1}}{l} \pmod{p^{s+4}}.$$

But this clearly gives

$$\binom{(k+1)p^{s+2}}{rp^{s+2}} \equiv \binom{(k+1)p^{s+1}}{rp^{s+1}} \pmod{p^{s+4}}.$$

This completes the inductive proof of assertion (2) and establishes the theorem.

Remark: Professor Ira Gessel has called the author's attention to a result which implies Theorem 2.2. See Ira Gessel, "Some Congruences for Generalized Euler Numbers," *Can. J. Math.* *35.4* (1983):687-709.

References

1. D. F. Bailey. "Two p^3 Variations of Lucas' Theorem." *J. Number Theory* *35.2* (1990):208-15.
2. D. F. Bailey. "Some Binomial Coefficient Congruences." *Applied Math. Letters* *4.4* (1991):1-5.
3. N. J. Fine. "Binomial Coefficients Modulo a Prime." *Amer. Math. Monthly* *54* (1947):589-92.
4. Edouard Lucas. "Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier." *Bull Soc. Math. France* *6* (1878):49-54.
5. David Singmaster. "Divisibility of Binomial and Multinomial Coefficients by Primes and Prime Powers." *A Collection of Manuscripts Related to the Fibonacci Sequence.* Santa Clara, Calif: The Fibonacci Association, 1980, pp. 98-113.

*****

k-REVERSE MULTIPLES

Anne Ludington Young
Loyola College in Maryland, Baltimore, MD 21210

(Submitted May 1990)

We begin with the simple observation that $4 \cdot (2178) = 8712$. That is, when 2187 is multiplied by 4, the result is 8712 which is 2178 with the digits reversed. Since 4 is the multiplier that produces the reversal of digits, we call 2178 a *4-reverse multiple*. More generally, let x be an n-digit, base g number

$$(1) \qquad x = \sum_{i=0}^{n-1} a_i g^i$$

with $0 \le a_i < g$ and $a_{n-1} \neq 0$. Then x is called a *k-reverse multiple* if, for some integer k, $1 < k < g$,

$$(2) \qquad kx = \sum_{i=0}^{n-1} a_{n-1-i} g^i.$$

Previously, most work on k-reverse multiples has focused on either finding all those less than a given m [1], or characterizing, for a given n, those with n-digits. This latter problem seems to be quite difficult and has been completely solved only for the 2- and 3-digit cases (see [1] and [3]). Additionally, various schemes have been advanced for calculating these multiples (see [2] and [3]). Beyond this, it has been noted that once a k-reverse multiple is known, it may be used to create others. For example, it is easily verified that 21782178 and 21978 are also base 10, 4-reverse multiples.

What has not been discussed previously is how to find *all* k-reverse multiples once those with a small number of digits are known. For example, in base 11, 118 and 1298 are 7-reverse multiples. While it is clear that 118118 is a 7-reverse multiple, it is not as obvious that 11918 is also such a multiple. This question, of how to form multiples having a large number of digits from those with a small number, is the focus of our discussion. As we will see, the solution has a graphic representation.

We begin by supposing that x is an n-digit, base g, k-reverse multiple. From (1) and (2), we obtain the following set of equations by comparing corresponding digits of kx:

$$(3) \qquad \begin{array}{llll} ka_0 & & = a_{n-1} & + r_0 g \\ ka_1 & + r_0 & = a_{n-2} & + r_1 g \\ & & \cdots & \\ ka_i & + r_{i-1} & = a_{n-1-i} & + r_i g \\ & & \cdots & \\ ka_{n-2} & + r_{n-3} & = a_1 & + r_{n-2} g \\ ka_{n-1} & + r_{n-2} & = a_0 & \end{array}$$

where $0 \le r_i < g$ for $i = 0, \ldots, n-2$. The last equation implies $a_0 \neq 0$ since $a_{n-1} \neq 0$. The r_i's are the so-called "carry numbers." As we will see, these numbers determine the character of k-reverse multiples.

To determine whether there are any k-reverse multiples for a given g and k, we consider the equations in (3) two at a time. For convenience, let $r_{-1} = r_{n-1} = 0$. At the $(i+1)^{\text{st}}$ step, $i = 0, 1, \ldots$, we examine the pair of equations

$$(4)\qquad \begin{cases} ka_i + r_{i-1} = a_{n-1-i} + r_i g \\ ka_{n-1-i} + r_{n-2-i} = a_i + r_{n-1-i} g \end{cases}$$

where r_{i-1} and r_{n-1-i} are known from the previous step. That is, we seek nonnegative integers a_i, a_{n-1-i}, r_i, and r_{n-2-i} which, in addition to (4), satisfy

$$(5)\qquad \begin{cases} 0 < a_0,\ a_{n-1} \\ a_i < g,\ i = 0, 1, \ldots, n-1 \end{cases}$$

and

$$(6)\qquad r_i < g,\ i = 0, 1, \ldots, n-2.$$

The equations in (4) along with the inequalities in (5) imply tighter restrictions in (6). That is the content of the following lemma.

Lemma 1: Suppose there exist nonnegative integers which satisfy (4) and (5) for $i = 0, 1, \ldots, n-1$. Then the following hold:

$$(7)\qquad \begin{cases} 0 < r_0 \\ r_i < k \text{ for } i = 0, \ldots, n-2. \end{cases}$$

Proof: Solving (4) for a_i gives

$$(8)\qquad a_i = (kr_i g - kr_{i-1} + r_{n-1-i}g - r_{n-2-i})/(k^2 - 1).$$

Letting $i = 0$ and using $r_{-1} = r_{n-1} = 0$ in (8) gives

$$a_0(k^2 - 1) = kr_0 g - r_{n-2}.$$

Hence, $0 < r_0$ since $1 < k$, $0 < a_0$, and $0 \le r_{n-2}$.

To show the second part of (7), suppose $r_{i-1} < k$; note that when $i = 0$, the supposition is valid. Then from the general equation in (3) we have

$$r_i g \le ka_i + r_{i-1} < ka_i + k = k(a_i + 1) \le kg$$

and hence $r_i < k$. □

One convenient way to proceed is to look for nonnegative integers a_i and a_{n-1-i} satisfying (5) such that

$$(9)\qquad \begin{cases} ka_i + r_{i-1} \equiv a_{n-1-i} \pmod{g} \\ 0 \le a_i + r_{n-1-i}g - ka_{n-1-i} < k \end{cases}$$

where r_{i-1} and r_{n-1-i} have been determined in the previous step. If the a's exist, then r_i and r_{n-2-i} can be found by (4):

$$(10)\qquad \begin{cases} r_i = (ka_i + r_{i-1} - a_{n-1-i})/g \\ r_{n-2-i} = a_i + r_{n-1-i}g - ka_{n-1-i}. \end{cases}$$

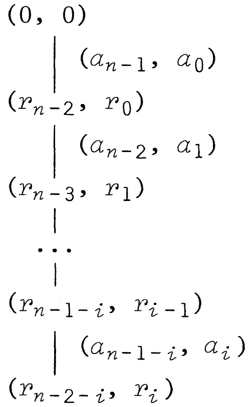
The restrictions in (9) guarantee the r's in (10) are nonnegative.

The above procedure is successful when, at each step, there are nonnegative integers a_i and a_{n-1-i} which satisfy (5) and (9). The following graphical notation will be convenient. If r_{n-1-i}, r_{i-1}, a_{n-1-i}, a_i, r_{n-2-i}, and r_i satisfy (4), (5), and (7), then we will write

$$(11)\qquad \begin{tikzcd} (r_{n-1-i}, r_{i-1}) \arrow[d, dash, "{(a_{n-1-i}, a_i)}"] \\ (r_{n-2-i}, r_i) \end{tikzcd}$$

and conversely. Thus, we hope to generate a graph, or more precisely, a rooted tree in which a path from the root to a node has the following form and labels:

(12)



We will use this notation in the examples below. Since $0 \le r_i < k$, there can be at most k^2 different pairs of r_i's used as node labels in the tree. If a node is labeled with an r-pair that has already appeared in the tree, the tree can be pruned after this node, since no new information will be obtained beyond this point. When needed for analysis, a pruned tree can be extended by replicating earlier sections of it. Before proceeding further with the exposition, we look at the tree for the 4-reverse multiple, 2178.

Example 1: $g = 10$, $k = 4$.

Let us begin by considering (9) with $i = 0$. The various possibilities are:

(13)

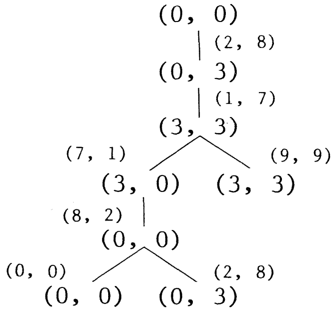
a_0	$a_{n-1} \equiv 4a_0$	$a_0 - 4a_{n-1}$
1	4	-15
2	8	-30
3	2	-5
4	6	-20
5	0	5
6	4	-10
7	8	-25
8	2	0
9	6	-15

Only $a_0 = 8$ satisfies the required condition

$$0 \le a_0 - 4a_{n-1} < k = 4.$$

Using (10), it can be shown that $r_{n-2} = 0$ and $r_0 = 3$. Continuing in this manner and using the above notation, the following is obtained:

(14)



The tree is not continued any further since (0, 0), (0, 3), and (3, 3) have appeared previously. The careful reader will observe that

$$\begin{array}{l}(0,\ 0)\\ \quad\Big|\ {\scriptstyle (0,\ 0)}\\ (0,\ 0)\end{array}$$

appears at the end of the tree, but not initially. This will always be the case since the equations in (4) are satisfied by the trivial or zero solution. Although $r_0 \neq 0$, the r-pair (0, 0) is permissible after the first step. □

The following question arises immediately. How do we use such a tree to find k-reverse multiples? The next two theorems provide answers.

Theorem 1: For a given g and k, suppose a tree of the form (12) exists; that is, suppose nonnegative solutions to (4), (5), and (7) exist. Then there is an $n = 2i + 2$-digit number satisfying (2) if and only if $r_{n-2-i} = r_i$. In this case, x is given by

$$x = a_{n-1}a_{n-2} \cdots a_{n-1-i}a_i \cdots a_1a_0. \tag{15}$$

Proof: In forming (12), the equations to be considered at the $(i+1)^{\text{st}}$ step are

$$\begin{cases} ka_i + r_{i-1} = a_{n-1-i} + r_i g \\ ka_{n-1-i} + r_{n-2-i} = a_i + r_{n-1-i}g \end{cases} \tag{16}$$

The two quantities in bold type are the r's to be determined at this step. If $n = 2i + 2$, then this is the last set of equations to be considered. Since

$$n - 2 - i = (2i + 2) - 2 - i = i,$$

$r_{n-2-i} = r_i$ and the conclusion follows. Conversely, if $r_{n-2-i} = r_i$, then we may stop with (16) by letting $n - 2 - i = i$ to give $n = 2i + 2$. □

Corollary 1: For base g, suppose there are k-reverse multiples. Let n be an even number. Then there exists an n-digit multiple if and only if the corresponding infinite tree contains a path of length $n/2$ from the root to a node designated by (u, u).

Proof: This is simply a restatement of Theorem 1. □

Example 1 continued: By Corollary 1, to find all base 10, 4-reverse multiples with an even number of digits, we traverse the tree in (14) stopping at nodes of the form (u, u). Thus, we see that (3, 3) gives rise to a 4-digit multiple. To find this number, we use (15) of Theorem 1. We read it off from the a-pairs, starting at the root, reading down the left-hand side and then back up the right. Thus, we find that 2178 is a 4-reverse multiple. So, too, are the following numbers:

219978, 21782178, 21999978,
2178002178, 2197821978, 2199999978.

Of course, there are infinitely many, but these are the ones with the least number of even digits. It should be remembered that the tree is actually infinite, and that pruned branches may be extended when needed to obtain additional desired numbers.

Theorem 2: For a given g and k, suppose a tree of the form (12) exists; that is, suppose nonnegative solutions to (4), (5), and (7) exist. Then there is an $n = 2i + 3$-digit number satisfying (2) if and only if

$$(k - 1) \mid (r_{n-2-i}g - r_i) \quad \text{and} \quad 0 \le (r_{n-2-i}g - r_i)/(k - 1) < g.$$

In this case, x is given by

$$x = a_{n-1}a_{n-2} \;\cdots\; a_{n-1-i}Ma_i \;\cdots\; a_1a_0 \tag{17}$$

where $M = (r_{n-2-i}g - r_i)/(k - 1)$.

Proof: If $n = 2i + 3$, then there are an odd number of equations in (3). After $(i+1)$ steps, we are left with

$$ka_{i+1} + r_i = a_{n-2-i} + r_{i+1}g. \tag{18}$$

Since $n - 2 - i = i + 1$, (18) becomes

$$ka_{i+1} + r_i = a_{i+1} + r_{n-2-i}g. \tag{19}$$

Because r_i and r_{n-2-i} are already known, we must have

$$a_{i+1} = (r_{n-2-i}g - r_i)/(k - 1). \tag{20}$$

Thus, after determining r_{n-2-i} and r_i, we can stop if and only if

$$(k - 1)\,|\,(r_{n-2-i}g - r_i) \quad \text{and} \quad 0 \le (r_{n-2-i}g - r_i)/(k - 1) < g.$$

When this occurs, x is given by (17). □

In order to apply Theorem 2 to a tree, we must check at each step to see if $(k - 1)\,|\,(r_{n-2-i}g - r_i)$ and $0 \le (r_{n-2-i}g - r_i)/(k - 1) < g$. Thus, in Example 1, since $3\,|\,(3 \cdot 10 - 3)$ and $0 \le (3 \cdot 10 - 3)/3 < 10$, the r-pair (3, 3) yields the 4-reverse multiple 21978. The following theorem simplifies this tedious checking process.

Theorem 3: For a given g and k, suppose a tree of the form (12) exists; that is, suppose nonnegative solutions to (4), (5), and (7) exist. Then there is an $n = 2i + 3$-digit number satisfying (2) if and only if the graph contains

$$\begin{array}{ll}
(r_{n-1-i},\ r_{i-1}) & \\
\quad\Big| & (a_{n-1-i},\ a_i) \\
(r_{n-2-i},\ r_i) & \\
\quad\Big| & (a_{n-2-i},\ a_{i+1}) \\
(r_i,\ r_{n-2-i}). &
\end{array}$$

Further, when this occurs, $a_{n-2-i} = a_{i+1} = M = (r_{n-2-i}g - r_i)/(k - 1)$.

$$a_{n-2-i} = a_{i+1} = M = (r_{n-2-i}g - r_i)/(k - 1).$$

The desired n-digit number x is given by (17).

Proof: Suppose there is a $2i + 3$-digit k-reverse multiple. The first piece of the above graph exists by assumption. We must show the existence of the second piece. Equations (4) at the $(i + 2)^{\text{nd}}$ step are

$$\left\{\begin{array}{lcl} ka_{i+1} + r_i & = & a_{n-2-i} + r_{i+1}g \\ ka_{n-2-i} + r_{n-3-i} & = & a_{i+1} + r_{n-2-i}g. \end{array}\right. \tag{21}$$

From (19) and (20) in the proof of Theorem 2, we have

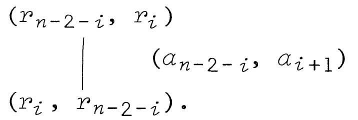
$$kM + r_i = M + r_{n-2-i}g.$$

Thus, one solution to (21) is

$$\begin{array}{ll} a_{n-2-i} = M; & a_{i+1} = M \\ r_{n-3-i} = r_i; & r_{i+1} = r_{n-2-i} \end{array}$$

and the result follows.

Now suppose for a given g and k there exists a graph containing



By hypothesis, (4) becomes

$$(22)\quad \begin{cases} ka_{i+1} + r_i = a_{n-2-i} + r_{n-2-i}g \\ ka_{n-2-i} + r_i = a_{i+1} + r_{n-2-i}g. \end{cases}$$

Subtracting one equation from the other gives $a_{i+1} = a_{n-2-i}$. From this, it follows that $(k - 1) | (r_{n-2-i}g - r_i)$ and $a_{n-2-i} = a_{i+1} = (r_{n-2-i}g - r_i)/(k - 1)$, so by Theorem 2 there exists an $n = 2i + 3$-digit k-reverse multiple. □

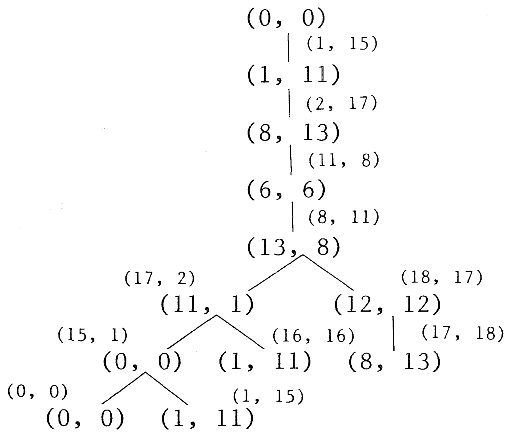
Corollary 2: For base g, suppose there are k-reverse multiples. Let n be an odd number. Then there exists an n-digit multiple if and only if the corresponding infinite tree contains a path of length $(n - 1)/2$ from the root to nodes designated by (u, v) followed by (v, u).

Proof: This is simply a restatement of Theorem 3. □

The importance of Corollaries 1 and 2 cannot be overstated. Suppose it is known that for a given g there are k-reverse multiples. Then we use the procedure suggested by (9) to create a pruned tree. By traversing the tree, replicating earlier sections when necessary, and stopping at those pairs which have the form given in the above corollaries, we are able to find all k-reverse multiples for a given n. This procedure is illustrated in the following example.

Example 2: $g = 19$, $k = 14$.

The tree in this case is:



By Corollaries 1 and 2, we can traverse the tree stopping at (6, 6), (12, 12), (11, 1), and (0, 0). The first two nodes give 14-reverse multiples with an even number of digits, while the third gives rise to those with an odd number of digits. The pair (0, 0) of course always accounts for multiples with both an even and an odd number of digits. So there are 6-, 10-, 11-, 12-, ...-digit 14-reverse multiples.

Those with the least number of digits are:

1 2 11 8 17 15
1 2 11 8 18 17 11 8 17 15
1 2 11 8 17 16 2 11 8 17 15

It would be difficult, using these, to see that

1 2 11 8 18 17 11 8 18 17 11 8 17 15

and

1 2 11 8 17 16 2 11 8 18 17 11 8 17 16 2 11 8 17 15

are also k-reverse multiples. Yet, using the tree, it is clear that they are.□

References

1. C. A. Grimm & D. W. Ballew. "Reversible Multiples." *J. Rec. Math.* *8* (1975-1976):89-91.
2. L. F. Klosinski & D. C. Smolarski. "On the Reversing of Digits." *Math. Mag.* *42* (1969):208-10.
3. Alan Sutcliffe. "Integers that Are Multiplied When Their Digits Are Reversed." *Math. Mag.* *39* (1966):282-87.

*****

Announcement

FIFTH INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS

Monday through Friday, July 20-24, 1992

Department of Mathematical and Computational Sciences
University of St. Andrews
St. Andrews KY16 9SS
Fife, Scotland

LOCAL COMMITTEE

Colin M. Campbell, Co-chairman
George M. Phillips, Co-chairman
Dorothy M.E. Foster
John H. McCabe
John J. O'Connor
Edmund F. Robertson

INTERNATIONAL COMMITTEE

A.F. Horadam (Australia), Co-chair
A.N. Philippou (Cyprus), Co-chair
S. Ando (Japan)
G.E. Bergum (U.S.A.)
P. Filipponi (Italy)
H. Harborth (Germany)
M. Johnson (U.S.A.)
P. Kiss (Hungary)
C.T. Long (U.S.A.)
B.S. Popov (Yugoslavia)
J. Turner (New Zealand)
M.E. Waddill (U.S.A.)

LOCAL INFORMATION

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

Dr. G.M. Phillips
Mathematical Institute
University of St. Andrews
North Haugh
ST. ANDREWS, Fife KY16 9SS
Scotland

The FIFTH INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS will take place at The University of St. Andrews, St. Andrews, Scotland from July 20 to July 24, 1992. This Conference is sponsored jointly by the Fibonacci Association and The University of St. Andrews. For more information contact:

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

ON THE EQUATIONS $U_n = U_q x^2$, WHERE q IS ODD, AND $V_n = V_q x^2$, WHERE q IS EVEN

Richard André-Jeannin
IUTGEA, Route de Romain, 54400, Longwy, France

(Submitted May 1990)

1. Introduction

Let $\{w_n\}$ be the sequence satisfying the second-order linear recurrence

(1.1) $w_n = pw_{n-1} + w_{n-2},\ n \in \mathbb{Z}$,

where w_0, w_1 are given integers and p is an *odd* positive integer.

Of particular interest are the generalized Fibonacci and Lucas sequences, $\{U_n(p)\}$ and $\{V_n(p)\}$, respectively, which are defined by (1.1) and the initial conditions

$$U_0(p) = 0,\ U_1(p) = 1,$$

and

$$V_0(p) = 2,\ V_1(p) = p.$$

Cohn [2] has proved the two theorems below, which we shall need later.

Theorem 1: The equation $V_n(p) = x^2$ has:

(1) if $p = 1$, two solutions $n = 1, 3$;
(2) if $p = 3$, one solution $n = 3$;
(3) if $p \neq 1$ is a perfect square, one solution $n = 1$;
(4) no solution otherwise.

The equation $V_n(p) = 2x^2$ has the solution $n = 0$, and for a finite number of values of p also $n = \pm 6$, but no other solutions.

Theorem 2: The equation $U_n(p) = x^2$ has:

(1) the solutions $n = 0$, and $n = \pm 1$;
(2) if p is a perfect square, the solution $n = 2$;
(3) if $p = 1$, the solution $n = 12$,
(4) no other solutions.

Recently, Goldman [3] has shown that if $L_n = L_{2^m}x^2$, where L_{2^m} is prime, then $n = \pm 2^m$. Adapting Cohn's and Goldman's method, we shall prove here the following theorems.

Theorem A; Let $q \geq 2$ be an *even* integer. Then $V_n(p) = V_q(p)x^2$, if and only if $n = \pm q$.

Theorem B: Let $q \geq 3$ be an *odd* integer. Then the equation $U_n(p) = U_q(p)x^2$ has the solutions

(1) $n = 0$, and $n = \pm q$,
(2) if $p = 1$ or 3, $q = 3$, and $n = 6$,

and no other solutions.

2. Preliminaries

The following formulas are well known (see [1], [4], [5]) or easily proved (recall that p is odd). For the sake of brevity, we shall write U_n and V_n, instead of $U_n(p)$ and $V_n(p)$.

(a) $U_{-n} = (-1)^{n+1}U_n$, and $V_{-n} = (-1)^n V_n$,
(b) $U_{2n} = U_n V_n$,
(c) if $d = \gcd(m, n)$, then $U_d = \gcd(U_m, U_n)$,
(d) if $q \geq 3$, then $U_q | U_n$ iff $q | m$,
(e) if $q \geq 2$, then $V_q | V_n$ iff $q | n$, and n/q is odd,
(f) if an *odd* prime number divides V_q and V_k, then $v_2(q) = v_2(k)$, where $v_2(s)$ is the 2-adic value of the integer s,
(g) $2 | V_n$ iff $3 | n$,
(h) if $k \equiv \pm 2 \pmod 6$, then $V_k \equiv 3 \pmod 4$,
(i) $\gcd(U_n, V_n) = 1$ or 2,
(j) if $\{w_n\}$ is a sequence satisfying (1.1), then, for all integers n, k,

$$w_{n+2k} + (-1)^k w_n = w_{n+k} V_k.$$

The following fundamental lemma (see [2], [3]) is recalled here with a new proof.

Lemma 1: If $\{w_n\}$ is a sequence satisfying (1.1), and k an even number, then, for all integers n, t

$$w_{n+2kt} \equiv (-1)^t w_n \pmod{V_k}.$$

Proof: By (j) we have, since k is even

$$w_{n+2k} \equiv -w_n \pmod{V_k},$$

and the proof follows by induction upon t. Q.E.D.

We shall also need the next result.

Lemma 2: If q and k are integers, with q odd and $k \equiv \pm 2 \pmod 6$, then

$$\gcd(U_q, V_k) = 1.$$

Proof: By (h) and (i), notice that $\gcd(U_k, V_k) = 1$, since V_k is odd. Let

$$d = \gcd(q, k) = \gcd(q, 2k).$$

By (b) and (c), we have

$$\gcd(U_q, V_k) | \gcd(U_q, U_{2k}) = U_d,$$

and $U_d | U_k$, since $d | k$. Thus,

$$\gcd(U_q, V_k) | U_k,$$

and so $\gcd(U_q, V_k) = 1$, since $\gcd(U_k, V_k) = 1$. Q.E.D.

3. Proofs of Theorems

Proof of Theorem A: Assume that $V_n = V_q x^2$, where $q \geq 2$ is even, and $n \neq \pm q$. Since $V_q | V_n$, it follows from (e) that

$$\begin{aligned} n &= (\pm 1 + 4j)q, \; j \neq 0 \\ &= \pm q + 2.3^r k, \end{aligned}$$

where $2jq = 3^r k$, and $k \equiv \pm 2 \pmod 6$. By Lemma 1 and (a),

$$V_n \equiv -V_{\pm q} = -V_q \pmod{V_k},$$

since q is even; hence,

$$-V_q \equiv V_q x^2 \pmod{V_k}.$$

Since $2jq = 3^r k$, then $v_2(k) > v_2(q)$, so by (f) and (g), $\gcd(V_q, V_k) = 1$ since V_k is odd; hence,

$$-1 \equiv x^2 \pmod{V_k},$$

which is impossible, since $V_k \equiv 3 \pmod 4$. Q.E.D.

Proof of Theorem B: Assume that $U_n = U_q x^2$, where $q \geq 3$ is odd, and $n \neq \pm q$. Since $U_q | U_n$, it follows from (d) that $q | n$.

Assume first that n is even, $n = 2jq$, and note that $j \geq 1$, since n even and negative would imply that $U_n < 0$. By (b), we get

$$U_{jq} V_{jq} = U_q x^2;$$

hence,

$$V_{jq} = y^2 \quad \text{or} \quad V_{jq} = 2y^2,$$

since $U_q | U_{jq}$ and $\gcd(U_{jq}, V_{jq}) = 1$ or 2.

If $j = 1$, then $V_q = y^2$ or $V_q = 2y^2$, which imply by Theorem 1 that $p = 1$ or 3, and $q = 3$, $n = 6$; it can be verified that

$$U_6(1) = U_3(1).2^2 \quad \text{and} \quad U_6(3) = U_3(3).6^2.$$

If $j \geq 2$, then $V_{jq} = y^2$ must be rejected by Theorem 1, since $jq > 3$ and $V_{jq} = 2y^2$ can be satisfied only if $jq = 6$, by Theorem 2, i.e., for $q = 3$, $j = 2$, and $n = 12$. However,

$$U_{12} = U_3 x^2$$

can be written, by (b),

$$U_3 V_3 V_6 = U_3 x^2 \quad \text{or} \quad V_3 V_6 = x^2.$$

Since $V_6 = 2y^2$, then $V_3 = 2z^2$, and this is impossible by Theorem 1.

Second, assume that $U_n = U_q x^2$, where n is odd,

$$\begin{aligned} n &= (\pm 1 + 4j)q,\ j \neq 0, \\ &= \pm q + 2.3^r k, \end{aligned}$$

where $k \equiv \pm 2 \pmod 6$. Then, by Lemma 1 and (a),

$$U_n \equiv -U_{\pm q} = -U_q \pmod{V_k},$$

since q is odd. Therefore, by Lemma 2 and hypothesis,

$$-1 \equiv x^2 \pmod{V_k},$$

which is impossible, as above. Q.E.D.

References

1. R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$." *Annals of Math.* *15* (1913):30-70.
2. J. H. E. Cohn. "Eight Diophantine Equations." *Proc. London Math. Soc.* *3* (1966):153-66.
3. M. Goldman. "Lucas Numbers of the Form px^2, Where p = 3, 7, 47 or 2207." *C. R. Math. Rep. Acad. Sci. Canada X.3* (1988):139-41.
4. A. F. Horadam. "Basic Properties of a Certain Generalized Sequence of Numbers." *Fibonacci Quarterly 3.2* (1965):161-76.
5. E. Lucas. "Théorie des fonctions numériques simplement périodiques." *Am. J. Math.* *I* (1878):184-240, 289-321.

*****

BOUNDS FOR THE CATALAN NUMBERS

A. V. Boyd
University of the Witwatersrand, Johannesburg 2050, South Africa

(Submitted May 1990)

1. Introduction

For the simple symmetric random walk on a two-dimensional lattice, it is well known (see, e.g., Feller [4], p. 361) that the probability of the origin begin revisited at the $2n^{\text{th}}$ step is

$$u_{2n} = 4^{-2n}\binom{2n}{n}^2, \quad (n = 0, 1, 2, \ldots);$$

and the Catalan number

$$c_n = \frac{1}{n+1}\binom{2n}{n}$$

(see Constantine [2], p. 61) is expressible as

$$c_n = \frac{2^{2n}}{n+1}\sqrt{u_{2n}}.$$

In a study of the transient behavior of the random walk Downham & Fotopoulos [3] have shown after much computation that

$$\frac{1}{\pi n}\left(1 - \frac{1}{4n} + \frac{1}{32n^2}\right) < u_{2n} < \frac{1}{\pi n}\left(1 - \frac{1}{4n} + \frac{1}{32n^2} + \frac{1}{32n^3}\right)$$

for $n = 1, 2, \ldots$, and this leads to inequalities for c_n which we strengthen by using standard analytical techniques. It is shown that, for $k \geq 3$ and every positive integer n,

$$1 + f(n, k) < \frac{1}{\pi n u_{2n}} < 1 + f(n, k) + \varepsilon_{k+1}$$

where

$$f(n, k) = \sum_{r=1}^{k} \frac{r!\binom{1/2}{r}^2}{n(n+1)\cdots(n+r-1)}$$

and

$$\varepsilon_{k+1} = \frac{(k-2)!}{4\pi(n+1)\cdot n(n+1)\cdots(n+k-1)}.$$

For any positive integer n,

$$\lim_{k\to\infty} \varepsilon_{k+1} = 0$$

and so both the bounds given by the inequalities tend to $1/\pi n u_{2n}$ as k increases; hence, u_{2n} can be approximated as accurately as desired.

Explicitly, for $k = 3$, the above results give

$$1 + \frac{1}{4n} + \frac{1}{32n(n+1)} + \frac{3}{128n(n+1)(n+2)} + \frac{1}{4\pi n(n+1)^2(n+2)}$$

$$> \frac{1}{\pi n u_{2n}} > 1 + \frac{1}{4n} + \frac{1}{32n(n+1)} + \frac{3}{128n(n+1)(n+2)}$$

and these are stronger than the inequalities of Downham & Fotopoulos.

2. Proof of the Inequalities

It is easily verified that

$$u_{2n} = \left\{\frac{\Gamma\left(n + \frac{1}{2}\right)}{n!\Gamma\left(\frac{1}{2}\right)}\right\}^2 = \frac{1}{\pi n} \Bigg/ \frac{\Gamma(n)\Gamma(n + 1)}{\Gamma^2\left(n + \frac{1}{2}\right)}$$

and then, by Gauss's theorem (see Whittaker & Watson [5], p. 281):

$$F(a,\ b;\ c;\ 1) = \frac{\Gamma(c)\Gamma(c - a - b)}{\Gamma(c - a)\Gamma(c - b)} \text{ for } \mathrm{Re}(c - a - b) > 0,$$

it follows that

$$u_{2n} = 1/\pi n F\left(-\frac{1}{2},\ -\frac{1}{2};\ n;\ 1\right) \text{ since } n \text{ is a positive integer}$$

$$= 1/\pi n\left\{1 + \sum_{r=1}^{\infty} v_r\right\}$$

where

$$v_r = \frac{\left\{-\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdot \cdots\cdot \left(r - \frac{3}{2}\right)\right\}^2}{r!n(n + 1)\ \cdots\ (n + r - 1)} = \frac{u_{2r-2}(r - 1)!}{4rn(n + 1)\ \cdots\ (n + r - 1)}.$$

Since $v_r > 0$ $(r \geq 1)$, it follows that $u_{2n} < 1/\pi n$ and so, if $r \geq 3$, then

$$v_r < \frac{(r - 2)!/\pi}{4rn(n + 1)\ \cdots\ (n + r - 1)} < \frac{(r - 3)!}{4\pi n(n + 1)\cdots\ (n + r - 1)};$$

hence, for $k \geq 4$,

$$\sum_{r=k}^{\infty} v_r < \frac{1}{4\pi}\sum_{r=k}^{\infty}\frac{(r - 3)!}{n(n + 1)\ \cdots\ (n + r - 1)}$$

$$= \frac{(k - 4)!}{4\pi n(n + 1)\ \cdots\ (n + k - 2)}\left\{\frac{k - 3}{n + k - 1} + \frac{(k - 3)(k - 2)}{(n + k - 1)(n + k)} + \cdots\right\}$$

$$= \frac{(k - 4)!}{4\pi n(n + 1)\ \cdots\ (n + k - 2)}\{F(k - 3,\ 1;\ n + k - 1;\ 1) - 1\}$$

$$= \frac{(k - 4)!}{4\pi n(n + 1)\ \cdots\ (n + k - 2)}\left\{\frac{\Gamma(n + k - 1)\Gamma(n + 1)}{\Gamma(n + 2)\Gamma(n + k - 2)} - 1\right\}$$

by Gauss's theorem, since $n > -1$. This simplifies to

$$\sum_{r=k}^{\infty} v_r < \frac{(k - 3)!}{(n + 1)\cdot 4\pi n(n + 1)\ \cdots\ (n + k - 2)}.$$

From

$$1 + \sum_{r=1}^{k} v_r < 1 + \sum_{r=1}^{\infty} v_r < 1 + \sum_{r=1}^{k} v_r + \frac{(k - 2)!}{(n + 1)\cdot 4\pi n(n + 1)\ \cdots\ (n + k - 1)}$$

it then follows that, for $k \geq 3$,

$$1 + f(n,\ k) < \frac{1}{\pi n u_{2n}} < 1 + f(n,\ k) + \varepsilon_{k+1}$$

where

$$0 < \varepsilon_{k+1} \leq \frac{(k - 2)!}{8\pi k!} = \frac{1}{8\pi(k - 1)k} \to 0 \text{ as } k \to \infty.$$

3. Numerical Comparisons

The following table shows some bounds given in the cases $k = 3$ and $k = 4$ as well as the bounds obtained from the inequalities of Downham & Fotopoulos. For problems related to the computation of the integer c_n when n is large, see Campbell [1].

n		u_{2n}		c_n	
		Lower Bound	Upper Bound	Lower Bound	Upper Bound
1	D & F	.24868	.25863	.9974	1.0171
	$k = 3$	.24942	.25073	.9989	1.0015
	$k = 4$	.249778	.250429	.99956	1.00086
		$u_2 = .25$		$c_1 = 1$	
2	D & F	.140 504	.141 126	1.99914	2.00356
	$k = 3$	.140 560	.140 698	1.99954	2.00052
	$k = 4$	.140 605	.140 660	1.99986	2.00025
		$u_4 = .140\ 625$		$c_2 = 2$	
10	D & F	.031 045 161	.031 046 156	16795.935	16796.204
	$k = 3$	.031 045 315	.031 045 481	16795.977	16796.022
	$k = 4$	.031 045 390	.031 045 416	16795.997	16796.004
		$u_{20} = .031\ 045\ 401$		$c_{10} = 16796$	
100	D & F	.003 175 151 061	.003 175 151 160	$c_{100} \approx .896\ 5199 \times 10^{57}$	
	$k = 3$	.003 175 151 085	.003 175 151 088		
	$k = 4$	.003 175 151 086 636	.003 175 151 086 683		
		$u_{200} = .003\ 175\ 151\ 086\ 657$			

References

1. D. M. Campbell. "The Computation of Catalan Numbers." *Math. Magazine* 57 (1984):195-208.
2. G. M. Constantine. *Combinatorial Theory and Statistical Design*. New York: Wiley, 1987.
3. D. Y. Downham & S. B. Fotopoulos. "The Transient Behaviour of the Simple Random Walk in the Plane." *J. Appl. Prob.* 25 (1988):58-69.
4. W. Feller. *An Introduction to Probability Theory and Its Applications*. Vol. I, 3rd ed. New York: Wiley, 1968.
5. E. T. Whittaker & G. N. Watson. *A Course of Modern Analysis*. Cambridge, Mass.: Cambridge University Press, 1927.

*****

PROJECTIVE MAPS OF LINEAR RECURRING SEQUENCES WITH MAXIMAL *p-adic* PERIODS

Huang Minqiang
Institute of Systems Science, Academia Sinica, PRC

Dai Zongduo
Graduate School of USTC, Academia Sinica, PRC

(Submitted June 1990)

1. Introduction

Let $\alpha = \sum_{i \geq 0} p_i \alpha^i$ be the *p-adic* expansion of an n^{th}-order linear recurring sequence α of rational (or *p-adic*) integers. In this paper the projective map $\phi_d\colon \alpha \to \alpha_{d-1}$ is shown to be injective modulo p^d for linear sequences having maximal modulo p^d periods.

Let R be the ring of rational (or *p-adic*) integers, p a prime number. For a polynomial $f(x) = \sum_{i=0}^{n} c_i x^i \in R[x]$ and a sequence α over R, define the operation

$$f(x)\alpha = \sum_{i=0}^{n} c_i \mathbf{L}^i \alpha$$

where $\mathbf{L}$ is the left-shift operator of sequences. α is said to be an n^{th}-order linear recurring sequence modulo p^d [or over $R_d = R/(p^d)$] generated by $f(x)$ if $f(x)$ is monic and $f(x)\alpha \equiv 0 \pmod{p^d}$. It is well known ([3], [4], [6], [7]) that the residue sequence $\alpha \bmod p^d$ is ultimately periodic with the period

$$(1) \qquad \text{per}(\alpha)_{p^d} \leq p^{d-1}(p^n - 1).$$

Definition: An n^{th}-order linear sequence α attaining the upper bound in (1) is said to be primitive over R_d. Furthermore, α is primitive over R if it is primitive over R_d for all $d \geq 2$.

The arithmetical properties of this special class of sequences have been studied in [1], [2], [3], and [6]. Write α in its *p-adic* form

$$\alpha = \alpha_0 + p\alpha_1 + p^2\alpha_2 + \cdots,$$

where the α_i's are p-ary sequences, and consider the d^{th} projective map

$$\phi_d\colon \alpha \to \alpha_{d-1}.$$

The purpose of this paper is to prove that ϕ_d is a modulo p^d injection on the set of $f(x)$-generated R_d-primitive sequences. More precisely, our main result is

Theorem 1: Suppose α and α' are n^{th}-order primitive sequences generated by $f(x)$ over R_d. Then $\alpha_{d-1} = \alpha'_{d-1}$ if and only if $\alpha \equiv \alpha' \pmod{p^d}$.

The proof is given in Sections 3 and 4.

2. Primitive Sequences and Polynomials over R_d

For a monic polynomial $f(x) \in R[x]$, define its modulo p^d period as follows

$$\text{per}(f(x))_{p^d} = \min\{t > 0 \mid x^t \equiv 1 \bmod (f(x), p^d)\}.$$

Let $T = \text{per}(f(x))_p$. By definition, there is an $h(x) \in R[x]$ so that

$$(2) \qquad x^T \equiv 1 + ph_1(x) \pmod{f(x)}.$$

For $i \geq 1$, let

$$(3) \qquad h_{i+1}(x) = \sum_{i \leq r \leq p} \binom{p}{r} p^{ri-i-1} h_i(x)^r .$$

It follows immediately that

$$(4) \qquad x^{p^{i-1}T} \equiv 1 + p^i h_i(x) \pmod{f(x)}, \quad 1 \leq i \leq d,$$

which implies

$$(5) \qquad \operatorname{per}(f(x))_{p^i} \,|\, p^{i-1}T \leq p^{i-1}(p^n - 1), \quad 1 \leq i \leq d.$$

Similar to the case of sequences, $f(x)$ is said to be primitive over R_d if

$$\operatorname{per}(f(x))_{p^d} = p^{d-1}(p^n - 1).$$

By (4) and (5), this is clearly equivalent to the fact that $f(x)$ is primitive over $GF(p)$ (i.e., $T = p^n - 1$) where $GF(p)$ denotes the finite field of order p, a prime, and

$$(6) \qquad h_i(x) \not\equiv 0 \bmod(f(x), p), \quad 1 \leq i < d.$$

By the inductive definition of $h_i(x)$, when $i \geq 2$ we have

$$(7) \qquad h_i(x) \equiv \begin{cases} h_1(x) \bmod(p, f(x)), & \text{if } p \geq 3, \\ h_2(x) \equiv h_1(x) + h_1(x)^2 \bmod(2, f(x)), & \text{if } p = 2. \end{cases}$$

Therefore, (6) is equivalent to

$$(8) \qquad h_1(x) \not\equiv \begin{cases} 0, \quad \bmod(p, f(x)), & \text{if } p \geq 3, \text{ or } p = 2 \text{ and } d = 2, \\ 0, 1 \quad \bmod(2, f(x)), & \text{if } p = 2 \text{ and } d \geq 3. \end{cases}$$

An explicit criterion for $f(x)$ to be primitive over R_d is given in [2]. Ward had shown in [6] that an $f(x)$-generated linear sequence α is primitive over R_d if and only if $\alpha \not\equiv 0 \pmod{p}$ and $f(x)$ is primitive over R_d. Now assume this is the case and write

$$\alpha = \sum_{i \geq 0} \alpha_i p^i .$$

For $1 \leq i < d$, notice that $\operatorname{per}(\alpha)_{p^i} \,|\operatorname{per}(f(x))_{p^i} = p^{i-1}T$, we have

$$(9) \qquad (x^{p^{i-1}T} - 1)\alpha = (x^{p^{i-1}T} - 1)\sum_{k \geq i} \alpha_k p^k \equiv p^i(x^{p^{i-1}T} - 1)\alpha_i \pmod{p^{i+1}}.$$

On the other hand, applying (4) to α gives

$$(10) \qquad (x^{p^{i-1}T} - 1)\alpha \equiv p^i h_i(x)\alpha \pmod{p^{i+1}}.$$

From (9) and (10), we obtain the relation over $GF(p)$

$$(11) \qquad (x^{p^{i-1}T} - 1)\alpha_i = h_i(x)\alpha_0 = \begin{cases} h_1(x)\alpha_0, & \text{if } p \geq 3, \text{ or } p = 2 \text{ and } i = 1, \\ h_2(x)\alpha_0, & \text{if } p = 2 \text{ and } i \geq 2. \end{cases}$$

In what follows, discussions of p-ary sequences are over $GF(p)$.

For any $g(x) \in GF(p)[x]$, denote by $G(g(x))$ the set of sequences over $GF(p)$ generated by $g(x)$. Let $m_0 = \alpha_0$,

$$(12) \qquad m_i = (x^{p^{i-1}T} - 1)\alpha_i = h_i(x)m_0, \quad 1 \leq i < d.$$

Clearly, m_i, $i = 0, 1, \ldots,$ are primitive sequences in $G(f_0(x))$. They are the key factors in our approach to proving the main theorem. The following Lemma, which will play a technical role in Sections 3 and 4, can be derived from (11) and the theory of primitive sequence products ([4, Ch. 8], [5]).

Lemma 1: (i) The product of two primitive sequences over $GF(p)$ is not zero.

(ii) Let $\lambda = \sum_{i \geq 0} p^i \lambda_i$ be any $f(x)$-generated sequence over R_d. If there is a p-ary primitive sequence $m \in G(f_0(x))$ such that

$$m\lambda_{d-1} \equiv m\lambda_{d-2} \mod G(x^T - 1),$$

then $\lambda \equiv 0 \pmod{p^{d-1}}$.

3. Proof of Theorem 1 for $p \geq 3$

Let $\rho = \sum_{i \geq 0} \rho_i p^i$ be the *p-adic* form of $\alpha' - \alpha$. We want to show that

$\alpha'_{d-1} = \alpha_{d-1}$ implies $\rho \equiv 0 \pmod{p^{d-1}}$.

Assume on the contrary that $\rho = p^e \beta$, with $0 \leq e < d - 1$ and

$$\beta = \sum_{i \geq 0} \beta_i p^i \not\equiv 0 \pmod{p}.$$

Obviously, β is generated by $f(x)$ over R_{d-e}. By (11),

$$m = (x^{p^{d-e-2}} - 1)\beta_{d-e-1}$$

is a primitive sequence generated by $f(x)$ over $GF(p)$. On the other hand, let

$$\alpha = (\alpha(t))_{t \geq 0}, \quad \alpha' = (\alpha'(t))_{t \geq 0}, \quad \beta_{d-e-1} = (\beta(t))_{t \geq 0}$$

and define the "borrow" sequence $\delta_{d-1} = (\delta(t))_{t \geq 0}$ by

$$\delta(t) = \begin{cases} 0, & \text{if } \alpha'(t) \bmod p^{d-1} \geq \alpha(t) \bmod p^{d-1}, \\ 1, & \text{otherwise.} \end{cases}$$

Then

$$\beta(t) = (\alpha'_{d-1}(t) - \alpha_{d-1}(t) - \delta(t)) \bmod p = (-\delta(t)) \bmod p = 0 \text{ or } p - 1$$

for all t. Therefore, the $GF(p)$-primitive sequence

$$m = (x^{p^{d-e-2}} - 1)\beta_{d-e-1}$$

consists of at most three elements: 0, 1, and $p - 1$. When $p \geq 5$, this is impossible because a primitive sequence contains all p elements in $GF(x)$. Now, assume $p = 3$, and write $m = (m(t))_{t \geq 0}$. From the equation

$$\beta(t + p^{d-e-2}T) - \beta(t) = m(t)$$

and the fact that $\beta(t) = 0$ or 2 for all t, we have $\beta(t) = 2$ when $m(t) = 1$, and $\beta(t) = 0$ when $m(t) = 2$. Hence,

$$m(t)\ (t) = m(t)(m(t) + 1) \text{ for all } t \geq 0,$$

or equivalently,

(13) $\quad m\beta_{d-e-1} = m(m + 1).$

Applying the operator $x^{p^{d-e-2}} - 1$ to both sides of (13) gives rise to $m^2 = 0$, which contradicts (i) of Lemma 1.

So Theorem 1 has been proved for $p \geq 3$.

4. Proof of Theorem 1 for $p = 2$

When $p = 2$, our main theorem is obviously equivalent.

Theorem 2: Let α and α' be as in Theorem 1. Then for $d \geq 2$,

$$\alpha_{d-1} + \alpha'_{d-1} \in G(f_0(x)) \text{ if and only if } \alpha \equiv \alpha' \pmod{2^{d-1}}.$$

The "if" part is clear. To prove the other direction, we need some preparations. Suppose $\rho = \alpha' - \alpha$ and $\omega = \alpha + \alpha'$, with 2-*adic* expansions

$$\rho = \sum_{i \geq 0} 2^i \rho_i \quad \text{and} \quad \omega = \sum_{i \geq 0} 2^i \omega_i.$$

Let $\theta_i = \alpha_i + \alpha_i'$, then over $GF(2)$ we have

(14) $\omega_i = \theta_i + \gamma_i$,

(15) $\rho_i = \theta_i + \delta_i$

where γ_i is the "carry" from α mod 2^i and α' mod 2^i, and δ_i is the "borrow" defined by α mod 2^i and α' mod 2^i. Denote by $\overline{\theta}_i$ the binary complement of θ_i, it is easily seen that

(16) $\delta_i = \theta_{i-1}\alpha_{i-1} + \overline{\theta}_{i-1}\delta_{i-1}$,

(17) $\gamma_i = \overline{\theta}_{i-1}\alpha_{i-1} + \theta_{i-1}\gamma_{i-1}$.

Lemma 2: Suppose α and α' are $f(x)$-generated primitive sequences over R_d. If $\theta_{d-1} - G(x^T + 1)$, then

$$\theta_{d-2}m_{d-2} = \varepsilon m_{d-2}$$

where $\varepsilon = 0$ or 1. Furthermore, we have $\rho \equiv 0 \pmod{2^{d-1}}$ or $\omega \equiv 0 \pmod{2^{d-1}}$, respectively, according to $\varepsilon = 0$ or 1.

Proof: The fact that $(x^T + 1)\theta_{d-1} = 0$ implies $m_i = m_i'$ and $\theta_i \in G(x^{2^{i-1}T} + 1)$ for all $i \leq d - 1$.

If $d = 2$, we have $m_0 = m_0'$, and the conclusion holds.

Now assume $d \geq 3$. Notice that $\rho \equiv 0 \pmod 2$, and

$$\rho' = \rho/2 = \sum_{i \geq 0} 2^i \rho_{i+1}$$

is generated by $f(x)$ over R_{d-1}. From (11) it follows that

$$(x^{2^{d-3}T} + 1)\rho_{d-1} = h_{d-2}(x)\rho_1 \in G(f_0(x)).$$

On the other hand, by the observation that per$(\delta_{-2}) | 2^{d-3}T$ and

(18) $\rho_{d-1} = \theta_{d-1} + \theta_{d-2}\alpha_{d-2} + \overline{\theta}_{d-2}\delta_{d-2}$,

we have

(19) $(x^{2^{d-3}T} + 1)\rho_{d-1} = \theta_{d-2}(x^{2^{d-3}T} + 1)\alpha_{d-2} = \theta_{d-2}m_{d-2}$.

Therefore, $\theta_{d-2}m_{d-2} = \varepsilon m_{d-2}$ with $\varepsilon = 0$ or 1.

If $\varepsilon = 0$, i.e., $\theta_{d-2}m_{d-2} = 0$, then $\overline{\theta}_{d-2}m_{d-2} = m_{d-2}$. From (18) and (15), we can derive

$$m_{d-2}\rho_{d-1} = m_{d-2}\theta_{d-1} + m_{d-2}\delta_{d-2} \equiv m_{d-2}\rho_{d-1} \bmod G(x^T + 1)$$

which leads to $\rho \equiv 0 \pmod{2^{d-1}}$ by Lemma 1.

The case of $\varepsilon = 1$ can be shown in a similar way. The proof is thus completed.

Corollary: If $(x^T + 1)\theta_2 = 0$, then $\alpha \equiv \alpha' \pmod 4$.

Proof: Assume, on the contrary, that $\varepsilon = 1$ and $\theta_1 m_1 = m_1$. Since $m_0 = m_0'$ and $\theta_1 \in G(f_0(x))$, we have $\theta_1 = m_1$.

On the other hand, the fact that $\omega \equiv 0 \pmod 4$ and $\omega_1 = \theta_1 + m_0$ implies $\theta_1 = m_0$. Therefore

$$m_1 = \theta_1 = m_0$$

which is impossible by (12) and (8).

Now we are in a position to give an inductive proof of the remaining part of Theorem 2:

$$\theta_{d-1} \in G(f_0(x)) \text{ implies } \alpha \equiv \alpha' \pmod{2^{d-1}}.$$

The conclusions for $d = 2$ and 3 are proved above.

Suppose $d \geq 4$ and the theorem holds for $d - 1$. If it fails for d, we would have $\theta_{d-2}m_{d-2} = m_{d-2}$ and $\omega \equiv 0 \pmod{2^{d-1}}$. Consequently,

$$\omega_{d-2} = \theta_{d-2} + \gamma_{d-2} = 0,$$

$$\omega_{d-1} = \theta_{d-1} + \overline{\theta}_{d-2}\alpha_{d-2} + \theta_{d-2} \in G(f_0(x)),$$

$$m_{d-2}\omega_{d-1} = m_{d-2}\theta_{d-1} + m_{d-2} = m_{d-2}(\theta_{d-1} + m_{d-2}). \tag{20}$$

Since m_{d-2}, ω_{d-1}, and $\theta_{d-1} \in G(f_0(x))$, by Lemma 1(i), equation (20) leads to

$$\theta_{d-1} + m_{d-2} = \omega_{d-1} = \theta_{d-1} + \overline{\theta}_{d-2}\alpha_{d-2} + \theta_{d-2},$$

and hence $m_{d-2} = \theta_{d-2}\alpha_{d-2} + \theta_{d-2}$. Multiplying both sides by θ_{d-2} gives

$$m_{d-2} = \theta_{d-2}m_{d-2} = \theta_{d-2}.$$

Now we have reduced the case to $d - 1$. By the inductive assumption, we have $\rho \equiv 0 \pmod{2^{d-2}}$, and hence

$$\alpha = (\omega - \rho)/2 \equiv 0 \pmod{2^{d-3}}$$

which contradicts the fact that α is primitive over R_d and $d \geq 4$.

The theorem is thus proved.

References

1. Zongduo Dai & Minqiang Huang. "A Criterion for Primitiveness of Polynomials over $\mathbb{Z}$ mod 2^d." *Chinese Science Bulletin* (Chinese ed.) *35* (1990):1129-31 (English ed. will appear in 1990).
2. Minqiang Huang. "Maximal Period Polynomials over $\mathbb{Z}$ mod p^d." Preprint.
3. M. Hall. "An Isomorphism between Linear Recurring Sequences and Algebraic Rings." *Trans. Amer. Math. Soc. 44* (1938):196-218.
4. R. Lidl & H. Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and Its Applications, Vol. 20. New York: Addison-Wesley, 1983 (now distributed by Cambridge University Press).
5. W. H. Mills & N. Zierler. "Products of Linear Recurring Sequences." *J. Algebra 27* (1973):147-57.
6. M. Ward. "The Arithmetical Theory of Linear Recurring Series." *Trans. Amer. Math. Soc. 35* (1933):600-28.
7. A. Vince. "Period of a Linear Recurrence." *Acta Arith. 39* (1981):303-11.

*****

CONTINUED FRACTIONS AND PYTHAGOREAN TRIPLES

William C. Waterhouse[*]
The Pennsylvania State University, University Park, PA 16802

(Submitted June 1990)

Introduction

A Pythagorean triple is an ordered triple of positive integers (x, y, z) with $x^2 + y^2 = z^2$. It is called primitive if x and y have no common factors. In recent work, A. G. Schaake & J. C. Turner have discovered an unexpected representation for the primitive Pythagorean triples: they are precisely the triples of the form

$$x = (Q - R)/N, \quad y = (P + S)/N, \quad z = (Q + R)/N$$

where P/Q is the value of a continued fraction of the form

$$[0; u_1, u_2, \ldots, u_i, v, 1, j, (v + 1), u_i, \ldots, u_2, u_1],$$

R/S is the previous convergent of that continued fraction, and N depends on the entries but is either $(j + 1)$ or $2(j + 1)$. This work was drawn to my attention by the review [4]; Professor Turner was then kind enough to send me relevant parts of their privately published book and research report [2], [3]. The representation is derived there as part of a more general investigation, with the equation rewritten in the form $ps = qr - 1$. In this paper, I shall isolate the material bearing directly on Pythagorean triples, proving a slightly simpler variant of their result and showing how closely it is related to the usual parametrization of Pythagorean triples. The only unfamiliar step will be an identity on continued fractions that we can easily prove from scratch.

1. An Identity on Continued Fractions

We briefly recall some of the basic information about continued fractions (see, e.g., [1], Ch. IV). For positive integers $u_1, \ldots, u_m$, the continued fraction $[0; u_1, \ldots, u_m]$ is a number between 0 and 1 defined inductively by $[0; u] = 1/u$ and

$$[0; u_1, \ldots, u_m] = 1/\{u_1 + [0; u_2, \ldots, u_m]\}.$$

If we define two sequences p_j and q_j by the initial values

$$p_0 = 0, \; q_0 = 1, \; p_1 = 1, \; q_1 = u_1$$

and the recursion relations

$$p_{j+1} = u_{j+1}p_j + p_{j-1}, \; q_{j+1} = u_{j+1}q_j + q_{j-1},$$

then p_j and q_j are relatively prime and

$$[0; u_1, \ldots, u_m] = p_m/q_m.$$

Every fraction between 0 and 1 occurs as some $[0; u_1, \ldots, u_m]$, and the expression is unique so long as we require the last entry u_m to be bigger than 1.

Lemma: Let $[0, \sim\sim\sim] = A/B$ be a continued fraction, and let $[0; \sim\sim\sim, g] = C/D$. For any u, then

[*] This work was supported in part by the U.S. National Science Foundation Grant no. DMS8701690.

$$[0;\ u,\ \sim\sim\sim,\ g] = D/(uD + C)$$

and

$$[0;\ u,\ \sim\sim\sim,\ g,\ u] = (uD + B)/(u^2D + uB + uC + A).$$

Proof: Clearly,

$$D/(uD + C) = 1/\{u + [0;\ \sim\sim\sim,\ g]\}.$$

Similarly,

$$B/(uB + A) = [0;\ u,\ \sim\sim\sim].$$

Then the recursion relations show us that the numerator of $[0;\ u,\ \sim\sim\sim,\ g,\ u]$ is $uD + B$ and the denominator is $u(UD + C) + (uB + A)$. □

Theorem 1 (Schaake & Turner): Let $[0;\ u_n,\ u_{n-1},\ \ldots,\ u_1,\ w]$ be a continued fraction with the u_i and w positive integers, $w > 1$, and $n \geq 0$. Let its value be p/q. Then the continued fraction

$$[0;\ u_n,\ \ldots,\ u_2,\ u_1,\ w - 1,\ w + 1,\ u_1,\ u_2,\ \ldots,\ u_n]$$

has numerator $pq + (-1)^n$ and denominator q^2, and the previous convergent

$$[0;\ u_n,\ \ldots,\ u_2,\ u_1,\ w - 1,\ w + 1,\ u_1,\ u_2,\ \ldots,\ u_{n-1}]$$

has numerator p^2 and denominator $pq - (-1)^n$.

Proof: We prove this by induction on n (which is why the entries in the continued fraction have been numbered backward). The case $n = 0$ is straightforward: we have $[0;\ w] = 1/w$ and $[0;\ w - 1] = 1/(w - 1)$, while $[0;\ w - 1,\ w + 1]$ has numerator $(w + 1)$ and denominator $(w + 1)(w - 1) + 1 = w^2$.

Assuming the result for n, let us consider the fractions for $n + 1$. If p/q is the value for n, the lemma shows that

$$[0;\ u_{n+1},\ u_n,\ \ldots,\ u_2,\ u_1,\ w] = q/\{qu_{n+1} + p\}.$$

In short, the new numerator p' is q, and the new denominator q' is $qu_{n+1} + p$. Applied to the longer fractions, the lemma now shows that

$$[0;\ u_{n+1},\ \ldots,\ u_2,\ u_1,\ w - 1,\ w + 1,\ u_1,\ u_2,\ \ldots,\ u_n]$$
$$= q^2/\{u_{n+1}q^2 + pq + (-1)^n\} = (p')^2/\{p'q' - (-1)^{n+1}\},$$

while

$$[0;\ u_{n+1},\ \ldots,\ u_2,\ u_1,\ w - 1,\ w + 1,\ u_1,\ u_2,\ \ldots,\ u_{n+1}]$$

has numerator equal to

$$u_{n+1}(q^2) + \{pq - (-1)^n\} = p'q' + (-1)^{n+1}$$

and denominator equal to

$$u_{n+1}\{q^2u_{n+1} + pq + (-1)^n\} + \{(pq - (-1)\ )u_{n+1} + p^2\} = (q')^2. \quad \square$$

Example: Suppose we start with $[0;\ 3,\ 5,\ 2]$. Computing the sequence of values $(p_j,\ q_j)$ by the recursion, we get (0, 1), (1, 3), (5, 16), and (11, 35). For $[0;\ 3,\ 5,\ 1,\ 3,\ 5,\ 3]$, the sequence is (0, 1), (1, 3), (5, 16), (6, 19), (23, 73), (121, 384), and (386, 1225). We see, e.g., that $386 = (11)(35) + (-1)^2$ and $1225 = (35)^2$.

Remark 1: I have stated the theorem for positive integers, but the proof shows that it is a purely formal identity.

Remark 2: In Schaake & Turner, Theorem 1 occurs as a special case (the formal result of setting $j = 0$) in a more general statement ([3], pp. 92-96); in our notation, it says that the continued fraction

$$[0;\ u_n,\ \ldots,\ u_2,\ u_1,\ (w - 1),\ 1,\ j,\ w,\ u_1,\ u_2,\ \ldots,\ u_n]$$

has numerator $(j + 1)pq + (-1)^n$ and denominator $(j + 1)q^2$, while the previous convergent has numerator $(j + 1)p^2$ and denominator $(j + 1)pq - (-1)^n$. The induction argument given here will also establish that statement. Their proof is slightly different, and in [2] the result is viewed primarily as a computational simplification. From my present viewpoint, the more general expression simply winds up introducing a common factor of $(j + 1)$ in the Pythagorean triples, and so it is not needed.

2. Relation to Pythagorean Triples

Now we recall the standard analysis of Pythagorean triples, as in ([1], pp. 153-55). If (x, y, z) is a Pythagorean triple, then so is (mx, my, mz) for any positive integer m. Every Pythagorean triple arises in this way from a uniquely determined primitive triple. Setting $\bar{x} = x/z$ and $\bar{y} = y/z$, we thus get a correspondence between the primitive triples and the points with rational coordinates on the first quadrant of the unit circle. What we might call the "standard" rational parameter for the circle is

$$t = y/(x + z) = \bar{y}/(\bar{x} + 1);$$

the values $\bar{x}$ and $\bar{y}$ (with squares adding to 1) can be recovered as

$$\bar{x} = (1 - t^2)/(1 + t^2) \quad \text{and} \quad \bar{y} = 2t/(1 + t^2).$$

We get positive values for $\bar{x}$ and $\bar{y}$ exactly when $0 < t < 1$. If $t = p/q$ in lowest terms, we have

$$\bar{x} = (p^2 - q^2)/(p^2 + q^2) \quad \text{and} \quad \bar{y} = 2pq/(q^2 + p^2).$$

The obvious Pythagorean triple corresponding to this value of t then is

$$x = p^2 - q^2, \quad y = 2pq, \quad z = p^2 + q^2.$$

This triple is in fact the primitive one if either p or q is even. If both of them are odd, then the primitive triple for parameter $t = p/q$ is

$$x = (p^2 - q^2)/2, \quad y = pq, \quad z = (p^2 + q^2)/2.$$

The classification is sometimes stated a bit differently, so I should add one further remark. Interchanging x and y in a Pythagorean triple gives another Pythagorean triple. On the rational parameter, this corresponds to the operation sending t to $(1 - t)/(1 + t)$. If $t = p/q$ in lowest terms, the new value is $(q - p)/(q + p)$. This new numerator and denominator have at most a common factor of 2. If either p or q is even, then the fraction is in lowest terms and has odd numerator and denominator. If both p and q are odd, then either $p - q$ or $p + q$ (but not both) is divisible by 4; hence, when we cancel the common factor of 2, we get a fraction where either the numerator or the denominator is even. Thus, the two possible types of t are interchanged by the interchange of x and y. Specifically, the p/q with either p or q even give the primitive triples in which y is even, while the p/q with both p and q odd give the primitive triples where x is even.

We can now prove the main result, showing how the continued fraction is related to the rational parameter.

Theorem 2:

(a) For $n \geq 0$ and any positive integers $w, u_1, u_2, \ldots, u_n$ with $w > 1$, let P/Q be the value of the continued fraction

$$[0; u_n, \ldots, u_2, u_1, w - 1, w + 1, u_1, u_2, \ldots, u_n],$$

and let R/S be the value of its previous convergent

$$[0; u_n, \ldots, u_2, u_1, w - 1, w + 1, u_1, u_2, \ldots, u_{n-1}].$$

Set $N = 2$ if both Q and R are odd, and set $N = 1$ otherwise. Define

$$X = (Q - R)/N, \quad Y = (P + S)/N, \quad Z = (Q + R)/N.$$

Then (X, Y, Z) is a primitive Pythagorean triple.

(b) Every primitive Pythagorean triple arises in this way from exactly one sequence $w, u_1, u_2, \ldots, u_n$.

(c) The rational parameter for the triple is precisely $[0; u_n, u_{n-1}, \ldots, u_1, w]$.

Proof: Set $t = p/q = [0; u_n, \ldots, u_2, u_1, w]$. By Theorem 1, we know that

$$P = pq + (-1)^n, \quad Q = q^2, \quad R = p^2, \quad S = pq - (-1)^n.$$

Thus, $Q - R = q^2 - p^2$ and $Q + R = q^2 + p^2$ and $P + S = 2pq$. The standard theory shows then that (X, Y, Z) is the primitive triple corresponding to parameter t. As each t arises from a unique sequence, the same is true for the triples. □

References

1. H. Davenport. *The Higher Arithmetic*. New York: Dover, 1983 (a reprint of the original edition [London: Hutchison], 1952).
2. A. G. Schaake & J. C. Turner. *A New Chapter for Pythagorean Triples*. Privately published by the authors, Hamilton, New Zealand, 1989.
3. A. G. Schaake & J. C. Turner. "New Methods for Solving Quadratic Diophantine Equations." Research Report 192, University of Waikato, Hamilton, New Zealand, 1989.
4. Review of *A New Chapter for Pythagorean Triples* by A. G. Schaake & J. C. Turner. *Fibonacci Quarterly 28.2* (1990):140 and 155.

*****

SCHUR FUNCTIONS AND FIBONACCI IDENTITIES

John B. Kelly
Arizona State University, Tempe, AZ 85287-1804
(Submitted June 1990)

1. Introduction

In this article we use the elementary theory of symmetric functions and the theory of characters of representations of the symmetric group to derive identities involving generalized Fibonacci and Lucas numbers. Not all the identities obtained are new; what is possibly of greater interest is the approach, which may lead to further results. We have included some preparatory material on partitions, Schur functions and characters in Sections 2, 3, and 5. Proofs of the statements made there may be found, among many other places, in [1] and [2]. Character calculations similar to those carried out in this paper are found in [3].

Let a and b be any two unequal complex numbers. Define the Lucasian pairs $\{U_n\}$ and $\{V_n\}$ by

$$U_n = \frac{a^n - b^n}{a - b}, \quad V_n = a^n + b^n; \quad n = 0, 1, 2, \ldots .$$

Then U_n and V_n satisfy the recurrences

$$U_{n+2} = PU_{n+1} - QU_n, \quad V_{n+2} = PV_{n+1} - QV_n,$$

where $P = a + b$, $Q = ab$, $P^2 - 4Q \neq 0$. In case $P = 1$, $Q = -1$, put $U_n = F_n$, $V_n = L_n$. Then F_n and L_n are the Fibonacci and Lucas numbers, respectively.

Let $\rho_1 \geq \rho_2 \geq \cdots \geq \rho_k$ be positive integers. One of our basic identities has the form

$$(1.1) \qquad V_{\rho_1} V_{\rho_2} \ldots V_{\rho_k} = \sum_{j=0}^{\left[\frac{n}{2}\right]} A_{\rho_1, \rho_2, \ldots, \rho_k; j} U_{n-2j+1}$$

where the A's are simply expressible in terms of Q and certain characters of the symmetric group. An identity inverse to (1.1) is also obtained. For certain choices of $\{\rho_1, \rho_2, \ldots, \rho_k\}$, the relevant characters can be fairly readily computed. In this way we obtain, for instance, the identity

$$(1.2) \qquad \sum_{j=0}^{\left[\frac{m}{2}\right]} \left[\binom{m - 2^q + 1}{j} - \binom{m - 2^q + 1}{j - 2^q}\right] Q^j U_{m-2j+1} = P^{m-2^q+1} U_{2^q}.$$

In Section 7 we use a different approach to derive identities involving Lucas numbers and certain generalized binomial coefficients.

2. Partitions and Tableaux

A partition is a finite sequence of nonnegative integers:

$$\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_t)$$

in nonincreasing order. A part of λ is a nonzero member of $\{\lambda_1, \lambda_2, \ldots, \lambda_t\}$. The number of parts is the length, $\ell(\lambda)$, of λ. The sum $|\lambda| = \lambda_1, \lambda_2, \ldots, \lambda_k$, where $k = \ell(\lambda)$ is the weight of λ. λ is said to be a partition of $|\lambda|$. Occasionally we use an "exponential" notation for λ:

$$\lambda = 1^{\beta_1} 2^{\beta_2} \ldots m^{\beta_m}.$$

Here, β_i is the number of times i occurs in the sequence $(\lambda_1, \lambda_2, \ldots, \lambda_k)$.

$[\lambda]$, the diagram of λ, is the set of all points (i, j) in Z^2 such that $1 \le j \le \lambda_i$. Thus, the diagram of (3, 3, 2, 1) is

• • •
• • •
• •
•

Sometimes it is convenient to use squares rather than dots. Let λ and μ be partitions with $|\tau| = |\mu|$. A semi-standard tableau of shape λ and content μ is an arrangement of μ_1 1's, μ_2 2's, μ_3 3's, etc., in the squares of the diagram of λ so that the rows are nondecreasing and the columns are strictly increasing. For example, the semi-standard tableaux of shape (4, 2) and content (3, 2, 1) are

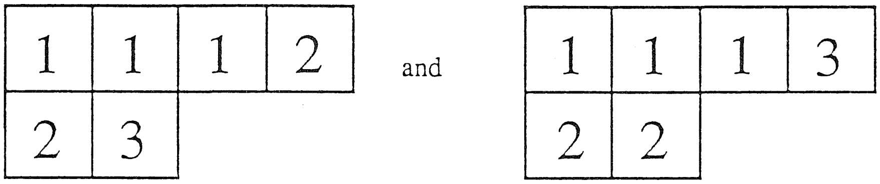


Figure 1

Partitions may be ordered lexicographically. That is,

$\lambda > \mu$ if $\lambda_1 > \mu_1$ or if $\lambda_1 = \mu_1$ and $\lambda_2 > \mu_2$

or if $\lambda_1 = \mu_1$, $\lambda_2 = \mu_2$, and $\lambda_3 > \mu_3$, etc.

Semi-standard tableaux of shape λ and content μ can exist only if $\lambda \ge \mu$. (This condition is not sufficient.)

3. Schur Functions

We shall be working in the ring $Z[x_1, x_2, \ldots, x_n]$ of polynomials in n independent variables with integer coefficients. Such a polynomial is symmetric if it is invariant under all permutations of the variables. For each n-tuple $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ in N^n, we denote by x^α the monomial

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x^{\alpha_n}.$$

If λ is a partition of length $\le n$, the polynomial

$$m_\lambda(x_1, x_2, \ldots, x_n) = \sum x^\alpha,$$

where the summation is over all permutations α of $\{\lambda_1, \lambda_2, \ldots, \lambda_i\}$ is symmetric. The power sums

$$p_r = \sum_{i=1}^{n} x_i^r$$

are symmetric, as are the products

$$p_\rho = p_{\rho_1} p_{\rho_2} \ldots p_{\rho_k} \qquad (\rho = (\rho_1, \rho_2, \ldots, \rho_k))$$

With every partition λ we can associate another type of symmetric function, called a Schur function, or S-function. Let λ be a partition $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ and put $\delta = (n - 1, n - 2, \ldots, 1, 0)$. Define

$$a_{\lambda+\delta} = \det(x_i^{\lambda_j+n-j}), \ 1 \le i \le n, \ 1 \le j \le n.$$

Then

$$a_\delta = \det(x_i^{m-j}) = \prod_{1 \le i < j \le m} (x_i - x_j)$$

is the Vandermonde determinant. Clearly, a_δ divides $a_{\lambda+\delta}$. The quotient

$$s_\lambda = s_\lambda(x_1, x_2, \ldots, x_m) = \frac{a_{\lambda+\delta}}{a_\delta}$$

is a symmetric homogeneous polynomial of degree $|\lambda|$ which is called a Schur function.

The sets $M_m = \{m_\lambda | \ell(\lambda) \le m\}$ and $S = \{s_\lambda | \ell(\lambda) \le m\}$ are Z-bases for Λ_m, the set of symmetric polynomials in m variables with coefficients in Z. Thus, for example, we may express the polynomials s_λ as integral linear combinations of the polynomials m_μ. We have

$$(3.1) \qquad s_\lambda = \sum_{|\mu| = |\lambda|} K_{\lambda,\mu} m_\mu.$$

It is possible to show that the Kostka number $K_{\lambda,\mu}$ is the number of semi-standard tableaux of shape λ and content μ. Therefore, $K_{\lambda,\mu}$ is a nonnegative integer that vanishes if $\lambda < \mu$.

To express the polynomials p_ρ as integral linear combinations of Schur functions, we require the characters of Σ_m, the symmetric group on m letters. We have

$$(3.2) \qquad p_\rho = \sum_{|\lambda| = |\rho|} \chi_\rho^\lambda s_\lambda,$$

where χ_ρ^λ is the character of the irreducible representation of Σ_m determined by λ evaluated at the conjugate class of Σ_m consisting of permutations with cycle-partition ρ.

Inverse to (3.2) is the relation

$$(3.3) \qquad s_\lambda = \frac{1}{m!} \sum_{|\rho| = |\lambda|} c_\rho \chi_\rho^\lambda p_\rho$$

where c_ρ is the number of permutations with cycle-partition ρ; i.e.,

$$c_\rho = \frac{m!}{1^{\gamma_1} 2^{\gamma_2} \ldots m^{\gamma_m} (\gamma_1)!(\gamma_2)! \ldots (\gamma_m)!}$$

with $\rho = 1^{\gamma_1} 2^{\gamma_2} \ldots m^{\gamma_m}$ and $|\rho| = m$.

4. Basic Identities

If there are only two independent variables x_1 and x_2, and if $\ell(\mu) \ge 3$, then $m_\mu = 0$. In this case (3.1) may be put in the form

$$(4.1) \qquad s_\lambda(x_1, x_2) = \sum_{k=0}^{\left[\frac{n}{2}\right]} K_{\lambda,(k,n-k)} m_{(k,n-k)}(x_1, x_2),$$

where $n = |\lambda|$. There can be no semi-standard tableau of shape λ and content μ if $\ell(\lambda) > \ell(\mu)$ because each of the $\ell(\lambda)$ rows of the tableau must be headed by a distinct integer chosen from a set of $\ell(\mu)$ integers. Thus, the only nontrivial case of (4.1) occurs when $\ell(\lambda) \le 2$. In this case it is not hard to see that, if $0 \le j \le \left[\frac{n}{2}\right]$ and $0 \le k \le \left[\frac{n}{2}\right]$, we have

$$K_{(j,n-j),(k,n-k)} = 1 \text{ if } k \ge j, \text{ and}$$

$$K_{(j,n-j),(k,n-k)} = 0 \text{ if } k < j,$$

whence

$$s(j,\ n-j)(x_1,\ x_2) = \sum_{k=j}^{\left[\frac{n}{2}\right]} m_{(k,\ n-k)}(x_1,\ x_2)$$

$$= x_1^j x_2^j (x_1^{n-2j} + x_1^{n-2j-1}x_2 + \cdots + x_2^{n-2j})$$

or

$$(4.2)\qquad s_{(j,\ n-j)}(x_1,\ x_2) = \frac{(x_1 x_2)\ (x_1^{n-2j+1} - x_2^{n-2j+1})}{x_1 - x_2}.$$

With U_n and V_n defined as in the introduction and $\rho = (\rho_1,\ \rho_2,\ \ldots,\ \rho_n)$, put

$$(4.3)\qquad V_\rho = V_{\rho_1} V_{\rho_2}\ \ldots\ V_{\rho_k}.$$

Then, from (4.2), we have

$$(4.4)\qquad s_{(j,\ n-j)}(a,\ b) = Q^j U_{n-2j+1}.$$

Moreover,

$$p_r(a,\ b) = V_r$$

so that, with $|\rho| = n$, (3.2) becomes

$$(4.5)\qquad V_\rho = \sum_{j=0}^{\left[\frac{n}{2}\right]} \chi_\rho^{(j,\ n-j)} Q^j U_{n-2j+1},$$

our first basic identity. For example, in the Fibonacci case, taking $\rho = (5,\ 3,\ 2)$ and referring to the table of characters of Σ_{10} in [1], we have

$$\begin{aligned}(-1)\ \chi_{(5,\ 3,\ 2)}^{(j,\ 10-j)} F_{11-2j} &= F_{11} - (-1)F_9 + F_7 - 0 \cdot F_5 + (-1)F_3 - 2F_1\\ &= 89 + 34 + 13 - 0 - 2 - 2 = 132\\ &= 11 \cdot 4 \cdot 3 = L_5 L_3 L_2 = L_{(5,\ 3,\ 2)}.\end{aligned}$$

From (3.3) we get our second basic identity

$$(4.6)\qquad \begin{cases} Q^j n!\, U_{n-2j+1} = \displaystyle\sum_{|\rho|=n} c_\rho \chi_\rho^{(j,\ n-j)} V_\rho, & \text{where } 0 \le j \le \dfrac{n}{2}\\[2ex] 0 = \displaystyle\sum_{|\rho|=n} c_\rho \chi_\rho^\lambda V_\rho, & \text{if } \ell(\lambda) \ge 3.\end{cases}$$

5. Special Cases of the First Basic Identity

In some cases it is not difficult to compute $\chi_\rho^{(j,\ n-j)}$. We use the Murnaghan-Nakayama Rule, which permits an inductive calculation. This requires some preliminary explanation.

Let $(i\ ,\ j)$ be the point in the i^{th} row (counting downward) and j^{th} column (counting to the right) in $[\rho]$, the diagram of ρ. The hook $H_{i,\ j}^\rho$ consists of the point $(i\ ,\ j)$ together with the points of $[\rho]$ directly to its right and directly below. The number of points in $H_{i,\ j}^\rho$, the length of the hook, is denoted by $h_{i,\ j}^\rho$. The points $(k,\ j)$, $k > i$, form the leg of $H_{i,\ j}^\rho$. The number of points in the leg of $H_{i,\ j}^\rho$ is called the leg-length and is denoted by $\ell_{i,\ j}^\rho$. The point of $H_{i,\ j}^\rho$ furthest to the right of $(i\ ,\ j)$ is called the hand of the hook, while the point of $H_{i,\ j}^\rho$ furthest below $(i\ ,\ j)$ is called its foot. To $H_{i,\ j}^\rho$ corresponds a portion of the rim of $[\rho]$ which is of the same length. It consists of the points on the rim between the hand and the foot. To $H_{1,\ 2}^{5,\ 3,\ 1}$, for example, there correspond the encircled points of [5, 3, 1] as follows:

• • ⊙ ⊙ ⊙
• ⊙ ⊙
•

The associated part of the rim, $R^{\rho}_{i,j}$, is called a rim-hook. It is important to notice that the result

$$[\rho]\backslash R^{\rho}_{i,j}$$

of removing $R^{\rho}_{i,j}$ from $[\rho]$ is again the diagram of a partition; e.g.,

$$[5,\ 3,\ 1]\backslash R^{(5,\ 3,\ 1)}_{1,\ 2} = \begin{array}{ll} \bullet & \bullet \\ \bullet & \\ \bullet & \end{array} = [2,\ 1^2].$$

The Murnaghan-Nakayama Rule is the following: Let λ and ρ be partitions of m, with

$$\rho = (1^{\beta},\ 2^{\beta_2}\ \ldots\ k^{\beta_k}\ \ldots\ m^{\beta_m}).$$

Suppose $\beta_k \geq 1$ and let

$$\pi = (1^{\beta_1}\ 2^{\beta_2}\ \ldots\ k^{\beta_k - 1}\ \ldots\ m^{\beta_m}).$$

Then

$$(5.1)\qquad \chi^{\lambda}_{\rho} = \sum_{\substack{i,\ j \\ h^{\lambda}_{ij} = k}} (-1)^{\rho^{\lambda}_{ij}}\ \chi^{\lambda\backslash R^{\lambda}_{ij}}_{\pi}.$$

Thus, by removing one occurrence of k from ρ and all k rim-hooks from λ, we can express χ^{λ}_{ρ} in terms of characters of lower order. Repeated application of this procedure allows us to compute χ^{λ}_{ρ} for any λ and ρ.

Let us assume that $j \leq m/2$. In case $\rho = (r,\ 1^{m-r})$ we can compute $\chi^{(j,\ m-j)}_{\rho}$ inductively by removing 1-hooks from $[j,\ m-j]$. The Murnaghan-Nakayama Rule yields

$$(5.2)\qquad \begin{cases} \chi^{(j,\ m-j)}_{(r,\ 1^{m-r})} = \chi^{(j-1,\ m-j)}_{r,\ 1^{m-r-1}} + \chi^{(j,\ m-j-1)}_{r,\ 1^{m-r-1}} & \text{if } j < \dfrac{m}{2} \\ \chi^{(j,\ j)}_{(r,\ 1^{m-r})} = \chi^{(j-1,\ j)}_{r,\ 1^{m-r-1}} & \text{if } j = \dfrac{m}{2} \end{cases}$$

Note the resemblance between (5.2) and the binomial recurrence. It is not hard to show, using induction on m, that

$$(5.3)\qquad \chi^{(j,\ m-j)}_{(r,\ 1^{m-r})} = \binom{m-r}{j} - \binom{m-r}{j-1} + \binom{m-r}{j-r} - \binom{m-r}{j-r-1}.$$

If $r = 1$, (5.3) becomes

$$(5.4)\qquad \chi^{(j,\ m-j)}_{1^m} = \binom{m-1}{j} - \binom{m-1}{j-2}$$

(**Remark**: (5.4) may also be obtained from the Frame-Robinson-Thrall formula for the degree of an irreducible representation of Σ_n.)

When $r = 2$, (5.3) can be written

$$(5.5)\qquad \chi^{(j,\ m-j)}_{2,\ 1^{m-2}} = \binom{m-3}{j} - \binom{m-3}{j-4}.$$

Using the same method as that used to establish (5.3), we can show that

$$(5.6)\qquad \chi^{(j,\ m-j)}_{r,\ s,\ 1^{m-r-s}} = \binom{m-r-s}{j} - \binom{m-r-s}{j-1} + \binom{m-r-s}{j-r} - \binom{m-r-s}{j-r-1}$$
$$+ \binom{m-r-s}{j-s} - \binom{m-r-s}{j-s-1}$$
$$+ \binom{m-r-s}{j-r-s} - \binom{m-r-s}{j-r-s-1}.$$

If $s = 2$, we have

$$(5.7)\qquad \chi^{(j,m-j)}_{r,2,1^{m-r-2}} = \binom{m-r-3}{j} - \binom{m-r-3}{j-4} + \binom{m-r-3}{j-r} - \binom{m-r-3}{j-r-4}$$

and if, in addition, $r = 4$, then

$$(5.8)\qquad \chi^{(j,m-j)}_{4,2,1^{m-6}} = \binom{m-7}{j} - \binom{m-7}{j-8}.$$

Each of (5.3) through (5.8) yields, via (4.5), a Fibonacci identity. We have, for example,

$$(5.4)'\qquad \sum_{j=0}^{\left[\frac{m}{2}\right]} Q^j\left[\binom{m-1}{j} - \binom{m-1}{j-2}\right]U_{m-2j+1} = V_1^m = P^{m-1}U_2,$$

$$(5.5)'\qquad \sum_{j=0}^{\left[\frac{m}{2}\right]} Q^j\left[\binom{m-3}{j} - \binom{m-3}{j-4}\right]U_{m-2j+1} = V_1^{m-2}V_2 = P^{m-3}U_4,$$

$$(5.8)'\qquad \sum_{j=0}^{\left[\frac{m}{2}\right]} Q^j\left[\binom{m-7}{j} - \binom{m-7}{j-8}\right]U_{m-2j+1} = V_1^{m-6}V_2V_4 = P^{m-7}U_8.$$

An expression similar to (5.6) but involving 2^{q+1} binomial coefficients may be given for

$$\chi^{(j,m-j)}_{t_1,t_2,\ldots,t_q,1^{m-(t_1+\cdots+t_q)}}$$

In case $t_i = 2^i$, $1 \le i \le q - 1$, this expression may be simplified to give the expected generalization of (5.4), (5.5) and (5.8):

$$(5.9)\qquad \chi^{(j,m-j)}_{2,4,8,\ldots,2^{q-1},1^{m-2q+2}} = \binom{m-2+1}{j} - \binom{m-2+1}{j-2},$$

yielding the Fibonacci identity

$$(5.9)'\qquad \sum_{j=0}^{\left[\frac{m}{2}\right]} Q^j\left[\binom{m-2^q+1}{j} - \binom{m-2^q+1}{j-2^q}\right]U_{m-2j+1} = V_1^{m-2^q+2}V_2V_4\ \ldots\ V_{2^q}$$
$$= P^{m-2^q+1}U_{2^q}.$$

If we reason similarly with rectangular partitions, i.e., partitions of the form t^k we obtain, from (4.5), the formulas

$$V_t^k = \sum^{\frac{k-1}{2}} \binom{k}{i} Q^{it}V_{(k-2i)t} \qquad k \text{ odd},$$

and

$$V_t^k = \sum^{\frac{k}{2}-1} \binom{k}{i} Q^{it}V_{(k-2i)t} + \binom{k}{\frac{1}{2}k} Q^{\frac{tk}{2}} \qquad k \text{ even}.$$

However, these identities are well known and not especially difficult to prove directly (see [4]).

6. Special Cases of the Second Basic Identity

If $\lambda = (n)$, then χ^λ_ρ is the identity character and (4.6) gives

$$(6.1)\qquad \sum_{|\rho|=n} c_\rho V_\rho = n!U_{n+1}.$$

If $\lambda = 1^n$, then $\chi_\rho^\lambda = \varepsilon(\rho)$, the alternating character. That is, $\varepsilon(\rho) = 1$ if the permutations with cycle-partition type ρ are even and $\varepsilon(\rho) = -1$ if these permutations are odd. From (4.6) we deduce

$$(6.2) \qquad \sum_{|\rho|=n} c_\rho \varepsilon_\rho V_\rho = 0 \quad \text{if } n \geq 3.$$

If $\lambda = (1, n-1)$, then χ^λ is the so-called "natural" character and $\chi_\rho^\lambda = \gamma_1 - 1$ where $\rho = 1^{\gamma_1} 2^{\gamma_2} \ldots n^{\gamma_n}$. In other words, χ_ρ^λ is one less than the number of elements left fixed by permutations with cycle-partition ρ. From (4.6) we have

$$\sum_{|\rho|=n} c_\rho (\gamma_1(\rho) - 1) V_\rho = Qn! U_{n-1}$$

which, in conjunction with (6.1) gives

$$\sum_{|\rho|=n} c(\rho)\gamma_1(\rho) L_\rho = \sum_{|\rho|=n} c_\rho V_\rho + Qn! U_{n-1} = n!(U_{n+1} + QU_{n-1})$$

or, finally,

$$(6.3) \qquad \sum_{|\rho|=n} c_\rho \gamma_1(\rho) V_\rho = n! PU_n = n! V_1 U_n.$$

Lastly, if $\lambda = (2, 1^{n-2})$, then χ^λ is the character conjugate to the natural character, i.e.,

$$\chi_\rho^{2,1^{n-2}} = \varepsilon(\rho)(\gamma_1(\rho) - 1).$$

Then, (4.6) yields, using (6.2),

$$(6.4) \qquad \sum_{|\rho|=n} c_\rho \varepsilon(\rho) \gamma_1(\rho) V_\rho = 0 \quad \text{if } n \geq 4.$$

The following chart illustrates (6.1) through (6.4) for $n = 4$ in the Fibonacci case.

ρ	c_ρ	$\varepsilon(\rho)$	$\gamma_1(\rho)$	L_ρ	$c_\rho L_\rho$	$c_\rho \varepsilon_\rho L_\rho$	$c_\rho \gamma_1(\rho) L_\rho$	$c_\rho \varepsilon(\rho) \gamma_1(\rho) L_\rho$
1	1	1	4	1	1	1	4	4
21	6	-1	2	3	18	-18	36	-36
2	3	1	0	9	27	27	0	0
31	8	1	1	4	32	32	32	32
4	6	-1	0	7	42	-42	0	0
		sums			$120 = 4!F_5$	0	$72 = 4!F_4$	0

A Generalization

Using a different approach, we generalize the identities established in Section 6. First, several additional concepts will be introduced.

Let

$$\rho = 1^{\gamma_1} 2^{\gamma_2} \ldots n^{\gamma_n} \quad \text{and} \quad \sigma = 1^{\beta_1} 2^{\beta_2} \ldots n^{\beta_n}$$

be partitions. We define the "generalized binomial coefficient" $\binom{\rho}{\sigma}$ by

$$(7.1) \qquad \binom{\rho}{\sigma} = \binom{\gamma_1}{\beta_1}\binom{\gamma_2}{\beta_2} \cdots \binom{\gamma_n}{\beta_n}$$

when the quantities on the right are ordinary binomial coefficients. $\binom{\rho}{\sigma}$ is itself an ordinary binomial coefficient when ρ and σ are suitable rectangular partitions. Clearly $\binom{\rho}{\sigma} = 0$ if $\gamma_i < \beta_i$ for some i, $1 \leq i \leq n$.

If $\gamma_i \geq \beta_i$, $1 \leq i \leq n$, we define the partition $\rho - \sigma$ by

$$(7.2) \qquad \rho - \sigma = 1^{\gamma_1 - \beta_1} 2^{\gamma_2 - \beta_2} \ldots n^{\gamma_n - \beta_n}.$$

Let

$$(7.3) \qquad z_\rho = \frac{n!}{c_\rho} = 1^{\gamma_1} 2^{\gamma_2} \ \ldots \ n^{\gamma_n} \gamma_1! \gamma_2! \ \ldots \ \gamma_n!$$

(z_ρ is the order of the centralizer of a permutation of cycle-type ρ). It is easy to show that

$$(7.4) \qquad \binom{\rho}{\sigma} = \frac{z_\rho}{z_\sigma z_{\rho - \sigma}}$$

whenever $\rho - \sigma$ is defined.

The r^{th} elementary symmetric function $e_r(x_1, \ldots, x_m)$ is the sum of all products of r distinct variables x_i so that $e_0 = 1$ and

$$e_r = \sum_{1 \le i_1 < i_2 < \cdots < i_r \le m} x_{i_1} x_{i_2} \ \ldots \ x_{i_r}.$$

The r^{th} *complete* symmetric function $h_r(x_1, \ldots, x_m)$ is the sum of all monomials of total degree r, so that, for example,

$$h_3(x_1, x_2, \ldots, x_m) = x_1^3 + x_2^3 + \cdots + x_1^2 x_2 + \cdots + x_1 x_2 x_3 + \cdots .$$

In particular, $h_0 = 1$ and $h_1 = e_1$. For $r < 0$, it is convenient to put $h_r = e_r = 0$.

Our generalizations of the results of Section 6 are based on the identities

$$(7.5) \qquad \sum_{|\rho| = n} \frac{\binom{\rho}{\sigma}}{z_\rho} p_\rho = \frac{p_\sigma h_{n - |\sigma|}}{z_\sigma}$$

and

$$(7.6) \qquad \sum_{|\rho| = n} \frac{\varepsilon_\rho \binom{\rho}{\sigma}}{z_\rho} p_\rho = \frac{\varepsilon_\sigma p_\sigma e_{n - |\sigma|}}{z_\sigma}.$$

We prove only (7.5); the proof of (7.6) is similar.

Our proof of (7.5) is based on (7.4) and the identity

$$(7.7) \qquad \sum_{|\rho| = n} \frac{p_\rho}{z_\rho} = h_n.$$

(For a proof of (7.7), see [2], p. 17.)

Noting that $p \quad = p \ p \quad$, we have

$$\sum_{|\rho| = n} \frac{\binom{\rho}{\sigma}}{z_\rho} p_\rho = p_\sigma \sum_{|\rho| = n} \frac{\binom{\rho}{\sigma}}{z_\rho} p_{\rho - \sigma} = \frac{p_\sigma}{z_\sigma} \sum_{|\rho| = n} \frac{p_{\rho - \sigma}}{z_{\rho - \sigma}} = \frac{p_\sigma}{z_\sigma} \sum_{|\tau| = n - |\sigma|} \frac{p_r}{z_r}$$

$$= \frac{p_\sigma}{z_\sigma} h_{n - |\sigma|},$$

thus proving (7.5).

Observing that

$$h_r(a, b) = a_1^r + a^{r-1} b + \cdots + b^r = \frac{a^{r+1} - b^{r+1}}{a - b} = U_{r+1},$$

we find, on putting $x_1 = a_1$, $x_2 = b_2$, $x_3 = x_4 = \cdots = 0$ in (7.5), the identity

$$(7.8) \qquad \sum_{|\rho| = n} \frac{\binom{\rho}{\sigma} V_\rho}{z_\rho} = \frac{V_\sigma}{z_\sigma} U_{n - |\sigma| + 1},$$

which, using (7.3), can be written

$$(7.9) \qquad \sum_{|\rho| = n} c_\rho \binom{\rho}{\sigma} V_\rho = \frac{n! c_\sigma V_\sigma U_{n - |\sigma| + 1}}{|\sigma|!}.$$

Likewise, since

$$e_1(a, b, 0, \ldots) = a + b = P,$$
$$e_2(a, b, 0, \ldots) = ab = Q,$$
$$e_r(a, b, 0, \ldots) = 0, \text{ if } r \geq 3,$$

we obtain from (7.6),

$$(7.10) \quad \sum_{|\rho| = n} \varepsilon_\rho \binom{\rho}{\sigma} c_\rho V_\rho = \frac{\varepsilon_\sigma c_\sigma n! P V_\sigma}{|\sigma|}$$

if $|\sigma| = n - 1$,

$$(7.11) \quad \sum_{|\rho| = n} \varepsilon_\rho \binom{\rho}{\sigma} c_\rho V_\rho = \frac{\varepsilon_\sigma c_\sigma n! Q V_\sigma}{|\sigma|}$$

if $|\sigma| \leq n - 2$, and

$$(7.12) \quad \sum_{|\rho| = n} \varepsilon_\rho \binom{\rho}{\sigma} c_\rho V_\rho = 0$$

if $|\sigma| \leq n - 3$.

If we specialize σ to be a partition of length 1, i.e., $\sigma = k^1$, then $\binom{\rho}{\sigma} = \gamma_k(\rho)$, $\varepsilon_\sigma = (-1)^{k-1}$, $c_\sigma = (k - 1)!$, and (7.9), (7.10), (7.11), and (7.12) yield

$$(7.13) \quad \sum_{|\rho| = n} c_\rho \gamma_k(\rho) V_\rho = \frac{n! V_k U_{n-k+1}}{k},$$

$$(7.14) \quad \sum_{|\rho| = n} \varepsilon_\rho c_\rho \gamma_k(\rho) V_\rho = \frac{(-1)^n n! P V_k}{k} \text{ if } k = n - 1,$$

$$(7.15) \quad \sum_{|\rho| = n} \varepsilon_\rho c_\rho \gamma_k(\rho) V_\rho = \frac{(-1)^{n-1} n! Q V_k}{k} \text{ if } k = n - 2,$$

and

$$(7.16) \quad \sum_{|\rho| = n} \varepsilon_\rho c_\rho \gamma_k(\rho) V_\rho = 0 \text{ if } k \leq n - 3,$$

which are generalizations of (6.3) and (6.4).

References

1. G. James & A. Kerber. *The Representation Theory of the Symmetric Group*. New York: Addison Wesley, 1981.
2. I. G. Macdonald. *Symmetric Functions and Hall Polynomials*. Oxford: Clarendon Press, 1979.
3. F. D. Murnaghan. *The Theory of Group Representations*. Baltimore: The Johns Hopkins Press, 1938.
4. S. Vajda. *Fibonacci and Lucas Numbers and the Golden Section: Theory and Applications*. New York: Ellis Horwood Ltd., Wiley, 1989.

*****

GCD-CLOSED SETS AND THE DETERMINANTS OF GCD MATRICES

Scott Beslin
Nicholls State University, Thibodaux, LA 70310

Steve Ligh
Southeastern Louisiana University, Hammond, LA 70402

(Submitted July 1990)

1. Introduction

Let $S = \{x_1, x_2, \ldots, x_n\}$ be a finite ordered set of distinct positive integers. The $n \times n$ matrix $[S] = (s_{ij})$, where $s_{ij} = (x_i, x_j)$, the greatest common divisor of x_i and x_j, is called the greatest common divisor (GCD) matrix on S (see [2]). In [6], H. J. S. Smith showed that if S is a factor-closed set, then the determinant of $[S]$, det$[S]$, is $\phi(x_1)\,\phi(x_2)\,\ldots\,\phi(x_n)$, where $\phi(x)$ is Euler's totient function. A set S of positive integers is said to be factor-closed if all positive factors of any member of S belong to S. In [2], we considered GCD matrices in the direction of their structure, determinant, and arithmetic in Z_n, the ring of integers modulo n. In [1], we generalized Smith's result by extending the factor-closed sets to a larger class of sets called gcd-closed sets. A set $S = \{x_1, x_2, \ldots, x_n\}$ as above is said to be gcd-closed if for every i and $j = 1, 2, \ldots, n$, (x_i, x_j) is in S. Every factor-closed set is gcd-closed, but not conversely.

Using structure theorems in [2], Zhongshan Li [4] obtained the value of the determinant of a GCD matrix defined on an arbitrary ordered set of distinct positive integers, and proved the converse of Smith's result. Since the formula derived in [4] is valid for any GCD matrix, it also solves the problem stated in [5] for arithmetic progressions.

In this paper we shall provide another formula for the determinant of a GCD matrix based on the class of gcd-closed sets. Li's formula comes as a corollary. We also use this new formula to find closed-form expressions for the determinants of some special GCD matrices.

2. Preliminary Results

It was remarked in [2] that the determinant of the GCD matrix defined on a set S is independent of the order of the elements of S. Thus, if $S = \{x_1, x_2, \ldots, x_n\}$, we may henceforth assume that $x_1 < x_2 < \cdots < x_n$. Given this natural order on S, we let $B(x_i)$ denote the sum

$$B(x_i) = \sum_{\substack{d \mid x_i \\ d \nmid x_t \\ t < i}} \phi(d),$$

for all $i = 1, 2, \ldots, n$. We note that $B(x_i) = \phi(x_i)$ for all i if and only if S is factor-closed.

The following proposition can be found in [1].

Proposition A: Let $S = \{x_1, x_2, \ldots, x_n\}$ be gcd-closed with $x_1 < x_2 < \cdots < x_n$. Then, for every i and $j = 1, 2, \ldots, n$,

$$(x_i, x_j) = \sum_{x_k \mid (x_i, x_j)} B(x_k).$$

It is clear that any set S of positive integers is contained in a gcd-closed set. By $\overline{S}$ we mean the minimal such gcd-closed set, or *gcd-closure* of S.

It is worthwhile to observe that $\overline{S}$ usually contains considerably fewer elements than any factor-closed set containing S. We now prove a structure theorem for GCD matrices.

Theorem 1: Let $\overline{S} = \{x_1, x_2, \ldots, x_m\}$ be the gcd-closure of $S = \{y_1, y_2, \ldots, y_n\}$ with $x_1 < x_2 < \cdots < x_m$ and $y_1 < y_2 < \cdots < y_n$. Then $[S]$ is the product of an $n \times m$ matrix A and the incidence matrix C corresponding to the transpose of A.

Proof: Define $A = (a_{ij})$ via

$$a_{ij} = \begin{cases} B(x_j) & \text{if } x_j \text{ divides } y_i, \\ 0 & \text{otherwise.} \end{cases}$$

If we let $C = (c_{ij})$ be the incidence matrix corresponding to the transpose of A, then the (i, j)-entry of AC is equal to

$$\sum_{k=1}^{n} a_{ik}c_{kj} = \sum_{\substack{x_k | y_i \\ x_k | y_j}} a_{ik} = \sum_{x_k | (y_i, y_j)} B(x_k),$$

which is equal to (y_i, y_j) by Proposition A and the fact that $\overline{S}$ is gcd-closed.

Remark 1: In the above theorem, $\overline{S}$ may actually be replaced with any gcd-closed set containing S.

The following corollaries appeared in [1].

Corollary 1: If $S = \{x_1, x_2, \ldots, x_n\}$ is gcd-closed with $x_1 < x_2 < \cdots < x_n$, then

$$\det[S] = B(x_1)B(x_2) \ldots B(x_n).$$

Corollary 2 (Smith): If $S = \{x_1, x_2, \ldots, x_n\}$ is factor-closed, then

$$\det[S] = \phi(x_1)\phi(x_2) \ldots \phi(x_n).$$

Corollary 3: Let $S = \{x_1, x_2, \ldots, x_n\}$ be gcd-closed. Then

$$\det[S] = \phi(x_1)\phi(x_2) \ldots \phi(x_n)$$

if and only if S is factor-closed.

Remark 2: It was actually shown in [4] that the converse of Corollary 2 is true.

3. The Value of det[S]

The (i, j)-entry of the matrix A in Theorem 1 may be written as $e_{ij}B(x_j)$, where $e_{ij} = 1$ if x_j divides y_i, and 0 otherwise. Let E be the $n \times m$ matrix (e_{ij}). Thus, $C = E^{\mathsf{T}}$, the transpose of E. If Λ is the $m \times m$ diagonal matrix with diagonal $(B(x_1), B(x_2), \ldots, B(x_m))$, we have that $AC = E\Lambda E^{\mathsf{T}}$.

Now let $k_1, k_2, \ldots, k_n$ be distinct positive integers such that

$$1 \le k_1 < k_2 < \cdots < k_n \le m,$$

and let $E_{(k_1, k_2, \ldots, k_n)}$ denote the submatrix of E consisting of the k_1th, ..., k_nth columns of E. Define $A_{(k_1, \ldots, k_n)}$ similarly. It is clear that

$$\det A_{(k_1, \ldots, k_n)} = B(x_{k_1})B(x_{k_2}) \ldots B(x_{k_n}) \cdot \det E_{(k_1, \ldots, k_n)},$$

since

$$A_{(k_1, \ldots, k_n)} = E_{(k_1, \ldots, k_n)} \cdot D,$$

where D is the $n \times n$ diagonal submatrix of Λ with diagonal $(B(x_{k_1}), \ldots, B(x_{k_n}))$.

The following theorem gives the value of $\det[S]$ in terms of $B(x_1)$, $B(x_2)$, $\ldots$, $B(x_m)$.

Theorem 2: Let S and $\overline{S}$ be as in Theorem 1. Then $\det[S]$ is given by the sum

$$\sum_{1 \le k_1 < k_2 < \cdots < k_n \le m} (\det E_{(k_1, \ldots, k_n)})\ B(x_{k_1})\ \ldots\ B(x_{k_n}).$$

Proof: From Theorem 1, $[S] = AC$. Now apply the Cauchy-Binet formula (see [3], p. 22) to obtain

$$\det[S] = \det(AC) = \sum_{1 \le k_1 < k_2 < \cdots < k_n \le m} \det A_{(k_1, \ldots, k_n)} \cdot \det(E_{(k_1, \ldots, k_n)})^{\mathrm{T}};$$

the result follows from the preceding remarks.

Corollary 4 (Li [4], Theorem 2): Let S be as in Theorem 1 and let $S^* = \{x_1, x_2, \ldots, x_m\}$ be the minimal factor-closed set containing S, with $x_1 < x_2 < x_3 < \cdots < x_m$. Then

$$\det[S] = \sum_{1 \le k_1 < k_2 < \cdots < k_n \le m} (\det E_{(k_1, \ldots, k_n)})^2 \phi(x_{k_1})\ \ldots\ \phi(x_{k_n}).$$

Remark 3: By using a proof similar to that occurring in Li's paper for the converse of Corollary 2 (see [4], Theorem 3), one may establish the converse of Corollary 1.

4. Determinants of Special Matrices

Although the matrices $E_{(k_1, \ldots, k_n)}$ in Theorem 2 are (0, 1)-matrices, it is not true in general that $\det E_{(k_1, \ldots, k_n)} = \pm 1$. In this section, we consider certain sets S which have the property that every such submatrix $E_{(k_1, \ldots, k_n)}$ has determinant equal to 1 or -1, and thus find a closed-form expression for $\det[S]$.

A set $S = \{x_1, x_2, \ldots, x_n\}$ is said to be a k-set if $(x_i, x_j) = k$ for every $i, j = 1, 2, \ldots, n$. For example, $\{6, 9, 15, 21, 33\}$ is a 3-set. Let S be a k-set. Then either $\overline{S} = S \cup \{k\}$ or $\overline{S} = S$.

Case 1. If $x_1 < x_2 < \cdots < x_n$ and $k = x_1$, then S is gcd-closed, and $B(x_i) = x_i - k$ for $i = 2, 3, \ldots, n$. Hence, by Corollary 1,

$$\det[S] = k(x_2 - k)\ \ldots\ (x_n - k).$$

Case 2. Suppose $k \ne x_1$ so that $\overline{S} = \{k = x_0, x_1, x_2, \ldots, x_n\}$. By Theorem 2,

$$\det[S] = \sum_{0 \le t_1 < t_2 < \cdots < t_n \le n} (\det E_{(t_1, \ldots, t_n)})^2 B(x_{t_1}) B(x_{t_2})\ \ldots\ B(x_{t_n}).$$

Lemma 1: $\det E_{(t_1, \ldots, t_n)} = \pm 1$.

Proof: If $(t_1, \ldots, t_n) = (0, 2, 3, \ldots, n)$ or $(1, 2, 3, \ldots, n)$, then $E_{(t_1, \ldots, t_n)}$ is a lower triangular matrix with diagonal $(1, 1, \ldots, 1)$. Thus, $\det E_{(t_1, \ldots, t_n)} = 1$. If

$$(t_1, \ldots, t_n) = (0, 1, \ldots, s - 1, s + 1, \ldots, n) \text{ for } 2 \le s \le n,$$

then Row s of $E_{(t_1, \ldots, t_n)}$ is $(1, 0, 0, \ldots, 0)$. Moreover, the submatrix of $E_{(t_1, \ldots, t_n)}$ formed by removing Column 1, i.e.,

$$\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix},$$

and Row s is the $(n - 1) \times (n - 1)$ identity matrix. Hence,

$$\det E_{(t_1, \ldots, t_n)} = \pm 1.$$

This completes the proof.

Now $B(x_0) = k$ and $B(x_i) = x_i - k$ for $i > 0$. Thus, by Theorem 2,

$$\det[S] = k \cdot \left(\sum_{i=1}^{n} \frac{(x_1 - k) \cdots (x_n - k)}{(x_i - k)} \right) + (x_1 - k) \cdots (x_n - k).$$

Cases 1 and 2 above may therefore be combined into the following theorem.

Theorem 3: If $S = \{x_1, x_2, \ldots, x_n\}$ is a k-set with $x_1 < x_2 < \cdots < x_n$, then

$$\det[S] = k(x_2 - k) \cdots (x_n - k)$$
$$+ [k(x_1 - k) \cdots (x_n - k)]\left[\frac{1}{k} + \frac{1}{x_2 - k} + \cdots + \frac{1}{x_n - k}\right].$$

Corollary 5: Let $S = \{x_1, x_2, \ldots, x_n\}$ consist of pairwise coprime positive integers. If $x_1 < x_2 < \cdots < x_n$, then

$$\det[S] = (x_2 - 1) \cdots (x_n - 1)$$
$$+ [(x_1 - 1) \cdots (x_n - 1)]\left[1 + \frac{1}{x_2 - 1} + \cdots + \frac{1}{x_n - 1}\right].$$

Corollary 6: Let $p_1, p_2, \ldots, p_n$ be primes with $p_1 < p_2 < \cdots < p_n$. If $S = \{p_1, p_2, \ldots, p\}$, then

$$\det[S] = (p_1 - 1) \cdots (p_n - 1)\left[1 + \frac{1}{p_1 - 1} + \cdots + \frac{1}{p_n - 1}\right]$$
$$= \phi(p_1) \cdots \phi(p_n)\left[1 + \frac{1}{\phi(p_1)} + \cdots + \frac{1}{\phi(p_n)}\right].$$

Finally, in view of Lemma 1, and for lack of a counterexample, we make the following conjecture and leave it as a problem.

Conjecture: Let S and $\bar{S}$ be as in Theorem 3, with $n > 3$. If $\det E_{(k_1, k_2, \ldots, k_n)} = \pm 1$ for every choice of $k_1, k_2, \ldots, k_n$, then either S is gcd-closed or S is a k-set for some positive integer k.

References

1. S. Beslin & S. Ligh. "Another Generalization of Smith's Determinant." *Bull. Australian Math. Soc.* *(3) 40* (1989):413-15.
2. S. Beslin & S. Ligh. "Greatest Common Divisor Matrices." *Linear Algebra and Its Applications* *118* (1989):69-76.
3. R. Horn & C. Johnson. *Matrix Analysis.* Cambridge: Cambridge University Press, 1985.
4. Zhongshan Li. "The Determinants of GCD Matrices." *Linear Algebra and Its Applications* *134* (1990):137-43.
5. S. Ligh. "Generalized Smith's Determinant." *Linear and Multilinear Algebra* *22* (1988):305-06.
6. H. J. S. Smith. "On the Value of a Certain Arithmetical Determinant." *Proc. London Math. Soc.* *7* (1875-1876):208-12.

*****

ON THE LEAST ABSOLUTE REMAINDER EUCLIDEAN ALGORITHM

Thomas E. Moore
Bridgewater State College, Bridgewater, MA 02325

(Submitted July 1990)

To the memory of my friend and mentor Fr. Thomas E. Lockary, C.S.C.

1. Introduction

The usual operation of the Euclidean algorithm uses the least positive remainder at each step of division. However, the Euclidean algorithm can be modified to allow positive or negative remainders provided the absolute value of the remainder is less than the divisor in each step of division.

For example, in computing the greatest common divisor of 3 and 5, there are three Euclidean algorithms in this extended sense:

$$\begin{array}{lll} 5 = 3(2) - 1 & 5 = 3(1) + 2 & 5 = 3(1) + 2 \\ 3 = 1(3) + 0 & 3 = 2(1) + 1 & 3 = 2(2) - 1 \\ & 2 = 1(2) + 0 & 2 = 1(2) + 0 \end{array}$$

the first of which uses the least absolute remainder at each step and which is shorter than the others.

A theorem of Kronecker, see Uspensky & Heaslet [3], says that no Euclidean algorithm is shorter than the one obtained by taking the least absolute remainder at each step of division.

Goodman & Zaring [1] have shown that the number of steps of division in the least positive remainder Euclidean algorithm exceeds the number of steps in the least absolute remainder Euclidean algorithm by just the number of negative remainders occurring in the least absolute remainder variant.

We became interested in exactly which pairs M and N of positive integers have their greatest common divisor, denoted gcd(M, N), computed in strictly fewer steps by the least absolute remainder (LAR) Euclidean algorithm than by the least positive remainder (LPR) Euclidean algorithm.

Accordingly, a computer program to graphically display such pairs was written in Applesoft BASIC (see Figure 1) and can be modified easily for other BASICs. The program uses counters DC and ADC to count the number of steps of division needed by the LPR and LAR Euclidean algorithms, respectively, in computing gcd(M, N) with $M \geq N$. The program lights a pixel on the monitor at screen location (M, N) provided ADC < DC in this computation.

When performing the LAR Euclidean algorithm, the program (lines 320-390) chooses between the quotient Q with least positive remainder R and the quotient $Q + 1$ with the alternative negative remainder AR and, if $R = ABS(AR)$, then it breaks the tie by selecting Q and R in agreement with [1].

The resulting image (see Figure 2) reveals some interesting features of the distribution of the lit (black) points (M, N) in the range $1 \leq M \leq 191$, $1 \leq N \leq 191$, with $M \geq N$. Some of these are described in Section 2.

2. Analysis

Definition: If $M \geq N$ is a pair of positive integers for which the LAR Euclidean algorithm is shorter than the LPR Euclidean algorithm, then we will say that *M is a Kronecker number for N* and also that (M, N) is an (ordered) *Kronecker pair*.

```
90 REM STUDY OF LAR VERSUS LPR ALGORITHMS
110 REM DC COUNTS STEPS OF LPR ALGORITHM
120 REM ADC COUNTS STEPS OF LAR ALGORITHM
125 HGR2:REM HI-RES GRAPHICS PAGE IN MEMORY
128 HCOLOR=3:HPLOT 0,0 TO 0, 191 TO 191,191
130 FOR N=1 TO 191
140 FOR M=N TO 191
150 DC=0:ADC=0
170 GOSUB 240
180 GOSUB 310
190 IF ADC>=DC THEN 220
200 REM PLOT ONLY KRONECKER PAIRS
210 HPLOT M, 192-N
220 NEXT M
230 NEXT N
235 GOTO 999
240 REM ROUTINE FOR USUAL LPR ALGORITHM
250 M1=M:N1=N
255 Q=INT(M1/N1)
260 R=M1-N1*Q
270 DC=DC+1
280 M1=N1
290 N1=R
300 IF R>0 THEN 255
305 RETURN
310 REM ROUTINE FOR LAR ALGORITHM
320 M1=M:N1=N
325 Q=INT(M1/N1)
330 R=M1-N1*Q
340 AR=M1-N1*(Q+1)
345 ADC=ADC+1
350 IF R<=ABS(AR) THEN 380
360 M1=N1
370 N1=ABS(AR):GOTO 400
380 M1=N1
390 N1=R
400 IF N1>0 THEN 325
410 RETURN
999 END
```

Figure 1

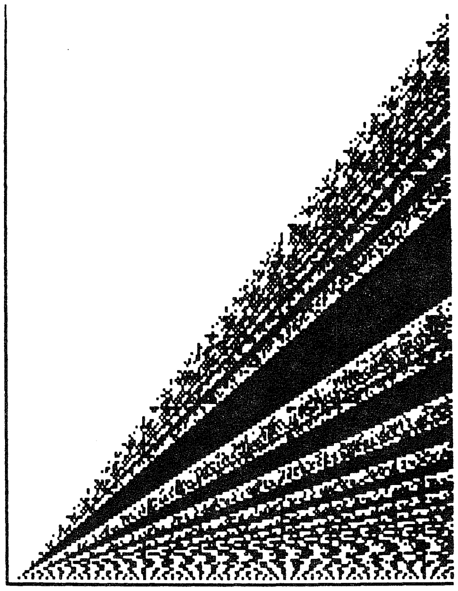


Figure 2

Looking again at Figure 2, we observe the densest region of contiguous Kronecker pairs that is bounded by the lines $N = (2/3)M$ and $N = (1/2)M$.

Considering the coordinates of lit points in this region, we construct a table (see Table 1) of Kronecker numbers M for each N, along with the lengths of the blocks of these consecutive M.

Table 1

N	Consecutive Kronecker Numbers $M > N$	Block Length
3	5	1
4	7	1
5	8, 9	2
6	10, 11	2
7	11, 12, 13	3
8	13, 14, 15	3
9	14, 15, 16, 17	4
10	16, 17, 18, 19	4
11	17, 18, 19, 20, 21	5
12	19, 20, 21, 22, 23	5
13	20, 21, 22, 23, 24, 25	6
14	22, 23, 24, 25, 26, 27	6

Table 1 suggests the next result.

Theorem 1: (i) For $N = 2t + 1$, $t \geq 1$, the t consecutive integers

$$(3N + 1)/2,\ (3N + 3)/2,\ \ldots,\ 2N - 1$$

are all Kronecker numbers for N.

(ii) For $N = 2t$, $t \geq 2$, the $t - 1$ consecutive integers

$$(3N + 2)/2,\ (3N + 4)/2,\ \ldots,\ 2N - 1$$

are all Kronecker numbers for N.

Proof: We prove part (i).

For a fixed integer $t \geq 1$ and any one of the integers $(3N+1)/2$, $(3N+3)/2$, $\ldots$, $2N+1$, say $(3N + k)/2$, where $1 \leq k \leq N - 2$ and k is odd, the LAR Euclidean algorithm must decide, in the first step of division, between the two choices

$$(3N + k)/2 = N(1) + (N + k)/2,$$

in which $(N + k)/2 < N$ because $k \leq N - 2$, or

$$(3N + k)/2 = N(2) + (k - N)/2,$$

in which $\text{ABS}((k - N)/2) < N$ because $N > -k$.

The decision is made for the latter choice according to the comparison

$$\text{ABS}((k - N)/2) < (N + k)/2,$$

which is true since $N - k < N + k$.

The result now follows from the Goodman & Zaring result.

Part (ii) of the theorem is proved similarly.

Corollary 1: For each $t \geq 2$, we may specify a positive integer N and t consecutive integers that are all Kronecker numbers for N.

Proof: Immediate.

Lemma 1: If M is a Kronecker number for N, then $M + Nk$ is also a Kronecker number for N, for all integers $k \geq 1$.

Proof: Suppose the LAR Euclidean algorithm for $\gcd(M, N)$ is

$$\begin{aligned} M &= Nq_1 + e_1r_1,\ r_1 < N,\\ N &= r_1q_2 + e_2r_2,\ r_2 < r_1,\\ r_1 &= r_2q_3 + e_3r_3,\ r_3 < r_2,\\ &\vdots\\ r_s &= r_{s+1}q_{s+2} \end{aligned}$$

so that $\gcd(M, N) = r_{s+1}$ and each $e_i = \pm 1$.

Since M is a Kronecker number for N, at least one $e_i = -1$, by the Goodman & Zaring result.

The LAR Euclidean algorithm for $M + Nk$ and N is then

$$\begin{aligned} M + Nk &= N(q_1 + k) + e_1r_1,\\ N &= r_1q_2 + e_2r_2,\\ &\vdots\\ r_s &= r_{s+1}q_{s+2} \end{aligned}$$

with the same set of values r_i and e_i. Hence, at least one negative e_i occurs and, again by the result of Goodman & Zaring, $M + Nk$ is a Kronecker number for N.

Once more observing the patterns in the lit points in Figure 2 we see that, for each second coordinate N, the values of first coordinates fall into certain progressions.

Theorem 2: For each integer $N \geq 3$ there are arithmetic progressions of integers $M > N$ that are all Kronecker numbers for N. More precisely,

(i) if $N = 2t + 1$, $t \geq 1$, then the arithmetic progressions

$$\{Nk + t + 1\}, \{Nk + t + 2\}, \ldots, \{Nk + t + (N - 1)/2\}, k \geq 1,$$

consist of integers each of which is a Kronecker number for N, and

(ii) if $N = 2t$, $t \geq 2$, then the arithmetic progressions

$$\{Nk + t + 1\}, \{Nk + t + 2\}, \ldots, \{Nk + t + (N - 2)/2\}, k \geq 1,$$

consist of integers each of which is a Kronecker number for N.

Proof: We prove part (i).

By Lemma 1, since the common difference in each progression is N, it is enough to show that the first term in each progression is a Kronecker number for N.

When $k = 1$ the first terms are, respectively,

$$N + t + 1, N + t + 2, \ldots, N + t + (N - 1)/2.$$

Since $t = (N - 1)/2$, these terms are, respectively,

$$(3N + 1)/2, (3N + 3)/2, \ldots, 2N - 1,$$

which are Kronecker numbers for N by Theorem 1.

In the above theorems we have begun with the smaller value N of a Kronecker pair and then constructed the companion number M. In the reverse direction, we offer the next result.

Theorem 3: (i) If M is odd, $M \geq 7$, then M is a Kronecker number for both $(M \pm 1)/2$.

(ii) If M is even, $M \geq 8$, then M is a Kronecker number for both $(M \pm 2)/2$.

Proof: (i) We prove the case $(M + 1)/2$. The LPR Euclidean algorithm here is

$$\begin{aligned} M &= (1)((M + 1)/2) + (M - 1)/2, \\ (M + 1)/2 &= (1)((M - 1)/2) + 1, \\ (M - 1)/2 &= ((M - 1)/2)(1) + 0, \end{aligned}$$

done in three steps, while the LAR Euclidean algorithm begins

$$M = (2)((M + 1)/2) + -1,$$

because ABS(-1) $< (M - 1)/2$, since $M > 3$, and continues

$$(M + 1)/2 = ((M + 1)/2)(1) + 0,$$

done in two steps.

Similarly, we can show that M is also a Kronecker number for $(M - 1)/2$.

(ii) We prove the case $(M + 2)/2$. The LPR Euclidean algorithm here begins

$$\begin{aligned} M &= (1)((M + 2)/2) + (M - 2)/2, \\ (M + 2)/2 &= (1)((M - 2)/2) + 2, \end{aligned}$$

and the next division [by 2 into $(M - 2)/2$] is the last step, or next to last, according as $(M - 2)/2$ is even or odd. So this routine takes three or four steps, accordingly.

The LAR Euclidean algorithm begins

$$M = (2)((M + 2)/2) + -2,$$

because ABS(-2) < $(M - 2)/2$, since $M > 6$, and there are either one or two steps more according to the parity of $(M + 2)/2$. Since $(M + 2)/2$ and $(M - 2)/2$ have the same parity, this means that the LAR variant is accomplished in one step less than the LPR Euclidean algorithm.

Similarly, we can show that M is a Kronecker number for $(M - 2)/2$.

3. The Fibonacci Numbers

The Fibonacci numbers, which are defined by the relations $F_1 = F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$, play an extremal role in questions relating to the number of steps in the LPR Euclidean algorithm. For example, in [2] Shea shows that the pair of integers with the smallest sum whose gcd takes exactly k steps using the LPR Euclidean algorithm is F_{k+1}, F_{k+2}. Not surprisingly, the Fibonacci numbers enter our investigation in a similar way.

Theorem 4: Any positive integer n may be specified as the difference in the number of steps of division performed in computing gcd(M, N) by the LPR and LAR Euclidean algorithms. In fact, this difference n is attained in the computation of both gcd(F_{2n+2}, F_{2n+3}) and gcd(F_{2n+3}, F_{2n+4}).

Proof: It is well known that the LPR Euclidean algorithm applied to consecutive Fibonacci numbers F_k and F_{k+1} takes $k - 1$ steps of division, each with quotient 1 and hence with sequence of remainders F_{k-1}, F_{k-2}, F_{k-3}, ..., F_2, and 0.

The first quotient in the LAR Euclidean algorithm applied to F_k and F_{k+1} is 2 with remainder $-F_{k-2}$. If k is an even integer, then each subsequent division uses a quotient of 3, because of the inequality

$$2F_{2t} < F_{2t+2} < 3F_{2t} \text{ for all } t \geq 2,$$

which may be proved by induction on t. Thus, the sequence of remainders is $-F_{k-2}$, $-F_{k-4}$, $-F_{k-6}$, ..., $-F_2$, and 0. So there are $k/2$ steps of division.

Hence, the difference in the number of steps of the two methods is

$$(k - 1) - k/2 = (k - 2)/2.$$

As k varies over the even integers, $k \geq 4$, this difference $(k - 2)/2$ varies over all the positive integers. For $k = 2n + 2$ in particular, gcd(F_{2n+2}, F_{2n+3}) shows a difference of exactly n steps of division.

The rest of the theorem is proved similarly.

As noted by an anonymous referee, it seems interesting to point out that, whereas the usual Euclidean algorithm leads to the familiar continued fraction

$$F_{2k+3}/F_{2k+2} = (1; 1, 1, \ldots, 1), \; 2k + 1 \text{ ones},$$

the least absolute remainder Euclidean algorithm leads to

$$F_{2k+3}/F_{2k+2} = (2; -3, -3, \ldots, -3), \; k \text{ threes}.$$

References

1. A. W. Goodman & W. M. Zaring. "Euclid's Algorithm and the Least-Remainder Algorithm." *Amer. Math. Monthly* 59 (1952):156-59.
2. D. D. Shea. "On the Number of Divisions Needed in Finding the Greatest Common Divisor." *Fibonacci Quarterly* 7.4 (1969):337-40.
3. J. V. Uspensky & M. A. Heaslet. *Elementary Number Theory.* New York and London: McGraw-Hill, 1939.

*****

TREES FOR k-REVERSE MULTIPLES

Anne Ludington Young
Loyola College in Maryland, Baltimore, MD 21210

(Submitted July 1990)

Let x be an n-digit, base g number

$$x = \sum_{i=0}^{n-1} a_i g^i \tag{1}$$

with $0 \le a_i < g$ and $a_{n-1} \ne 0$. If, for some integer k, where $1 < k < g$,

$$kx = \sum_{i=0}^{n-1} a_{n-1-i} g^i \tag{2}$$

then x is called a *k-reverse multiple*, Previously, this author showed that all k-reverse multiples may be found using rooted trees [3]. A more detailed examination of these trees is the focus of this paper.

If x is a k-reverse multiple, then we obtain from (1) and (2) the following equations

$$ka_i + r_{i-1} = a_{n-1-i} + r_i g,\ i = 0, \ldots, n-1, \tag{3}$$

where $0 \le r_i < g$ for $i = 0, \ldots, n-2$ and $r_{-1} = r_{n-1} = 0$. Letting $i = n-1$ in (3) gives $a_0 \ne 0$ since $a_{n-1} \ne 0$. To determine whether there are any k-reverse multiples for a given g, we consider the equations in (3) two at a time. At the $(i+1)^{\text{st}}$ step, $i = 0, 1, \ldots$, we examine the pair of equations

$$\begin{cases} ka_i + r_{i-1} = a_{n-1-i} + r_i g \\ ka_{n-1-i} + r_{n-2-i} = a_i + r_{n-1-i} g \end{cases} \tag{4}$$

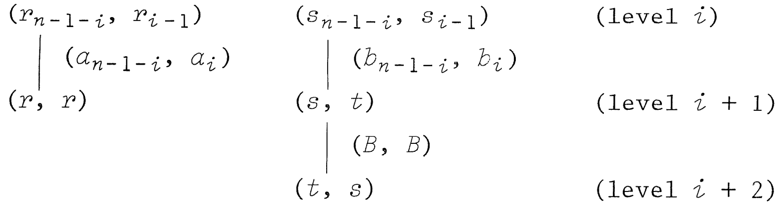
seeking nonnegative integers a_i, a_{n-1-i}, r_i, and r_{n-2-i} less than g, where r_{i-1} and r_{n-1-i} are known from the previous step. The following graphical notation is convenient. If r_{n-1-i}, r_{i-1}, a_{n-1-i}, a_i, r_{n-2-i}, and r_i satisfy (4), then we will write

$$\begin{array}{l} (r_{n-1-i},\ r_{i-1}) \\ \quad\Big| \quad (a_{n-1-i},\ a_i) \\ (r_{n-2-i},\ r_i) \end{array} \tag{5}$$

(Implicit in this notation is the assumption that the a's and r's are nonnegative integers less than g.)

When a given g has k-reverse multiples, we are able to generate a rooted tree. We call the root of the tree $(r_{n-1}, r_{-1}) = (0, 0)$, the 0^{th} level and the node designated by (r_{n-2-i}, r_i), the $(i+1)^{\text{st}}$ level. Since $0 \le r_i < g$, there are only a finite number of possible distinct nodes. If a node is labeled with a pair that has already appeared in the tree, the tree can be pruned. The following theorem shows how a tree is used to determine k-reverse multiples. The proof appeared in [3] and hence is omitted here.

Theorem 1: For a given g, suppose there are k-reverse multiples; that is, suppose a tree exists. There is a $2i+2$-digit or a $2i+3$-digit number satisfying (2) if and only if the tree contains at the i, $i+1$, and $i+2$ levels, respectively,



where, in the second case, $B = (gs - t)/(k - 1)$. In these cases, x is given, respectively, by

$$x = a_{n-1}a_{n-2} \dots a_{n-1-i}a_i \dots a_1a_0 \qquad n = 2i + 2$$
$$x = b_{n-1}b_{n-2} \dots b_{n-1-i}Bb_i \dots b_1b_0 \qquad n = 2i + 3. \quad \square$$

Theorem 1 shows the connection between a rooted tree and k-reverse multiples. A node of the form (r, r) gives rise to a k-reverse multiple with an even number of digits. Consecutive nodes (s, t) and (t, s) produce a multiple with an odd number of digits. The following example illustrates the use of this theorem.

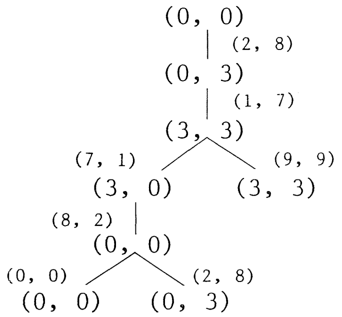
Example 1: $g = 10$, $k = 4$.

We begin by letting $r_{n-1} = r_{-1} = 0$ in (4) and solve the system:

$$\begin{aligned} 4a_0 \quad + 0 \quad &= a_{n-1} + 10r_0 \\ 4a_{n-1} + r_{n-2} &= a_0 \quad + \quad 0. \end{aligned}$$

The only solution is $r_{n-2} = 0$, $r_0 = 3$, $a_{n-1} = 2$, and $a_0 = 8$. This gives the node and edge labels for the first level of the tree. We continue in this manner and obtain the following pruned tree:

(6)



The tree is not continued any further since (0, 0), (0, 3), and (3, 3) have appeared previously.

Observe that the node label (0, 0) follows (0, 0) at level 5, but not at level 1. This will always be the case since the equations in (4) are satisfied by the trivial or zero solution. Although $r_0 \neq 0$, the node label (0, 0) is permissible after the first level.

By Theorem 1, the node (3, 3) at the second level gives rise to the 4-digit 4-reverse multiple 2178. Moreover, the consecutive nodes (3, 3) and (3, 3) produce the 5-digit multiple 21978. Extending this portion of the pruned tree shows that all numbers of the form 219...978 are 4-reverse multiples. Thus, there are n-digit 4-reverse multiples for all $n \geq 4$.

The relationship between the node and edge labels and verifying that a specific base g number x is, in fact, a k-reverse multiple may be demonstrated by performing base g multiplication of x by k, explicitly indicating all carries from one digit to the next. It should be noted that when some x is known to be a k-reverse multiple this computation provides an alternate way to obtain some of the node labels.

For example, 21782178 is a base 10 4-reverse multiple [corresponding to the path from the root to node (0, 0) at level 4 in (6) above]. The multiplication verifying this fact is:

$$\begin{array}{cccccccc}
{\scriptstyle 0} & {\scriptstyle 3} & {\scriptstyle 3} & {\scriptstyle 0} & {\scriptstyle 0} & {\scriptstyle 3} & {\scriptstyle 3} & {\scriptstyle 0} \\
2 & 1 & 7 & 8 & 2 & 1 & 7 & 8 \\
 & & & & & & \times & 4 \\
\hline
8 & 7 & 1 & 2 & 8 & 7 & 1 & 2
\end{array}$$

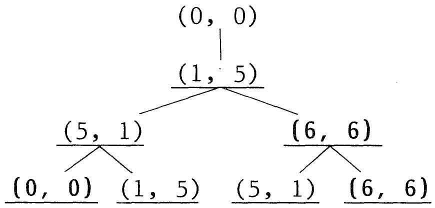
The carries from the node pairs and the digits of x form the edge labels.

From Theorem 1, the digits of 21782178 are the first elements of the edge labels from the root to node (0, 0) at level 4 followed by the second elements for the same edge labels taken from node (0, 0) at level 4 back up to the root. Similarly, the carry numbers noted above the digits of x are the elements of the node labels along the path. The first four carries are the first elements of the node labels from level 1 to level 4, and the second four carries are the second elements of the same node labels from level 3 back up to level 0. The root is always labeled (0, 0) and by Theorem 1 (since 21782178 has an even number of digits) the node label at level 4 must have both digits the same. □

The following examples illustrate some characteristics exhibited by trees for k-reverse multiples like the one shown in (6). We will use bold type for a node that determines a k-reverse multiple with an even number of digits and underlining for one that determines a k-multiple with an odd number of digits. Further, since we recognize the existence of k-reverse multiples graphically by particular types of node labels, we will omit the edge labels. There is no loss in doing this, for we may always use (4) to solve for

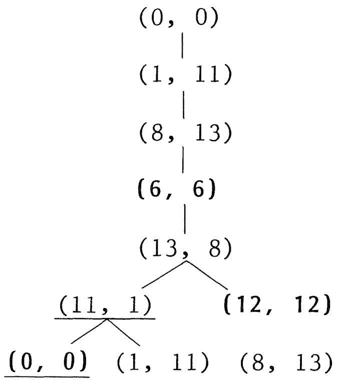
$$a_{n-1-i} = (kr_{n-1-i}g - kr_{n-2-i} + r_i g - r_{i-1})/(k^2 - 1),$$
$$a_i = (kr_i g - kr_{i-1} + r_{n-1-i}g - r_{n-2-i})/(k^2 - 1).$$

Example 2: $g = 11$, $k = 7$.



By Theorem 1, the node (1, 5) along with its child (5, 1) determines a 3-digit multiple and (6, 6), a 4-digit one. Both (5, 1), with its child (1, 5), and (6, 6), with its child (6, 6), give rise to 5-digit multiples. In fact, there are n-digit 7-reverse multiples for $n \geq 3$. □

Example 3: $g = 19$, $k = 14$.



In this case, there are n-digit 14-reverse multiples for $n = 6$ and $n \geq 10$. □

Although we require $r_i < g$, in the examples above it happens that $r_i < k$. In [3] this was shown always to be the case.

In many instances the entire pruned tree can be determined from just an initial branch. The following theorem gives one way in which this can be done.

Theorem 2: If
$$\begin{tikzcd}(r,\ s) \arrow[d, dash, "(a,\ b)"] \\ (u,\ v)\end{tikzcd}$$
then
$$\begin{tikzcd}(v,\ u) \arrow[d, dash, "(b,\ a)"] \\ (s,\ r)\end{tikzcd}$$
.

Proof: By hypothesis, the equations in (4) must be satisfied. Switching the order of the two equations gives the desired result. □

As an illustration of Theorem 2, consider the tree in Example 3. Suppose we know

$$\begin{tikzcd}(0,\ 0) \arrow[d, dash] \\ (1,\ 11) \arrow[d, dash] \\ (8,\ 13) \arrow[d, dash] \\ (6,\ 6)\end{tikzcd}$$

Then Theorem 2 allows us to derive

$$\begin{tikzcd}(6,\ 6) \arrow[d, dash] \\ (13,\ 8) \arrow[d, dash] \\ (11,\ 1) \arrow[d, dash] \\ (0,\ 0)\end{tikzcd}$$

immediately without using (4).

We will use the notation

$$\begin{tikzcd}\lbrack r,\ s\rbrack \arrow[d, dash, "\lbrack a,\ b\rbrack"] \\ \lbrack u,\ v\rbrack\end{tikzcd} \tag{7}$$

to indicate solely that the equations in (4) are satisfied by integers; that is,

$$\begin{cases} kb + s = a + vg, \\ ka + u = b + rg. \end{cases} \tag{8}$$

Thus, the notation in (7) does not imply that the integers are nonnegative and less than g. As before, when these latter restrictions do occur, we will use the (., .) notation instead of [., .]. The next two technical lemmas will be useful in the theorems that follow.

Lemma 1: Suppose there are integers such that

$$\begin{tikzcd}\lbrack r,\ s\rbrack \arrow[d, dash, "\lbrack a,\ b\rbrack"] \\ \lbrack u,\ v\rbrack\end{tikzcd}$$

with s, $u < g$ and $0 < r$, v. Then $0 < a$, b.

Proof: Eliminating b from the equations in (8) and rearranging, we find

$$a(k^2 - 1) = k(rg - u) + (vg - s).$$

Thus, given the hypotheses, $0 < a$. Similarly, $0 < b$. □

Lemma 2: Suppose there are integers such that

$$\begin{array}{l} [r,\ s] \\ \quad \Big|\ [a,\ b] \\ [u,\ v] \end{array}$$

with

$$(10) \qquad \begin{cases} 0 \le s,\ u, \\ r,\ v < k, \\ r \ne k - 1,\ v \ne k - 1,\ s \ne 0, \text{ or } u \ne 0. \end{cases}$$

Then $a,\ b < g$.

Proof: From (9) we have

$$\begin{aligned} a(k^2 - 1) &= krg - ku + vg - s \\ &\le g(kr + v) \\ &\le g(k(k - 1) + (k - 1)) \\ &= g(k^2 - 1). \end{aligned}$$

Given the restrictions in the third part of (10), one of the above two inequalities must be strict. Thus, $a < g$. Similarly, $b < g$. □

Theorem 3: If there are integers such that

$$(11) \qquad \begin{array}{l} (r,\ s) \\ \quad \Big|\ (a,\ b) \\ (u,\ v) \end{array} \quad \text{and} \quad \begin{array}{l} (r',\ s') \\ \quad \Big|\ (a',\ b') \\ (u',\ v') \end{array}$$

then

$$(12) \qquad \begin{array}{l} (r + r',\ s + s') \\ \qquad\quad \Big|\ (a + a',\ b + b') \\ (u + u',\ v + v') \end{array}$$

so long as

$$\begin{cases} s + s',\ u + u' < g, \\ r + r',\ v + v' < k, \\ r + r' \ne k - 1,\ v + v' \ne k - 1,\ s + s' \ne 0, \text{ or } u + u' \ne 0. \end{cases}$$

Proof: By hypothesis, (8) must be satisfied by $r, s, \ldots,$ and by $r', s', \ldots$. Adding the corresponding equations gives the desired equations for (12). Since all the numbers in (11) are nonnegative, those in (12) must be also. By Lemma 2, $a + a'$ and $b + b'$ must be less than g. □

Theorem 4: If there are integers such that

$$(13) \qquad \begin{array}{l} (r,\ s) \\ \quad \Big|\ (a,\ b) \\ (u,\ v) \end{array} \quad \text{and} \quad \begin{array}{l} (r',\ s') \\ \quad \Big|\ (a',\ b') \\ (u',\ v') \end{array}$$

then

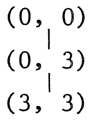
$$(14) \qquad \begin{array}{l} (r - r',\ s - s') \\ \qquad\quad \Big|\ (a - a',\ b - b') \\ (u - u',\ v - v') \end{array}$$

so long as

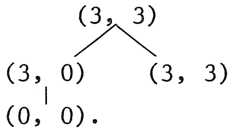
$$\begin{cases} 0 \le s - s',\ u - u', \\ 0 < r - r',\ v - v'. \end{cases}$$

Proof: By hypothesis, (8) must be satisfied by r, s, ..., and by r', s', ... Subtracting the corresponding equations gives the desired equations for (14). Since all the integers in (13) are less than g, those in (14) must be also. By Lemma 1, $a - a'$ and $b - b'$ are positive. □

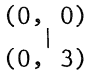
The above theorems allow the completion of all or at least large portions of a pruned tree when only an initial piece is known. Suppose, in Example 1, only

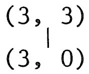
(15) 

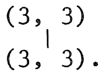
were known. We would be able immediately to derive the rest:



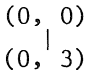
The left side follows from Theorem 2; the right from Theorem 3, since

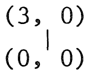


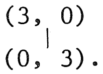
and 

imply 

Note that by the restrictions in Lemma 2,



and 

do not imply 

Thus, we are able to derive the entire pruned tree for Example 1 knowing only (15) or, equivalently, knowing only that 2178 is a 4-reverse multiple. Similarly, a careful examination of the trees in Examples 2 and 3 shows that each follows, respectively, from the 3-digit number 118 and the 6-digit number 1 2 11 8 17 15.

It may sound very restrictive to assume that we know an initial portion of a tree. However, this is equivalent to assuming that a k-reverse multiple for a given g is known. The problem then is to find or characterize all other multiples and this is done using the associated pruned tree. Hence, if we know an n-digit k-reverse multiple for some small n, then we do know an initial portion of the tree. The problem is then to complete the tree quickly and easily. As an illustration, consider the following, more complicated, example.

Example 4: $g = 44$, $k = 27$.

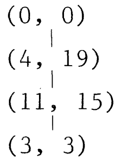
The 6-digit number

(16) 1 7 18 5 24 31

is a base 44, 27-reverse multiple; this can be verified through multiplication:

$$\begin{array}{rrrrrr} {}^{4} & {}^{11} & {}^{3} & {}^{15} & {}^{19} & \\ 1 & 7 & 18 & 5 & 24 & 31 \\ & & & & & \times\ 27 \\ \hline 31 & 24 & 5 & 18 & 7 & 1 \end{array}$$

The carry numbers are numbers in the node labels of the initial portion of the tree, so we have

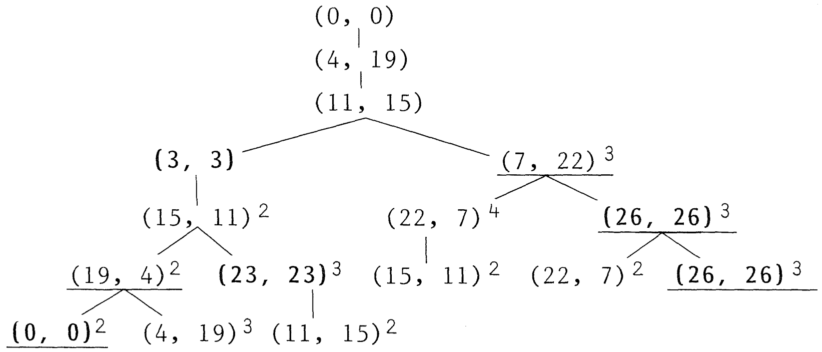


We complete the tree using the above theorems. For example, by Theorem 3

$$\begin{array}{c}(4,\ 19)\\ |\\ (11,\ 15)\end{array} \quad \text{and} \quad \begin{array}{c}(3,\ 3)\\ |\\ (15,\ 11)\end{array} \quad \text{imply} \quad \begin{array}{c}(7,\ 22)\\ |\\ (26,\ 26)\end{array}$$

In the tree that follows, the superscript j on a particular node indicates that it was derived using Theorem j, $j = 2, 3, 4$. So in the above case, we would write $(26, 26)^3$.

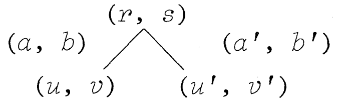
(17)



Note that the theorems above do not guarantee that the pruned tree of (17) is complete and that no branches are missing. The next theorem addresses this concern.

Theorem 5: Suppose g has a k-reverse multiple; further, suppose the tree contains

(18)



where $u > u'$ and $v \leq v'$. Then

$$\begin{array}{l}[0,\ 0]\\ \quad\Big|\ [a - a',\ b - b']\\ [u - u',\ v - v']\end{array}$$

where $0 < u - u' < k$, $-k < v - v' \leq 0$, $-g < a - a' < 0$ and $-g < b - b' < 0$.

Proof: Recall that if (18) occurs in a tree, then each number in the node label must be less than k and each number in the edge label must be less than g. Thus, all the claims in the conclusion follow immediately except for $a - a'$, $b - b' < 0$. From (9) we know that

$$a - a' = (-k(u - u') + (v - v')g)/(k^2 - 1).$$

Hence, $a - a' < 0$. Similarly, $b - b' < 0$. □

Suppose, for a given g, that we know some k-reverse multiple and thus are able to obtain the initial portion of the tree. We apply Theorems 2, 3, and 4 whenever possible until all branches end with nodes that have appeared previously. At this point, we are in the position of asking if there are any missing branches. By Theorem 5, if there are *no* integers c, d, t, w for which

(19a)
$$\begin{tikzcd} {[0,\ 0]} \arrow[d, dash, "{[-c,\ -d]}"] \\ {[t,\ -w]} \end{tikzcd}$$

where

(19b) $0 < t < k,\ 0 \le w < k,\ 0 < c < g,\ 0 < d < g,$

then we can be assured that there are *no* missing branches in the tree.

In all the examples considered thus far, (19) is never satisfied. To verify this for Example 1, we must consider the equations

$$(20)\qquad \begin{aligned} -4d &= -c - 10w \\ -4c + t &= -d. \end{aligned}$$

obtained from equations (4). Eliminating d in (20) gives $4t = 15c - 10w$; thus, $5|t$. However, $0 < t < 5$. Consequently, there are no solutions to (20) and, hence, to (19). Thus, by Theorem 5, the tree in (6) is complete.

Theorem 6: Suppose g has a k-reverse multiple and the tree contains

$$\begin{tikzcd} (r,\ s) \arrow[d, dash, "{(a,\ b)}"] \\ (u,\ v) \end{tikzcd}$$

Further, suppose

$$\begin{tikzcd} {[0,\ 0]} \arrow[d, dash, "{[-c,\ -d]}"] \\ {[t,\ -w]} \end{tikzcd}$$

with $0 < t < k$, $0 \le w < k$, $0 < c < g$, and $0 < d < g$. Then

$$\begin{tikzcd} (r,\ s) \arrow[d, dash, "{(a - c,\ b - d)}"] \\ (u + t,\ v - w) \end{tikzcd} \qquad \text{or} \qquad \begin{tikzcd} (r,\ s) \arrow[d, dash, "{(a + c,\ b + d)}"] \\ (u - t,\ v + w) \end{tikzcd}$$

so long as either the three conditions $u + t < g$, $0 < v - w$, and $0 < r$ or the two conditions $0 < u - t$ and $v + w < k$ are fulfilled.

Proof: The first piece follows from Lemma 1; the second from Lemma 2. □

The following example illustrates the use of Theorem 6.

Example 5: $g = 40$, $k = 13$.

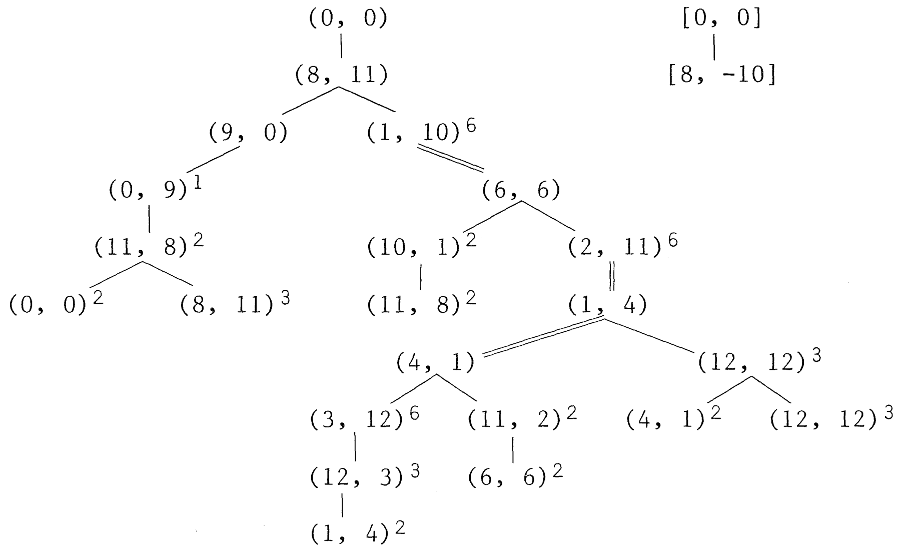
The 5-digit number

(21) 2 24 30 1 34

is a 13-reverse multiple. As in Example 4, the number in (21) gives the initial portion of the tree which has node labels (0, 0), (8, 11), and (9, 0). There is just one solution to (19); namely,

$$\begin{tikzcd} {[0,\ 0]} \arrow[d, dash] \\ {[8,\ -10].} \end{tikzcd}$$

We now use Theorems 2, 3, 4, and 6 to complete the tree:



The double bar edges leading to nodes without a superscript indicate that none of the above theorems apply. In these cases the nodes were found using (4). Note that there are only 3 such instances. On the other hand, the 16 superscripted nodes were found easily using the theorems indicated by the superscript as in Example 4.

As we have noted, there is just one solution to (19). We used this solution in conjunction with Theorem 6 to find 3 nodes. If the tree contained any missing nodes, then by Theorem 5 equations (19) would have another solution. Since that is not the case, the tree is complete.

Acknowledgment

The author is grateful to the referee for many helpful suggestions.

References

1. C. A. Grimm & D. W. Ballew. "Reversible Multiples." *J. Rec. Math.* *8* (1975-1976):89-91.
2. L. F. Klosinski & D. C. Smolarski. "On the Reversing of Digits." *Math. Mag.* *42* (1969):208-10.
3. Anne Ludington Young. "k-Reverse Multiples." *Fibonacci Quarterly* *30.2* (1992):126-32.
4. Alan Sutcliffe. "Integers That Are Multiplied When Their Digits Are Reversed." *Math. Mag.* *39* (1966):282-87.

*****

ON REPRESENTATIONS OF NUMBERS BY SUMS OF TWO TRIANGULAR NUMBERS

John A. Ewell
Northern Illinois University, DeKalb, IL 60115

(Submitted July 1990)

1. Introduction

We begin our discussion with a definition.

Definition: As usual,

$$Z:=\{0,\ \pm1,\ \pm2,\ \dots\},\quad N:=\{0,\ 1,\ 2,\ \dots\},\quad P:=N\backslash\{0\}.$$

Then, for each $n \in N$,

$$r_2(n) := |\{(x,\ y) \in Z^2 | n = x^2 + y^2\}|,$$

$$t_2(n) := |\{(x,\ y) \in N^2 | n = x(x+1)/2 + y(y+1)/2\}|.$$

Also, for each $n \in P$ and each $i \in \{1,\ 3\}$,

$$d_i(n) = \sum_{\substack{d|n \\ d \equiv i \pmod 4}} 1.$$

We can now state two theorems.

Theorem 1 (Jacobi): For each $n \in P$,

$$r_2(n) = 4\{d_1(n) - d_3(n)\}.$$

Theorem 2: For each $n \in N$,

$$t_2(n) = d_1(4n+1) - d_3(4n+1).$$

Clearly, $r_2(0) = t_2(0) = 1$. Next, we observe that, for positive integers, Theorem 2 can be deduced from Theorem 1. In this note we give an independent proof of Theorem 2. Our proof is based on the triple-product identity

$$(1)\qquad \prod_1^\infty (1 - x^{2n})(1 - ax^{2n-1})(1 - a^{-1}x^{2n-1}) = \sum_{-\infty}^{\infty} (-1)^n x^{n^2} a^n,$$

which is valid for each pair of complex numbers a, x such that $a \neq 0$ and $|x| < 1$. Hirschhorn [2] showed how to deduce Jacobi's theorem from the triple-product identity. The reader will doubtless note that our method is similar to that of Hirschhorn.

2. Proof of Theorem 2

Separating even and odd terms on the right side of (1), and then again using (1) to replace the series in the resulting identity by infinite products, we get

$$\prod_1^\infty (1 - x^{2n})(1 - ax^{2n-1})(1 - a^{-1}x^{2n-1})$$

$$= \sum_{-\infty}^{\infty} x^{4n^2} a^{2n} - ax \sum_{-\infty}^{\infty} x^{4n(n+1)} a^{2n}$$

$$= \prod_1^\infty (1 - x^{8n})(1 + a^2x^{8n-4})(1 + a^{-2}x^{8n-4})$$

$$- (a + a^{-1})x \prod_1^\infty (1 - x^{8n})(1 + a^2x^{8n})(1 + a^{-2}x^{8n}).$$

With D_a denoting derivation with respect to a, we then operate on both sides of the foregoing identity with aD_a to get

$$(2)\quad -\prod_1^\infty(1-x^{2n})(1-ax^{2n-1})(1-a^{-1}x^{2n-1})\sum_1^\infty v_k(x)(a^k-a^{-k})$$
$$= 2\prod_1^\infty(1-x^{8n})(1+a^2x^{8n-4})(1+a^{-2}x^{8n-4})\sum_1^\infty(-1)^{k-1}v_k(x^4)(a^{2k}-a^{-2k})$$
$$-(a-a^{-1})x\prod_1^\infty(1-x^{8n})(1+a^{-2}x^{8n})(1+a^{-2}x^{8n})$$
$$-(a+a^{-1})2x\prod_1^\infty(1-x^{8n})(1+a^2x^{8n})(1+a^{-2}x^{8n})\sum_1^\infty(-1)^{k-1}u_k(x^8)(a^{2k}-a^{-2k}),$$

where, for convenience $u_k(x) := x^k \cdot (1-x^k)^{-1}$, $v_k(x) := x^k \cdot (1-x^{2k})^{-1}$, $k \in P$, and x is a complex number with $|x| < 1$. Now, in (2), let $a = i$ and divide the resulting identity by $-2i$ to get

$$\prod_1^\infty(1-x^{2n})(1+x^{4n-2})\sum_0^\infty(-1)^k v_{2k+1}(x) = x\prod_1^\infty(1-x^{8n})^3,$$

or, equivalently,

$$x\prod_1^\infty\frac{(1-x^{8n})^3}{(1-x^{2n})(1+x^{4n-2})} = \sum_0^\infty(-1)^k\frac{x^{2k+1}}{1-x^{4k+2}}.$$

Hence,

$$x\prod_1^\infty\frac{(1-x^{8n})^2}{(1-x^{8n-4})^2} = \sum_0^\infty(-1)^k\frac{x^{2k+1}}{1-x^{4k+2}} = \sum_{k=0}^\infty(-1)^k\sum_{j=0}^\infty x^{(2j+1)(2k+1)}.$$

Owing to a well-known identity of Gauss ([1], p. 284), it then follows that

$$\sum_0^\infty t_2(n)x^{4n+1} = x\left\{\sum_0^\infty x^{2n(n+1)}\right\}^2 = x\prod_1^\infty\frac{(1-x^{8n})^2}{(1-x^{8n-4})^2}$$
$$= \sum_{k=0}^\infty(-1)^k\sum_{j=0}^\infty x^{(2j+1)(2k+1)} = \sum_{m=0}^\infty x^{2m+1}\sum_{d|2m+1}(-1)^{(d-1)/2}$$
$$= \sum_{n=0}^\infty x^{4n+1}\sum_{d|4n+1}(-1)^{(d-1)/2} + \sum_{n=0}^\infty x^{4n+3}\sum_{d|4n+3}(-1)^{(d-1)/2}.$$

Equating coefficients of like powers of x, we get, for each $n \in \mathbb{N}$,

$$t_2(n) = \sum_{d|4n+1}(-1)^{(d-1)/2} = \sum_{\substack{d|4n+1\\ d\equiv 1 \pmod 4}} 1 - \sum_{\substack{d|4n+1\\ d\equiv 3 \pmod 4}} 1$$
$$= d_1(4n+1) - d_3(4n+1),$$

$$\sum_{d|4n+3}(-1)^{(d-1)/2} = 0.$$

This proves Theorem 2. In passing we note that the second conclusion follows easily from the following independent argument. For each $n \in \mathbb{N}$ and each divisor d (and codivisor d') of $4n+3$, exactly one of the pair (d, d') is $\equiv 1 \pmod 4$ and exactly one is $\equiv 3 \pmod 4$. Hence,

$$(-1)^{(d-1)/2} + (-1)^{(d'-1)/2} = 0.$$

Summing over all of these pairs, we obtain the desired result.

Finally, we prove that Theorems 1 and 2 are actually *equivalent*. To this end, we first recall the following well-known result.

Theorem: For an arbitrary positive integer $n > 1$, let

$$n = \prod_{i=1}^{i=r} p_i^{e_i}$$

denote its prime-power decomposition. Then, n is representable as a sum of two squares if and only if, for each $i \in \{1, 2, \ldots, r\}$ such that $p_i \equiv 3 \pmod 4$, e_i is even.

It then follows that counting representations of positive integers by sums of two squares can be restricted to positive integers of the form $2^f(4k + 1)$, $f, k \in \mathbb{N}$. Equivalence of Theorems 1 and 2 will then be an easy consequence of the following lemma.

Lemma: If for each $k \in \mathbb{N}$,

$$S = S(k) := \{(x, y) \in \mathbb{N} \times \mathbb{P} \mid 4k + 1 = x^2 + y^2\}$$

and

$$T = T(k) := \{(i, j) \in \mathbb{N}^2 \mid k = i(i + 1)/2 + j(j + 1)/2\},$$

then

$$|S| = |T|.$$

Proof: To see this we define a function $\theta : T \to S$ as follows: for each $(i, j) \in T$,

$$\theta(i, j) := \begin{cases} (0, 2i + 1), & \text{if } i = j, \\ (i - j, i + j + 1), & \text{if } i > j, \\ (i + j + 1, j - i), & \text{if } i < j. \end{cases}$$

Simple calculation reveals that θ is single-valued, and always $\theta(i, j) \in S$. So, we proceed to show that θ is one-to-one from T onto S.

Suppose that (g, h), $(i, j) \in T$, and $\theta(g, h) = \theta(i, j)$. If (a) $g = h$, then

$$\theta(g, h) := (0, 2g + 1).$$

Therefore, $\theta(i, j) \in \mathbb{N} \times \mathbb{P}$ must also have first coordinate equal to 0: that is, $\theta(i, j) = (0, y)$, with $i = j$ and $y = 2i + 1$. So, $2g + 1 = 2i + 1$, whence $g = i$, whence $g = h = i = j$, whence $(g, h) = (i, j)$. If (b) $g > h$, then

$$\theta(g, h) := (g - h, g + h + 1).$$

Therefore, $\theta(i, j) = (x, y) \in \mathbb{P}^2$, with $x < y$, whence $x = i - j$ and $y = i + j + 1$, whence $i - j = g - h$ and $i + j + 1 = g + h + 1$, whence $(i, j) = (g, h)$. If (c) $g < h$, then

$$\theta(g, h) := (g + h + 1, h - g).$$

As before, we must have:

$$g + h = i + j \quad \text{and} \quad -g + h = -i + j,$$

whence $(g, h) = (i, j)$. Thus, θ is one-to-one.

Pick any $(x, y) \in S(k)$, and split two cases: (i) $x = 0$ or (ii) $x > 0$. Under (i) we have

$$4k + 1 = 0^2 + y^2, \text{ whence } y = 2i + 1, \text{ for some } i \in \mathbb{N}.$$

Hence, for $i = j := (y - 1)/2$, we have

$$(x, y) = (0, 2i + 1) = \theta(i, j), \text{ where } (i, j) \in T(k).$$

Under case (ii) we split two further subcases: (ii′) $x < y$ or (ii″) $x > y$. Then under (ii′) we put $i - j = x$ and $i + j + 1 = y$ to find

$$i = (x + y - 1)/2 \quad \text{and} \quad j = (-x + y - 1)/2.$$

Thus, $i > j$, $i - j = x$, and $i + j + 1 = y$, whence $(x, y) = \theta(i, j)$. [Clearly, $(i, j) \in T(k)$.] Under (ii″) we put $i + j + 1 = x$ and $-i + j = y$ to find

$$i = (x - y - 1)/2 \quad \text{and} \quad j = (x + y - 1)/2.$$

As before, $i < j$ and $(x, y) = \theta(i, j)$, where $(i, j) \in T(k)$. This proves that θ is onto S.

Now let us assume that Theorem 2 holds. Then, for each $k \in \mathbf{N}$,

$$|S(k)| = |T(k)| = d_1(4k + 1) - d_3(4k + 1).$$

Therefore,

$$\begin{aligned} r_2(4k + 1) &= |\{(x, y) \in \mathbf{Z}^2 | 4k + 1 = x^2 + y^2\}| \\ &= 4\{d_1(4k + 1) - d_3(4k + 1)\}, \end{aligned}$$

since each solution $(x, y) \in S$ yields 4 solutions $(\pm x, \pm y) \in \mathbf{Z}^2$.

Conversely, let us assume that Theorem 1 holds. Then, for each $k \in \mathbf{N}$,

$$|S(k)| = r_2(4k + 1)/4 = d_1(4k + 1) - d_3(4k + 1),$$

whence (owing to our Lemma),

$$t_2(k) := |T(k)| = d_1(4k + 1) - d_3(4k + 1),$$

as well.

Since $r_2(2^f(4k + 1)) = r_2(4k + 1)$, equivalence of Theorems 1 and 2 follows.

Owing to the equivalence of the two theorems, our proof of Theorem 2 is a new one for both theorems.

Acknowledgment

The author would like to thank the referee for suggested improvement of the exposition.

References

1. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*. 4th ed. Oxford: Clarendon Press, 1960.
2. M. D. Hirschhorn. "A Simple Proof of Jacobi's Two-Square Theorem." *Amer. Math. Monthly 92* (1985):579-80.

*****

ACCELERATION OF THE SUM OF FIBONACCI RECIPROCALS

Peter Griffin
California State University, Sacramento, CA 95819

(Submitted July 1990)

The topic of Aitken acceleration (sometimes called "Aitken's Δ^2 process") appears in many numerical analysis texts but is usually confined to the solution of equations by fixed-point iteration. (Interesting examples of this occur in [4] and [6], wherein $x = 1 + 1/x$, equivalent to the characteristic equation of the Fibonacci difference relation, is solved by iteration.) Conspicuous in suggesting its applicability in other contexts are [1], [2], [5], and [7].

Briefly, a convergent sequence $x_1, x_2, \ldots, x_n$ with limit x is amenable to acceleration if the ratio of consecutive errors is approximately constant $(x - x_n)/(x - x_{n-1}) \sim r$. It follows that r is approximately the ratio of consecutive differences $r \sim (x_n - x_{n-1})/(x_{n-1} - x_{n-2})$. Substituting this value of r into the approximation for the ratio of errors, solving for x, and relabeling x as x_n^* yields the more rapidly converging sequence

$$x_n^* = x_n - (x_n - x_{n-1})^2/(x_n - 2x_{n-1} + x_{n-2}) = x_n - (\Delta_n)^2/\Delta_n^2,$$

where the second form uses the Δ notation for first and second differences,

$$\Delta_n = x_n - x_{n-1} \quad \text{and} \quad \Delta_n^2 = \Delta_n - \Delta_{n-1}.$$

An occasionally mentioned use other than functional iteration is the accelerated convergence of Taylor series [5], often possible because of the behavior of the error term. A trivial but revealing example of this is the geometric series; acceleration of any three consecutive partial sums takes us directly to the limit since the ratio of errors (or differences) is, in fact, exactly constant.

Because of its intriguing resemblance to a geometric series, the sum of Fibonacci reciprocals provides a dramatic illustration of both the increase in speed of convergence attainable and the rarely mentioned possibilities of repeated acceleration. To be sure, in 1972 Brousseau achieved at least 83-digit accuracy in

$$S = \sum_{j=1}^{\infty} 1/F_j = 3.3598856662\ldots$$

by evaluating $S_{400} = \sum_{j=1}^{400} 1/F_j$ to 400 digits (see [3] for an extensive bibliography), but this need not detract from what can be learned by pursuing this example.

Although $S_7 = 5047/1560 = 3.235\ldots$ has a relative error of 4%, it and the six previous partial sums themselves can be accelerated with pencil-and-paper arithmetic to produce $1391/414 = 3.359903\ldots$, with relative error only .0005%. Accelerating the information provided by the first seven terms has reduced the inaccuracy in our estimate of S by a factor of 7000.

$x_n = S_n$	Δ_n	Δ_n^2	x_n^*	Δ_n^*	Δ_n^{2*}	x_n^{**}	Δ_n^{**}	Δ_n^{2**}	x_n^{***}
1									
2	1/1								
5/2	1/2	-1/2	3						
17/6	1/3	-1/6	7/2	1/2					
91/30	1/5	-2/15	10/3	-1/6	-2/3	27/8			
279/120	1/8	-3/40	101/30	1/30	1/5	121/36	-1/72		
5047/1560	1/13	-5/104	403/120	-1/120	-1/24	84/25	-1/900	23/1800	1391/414

Observe that the ratios of consecutive differences are close to $1/\alpha$, $-1/\alpha^3$, and $1/\alpha^5$ in the three stages of acceleration, where $\alpha = (\sqrt{5} + 1)/2 = 1.618\ldots$.

An explanation for this lies in the Binet formula for the j^{th} Fibonacci number

$$F_j = \alpha^j(1 - (-1/\alpha^2)^j)/\sqrt{5},$$

from which

$$1/F_j = \frac{\sqrt{5}}{\alpha^j}\sum_{k=0}^{\infty}(-1/\alpha^2)^{jk}.$$

Thus, a partial sum is given by

$$S_n = \sum_{j=1}^{n} 1/F_j = \sqrt{5}\sum_{k=0}^{\infty}\sum_{j=1}^{n}(-1)^{jk}/\alpha^{(2k+1)j}$$

and the error, or tail, is the double sum

$$S - S_n = \sqrt{5}\sum_{k=0}^{\infty}\sum_{j=n+1}^{\infty}(-1)^{jk}/\alpha^{(2k+1)j} = \sqrt{5}\sum_{k=0}^{\infty}\frac{(-1)^{k+kn}}{(\alpha^{2k+1} - (-1)^k)(\alpha^{2k+1})^n}.$$

Each stage of the acceleration will eliminate the currently dominant component of the error term, in this case successively peeling off those of order $(1/\alpha)^n$, $(-1/\alpha^3)^n$, $(1/\alpha^5)^n$, etc. [7]. Generally, if the error in a sequence is $\sum c_i a_i^n$, with $1 > |a_1| > |a_2| > \cdots$, then acceleration changes the error by removing the a_1 term, altering the coefficients of the other a_i^n, and possibly introducing new terms of order

$$\left[\prod_j (a_j/a_1)^{k_j} a_i\right]^n < a_2^n.$$

In the Fibonacci case the orders of the new terms happen to coincide with those of terms already present. Acton [1] points out that when convergence is near, roundoff error can be amplified by the process, causing later accelerations to wander off the mark.

Another possibility for approximating S is to correct the partial sums S_n by estimating their tails as α/F_n, making use of the well-known asymptotic $F_{n+j} \sim \alpha^j F_n$ (the inherent "geometric" character of the Fibonacci reciprocals). For example, $S_7 + \alpha/F_7 = 3.35972\ldots$ is already quite good, and repeated acceleration of the first seven such corrected terms produces 3.35988567, competitive with four accelerations of the first nine partial sums themselves, the correction being equivalent to starting with one acceleration already achieved.

Incidentally, passing to the limit in the expression for S_n gives an alternative formula for S itself, apparently not widely known:

$$S = \sum_{j=1}^{\infty} 1/F_j = \sqrt{5}\sum_{k=0}^{\infty}\frac{(-1)^k}{\alpha^{2k+1} - (-1)^k}$$

$$= \sqrt{5}[1/(\alpha - 1) - 1/(\alpha^3 + 1) + 1/(\alpha^5 - 1) - \cdots].$$

And yes, this too can be accelerated, about as well as $S_n + \alpha/F_n$!

Acknowledgment

I would like to thank the referee for some helpful comments, including the observation that this final expression for S can also be derived by applying formula 4.17 from [3], with $q = -1$ and $\beta = -1/\alpha$.

Referemces

1. F. Acton. *Numerical Methods That Work.* New York: Harper & Row, 1970.
2. P. Henrici. *Essentials of Numerical Analysis.* New York: Wiley, 1982.
3. A. F. Horadam. "Elliptic Functions and Lambert Series in the Summation of Reciprocals in Certain Recurrence-Generated Sequences." *Fibonacci Quarterly 26.2* (1988):98-114.
4. M. Jamieson. "Fibonacci Numbers and Aitken Sequences Revisited." *Amer. Math. Monthly 97* (1990):829-31.
5. L. Johnson & R. Riess. *Numerical Analysis*. Reading, Mass.: Addison-Wesley, 1977.
6. G. Phillips. "Aitken Sequences and Fibonacci Numbers." *Amer. Math. Monthly 91* (1984):354-57.
7. J. Todd. *Survey of Numerical Analysis.* New York: McGraw-Hill, 1962.

*****

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 72717.3515@compuserve.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.

Dedication. This year's column is dedicated to **Dr. A. P. Hillman** in recognition of his 27 years of devoted service as editor of the Elementary Problems Section. Devotees of this column are invited to thank Abe by dedicating their next proposed problem to Dr. Hillman.

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-712 *Proposed by Herta T. Freitag, Roanoke, VA*

Prove that for all positive integers n, $\alpha(\sqrt{5}\alpha^n - L_{n+1})$ is a Lucas number.

B-713 *Proposed by Herta T. Freitag, Roanoke, VA*

Dedicated to Dr. A. P. Hillman

(a) Let S be a set of three consecutive Fibonacci numbers. In a Pythagorean triple, (a, b, c), a is the product of the elements in S; b is the product of two Fibonacci numbers (both larger than 1), one of them occurring in S; and c is the sum of the squares of two members of S. Determine the Pythagorean triple and prove that the area of the corresponding Pythagorean triangle is the product of four consecutive Fibonacci numbers.

(b) Same problem as part (a) except that Fibonacci numbers are replaced by Lucas numbers.

B-714 *Proposed by J. R. Goggins, Whiteinch, Glasgow, Scotland*

Dedicated to Dr. A. P. Hillman

Define a sequence G_n by $G_0 = 0$, $G_1 = 4$, and $G_{n+2} = 3G_{n+1} - G_n - 2$ for $n \geq 0$. Express G_n in terms of Fibonacci and/or Lucas numbers.

B-715 *Proposed by Piero Filipponi, Fond. U. Bordoni, Rome, Italy*

Dedicated to Dr. A. P. Hillman

Prove that if $s > 2$,

$$F_m \equiv 0 \pmod{F_s^2} \text{ if and only if } m \equiv 0 \pmod{sF_s}.$$

B-716 *Proposed by Stanley Rabinowitz, MathPro Press, Westford, MA*

Dedicated to Dr. A. P. Hillman

If a and b have the same parity, prove that $L_a + L_b$ cannot be a prime larger than 5.

B-717 *Proposed by L. Kuipers, Sierre, Switzerland*

Show that

$$\arctan\frac{2}{5} = \sum_{n=0}^{\infty}\frac{(-1)^n}{2n+1}\cdot\frac{L_{2n+1}}{2^{2n+1}}.$$

SOLUTIONS

Edited by A. P. Hillman

Differences in {1, 2}

B-688 *Proposed by Russell Euler, Northwest Missouri State U., Maryville, MO*

Find the number of increasing sequences of integers such that 1 is the first term, n is the last term, and the difference between successive terms is 1 or 2. [For example, if $n = 8$, then one such sequence is 1, 2, 3, 5, 6, 8 and another is 1, 3, 4, 6, 8.]

Solution by H.-J. Seiffert, Berlin, Germany

Let A_n denote the set of all sequences having the desired properties. If $|A_n|$ denotes the number of elements of A_n, then clearly $|A_1| = |A_2| = 1$. We shall prove that $|A_n| = F_n$. This is true for $n = 1, 2$. Assume that it holds for all $k \in \{1, \ldots, n-1\}$ $(n \geq 3)$. If B_n and C_n denote the set of all sequences of A_n, where the second term from the right equals $n-2$ and $n-1$, respectively, then we obviously have

$$|B_n| = |A_{n-2}| \quad\text{and}\quad |C_n| = |A_{n-1}|.$$

Since $A_n = B_n \cup C_n$ and $B_n \cap C_n = \emptyset$, the induction hypothesis gives

$$|A_n| = |B_n| + |C_n| = |A_{n-2}| + |A_{n-1}| = F_{n-2} + F_{n-1} = F_n.$$

This completes the induction proof.

Also solved by Charles Aschbacher, Glenn Bookhout, Paul S. Bruckman, Russell Jay Hendel, Douglas E. Iannucci, Norbert Jensen, Carl Libis, Ray Melham, Bob Prielipp, Sahib Singh, Lawrence Somer, Shanon Stamp, and the proposer.

Numbers with Even Zeckendorf Representations

B-689 *Proposed by Philip L. Mana, Albuquerque, NM*

Show that $F_n^2 - 1$ is a sum of Fibonacci numbers with distinct positive even subscripts for all integers $n \geq 3$.

Solution by Lawrence Somer, Washington, D.C.

It follows by identity I_{10} on page 56 of Hoggatt's *Fibonacci and Lucas Numbers* that

$$F_n^2 - F_{n-2}^2 = F_{2n-2}.$$

Thus,

$$F_n^2 - 1 = F_{2n-2} + (F_{n-2}^2 - 1).$$

The result now follows by induction upon noting that

$$F_3^2 - 1 = 2^2 - 1 = 3 = F_4 \quad \text{and} \quad F_4^2 - 1 = 3^2 - 1 = 8 = F_6.$$

Also solved by Paul S. Bruckman, Herta T. Freitag, Russell Jay Hendel, Douglas E. Iannucci, Norbert Jensen, Joseph J. Kostal, Ray Melham, Alex Necochea, Bob Prielipp, H.-J. Seiffert, Sahib Singh, and the proposer.

Golden Geometric Progressions

B-690 *Proposed by Herta T. Freitag, Roanoke, VA*

Let $S_k = \alpha^{10k+1} + \alpha^{10k+2} + \alpha^{10k+3} + \cdots + \alpha^{10k+10}$, where $\alpha = (1 + \sqrt{5})/2$. Find positive integers b and c such that $S_k/\alpha^{10k+b} = c$ for all nonnegative integers k.

Solution by Paul S. Bruckman, Edmonds, WA

$$S_k = \sum_{i=1}^{10} \alpha^{10k+i} = \alpha^{10k}\left(\frac{\alpha^{11} - \alpha}{\alpha - 1}\right) = \frac{\alpha^{10k+1}}{\alpha^{-1}}(\alpha^{10} - 1)$$

$$= \alpha^{10k+2} \cdot \alpha^5(\alpha^5 + \beta^5) = 11\alpha^{10k+7}.$$

We see that the values $b = 7$, $c = 11$ solve the problem.

Also solved by Tareq Al-Naffouri, Glenn Bookhout, Russell Jay Hendel, Norbert Jensen, Ray Melham, Bob Prielipp, H.-J. Seiffert, Sahib Singh, and the proposer.

Rectangles in Similar Rectangles

B-691 *Proposed by Heiko Harborth, Technische U. Braunschweig, W. Germany*

Herta T. Freitag asked whether a golden rectangle can be inscribed into a larger golden rectangle (all four vertices of the smaller are points on the sides of the larger one). An answer follows from the solution of the generalized problem: Which rectangles can be inscribed into larger similar rectangles?

Solution by Russell Jay Hendel, Dowling College, Oakdale, NY

All nonsquare rectangles can be inscribed in larger similar rectangles.

Indeed, suppose a given rectangle, R_1, has sides a and b with $a \neq b$. Set

$$c = \{\max(a, b)\}^2/\{\min(a, b)\}$$

and consider the rectangle, R_2, with sides $\max(a, b)$ and c.

R_2 is similar to R_1, because

$$c/\max(a, b) = \max(a, b)/\min(a, b),$$

R_1 can be inscribed in R_2, with common side $\max(a, b)$, because $c \geq \min(a, b)$, and R_2 is larger than R_1 because $c > \neq\min(a, b)$ when $a \neq b$. This completes the proof.

Editor's Note: The proposer made the tacit assumption that all the vertices of the smaller rectangle are *interior* points of the sides of the larger one. With this assumption, Paul S. Bruckman, Herta T. Freitag, and the proposer showed that the rectangles have to be squares.

A Fibonacci Factorization

B-692 *Proposed by Gregory Wulczyn, Lewisburg, PA*

Let $G(a, b, c) = -4 + L_{2a}^2 + L_{2b}^2 + L_{2c}^2 + L_{2a}L_{2b}L_{2c}$. Prove or disprove that each of F_{a+b+c}, F_{b+c-a}, F_{c+a-b}, and F_{a+b-c} is an integral divisor of $G(a, b, c)$ for all odd positive integers a, b, and c.

Solution by Russell Jay Hendel, Dowling College, Oakdale, NY

We prove the stronger assertion

$$25F_{a+b+c}F_{a+b-c}F_{a-b+c}F_{c+b-a} = L_{2a}L_{2b}L_{2c} + L_{2a}^2 + L_{2b}^2 + L_{2c}^2 - 4.$$

The proof is verbatim identical to the published solution to B-669, Vol. 29, no. 2, p. 185, with, however, the word *odd* replaced by *even*.

"From the identity

$$5F_{m+n}F_{m-n} = L_{2m} - (-1)^{m+n}L_{2n}$$

we get [setting $(-1)^{a+b+c} = \mathrm{e}$)

$$\begin{aligned}25F_{a+b+c}F_{a+b-c}F_{a-b+c}F_{c+b-a} &= [L_{2a+2b} - \mathrm{e}L_{2c}][L_{2c} - \mathrm{e}L_{2a-2b}]\\ &= L_{2c}[L_{2a+2b} + L_{2a-2b}] - \mathrm{e}L_{2c}^2 - \mathrm{e}L_{2a+2b}L_{2a-2b}\\ &= L_{2c}[L_{2a}L_{2b}] - \mathrm{e}L_{2c}^2 - \mathrm{e}[L_{4a} + L_{4b}]\\ &= L_{2a}L_{2b}L_{2c} - \mathrm{e}[L_{2a}^2 + L_{2b}^2 + L_{2c}^2 - 4],\end{aligned}$$

and for a, b, and c odd (actually for $a + b + c$ odd), the given identity is established."

Also solved by Paul S. Bruckman, Norbert Jensen, Bob Prielipp, and the proposer.

A Combinatorial Problem

B-693 *Proposed by Daniel C. Fielder & Cecil O. Alford, Georgia Tech, Atlanta, GA*

Let A consist of all pairs $\{x, y\}$ chosen from $\{1, 2, \ldots, 2n\}$, B consist of all pairs from $\{1, 2, \ldots, n\}$, and C of all pairs from $\{n + 1, n + 2, \ldots, 2n\}$. Let S consist of all sets $T = \{P_1, P_2, \ldots, P_k\}$ with the P_i (distinct) pairs in A. How many of the T in S satisfy at least one the the conditions:

(i) $P_i \cap P_j \neq \emptyset$ for some i and j, with $i \neq j$,

(ii) $P_i \in B$ for some i, or

(iii) $P_i \in C$ for some i?

Solution by Philip L. Mana, Albuquerque, NM

Let $C(n, k)$ denote $\binom{n}{k}$. There are $C(2n, 2)$ pairs in A; thus $C(C(2n, 2), k)$ sets T in S. The sets T meeting none of the conditions (i), (ii), (iii) can be written in the form

$$U = \{\{x_1, y_1\}, \{x_2, y_2\}, \ldots, \{x_k, y_k\}\}$$

with the x_i a set of k integers chosen from $\{1, 2, \ldots, n\}$ and satisfying

$$x_1 < x_2 < \cdots < x_k$$

and the y_i a permutation of k distinct integers from $\{n + 1, n + 2, \ldots, 2n\}$. The number of such sets U is

$$C(n, k)P(n, k) = k!\binom{n}{k}^2;$$

hence, the number of sets T satisfying at least one of the conditions is

$$C(C(2n, 2), k) - C(n, k)P(n, k).$$

Also solved by the proposers, who indicated that the problem arose in a combinatorial study in parallel processing.

*****

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-466 *Proposed by Paul S. Bruckman, Edmonds, WA*

Let p be a prime of the form $ax^2 + by^2$, where a and b are relatively prime natural numbers neither of which is divisible by p; x and y are integers. Prove that x and y are uniquely determined, except for trivial variations of sign.

H-467 *Proposed by Larry Taylor, Rego Park, NY*

Let (a_n, b_n, c_n) be a primitive Pythagorean triple for $n = 1, 2, 3, 4$ where a_n, b_n, c_n are positive integers and b_n is even. Let $p \equiv 1 \pmod 8$ be prime; $r^2 + s^2 \equiv t^2 \pmod p$ where the Legendre symbol

$$\left(\frac{(t + r)/2}{p}\right) = 1.$$

Solve the following twelve simultaneous congruences:

$$(a_1, b_1, c_1) \equiv (r, s, t),$$
$$(a_2, b_2, c_2) \equiv (r, s, -t),$$
$$(a_3, b_3, c_3) \equiv (s, r, t),$$
$$(a_4, b_4, c_4) \equiv (s, r, -t) \quad \pmod p.$$

For example, if $(r, s, t) \equiv (3, 4, 5) \pmod{17}$,

$$(a_1, b_1, c_1) = (3, 4, 5),$$
$$(a_2, b_2, c_2) = (105, 208, 233),$$
$$(a_3, b_3, c_3) = (667, 156, 685),$$
$$(a_4, b_4, c_4) = (21, 20, 29).$$

H-468 *Proposed by Lawrence Somer, Washington, DC*

Let $\{v_n\}_{n=0}^{\infty}$ be a Lucas sequence of the second kind satisfying the recursion relation

$$v_{n+2} = av_{n+1} + bv_n,$$

where a and b are positive odd integers and $v_0 = 2$, $v_1 = a$. Show that v_{2n} has an odd prime divisor $p \equiv 3 \pmod 4$ for $n \geq 1$. (This was proved by Sahib Singh for the special case of the recurrence $\{L_n\}$ on page 136 of the paper "Thoro's Conjecture and Allied Divisibility Property of Lucas Numbers" in the April 1980 issue of *The Fibonacci Quarterly*.)

SOLUTIONS

A Triggy Problem

H-466 *Proposed by J. A. Sjogren, U. of Santa Clara, Santa Clara, CA (Vol. 28, no. 4, November 1990)*

Establish the following result:

Let n be a whole number and, for any rational number q, let $[q]$ be the greatest integer contained in q. Then

$$f_n = \prod_{k=1}^{\left[\frac{n-1}{2}\right]}\left(3 + 2\cos\frac{2\pi k}{n}\right).$$

Here, an *empty* product is to be interpreted as unity.

Solution by Paul S. Bruckman, Edmonds, WA

We consider the Chebychev polynomials of the second kind, defined as follows:

$$(1)\qquad U_n(x) = \frac{a^{n+1} - b^{n+1}}{a - b}, \quad n = 0, 1, 2, \ldots,$$

where

$$(2)\qquad a = a(x) = x + \sqrt{x^2 - 1}, \; b = b(x) = x - \sqrt{x^2 - 1}.$$

It may be shown that $U_n(x) = 0$ iff $x = \cos(\pi k/(n + 1))$, $k = 1, 2, \ldots, n$. The $U_n(x)$ are polynomials of degree n, and their leading term is $(2x)^n$. Therefore,

$$(3)\qquad U_n(x) = 2^n \prod_{k=1}^{n}\left(x - \cos\frac{k\pi}{n+1}\right).$$

It follows that

$$U_n(ix)U_n(-ix) = 4^n \prod_{k=1}^{n}\left(x^2 + \cos^2\frac{k\pi}{n+1}\right).$$

By a change in variable from n to $n - 1$:

$$(4)\qquad U_{n-1}(ix)U_{n-1}(-ix) = \prod_{k=1}^{n-1}\left(4x^2 + 2 + 2\cos\frac{2k\pi}{n}\right).$$

In particular, setting $x = 1/2$, we obtain:

$$(5)\qquad U_{n-1}(i/2)U_{n-1}(-i/2) = \prod_{k=1}^{n-1}\left(3 + 2\cos\frac{2k\pi}{n}\right).$$

Next, using (1) and (2), we obtain

$$a(i/2) = \frac{1}{2}i(1 \pm \sqrt{5}) = i\alpha \text{ or } i\beta,$$

where α and β are the usual Fibonacci constants; also

$$b(i/2) = \frac{1}{2}i(1 \mp \sqrt{5}) = i\beta \text{ or } i\alpha,$$

respectively. In either case,

$$U_{n-1}(i/2) = i^{n-1}F_n.$$

Likewise,

$$U_{n-1}(-i/2) = (-i)^{n-1}F_n.$$

Consequently,

(6) $$U_{n-1}(i/2)U_{n-1}(-i/2) = F_n^2, \quad n = 1, 2, 3, \ldots .$$

Now, let A_n denote the product expression indicated in the statement of the problem. For brevity, let $\theta_k = 3 + 2\cos(2k\pi/n)$. Note that $\theta_{n-k} = \theta_k$. We consider two cases:

Case 1: $n = 2m$

Then $A_n = \prod_{k=1}^{m-1}\theta_k = \prod_{k=m+1}^{n-1}\theta_k$. Also, $\theta_m = 1$.

Hence, $A_n^2 = \prod_{k=1}^{n-1}\theta_k$.

Case 2: $n = 2m + 1$

Then $A_n = \prod_{k=1}^{m}\theta_k = \prod_{k=m+1}^{n-1}\theta_k$, so $A_n^2 = \prod_{k=1}^{n-1}\theta_k$.

In either case, we have

(7) $$A_n^2 = \prod_{k=1}^{n-1}\left(3 + 2\cos\frac{2k\pi}{n}\right).$$

Comparing this last expression with (5) and (6), we see that

(8) $$A_n^2 = F_n^2, \quad n = 1, 2, \ldots .$$

Since $\theta_k \geq 1$, we see that $A_n \geq 1$. From this it follows that

(9) $$A_n = F_n, \quad n = 1, 2, \ldots . \qquad \text{Q.E.D.}$$

Also solved by S. Rabinowitz and H.-J. Seiffert.

Rings True

H-448 *Proposed by T. V. Padmakumar, Trivandrum, South India (Vol. 28, no. 4, November 1990)*

If n is any number and $a_1, a_2, \ldots, a_m$ are prime to n ($n > a_1, a_2, \ldots, a_m$), then $(a_1a_2 \ldots a_m)^2 \equiv 1 \pmod{n}$. [The number of positive integers less than n and prime to it is denoted by $\phi(n) = m$.]

Solution by R. André-Jennin, Tunisia

Put $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, (\overline{n-1})\}$, and $U = \{\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m\}$. By hypothesis, U is the multiplicative group of the invertible elements of the ring $\mathbb{Z}/n\mathbb{Z}$.

It is clear that the map $\overline{x} \to \overline{x}^{-1}$ is a one-to-one mapping of U onto itself. Hence,

$$\overline{a}_i^{-1} = \overline{a}_{\sigma(i)}, \text{ for } i = 1, \ldots, m,$$

where σ is a permutation of $\{1, 2, \ldots, m\}$.

Thus, in the ring $\mathbb{Z}/n\mathbb{Z}$,

$$(\overline{a}_1\overline{a}_2 \ldots \overline{a}_m)^{-1} = \overline{a}_1^{-1} \ldots \overline{a}_m^{-1} = \overline{a}_{\sigma(1)} \ldots \overline{a}_{\sigma(m)} = \overline{a}_1 \ldots \overline{a}_m,$$

and so

$$(\overline{a}_1 \ldots \overline{a}_m)^2 = \overline{1},$$

or, in other words,

$$(a_1 \ldots a_m)^2 \equiv 1 \pmod{n}.$$

Also solved by D. Redmond and the proposer.

A Recurrent Theme

H-449 *Proposed by Ioan Sadoveanu, Ellensburg, WA*
(Vol. 29, no. 1, February 1991)

Let $G(x) = x^k + a_1x^{k-1} + \cdots + a_k$ be a polynomial with c as a root of order p. If $G^{(p)}(x)$ denotes the p^{th} derivative of $G(x)$, show that

$$\left\{\frac{n^pc^{n-p}}{G^{(p)}(c)}\right\} \text{ is a solution to the recurrence}$$

$$u_n = c^{n-k} - a_1u_{n-1} - a_2u_{n-2} - \cdots - a_ku_{n-k}.$$

Solution by Y. H. Harris Kwong, SUNY College at Fredonia, Fredonia, NY

The result is trivial if $c = 0$, so we shall assume that $c \neq 0$. Write

$$G(x) = (x - c)^pH(x),$$

where $H(c) \neq 0$. Let

$$g(x) = x^kG(1/x) \quad \text{and} \quad h(x) = x^{k-p}H(1/x)$$

such that $g(x) = (1 - cx)^ph(x)$, where $h(1/c) \neq 0$. Denote the generating function of u_n by $U(x)$. It is straightforward to check that

$$g(x)U(x) = g(x)\left(\sum_{n=0}^{\infty} u_nx^n\right) = w_1(x) + \frac{x^k}{1 - cx}$$

for some polynomial $w_1(x)$ which depends on $u_0, u_1, \ldots, u_{k-1}$. Therefore,

$$(1) \qquad U(x) = \frac{(1 - cx)w_1(x) + x^k}{(1 - cx)g(x)} = \frac{(1 - cx)w_1(x) + x^k}{(1 - cx)^{p+1}h(x)}.$$

It follows that the characteristic equation for the recurrence is

$$(x - c)^{p+1}H(x) = 0.$$

Hence, $u_n = n^pc^n$ is a solution. We now proceed to improve this result.

There exist a polynomial $w_2(x)$ and constants $A_1, \ldots, A_{p+1}$ such that

$$(2) \qquad U(x) = \frac{w_2(x)}{h(x)} + \frac{A_1}{1 - cx} + \cdots + \frac{A_{p+1}}{(1 - cx)^{p+1}}.$$

Consider

$$\frac{1}{(1 - cx)^t} = \sum_{n=0}^{\infty}\binom{t + n - 1}{t - 1}(cx)^n.$$

Since $\binom{t+n-1}{t-1}$ is a polynomial in n of degree $t - 1$, it is clear that

$$A_{p+1}/(1 - cx)^{p+1}$$

is the only expansion in which the coefficient of x^n contains n^p. Indeed, this coefficient is precisely $A_{p+1}n^pc^n/p!$. Equating the numerators in (1) and (2), we obtain

$$(1 - cx)w_1(x) + x^k = w_2(x)(1 - cx)^{p+1} + h(x)\{A_1(1 - cx)^p + \cdots + A_{p+1}\}.$$

Thus

$$A_{p+1} = \frac{(1/c)^k}{h(1/c)} = \frac{1}{c^p H(c)}.$$

From the observation

$$(p + 1)!H(c) = \frac{d^{p+1}}{dx^{p+1}}\{(x - c)^{p+1}H(x)\}\bigg|_{x=c} = \frac{d^{p+1}}{dx^{p+1}}\{(x - c)G(x)\}\bigg|_{x=c}$$

$$= (p + 1)G^{(p)}(c),$$

we conclude that

$$u_n = \frac{A_{p+1}n^p c_n}{p!} = \frac{n^p c^{n-p}}{G^{(p)}(c)}$$

is a solution to the given recurrence relation.

Also solved by P. Bruckman, R. André-Jeannin, and the proposer.

Comparable

H-450 *Proposed by R. André-Jeannin, Tunisia*
(Vol. 29, no. 1, February 1991)

Compare the numbers

$$\Theta = \sum_{n=1}^{\infty} \frac{1}{F_n}$$

and

$$\Theta' = 2 + \sum_{n=1}^{\infty} \frac{1}{F_n(2F_{n-1}^2 + (-1)^{n-1})(2F_n^2 + (-1)^n)}.$$

Solution by P. Bruckman, Edmonds, WA

We let

(1) $A_n = 2F_n^2 + (-1)^n, \quad n = 0, 1, 2, \ldots,$

(2) $D_n = F_n A_n A_{n-1}, \quad n = 1, 2, 3, \ldots .$

We will prove the identity:

(3) $$\frac{1}{D_n} = \frac{1}{F_n} + \frac{2F_{n+1}}{A_n} - \frac{2F_n}{A_{n-1}}, \quad n = 1, 2, 3, \ldots .$$

The right member of (3) is equal to

$$\frac{1}{D_n}[A_n A_{n-1} + 2F_n(F_{n+1}A_{n-1} - F_n A_n)];$$

therefore, it suffices to prove the identity:

(4) $A_n A_{n-1} + 2F_n(F_{n+1}A_{n-1} - F_n A_n) = 1, \quad n = 1, 2, 3, \ldots .$

Let S_n denote the left member of (4). We see from (1) that $A_0 = A_1 = 1$; hence, $S_1 = 1$. It suffices to prove that $S_{n+1} - S_n = 0$, $n = 1, 2, \ldots$, for this would imply (4). We first require some basic identities:

(5) $A_n = F_n^2 + F_{n+1}F_{n-1} = F_{n+1}^2 - F_n F_{n-1} = F_{n-1}^2 + F_n F_{n+1};$

(6) $A_{n+1} - A_n = 2F_{n+1}F_n$;

(7) $A_{n+1} - A_{n-1} = 2F_{2n}$;

(8) $F_{n+1}A_{n+1} + F_nA_{n-1} = A_n(F_{n+2} + 2F_n)$.

Proof of (5): Since $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$,

$$\begin{aligned} A_n &= 2F_n^2 + F_{n+1}F_{n-1} - F_n^2 = F_n^2 + F_{n+1}F_{n-1} = (F_{n+1} - F_{n-1})^2 + F_{n+1}F_{n-1} \\ &= F_{n+1}^2 - F_{n+1}F_{n-1} + F_{n-1}^2 = F_{n+1}^2 - F_{n-1}(F_{n+1} - F_{n-1}) = F_{n+1}^2 - F_nF_{n-1} \\ &= F_{n-1}^2 + F_{n+1}(F_{n+1} - F_{n-1}) = F_{n-1}^2 + F_nF_{n+1}. \end{aligned}$$

Proof of (6): $A_{n+1} - A_n = F_{n+1}^2 + F_{n+2}F_n - F_{n+1}^2 + F_nF_{n-1}$

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

Proof of (7): $A_{n+1} - A_{n-1} = F_{n+1}^2 + F_{n+2}F_n - F_{n-1}^2 - F_nF_{n-2}$

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

$= F_nL_n + F_n(F_{n+1} + F_n - F_n + F_{n-1}) = 2F_nL_n = 2F_{2n}$.

Proof of (8): $F_{n+1}A_{n+1} + F_nA_{n-1} = F_{n+1}(A_n + 2F_{n+1}F_n) + F_n(A_n - 2F_nF_{n-1})$ [by (6)]

$= (F_{n+1} + F_n)A_n + 2F_n(F_{n+1}^2 - F_nF_{n-1}) = F_{n+2}A_n + 2F_nA_n$ [using (5)]

$= (F_{n+2} + 2F_n)A_n$.

Therefore,

$$\begin{aligned} S_{n+1} - S_n &= A_{n+1}A_n + 2F_{n+1}(F_{n+2}A_n - F_{n+1}A_{n+1}) - A_nA_{n-1} - 2F_n(F_{n+1}A_{n-1} - F_nA_n) \\ &= A_n(A_{n+1} - A_{n-1}) + 2A_n(F_n^2 + F_{n+1}F_{n+2}) - 2F_{n+1}(F_{n+1}A_{n+1} + F_nA_{n-1}) \\ &= A_n(2F_{2n}) + 2A_nA_{n+1} - 2F_{n+1}A_n(F_{n+2} + 2F_n) \quad \text{[using (5), (7), (8)]} \\ &= 2A_n(F_{2n} + A_{n+1} - F_{n+1}(F_{n+2} + 2F_n)) \\ &= 2A_n(F_{2n} + F_n^2 + F_{n+1}F_{n+2} - F_{n+1}F_{n+2} - 2F_nF_{n+1}) = 2A_n(F_{2n} - F_n(2F_{n+1} - F_n)) \\ &= 2A_n(F_{2n} - F_n(F_{n+1} + F_{n-1})) = 2A_n(F_{2n} - F_nL_n) = 0. \end{aligned}$$

This completes the proof of (4), and hence of (3).

We may now sum both sides of 93) over all natural numbers n, observing that all sums are absolutely convergent. The left sum is equal to

$$\sum_{n=1}^{\infty} \frac{1}{D_n} = \Theta' - 2.$$

Let $u_n = 2F_{n+1}/A_n$. The right sum is equal to

$$\left[\sum_{n=1}^{\infty} \frac{1}{F_n} + u_n - u_{n-1}\right] = \sum_{n=1}^{\infty} \frac{1}{F_n} - u_0 = \Theta - 2$$ (using the fact that $u_n \to 0$ as $n \to \infty$).

We conclude:

(9) $\Theta' = \Theta$.

Comment: This very interesting result furnishes us with a series equivalent to the much-studied series $\sum_{n=1}^{\infty} 1/F_n$, but converging much more rapidly than the latter series. Thus,

$$\Theta = 3 + 1/3 + 1/42 + 1/399 + 1/4655 + 1/50568 + \cdots \doteq 3.3599.$$

*****

BOOKS AVAILABLE

THROUGH THE FIBONACCI ASSOCIATION

Introduction to Fibonacci Discovery by Brother Alfred Brousseau. Fibonacci Association (FA), 1965.

Fibonacci and Lucas Numbers by Verner E. Hoggatt, Jr. FA, 1972.

A Primer for the Fibonacci Numbers. Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1972.

Fibonacci's Problem Book. Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1974.

The Theory of Simply Periodic Numerical Functions by Edouard Lucas. Translated from the French by Sidney Kravitz. Edited by Douglas Lind. FA, 1969.

Linear Recursion and Fibonacci Sequences by Brother Alfred Brousseau. FA, 1971.

Fibonacci and Related Number Theoretic Tables. Edited by Brother Alfred Brousseau. FA, 1972.

Number Theory Tables. Edited by Brother Alfred Brousseau. FA, 1973.

Tables of Fibonacci Entry Points, Part One. Edited and annotated by Brother Alfred Brousseau. FA, 1965.

Tables of Fibonacci Entry Points, Part Two. Edited and annotated by Brother Alfred Brousseau. FA, 1965.

A Collection of Manuscripts Related to the Fibonacci Sequence—18th Anniversary Volume. Edited by Verner E. Hoggatt, Jr. and Marjorie Bicknell-Johnson. FA, 1980.

Fibonacci Numbers and Their Applications. Edited by A.N. Philippou, G.E. Bergum and A.F. Horadam.

Applications of Fibonacci Numbers, Volumes 2 and 3. Edited by A.N. Philippou, A.F. Horadam and G.E. Bergum.

Please write to the Fibonacci Association, Santa Clara University, Santa Clara CA 95053, U.S.A., for current prices.

SUSTAINING MEMBERS

I. Adler
*H.L. Alder
G.L. Alexanderson
S. Ando
R. Andre-Jeannin
*J. Arkin
D.C. Arney
C. Ashbacher
M.K. Azarian
N. Balasubramania
L. Bankoff
M. Berg
J.G. Bergart
G. Bergum
G. Berzsenyi
*M. Bicknell-Johnson
P. Bien
P.S. Bruckman
M.F. Bryn
G.D. Chakerian
C. Chouteau
C.K. Cook
J.W. Creely
P.A. DeCaux
M.J. DeLeon
J. Desmond
H. Diehl
V. Dudley
T.H. Engel
D.R. Farmer
D.C. Fielder
F. Firoozbakht
Emerson Frost
Anthony Gioia
R.M. Giuli
H.W. Gould
P. Hagis, Jr.
H. Harborth
Y. Harris Kwong
P. Haukkanen
A.P. Hillman
*A.F. Horadam
F.T. Howard
R.J. Howell
S. Howell
R.E. Kennedy
C.H. Kimberling
A. Knopfmacher
R.P. Kovach
J. Lahr
J.C. Lagarias
L.H. Lange
C.T. Long
Br. J.M. Mahon
*J. Maxwell
F.U. Mendizabal
M.G. Monzingo
J.F. Morrison
K. Nagasaka
S.A. Obaid
D.J. Pedwell
A. Prince
S. Rabinowitz
S. Sato
J.A. Schumaker
A.G. Shannon
L.W. Shapiro
J.R. Siler
D. Singmaster
J. Sjoberg
L. Somer
M.N.S. Swamy
*D. Thoro
J.C. Turner
T.P. Vaughan
K. Velupiliai
J.N. Vitale
M. Waddill
J.E. Walton
G. Weekly
R.E. Whitney
B.E. Williams

*Charter Members

INSTITUTIONAL MEMBERS

ACADIA UNIVERSITY LIBRARY
Wolfville, Nova Scotia

THE BAKER STORE EQUIPMENT COMPANY
Cleveland, Ohio

CALIFORNIA STATE UNIVERSITY SACRAMENTO
Sacramento, California

ETH-BIBLIOTHEK
Zurich, Switzerland

FERNUNIVERSITAET HAGEN
Hagen, West Germany

HOWELL ENGINEERING COMPANY
Bryn Mawr, California

KLEPCO, INC.
Sparks, Nevada

MATHEMATICS SOFTWARE COMPANY
Evansville, Indiana

MISSOURI SOUTHERN STATE COLLEGE
Joplin, Missouri

PRINCETON UNIVERSITY
Princeton, New Jersey

SAN JOSE STATE UNIVERSITY
San Jose, California

SANTA CLARA UNIVERSITY
Santa Clara, California

SIMON FRASER UNIVERSITY
Burnaby, B.C. Canada

UNIVERSITY OF NEW ENGLAND
Armidale, N.S.W. Australia

UNIVERSITY OF ROMA
"LA SAPIENZA"
Roma, Italy

UNIVERSITY OF TECHNOLOGY
Sydney, N.S.W. Australia

WAKE FOREST UNIVERSITY
Winston-Salem, North Carolina

WASHINGTON STATE UNIVERSITY
Pullman, Washington

JOVE STATISTICAL TYPING SERVICE
2088 Orestes Way
Campbell, California 95008