

## THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

## TABLE OF CONTENTS

Extensions of the Hermite G.C.D. Theorems for Binomial  Coefficients	386
Seventh International Research Conference	391
Notes on a Conjecture of Singmaster Leetsch Charles Hsu, Peter Jau-shyong Shiue and Yi Wang	392
Real Pell and Pell-Lucas Numbers with Real Subscripts	398
On Decimation of Linear Recurring Sequences	407
Book Announcement: Generalized Pascal Triangles and Pyramids: Their Fractals, Graphs, and Applications	411
Roots of Unity and Circular Subsets without Consecutive Elements	412
Some Discrete Distributions Related to Extended Pascal Triangles	415
Fifth International Conference Proceedings	425
The Distribution of Spaces on Lottery Tickets	426
The Switch, Subtract, Reorder Routine	432
Linear Recurrences in Difference Triangles Edith H. Luchins, Russell Hendel, Paul Lemke and David Tuller	441
Differential Properties of a General Class of Polynomials	453
Author and Title Index for Sale	458
Polynomial Divisibility in Finite Fields, and Recurring Sequences	459
Some Conditions for "All or None" Divisibility of a Class of Fibonacci-Like Sequences	464
Elementary Problems and Solutions Edited by Stanley Rabinowitz	466
Advanced Problems and Solutions Edited by Raymond E. Whitney	466
Volume Index	478

VOLUME 33 NOVEMBER 1995 NUMBER 5

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

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

Two copies of the manuscript should be submitted to: GERALD E. BERGUM, EDITOR, THE FIBONACCI QUARTERLY, DEPARTMENT OF COMPUTER SCIENCE, SOUTH DAKOTA STATE UNIVERSITY, BOX 2201, BROOKINGS, SD 57007-1596.

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

## SUBSCRIPTIONS, ADDRESS CHANGE, AND REPRINT INFORMATION

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

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

Annual domestic Fibonacci Association membership dues, which include a subscription to **THE FIBONACCI QUARTERLY**, are \$37 for Regular Membership, \$42 for Library, \$47 for Sustaining Membership, and \$74 for Institutional Membership; foreign rates, which are based on international mailing rates, are somewhat higher than domestic rates; please write for details. **THE FIBONACCI QUARTERLY** is published each February, May, August and November.

All back issues of THE FIBONACCI QUARTERLY are available in microfilm or hard copy format from UNIVERSITY MICROFILMS INTERNATIONAL, 300 NORTH ZEEB ROAD, DEPT. P.R., ANN ARBOR, MI 48106. Reprints can also be purchased from UMI CLEARING HOUSE at the same address.

## Ge 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 57007-1596 e-mail: Bergumg@mg.sdstate.edu

#### EDITORIAL BOARD

DAVID M. BRESSOUD, Macalester College, St. Paul, MN 55105-1899 JOHN BURKE, Gonzaga University, Spokane, WA 99258-0001 LEONARD CARLITZ, Emeritus Editor, Duke Univesity, Durham, NC 27708-0251 HENRY W. GOULD, West Virginia University, Morgantown, WV 26506-0001 A.F. HORADAM, University of New England, Armidale, N.S.W. 2351, Australia CLARK KIMBERLING, University of Evansville, Evansville, IN 47722-0001 RICHARD MOLLIN, University of Calgary, Calgary T2N 1N4, Alberta, Canada GARY L. MULLEN, The Pennsylvania State University, University Park, PA 16802-6401 SAMIH OBAID, San Jose State University, San Jose, CA 95192-0103 NEVILLE ROBBINS, San Francisco State University, San Francisco, CA 94132-1722 DONALD W. ROBINSON, Brigham Young University, Provo, UT 84602-6539 LAWRENCE SOMER, Catholic University of America, Washington, D.C. 20064-0001 M.N.S. SWAMY, Concordia University, Montreal H3G 1M8, Quebec, Canada ROBERT F. TICHY, Technical University, Graz, Austria WILLIAM WEBB, Washington State University, Pullman, WA 99164-3113 ANNE LUDINGTON YOUNG, Loyola College in Maryland, Baltimore, MD 21210-2699

## BOARD OF DIRECTORS THE FIBONACCI ASSOCIATION

CALVIN LONG (President)

Northern Arizona University, Flagstaff, AZ 86011-5717

G.L. ALEXANDERSON

Santa Clara University, Santa Clara, CA 95053-0001

ANDREW GRANVILLE

University of Georgia, Athens, GA 30601-3024

PETER HAGIS, JR.

880 Edison Avenue, Philadelphia, PA 19116

FRED T. HOWARD

Wake Forest University, Winston-Salem, NC 27106-5239

MARJORIE JOHNSON (Secretary-Treasurer)

665 Fairlane Avenue, Santa Clara, CA 95051

LESTER LANGE

Moss Landing Marine Labs, Moss Landing, CA 95039-0450

JEFF LAGARIAS

Bell Laboratories, Murray Hill, NJ 07974-0636

THERESA VAUGHAN

University of North Carolina, Greensboro, NC 27410-5608

## EXTENSIONS OF THE HERMITE G.C.D. THEOREMS FOR BINOMIAL COEFFICIENTS

## H. W. Gould

Department of Mathematics, West Virginia University, PO Box 6310, Morgantown, WV 26506-6310; Email: gould@math.wvu.edu

## Paula Schlesinger

124 Lawson Drive, Spruce Pine, NC 28777 (Submitted November 1993)

## 1. INTRODUCTION

Dickson [1], in his History of the Theory of Numbers, attributes the divisibility theorems

$$\frac{n}{(n,k)} \left| \binom{n}{k} \right| \tag{1.1}$$

and

$$\frac{n-k+1}{(n+1,k)} \binom{n}{k},\tag{1.2}$$

where (n, k) denotes the greatest common divisor of n and k to Hermite [9], [10] whose proofs use the Euclidean algorithm. In [5] and [6] the proofs were extended by one of us to generalized binomial coefficients defined by

$${n \brace k} = \frac{A_n A_{n-1} \cdots A_{n-k+1}}{A_k A_{k-1} \cdots A_1} \quad \text{with } {n \brace 0} = 1,$$
 (1.3)

where  $\{A_n\}$  is a sequence of integers such that  $A_0 = 0$ ,  $A_n \neq 0$  for  $n \geq 1$ , and such that the ratio in (1.3) is always an integer. Of course, the ordinary binomial coefficients occur when  $A_n = n$ . When  $A_n = F_n$ , the n<sup>th</sup> Fibonacci number, we obtain the well-known "Fibonomial" coefficients. Another very well-known case is when  $A_n = q^n - 1$ , in which case the coefficients determined by (1.3) are the Gaussian or q-binomial coefficients. The generalized forms of Hermite's theorems obtained in [6] are as follows:

$$\frac{A_n}{(A_n, A_k)} \begin{Bmatrix} n \\ k \end{Bmatrix} \tag{1.4}$$

and

$$\frac{A_{n-k+1}}{(A_{n+1}, A_k)} \begin{vmatrix} n \\ k \end{vmatrix} \quad \text{provided } (A_{n+1}, A_k) | A_{n-k+1}. \tag{1.5}$$

In this paper we will replace (1.1) and (1.2) by the following theorems:

$$\frac{n}{(n,k)} \text{g.c.d.} \left( \binom{n}{k}, \binom{n-1}{k-1} \right) = \binom{n}{k}$$
(1.6)

and

$$\frac{n+1-k}{(n+1,k)} \operatorname{g.c.d.}\left(\binom{n}{k}, \binom{n}{k-1}\right) = \binom{n}{k}, \tag{1.7}$$

so that the explicit quotients in the original Hermite statements are made evident as just g.c.d.'s of two binomial coefficients.

What is more, the corresponding extensions to generalized binomials take the forms

$$\frac{A_n}{(A_n, A_k)} \text{g.c.d.} \left( \begin{cases} n \\ k \end{cases}, \begin{cases} n-1 \\ k-1 \end{cases} \right) = \begin{Bmatrix} n \\ k \end{Bmatrix}$$
(1.8)

and

$$\frac{A_{n-k+1}}{(A_{n+1-k}, A_k)} \operatorname{g.c.d.} \left( \begin{Bmatrix} n \\ k \end{Bmatrix}, \begin{Bmatrix} n \\ k-1 \end{Bmatrix} \right) = \begin{Bmatrix} n \\ k \end{Bmatrix}. \tag{1.9}$$

Note especially now that in (1.9) the greatest common divisor automatically divides  $A_{n+1-k}$  whereas in (1.5) this was not necessarily the case.

Some variations of these theorems will be presented so that the problem raised by Gould in [3] (no solution having appeared in the interim in the *Monthly*) will have a better formulation due to the nature of our present attack. That problem asked for a way to unify Hermite's two theorems into a general result of the form

$$\frac{an+bk+c}{(rn+s,uk+v)} \binom{n}{k} \tag{1.10}$$

for suitable parameters

The explicit forms (1.6) and (1.7) were obtained by Schlesinger in November 1986, and are now being published here for the first time.

It should be remarked that Dickson [1] also traces (1.1) in a form valid for multinomial coefficients back to Schönemann [15] who, in 1839, used symmetric functions and  $p^{th}$  roots of unity.

## 2. PROOF OF (1.6) AND (1.7) AND VARIATIONS

We need only the simplest properties of the binomial coefficients and the greatest common divisor to see that

$$n \text{ g. c. d.} \left( \binom{n}{k}, \binom{n-1}{k-1} \right) = \text{g. c. d.} \left( n \binom{n}{k}, n \binom{n-1}{k-1} \right)$$
$$= \text{g. c. d.} \left( n \binom{n}{k}, k \binom{n}{k} \right) = \binom{n}{k} \text{g. c. d.} (n, k)$$

which proves (1.6). Similarly,

$$(n+1-k) \text{ g. c. d.} \left( \binom{n}{k}, \binom{n}{k-1} \right) = \text{ g. c. d.} \left( (n+1-k) \binom{n}{k}, (n+1-k) \binom{n}{k-1} \right)$$
$$= \text{ g. c. d.} \left( (n+1-k) \binom{n}{k}, k \binom{n}{k} \right) = \binom{n}{k} \text{ g. c. d.} (n+1-k, k)$$

which proves (1.7), since g.c.d.(n+1-k, k) = g.c.d.(n+1, k).

The improvement offered by this approach is that we avoid the use of the Euclidean algorithm which only told us that g.c.d.(n, k) = nx + ky for *some* integers x and y. What we have now are explicit values and the only property of the g.c.d. used is linearity, i.e., that n g.c.d.(A, B) = g.c.d.(nA, nB).

In the same manner in which we proved (1.6) and (1.7), the reader may establish the following variations:

$$\frac{n}{(n,k)} g.c.d. \left( \binom{n}{k}, \binom{n-1}{k} \right) = \binom{n}{k}; \tag{2.1}$$

$$\frac{n+1-k}{(n+1-k, n+1)} \text{g. c. d.} \left( \binom{n}{k}, \binom{n+1}{k} \right) = \binom{n}{k}; \tag{2.2}$$

$$\frac{k+1}{(k+1, n-k)} \operatorname{g.c.d.}\left(\binom{n}{k}, \binom{n}{k+1}\right) = \binom{n}{k}; \tag{2.3}$$

$$\frac{k+1}{(k+1,n+1)} \operatorname{g.c.d.} \left( \binom{n}{k}, \binom{n+1}{k+1} \right) = \binom{n}{k}. \tag{2.4}$$

Note that in (1.6), (1.7), (2.1), (2.2), (2.3), and (2.4) we have in each case the g.c.d. of  $\binom{n}{k}$  and  $\binom{n+a}{k+b}$ , where a and b assume only the values -1, 0, +1 and in some special manner.

Here is a different-looking result, easily verified:

$$(n+1-k)(k+1)$$
 g.c.d. $\binom{n}{k-1}$ ,  $\binom{n}{k+1}$  =  $\binom{n}{k}$  g.c.d. $(k(k+1), (n-k)(n+1-k))$ , (2.5)

so that if we try to shift a unit in both coefficients we get quadratic factors appearing.

Relation (1.6) may be extended easily by shifting both k and n in the one binomial coefficient by the same amount. Thus, if we let  $0 \le i \le k$ , we find

$$(n-i) \operatorname{g.c.d.}\left(\binom{n}{k}, n(n-1) \cdots (n-i+1)\binom{n-i-1}{k-i-1}\right)$$

$$= \operatorname{g.c.d.}\left((n-i)\binom{n}{k}, n(n-1) \cdots (n-i+1)(n-i)\binom{n-i-1}{k-i-1}\right)$$

$$= \operatorname{g.c.d.}\left((n-i)\binom{n}{k}, k(k-1) \cdots (k-i)\binom{n-i-1}{k-i-1}\right)$$

$$= \binom{n}{k} \operatorname{g.c.d.}(n-i, k(k-1) \cdots (k-i)),$$

so that we have proved

$$\frac{n-i}{((n-i),k(k-1)\cdots(k-i))} \binom{n}{k} \tag{2.6}$$

for every i with  $0 \le i \le k$ , and the quotient is

g.c.d.
$$\binom{n}{k}$$
,  $n(n-1)\cdots(n-i+1)\binom{n-i-1}{k-i-1}$ .

The corresponding proof by the original method of Hermite, using the Euclidean algorithm runs as follows. Let  $d = g.c.d.(n-i, k(k-1)\cdots(k-1))$ . Then there exist integers x and y such that  $(n-i)x+k(k-1)\cdots(k-i)y=d$ . Thus,

388 [NOV.

$$((n-i)x + k(k-1)\cdots(k-i)y)\binom{n}{k} = (n-i)x\binom{n}{k} + k(k-1)\cdots(k-i)y\binom{n}{k}$$
$$= (n-i)x\binom{n}{k} + n(n-1)\cdots(n-i)y\binom{n-i-1}{k-i-1},$$

whence the result follows; however, it does not yield the explicit quotient value.

Two formulas that are similar to (2.5) and which may be verified by the reader are:

$$n(k+1)$$
 g.c.d. $\binom{n-1}{k}$ ,  $\binom{n+1}{k+1}$  =  $\binom{n}{k}$  g.c.d. $((k+1)(n-k), n(n+1))$  (2.7)

and

$$n(n+1-k)$$
 g.c.d. $\binom{n-1}{k-1}$ ,  $\binom{n+1}{k}$  =  $\binom{n}{k}$  g.c.d. $((n+1-k)k, n(n+1))$ . (2.8)

## 3. EXTENSION TO GENERALIZED BINOMIAL COEFFICIENTS

The proof of (1.8) runs as follows:

$$\begin{split} A_n & \text{g. c. d.} \left( \left\{ \begin{matrix} n \\ k \end{matrix} \right\}, \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\} \right) = \text{g. c. d.} \left( A_n \left\{ \begin{matrix} n \\ k \end{matrix} \right\}, A_n \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\} \right) \\ & = \text{g. c. d.} \left( A_n \left\{ \begin{matrix} n \\ k \end{matrix} \right\}, A_k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} \right) = \left\{ \begin{matrix} n \\ k \end{matrix} \right\} \text{g. c. d.} \left( A_n, A_k \right), \end{split}$$

while for (1.9), we have

$$A_{n+1-k} \text{ g. c. d.} \left( \begin{Bmatrix} n \\ k \end{Bmatrix}, \begin{Bmatrix} n \\ k-1 \end{Bmatrix} \right) = \text{ g. c. d.} \left( A_{n+1-k} \begin{Bmatrix} n \\ k \end{Bmatrix}, A_{n+1-k} \begin{Bmatrix} n \\ k-1 \end{Bmatrix} \right)$$

$$= \text{ g. c. d.} \left( A_{n+1-k} \begin{Bmatrix} n \\ k \end{Bmatrix}, A_{n} \begin{Bmatrix} n \\ k \end{Bmatrix} \right) = \begin{Bmatrix} n \\ k \end{Bmatrix} \text{ g. c. d.} \left( A_{n+1-k}, A_{k} \right).$$

A simple but important application of (1.9) is to show that the Fibonomial Catalan numbers are in fact integers. Let  $A_n = F_n = n^{\text{th}}$  Fibonacci number. Then by (1.9), with the substitutions  $n \leftarrow 2n, k \leftarrow n$ , we have that  $\binom{n}{k}_F$  is divisible by  $F_{n+1}/(F_{n+1}, F_n)$ . But  $(F_{n+1}, F_n) = 1$ , whence the  $n^{\text{th}}$  Fibonomial Catalan number

$$\frac{1}{F_{n+1}} \begin{Bmatrix} 2n \\ n \end{Bmatrix}_F \tag{3.1}$$

is an integer. This makes a shorter proof than what was done in [4, p. 363].

## 4. THEOREMS ABOUT LEAST COMMON MULTIPLES

Since (a, b)[a, b] = ab, where [a, b] denotes the least common multiple of a and b, for positive integers a and b, we may convert our theorems to statements about least common multiples. Relation (1.7) may be restated as

$$g.c.d.\left(\binom{n}{k}, \binom{n}{k-1}\right) = \frac{(n+1,k)}{n+1-k} \binom{n}{k}$$

$$(4.1)$$

so that, in terms of least common multiples

1. c. m. 
$$\binom{n}{k}$$
,  $\binom{n}{k-1}$  =  $\frac{n+1-k}{(n+1,k)}\binom{n}{k-1}$ . (4.2)

These then give interesting and useful statements about the g.c.d. and l.c.m. of consecutive binomial coefficients on the  $n^{th}$  row of the Pascal triangle. In principle, we may find relations for the g.c.d. and l.c.m. of  $\binom{n}{k}$  and  $\binom{m}{i}$ .

## REFERENCES

- 1. L. E. Dickson. *History of the Theory of Numbers*. Vol. 1. Washington, D.C.: Carnegie Institution, 1919; rpt. New York: Chelsea, 1952.
- 2. Hugh M. Edgar. "The Least Common Multiple of Some Binomial Coefficients." *The Fibonacci Quarterly* **24.4** (1986):310-12.
- 3. H. W. Gould. Problem 5777\*. Amer. Math. Monthly 78 (1971):202.
- 4. H. W. Gould. "A New Primality Criterion of Mann and Shanks and Its Relation to a Theorem of Hermite with Extension to Fibonomials." *The Fibonacci Quarterly* **10.4** (1972): 355-72.
- 5. H. W. Gould. "A New Greatest Common Divisor Property of the Binomial Coefficients." *The Fibonacci Quarterly* **10.6** (1972):579-84, 628.
- 6. H. W. Gould. "Generalization of Hermite's Divisibility Theorems and the Mann-Shanks Primality Criterion for s-Fibonomial Arrays." *The Fibonacci Quarterly* **12.2** (1974):157-66.
- 7. H. W. Gould & W. E. Greig. "A Lucas Triangle Primality Criterion Dual to that of Mann-Shanks." *The Fibonacci Quarterly* **23.1** (1985):66-69.
- 8. H. Gupta. "On a Problem in Parity." *Indian J. Math.* 11 (1969):157-63.
- 9. C. Hermite. Problems 257-258. *Jour. de math. Speciales* (1889):19-22; (1891):70. Solutions given by E. Catalan.
- 10. C. Hermite & T. J. Stieltjes. *Correspondance d'Hermite et de Stieltjes* 1 (1905):415-16. Letter of 17 April 1889.
- 11. Henry B. Mann & Daniel Shanks. "A Necessary and Sufficient Condition for Primality and Its Source." *J. Comb. Theory*, Ser. Z, **13** (1972):131-34.
- 12. G. B. Mathews. Math. Quest. Educ. Times 52 (1890):63.
- 13. Glenn N. Michael. "A New Proof of an Old Property." *The Fibonacci Quarterly* **2.1** (1964): 57-58.
- 14. G. Ricci. "Sui coefficienti binomali e polinomiali: Una dimostrazione del teorema di Staudt-Clausen sui numeri di Bernoulli." *Gior. Mat. Battaglini* **69** (1931):9-12.
- 15. Theodor Schönemann. "Theorie der symmetrischen Functionen der Wurzeln einer Gleichung: Allgemeine Sätze über Congruenzen nebst einigen Anwendungen derselben." *J. Reine Angew. Math.* 19 (1839):231-43, 289-308.
- 16. Marlow Sholander. "Least Common Multiples and Highest Common Factors." *Amer. Math. Monthly* **68** (1961):984.
- 17. David Singmaster. "Notes on Binomial Coefficients: I; II; III." *J. London Math. Soc.*, Series 2, **8** (1974):545-48; 549-54; 555-60.
- 18. David Singmaster. "Notes on Binomial Coefficients: IV—Proof of a Conjecture of Gould on the G.C.D.'s of Two Triples of Binomial Coefficients." *The Fibonacci Quarterly* 11.3 (1973):282-84.
- 19. David Singmaster. "Divisibility of Binomial and Multinomial Coefficients by Primes and Prime Powers." Unpublished 47-page manuscript, January 1973.

390 [NOV.

- 20. Problem E 2686. *Amer. Math. Monthly* **84** (1977):820; Solution, **89** (1979):131. (Posed by Peter L. Montgomery.)
- 21. Problem E 3431. Amer. Math. Monthly 98 (1991):264; Editorial comment, 99 (1992):877, citing Problem E 2686 and a related paper of M. Nair. (Posed by Jeffrey Shallit.)
- 22. M. Nair. "On Chebyshev-Type Inequalities for Primes." *Amer. Math. Monthly* **89** (1982): 126-29.

AMS Classification Numbers: 11A05, 11B39, 05A10

\*\*\*

#### Announcement

# SEVENTH INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS

July 14-July 19, 1996 INSTITUT FÜR MATHEMATIK TECHNISCHE UNIVERSITÄT GRAZ STEYRERGASSE 30 A-8010 GRAZ, AUSTRIA

#### LOCAL COMMITTEE

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

## INTERNATIONAL COMMITTEE

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

#### LOCAL INFORMATION

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

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

#### Call for Papers

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

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

PROFESSOR GERALD E. BERGUM
THE FIBONACCI QUARTERLY
COMPUTER SCIENCE DEPARTMENT
BOX 2201
SOUTH DAKOTA STATE UNIVERSITY
BROOKINGS, SD 57007-1596

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

## NOTES ON A CONJECTURE OF SINGMASTER

#### Leetsch Charles Hsu

Institute of Applied Mathematics, Dalian University of Technology, Dalian, China

## **Peter Jau-Shyong Shiue**

Department of Mathematical Sciences, University of Nevada, Las Vegas, NV 89154-4020

## Yi Wang

Institute of Applied Mathematics, Dalian University of Technology, Dalian, China (Submitted January 1994)

## 1. INTRODUCTION

Let  $\{a_i\}_{i=1}^n$  be a sequence of positive integers in nondecreasing order. Following Guy [1],  $\{a_i\}$  is a sum=product sequence of size n if  $\sum_{i=1}^n a_i = \prod_{i=1}^n a_i$ . For example, it is easily shown that  $\{2,2\}$ ,  $\{1,2,3\}$ , and  $\{1,1,2,4\}$  are the only sum=product sequences having sizes 2, 3, and 4, respectively. Let N(n) denote the number of different sum=product sequences of size n. Basing his research on various numerical data obtained by computer, David Singmaster has made some conjectures about N(n). These conjectures were proposed during the closing session of the Fifth International Conference on Fibonacci Numbers and Their Applications (St. Andrews, Scotland, 1992); namely, N(n) > 1 for n > 444, N(n) > 2 for n > 6324, and N(n) > 3 for n > 11874. The most attractive conjecture is the statement that  $N(n) \to \infty$  as  $n \to \infty$ .

The object of this note is twofold. First, we give an explicit expression for N(n). Second, we investigate an extended conjecture for the number N(n, k) of different  $(\text{sum})^k = \text{product}$  sequences of size n  $(n > k \ge 2)$ . Then our extended conjecture is the assertion that  $N(n) = \infty$  for  $n > k \ge 2$ . We prove this extended conjecture.

## 2. AN EXPRESSION FOR N(n)

As usual, denote by [x] the integer part of x > 0. Let  $r_k(n)$  denote the number of different ordered solutions of the Diophantine equation, with  $2 \le x_1 \le x_2 \le \cdots \le x_k$ ,

$$\prod_{i=1}^{k} x_i - \sum_{i=1}^{k} x_i = n - k \quad (n > k \ge 2).$$
 (1)

Moreover, we introduce a unit function  $I\{x\}$  defined for rational numbers x by the following:

$$I\{x\} = \begin{cases} 1 & \text{if } x \text{ is a nonnegative integer,} \\ 0 & \text{otherwise.} \end{cases}$$
 (2)

**Proposition 1:** Let d(n) be the divisor function representing the number of divisors of n. For n > 3, we have

$$N(n) = \left[\frac{1}{2}(d(n-1)+1)\right] + \sum_{k=3}^{m} r_k(n),$$
(3)

where  $m = \lceil \log_2 n \rceil + 2$  and  $r_k(n)$  may be expressed in the form

$$r_k(n) = \sum_{2 \le x_1 \le \dots \le x_{k-1}} I\left\{ \frac{n - k + x_1 + \dots + x_{k-1}}{(x_1 \dots x_{k-1}) - 1} - x_{k-1} \right\},\tag{4}$$

the summation being taken over all integers  $x_i$  with  $2 \le x_1 \le \cdots \le x_{k-1}$ .

**Proof:** Notice that for any ordered solution  $(x_1, ..., x_k)$  of (1) with  $k \ge 2$  and  $x_1 \ge 2$  we may write

$$\sum_{i=1}^{n-k} 1 + \sum_{i=1}^{k} x_i = \left(\prod_{i=1}^{n-k} 1\right) \prod_{i=1}^{k} x_i$$

so that it yields a sum=product sequence of size n. Thus, N(n) may be expressed in the form

$$N(n) = r_2(n) + r_3(n) + \cdots$$

Here the first term  $r_2(n)$  just represents the number of ordered solutions of the equation  $x_1x_2 - x_1 - x_2 = n - 2$ , which may be rewritten as  $(x_1 - 1)(x_2 - 1) = n - 1$ . Since the number of divisors of (n-1) is given by d(n-1), it is clear that the number of distinct pairs  $(x_1 - 1, x_2 - 1)$  with  $x_1 \le x_2$  should be equal to  $\left[\frac{1}{2}(d(n-1)+1)\right]$ , which is precisely the first term of (3).

To show that  $m = [\log_2 n] + 2$ , it suffices to determine the largest possible k such that equation (1) with  $n > k \ge 3$  may have integer solutions in  $x_i \ge 2$ . Now, by induction on k, it can be shown that the following inequality,

$$\prod_{i=1}^{k} x_i - \sum_{i=1}^{k} x_i \ge \frac{1}{4} \prod_{i=1}^{k} x_i,$$

holds for all  $x_i \ge 2$  and  $k \ge 3$ . (Here the routine induction proof is omitted.) Consequently, we may infer the following from (1):

$$\frac{1}{4}x_1x_2\cdots x_k \le n-k < n.$$

Clearly, the largest possible k, viz.  $m = \max\{k\}$ , may be obtained by setting all  $x_i = 2$ . Thus, we have  $2^{m-2} < n$ , and we obtain  $m = [\log_2 n] + 2$ .

Finally, let us show that  $r_k(n)$  has the expression (4). As may be observed, one may solve (1) for  $x_k$  in terms of integers  $x_i \ge 2$  (i = 1, ..., k - 1),

$$x_k = \left(n - k + \sum_{i=1}^{k-1} x_i\right) / \left(\prod_{i=1}^{k-1} x_i - 1\right).$$

Therefore, every ordered solution of (1) with  $2 \le x_1 \le \cdots \le x_k$  just corresponds to the condition  $I\{x_k - k_{k-1}\} = 1$  and vice versa. Consequently, the number  $r_k(n)$  (with  $n > k \ge 3$ ) can be expressed as the summation (4).  $\square$ 

As may be verified, (4) can be used in a straightforward manner to give the value  $r_2(n) = \left[\frac{1}{2}(d(n-1)+1)\right]$ . However, there seems to be no way to simplify the summation (4) for the general case  $k \ge 3$ , although for given n and k the sum can be found using a computer.

**Corollary 1:**  $N(n) \ge \left[\frac{1}{2}(d(n-1)+1)\right]$  for  $n \ge 3$ .

Corollary 2:  $\lim_{n\to\infty} \sup N(n) = \infty$ .

Corollaries 1 and 2 were also observed by Singmaster and his coauthors (cf. their preprint [2]). The following simple examples are immediate consequences of the corollaries.

**Example 1:** For m > 1, we have  $N(m^n + 1) \rightarrow \infty$   $(n \rightarrow \infty)$ .

**Example 2:** If  $\{p_n\}$  is the sequence of prime numbers, then we have  $N(p_1p_2\cdots p_n+1)\to\infty$  as  $n\to\infty$ .

### 3. THE EXTENDED CONJECTURE

Given n and k with  $n > k \ge 2$ . The so-called extended conjecture is the statement that the number of different solutions of the Diophantine equation

$$\left(\sum_{i=1}^n x_i\right)^k = \prod_{i=1}^n x_i$$

is infinite, namely,  $N(n, k) = \infty$ .

In what follows, we will prove the extended conjecture.

**Theorem 1:** For  $n > k \ge 2$ , the Diophantine equation

$$\left(\sum_{i=1}^{n} x_i\right)^k = \prod_{i=1}^{n} x_i \tag{5}$$

has infinitely many solutions, namely,  $N(n, k) = \infty$ .

We shall accomplish the proof using three lemmas.

**Lemma 1:** For given integers  $m \ge 0$ ,  $\lambda \ge 1$ , and  $r \ge 2$ , if the equation

$$\left(m + \sum_{i=1}^{r} x_i\right)^2 = \lambda \prod_{i=1}^{r} x_i \tag{6}$$

has a solution, then it has infinitely many solutions.

**Proof:** For the simplest case m = 0 and r = 2, let the equation

$$(x_1 + x_2)^2 = \lambda x_1 x_2 \tag{7}$$

have a solution  $(x_1, x_2) = (a_1, a_2)$ . Without loss of generality, assume  $gcd(a_1, a_2) = 1$ . Then (7) implies  $a_1 | a_2^2$ ,  $a_2 | a_1^2$ , so that  $a_1 = a_2 = 1$  and consequently  $\lambda = 4$ . Now, evidently, (7) has infinitely many solutions  $(x_1, x_2)$  with  $x_1 = x_2$  and  $\lambda = 4$ .

Consider the general case m > 0 or r > 2. Now suppose (6) has a solution  $A = (a_1, a_2, ..., a_r)$  with  $a_1 \ge a_2 \ge \cdots \ge a_r$ . We shall construct a solution  $B = (b_1, b_2, ..., b_r)$  with  $b_1 \ge b_2 \ge \cdots \ge b_r$  different from A as follows. Denote  $||A|| = \max_{1 \le i \le r} a_i = a_1$ . Consider the quadratic equation in t:

$$\left(m + \sum_{i=1}^{r-1} a_i + t\right)^2 = \lambda \left(\prod_{i=1}^{r-1} a_i\right) t. \tag{8}$$

i.e.,

$$t^{2} + \left\{ 2\left(m + \sum_{i=1}^{r-1} a_{i}\right) - \lambda \prod_{i=1}^{r-1} a_{i} \right\} t + \left(m + \sum_{i=1}^{r-1} a_{i}\right)^{2} = 0.$$

By supposition, (8) has a root  $t_1 = a_r$ . Using the relations between the roots and coefficients (Vieta's theorem), we see that the second root is given by

$$t_2 = \lambda \sum_{i=1}^{r-1} a_i - 2 \left( m + \sum_{i=1}^{r-1} a_i \right) - t_1 = \left( m + \sum_{i=1}^{r-1} a_i \right)^2 / t_1.$$
 (9)

From (9), we see that  $t_2$  is an integer and, moreover,

$$t_2 = \left(m + \sum_{i=1}^{r-1} a_i\right)^2 / a_r > a_1^2 / a_r \ge a_1.$$

Now let us take  $b_1 = t_2$ ,  $b_2 = a_1$ ,  $b_3 = a_2$ , ...,  $b_r = a_{r-1}$ . From (8), it is clear that  $B = (b_1, b_2, ..., b_r)$  is a solution of (6) with  $||B|| = \max_i b_i = b_1 = t_2 > a_1 = ||A||$ , i.e., ||B|| > ||A||.

Generally, if (6) has a solution  $x^{(0)} = (x_1^{(0)}, x_2^{(0)}, ..., x_r^{(0)})$  with  $x_1^{(0)} \ge x_2^{(0)} \ge ... \ge x_r^{(0)}$ , then the recursive algorithm

$$\begin{cases} x_1^{(j+1)} = \lambda \prod_{i=1}^{r-1} x_i^{(j)} - 2 \left( m + \sum_{i=1}^{r-1} x_i^{(j)} \right) - x_r^{(j)}, \\ x_2^{(j+1)} = x_1^{(j)}, x_3^{(j+1)} = x_i^{(j)}, \dots, x_r^{(j+1)} = x_{r-1}^{(j)}, \end{cases}$$
(10)

will yield infinitely many solutions  $x^{(j)} = (x_1^{(j)}, x_2^{(j)}, ..., x_r^{(j)}), j = 0, 1, 2, ...,$  such that  $||x^{(0)}|| < ||x^{(1)}|| < ||x^{(2)}|| < \cdots$ .

**Lemma 2:** Let m > 0 and  $r \ge 3$ . Then the equation

$$\left(m + \sum_{i=1}^{r} x_i\right)^2 = \prod_{i=1}^{r} x_i \tag{11}$$

has infinitely many solutions.

**Proof:** Equation (11) is a form of (6) with  $\lambda = 1$ . Now (11) has a solution  $x_1 = 5(m+r+2)$ ,  $x_2 = 4(m+r+2)$ ,  $x_3 = 5$ ,  $x_i = 1$ , i = 4, 5, ..., r. In fact,

$$\left(m + \sum_{i=1}^{r} x_i\right)^2 = \left(m + 5(m+r+2) + 4(m+r+2) + 5 + (r-3)\right)^2 = 100(m+r+2)^2 = \prod_{i=1}^{r} x_i. \quad \Box$$

Hence, Lemma 2 follows from Lemma 1.

In particular, taking m = 0 in (11), we get

Corollary 3:  $N(n, 2) = \infty$ , where  $n \ge 3$ .

**Lemma 3:** Let  $m \ge 1, r \ge 3$ . Then

$$m\left(\sum_{i=1}^{r} x_i\right)^2 = \prod_{i=1}^{r} x_i \tag{12}$$

has infinitely many solutions.

**Proof:** For the case r = 3, the substitution  $x_i - my_i$  (i = 1, 2, 3) in (12) leads to

$$\left(\sum_{i=1}^3 y_i\right)^2 = \prod_{i=1}^3 y_i.$$

For the case r > 3, taking  $x_r = m$ , we find that (12) becomes

$$\left(m + \sum_{i=1}^{r-1} x_i\right)^2 = \prod_{i=1}^{r-1} x_i.$$

Hence, Lemma 3 is implied by Lemma 2. □

**Proof of Theorem 1:** It suffices to prove the theorem " $N(n, k) = \infty$ " for the case  $k \ge 3$ . In (12), let us take

$$m = 2^{(k-2)(k+3)/2}, \quad r = n-k+2.$$

We will now show that from every solution  $A = (a_1, a_2, ..., a_r)$  with  $a_1 \le a_2 \le ... \le a_r$  of (12) there can be constructed a solution  $x = (x_1, ..., x_n)$  of (9) by the following:

$$\begin{cases} x_i = a_1, \ 1 = 1, 2, ..., r; \\ x_{r+j} = 2^{j-1} \sum_{i=1}^r a_i, \ j = 1, 2, ..., k-2. \end{cases}$$
 (13)

In fact we have, by computation:

$$\left(\sum_{i=1}^{n} x_{i}\right)^{k} = \left[\sum_{i=1}^{r} a_{i} + \sum_{j=1}^{k-2} \left(2^{j-1} \sum_{i=1}^{r} a_{i}\right)\right]^{k} = \left(1 + \sum_{j=1}^{k-2} 2^{j-1}\right)^{k} \left(\sum_{i=1}^{r} a_{i}\right)^{k} = 2^{k(k-2)} \left(\sum_{i=1}^{r} a_{i}\right)^{k},$$

and

$$\prod_{i=1}^{n} x_{i} = \prod_{i=1}^{r} a_{i} \cdot \prod_{i=1}^{k-2} \left( 2^{j-1} \sum_{i=1}^{r} a_{i} \right)^{2} = m \left( \sum_{i=1}^{r} a_{i} \right)^{2} \cdot 2^{(k-2)(k+3)/2} \left( \sum_{i=1}^{r} a_{i} \right)^{k-2} = 2^{k(k-2)} \left( \sum_{i=1}^{r} a_{i} \right)^{k}.$$

That is,

$$\left(\sum_{1}^{n} x_{i}\right)^{k} = \prod_{1}^{n} x_{i}.$$

Clearly,  $x_1 \le x_2 \le \cdots \le x_{r+k-2} = x_n$  so that ||x|| > ||A||. The recursive algorithm (10) implies that  $\{||A||\}$  is unbounded, so is  $\{||x||\}$ . Hence, (5) also has infinitely many solutions.  $\square$ 

**Theorem 2:** For  $n \ge 2k \ge 4$ , the Diophantine equation

$$\left(\sum_{i=1}^n x_i\right)^k = \prod_{i=1}^m x_i$$

has at least p(k) distinct solutions  $(x_i, ..., x_n)$  which are contained in the simplex domain

$$0 < \sum_{i=1}^{n} x_{i} < (k+1)^{k+1} + (k+1)n \quad (x_{i} > 0),$$

where p(k) is the partition function of k.

**Proof:** Every partition of k may be represented by the summation

$$k = \alpha_1 + \alpha_2 + \dots + \alpha_v \quad (1 \le v \le k),$$

where  $\alpha_i$  are positive integers such that  $1 \le \alpha_1 \le \alpha_2 \le \cdots \le \alpha_v$ . Denote n = m + k + 1 with  $m \ge k - 1$ . Then, corresponding to each partition  $(\alpha_1 + \alpha_2 + \cdots + \alpha_v)$  of k, one can construct a solution of the equation as follows:

$$\begin{cases} x_i = (k+1)^{\alpha_1} + (k+1)^{\alpha_2} + \dots + (k+1)^{\alpha_{\nu}} + m - \nu + 1 \text{ for } i = 1, \dots, k, \\ x_{k+1} = (k+1)^{\alpha_1}, x_{k+2} = (k+1)^{\alpha_2}, \dots, x_{k+\nu} = (k+1)^{\alpha_{\nu}}; \\ x_j = 1 \text{ for } j = k + \nu + 1, \dots, k + m + 1. \end{cases}$$

In fact, it may be verified at once that

$$\left(\sum_{i=1}^{n} x_{i}\right)^{k} = \left\{ \left[k(k+1)^{\alpha_{1}} + \dots + (k+1)^{\alpha_{v}} + m - v + 1\right] \cdot k + \sum_{i=1}^{v} (k+1)^{\alpha_{i}} + m - v + 1\right\}^{k}$$

$$= \left[(k+1)^{\alpha_{1}} + \dots + (k+1)^{\alpha_{v}} + m - v + 1\right]^{k} \cdot (k+1)^{k}$$

$$= \left[(k+1)^{\alpha_{1}} + \dots + (k+1)^{\alpha_{v}} + m - v + 1\right]^{k} \prod_{i=1}^{v} (k+1)^{\alpha_{i}} = \prod_{i=1}^{n} x_{i}.$$

Evidently the solution constructed above satisfies the condition

$$\sum_{i=1}^{n} x_i = [(k+1)^{\alpha_1} + \dots + (k+1)^{\alpha_{\nu}} + m - \nu + 1](k+1)$$

$$\leq [(k+1)^k + m](k+1) < (k+1)^{k+1} + (k+1)n.$$

Hence, all the p(k) distinct solutions are contained in the simplex domain as mentioned in the theorem.  $\Box$ 

**Example 3:** For n = 10, k = 5, the equation  $(\sum_{i=1}^{10} x_i)^5 = x_1 x_2 \cdots x_{10}$  has as least p(5) = 7 different solutions contained in the interior of the region:  $0 < x_1 + x_2 + \cdots + x_{10} < 6^6 + 60$   $(x_i \ge 0)$ .

## **ACKNOWLEDGMENTS**

The authors thank the referee and Professor John Selfridge for their useful suggestions that led to an improved version of this manuscript.

## REFERENCES

- 1. R. K. Guy. *Unsolved Problems in Number Theory (Problem D24)*. 2nd ed. New York-Heidelberg-Berlin: Springer-Verlag, 1994.
- 2. David Singmaster, Mike Bennett, & Andrew Dunn. "Sum=Product Sequences." Preprint. Polytechnic of the South Bank, London, SE1 0AA, England, 1993.
- 3. David Singmaster. "Untitled Brain Twister." *The Daily Telegraph*, Weekend Telegraph Section (9 E 16 April 1988), XV.

AMS Classification Numbers: 11A25, 11D41, 11D72

## REAL PELL AND PELL-LUCAS NUMBERS WITH REAL SUBSCRIPTS

## Alwyn F. Horadam

University of New England, Armidale, NSW 2351, Australia

## Piero Filipponi

Fondazione Ugo Bordoni, Via B. Castiglione 59, I-00142, Rome, Italy (Submitted February 1994)

## 1. INTRODUCTION AND GENERALITIES

The aim of this note is to extend the ideas explored in [3] to Pell numbers  $P_n$  and Pell-Lucas numbers  $Q_n$ .

More precisely, we shall parallel the arguments of [3] (the contents of which the reader is assumed to be aware of) to obtain expressions for both Pell numbers  $P_x$  and Pell-Lucas numbers  $Q_x$  which are *real* when the subscript  $x \ge 0$  is a real quantity. Of course, these numbers (or better, functions) and the usual Pell numbers and Pell-Lucas numbers coincide when x = n is an integer. It will be shown that  $P_x$  and  $Q_x$  enjoy some of the main properties of  $P_n$  and  $Q_n$ .

For the convenience of the reader, let us recall the Binet forms for Pell and Pell-Lucas numbers and some identities involving them. These are (e.g., see [1], [5])

$$P_n = (\alpha^n - \beta^n) / \sqrt{8} \quad \text{(Binet form)}, \tag{1.1}$$

$$Q_n = \alpha^n + \beta^n$$
 (Binet form), (1.2)

where

$$\alpha = -1/\beta = 2 - \beta = 1 + \sqrt{2}, \tag{1.3}$$

$$P_{n+2} = 2P_{n+1} + P_n$$
 [ $P_0 = 0, P_1 = 1$ ] (recurrence relation), (1.4)

$$Q_{n+2} = 2Q_{n+1} + Q_n \quad [Q_0 = Q_1 = 2]$$
 (recurrence relation), (1.5)

$$Q_n = P_{n-1} + P_{n+1}, (1.6)$$

$$P_n Q_n = P_{2n}, \tag{1.7}$$

$$P_{n-1}P_{n+1} = P_n^2 + (-1)^n \quad \text{(Simson formula analogue)}, \tag{1.8}$$

and

$$8P_n^2 = Q_n^2 - 4(-1)^n. (1.9)$$

In section 2 the *exponential* representations for  $P_x$  and  $Q_x$  are defined for all x and coincide with  $P_n$  and  $Q_n$ , respectively, when n is an integer. In section 3 the *polynomial-exponential* representation for  $P_x$  is defined only for  $x \ge 0$  and coincides with  $P_n$  when n is a nonnegative integer, whereas the *polynomial-exponential* representation for  $Q_x$  is defined only for x > 0 and coincides with  $Q_n$  when n is a positive integer. In both sections some properties of these numbers are established. Finally, the application of a useful idea [7] is discussed briefly in section 4. It must be noted that, despite the fact that the numbers defined in sections 2-4 coincide only when x = n is an integer, they are denoted by the same symbol. Nevertheless, no misunderstanding can arise since each definition applies only to the appropriate section. The notation

 $\lambda(x)$ , the greatest integer not exceeding x,

 $\phi(x) = x - \lambda(x)$ , the fractional part of x,

will be used, and the following properties of  $\lambda(x)$  will be taken into account throughout the proofs:

$$\lambda[(x\pm 1)/2] = \lambda(x/2) \pm [1\mp (-1)^{\lambda(x)}]/2, \tag{1.10}$$

$$\lambda[(x-2)/2] = \lambda(x/2) - 1, \tag{1.11}$$

$$2\lambda(x/2) = \lambda(x) - [1 - (-1)^{\lambda(x)}]/2, \qquad (1.12)$$

$$\lambda(-x) = -\lambda(x) - 1$$
 [i.e.,  $\lambda(x) + \lambda(-x) = -1$ ], if  $\phi(x) > 0$ . (1.13)

The proofs of (1.10)-(1.13) are not difficult but they are very lengthy and tedious. They are left to the perseverance of the reader. Further, the conventions

$$\begin{pmatrix} x \\ -k \end{pmatrix} = 0$$
, if  $k \ge 1$  is an integer ([2], p. 48) (1.14)

and

$$\sum_{i=a}^{b} f(i) = 0, \text{ if } b < a$$
 (1.15)

will be assumed.

## 2. EXPONENTIAL REPRESENTATION OF $P_x$ AND $Q_x$

Keeping the Binet forms (1.1) and (1.2), and the definitions (2.13) and (2.14) of [3] in mind, leads us to define

$$P_{x} = \left[\alpha^{x} - (-1)^{\lambda(x)} \alpha^{-x}\right] / \sqrt{8}$$
 (2.1)

and

$$Q_x = \alpha^x + (-1)^{\lambda(x)} \alpha^{-x}$$
 (2.2)

As an illustration, the behavior of  $P_x$  vs x is shown in Figure 1 for  $0 \le x \le 8$ .

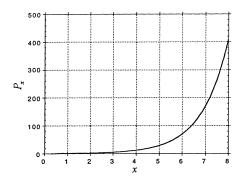


FIGURE 1. Behavior of  $P_x$  vs x for  $0 \le x \le 8$ 

The same function is plotted, within the interval  $0.5 \le x \le 2.5$  in Figure 2, to reveal the (rapidly decreasing) discontinuities connected with the integral values of x which are due to the greatest integer function inherent in the definition (2.1).

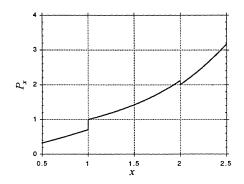


FIGURE 2. Graph of  $P_x$  vs x for  $0.5 \le x \le 2.5$ 

## 2.1. Some Properties of $P_x$ and $Q_x$

The numbers  $P_x$  and  $Q_x$  enjoy several properties of the usual Pell and Pell-Lucas numbers. For example, the identities (1.4)-(1.9) remain valid when n is replaced by x with only one exception. The exception is (1.7) which must be restated as follows.

## Proposition 1:

$$P_x Q_x = \begin{cases} P_{2x}, & \text{if } \phi(x) < \frac{1}{2}, \\ P_{2x} - \alpha^{-2x} / \sqrt{2} = Q_{2x} / \sqrt{8}, & \text{if } \phi(x) \ge \frac{1}{2}. \end{cases}$$

This will be proved later. Moreover, it must be noted that the quantity  $(-1)^n$  has to be replaced by  $(-1)^{\lambda(x)}$  in (1.8) and (1.9).

The evaluation of finite sums analogous to those considered in [3] gives the results

$$\sum_{k=0}^{n} T_{x+k} = \frac{1}{2} (T_{n+1+x} + T_{n+x} - T_x - T_{x-1}), \tag{2.3}$$

where T stands separately for P and O, and

$$\sum_{k=0}^{n-1} P_{k/n} = \frac{P_{(n-1)/n} + P_{1/n} - 1/\sqrt{2}}{2 - Q_{1/n}} \quad (n \ge 2),$$
 (2.4)

$$\sum_{k=0}^{n-1} Q_{k/n} = \frac{Q_{(n-1)/n} - Q_{1/n} - 2(\sqrt{2} - 1)}{2 - Q_{1/n}} \quad (n \ge 2).$$
 (2.5)

The identities (2.3)-(2.5) can be proved by using (2.1), (2.2), and the geometric series formula.

The extension of  $P_x$  and  $Q_x$  to negative values of the subscript x can be obtained by replacing x by -x in the definitions (2.1) and (2.2), and by taking (1.13) into account. To our great surprise, some simple calculations led to the following unexpected results

$$\begin{cases} P_{-x} = (-1)^{\lambda(x)} Q_x / \sqrt{8} \\ Q_{-x} = (-1)^{\lambda(x)+1} P_x \sqrt{8} \end{cases}$$
 for  $\phi(x) > 0$ , (2.6)

$$Q_{-r} = (-1)^{\lambda(x)+1} P_r \sqrt{8}$$
 for  $\varphi(x) > 0$ , (2.7)

which hold whenever x is not an integer. In spite of the unexpectedness of expessions (2.6) and (2.7), the numbers  $P_{-x}$  and  $Q_{-x}$  preserve many properties of  $P_{-n} = (-1)^{n+1}P_n$  and  $Q_{-n} = (-1)^nQ_n$ . For example, the identity

$$P_{-x}Q_{-x} = -P_xQ_x \quad \text{(see Proposition 1)}$$
 (2.8)

holds whatever the nature of x.

### 2.2. Some Detailed Proofs

For space reasons, only a few among the properties stated in section 2.1 will be proved in detail. It is worth mentioning that the following equalities involving the quantity  $\alpha$  [see (1.3)] are to be used in the proofs of (1.4)-(1.6):

$$2\alpha + 1 = \alpha^2, \tag{2.9}$$

$$1 - 2\alpha^{-1} = \alpha^{-2},\tag{2.10}$$

$$1 + \alpha^2 = \alpha \sqrt{8} \,. \tag{2.11}$$

**Proof of (1.5) (for n replaced by x):** By (2.2),

$$2Q_{x+1} + Q_x = 2[\alpha^{x+1} + (-1)^{\lambda(x+1)}\alpha^{-x-1}] + \alpha^x + (-1)^{\lambda(x)}\alpha^{-x}$$

$$= \alpha^x (2\alpha + 1) + (-1)^{\lambda(x)}\alpha^{-x} (1 - 2\alpha^{-1}) \quad [\text{since } \lambda(x+k) = \lambda(x) + k, k \text{ an integer})$$

$$= \alpha^{x+2} + (-1)^{\lambda(x)}\alpha^{-(x+2)} \quad [\text{by } (2.9), (2.10)]$$

$$= \alpha^{x+2} + (-1)^{\lambda(x)+2}\alpha^{-(x+2)}$$

$$= \alpha^{x+2} + (-1)^{\lambda(x+2)}\alpha^{-(x+2)}$$

$$= \alpha^{x+2} + (-1)^{\lambda(x+2)}\alpha^{-(x+2)}$$

$$= Q_{x+2} \quad [\text{by } (2.2)]. \quad \text{Q.E.D.}$$

**Proof of (1.8) (for n replaced by x):** By (2.1),

$$\begin{split} P_{x-1}P_{x+1} - P_x^2 &= ([\alpha^{x-1} + (-1)^{\lambda(x)}\alpha^{-x+1}][\alpha^{x+1} + (-1)^{\lambda(x)}\alpha^{-x-1}] - [\alpha^x - (-1)^{\lambda(x)}\alpha^{-x}]^2) / 8 \\ &= ([\alpha^{2x} + \alpha^{-2x} + (-1)^{\lambda(x)}(\alpha^2 + \alpha^{-2})] - [\alpha^{2x} + \alpha^{-2x} - 2(-1)^{\lambda(x)}]) / 8 \\ &= (-1)^{\lambda(x)}(\alpha^2 + \alpha^{-2} - 2) / 8 \\ &= (-1)^{\lambda(x)}(\alpha - \alpha^{-1})^2 / 8 \\ &= (-1)^{\lambda(x)} \quad \text{[since } \alpha - \alpha^{-1} = 2\sqrt{2}, \text{ by (1.3)].} \quad \text{Q.E.D.} \end{split}$$

**Proof of Proposition 1:** By (2.1) and (2.2),

$$\begin{split} P_{x}Q_{x} - P_{2x} &= (\alpha^{2x} - \alpha^{-2x}) / \sqrt{8} - [\alpha^{2x} - (-1)^{\lambda(2x)} \alpha^{-2x}] / \sqrt{8} \\ &= \alpha^{-2x} [(-1)^{\lambda(2x)} - 1] / \sqrt{8} \\ &= \begin{cases} 0, & \text{if } \lambda(2x) \text{ is even [i.e., if } \phi(x) < \frac{1}{2}], \\ -\alpha^{-2x} / \sqrt{2}, & \text{if } \lambda(2x) \text{ is odd [i.e., if } \phi(x) \ge \frac{1}{2}]. \end{cases} \quad \text{Q.E.D.} \end{split}$$

## 3. POLYNOMIAL-EXPONENTIAL REPRESENTATION OF $P_x$ AND $Q_x$

Keeping the definitions (1.6) and (1.7) of [4] and the definitions (3.4) and (3.5) of [3] in mind, leads us to define

$$P_{x} = \sum_{j=0}^{\lambda[(x-1)/2]} {x-1-j \choose j} 2^{x-1-2j} \quad (x \ge 0)$$
 (3.1)

and

$$Q_{x} = \sum_{j=0}^{\lambda(x/2)} \frac{x}{x+j} {x-j \choose j} 2^{x-2j} \quad (x>0).$$
 (3.2)

Observe that the binomial coefficient defined as

$$\begin{pmatrix} x \\ 0 \end{pmatrix} = 1, \quad \begin{pmatrix} x \\ k \end{pmatrix} = \frac{x(x-1)\cdots(x-k+1)}{k!} \quad (k \ge 1, \text{ an integer})$$
 (3.3)

makes sense ([2], p. 48) also if x is any real quantity. Moreover, observe that

- (i) for x = 0, the expression (3.2) gives the indeterminate form 0/0 so that  $Q_0 = 2$  cannot be defined by (3.2),
- (ii) by (1.13) and (1.15), we see that the expression (3.1) allows us to get  $P_0 = 0$ , and the extension to negative values of x yields  $P_{-x} = Q_{-x} = 0$ .

As an illustration, we show the first few values of  $P_x$  and  $Q_x$ . They are

$$\begin{split} P_x &= 0 \quad (0 \le x < 1), \\ P_x &= 2^{x-1} \quad (1 \le x < 3), \\ P_x &= 2^{x-3}(x+2) \quad (3 \le x < 5), \\ P_x &= 2^{x-6}(x^2 + x + 28) \quad (5 \le x < 7) \\ P_x &= 2^{x-8} \bigg( \frac{1}{3} x^3 - x^2 + \frac{86}{3} x + 72 \bigg) \quad (7 \le x < 9) \\ P_x &= 2^{x-11} \bigg( \frac{1}{6} x^4 - \frac{5}{3} x^3 + \frac{203}{6} x^2 + \frac{155}{3} x + 856 \bigg) \quad (9 \le x < 11), \end{split}$$

and

$$Q_{x} = 2^{x} (0 < x < 2),$$

$$Q_{x} = 2^{x-2}(x+4) (2 \le x < 4),$$

$$Q_{x} = 2^{x-5}(x^{2} + 5x + 32) (4 \le x < 6),$$

$$Q_{x} = 2^{x-7} \left(\frac{1}{3}x^{3} + x^{2} + \frac{80}{3}x + 128\right) (6 \le x < 8),$$

$$Q_{x} = 2^{x-10} \left(\frac{1}{6}x^{4} - \frac{1}{3}x^{3} + \frac{155}{6}x^{2} + \frac{535}{3}x + 1024\right) (8 \le x < 10).$$

The behavior of  $P_x$  vs x is shown in Figure 3 for  $0 \le x \le 5.5$ .

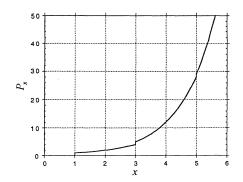


FIGURE 3. Behavior of  $P_x$  vs x for  $0 \le x \le 5.5$ 

## 3.1. Some Properties of $P_x$ and $Q_x$

Proposition 2:

$$2P_{x+1} + P_x = \begin{cases} P_{x+2}, & \text{if } \lambda(x) \text{ is even,} \\ P_{x+2} - \binom{x - \lambda(x/2) - 1}{\lambda(x/2) + 1} 2^{\phi(x)}, & \text{if } \lambda(x) \text{ is odd.} \end{cases}$$

Proposition 3:

$$2Q_{x+1} + Q_x = \begin{cases} Q_{x+2} - \frac{x+1}{x - \lambda(x/2)} \binom{x - \lambda(x/2)}{\lambda(x/2) + 1} 2^{\phi(x)}, & \text{if } \lambda(x) \text{ is even,} \\ Q_{x+2}, & \text{if } \lambda(x) \text{ is odd.} \end{cases}$$

**Proposition 4:**  $P_{x+1} + P_{x-1} = Q_x$ .

### 3.2. Proofs

**Proof of Proposition 2:** 

Case 1:  $\lambda(x)$  even. By (3.1) and (1.10), write

$$P_{x} + 2P_{x+1} = \sum_{j=0}^{\lambda(x/2)-1} {x-1-j \choose j} 2^{x-1-2j} + \sum_{j=0}^{\lambda(x/2)} {x-j \choose j} 2^{x+1-2j}$$
$$= \sum_{j=1}^{\lambda(x/2)} {x-j \choose j-1} 2^{x+1-2j} + \sum_{j=0}^{\lambda(x/2)} {x-j \choose j} 2^{x+1-2j}.$$

Taking (1.14) and (1.10) into account and using the basic recurrence ([8], p. 1) for the binomial coefficients (which holds also when the upper argument is not an integer) yields

$$P_{x} + 2P_{x+1} = \sum_{j=0}^{\lambda(x/2)} \left[ {x-j \choose j-1} + {x-j \choose j} \right] 2^{x+1-2j} = \sum_{j=0}^{\lambda(x/2)} {x+1-j \choose j} 2^{x+1-2j}$$
$$= \sum_{j=0}^{\lambda[(x+1)/2]} {x+1-j \choose j} 2^{x+1-2j} = P_{x+2}.$$

Case 2:  $\lambda(x)$  odd. By (3.1), (1.10), and (1.12), write

$$\begin{split} P_{x} + 2P_{x+1} &= \sum_{j=0}^{\lambda(x/2)} \binom{x-1-j}{j} 2^{x-1-2j} + \sum_{j=0}^{\lambda(x/2)} \binom{x-j}{j} 2^{x+1-2j} \\ &= \sum_{j=1}^{\lambda(x/2)+1} \binom{x-j}{j-1} 2^{x+1-2j} + \sum_{j=0}^{\lambda(x/2)} \binom{x-j}{j} 2^{x+1-2j} \\ &= \sum_{j=0}^{\lambda(x/2)+1} \binom{x-j}{j-1} 2^{x+1-2j} + \sum_{j=0}^{\lambda(x/2)+1} \binom{x-j}{j} 2^{x+1-2j} - X, \end{split} \tag{3.4}$$

where

$$X = {x - \lambda(x/2) - 1 \choose \lambda(x/2) + 1} 2^{x + 1 - 2\lambda(x/2) - 2} = {x - \lambda(x/2) - 1 \choose \lambda(x/2) + 1} 2^{x - \lambda(x)}.$$
 (3.5)

By (1.10), (3.5), and the basic recurrence for the binomial coefficients, expression (3.4) can be rewritten as

$$P_x + 2P_{x+1} = \sum_{j=0}^{\lambda[(x+1)/2]} {x+1-j \choose j} 2^{x+1-2j} - X = P_{x+2} - X.$$

The proposition follows, since  $\phi(x) = x - \lambda(x)$ . Q.E.D.

**Note:** (1) Since the upper argument of the binomial coefficient in (3.5) is less than the lower one, X = 0 whenever  $x \ge 1$  is an (odd) integer, giving  $2P_{x+1} + P_x = P_{x+2}$ .

(2) Proposition 3 may be proved in a way similar to Proposition 2.

**Proof of Proposition 4:** First, by (3.1), (3.2), and the binomial identity available in ([8], p. 64), write

$$Q_{x} = \sum_{j=0}^{\lambda(x/2)} \left[ {x-j \choose j} + {x-1-j \choose j-1} \right] 2^{x-2j} = P_{x+1} + \sum_{j=0}^{\lambda(x/2)} {x-1-j \choose j-1} 2^{x-2j}$$

$$= P_{x+1} + \sum_{j=-1}^{\lambda(x/2)-1} {x-2-j \choose j} 2^{x-2-2j}.$$
(3.6)

Then, use (1.14), (1.11), and (3.1) to rewrite (3.6) as

$$Q_x = P_{x+1} + \sum_{j=0}^{\lambda[(x-2)/2]} {x-2-j \choose j} 2^{x-2-2j} = P_{x+1} + P_{x-1}. \quad Q.E.D.$$

## 4. CONCLUDING REMARKS

In this note, definitions have been proposed for Pell numbers  $P_x$  and Pell-Lucas numbers  $Q_x$  which are real when the subscript x is real. We feel that this particular study might be concluded suitably by observing that the idea explored in [7] applies beautifully to the afore-said numbers (see also [6]). In fact, following [7], we can define

$$P_x = \left[\alpha^x - \cos(\pi x)\alpha^{-x}\right]/\sqrt{8} \tag{4.1}$$

and

$$Q_x = \alpha^x + \cos(\pi x)\alpha^{-x}. (4.2)$$

The numbers  $P_x$  and  $Q_x$  defined in this way and the usual Pell and Pell-Lucas numbers obviously coincide when x is an integer. Moreover, their behavior vs x does not present any discontinuity, as shown in Figure 4 in the case of  $Q_x$ .

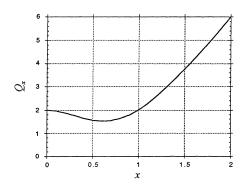


FIGURE 4. Behavior of  $Q_x$  vs x for  $0 \le x \le 2$ 

Some properties of these numbers are reported in the sequel. Their proofs are left as an exercise for the interested reader. It should be noted that (4.1) and (4.2) occur in [6] as x coordinates of points on Pell and Pell-Lucas curves. Both x- and y-coordinates for these curves were obtained independently of [7] as special cases of coordinates for a system of more general curves [6].

The identities (1.4)-(1.6) remain valid for  $P_x$  and  $Q_x$ , whereas the identity (1.7) does not. More precisely, we have

$$P_{x}Q_{x} = P_{2x} - \left[\sin^{2}(\pi x)\alpha^{-2x}\right] / \sqrt{8}. \tag{4.3}$$

Moreover, the analogue of (1.8) is

$$P_{x-1}P_{x+1} - P_x^2 = \cos(\pi x). \tag{4.4}$$

The extensions of (4.1) and (4.2) to negative values of x lead to

$$P_{-x} = \begin{cases} \left[\sin^2(\pi x)\alpha^x / \sqrt{8} - P_x\right] / \cos(\pi x), & \text{if } \phi(x) \neq \frac{1}{2}, \\ P_x^{-1} / 8, & \text{if } \phi(x) = \frac{1}{2}, \end{cases}$$
(4.5)

and

$$Q_{-x} = \begin{cases} [Q_x - \sin^2(\pi x)\alpha^x] / \cos(\pi x), & \text{if } \phi(x) \neq \frac{1}{2}, \\ Q_x^{-1}, & \text{if } \phi(x) = \frac{1}{2}. \end{cases}$$
(4.6)

Since the reader might find some difficulty in deriving (4.5) and (4.6), we give a sketch of the proof of (4.5).

**Proof of (4.5) (a sketch):** Replace x by -x in (4.1), thus getting

$$P_{-x} = [\alpha^{-x} - \cos(\pi x)\alpha^{x}]/\sqrt{8}$$
 [since  $\cos(-y) = \cos y$ ]. (4.7)

If  $\phi(x) = \frac{1}{2}$ , then  $\cos(\pi x) = 0$  so that  $P_x = \alpha^x / \sqrt{8}$  [see (4.1)], and  $P_x^{-1} = \sqrt{8}\alpha^{-x} = 8\alpha^{-x} / \sqrt{8} = 8P_{-x}$  [see (4.7)]. If  $\phi(x) \neq \frac{1}{2}$  [i.e.,  $\cos(\pi x) \neq 0$ ], multiply both sides of (4.7) by  $\cos(\pi x)$ , and use the identity  $\cos^2 y = 1 - \sin^2 y$  to obtain the right-hand side of (4.5). Q.E.D.

The proof of (4.6) is similar. Observe that (4.5) and (4.6) do not satisfy the analogue of (2.8) for  $\phi(x) > 0$ . In particular, when  $\phi(x) = \frac{1}{2}$  (i. e.,  $x = n + \frac{1}{2}$ ), we have

$$P_x Q_x + P_{-x} Q_{-x} = P_{2n+1}. (4.8)$$

Furthermore, the identity (2.3) remains valid for  $P_x$  and  $Q_x$ , whereas an attempt to find the identities corresponding to (2.4) and (2.5) required a great amount of calculations involving the use of Euler formulas for circular functions and the geometric series formula, and produced a couple of very unpleasant expressions. As an illustration, we exhibit the second one. This is

$$\sum_{k=0}^{n-1} Q_{k/n} = \frac{\sqrt{2} \left[ \sqrt{8} P_{1/n} + \alpha^{-2/n} - \cos(\pi/n) \right]}{Q_{1/n} + \alpha^{-1/n} - \alpha^{-2/n} + (\alpha^{-1/n} - 2) \cos(\pi/n) - 1}.$$
(4.9)

The closed-form expression of the analogous sum

$$\sum_{k=0}^{n-1} Q_{k/n} \alpha^{k/n} = \frac{\alpha^2 - 1}{\alpha^{2/n} - 1} + 1$$
 (4.10)

is much simpler even though perhaps less interesting.

#### **ACKNOWLEDGMENT**

The contribution of the second author has been given within the framework of an agreement between the Italian PT Administration and the Fondazione Ugo Bordoni.

## REFERENCES

- M. Bicknell. "A Primer on the Pell Sequence and Related Sequences." The Fibonacci Quarterly 13.4 (1975):345-49.
- 2. W. Feller. *An Introduction to Probability Theory and Its Applications*. Vol I. 2nd ed. New York: Wiley, 1957.
- 3. P. Filipponi. "Real Fibonacci and Lucas Numbers with Real Subscripts." *The Fibonacci Quarterly* **31.4** (1993):307-14.
- 4. P. Filipponi & A. F. Horadam. "Derivative Sequences of Fibonacci and Lucas Polynomials." In *Applications of Fibonacci Numbers*, **4:**99-108. Ed. G. E. Bergum, A. N. Philippou, & A. F. Horadam. Dordrecth: Kluwer, 1991.
- 5. A. F. Horadam & Bro. J. M. Mahon. "Pell and Pell-Lucas Polynomials." *The Fibonacci Quarterly* **23.1** (1985):7-20.
- 6. A. F. Horadam. "Jacobsthal and Pell Curves." The Fibonacci Quarterly 26.1 (1988):77-83.
- 7. F. D. Parker. "A Fibonacci Function." The Fibonacci Quarterly 6.1 (1968):1-2.
- 8. J. Riordan. Combinatorial Identities. New York: Wiley, 1968.

AMS Classification Numbers: 11B65, 33B10, 11B39

## ON DECIMATION OF LINEAR RECURRING SEQUENCES

## Jovan Dj. Golić

Information Security Research Centre, Queensland University of Technology GPO Box 2434, Brisbane Qld 4001, Australia School of Electrical Engineering, University of Belgrade (Submitted March 1994)

#### 1. INTRODUCTION

The problem of obtaining a linear recursion for a decimated sequence in terms of the linear recursion for the original finite field sequence has been studied extensively in the literature either from a mathematical point of view or in connection with various applications mostly having to do with high-speed parallel generation of linear recurring sequences. A survey of such applications, mainly in spread spectrum communications and cryptography, can be found in [4]. The special case of sequences satisfying primitive or irreducible polynomials was treated in [10], [7], and [3], whereas the general case was settled in [2]. Alternative approaches to the general case were given in [5], [6], [8], and [4]. Recently, the results from [2] have been extended to arbitrary fields [1] by using the results on products of linear recurring sequences from [11]. Unlike the method from [2], which is based on the decimation of individual sequences, the method from [1] deals with vector spaces of sequences.

In this paper we develop a novel approach that enables us to determine the minimum generating polynomial of decimated sequences over an arbitrary field in a simple and self-contained way. This is achieved starting from a new characterization of this polynomial and by using some facts from the general field theory, without invoking any results on product sequences. Some new properties of decimated sequences are also pointed out.

## 2. PRELIMINARIES

Let F be an arbitrary field, let  $s = \{s(t)\}_{t=0}^{\infty}$  denote a sequence over F, and let  $f(x) = \sum_{i=0}^{n} c_i x^i$  be a polynomial over F such that  $f(0) \neq 0$ . Then s is called a *linear recurring sequence* satisfying f if

$$\sum_{i=0}^{n} c_{i} s(t+i) = 0, \quad t \ge 0.$$
 (1)

Let  $L_F(f)$  or simply L(f) denote the set of all s over F that satisfy f. If the degree of f is n, then L(f) is an n-dimensional vector space over F which is closed under the translate operator  $Ts = \{s(t+1)\}_{t=0}^{\infty}$ . For every linear recurring sequence s over F, the unique monic polynomial g over F of lowest degree satisfied by s is called the *minimum polynomial* of s and s is called a *regular sequence* of g, see [2]. The minimum polynomial of a finite set of linear recurring sequences is defined analogously and is equal to the least common multiple of the minimum polynomials of individual sequences, see [10].

Given a sequence s over F and a positive integer d, the decimation of s by d,  $s^{(d)}$ , is defined by  $s^{(d)}(t) = s(td)$ ,  $t \ge 0$ . Analogously, given a set S of sequences over F, the decimation of S by d,  $S^{(d)}$ , is defined by  $S^{(d)} = \{s^{(d)} : s \in S\}$ . Besides, given a nonnegative integer  $\tau$ , the translate of s by  $\tau$ ,  $s_{(\tau)}$ , is defined by  $s_{(\tau)}(t) = s(t+\tau)$ ,  $t \ge 0$ , that is,  $s_{(\tau)} = T^{\tau}s$ .

The set  $L^{(d)}(f)$  is a vector space over F generated by the set  $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{n-1}$  of decimated sequences obtained from the successive translates of any regular sequence s of f of degree n. Since  $L^{(d)}(f)$  is closed under the translate operator,  $L^{(d)}(f) = L(h)$ , where h is the minimum polynomial of the set  $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{n-1}$ . Moreover, since every sequence from  $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{n-1}$  is a translate of a sequence from  $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{n-1}$  and since the minimum polynomial of a translate divides the minimum polynomial of the original sequence, h is also the minimum polynomial of the set  $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{d-1}$ . This set is important for the high-speed parallel generation of s, because s can be obtained by interleaving the corresponding decimated sequences generated at d times lower speed than s.

For a finite field F, Duvall and Mortick [2] obtained the minimum polynomial h in terms of f, d, and the characteristic of F, by considering the decimations of sequences from an appropriate basis of L(f). Recently, by using the results from [11] on product sequences, Buck and Zierler [1] have developed a new method which enabled them to extend the result [2] to arbitrary fields. Polynomials with multiple roots in both [2] and [1] are dealt with in relatively involved ways, which is also the case with inseparable polynomials in [1]. In the next section, we show how the minimum polynomial of decimated sequences can be derived in a new way that is both simple and compact. Instead of the results on product sequences, it is based on some facts from the general field theory and treats the inseparable and separable polynomials in a unified way.

## 3. MINIMUM POLYNOMIAL OF DECIMATED SEQUENCES

Our objective is to derive the minimum polynomial of the set  $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{d-1}$  of d sequences obtained from the decimation by d of d successive translates of an arbitrary linear recurring sequence s over a field F. To this end, first note that the original sequence s can be obtained by interleaving the considered d decimated sequences. Second, for an arbitrary polynomial g over F such that  $g(0) \neq 0$ ,  $L(g(x^d))$  is the set of all the sequences obtained by interleaving d members of L(g(x)), see [1]. Therefore, for an arbitrary polynomial g over F,  $g(0) \neq 0$ , if s is a regular sequence of a polynomial f over F,  $f(0) \neq 0$ , then  $f(x)|g(x^d)$  holds if and only if the decimated sequences  $s_{(\tau)}^{(d)}$ ,  $0 \leq \tau \leq d-1$ , all satisfy g. In view of the definition of minimum polynomials, we thus obtain the following simple characterization of the minimum polynomial of the considered decimated sequences.

**Theorem 1:** Let f be a monic polynomial over F,  $f(0) \neq 0$ , let d be a positive integer, and let s be a regular sequence of f. The minimum polynomial of the set of decimated sequences  $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{d-1}$  is then equal to the unique monic polynomial g over F of minimum degree such that  $f(x)|g(x^d)$ .

Since the minimum polynomial established in Theorem 1 depends only of f and d, we adopt the notation  $f_{(d)}$ . It remains to find out an explicit characterization of  $f_{(d)}$ . We proceed in three steps by proving the following lemmas.

**Lemma 1:** Let  $f = 1.c.m.(f_1, f_2)$ , where  $f_1$  and  $f_2$  are monic polynomials over F,  $f_1(0) \neq 0$ ,  $f_2(0) \neq 0$ . Then  $f_{(d)} = 1.c.m.(f_{1,(d)}, f_{2,(d)})$ .

**Proof:** Let  $h = 1.c.m.(f_{1,(d)}, f_{2,(d)})$ . We use the fact, already noted in the proof of Theorem 1, that  $a(x)|b(x^d) \Leftrightarrow a_{(d)}|b$ , for arbitrary monic polynomials a and b over F,  $a(0) \neq 0$ ,  $b(0) \neq 0$ .

Accordingly, for an arbitrary monic polynomial g over F,  $g(0) \neq 0$ , it follows that  $f(x)|g(x^d) \Leftrightarrow f_i(x)|g(x^d)$ ,  $i = 1, 2 \Leftrightarrow f_{i,(d)}|g$ ,  $i = 1, 2 \Leftrightarrow h|g$ . Hence,  $h = f_{(d)}$ .

**Lemma 2:** Let f be a monic and irreducible polynomial over F,  $f(0) \neq 0$ , and let  $\alpha$  be any root of f in a splitting field E of f. Then  $f_{(d)}$  is the minimum polynomial of  $\alpha^d$  over F.

**Proof:** First, note that the minimum polynomial h of  $\alpha^d$  over F exists because E is an algebraic extension of F. We employ the well-known result, see [9], that the minimum polynomial of an element  $\gamma$  algebraic over F must divide every polynomial g over F such that  $g(\gamma) = 0$ . It suffices to prove that  $f(x)|g(x^d) \Leftrightarrow g(\alpha^d) = 0$  for an arbitrary monic polynomial g over F,  $g(0) \neq 0$ . Namely, by the definition of the minimum polynomial, it then follows that  $f_{(d)} = h$ . The implication " $\Rightarrow$ " is clear because  $\alpha$  is then a root of  $g(x^d)$ . The implication " $\Leftarrow$ " is true because, if  $\alpha$  is a root of  $g(x^d)$ , then the minimum polynomial of  $\alpha$ , which is f, must divide  $g(x^d)$ .  $\bullet$ 

**Lemma 3:** Let  $f = g^r$ , where g is a monic and irreducible polynomial over F,  $g(0) \neq 0$ , and r is a positive integer. If F has characteristic p = 0, then  $f_{(d)} = g_{(d)}^r$ . If F has characteristic p > 0,  $d = kp^c$ ,  $p \nmid k$ , and  $e \geq 0$  is the exponent of inseparability of g, then  $f_{(d)} = g_{(d)}^{[r/p^{\max(e-e,0)}]}$ , [z] denoting the smallest integer not smaller than a real number z.

**Proof:** We first prove that  $f_{(d)} = g_{(d)}^t$  for some positive integer t. Note that by Lemma 2  $g_{(d)}$  is irreducible. Assume that  $f_{(d)} = ag_{(d)}^t$ , where  $g_{(d)} \nmid a$ . Then the minimality of  $f_{(d)}$  implies that  $g^r(x)|a(x^d)g_{(d)}^t(x^d)$  and  $g^r(x)\nmid g_{(d)}^t(x^d)$ . Since g is irreducible, then  $g(x)|a(x^d)$ ; hence,  $g_{(d)}|a$ , which contradicts the assumption.

To determine t, we should analyze the multiplicities of the roots of g,  $g_{(d)}$ , and  $g_{(d)}(x^d)$ . We use some well-known facts from the general field theory (see [9], Ch. II, §1-6). If the characteristic p of F is zero, then both g and  $g_{(d)}$  are separable and the roots of g,  $g_{(d)}$ , and  $g_{(d)}(x^d)$  are all simple. Then t = r. If F has characteristic p > 0,  $d = kp^c$ ,  $p \nmid k$ , and  $e \ge 0$  is the exponent of inseparability of g (g is separable if e = 0), then all the roots of g have multiplicity  $p^e$ . Note that the exponent of inseparability of g is equal to the minimum nonnegative integer i such that  $\alpha^{p^i}$  is separable over F, where  $\alpha$  is is a root of g in a splitting field of g. Therefore, the exponent of inseparability of the minimum polynomial  $g_{(d)}$  of  $\alpha^d$  is  $\max(e-c,0)$ ; hence, all the roots of  $g_{(d)}$  have multiplicity  $p^{\max(e-c,0)}$ . Finally, all the roots of  $g_{(d)}(x^d)$  have  $p^c$  times larger multiplicity than the roots of  $g_{(d)}$ , that is,  $p^{\max(e,c)}$ . Then t is the minimum positive integer j such that  $rp^e \le jp^{\max(e,c)}$ .

Consequently, in view of Theorem 1, Lemmas 1, 2, and 3 result in the following characterization of the minimum polynomial of decimated sequences.

**Theorem 2:** Let f be a monic polynomial over F,  $f(0) \neq 0$ , that factors as  $f = \prod_{i=1}^m f_i^{r_i}$ , where  $f_i$  are distinct monic and irreducible polynomials, let d be a positive integer, and let s be a regular sequence of f. Then the minimum polynomial of the set of decimated sequences  $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{d-1}$  is given by

$$f_{(d)} = 1. \text{ c. m.} \left( f_{i,(d)}^{t_i} : 1 \le i \le m \right),$$
 (2)

where  $f_{i,(d)}$  is the minimum polynomial of  $\alpha_i^d$  over F,  $\alpha_i$  being any root of  $f_i$  in a splitting field of f,  $t_i = r_i$  if F has characteristic zero, and  $t_i = [r_i / p^{\max(c - e_i, 0)}]$  if F has characteristic p > 0,  $d = kp^c$ ,  $p \nmid k$ , and  $e_i \ge 0$  is the exponent of inseparability of  $f_i$ ,  $1 \le i \le m$ .

Theorem 2 specifies  $f_{(d)}$  as the minimum polynomial of a set of d decimated sequences rather than the set of all the decimated sequences, which is interesting for parallel generation of linear recurring sequences. As is shown in Section 2,  $L^{(d)}(f) = L(f_{(d)})$  also holds, so that expression (2) is equivalent to the one from [1]. However, our characterization is slightly different because of the unified treatment of inseparable and separable polynomials and because of the different treatment of the root multiplicities.

Finally, we also prove the following properties yielding a necessary and sufficient condition for the minimum polynomial of a decimated sequence to depend only on the minimum polynomial of the original sequence, which is interesting for cryptographic applications. Note that the proof makes no use of Theorem 2.

**Proposition:** Let f be a monic polynomial over F,  $f(0) \neq 0$ , and let d be a positive integer. Then the decimation by d defines a homomorphism of L(f) onto  $L(f_{(d)})$ ; hence,  $\deg f_{(d)} \leq \deg f$ . If and only if  $\deg f_{(d)} = \deg f$ , then the decimation by d defines an isomorphism of L(f) onto  $L(f_{(d)})$ . Furthermore, if  $\deg f_{(d)} = \deg f$ , then the minimum polynomial of  $s^{(d)}$  is  $f_{(d)}$  for every regular sequence s of f.  $\bullet$ 

**Proof:** The proof of the first assertion is straightforward. The second assertion directly follows from the well-known fact in the theory of vector spaces (see [9], Ch. I, §21), that a homomorphism of a finite-dimensional vector space onto another vector space is an isomorphism if and only if their dimensions are equal (otherwise, the dimension of the image vector space is strictly smaller than the dimension of the original one). As for the third assertion, assume that there exists a regular sequence s of f such that  $s^{(d)}$  is a regular sequence of h, where h is a proper factor of  $f_{(d)}$ . From the definition of  $f_{(d)}$ , it then follows that the polynomial  $g(x) = g.c.d.(f(x), h(x^d))$  is a proper factor of f such that  $g_{(d)} = h$ . Then  $f_{(d)}(g) = f_{(d)}(g) = f_{$ 

## ACKNOWLEDGMENT

The author is grateful to an anonymous referee for useful comments.

### REFERENCES

- 1. M. Buck & N. Zierler. "Decimations of Linear Recurring Sequences." In *Proceedings of Golombfest*, Oxnard, California, May 1992.
- 2. P. F. Duvall & J. C. Mortick. "Decimation of Periodic Sequences." SIAM J. Appl. Math. 21 (1971):367-72.
- 3. S. W. Golomb. Shift Register Sequences. San Francisco: Holden-Day, 1967.
- 4. C. G. Günther. "Parallel Generation of Recurring Sequences." In Advances in Cryptology-EUROCRYPT '89. Lect. Notes in Comp. Sci. 434 (1990):503-22.
- 5. H. Niederreiter. "Some New Cryptosystems Based on Feedback Shift Register Sequences." *Math. J. Okayama Univ.* **30** (1988):121-49.

- 6. H. Niederreiter. "A Simple and General Approach to the Decimation of Feedback Shift-Register Sequences." *Probl. of Control and Inform. Theory* 17 (1988):327-31.
- 7. E. S. Selmer. *Linear Recurrence Relations Over Finite Fields*. Lecture Notes, University of Bergen, Norway, 1966.
- 8. B. Smeets. "Some Results on Linear Recurring Sequences." Ph.D. Dissertation, University of Lund. Sweden, 1987.
- 9. O. Zarriski & P. Samuel. Commutative Algebra. Vol. I. Princeton: D. Van Nostrand, 1958.
- 10. N. Zierler. "Linear Recurring Sequences." J. Soc. Indust. Appl. Math. 7 (1959):31-48.
- 11. N. Zierler & W. H. Mills. "Products of Linear Recurring Sequences." J. Algebra 27 (1973): 147-57.

AMS Classification Numbers: 11B37, 12E05, 94A60



## GENERALIZED PASCAL TRIANGLES AND PYRAMIDS: THEIR FRACTALS, GRAPHS, AND APPLICATIONS

by Dr. Boris A. Bondarenko

Associate member of the Academy of Sciences of the Republic of Uzbekistan, Tashkent

#### Translated by Professor Richard C. Bollinger

Penn State at Erie, The Behrend College

This monograph was Wrst published in Russia in 1990 and consists of seven chapters, a list of 406 references, an appendix with another 126 references, many illustrations and specific examples. Fundamental results in the book are formulated as theorems and algorithms or as equations and formulas. For more details on the contents of the book, see *The Fibonacci Quarterly* 31.1 (1993):52.

The translation of the book is being reproduced and sold with the permission of the author, the translator, and the "FAN" Edition of the Academy of Science of the Republic of Uzbekistan. The book, which contains approximately 250 pages, is a paperback with a plastic spiral binding. The price of the book is \$31.00 plus postage and handling where postage and handling will be \$6.00 if mailed anywhere in the United States or Canada, \$9.00 by surface mail or \$16,00 by airmail elsewhere. A copy of the book can be purchased by sending a check make out to THE FIBONACÇI ASSOCIATION for the appropriate amount along with a letter requesting a copy of the book to: MR. RICHARD S. VINE, SUBSCRIPTION MANAGER, THE FIBONACCI ASSOCIATION, SANTA CLARA UNIVERSITY, SANTA CLARA, CA 95053.

## ROOTS OF UNITY AND CIRCULAR SUBSETS WITHOUT CONSECUTIVE ELEMENTS

## John Konvalina

Department of Mathematics and Computer Science, University of Nebraska at Omaha, NE 68182 (Submitted March, 1994)

## 1. INTRODUCTION

Recall that the  $n^{th}$  roots of unity are the roots of the polynomial  $x^n-1$ . Also, they have a geometrical interpretation in terms of the vertices of a regular polygon with n sides inscribed in the unit circle. Now consider the polynomial of degree n with the property that each of its roots is the sum of an  $n^{th}$  root of unity and its square. That is, let  $U_n$  denote the set of  $n^{th}$  roots of unity and consider the polynomial

$$P_n(x) = \prod_{\zeta \in U_n} (x - (\zeta + \zeta^2)).$$

What are the coefficients of  $P_n(x)$ ? A priori the coefficients are complex numbers. However, we will show they are actually integers. In fact, we will prove the unexpected result that the absolute value of the coefficient of  $x^k$  has a combinatorial interpretation in terms of the number of k-subsets of n objects arranged in a circle with no two selected objects being consecutive. The sum of the coefficients is expressed in terms of Lucas numbers.

## 2. COMBINATORIAL IDENTITIES

Before proving the theorem, we will state some known combinatorial identities. We assume throughout the paper that n > 0. It is well known that the number of k-subsets without consecutive elements chosen from n objects arranged in a circle is (see Riordan [3], p. 198)

$$\frac{n}{n-k}\binom{n-k}{k}.$$

The generating function of this sequence has the following closed form:

$$\sum_{k=0}^{\left[\frac{n}{2}\right]} \frac{n}{n-k} \binom{n-k}{k} x^k = \left(\frac{1+\sqrt{1+4x}}{2}\right)^n + \left(\frac{1-\sqrt{1+4x}}{2}\right)^n. \tag{1}$$

When x = -1 we obtain the following identity [since  $\frac{1}{2}(1 \pm \sqrt{-3})$  are sixth roots of unity]:

$$\sum_{k=0}^{\left[\frac{n}{2}\right]} \frac{n}{n-k} \binom{n-k}{k} (-1)^k = \begin{cases} 2(-1)^n & \text{if } n \equiv 0 \pmod{3}, \\ (-1)^{n-1} & \text{if } n \not\equiv 0 \pmod{3}. \end{cases}$$
 (2)

The following identity will also be used:

$$\sum_{k=0}^{\left[\frac{n}{2}\right]} \binom{n-k}{k} (-1)^k = \frac{(-1)^{\left[\frac{n}{3}\right]} + (-1)^{\left[\frac{n+1}{3}\right]}}{2}.$$
 (3)

References for these combinatorial identities include Graham, Knuth, & Patashnik [2], pp. 178-79 and 204, or Riordan [4], pp. 75-77, or Gould [1], Identities 1.64, 1.68, and 1.75.

#### 3. THE THEOREM

**Theorem:** The roots of the polynomial

$$P_n(x) = x^n + (-1)^n - \sum_{k=0}^{\left[\frac{n}{2}\right]} \frac{n}{n-k} \binom{n-k}{k} x^k \tag{4}$$

are precisely the *n* complex numbers (not necessarily distinct) of the form  $\zeta + \zeta^2$ , where  $\zeta$  ranges over  $U_n$  the n<sup>th</sup> roots of unity. That is,

$$\prod_{\zeta \in U_n} (x - (\zeta + \zeta^2)) = x^n + (-1)^n - \sum_{k=0}^{\left[\frac{n}{2}\right]} \frac{n}{n-k} \binom{n-k}{k} x^k.$$

**Proof:** Let  $\zeta$  denote any  $n^{\text{th}}$  root of unity. Then  $x = \zeta + \zeta^2$  is a root of  $P_n(x)$  of and only if

$$\sum_{k=0}^{\left[\frac{n}{2}\right]} \frac{n}{n-k} \binom{n-k}{k} (\zeta + \zeta^2)^k = (\zeta + \zeta^2)^n + (-1)^n = (1+\zeta)^n + (-1)^n.$$
 (5)

But (5) follows immediately from (1) since  $1+4(\zeta+\zeta^2)=(2\zeta+1)^2$  and  $\zeta^n=1$ . Hence, if the *n* complex numbers,  $\zeta+\zeta^2$ , are distinct as  $\zeta$  ranges over  $U_n$ , then all roots of  $P_n(x)$  have been determined.

To complete the proof, we will show all the roots are distinct except when  $n \equiv 0 \pmod{3}$ . In that case, x = -1 will be a double root. To verify this, first observe that by (2) and (4) x = -1 is a root of  $P_n(x)$  if and only if  $n \equiv 0 \pmod{3}$ . Now the derivative of  $P_n(x)$  is

$$P_n'(x) = nx^{n-1} - n\sum_{k=0}^{\left[\frac{n-2}{2}\right]} \binom{n-2-k}{k} x^k.$$
 (6)

So x = -1 is a root of  $P'_n(x)$  if and only if

$$\sum_{k=0}^{\left[\frac{n-2}{2}\right]} \binom{n-2-k}{k} (-1)^k = (-1)^{n-1}.$$
 (7)

But, if  $n \equiv 0 \pmod{3}$ , then (7) follows immediately from (3) with n replaced by n-2 and noting that [since  $(-1)^{n/3} = (-1)^n$ ]

$$(-1)^{\left[\frac{n-2}{3}\right]} = (-1)^{\frac{n-3}{3}} = (-1)^{n-1}$$

Thus, x = -1 is at least a double root of  $P_n(x)$  when  $n \equiv 0 \pmod{3}$ . Finally, we will show x = -1 is in fact a double root. First, however, a lemma to determine when the sum of two  $n^{th}$  roots of unity is equal to -1.

**Lemma:** Let  $\zeta_n$  denote the primitive  $n^{\text{th}}$  root of unity  $\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ . Suppose  $0 \le j < k < n$ . Then, for some j and k,  $\zeta_n^j + \zeta_n^k = -1$  if and only if n = 3j and k = 2j.

**Proof:** If n=3j and k=2j, then  $\zeta_{3j}^j+\zeta_{3j}^{2j}$  is a sum of the primitive cube roots of unity and, hence, is equal to -1. Conversely, suppose the sum of the two  $n^{\text{th}}$  roots of unity is equal to -1. Equating real and imaginary parts, we obtain  $\cos\frac{2\pi}{n}j+\cos\frac{2\pi}{n}k=-1$  and  $\sin\frac{2\pi}{n}j+\sin\frac{2\pi}{n}k=0$ . Now solve for  $\cos\frac{2\pi}{n}k$  and  $\sin\frac{2\pi}{n}k$ :

$$\cos\frac{2\pi}{n}k = -1 - \cos\frac{2\pi}{n}j\tag{8}$$

and

$$\sin\frac{2\pi}{n}k = -\sin\frac{2\pi}{n}j. \tag{9}$$

Next, square both sides of (8) and (9), then add to obtain  $\cos\left(\frac{2\pi}{n}j\right) = -\frac{1}{2}$ . Similarly, solving the original equations for  $\cos\frac{2\pi}{n}j$  and  $\sin\frac{2\pi}{n}j$ , we obtain  $\cos\left(\frac{2\pi}{n}k\right) = -\frac{1}{2}$ . Since  $0 \le j < k < n$ , we must have  $\frac{2\pi}{n}j = \frac{2\pi}{3}$  and  $\frac{2\pi}{n}k = \frac{4\pi}{3}$ . Hence, n = 3j and 3k = 2n. Therefore, n = 3j and k = 2j, and the lemma is proved.

Now we return to the proof of the theorem to determine when the roots of  $P_n(x)$  will not be distinct. Suppose  $0 \le j < k < n$  and two roots are the same. Then

$$\zeta_n^j + \zeta_n^{2j} = \zeta_n^k + \zeta_n^{2k} \tag{10}$$

Hence,  $\zeta_n^j - \zeta_n^k = \zeta_n^{2k} - \zeta_n^{2j} = (\zeta_n^k - \zeta_n^j)(\zeta_n^k + \zeta_n^j)$ . So we must have

$$\zeta_n^j + \zeta_n^k = -1. \tag{11}$$

Therefore, by the lemma,  $\zeta_n^j$  and  $\zeta_n^k$  are the primitive cube roots of unity. Since the square of one primitive cube root of unity is the other primitive cube root, the root x = -1 will occur exactly twice in  $\zeta + \zeta^2$  as  $\zeta$  ranges over the  $n^{\text{th}}$  roots of unity for  $n \equiv 0 \pmod{3}$ .

Corollary:  $P_n(1) = \begin{cases} -L_n & \text{if } n \text{ is odd,} \\ -L_n + 2 & \text{if } n \text{ is even,} \end{cases}$  where  $L_n$  is the  $n^{\text{th}}$  Lucas number.

**Proof:** It is well known that  $\sum_{k\geq 0} \frac{n}{n-k} \binom{n-k}{k} = L_n$ , where  $L_n$  is the  $n^{\text{th}}$  Lucas number.

## REFERENCES

- 1. H. W. Gould. Combinatorial Identities. Morgantown, WV, 1972.
- 2. R. L. Graham, D. E. Knuth, & O. Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. Reading, MA: Addison-Wesley, 1989.
- 3. J. Riordan. An Introduction to Combinatorial Analysis. New York: Wiley, 1958.
- 4. J. Riordan. Combinatorial Identities. New York: Wiley, 1968.

AMS Classification Number: 05A15

## SOME DISCRETE DISTRIBUTIONS RELATED TO EXTENDED PASCAL TRIANGLES

## K. Balasubramanian

Indian Statistical Institute, New Delhi, India 110 016

## Román Viveros

Department of Mathematics & Statistics, McMaster University Hamilton, Ontario, Canada L8S 4K1

## N. Balakrishnan

Department of Mathematics & Statistics, McMaster University Hamilton, Ontario, Canada L8S 4K1 (Submitted March 1994)

#### 1. EXPERIMENTAL SETTING

Consider a die with m faces marked  $\{0, 1, 2, ..., m-1\}$ . Assume that the turn-up side probabilities are in geometric progression as follows:

Face (i) 0 1 2 ... 
$$m-1$$
Probability  $(p_i)$   $q^{m-1}$   $pq^{m-2}$   $p^2q^{m-3}$  ...  $p^{m-1}$  (1)

The necessary and sufficient restrictions on p and q are

$$q^{m-1} + pq^{m-2} + p^2q^{m-3} + \dots + p^{m-1} = 1, \quad 0 \le p \le 1, \quad 0 \le q \le 1.$$
 (2)

Note that the first restriction is equivalent to  $q^m - p^m = q - p$ .

The die just described becomes an ordinary coin when m=2. In this case p+q=1. Selecting  $p=q=m^{-1/(m-1)}$  will result in a fair die, i.e., each face will have probability  $m^{-1}$  of turning-up when the die is rolled. Also, from (2), when  $0 \le p < m^{-1/(m-1)}$  one must have  $m^{-1/(m-1)} < q \le 1$ , and vice versa.

For a given p, the function  $f(q) = q^m - q - p^m + p$  has derivative  $f'(q) = mq^{m-1} - 1$ . Thus, f(q) is strictly decreasing for  $0 \le q \le m^{-1/(m-1)}$  and strictly increasing for  $m^{-1/(m-1)} \le q \le 1$ . This fact in conjunction with the remarks in the previous paragraph assure that, for a given  $p = (0 \le p \le 1)$ , there is a unique q satisfying (2). The value of q, which is the root of a polynomial of degree m-1, cannot be given explicitly in general. However, q=1-p for m=2, and  $q=(-p+\sqrt{4-3p^2})/2$  for m=3.

Alternative parametrizations to (1) that may yield other useful interpretations are also possible. For instance, if  $p \le q$ , then defining  $\theta = p/q$  one can easily see that (1) is equivalent to  $p_i = (1-\theta)\theta^i/(1-\theta^m)$ ,  $0 \le i \le m-1$ . In this case, rolling the die is equivalent to generating a value of a geometric random variable constrained to the range  $\{0, 1, 2, ..., m-1\}$  with  $1-\theta$  and  $\theta$  being the success and failure probabilities, respectively.

## 2. THE EXTENDED BINOMIAL DISTRIBUTION AND PROPERTIES

The focus of this article is the random variable

$$X_n^{(m)}$$
 = total score in *n* rolls of the *m*-sided die with face probabilities as described in (1)-(2). (3)

It is clear that  $X_n^{(m)}$  has the familiar binomial distribution with index n and success probability p when m=2. For this reason, the distribution of  $X_n^{(m)}$  will be called the *extended binomial distribution of order m*, index n and parameter p, and will be denoted by EB(m, n, p).

Note that  $X_n^{(m)}$  is simply the convolution of n i.i.d. random variables corresponding to the scores of n rolls of the die. Therefore, the probability generating function (PGF) of  $X_n^{(m)}$  can be written as

$$G(t) = E(t^{X_n^{(m)}}) = \left\lceil \frac{q^m - p^m t^m}{q - pt} \right\rceil^n. \tag{4}$$

Expanding G(t) in powers of t yields an expression for the probability mass function (PMF) of  $X_n^{(m)}$  as

$$\Pr(X_n^{(m)} = r; p) = C_m(n, r) p^r q^{(m-1)n-r}, \quad 0 \le r \le (m-1)n,$$
(5)

where  $C_m(n,r)$  is the coefficient of  $t^r$  in  $[(1-t^m)/(1-t)]^n$ . Note the similarity between (5) and the ordinary binomial distribution.

The coefficients  $C_m(n,r)$ , which can be traced back to the classic work of Abraham De Moivre [6], were studied in detail by Freund [10], who discussed their role in occupancy theory. In particular,  $C_m(n,r)$  can be interpreted as "the number of ways of putting n indistinguishable objects into r numbered boxes with each box containing at most m-1 objects." Thus,

$$C_2(n,r) = \binom{n}{r}, \ 0 \le r \le n.$$

In the spirit of Bollinger [3] and [4], we will refer to the numbers  $C_m(n,r)$ ,  $0 \le r \le (m-1)n$ , as the extended binomial coefficients of order m.

From a mathematical point of view, many theoretical properties of  $C_m(n,r)$  have been established. For details, see [4] and [5] and the references therein. From a probabilistic point of view, in addition to the applications to occupancy problems discussed in [10] and those presented in this article,  $C_m(n,r)$  plays an important role in describing the distribution of discrete waiting time random variables based on run criteria. For instance, see [3] and [2].

A convenient way of computing  $C_m(n,r)$  is by means of the recursion

$$C_m(n,r) = \sum_{\ell=0}^{m-1} C_m(n-1,r-\ell).$$
 (6)

For the case m = 2, this recursion reduces to the well-known identity

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}.$$

In a manner similar to the calculation of the familiar Pascal triangle, (6) can be used to compute a table the  $n^{th}$  row of which will contain all the extended binomial coefficients of order m. These arrangements have been called *extended Pascal triangles*, see [4].

Alternatively,  $C_m(n, r)$  can be calculated by means of the explicit formula

$$C_m(n,r) = \sum_{\alpha=0}^{\alpha_1} (-1)^{\alpha} \binom{n}{\alpha} \binom{r+n-\alpha m-1}{n-1},\tag{7}$$

where  $\alpha_1 = \min\{n, \text{ integer part in } r/m\}$ . For a proof of (6)-(7), see [5] and [2].

The classical hypergeometric identity also extends to arbitrary m. Namely,

$$C_m(n_1 + n_2, r) = \sum_{a} C_m(n_1, a) C_m(n_2, r - a).$$
 (8)

Relationship (8) will be called the extended hypergeometric identity of order m in this article.

It is a minor exercise to show that the property of symmetry for ordinary binomial coefficients also holds for *m*-binomial coefficients. That is,

$$C_m(n,r) = C_m(n,(m-1)n-r), \quad 0 \le r \le (m-1)n. \tag{9}$$

As a result,

$$\Pr(X_n^{(m)} = r; p) = \Pr(X_n^{(m)} = (m-1)n - r; q), \quad 0 \le r \le (m-1)n, \tag{10}$$

where p and q satisfy (2). Note that the distribution of  $X_n^{(m)}$  is symmetric when  $p = m^{-1/(m-1)}$  since q = p in this case.

The PMF of  $X_n^{(m)}$  given in (5) can also be computed recursively as follows. Write the PGF (4) as

$$(q - pt)^n G(t) = (q^m - p^m t^m)^n. (11)$$

Then expand each factor in (11) using the binomial theorem and (5), and equate the coefficients of  $t^r$  from both sides to get

$$\sum_{i=0}^{\min\{n,r\}} (-1)^{j} \binom{n}{j} p^{j} q^{n-j} \Pr\left(X_{n}^{(m)} = r - j; p\right) = q^{n} \alpha_{r}, \tag{12}$$

for r = 0, 1, 2, ..., where

$$\alpha_r = \begin{cases} 0 & \text{if } b_r \neq 0, \\ (-1)^{a_r} \binom{n}{a_r} p^r q^{(m-1)n-r} & \text{if } b_r = 0, \end{cases}$$

and  $r = a_r m + b_r$  with  $0 \le b_r \le m - 1$ . From (12), one immediately obtains the recursion

$$\Pr(X_n^{(m)} = r; p) = \alpha_r - \sum_{j=1}^{\min\{r, n\}} (-1)^j \binom{n}{j} \left(\frac{p}{q}\right)^j \Pr(X_n^{(m)} = r - j; p), \quad 1 \le r \le (m - 1)n.$$
 (13)

As an illustration of the variety of shapes exhibited by the distribution of  $X_n^{(m)}$ , (5) was calculated numerically for m=4, n=10, and several values of (p,q) using the foregoing methods. The corresponding bar plots are depicted in Figure 1. Note that the distribution of  $X_n^{(m)}$  is positively skewed for  $p < m^{-1/(m-1)} = 0.63$  and negatively skewed for  $p > m^{-1/(m-1)}$ . This result holds generally for arbitrary m.

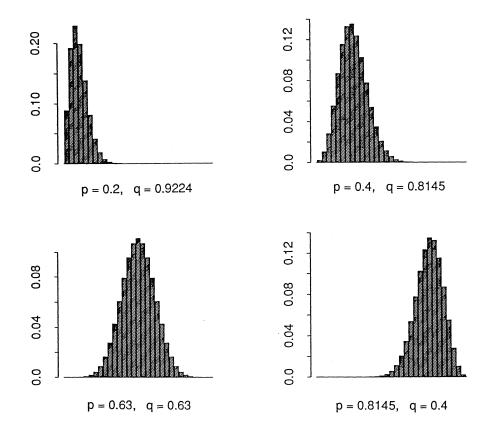


FIGURE 1. Shapes of the 4-Binomial Distribution with Index n = 10and Several Values of (p, q)

Because  $X_n^{(m)}$  arises as a convolution, it must have the reproductive property. Specifically, if  $Y_1, Y_2, ..., Y_k$  are independent with  $Y_i \sim EB(m, n_i, p)$ , then  $\sum_{i=1}^k Y_i \sim EB(m, \sum_{i=1}^k n_i, p)$ . Defining  $\theta = p/q$ , one can write the PMF of  $X_n^{(m)}$  given in (5) as

$$\Pr(X_n^{(m)} = r; p) = \frac{C_m(n, r)\theta^r}{g(\theta)}, \quad 0 \le r \le (m-1)n, \tag{14}$$

where  $0 \le \theta < \infty$  and

$$g(\theta) = \left(\frac{1 - \theta^m}{1 - \theta}\right)^n. \tag{15}$$

In the form (14)-(15), one can readily see that  $X_n^{(m)}$  has a power series distribution. Thus, any results on this general family of distributions will apply to the distribution of  $X_n^{(m)}$  as well. Note from (15) that  $g(\theta) = (1+\theta)^n$  for m=2 and  $g(\theta) = (1-\theta)^{-n}$  for  $m=\infty$  when  $0 \le \theta < 1$ , characterizing the binomial and negative binomial distributions, respectively. Using a standard argument, one can get the Poisson distribution by keeping m fixed, and letting  $n \to \infty$  and  $\theta \to 0$  in such a way that  $n\theta/(1+\theta) \to \lambda$ . By means of the central limit theorem, a normal approximation is also

guaranteed. Specifically,  $(X_n^{(m)} - \mu)/\sigma \approx N(0, 1)$  for *n* large, where  $\mu$  and  $\sigma^2$  are as given in (16) below.

From (4) or otherwise, the mean and variance of  $X_n^{(m)}$  are readily shown to be

$$\mu = E(X_n^{(m)}) = np \frac{1 - mp^{m-1}}{q - p}, \quad \sigma^2 = Var(X_n^{(m)}) = npq \frac{1 - m^2(pq)^{m-1}}{(q - p)^2}.$$
 (16)

In comparing  $\mu$  and  $\sigma^2$ , one can readily see that  $\mu < \sigma^2$  when and only when

$$mp^{m-2}(mq^m - q + 1) < 1.$$
 (17)

For any  $3 \le m < \infty$ , the left-hand side of (17) approaches 0 as  $p \to 0$  and m as  $p \to 1$ . Hence, both  $\mu < \sigma^2$  and  $\mu \ge \sigma^2$  are always possible. When m = 2, (16) gives  $\mu = np$  and  $\sigma^2 = npq$  with p + q = 1. This case corresponds to the binomial model for which  $\mu \ge \sigma^2$  for all  $0 \le p \le 1$ . When  $p \le q$  one can easily show that  $\mu = n\theta/(1-\theta)$ ,  $\sigma^2 = n\theta^3/(1-\theta)^2$  when  $m = \infty$  where  $\theta = p/q$ . Therefore,  $\mu \le \sigma^2$  for all  $0 \le \theta \le 1$  in this case, a well-known property for the negative binomial distribution.

Applying the results in [7, pp. 109-11, Th. 4.2], one can readily show that the turn-up face probability distribution (1) is strongly unimodal. Because the family of discrete strongly unimodal distributions is closed under convolution, it follows that the distribution of  $X_n^{(m)}$  is strongly unimodal (i.e., log-concave). In particular, the distribution of  $X_n^{(m)}$  is unimodal in the usual sense, i.e., there exists a point M such that

$$\Pr(X_n^{(m)} = r; p) \ge \Pr(X_n^{(m)} = r - 1; p)$$
 according as  $r \le M$ .

A consequence of the log-concavity of the distribution of  $X_n^{(m)}$  is the inequality

$$[C_m(n,r)]^2 \ge C_m(n,r-1)C_m(n,r+1), 1 \le r \le (m-1)n-1,$$

which simply shows the log-concavity of the extended binomial coefficients  $C_m(n,r)$ ,  $0 \le r \le (m-1)n$ . This shows, in particular, that the distribution of  $X_n^{(m)}$  is log-concave.

## 3. HISTORY AND PREVIOUS APPLICATIONS

The earliest reference to the extended binomial coefficients can be found in the work of Abraham De Moivre [6]. A detailed "theoretical" discussion appeared in the third edition of [6], pp. 39-43, with many illustrative examples throughout the book. His main result appeared in the form of a lemma which stated: "To find how many chances there are upon any number of dice, each of them of the same number of faces, to throw any given number of points" [6, p. 39]. Without giving the reference, De Moivre stated in [6] that the lemma was published by him for the first time in 1711.

A look at [6] indicates that: (a) De Moivre dealt with a fair die with an arbitrary number of faces; (b) he calculated  $C_m(n,r)$  numerically by explicit expansion of (7); (c) he was aware of the generating function for  $C_m(n,r)$ ,

$$\left(\frac{1-t^m}{1-t}\right)^n = \sum_{r=0}^{(m-1)n} C_m(n,r)t^{r},$$

which is given immediately after (5); (d) he was aware of the property of symmetry (9).

The distribution of  $X_n^{(m)} + n$  for the case of a fair die appears as an exercise in [8, pp. 284-85]. Generating functions and limits for the cumulative probabilities of  $X_n^{(m)} + n$  under this case are also presented as exercises by Feller [8, p. 285] who relates them to the work of Lagrange.

An important practical application of the extended binomial distribution was presented by Kalbfleisch and Sprott [14] in relation to the estimation of the "hit number," a parameter associated with an interesting dilution series model arising in virology. This model was originally proposed by Alling in [1]. The basics of the experiment, data, and assumptions are as follows: (a) a liquid medium containing a suspension of virus particles is successively diluted to form a geometric series of k+1 dilutions  $a^0$ , a,  $a^2$ , ...,  $a^k$ ; (b) these dilutions are poured over replicate cell sheets; (c) after a period of growth, the number  $N_i$  of plaques occurring at dilution level  $a^i$  is observed  $(0 \le i \le k)$ ; (d) the  $N_i$ 's are independent with  $N_i$  having a Poisson distribution with mean  $\eta \gamma^i$  ( $0 \le i \le k$ ). Here  $\eta$  is the expected number of plaques in the undiluted suspension (i = 0), and  $\gamma = a^{-h}$ , where  $\alpha$  is the known dilution factor and  $\alpha$  the "hit number," is the minimum number of virus particles that must attach themselves to a cell in order to form a plaque. The primary objective of the experiment was to estimate  $\alpha$ .

In their statistical analysis, Kalbfleisch and Sprott [14] first show that the statistics  $(S, T) = (\sum_{i=0}^k N_i, \sum_{i=0}^k i N_i)$  are jointly sufficient for  $(\eta, h)$ . Then they derive the conditional distribution of T given S = s, which turns out to be the extended binomial distribution in the form (14) with m = k + 1, n = s, and  $\theta = \gamma$ . They use this distribution to make inferences about  $h = -\ln \gamma / \ln \alpha$  that are unaffected by lack of knowledge on the remaining parameter  $\eta$ .

#### 4. INFERENTIAL ISSUES

# 4.1 Sufficiency, Completeness, and Consequences

Since for given m and n the distribution of  $X_n^{(m)}$  is a member of the family of power-series distributions, then  $\{\Pr(X_n^{(m)}=\cdot;p)\colon 0\leq p\leq 1\}$  is complete. Further, if  $Y_1,Y_2,...,Y_k$  are independent and identically distributed as  $X_n^{(m)}$ , then  $S=\sum_{i=1}^k Y_i$  is sufficient for p or any one-to-one parametric function such as  $\theta=p/q$ . Due to the already noted reproductive property, it follows that  $\{\Pr(S=\cdot;p)\colon 0\leq p\leq 1\}$  is also complete.

These facts, in conjunction with the Rao-Blackwell theorem (e.g., see [12, pp. 349-52]), imply that the only parametric functions for which minimum variance unbiased estimators exist are the linear combinations of  $\{p^rq^{(m-1)n-r}, 0 \le r \le (m-1)n\}$ . In particular, the sample mean  $\overline{Y} = \sum_{i=1}^k Y_i/k$  is the unique minimum variance unbiased estimator of the average value  $\mu$  of  $X_n^{(m)}$  given in (16).

# 4.2 Extended Fisher's Conditional Test and the Extended Hypergeometric Distribution

Consider two *m*-faced dice, labeled Die 1 and Die 2, with respective unknown parameter values  $p_1$  and  $p_2$ . On the basis of the scores  $Y_{11}, Y_{12}, ..., Y_{1n_1}$  in  $n_1$  rolls of Die 1 and  $Y_{21}, Y_{22}, ..., Y_{2n_2}$  in  $n_2$  rolls of Die 2, we would like to test

$$H_0$$
:  $p_1 = p_2$  vs  $H_1$ :  $p_1 \neq p_2$ .

420

In view of the sufficiency results of section 4.1, in developing a sensible test for  $H_0$  vs  $H_1$ , one should focus on the total scores  $Y_1 = \sum_{i=1}^{n_1} Y_{1i}$  and  $Y_2 = \sum_{i=1}^{n_2} Y_{2i}$ . Note that  $Y_1$  and  $Y_2$  are independent and have extended binomial distributions with parameters  $(m, n_1, p_1)$  and  $(m, n_2, p_2)$ , respectively. Letting  $\rho = p_1 q_2 / (q_1 p_2)$ , one can show that

$$\Pr(Y_1 = a, Y_2 = b; p_1, p_2) = C_m(n_1, a)C_m(n_2, b)\rho^a \left(\frac{p_2}{q_2}\right)^{a+b} q_1^{(m-1)n_1} q_2^{(m-1)n_2},$$

from which it is readily seen that  $T = Y_1 + Y_2$  is sufficient for  $p_2$  when  $\rho$  is specified. Therefore, the conditional distribution of  $Y_1$ , given the observed value of T, depends on the parameters only through  $\rho$ . In fact,

$$\Pr(Y_1 = a; \rho \mid T = t) = \frac{C_m(n_1, a)C_m(n_2, t - a)\rho^a}{\sum_{\nu} C_m(n_1, \nu)C_m(n_2, t - \nu)\rho^{\nu}}, \ 0 \le a \le t.$$

Since  $H_0$  and  $H_1$  are equivalent to  $H_0$ :  $\rho = 1$  and  $H_1$ :  $\rho \neq 1$ , respectively, then a test for  $H_0$  vs  $H_1$  can be developed using  $Y_1$  as a test statistic and its conditional null distribution

$$\Pr(Y_1 = a \mid T = t) = \frac{C_m(n_1, a)C_m(n_2, t - a)}{C_m(n_1 + n_2, t)}, \ 0 \le a \le t.$$
 (18)

P-values for testing  $H_0$  vs  $H_1$  can be calculated as tail probabilities from (18).

Note that the extended hypergeometric identity (8) has been used in deriving (18). Naturally, the test statistic reduces to Fisher's exact conditional test for homogeneity in  $2 \times 2$  tables (see [9, pp. 89-92]) when m = 2 and (18) becomes the classical hypergeometric distribution. For these reasons, (18) will be called the *extended hypergeometric distribution of order m*.

Analogous to the well-known asymptotic relation between the classical hypergeometric and binomial distributions, it can be shown here that, for every m, (18) converges to  $\binom{t}{a}\pi^a(1-\pi)^{t-a}$  as  $n_1 \to \infty$ ,  $n_2 \to \infty$  in such a way that  $n_1/(n_1+n_2) \to \pi$ .

## 5. NEGATIVE BINOMIAL EXTENSIONS

## 5.1 Total Score up to a Negative-Binomially-Stopped Roll

Consider consecutive rolls of the *m*-faced die with side probabilities (1)-(2). For a given positive integer k, define the random variable  $Z_k^{(m)}$  as

$$Z_k^{(m)}$$
 = total score until face marked 0 appears  $k$  times. (19)

Clearly,  $Z_k^{(m)}$  has the standard negative binomial distribution when m = 2.

In order to derive the PGF of  $Z_k^{(m)}$ , one can view the above experiment as a two-stage process as follows. First, generate a value n of  $T_k$  = (number of rolls until face marked 0 appears k times) – k. Then roll n times a "reduced" die with faces marked  $\{1, 2, ..., m-1\}$  and corresponding side probabilities  $pq^{m-2}/(1-q^{m-1})$ ,  $p^2q^{m-3}/(1-q^{m-1})$ , ...,  $p^{m-1}/(1-q^{m-1})$ . Then compute the total score among the n rolls to obtain  $Z_k^{(m)}$  with the convention that  $Z_k^{(m)} = 0$  whenever n = 0.

Note that  $T_k$  has the standard negative binomial distribution

$$\Pr(T_k = n; p) = \binom{n+k-1}{k-1} q^{(m-1)k} (1-q^{m-1})^n, \quad 0 \le n < \infty.$$

Thus,  $Z_k^{(m)}$  can be seen as the total score from a negative binomial random number of rolls of the reduced die. From the basic theory on compounding of distributions, see [13, pp. 344-45], the PGF of  $Z_k^{(m)}$  can be written

$$H(t) = E(t^{Z_k^{(m)}}) = G_{T_k}(G_R(t)),$$

where  $G_{T_k}(t)$  is the PGF of  $T_k$  and  $G_R(t)$  is the PGF of the score in one roll of the "reduced" die. Since

$$G_{T_k}(t) = \left(\frac{q^{m-1}}{1 - (1 - q^{m-1})t}\right)^k, \quad G_R(t) = \frac{pt}{1 - q^{m-1}} \frac{q^{m-1} - p^{m-1}t^{m-1}}{q - pt},$$

then

$$H(t) = q^{(m-1)k} \left[ 1 - pt \frac{q^{m-1} - p^{m-1}t^{m-1}}{q - pt} \right]^{-k}.$$
 (20)

Using the familiar negative binomial expansion in conjunction with the methods used to derive (4)-(5) yield

$$\Pr(Z_k^{(m)} = r; p) = q^{(m-1)k} \left(\frac{p}{q}\right)^r \sum_{i=0}^r {k+i-1 \choose i} C_{m-1}(i, r-i) q^{(m-1)i}, \quad 0 \le r < \infty.$$
 (21)

An alternative use of (20) is for moment calculations about  $Z_k^{(m)}$ . For instance, the average value of  $Z_k^{(m)}$  is

$$E(Z_k^{(m)}) = H'(1) = \frac{kp}{q^{m-1}} \frac{1 - mp^{m-1}}{q - p}.$$
 (22)

When m = 2, (22) gives  $E(Z_k^{(2)}) = kp/q$ , which is the expected value of a standard negative binomial random variate.

#### 5.2 An Extended Negative Binomial Distribution

Consider again the die with m faces and turn-up side probabilities given by (1)-(2). Perhaps a more natural negative binomial counterpart is the waiting time random variable

$$Y_N^{(m)}$$
 = number of rolls until a total score of  $N$  or more is observed for the first time. (23)

Clearly  $Y_N^{(m)}$  is a standard negative binomial variate when m = 2. For this reason the distribution of  $Y_N^{(m)}$  will be called the *extended negative binomial distribution of order m* and will be denoted as ENB(m, N, p).

It is readily seen that the fundamental identity

$$Pr(Y_N^{(m)} \le n; p) = Pr(X_n^{(m)} \ge N; p)$$
(24)

holds for every n. For the particular case m = 2, relationship (24) is well known from elementary probability courses. Using (24) in conjunction with (5) one can show that

$$\Pr(Y_N^{(m)} = n; p) = \sum_{r=0}^{N-1} C_m(n-1, r) p^r q^{(m-1)(n-1)-r} - \sum_{r=0}^{N-1} C_m(n, r) p^r q^{(m-1)n-r},$$
 (25)

for  $n \ge$  the smallest integer not less than N/(m-1).

Although (25) is adequate for numerical evaluations, further simplifications are possible in particular cases. For instance, when  $1 \le N \le m$ , with the help of (7) one can show that

$$\Pr(Y_N^{(m)} = n; p) = q^{(m-1)(n-1)} \sum_{r=0}^{N-1} \left(\frac{p}{q}\right)^r \left\{ \binom{n+r-2}{r} - q^{m-1} \binom{n+r-1}{r} \right\}, \tag{26}$$

for  $1 \le n < \infty$ . Note that  $Y_1^{(m)}$  is a geometric random variable equivalent to the number of coin tosses until "heads" appears for the first time where the probability of "heads" is  $1 - q^{m-1}$ .

#### 6. DISCUSSION

Richard C. Bollinger [4] concludes his article with the comment:

In conclusion, we hope that the discussion has shown that the  $T_m$  arrays really are "extensions" of the Pascal triangle, with many similar properties that seem to be the natural generalizations of those of  $T_2$ , but perhaps with a few surprises also.  $T_2$  has certainly been a rich source of interesting and useful mathematics. We suggest that its extended relatives potentially may serve as equally fruitful objects of study.

Here,  $T_m$  denotes the extended Pascal triangle formed by the extended binomial coefficients of order m, while  $T_2$  is the familiar Pascal triangle of the classical binomial coefficients. Our article justifies to some extent the hopes of Bollinger; we too share his suggestions that these objects may serve as a source of many more discrete distributions.

A referee has pointed out the possibility of relating the extended binomial coefficients to the Fibonacci sequence of order m,  $\{f_n^{(m)}\}_{n=0}^{\infty}$ , for which an extensive literature is available. See, for example, the work of Philippou [15] and [16], Philippou and Muwafi [18], and Gabai [11]. Indeed, such a connection exists. Perhaps the simplest relationship is

$$f_{n+1}^{(m)} = \sum_{\ell=S/GE(n)}^{n} C_m(\ell, n-\ell),$$
 (27)

where SIGE(x) denotes the smallest integer that is greater than or equal to x, also called the "ceiling" of x. The validity of (27) can be established by expanding the generating function of  $\{f_n^{(m)}\}_{n=0}^{\infty}$ , given, e.g., in [15], in conjunction with the generating function for  $\{C_m(n,r)\}_{r=0}^{(m-1)n}$  given in section 2, and then matching coefficients of identical powers in the generating variable. One immediate application of (27) is for numerical computation of  $f_{n+1}^{(m)}$  by means of any of the methods for calculating  $C_m(n,r)$  discussed in section 2. This approach is likely to be simpler than the formula for  $f_{n+1}^{(m)}$  in terms of multinomial coefficients given by Theorem 1 in [15]. On the other hand, the interesting work on the Fibonacci sequence of order m done by Philippou and others has some bearing on the extended binomial coefficients in view of relationship (27). This avenue has not been explored in this article and merits further consideration.

An important application of the Fibonacci sequence of order *m* discussed by Philippou [16], Philippou, Georghiou, and Philippou [17], Philippou and Muwafi [18], and others, is in the calculation of the discrete waiting time random variable

 $N_m$  = number of independent Bernoulli trials performed until m consecutive successes are observed,

where each trial can result in "success" or "failure" with probabilities p and q = 1 - p, respectively. Working with the probability generating function of  $N_m$ , which was derived by Feller [8, p. 323], in a manner similar to the derivation of (27) one can show that

$$\Pr(N_m = m + j) = \sum_{\ell = SIGE\left(\frac{j}{m}\right)}^{j} C_m(\ell, j - \ell) p^{m+j-\ell} q^{\ell}, \qquad (28)$$

for  $j \ge 0$ . Thus, (28) is an alternative to the formula for  $Pr(N_m = m + j)$  given by Theorem 3.1 in [18] in terms of multinomial coefficients.

It may also be of interest to look into possible continuous counterparts for the general discrete distributions presented in this article, just as beta and binomial, and exponential and geometric are naturally related. One interesting aspect is the study of the appropriate family of conjugate priors for the extended binomial distribution of order m. Work is currently being done in this direction.

## ACKNOWLEDGMENTS

The authors gratefully acknowledge the helpful comments of D. A. Sprott and the referee who brought to our attention some relevant references. This research was supported by grants from the Natural Sciences and Engineering Research Council (NSERC) of Canada.

#### REFERENCES

- 1. D.W. Alling. "Estimation of Hit Number." Biometrics 27 (1971):605-13.
- 2. N. Balakrishnan, K. Balasubramanian, & R. Viveros. "On Sampling Inspection Plans Based on the Theory of Runs." *The Math. Scientist* **18** (1993):113-26.
- 3. R. C. Bollinger. "Fibonacci k-Sequences, Pascal-T Triangles, and k-in-a Row Problems." *The Fibonacci Quarterly* **17.1** (1984):23-28.
- 4. R. C. Bollinger. "Extended Pascal Triangles." Math. Magazine 66 (1993):87-94.
- 5. R. C. Bollinger & Ch. L. Burchard. "Lucas's Theorem and Some Related Results for Extended Pascal Triangles." *Amer. Math. Monthly* 97 (1990):198-204.
- 6. A. De Moivre. The Doctrine of Chances: or, A Method of Calculating the Probabilities of Events in Play. 3rd ed. London: Millar, 1756; rpt. New York: Chelsea, 1967.
- 7. S. Dharmadhikari & K. Joag-dev. *Unimodality, Convexity, and Applications*. San Diego: Academic Press, 1988.
- 8. W. Feller. *An Introduction to Probability Theory and Its Applications*. Vol. I. 3rd ed. New York: Wiley, 1968.
- 9. R. A. Fisher. Statistical Methods and Scientific Inference. New York: Hafner Press, 1973.
- 10. J. E. Freund. "Restricted Occupancy Theory—A Generalization of Pascal's Triangles." *Amer. Math. Monthly* **63** (1956):20-27.
- 11. H. Gabai. "Generalized Fibonacci K-Sequences." The Fibonacci Quarterly 8.1 (1970):31-38.
- 12. R. V. Hogg & A. T. Craig. *Introduction to Mathematical Statistics*. 4th ed. New York: Macmillan, 1978.
- 13. N. L. Johnson, S. Kotz, & A. W. Kemp. *Univariate Discrete Distributions*. 2nd ed. New York: Wiley, 1992.
- 14. J. G. Kalbfleisch & D. A. Sprott. "Inference about Hit Number in a Virological Model." *Biometrics* **30** (1974):199-208.
- 15. A. N. Philippou. "A Note on the Fibonacci Sequence of Order K and the Multinomial Coefficients." *The Fibonacci Quarterly* **21** (1983):82-86.

424 [NOV.

- 16. A. N. Philippou. "Recursive Theorems for Success Runs and Reliability of Consecutive-Kout of N: F Systems." In Applications of Fibonacci Numbers 1:149-61. Ed. A. N. Philippou et al. Dordrecht: Kluwer, 1988.
- 17. A. N. Philippou, C. Georghiou, & G. N. Philippou. "A Generalized Geometric Distribution and Some of Its Properties." *Statistics & Probability Letters* 1 (1983):171-75.
- 18. A. N. Philippou & A. A. Muwafi. "Waiting for the Kth Consecutive Success and the Fibonacci Sequence of Order K." *The Fibonacci Quarterly* **20.1** (1982):28-32.

AMS Classification Numbers: 60C05, 62E15

\*\*\*

# APPLICATIONS OF FIBONACCI NUMBERS

#### VOLUME 5

New Publication

Proceedings of The Fifth International Conference on Fibonacci Numbers and Their Applications, University of St. Andrews, Scotland, July 20-24, 1992

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

This volume contains a selection of papers presented at the Fifth 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:

1993, 625 pp. ISBN 0-7923-2491-9 Hardbound Dfl. 320.00 / £123.00 / US\$180.00

AMS 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.

Volumes 1-4 can also be purchased by writing to the same addresses.

## THE DISTRIBUTION OF SPACES ON LOTTERY TICKETS

#### Norbert Henze

Institut für Mathematische Stochastik, Universität Karlsruhe, Englerstr. 2, 76128 Karlsruhe, Germany (Submitted March 1994)

## 1. INTRODUCTION

In many lotteries (e.g., Florida State, Canadian, German) people choose six distinct integers from 1 to 49 so that the set of all lottery tickets is given by

$$T = \{t = (t_1, t_2, \dots, t_6) : 1 \le t_1 < t_2 < \dots < t_6 \le 49\}.$$

Assuming a uniform distribution over all  $\binom{49}{6}$  tickets, Kennedy and Cooper [1] obtained the expectation and the distribution of the "smallest space" random variable

$$S(t) = \min\{t_{j+1} - t_j : j = 1, 2, 3, 4, 5\}$$

and asked for the distribution of the "largest spacing"

$$L(t) = \max\{t_{j+1} - t_j : j = 1, 2, 3, 4, 5\}.$$

By means of a certain "shrinking procedure," we provide a simple derivation of the results of Kennedy and Cooper. Moreover, we use this idea to obtain the distribution (and expectation) of L as well as the (joint) distribution of the individual "spacing" random variables given by

$$X_i(t) = t_{i+1} - t_i, \quad j = 1, ..., 5.$$
 (1.1)

A generalized lottery will be treated in the final section. As a bit of convenient but nonstandard notation, let

$$\binom{m}{n}^{+} = \begin{cases} 0, & \text{if } m < 0, \\ \binom{m}{n}, & \text{otherwise,} \end{cases}$$

denote a slight modification of the binomial coefficient  $\binom{m}{n}$ .

## 2. DISTRIBUTION OF A SINGLE SPACING

We first consider the distribution of the  $j^{\text{th}}$  spacing random variable  $X_j$  defined in (1.1). The crucial observation is that a 6-tuple  $t=(t_1,\ldots,t_6)$  from T satisfying  $t_{j+1}-t_j\geq k$ , where  $k\in\{1,2,\ldots,44\}$  may be "shrunk" into a 6-tuple  $u=(u_1,\ldots,u_6)$ , where

$$u_{v} = t_{v},$$
  $v = 1, 2, ..., j,$   
 $u_{v} = t_{v} - (k-1),$   $v = j+1, ..., 6.$ 

Obviously, this "shrinking procedure" is a one-to-one mapping from  $\{t \in T: t_{j+1} - t_j \ge k\}$  onto the set  $M = \{(u_1, ..., u_6): 1 \le u_1 < u_2 < \cdots < u_6 \le 49 - (k-1)\}$  which has cardinality  $\binom{50-k}{6}$ . We therefore obtain

$$P(X_j \ge k) = {50 - k \choose 6}^+ / {49 \choose 6}, k \ge 1,$$

and thus

$$P(X_{j} = k) = P(X_{j} \ge k) - P(X_{j} \ge k + 1)$$

$$= \binom{49}{6}^{-1} \left[ \binom{50 - k}{6}^{+} - \binom{49 - k}{6}^{+} \right] = \binom{49 - k}{5}^{+} / \binom{49}{6}, \quad k \ge 1.$$

Using the general fact that, for an integer-valued random variable N, expectation and variance may be computed from

$$E(N) = \sum_{k \ge 1} P(N \ge k) \tag{2.1}$$

and

$$Var(N) = 2\sum_{k>1} kP(N \ge k) - E(N) - (E(N))^2$$
(2.2)

(this is readily seen upon writing

$$E(N) = \sum_{j \ge 1} j P(N = j) = \sum_{j \ge 1} \left( \sum_{k=1}^{j} 1 \right) P(N = j),$$

$$E(N(N+1)) = \sum_{j \ge 1} j (j+1) P(N = j) = 2 \sum_{j \ge 1} \left( \sum_{k=1}^{j} k \right) P(N = j),$$

and then interchanging the order of summation); it follows that

$$E(X_j) = {49 \choose 6}^{-1} \sum_{k=1}^{44} {50 - k \choose 6} = \frac{50}{7} = 7.1428...$$

and

$$Var(X_j) = 2 \cdot {\binom{49}{6}}^{-1} \sum_{k=1}^{44} k \cdot {\binom{50-k}{6}} - E(X_j) - (E(X_j))^2 = \frac{3225}{98} = 32.9081...$$

Note that the distribution of  $X_j$  does not depend on j, which is intuitively obvious.

# 3. JOINT DISTRIBUTION OF SPACINGS

For the sake of lucidity, we first consider the joint distribution of two spacings  $X_i$  and  $X_j$ , where  $1 \le i < j \le 5$ . Here the idea is to "shrink" a ticket  $(t_1, ..., t_6) \in T$  satisfying  $t_{i+1} - t_i \ge k$ ,  $t_{j+1} - t_j \ge \ell$ , where  $k, \ell \ge 1, k + \ell \le 45$ , into the 6-tuple  $(u_1, ..., u_6)$ , where

$$u_{v} = t_{v},$$
  $v = 1, ..., i,$   
 $u_{v} = t_{v} - (k-1),$   $v = i+1, ..., j,$   
 $u_{v} = t_{v} - (k-1) - (\ell-1),$   $v = j+1, ..., 6.$ 

Since the "shrinking mapping" is now one-to-one from  $\{t \in T : t_{i+1} - t_i \ge k, t_{j+1} - t_j \ge \ell\}$  onto  $\{(u_1, ..., u_6) : 1 \le u_1 < \cdots < u_6 \le 49 - (k-1) - (\ell-1)\}$ , we obtain

$$P(X_i \ge k, X_j \ge \ell) = {51 - k - \ell \choose 6}^+ / {49 \choose 6}, k, \ell \ge 1,$$

and thus, by the inclusion-exclusion principle

$$P(X_{i} = k, X_{j} = \ell) = P(X_{i} \ge k, X_{j} \ge \ell) - P(X_{i} \ge k, X_{j} \ge \ell + 1)$$

$$-P(X_{i} \ge k + 1, X_{j} \ge \ell) + P(X_{i} \ge k + 1, X_{j} \ge \ell + 1)$$

$$= {49 \choose 6}^{-1} \left[ {51 - k - \ell \choose 6}^{+} - 2 {50 - k - \ell \choose 6}^{+} + {49 - k - \ell \choose 6}^{+} \right] = {49 - k - \ell \choose 4}^{+} / {49 \choose 6},$$
(3.1)

 $(k, \ell \ge 1)$ . From this and

$$E(X_i X_j) = \sum_{k \ge 1} \sum_{\ell \ge 1} k\ell P(X_i = k, X_j = \ell) = \sum_{k \ge 1} \sum_{\ell \ge 1} P(X_i \ge k, X_j \ge \ell)$$
$$= \binom{49}{6}^{-1} \sum_{k \ge 1} \sum_{\ell \ge 1} \binom{51 - k - \ell}{6}^{+} = \frac{1275}{28} = 45.535...$$

the correlation coefficient between  $X_i$  and  $X_j$  is given by

$$\rho(X_i, X_j) = \frac{E(X_i X_j) - E(X_i) E(X_j)}{(\text{Var}(X_i) \text{Var}(X_j))^{1/2}} = -\frac{1}{6}.$$
(3.2)

The fact that  $\rho(X_i, X_j)$  is negative is also intuitively obvious since large values of  $X_i$  tend to produce small values of  $X_i$  and vice versa.

It should now be clear how to obtain the joint distribution of more than two spacings. For example, a ticket  $(t_1, ..., t_6)$  satisfying

$$t_{i+1} - t_i \ge k_i, \quad i = 1, ..., 5,$$
 (3.3)

where  $k_1 + \cdots + k_5 \le 48$ , may be "shrunk" into the ticket  $(u_1, \dots, u_6)$ , where

$$u_1 = t_1$$
,  $u_j = t_j - \sum_{\nu=1}^{j-1} (k_{\nu} - 1)$ ,  $2 \le j \le 6$ .

This shrinking mapping is one-to-one from the set of tickets satisfying (3.3) onto the set of ordered 6-tuples from 1 to  $54 - \sum_{\nu=1}^{5} k_{\nu}$ . We therefore have

$$P(X_j \ge k_j \text{ for } j = 1, 2, ..., 5) = {54 - k_1 - k_2 - k_3 - k_4 - k_5 \choose 6}^{+} / {49 \choose 6}$$
 (3.4)

 $(k_1 \ge 1, ..., k_5 \ge 1)$ , and probabilities of the type  $P(X_j = \ell_j, j = 1, 2, ..., 5)$  may be obtained from (3.4) and the method of inclusion and exclusion by analogy with (3.1). Note that the joint distribution of  $(X_1, X_2, X_3, X_4, X_5)$  is invariant with respect to permutations of the  $X_j$ .

#### 4. THE DISTRIBUTION OF THE SMALLEST SPACING

The idea of "ticket shrinking" yields the following simple derivation of the results of Kennedy and Cooper [1] concerning the minimum spacing  $S = \min(X_1, X_2, X_3, X_4, X_5)$ .

Since  $S \ge k$  if and only if each of the  $X_i$  is not smaller than k, (3.4) entails

$$P(S \ge k) = {54 - 5k \choose 6}^+ / {49 \choose 6}, k \ge 1,$$

and thus

$$P(S = k) = P(S \ge k) - P(S \ge k + 1)$$

$$= {49 \choose 6}^{-1} \left[ {54 - 5k \choose 6}^{+} - {49 - 5k \choose 6}^{+} \right], \quad k \ge 1.$$

From (2.1) the expectation of S is

$$E(S) = {49 \choose 6}^{-1} \sum_{k=1}^{9} {54-5k \choose 6} = \frac{4381705}{2330636} = 1.88004...,$$

and, in addition to Kennedy and Cooper, the variance of S [computed from (2.2)] is given by

$$Var(S) = \frac{6842931587015}{5431864164496} = 1.25977....$$

## 5. THE DISTRIBUTION OF THE LARGEST SPACING

We now answer the question posed by Kennedy and Cooper [1] concerning the distribution of the largest spacing  $L = \max(X_1, X_2, X_3, X_4, X_5)$ .

Noting that  $L \ge k$  if and only if at least one of the  $X_j$  is not smaller than k, the reasoning of section 3 and the inclusion-exclusion formula yield

$$P(L \ge k) = P(X_1 \ge k \text{ or } X_2 \ge k \text{ or } \cdots \text{ or } X_5 \ge k)$$

$$= 5P(X_1 \ge k) - \binom{5}{2}P(X_1 \ge k, X_2 \ge k) + \binom{5}{3}P(X_1 \ge k, X_2 \ge k, X_3 \ge k)$$

$$-\binom{5}{4}P(X_j \ge k; \ j = 1, ..., 4) + 5P(X_j \ge k; \ j = 1, ..., 5)$$

$$= \binom{49}{6}^{-1}\sum_{j=1}^{5} (-1)^{j-1} \binom{5}{j} \binom{49-j(k-1)}{6}^{+}$$

 $[k \ge 1]$ ; note that  $P(L \ge k) = 0$  if  $k \ge 45$  and thus

$$P(L=k) = P(L \ge k) - P(L \ge k+1)$$

$$= \binom{49}{6}^{-1} \sum_{j=1}^{5} (-1)^{j-1} \binom{5}{j} \left[ \binom{49 - j(k-1)}{6}^{+} - \binom{49 - jk}{6}^{+} \right] \quad (k = 1, 2, ..., 44).$$

Figure 5.1 shows a bar chart of the probability distribution of the maximum spacing L.

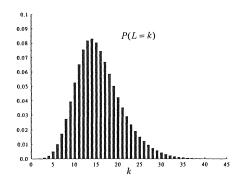


FIGURE 5.1. Distribution of the Largest Spacing on a "6/49" Lottery Ticket

Note that the distribution is skewed to the right. The mode is 14 and has a probability of 0.0828..., whereas the mean "largest space" is given by

$$E(L) = \sum_{k=1}^{44} P(L \ge k) = \frac{109376345}{6991908} = 15.643...$$

#### 6. THE GENERAL CASE

It is clear that the reasoning given above carries over nearly literally to the case of a generalized lottery where r numbers from the sequence 1, 2, ..., n are chosen. For a ticket  $t=(t_1,...,t_r)$  with  $1 \le t_1 < \cdots < t_r \le n$  let, as above,  $X_j(t) = t_{j+1} - t_j$ ,  $1 \le j \le r - t_j$ , denote a single spacing, and write  $S(t) = \min_{1 \le j \le r-1} X_j(t)$ ,  $L(t) = \max_{1 \le j \le r-1} X_j(t)$  for the smallest resp. the largest spacing.

As a simple consequence of the idea of "ticket shrinking," we have

$$P(X_{j_1} \ge k_1, X_{j_2} \ge k_2, ..., X_{j_m} \ge k_m) = \binom{n - \sum_{\nu=1}^{m} (k_{\nu} - 1)}{r} / \binom{n}{r}$$
(6.1)

 $(1 \le m \le r-1; \ 1 \le j_1 < j_2 < \dots < j_m \le r-1; \ k_1 \ge 1, \dots, k_m \ge 1)$  which entails that the individual spacings are exchangeable, i.e., the joint distribution of any subset of  $X_1, \dots, X_{r-1}$  depends only on the cardinality of this subset.

For a single spacing  $X_i$ , it follows that

$$P(X_{j} \ge k) = {n+1-k \choose r}^{+} / {n \choose r}, \quad k \ge 1,$$

$$P(X_{j} = k) = {n \choose r}^{-1} \left[ {n+1-k \choose r}^{+} - {n-k \choose r}^{+} \right] = {n-k \choose r-1}^{+} / {n \choose r}, \quad k \ge 1,$$

$$E(X_{j}) = \sum_{k=1}^{n+1-r} P(X_{j} \ge k) = \frac{n+1}{r+1},$$

$$Var(X_{j}) = 2 \cdot \sum_{k=1}^{n+1-r} kP(X_{j} \ge k) - \frac{n+1}{r+1} - \left( \frac{n+1}{r+1} \right)^{2} = \frac{(n+1)r(n-r)}{(r+1)^{2}(r+2)}.$$
(6.2)

Note that  $P(X_i = k) = 0 \text{ if } k > n+1-r$ .

For the smallest spacing S, we have

$$P(S \ge k) = \binom{n - (r - 1)(k - 1)}{r} / \binom{n}{r}, \quad k \ge 1,$$

$$P(S = k) = \left[ \binom{n - (r - 1)(k - 1)}{r} - \binom{n - (r - 1)k}{r} \right] / \binom{n}{r}, \quad k \ge 1,$$

$$E(S) = \binom{n}{r} \sum_{k=1}^{n-1} \binom{n - (r - 1)(k - 1)}{r}$$

(see also Kennedy and Cooper [1]).

430

Finally,

$$P(L \ge k) = \binom{n}{r}^{-1} \sum_{\nu=1}^{r-1} (-1)^{\nu-1} \binom{r-1}{\nu} \binom{n-\nu(k-1)}{r}^{+}, \quad k \ge 1,$$

$$P(L = k) = \binom{n}{r}^{-1} \sum_{\nu=1}^{r-1} (-1)^{\nu-1} \binom{r-1}{\nu} \left[ \binom{n-\nu(k-1)}{r}^{+} - \binom{n-\nu k}{r}^{+} \right], \quad k \ge 1,$$

$$E(L) = \binom{n}{r}^{-1} \sum_{k=1}^{n-(r-1)} \sum_{\nu=1}^{r-1} (-1)^{\nu-1} \binom{r-1}{\nu} \binom{n-\nu(k-1)}{r}^{+}.$$

Note that P(L = k) = 0 if k > n - r + 1 and P(S = k) = 0 if k > (n - 1) / (r - 1).

**Remark:** In addition to  $X_1(t), \ldots, X_{r-1}(t)$ , one could introduce the spacings  $X_0(t) = t_1$  and  $X_r(t) = n + 1 - t_r$ . By an obvious modification of the "shrinking argument," it is readily seen that (6.1) remains valid for the larger range  $1 \le m \le r + 1$ ,  $0 \le j_1 < j_2 < \cdots < j_m \le r$  which entails the exchangeability of  $X_0, X_1, \ldots, X_r$ .

Since  $\sum_{i=0}^{r} X_i = n+1$ , it follows that

$$n+1 = E\left(\sum_{j=0}^{r} X_j\right) = \sum_{j=0}^{r} E(X_j) = (r+1) \cdot E(X_j)$$

which gives a second derivation of (6.2). Moreover, from the equality

$$0 = \text{Var}\left(\sum_{j=0}^{r} X_{j}\right) = \sum_{j=0}^{r} \text{Var}(X_{j}) + \sum_{\substack{j=0\\j \neq k}}^{r} \sum_{k=0}^{r} \text{Cov}(X_{j}, X_{k})$$

and exchangeability, we obtain the covariance

$$Cov(X_j, X_k) = -\frac{1}{r} Var(X_j), \quad 0 \le j \ne k \le r,$$

and thus the correlation coefficient

$$\rho(X_j, X_k) = -\frac{1}{r}, \quad 0 \le j \ne k \le r,$$

which is a generalization of (3.2).

Finally, redefining S and L as to include the spacings  $X_0$  and  $X_r$ , the expressions for the distribution and expectation of S resp. L continue to hold if each "r-1" is replaced by "r+1" [of course,  $\binom{n}{r}$  remains unchanged].

## REFERENCE

 R. E. Kennedy & C. N. Cooper. "The Statistics of the Smallest Space on a Lottery Ticket." The Fibonacci Quarterly 29.4 (1991):367-70.

AMS Classification Numbers: 60C05, 05A99, 60E05

# THE SWITCH, SUBTRACT, REORDER ROUTINE

# **Anne Ludington Young**

Department of Mathematical Sciences, Loyola College in Maryland, Baltimore, MD 21210 (Submitted March 1994)

Let g be a positive integer greater than 1. An integer x is an **ordered 4-digit base** g **number** if

$$x = a_1 \cdot g^3 + a_2 \cdot g^2 + a_3 \cdot g + a_4 = a_1 a_2 a_3 a_4$$
 base g

with

$$g > a_1 \ge a_2 \ge a_3 \ge a_4 \ge 0$$
.

The following procedure, when applied to x, yields another ordered 4-digit base g number. Switch the first two digits of x with the last two digits; then subtract the "switched" number from x:

$$a_1 a_2 a_3 a_4 - a_3 a_4 a_1 a_2 = b_1 b_2 b_3 b_4$$
 base g.

Finally, rearrange the digits so that the result, R(x), is an ordered number. Thus,

$$R(x) = a_1' a_2' a_3' a_4'$$
 base g,

where the  $a_i'$ 's are a permutation of the  $b_i$ 's and  $a_i' \ge a_2' \ge a_3' \ge a_4'$ . This procedure is called the Switch, Subtract, Reorder (SSR) routine.

As an example of the SSR routine, consider the base 15 number  $x = 13\ 12\ 10\ 8$ . We switch the digits of x and subtract:

When we reorder, we get  $R(x) = 11 \ 11 \ 3 \ 3$ .

Returning to the general case, we can apply the SSR routine to the number R(x) to get  $R(R(x)) = R^2(x)$ . More generally,  $R^{i+1}(x) = R(R^i(x))$  for  $i \ge 1$ . Since there are only finitely many ordered 4-digit base g numbers, repetition must occur. That is,  $R^j(x) = R^i(x)$  for some i and j.

Continuing to use base 15 as an example, we will find the iterates of x = 13 12 10 8. For reasons which will become clear shortly, for each ordered number  $a_1 a_2 a_3 a_4$ , we will also calculate the difference  $diff = a_2 - a_4$ . The results are given in the following table:

TABLE 1

i	$R^{i}(x)$	diff
1 2 3 4 5	11 11 3 3 8 7 7 6 14 13 1 0 13 12 2 1 11 10 4 3	8 1 13 11 7
6	8 7 7 6	1

Notice that  $R^2(x) = R^6(x)$ . We write  $\langle R^2(x), R^3(x), R^4(x), R^5(x) \rangle$  and call this expression a cycle of length 4. We say that  $R^2(x)$  generates the cycle. Of course,  $R^3(x), R^4(x)$ , and  $R^5(x)$  also generate the cycle.

As the example above illustrates, for a given g the SSR routine always gives rise to at least one cycle. We will characterize the cycles by answering the following questions: How many are there? What number(s) is(are) in each cycle? What is the length of each cycle? What is the smallest i such that, for all x,  $R^i(x)$  is in a cycle?

The SSR routine is a variation of the Kaprekar routine. For the Kaprekar routine, we reverse the digits of x and subtract:

$$a_1 a_2 a_3 a_4 - a_4 a_3 a_2 a_1 = b_1 b_2 b_3 b_4$$
 base g.

Reordering the digits gives K(x). The Kaprekar routine has been studied extensively (see [1]-[8]). Among the questions addressed are those that appear at the end of the previous paragraph.

## A REDUCTION OF THE PROBLEM

For an ordered number  $x = a_1 \ a_2 \ a_3 \ a_4$ , the **digit differences** of x are  $D = a_1 - a_3$  and  $d = a_2 - a_4$ . Clearly,  $0 \le D$ , d < g. Now, if  $R(x) = a_1' \ a_2' \ a_3' \ a_4'$ , then the digit differences of R(x) are  $D' = a_1' - a_3'$  and  $d' = a_2' - a_4'$ . As a matter of terminology, if it should happen that D = d, then we will refer to this number as the **digit difference** of x. That is, we will use the singular form of the noun.

The reader may wonder why we would want to look at digit differences. In part, we do so because similar digit differences play an important role in the Kaprekar routine analysis. More importantly, for a given x, R(x) is completely determined by D and d. Moreover, as we now show, D' = d'. Thus, after one application of the SSR routine, the digit differences are equal. This observation will greatly simplify the problem of characterizing the SSR cycles.

**Theorem 1:** Let  $x = a_1 a_2 a_3 a_4$  be an ordered 4-digit base g number with digit differences D and d. Denote the digit differences of R(x) by D' = d'. Then

$$\begin{array}{ll} D' = d' = 0 & \text{if } D = d = 0, \\ D' = d' = g - D & \text{if } 0 < D \le (g+1)/2 \& d = 0, \\ D' = d' = D - 1 & \text{if } (g+1)/2 \le D \& d = 0, \\ D' = d' = |g - D - d| & \text{if } 0 \le D \le (g-1)/2 \& 0 < d \le (g+1)/2 \\ & \text{or } (g-1)/2 \le D \& (g+1)/2 \le d, \\ D' = d' = |D - d + 1| & \text{if } 0 \le D \le (g-1)/2 \& (g+1)/2 \le d \\ & \text{or } (g-1)/2 \le D \& 0 < d \le (g+1)/2. \end{array}$$

**Proof:** We consider three cases.

<u>Case 1.</u> Suppose D = 0 and d = 0. Then all the digits of x are equal. In that case, R(x) = 0 and D' = d' = 0.

<u>Case 2</u>. Suppose  $D \neq 0$  and d = 0. Since d = 0,  $a_2 = a_3 = a_4$ . We begin by switching and subtracting:

To find R(x), we reorder the digits in (1). There are two possibilities:

The first occurs when  $0 < D \le (g+1)/2$ ; in that case, D' = d' = g - D. The second occurs when  $(g+1)/2 \le D$ ; then D' = d' = D - 1.

<u>Case 3</u>. Suppose  $d \neq 0$ . We switch and subtract:

To find R(x), we reorder the digits in (2). Now  $D \ge d-1$  iff  $g-d \ge g-D-1$ ; also,  $D \ge g-d$  iff  $d-1 \ge g-D-1$ . Thus, R(x) equals one of the following eight ordered numbers:

R(x) equals one of the first four numbers when

$$0 \le D \le (g-1)/2 \& 0 < d \le (g+1)/2$$

or

$$(g-1)/2 \le D \& (g+1)/2 \le d$$
.

For these numbers, D' = d' = |g - D - d|. On the other hand, R(x) equals one of the last four numbers when

$$0 \le D \le (g-1)/2 \& (g+1)/2 \le d$$

or

$$(g-1)/2 \le D \& 0 < d \le (g+1)/2$$
.

For these numbers, D' = d' = |D - d + 1|.  $\square$ 

As stated above, we refer to d' as the digit difference of R(x). We now derive several corollaries. Since the first two follow immediately from the proof of Theorem 1, their proofs are omitted.

Corollary 1: Let x and y be ordered 4-digit base g numbers with digit differences  $D_x$ ,  $d_x$  and  $D_y$ ,  $d_y$ , respectively. If  $D_x = D_y$  and  $d_x = d_y$ , then R(x) = R(y).

**Corollary 2:** Let x be an ordered 4-digit base g number with equal digit differences; that is, D = d. Then

$$R(x) = 0 \ 0 \ 0$$
 if  $d = 0$ ,  
 $R(x) = g - d \ g - d - 1 \ d \ d - 1$  if  $0 < d < g/2$ ,  
 $R(x) = g/2 \ g/2 \ g/2 - 1 \ g/2 - 1$  if  $d = g/2$ ,  
 $R(x) = d \ d - 1 \ g - d \ g - d - 1$  if  $g/2 < d$ .

Corollary 3: Let x be an ordered 4-digit base g number with equal digit differences; that is, D = d. Denote the digit difference of R(x) by d'. Then d' = 0 if and only if d = 0. Moreover, if  $d \neq 0$ , then

$$d' = |g - 2d|$$
 if  $d \neq g/2$ ,  
 $d' = 1$  if  $d = g/2$ .

**Proof:** We use Corollary 2 to find R(x). The result follows immediately by computing the digit difference of R(x) in each case.  $\Box$ 

Corollary 4: Let x be an ordered 4-digit base g number. If  $R^i(x) = 0$  for some  $i \ge 1$ , then  $R^2(x) = 0$ .

**Proof:** Let d' be the digit difference of R(x). Since R'(x) = 0, its digit difference is 0. Applying Corollary 3, repeatedly if necessary, gives d' = 0. By Corollary 2,  $R^2(x) = 0$ .  $\square$ 

Since R(0) = 0, there is always one SSR cycle which contains the single number 0. We will call this the **zero cycle** and denote it by  $\langle 0 \rangle$ . By Corollary 4, we know that if x leads to the zero cycle, it will do so in two or fewer steps. Corollary 3 tells us that there are other numbers which do not lead to the zero cycle. Consequently, the SSR routine always has at least one nonzero cycle.

#### A RELATED FUNCTION

Suppose x generates a nonzero SSR cycle of length m. Since  $R^m(x) = x$ , the digit differences of x are equal and nonzero. Moreover, by Corollary 3, if the digit difference of x is  $d \neq g/2$ , then the digit difference of R(x) is |g-2d|. This observation leads us to consider |g-2d|.

The function F(d) = |g - 2d|,  $0 \le d \le g$ , was studied by this author in another context [9]. Since  $0 \le F(d) \le g$ , iteration of F gives rise to one or more cycles. As we will see, the cycles of F are in a one-to-one correspondence with the nonzero SSR cycles so long as the former do not contain 0, g/2, or g.

Before continuing, we consider an example. Earlier we applied the SSR routine to the base 15 number x = 13 12 10 8. We found R(x) = 11 11 3 3, which has a digit difference of 8. Now,

$$F(8) = |15-16| = 1,$$
  
 $F^{2}(8) = F(1) = |15-2| = 13,$   
 $F^{3}(8) = F(13) = |15-26| = 11,$   
 $F^{4}(8) = F(11) = |15-22| = 7,$   
 $F^{5}(8) = F(7) = |15-14| = 1.$ 

By Corollary 3, since the digit difference of R(x) is 8, the digit difference of  $R^2(x)$  is F(8). More generally, for  $i \ge 1$ , the digit difference of  $R^{i+1}(x)$  is  $F^i(8)$ . This is confirmed by examining the diff column in Table 1 and comparing it with the calculations above. Thus, we see that the F-cycle  $\langle 1, 13, 11, 7 \rangle$  corresponds to the SSR cycle  $\langle R^2(x), R^3(x), R^4(x), R^5(x) \rangle$ .

The relevant properties of F are listed below. Proofs may be found in [9]. We will write  $F_{\varrho}(d)$  in place of F(d) whenever the context requires this elaboration.

**Theorem 2:** Let k be the nonnegative integer such that  $2^k || g$ . Then, for 0 < d < g, we have:

- (a) F(g/2) = 0, F(0) = g, and F(g) = g.
- **(b)** d is in an F-cycle if and only if  $2^k || d$ .
- (c) For i > 1,  $i \cdot d$  is in an  $F_{ig}$ -cycle if and only if d is in an  $F_g$ -cycle. More generally,  $\langle i \cdot d_1, i \cdot d_2, ..., i \cdot d_n \rangle$  is an  $F_{ig}$ -cycle if and only if  $\langle d_1, d_2, ..., d_n \rangle$  is an  $F_g$ -cycle.
- (d) Let *i* be the nonnegative integer such that  $2^{i} || d$ . If  $i < k-1, 2^{i+1} || F(d)$ ; if  $i = k-1, 2^{k+1} || F(d)$ ; if  $i > k-1, 2^{k} || F(d)$ .
- (e) For i > 1,  $F^{i}(d)$  is congruent to either  $2^{i}d$  or  $-2^{i}d$  modulo g.
- (f)  $2^{k} || F^{i}(d)$  when i > k.

Several conclusions are immediate from Theorem 2. By (a), 0 and g/2 are not contained in an F-cycle. Moreover,  $\langle g \rangle$  is an F-cycle of length 1. This cycle is called the **trivial** cycle; all other cycles are **proper** cycles. Part (b) tells us that proper cycles exist if and only if g is not a power of 2. By (c), it suffices to determine cycles for odd g. Additionally, we need only consider those d which are relatively prime to g. We will call cycles containing such d **prime**. All other cycles are **composite** since they may be found using (c). Parts (b) and (f) together imply that  $F^i(d)$  is in a cycle whenever i > k.

Before continuing, we illustrate the previous theorem and definitions. We begin with g = 5. By Theorem 2(b), d is in an  $F_5$ -cycle if and only if d is odd. Since F(1) = |5-2| = 3 and F(3) = |5-6| = 1, the only proper  $F_5$ -cycle is  $\langle 1, 3 \rangle$ . The trivial cycle is  $\langle 5 \rangle$ .

As a second example, we let g = 20. By Theorem 2(b), d is in an  $F_{20}$ -cycle if and only if  $4 \| d$ . Since g is even, each proper cycle is composite and may be derived from an  $F_5$ -cycle by multiplying by 4. As we have just shown, the only proper  $F_5$ -cycle is  $\langle 1, 3 \rangle$ . Consequently,  $\langle 4, 12 \rangle$  is the only proper  $F_{20}$ -cycle.

Before considering a third example, we state another result which was proved in [9]. It tells us how to find the lengths of prime cycles.

**Theorem 3:** Let g be an odd positive integer and let m be the smallest integer such that  $2^m$  is congruent to either 1 or -1 modulo g. Then each prime F-cycle has length m. Moreover, there are  $\phi(g)/2m$  such cycles, where  $\phi(g)$  is the Euler Phi function.

We now consider g = 15. By Theorem 2(b), d is in an  $F_{15}$ -cycle if and only if d is odd. Since  $\phi(15) = 8$  and  $2^4 \equiv 1 \pmod{15}$ , there is one prime cycle of length 4. As we have already seen, this cycle is  $\langle 1, 13, 11, 7 \rangle$ . The composite  $F_{15}$ -cycles, found from the proper  $F_3$ - and  $F_5$ -cycles using Theorem 2(c), are  $\langle 5 \rangle$  and  $\langle 3, 9 \rangle$ .

## THE SSR-CYCLES

We now use the previous results to characterize the SSR cycles.

**Lemma 1:** Suppose d generates a proper F-cycle of length m. Then there exists a nonzero SSR cycle of length m. Moreover, this cycle is generated by an ordered number whose digit difference is d.

NOV.

436

**Proof:** Since g/2 is not in an F-cycle,  $F^i(d) \neq g/2$  for  $0 \le i$ . Let  $x = d \ d \ 0 \ 0$ . Clearly, x has equal digit differences of d. Hence, the digit differences of  $R^i(x)$  are  $F^i(d)$ ,  $i \ge 1$ . By hypothesis,  $F^i(d) \ne F^m(d)$ , 0 < i < m, and  $F^m(d) = d$ . This means that  $R^i(x) \ne R^m(x)$ ; further,  $R^m(x)$  and x have the same digit differences. Hence, by Corollary 1,  $R^{m+1}(x) = R(x)$ . Thus,  $\langle R(x), ..., R^m(x) \rangle$  is an SSR cycle of length m; it is generated by  $R^m(x)$ , whose digit difference is d.  $\square$ 

**Lemma 2:** Suppose x generates a nonzero SSR cycle of length m. Let d be the digit difference of x. If  $F^i(d) \neq g/2$ ,  $0 \le i < m$ , then d generates a proper F-cycle of length m.

**Proof:** The digit difference of  $R^i(x)$  is  $F^i(d) \neq g/2, i \geq 1$ . By hypothesis,  $R^m(x) = x$ ; hence,  $F^m(d) = d$  and d generates a proper F-cycle. If  $F^i(d) = d$  for some i, 0 < i < m, then by Corollary 1,  $R^{i+1}(x) = R(x)$ . But then the SSR cycle would have length i < m. Thus, the F-cycle generated by d has length m.  $\square$ 

**Theorem 4:** Suppose  $g = 2^k \cdot t$ , where  $0 \le k$  and t is an odd positive integer greater than 1. Let x be an ordered 4-digit base g number with equal digit differences of d. Then x generates an SSR cycle of length m if and only if d generates an F-cycle of length m.

**Proof:** By Lemmas 1 and 2, we need only consider the case when x is an ordered number with equal digit differences of g/2. Suppose that x generates a nonzero SSR cycle of length m. Then, by Corollary 3, the digit difference of R(x) is 1. Thus, for  $1 < i \le m$ , the digit differences of  $R^i(x)$  is  $F^{i-1}(1)$ . Since  $R^m(x) = x$ ,  $F^{m-1}(1) = g/2 = 2^{k-1} \cdot t$ . By Theorem 2(e),  $F^{m-1}(1)$  is congruent to either  $2^{m-1}$  or  $-2^{m-1}$  modulo g. As a shorthand notation, we will write  $F^{m-1}(1) \equiv \pm 2^{m-1} \pmod{g}$ . Hence,  $2^{k-1} \cdot t \equiv \pm 2^{m-1} \pmod{2^k \cdot t}$ . Since t is an odd positive integer greater than 1, we have reached a contradiction.  $\square$ 

**Theorem 5:** Suppose  $g = 2^k$ , where 0 < k. Then there is exactly one nonzero SSR cycle. This cycle has length k and contains:

$$w = 1 \ 1 \ 0 \ 0$$
 if  $g = 2$ ,  
 $w = 2^k - 2^{k-2} \ 2^k - 2^{k-2} - 1 \ 2^{k-2} \ 2^{k-2} - 1$  if  $g > 2$ .

**Proof:** Since g is a power of 2, there are no proper F-cycles. Hence, by Lemma 2, there is at most one nonzero SSR cycle. Moreover, it must be generated by an ordered number whose digit difference is g/2.

If g = 2, then  $\langle w \rangle$  is a nonzero SSR cycle, since R(w) = w. If g > 2, the digit difference of w is  $2^{k-1} = g/2$ . By Corollary 2,

$$R(w) = 2^{k-1} 2^{k-1} 2^{k-1} - 1 2^{k-1} - 1$$

and

$$R^{i+2}(w) = 2^k - 2^i \quad 2^k - 2^i - 1 \quad 2^i \quad 2^i - 1, \quad 0 \le i \le k - 2.$$

Thus,  $R^k(w) = w$ .  $\square$ 

Theorems 4 and 5 completely characterize the nonzero SSR cycles. If g is not a power of 2, then the nonzero SSR cycles are in a one-to-one correspondence with the proper F-cycles. The cycle lengths can be determined using Theorems 2(c) and 3. The numbers that generate the SSR

cycles can be found from the F-cycles using Corollary 2. If g is the k<sup>th</sup> power of 2, then there is exactly one nonzero SSR cycle; it has length k.

Returning to our base 15 example, previously we found that the F-cycles are  $\langle 1, 13, 11, 7 \rangle$ ,  $\langle 5 \rangle$ , and  $\langle 3, 9 \rangle$ : The SSR cycle which corresponds to the first F-cycle is given in Table 1. The SSR cycle which corresponds to the F-cycle  $\langle 5 \rangle$  is  $\langle u \rangle$ , where the digit difference of u is 5; by Corollary 2, u = 10.9.5 4. The SSR cycle which corresponds to the F-cycle  $\langle 3, 9 \rangle$  is  $\langle v, R(v) \rangle$ , where the digit difference of v is 3; by Corollary 2, v = 9.8.6.5.

# WHEN IS $R^{i}(x)$ IN A CYCLE?

We now consider the following question. If x is an ordered 4-digit base g number, what is the smallest i such that  $R^{i}(x)$  is in a cycle?

**Lemma 3:** Let k be the nonnegative integer such that  $2^k || g$ . For all d satisfying 0 < d < g,  $F^{k+1}(d)$  is in an F-cycle. Moreover,  $F^k(1)$  is not in an F-cycle.

**Proof:** The first statement follows immediately using parts (b) and (f) of Theorem 2. For the second, we use Theorem 2(d) to show that  $2^j ||F^j(1)|$  for  $j \le k-1$  and  $2^{k+1} |F^k(1)|$ . Hence, by Theorem 2(b),  $F^k(1)$  is not in an F-cycle.  $\square$ 

**Theorem 6:** Suppose  $g = 2^k \cdot t$ , where  $0 \le k$  and t is an odd positive integer greater than 1. Let x be an ordered 4-digit base g number. Then  $R^{2k+2}(x)$  is in an SSR cycle. Moreover, there exists an ordered 4-digit base g number y such that  $R^{2k+1}(y)$  is not in an SSR cycle.

**Proof:** Let d be the digit difference of R(x). If d = 0, then  $R^2(x) = 0$ . Hence, we can assume  $d \neq 0$ .

First, we consider the case when g is odd. The digit difference of  $R^2(x)$  is F(d) = |g - 2d|. Since F(d) is odd, it is in a proper F-cycle. Hence, by Theorem 4,  $R^2(x)$  is in a nonzero SSR cycle. Now consider  $y = 1 \ 0 \ 0$ . Calculating R(y), we find:

$$R(y) = g - 1 g - 1 0 0$$
.

The digit difference of R(y) equals g-1, which is even. Since g-1 is not in an F-cycle, R(y) is not in an SSR cycle, by Theorem 4.

Now suppose that g is even; i.e., k > 0. If  $F^i(d) \neq g/2$  for  $0 \le i$ , then  $F^i(d)$  is the digit difference of  $R^{i+1}(x)$ . By Lemma 3,  $F^{k+1}(d)$  is in a proper F-cycle. Hence,  $R^{k+2}(x)$  is in an SSR cycle. On the other hand, suppose that  $F^i(d) = g/2$  for some i,  $0 \le i \le k-1$ . Then the digit difference of  $R^{i+2}(x)$  is 1. Consequently,  $F^j(1)$  is the digit difference of  $R^{i+j+2}(x)$  for  $j \le k$ . Since  $F^k(1)$  is not in a proper F-cycle,  $R^{i+k+2}(x)$  is not in an SSR cycle, by Theorem 4. However, again by Theorem 4, because  $F^{k+1}(1)$  is in a proper F-cycle,  $R^{i+k+3}(x)$  is in an SSR cycle. Consequently, for all x,  $R^{2k+2}(x)$  is in an SSR cycle.

We now consider  $y = t \ 0 \ 0 \ 0$ . The digit differences of y are t and 0. By Theorem 1, the digit difference of R(y) is  $d = 2^k \cdot t - t$ . By induction, it is easily established that

$$F^{i}(d) = 2^{k} \cdot t - 2^{i} \cdot t, \quad 0 \le i \le k - 1.$$

Hence,  $F^{k-1}(d) = g/2$ . By the results established above,  $R^{2k+1}(y)$  is not in an SSR cycle.  $\Box$ 

**Lemma 4:** Suppose  $g = 2^k$ , where 1 < k. For all d satisfying 0 < d < g, there exists an integer i such that  $F^i(d) = g/2$  for  $0 \le i \le k-2$ .

**Proof:** Let j be the integer such that  $2^{j} \| d$ ; of course,  $0 \le j \le k-1$ . Then  $2^{k-1-j} \cdot d \equiv 2^{k-1} \pmod{2^k}$ . Since  $F^{k-1-j}(d) \equiv \pm 2^{k-1-j} \cdot d \pmod{g}$ ,  $F^{k-1-j}(d) = g/2$ .

If k = 2, then  $F^0(g-1) = g-1 \neq 2$ . If k > 2, for  $0 \le i \le k-2$ ,

$$F^{i}(g-1) = F^{i}(2^{k}-1) = 2^{k}-2^{i} \neq 2^{k-1}$$
.  $\Box$ 

**Theorem 7:** Suppose  $g = 2^k$ , where 1 < k. Let x be an ordered 4-digit base g number. Then  $R^k(x)$  is in an SSR cycle. Moreover, there exists an ordered 4-digit base g number y such that  $R^{k-1}(y)$  is not in an SSR cycle.

**Proof:** Let d be the digit difference of R(x). If d = 0, then  $R^2(x) = 0$ . Hence, we can assume  $d \neq 0$ . By Lemma 4,  $F^i(d) = g/2$  for some i,  $0 \le i \le k-1$ . By Theorem 5, this implies that  $R^{i+1}(x)$  is in the nonzero SSR cycle. Hence, for all x,  $R^k(x)$  is in an SSR cycle.

We now consider  $y = 1 \ 0 \ 0 \ 0$ . Calculating R(y), we find

$$R(y) = g - 1 g - 1 0 0.$$

The digit difference of R(y) is g-1. By Lemma 4,  $F^i(g-1) \neq g/2$  for  $i \leq k-2$ . Hence,  $R^{k-1}(y)$  is not in the SSR cycle.  $\square$ 

## WHEN DOES THE SSR ROUTINE YIELD A CONSTANT?

Finally, are there bases g for which the SSR routine yields a single, nonzero constant?

**Lemma 5:** Suppose  $1 \le d < g$ . Then  $\langle d \rangle$  is the only proper F-cycle if and only if d = g/3, where  $g = 2^k \cdot 3$  for some  $0 \le k$ .

**Proof:** First, suppose that  $\langle d \rangle$  is the only proper F-cycle. Since F(d) = d, |g-2d| = d and d = g/3. To prove that g has the stated form, we write  $g = 2^k \cdot 3 \cdot t$ , where t is odd. If 1 < t, then, by Theorem 2(b),  $2^k \cdot 3$  is in a proper F-cycle. But this implies there is a second proper F-cycle. Consequently, t = 1 and  $g = 2^k \cdot 3$ . The converse is easily established using Theorem 2(b).  $\square$ 

**Theorem 8:** Suppose  $g = 2^k \cdot 3$ , where  $0 \le k$ . Let

$$z = 2^{k+1} 2^{k+1} - 1 2^k 2^k - 1$$
.

If x is an ordered 4-digit base g number such that  $R^2(x) \neq 0$ , then  $R^{2k+2}(x) = z$ .

**Proof:** By Lemma 5, there is only one proper F-cycle,  $\langle 2^k \rangle$ . Consequently, by Theorem 4, there is only one nonzero SSR cycle and it has length 1. This cycle is  $\langle z \rangle$ , since R(z) = z. By Theorem 6,  $R^{2k+2}(x)$  is in a cycle; hence,  $R^{2k+2}(x) = z$ .  $\square$ 

#### REFERENCES

- 1. H. Hasse & G. D. Prichett. "The Determination of All Four-Digit Kaprekar Constants." J. Reine Angew Math. 299/300 (1978):113-24.
- 2. J. H. Jordan. "Self-Producing Sequences of Digits." Amer. Math. Monthly 71 (1964):61-64.
- 3. D. R. Kaprekar. "Another Solitaire Game." Scripta Mathematica 15 (1949):244-45.
- 4. D. R. Kaprekar. "An Interesting Property of the Number 6174." Scripta Mathematica 21 (1955):304.
- 5. J. F. Lapenta, A. L. Ludington, & G. D. Prichett. "Algorithm To Determine Self-Producing r-Digit g-Adic Integers." J. Reine Math. 310 (1979):100-10.
- 6. A. L. Ludington. "A Bound on Kaprekar Constants." J. Reine Angew Math. 310 (1979): 196-203.
- 7. G. D. Prichett. "Terminating Cycles for Iterated Difference Values of Five-Digit Integers." J. Reine Angew Math. 303/304 (1978):379-88.
- 8. G. D. Prichett, A. L. Ludington, & J. F. Lapenta. "The Determination of All Decadic Kaprekar Constants." *The Fibonacci Quarterly* **19.1** (1981):45-52.
- 9. A. Ludington Young. "A Variation on the Two-Digit Kaprekar Routine." *The Fibonacci Quarterly* **31.2** (1993):138-45.

AMS Classification Numbers: 11A99

\*\*\*

# LINEAR RECURRENCES IN DIFFERENCE TRIANGLES

# Edith H. Luchins

Department of Mathematical Sciences, Rensselaer Polytechnic Institute, Troy, NY 12180

#### Russell Hendel

University of Louisville, Louisville, KY 40208

## Paul Lemke

Center for Communications Research, Princeton, NJ 08540

## **David Tuller**

Department of Mathematical Sciences, Rensselaer Polytechnic Institute, Troy, NY 12180 (Submitted March 1994)

## INTRODUCTION

This paper arose from our interest in generalizing a problem in the February 1993 issue of *The Fibonacci Quarterly* proposed by Piero Filipponi:

Write down the Pell sequence, defined by  $P_0 = 0$ ,  $P_1 = 1$ , and  $P_{n+2} = 2P_{n+1} + P_n$  for  $n \ge 0$ . Form a difference triangle by writing down the successive differences in rows below it. . . . Identify the pattern that emerges down the left side and prove that this pattern continues. [1]

We investigate properties of difference triangles in which the sequence of numbers in the top row satisfies a linear homogeneous recurrence with constant coefficients. These coefficients and the entries in the sequences are integers in the examples in this paper. In the proofs, we assume that we are working over any field containing the integers.

#### 1. DEFINITIONS AND NOTATIONS

We represent difference triangles (e.g., Fig. 1a) in matrix form (Fig. 1b) and refer to their rows and columns (rather than to their diagonals). Let  $d^0$  denote the top (0<sup>th</sup>) row of a difference triangle and let  $d^i$ , i > 0, denote the  $i^{th}$  row. Similarly, let  $d_0$  denote the left-most (0<sup>th</sup>) column of a difference triangle and let  $d_j$ , j > 0, denote the  $j^{th}$  column. The same symbols also denote the corresponding sequences of numbers in the rows and columns.

Let  $d_j^i$  denote the element in the  $i^{th}$  row and the  $j^{th}$  column of the difference triangle (e.g.,  $d_2^1 = -2$  in Fig. 1b). The difference triangle itself may be considered as a double sequence  $\{d_j^i\}, i \geq 0, j \geq 0$ , which obeys

$$d_j^i = d_{j+1}^{i-1} - d_j^{i-1} \text{ for } i \ge 1, \ j \ge 0.$$
 (A)

If the top row of a difference triangle is given, then (A) will yield all the other rows recursively.

This paper deals with difference triangles whose top row satisfies a linear recurrence that is homogeneous and has constant coefficients (LRHCC). Such a recurrence can be characterized by a nonnegative integer k called the *order* of the recurrence, together with an ordered set of k constants  $c_0, c_1, \ldots, c_{k-1}$ . A sequence  $\{a_i\}$  is said to *satisfy* this recurrence if the following equation holds for each  $n \ge 0$ :

$$a_{n+k} = c_{k-1}a_{n+k-1} + \dots + c_1a_{n+1} + c_0a_n$$
 (B)

If k = 0, this becomes  $a_n = 0$  for  $n \ge 0$ .

FIGURE 1. Triangular form (1a) and matrix form (1b) of difference triangle arising from the sequence 1, 2, 7, 5, 9.

#### 2. RECURRENCE RELATIONS

**Theorem 1a:** Let  $\{d_j^i\}$  be a difference triangle, k a nonnegative integer, and  $c_0, c_1, ..., c_k$  constants such that, for all nonnegative integers n,

$$c_k d_{n+k}^i + c_{k-1} d_{n+k-1}^i + \dots + c_1 d_{n+1}^i + c_0 d_n^i = 0$$
 (C)

holds for i = m, where m is some nonnegative integer. Then (C) also holds for all i > m.

**Proof:** We suppose that (C) holds for i = p and show that it holds for i = p + 1. Subtracting (C) with i = p with n unchanged from (C) with i = p and with n replaced by n + 1, we obtain

$$c_k(d_{n+1+k}^p - d_{n+k}^p) + c_{k-1}(d_{n+k}^p - d_{n+k-1}^p) + \dots + c_1(d_{n+2}^p - d_{n+1}^p) + c_0(d_{n+1}^p - d_n^p) = 0$$

for  $n \ge 0$ .

Applying (A) to the parenthetical expressions, we get

$$c_k(d_{n+k}^{p+1}) + c_{k-1}(d_{n+k-1}^{p+1}) + \dots + c_1(d_{n+1}^{p+1}) + c_0(d_n^{p+1}) = 0$$

for  $n \ge 0$ , which is equation (C) with i = p + 1. Since (C) holds for i = m, it now follows by induction that it also holds for all i > m.

Corollary: If the top row of a difference triangle satisfies a given LRHCC, then every row of the triangle satisfies the same recurrence.

**Theorem 1b** Let  $\{d_j^i\}$  be a difference triangle, k a nonnegative integer, and  $b_0, b_1, ..., b_k$  constants such that, for all  $m \ge 0$ ,

$$b_k d_j^{m+k} + b_{k-1} d_j^{m+k-1} + \dots + b_1 d_j^{m+1} + b_0 d_j^m = 0$$

holds for j = n where n is some nonnegative integer. Then it also holds for all j > n.

442

**Proof:** Rewriting (A) as

$$d_{j+1}^{i-1} = d_j^{i-1} + d_j^i \quad \text{for } i \ge 1, j \ge 0,$$
 (A')

we obtain an analogous proof for the columns as for the rows in Theorem 1a.

Corollary: If the 0<sup>th</sup> (left-most) column of a difference triangle satisfies a given LRHCC, then every column of it satisfies the same recurrence.

**Lemma 1a:** 
$$d_j^i = \sum_{s=0}^{\ell} (-1)^s \binom{\ell}{s} d_{j+\ell-s}^{i-\ell}$$
 for  $i \ge \ell \ge 0, j \ge 0$ .

**Proof:** Iterate (A) to obtain

$$d_{j}^{i} = d_{j+1}^{i-1} - d_{j}^{i-1} = (d_{j+2}^{i-2} - d_{j+1}^{i-2}) - (d_{j+1}^{i-2} - d_{j}^{i-2})$$
$$= d_{j+2}^{i-2} - 2d_{j+1}^{i-2} + d_{j}^{i-2} \quad \text{for } i \ge 2, j \ge 0.$$

Continuing, we express an element of the difference triangle as a (linear) function of the elements in the row that is  $\ell$  rows above it:

$$d_{j}^{i} = \binom{\ell}{0} d_{j+\ell}^{i-\ell} - \binom{\ell}{1} d_{j+\ell-1}^{i-\ell} + \dots + (-1)^{\ell-1} \binom{\ell}{\ell-1} d_{j+1}^{i-\ell} + (-1)^{\ell} \binom{\ell}{\ell} d_{j}^{i-\ell} \quad \text{for } i \geq \ell \geq 0, \ j \geq 0.$$

**Lemma 1b:** 
$$d_j^i = \sum_{s=0}^{\ell} {\ell \choose s} d_{j-\ell}^{i+s}$$
 for  $i \ge 0, j \ge \ell \ge 0$ .

**Proof:** Iteration of (A') gives

$$d_{j}^{i} = {\ell \choose 0} d_{j-\ell}^{i} + {\ell \choose 1} d_{j-\ell}^{i+1} + \dots + {\ell \choose \ell-1} d_{j-\ell}^{i+\ell-1} + {\ell \choose \ell} d_{j-\ell}^{i+\ell} \quad \text{for } j \ge \ell \ge 0, i \ge 0.$$

Lemmas 1a and 1b are extensions of results found in the literature (cf. Hartree [2], p. 38, and Lakshmikantham & Trigiante [3], p. 3).

**Theorem 2:** If the top row of a difference triangle satisfies a  $k^{th}$  order LRHCC, then the left-most column also satisfies some  $k^{th}$  order LRHCC.

**Proof:** The LRHCC of the top row may be written as  $c_k d_{n+k}^0 + c_{k-1} d_{n+k-1}^0 + \cdots + c_1 d_{n+1}^0 + c_0 d_n^0 = 0$  for  $n \ge 0$ , where, in this case,  $c_k = -1$ . By Theorem 1a, we may replace the superscript 0 with any nonnegative integer *i*. Then setting *n* equal to 0, we obtain

$$[c_0, c_1, \dots, c_{k-1}, c_k] \begin{bmatrix} d_0^i \\ d_1^i \\ \vdots \\ d_k^i \end{bmatrix} = 0 \quad \text{for } i \ge 0.$$
 (D)

Now setting  $\ell = j$  in Lemma 1b for  $0 \le j \le k$ , and using matrix notation, we can write the above column vector as

$$\begin{bmatrix} d_0^i \\ d_1^i \\ \vdots \\ d_k^i \end{bmatrix} = \begin{bmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} & 0 & 0 & \cdots & 0 \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \begin{pmatrix} 1 \\ 1 \end{pmatrix} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ k & \vdots & \ddots & & \vdots \\ k & 0 \end{pmatrix} \begin{pmatrix} k \\ 1 \end{pmatrix} & \cdots & \cdots & \begin{pmatrix} k \\ k \end{pmatrix} \end{bmatrix} \begin{bmatrix} d_0^i \\ d_0^{i+1} \\ \vdots \\ d_0^{i+k} \end{bmatrix}$$
 for  $i \ge 0$ . (D')

Substitution of (D') into (D) yields

$$[c_0, c_1, \dots, c_{k-1}, c_k] \begin{bmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} & 0 & 0 & \cdots & 0 \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \begin{pmatrix} 1 \\ 1 \end{pmatrix} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ \begin{pmatrix} k \\ 0 \end{pmatrix} & \begin{pmatrix} k \\ 1 \end{pmatrix} & \cdots & \cdots & \begin{pmatrix} k \\ k \end{pmatrix} \end{bmatrix} \begin{bmatrix} d_0^i \\ d_0^{i+1} \\ \vdots \\ d_0^{i+k} \end{bmatrix} = 0 \quad \text{for } i \geq 0.$$

Multiplying the first two matrices, we obtain  $[b_0, b_1, b_2, ..., b_{k-1}, b_k]$ , where

$$b_j = \sum_{\ell=j}^k {\ell \choose j} c_\ell$$
 for  $j = 0, 1, ..., k$ , (D")

so that the equality

$$b_0 d_0^i + b_1 d_0^{i+1} + \dots + b_k d_0^{i+k} = 0$$

holds for each  $i \ge 0$ . Since the b's do not depend on i, and since  $b_k = -1$ , the left-most column satisfies a  $k^{\text{th}}$ -order LRHCC. Note that, generally, this LRHCC is not the same as for the rows. However, it does have integer coefficients if the recurrence of the top row has integer coefficients.

**Example:** Suppose the top row of the difference triangle is the Pell sequence (see Fig. 2, below).

FIGURE 2. Difference triangle for the Pell sequence satisfying  $P_{n+2} = 2P_{n+1} + P_n$ ,  $P_0 = 0$ ,  $P_1 = 1$ . Minimal polynomial is  $x^2 - 2x - 1$ . Triangle has displacement (2t, 0) with multiplier  $2^t$  for each integer t.

The corresponding recurrence is  $P_{n+2} = 2P_{n+1} + P_n$  for  $n \ge 0$ , so that  $c_2 = -1$ ,  $c_1 = 2$ ,  $c_0 = 1$ . Thus, equation (D") yields  $b_2 = -1$ ,  $b_1 = 0$ ,  $b_0 = 2$ , and the subsequent equality becomes  $d_0^{i+2} - 2d_0^i = 0$ . Hence, the recurrence for the left-most column may be written as  $d_0^{i+2} = 2d_0^i$ . The same recurrence holds for all columns by Theorem 1b or its corollary.

#### 3. POLYNOMIAL OF A SEQUENCE

**Definition:** We say that f(x) is a polynomial of a row (or column) and of the corresponding sequence  $\{a_i\}$  if  $f(x) = c_0 + c_1 x + \dots + c_k x^k$  for some nonnegative integer k and some constants  $c_0, c_1, \dots, c_k$ , and the equality  $c_0 a_n + c_1 a_{n+1} + \dots + c_k a_{n+k} = 0$  holds for all  $n \ge 0$ . Notice that this definition allows f(x) to be the zero polynomial (which is a polynomial of every sequence). Note also that if we express f(x) differently, by adding extra terms with coefficients of zero (thus increasing k), f(x) is still a polynomial of the sequence  $\{a_i\}$ . If  $c_k = 1$ , then we say that f(x) is a characteristic polynomial of the sequence.

**Theorem 3:** If  $\{d_j^i\}$  is a difference triangle, and f(x) is a polynomial of the top row  $d^0$ , then f(x+1) is a polynomial of the left-most column  $d_0$ .

**Proof:** Let 
$$f(x) = c_k x^k + \dots + c_1 x + c_0$$
. Then, by definition,  

$$c_k d_{n+k}^0 + c_{k-1} d_{n+k-1}^0 + \dots + c_0 d_n^0 \text{ for } n \ge 0.$$
(E)

As in the proof of Theorem 2, we obtain

$$b_k d_0^{m+k} + b_{k-1} d_0^{m+k-1} + \dots + b_0 d_0^m = 0$$
 for  $m \ge 0$ ,

where the b's are defined by (D''). Then  $g(x) = b_k x^k + b_{k-1} x^{k-1} + \dots + b_1 x + b_0$  is a polynomial of  $d_0$ . We may write this in vector notation as

$$g(x) = [b_0, b_1, \dots, b_k] \begin{bmatrix} 1 \\ x \\ \vdots \\ x^k \end{bmatrix}.$$

Substituting for the b's, using (D"), we obtain

so that f(x+1) is a polynomial of  $d_0$ . Clearly, if f(x) has integer coefficients, then so does f(x+1).

**Example:** Substitution of x+1 for x in  $x^2-2x-1$ , a characteristic polynomial of the Pell sequence, gives  $x^2-2$  as a characteristic polynomial of the left-most column  $d_0$  of its difference triangle. The corresponding recurrence may be written as  $d_0^{i+2}=2d_0^i$ , which agrees with the result in the example following Theorem 2.

**Lemma 2:** Let f(x) and g(x) be polynomials of a sequence  $\{a_i\}$ , let c be a constant, and let m be a nonnegative integer. Then each of the following is also a polynomial of the sequence  $\{a_i\}$ :

- (a) f(x) + g(x);
- **(b)** cf(x);
- (c)  $x^m f(x)$ .

**Proof:** These statements follow readily from the definition of a polynomial of a sequence.

**Theorem 4:** If f(x) is a polynomial of a sequence  $\{a_i\}$  and g(x) is any polynomial, then f(x)g(x) is a polynomial of  $\{a_i\}$ .

**Proof:** The proof follows from Lemma 2.

**Example:** The Fibonacci sequence defined by  $F_{n+2} = F_{n+1} + F_n$  for  $n \ge 0$ ,  $F_0 = 0$ ,  $F_1 = 1$ , has  $x^2 - x - 1$  as a characteristic polynomial. It has  $(x^2 - x - 1)(x + 1) = x^3 - 2x - 1$  as another characteristic polynomial corresponding to the recurrence  $F_{n+3} = 2F_{n+1} + F_n$ , which this sequence also satisfied.

**Corollary:** Let S be a finite set of sequences, each satisfying some LRHCC (not necessarily the same). Then there exists a recurrence that is satisfied by all the sequences.

**Proof:** Let  $f_1(x)$ ,  $f_2(x)$ , ...,  $f_n(x)$  be polynomials of the n sequences in S, respectively. By repeated use of Theorem 4, their product  $f_1(x)f_2(x)\cdots f_n(x)$  is a polynomial of each of the sequences in S. A recurrence corresponding to this polynomial is satisfied by every sequence in S.

**Example:** Let S consist of the Fibonacci and Pell sequences. Characteristic polynomials for the sequences are  $x^2 - x - 1$  and  $x^2 - 2x - 1$ , respectively. Multiplication of these polynomials yields  $x^4 - 3x^3 + 3x + 1$ . The corresponding recurrence is  $a_{n+4} = 3a_{n+3} - 3a_{n+1} - a_n$ , which is satisfied by both the Fibonacci and the Pell sequences.

**Definition:** A characteristic polynomial of a sequence is called a *minimal polynomial* of the sequence if it is of lowest degree. That a minimal polynomial is unique is a consequence of the next theorem.

**Theorem 5:** A minimal polynomial of a sequence divides every polynomial of the sequence.

**Proof:** Let f(x) be a minimal polynomial of the sequence  $\{a_i\}$  and let g(x) be a polynomial of  $\{a_i\}$ . Then by the division algorithm, g(x) = f(x)q(x) + r(x), where q(x) and r(x) are polynomials, with r(x) having lower degree than f(x), or else  $r(x) \equiv 0$ . By Theorem 4, f(x)q(x) is

446 [NOV.

a polynomial of  $\{a_i\}$  and, by Lemma 2, so is r(x) = g(x) - f(x)q(x). If  $r(x) \neq 0$ , then we can multiply r(x) by a constant to get a monic polynomial. By Lemma 2, this is a polynomial of  $\{a_i\}$ , thereby yielding a characteristic polynomial of degree less than that of f(x), which is a contradiction. Therefore,  $r(x) \equiv 0$ , and hence f(x) divides g(x). Note that, if f(x) and g(x) have integer coefficients, then so does g(x), since g(x) is monic; thus, divisibility of g(x) by g(x) would also hold in  $\mathbf{Z}[x]$ .

#### 4. DISPLACEMENTS

**Definition:** A difference triangle  $\{d_j^i\}$  is said to have a displacement (s, t) with multiplier M if there exist integers s, t and a number M such that the equality

$$d_{n+t}^{m+s} = Md_n^m \tag{F}$$

holds whenever m, n, m+s, and n+t are nonnegative integers. We also say that a sequence has a displacement (s, t) with multiplier M if the difference triangle of which it is the top row has that displacement. If s = t = 0, the displacement is called trivial, otherwise nontrivial.

**Example:** If the Fibonacci sequence is used for the top row, it generates a difference triangle that has displacement (t, t) with multiplier 1 for each integer t (see Fig. 3). The displacements (t, t) may be considered as t multiples of the displacement (1, 1). For an example of a difference triangle whose displacements cannot be expressed as multiples of a single displacement, see Figure 7 at the end of this section.

FIGURE 3. Difference triangle for the Fibonacci sequence satisfying  $F_{n+2} = F_{n+1} + F_n$ ,  $F_0 = 0, F_1 = 1$ . Minimal polynomial is  $x^2 - x - 1$ . Triangle has displacement (t, t) with multiplier 1 for each integer t.

**Theorem 6:** If a difference triangle has a nontrivial displacement, then its top row satisfies some LRHCC.

**Proof:** Let the difference triangle be  $\{d_j^i\}$ . First, assume that it has a displacement  $(s, t) \neq (0, 0)$  with  $s \geq 0$  and with multiplier M. Then we can use the definition of displacement and Lemma 1a to obtain

$$Md_n^0 = d_{n+t}^s = \sum_{\ell=0}^s (-1)^{\ell} \binom{s}{\ell} d_{n+\ell+s-\ell}^0 \quad \text{for } n \ge \max(0, -t).$$
 (G)

Subtracting  $Md_n^0$  from the left and right sides of the equation, and then replacing n with  $n+\max(0,-t)$ , we get an equation of the form (E) in Theorem 3 for some constants  $c_k, ..., c_1, c_0$ , where  $k = \max(t+s, s, -t)$ . Moreover, the c's are not all 0 except when s = t = 0 (and M = 1), which is the trivial displacement. Hence, we can write the last equation in the form of some LRHCC which  $d^0$  satisfies.

As a second case, let s < 0 and  $M \ne 0$ . Then we can write (F) in the definition of displacement as

$$d_{n'-t}^{m'-s} = \frac{1}{M} d_{n'}^{m'} \quad \text{for } m', n', m'-s, n'-t \ge 0$$

by substituting m'-s for m and n'-t for n. Thus,  $\{d_j^i\}$  also has a displacement (-s, -t) with multiplier 1/M, and since -s > 0, we can use the first case of this proof.

As a final case, suppose that s < 0 and M = 0. In (F) let m = -s and replace n with n - t, to get the equality  $d_n^0 = M d_{n-t}^{-s} = 0$ , which is valid for all  $n \ge \max(0, t)$ , so that  $d_n^0 = 0$  for each  $n \ge \max(0, t)$ . Hence,  $d^0$  satisfies any LRHCC of order  $\max(0, t)$  or greater with all coefficients zero.

**Example:** The Pell sequence (Fig. 2) has a displacement (2, 0) with multiplier 2. Hence, (G) becomes

$$2d_n^0 = \sum_{\ell=0}^2 (-1)^{\ell} \binom{2}{\ell} d_{n+2-\ell}^0 = d_{n+2}^0 - 2d_{n+1}^0 + d_n^0 \quad \text{for } n \ge 0$$
or
$$d_{n+2}^0 = 2d_{n+1}^0 + d_n^0 \quad \text{for } n \ge 0.$$

**Example:** The Tribonacci sequence (Fig. 4) has a displacement (3, 2) with multiplier 2. Thus, (G) becomes

$$2d_n^0 = \sum_{\ell=0}^3 (-1)^{\ell} {3 \choose \ell} d_{n+5-\ell}^0 = d_{n+5}^0 - 3d_{n+4}^0 + 3d_{n+3}^0 - d_{n+2}^0 \quad \text{for } n \ge 0$$
or
$$d_{n+5}^0 = 3d_{n+4}^0 - 3d_{n+3}^0 + d_{n+2}^0 + 2d_n^0 \quad \text{for } n \ge 0.$$

In this case, (G) does not give the lowest-order recurrence that the top row satisfies. The corresponding polynomial of  $d^0$ , namely,  $x^5 - 3x^4 + 3x^3 - x^2 - 2$ , is not the minimal polynomial, but has as a factor  $x^3 - x^2 - x - 1$ , which is the minimal polynomial. The other factor,  $x^2 - 2x + 2$ , corresponds to the recurrence  $d_{n+2}^0 = 2d_{n+1}^0 - 2d_n^0$ . Any difference triangle whose top row satisfies the latter will also have a displacement (3, 2) with multiplier 2.

**Theorem 7:** Let  $\{d_j^i\}$  be a difference triangle with displacement (s, t). Let f(x) be the minimal polynomial of  $d^0$ . Then, for any two roots  $\alpha$  and  $\beta$  of f(x) = 0,

$$(\alpha - 1)^s \alpha^t = (\beta - 1)^s \beta^t \tag{H}$$

where  $0^0$  is defined to be 1.

448

FIGURE 4. Difference triangle for a sequence satisfying  $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ ,  $T_0 = T_1 = 0$ ,  $T_2 = 1$ . Minimal polynomial is  $x^3 - x^2 - x - 1$ . Triangle has displacement (3t, 2t) with multiplier  $2^t$  for each integer t. Characteristic polynomial is  $x^2(x-1)^3 - 2 = x^5 - 3x^4 + 3x^3 - x^2 - 2$  which is divisible by the minimal polynomial  $x^3 - x^2 - x - 1$ .

**Proof:** Let M be the multiplier of the displacement. First, consider  $s, t \ge 0$ . Then (G) can be used to obtain a polynomial g(x) of  $d^0$ :

$$g(x) = \sum_{\ell=0}^{s} (-1)^{\ell} {s \choose \ell} x^{t+s-\ell} - M = x^{t} (x-1)^{s} - M.$$

By Theorem 4, the minimal polynomial f(x) divides g(x), so that any  $\alpha$ ,  $\beta$  that are zeros of the minimal polynomial f(x) are also zeros of g(x) and, therefore, (H) holds with both sides equal to M. For other cases of s and t, we obtain:

$$g(x) = (x-1)^{s} - Mx^{-t} \quad \text{when } s \ge 0, t < 0;$$

$$g(x) = (x-1)^{-s}x^{-t} - \frac{1}{M} \quad \text{when } s, t < 0, M \ne 0;$$

$$g(x) = (x-1)^{-s} - \frac{1}{M}x^{t} \quad \text{when } s < 0, t \ge 0, M \ne 0.$$

It can be verified that all these cases give rise to (H). Note that (H) is always defined because g(x) = 0 cannot have a root of 0 when t < 0 or a root of 1 when s < 0.

If M = 0 and s < 0, then, as in the last part of the proof of Theorem 6,  $d^0$  contains only a finite number of nonzero terms, and we can derive that  $g(x) = x^{\max(0, t)}$ . It follows that the minimal polynomial f(x) for  $d^0$  is a power of x and that the roots of f(x) = 0 are all 0, so that (H) holds. Theorem 7 is thus true in every case.

Theorem 7 shows that if a sequence with minimal polynomial f(x) has a displacement (s, t), then (H) holds. If f(x) has multiple roots, then the converse need not hold. For example, if  $f(x) = (x-2)^3$ , then (H) is trivially satisfied for any (s, t), but it can be shown that the corresponding sequence has only the trivial displacement. Theorems 8 and 9 give partial converses of Theorem 7.

**Theorem 8:** Let  $\{d_j^i\}$  be a difference triangle with  $d^0$  satisfying some LRHCC, and let f(x) be the minimal polynomial of  $d^0$ . If f(x) divides g(x) of Theorem 7 for some s, t, and M, then  $\{d_j^i\}$  has a displacement (s,t) with multiplier M.

**Proof:** From Theorem 4, g(x) is a polynomial of  $\{d^0\}$ . Consider the case where  $s, t \ge 0$ . By the definition of polynomial of a sequence, the left and right sides of (G) are equal. Hence, (F) follows, so that  $\{d^i_j\}$  has the displacement claimed. Similar reasoning holds for other cases of s and t.

**Theorem 9:** Let  $\{d_j^i\}$  be a difference triangle with  $d^0$  satisfying some LRHCC, and let f(x) be the minimal polynomial of  $d^0$ . Suppose that f(x) = 0 has no multiple roots. Then  $\{d_j^i\}$  has a displacement (s, t) if (H) holds for every pair of roots  $\alpha$  and  $\beta$  of f(x) = 0.

**Proof:** By (H),  $(\alpha - 1)^s \alpha^t$  has the same value for any  $\alpha$  that is a root of f(x) = 0. Call this value M and substitute it in g(x) as defined in Theorem 7. Every root of f(x) = 0 is a root of g(x) = 0. Since f(x) = 0 has no multiple roots, f(x) must divide g(x), so that the result follows by an application of Theorem 8.

Theorems 7-9 can be useful in determining what displacements a sequence has. Some examples follow.

**Example A:** A sequence satisfies  $a_{n+2} = a_{n+1} + ca_n$ ,  $c \ge 0$ ,  $a_0 = 0$ ,  $a_1 \ne 0$ . The minimal polynomial,  $x^2 - x - c$ , has two zeros:

$$\alpha = \frac{1 + \sqrt{4c + 1}}{2} \quad \text{and} \quad \beta = \frac{1 - \sqrt{4c + 1}}{2}.$$

Substitution of these values into (H) leads to

$$\left(\frac{1+\sqrt{4c+1}}{2}\right)^{t} \left(\frac{-1+\sqrt{4c+1}}{2}\right)^{s} = \left(\frac{1-\sqrt{4c+1}}{2}\right)^{t} \left(\frac{-1-\sqrt{4c+1}}{2}\right)^{s}$$

to be solved for integers s and t. Multiplying both sides by  $2^{s+t}(-1)^s$ , we obtain

$$(1+\sqrt{4c+1})^t(1-\sqrt{4c+1})^s=(1-\sqrt{4c+1})^t(1+\sqrt{4c+1})^s$$
.

The only solutions to this equation occur when s = t. Thus, the only nontrivial displacements for a sequence satisfying the given recurrence conditions are (t, t); e.g., (1, 1) is a displacement for the Fibonacci sequence when c = 1 and  $a_1 = 1$ .

**Example B:** A sequence satisfies  $a_{n+2} = ca_{n+1} + a_n$ , where c > 2,  $a_0 = 0$ ,  $a_1 \neq 0$ . The minimal polynomial  $x^2 - cx - 1$  has zeros  $\frac{c}{2} \pm \frac{\sqrt{c^2 + 4}}{2}$ , so that (H) becomes

$$\left(\frac{c+\sqrt{c^2+4}}{2}\right)^t \left(\frac{c-2+\sqrt{c^2+4}}{2}\right)^s = \left(\frac{c-\sqrt{c^2+4}}{2}\right)^t \left(\frac{c-2-\sqrt{c^2+4}}{2}\right)^s.$$

Multiplying both sides by  $2^{s+t}$ , and rearranging terms, we get

450

$$\left(\frac{c+\sqrt{c^2+4}}{c-\sqrt{c^2+4}}\right)^t = \left(\frac{c-2-\sqrt{c^2+4}}{c-2+\sqrt{c^2+4}}\right)^s.$$

Since c > 2, c - 2 > 0, and  $c^2 + 4 > 0$ , we find that

$$\left| \frac{c + \sqrt{c^2 + 4}}{c - \sqrt{c^2 + 4}} \right| > 1$$
 and  $\left| \frac{c - 2 - \sqrt{c^2 + 4}}{c - 2 + \sqrt{c^2 + 4}} \right| < 1$ .

Given these inequalities, the only way that the above equality can hold if  $s, t \ge 0$  (or  $s, t \le 0$ ) is that s = t = 0. Hence, a sequence satisfying such a recurrence has only the nontrivial displacement when s and t are both nonnegative or both nonpositive.

**Example C:** The "Mersenne sequence" (Robbins [4], p. 194), given by the formula  $M_n = 2^n - 1$ , satisfies the recurrence  $M_{n+2} = 3M_{n+1} - 2M_n$ ,  $M_0 = 0$ ,  $M_1 = 1$ . The minimal polynomial,  $x^2 - 3x + 2$ , has  $\alpha = 1$  and  $\beta = 2$  as zeros. Using these values in (H), we obtain

$$(0)^{s}(1)^{t} = (1)^{s}(2)^{t},$$

which cannot hold if  $s \neq 0$ , since that would yield  $0 = 2^t$ . If s = 0, then  $1 = 2^t$ , which indicates that t = 0 as well. This shows that the "Mersenne sequence" has only the trivial displacement.

Further examples of difference triangles and their displacements are considered in Figures 5, 6, and 7. Figure 5 shows a difference triangle for a sequence satisfying  $a_i = -na_{i-1}$  with  $a_0 = 1$ . The minimal polynomial is x + n = 0. The difference triangle has displacement (s, t) with multiplier  $(-1)^{s+t}(n+1)^s n^t$  for all integers s and t. Figure 6 shows a difference triangle generated by a sequence  $\{a_i\}$  satisfying  $a_{n+2} = 4a_{n+1} - 2a_n$  with  $a_0 = 0$  and  $a_1 = 1$ . The minimal polynomial is  $x^2 - 4x + 2$ . The difference triangle has displacement (2t, -2t) with multiplier  $2^t$  for each integer t. Figure 7 shows a difference triangle generated by a sequence  $\{a_i\}$  satisfying  $a_{n+2} = 2a_{n+1} - 2a_n$  with  $a_0 = 0$  and  $a_1 = 1$ . The minimal polynomial is  $x^2 - 2x + 2$ . Two displacements are (0, 4) with multiplier -4 and (1, 2) with multiplier -2. They are independent in the sense that a difference triangle has independent displacements (s, t) and (s', t') if  $st' \neq ts'$ . The authors are investigating conditions under which a difference triangle has independent displacements.

FIGURE 5. Difference triangle for a sequence satisfying  $a_i = -na_{i-1}$  with  $a_0 = 1$ . Minimal polynomial is x + n. Triangle has displacement (s, t) with multiplier  $(-1)^{s+t}(n+1)^s n^t$  for all integers s and t.

FIGURE 6. Difference triangle generated by the sequence  $\{a_i\}$  satisfying  $a_{n+2} = 4a_{n+1} - 2a_n$  with  $a_0 = 0$  and  $a_1 = 1$ . Minimal polynomial is  $x^2 - 4x + 2$ . Triangle has displacement (2t, -2t) with multiplier  $2^t$  for each integer t.

FIGURE 7. Difference triangle generated by the sequence  $\{a_i\}$  satisfying  $a_{n+2} = 2a_{n+1} - 2a_n$  with  $a_0 = 0$  and  $a_1 = 1$ . Minimal polynomial is  $x^2 - 2x + 2$ . Two independent displacements are (0, 4) with multiplier -4 and (1, 2) with multiplier -2.

# **ACKNOWLEDGMENTS**

We thank Nancy Comerato, secretary in the Department of Mathematical Sciences of Rensselaer Polytechnic Institute, for typesetting the manuscript and Jo Ann Vine of the Fibonacci Association for preparing it for publication.

#### REFERENCES

- 1. P. Filipponi. Problem B-733. The Fibonacci Quarterly 31.1 (1993):83.
- 2. D. R. Hartree. Numerical Analysis. London: Oxford University Press, 1958.
- 3. V. Lakshmikantham & D. Trigiante. *Theory of Difference Equations: Numerical Methods and Applications*. New York: Academic Press, 1988.
- 4. N. Robbins. Beginning Number Theory. Dubuque, Iowa: W. C. Brown, 1993.

AMS Classification Numbers: 11B37, 11B39, 39A10



# DIFFERENTIAL PROPERTIES OF A GENERAL CLASS OF POLYNOMIALS

## Richard André-Jeannin

IUT GEA, Route de Romain, 54400 Longwy, France (Submitted April 1994)

#### 1. INTRODUCTION

Let us consider the generalized Fibonacci polynomials  $U_n(p,q;x)$  and the generalized Lucas polynomials  $V_n(p,q;x)$  (or simply  $U_n$  and  $V_n$  if there is no danger of confusion) defined by

$$U_n = (x+p)U_{n-1} - qU_{n-2} \quad (U_0 = 0, U_1 = 1), \tag{1.1}$$

and

$$V_n = (x+p)V_{n-1} - qV_{n-2} \quad (V_0 = 2, V_1 = x+p). \tag{1.2}$$

The parameters p and q as well as the variable x are arbitrary real numbers and we denote by  $\alpha=\alpha(x)$  and  $\beta=\beta(x)$  the numbers such that  $\alpha+\beta=x+p$  and  $\alpha\beta=q$ . The polynomials  $U_n$  and  $V_n$  can be expressed by means of the Binet forms

$$U_n = \frac{\alpha^n - \beta^n}{\Delta^{1/2}}, \quad \text{for } \Delta \neq 0,$$
 (1.3)

and

$$V_n = \alpha^n + \beta^n, \tag{1.4}$$

where

$$\Delta = \Delta(x) = (x+p)^2 - 4q. \tag{1.5}$$

Recall that

$$\alpha = ((x+p) + \Delta^{1/2})/2, \quad \beta = ((x+p) - \Delta^{1/2})/2. \tag{1.6}$$

Notice that  $\Delta > 0$  for every x if q < 0 for all x sufficiently large if  $q \ge 0$ .

Particular cases of  $U_n(p,q;x)$  and  $V_n(p,q;x)$  are the Fibonacci and Lucas polynomials  $(F_n(x))$  and  $L_n(x)$ , the Pell and Pell-Lucas polynomials [6]  $(P_n(x))$  and  $Q_n(x)$ , the first and the second Fermat polynomials [7]  $(\Phi_n(x))$  and  $(\Phi_n(x))$ , the Morgan-Voyce polynomials [1, 2, 5, 8, 9, 10]  $(B_n(x))$  and  $(B_n(x))$  and the Chebyschev polynomials  $(S_n(x))$  and  $(S_n(x))$  given by

$$U_{n}(0,-1;x) = F_{n}(x), V_{n}(0,-1;x) = L_{n}(x)$$

$$U_{n}(0,-1;2x) = P_{n}(x), V_{n}(0,-1;2x) = Q_{n}(x)$$

$$U_{n}(0,2;x) = \Phi_{n}(x), V_{n}(0,2;x) = \Theta_{n}(x)$$

$$U_{n+1}(2,1;x) = B_{n}(x), V_{n}(2,1;x) = C_{n}(x)$$

$$U_{n}(0,1;2x) = S_{n}(x), V_{n}(0,1;2x) = 2T_{n}(x).$$
(1.7)

In earlier papers [1, 2] the author has discussed the combinatorial properties of the coefficients of  $U_n$  and  $V_n$ . Here, we shall investigate the differential properties satisfied by these polynomials, such as differential equations and Rodrigues' formulas.

Let us define the sequence  $\{c_{n,k}\}_{n\geq k\geq 0}$  by

$$c_{n,0} = 2 \frac{n!}{(2n)!}, \quad n \ge 0,$$
 (1.8)

and

$$c_{n,k} = 2 \frac{n!}{(2n)!} \frac{n}{n+k} \frac{(n+k)!}{(n-k)!}, \quad n \ge k \ge 1.$$
 (1.9)

Notice that

$$c_{n,k+1} = (n^2 - k^2)c_{n,k}, \quad n \ge k+1 \ge 1.$$
 (1.10)

Our main results are the following theorems.

**Theorem 1:** For every real number x, the polynomial

$$U_n^{(k-1)} = \frac{d^{k-1}}{dx^{k-1}} U_n, \quad k \ge 1,$$

and the polynomial

$$V_n^{(k)} = \frac{d^k}{dr^k} V_n, \quad k \ge 0,$$

satisfy the differential equation  $E_{n,k}$ :

$$\Delta z'' + (2k+1)(x+p)z' + (k^2 - n^2)z = 0. \tag{1.11}$$

**Theorem 2:** For every x such that  $\Delta > 0$ , we have

$$U_n = nc_{n,0} \Delta^{-1/2} \frac{d^{n-1}}{dx^{n-1}} \Delta^{n-1/2}, \quad n \ge 1,$$
(1.12)

and

$$V_n = c_{n,0} \Delta^{1/2} \frac{d^n}{dx^n} \Delta^{n-1/2}, \quad n \ge 0,$$
 (1.13)

where  $c_{n,0}$  is defined by (1.8).

More generally, we also have Rodrigues' formulas for  $U_n^{(k)}$  and  $V_n^{(k)}$ , namely,

**Theorem 3:** For every x such that  $\Delta > 0$  and every  $k \ge 0$ , we have

$$U_n^{(k)} = \frac{(n^2 - k^2)}{n} c_{n,k} \Delta^{-k-1/2} \frac{d^{n-k-1}}{dv^{n-k-1}} \Delta^{n-1/2}, \quad n \ge k+1,$$
 (1.14)

and

$$V_n^{(k)} = c_{n,k} \Delta^{-k+1/2} \frac{d^{n-k}}{dx^{n-k}} \Delta^{n-1/2}, \quad n \ge k,$$
(1.15)

where  $c_{n,k}$  is defined by (1.9).

Notice that Theorem 3 reduces to Theorem 2 for k = 0 and that (1.14) can be written, by (1.10),

$$U_n^{(k)} = \frac{c_{n,k+1}}{n} \Delta^{-k-1/2} \frac{d^{n-k-1}}{dx^{n-k-1}} \Delta^{n-1/2}, \quad n \ge k.$$
 (1.16)

454 [NOV.

#### 2. PROOF OF THEOREM 1

It is readily proven [3, 4] by (1.5) and (1.6) that, for every x such that  $\Delta > 0$ ,

$$\begin{cases} \alpha' = \alpha \Delta^{-1/2}, \\ \beta' = -\beta \Delta^{-1/2}, \end{cases}$$
 (2.1)

and thus that

$$\begin{cases} (\alpha^n)' = n\alpha^n \Delta^{-1/2}, \\ (\beta^n)' = -n\beta^n \Delta^{-1/2}. \end{cases}$$
 (2.2)

By this, (1.3), and (1.4), we see [3, 4] that

$$V_n' = nU_n \tag{2.3}$$

and therefore that

$$V_n^{(k)} = nU_n^{(k-1)}, \quad k \ge 1. \tag{2.4}$$

Notice that these identities are valid for every value of x, and not only when  $\Delta > 0$ , since the two members are polynomials. By (2.2), we also deduce that  $\alpha^n$  and  $\beta^n$ , whence  $V_n = \alpha^n + \beta^n$  satisfies the differential equation

$$\frac{d}{dx}(\Delta^{1/2}y') = n^2 \Delta^{-1/2}y, \quad \text{for } \Delta > 0,$$
(2.5)

which is equivalent, for  $\Delta > 0$ , to the equation  $E_{n,0}$  [see (1.11)], namely,

$$\Delta y'' + (x+p)y' - n^2 y = 0. \tag{2.6}$$

Notice that  $V_n$  satisfies  $E_{n,0}$  for every value of x, since, in that case, the first member of (2.6) is a polynomial.

Differentiating (2.6) k times and using Leibniz' rule, we see that  $z=y^{(k)}$  satisfies the differential equation  $E_{n,k}$  (1.11). Hence,  $E_{n,k}$  is satisfied by  $V_n^{(k)}$ ,  $k \ge 0$ , and  $U_n^{(k-1)} = \frac{1}{n}V_n^{(k)}$ ,  $k \ge 1$ . This concludes the proof.

For instance, the Morgan-Voyce polynomial  $B_n(x) = U_{n+1}(2,1;x)$  satisfies the differential equation  $E_{n+1,1}$ 

$$x(x+4)z''+3(x+2)z'-n(n+2)z=0$$
.

This result was first noticed by Swamy [10].

**Remark:** When  $\Delta > 0$ , it is easy to verify that  $E_{n,k}$  can be written as

$$\frac{d}{dx}[\Delta^{k+1/2}z'] = (n^2 - k^2)\Delta^{k-1/2}z,$$
(2.7)

which is a generalization of (2.5).

We now give another (nonpolynomial) solution of  $E_{n,k}$ .

**Proposition 1:** Let n and k be two integers such that  $n+k-1 \ge 0$ . Then, for  $\Delta > 0$ , the function  $\frac{d^{n+k-1}}{dx^{n+k-1}} \Delta^{n-1/2}$  is a solution of  $E_{n,k}$ .

1995] 455

**Proof:** It is easy to verify that, for  $\Delta > 0$ ,  $\Delta^{n-1/2}$  is a solution of the differential equation

$$\Delta y'' - (2n-3)(x+p)y' - (2n-1)y = 0. \tag{2.8}$$

Differentiating (2.8) (n+k-1) times and putting  $z=y^{(n+k-1)}$ , we obtain

$$\Delta z'' + 2\binom{n+k-1}{1}(x+p)z' + 2\binom{n+k-1}{2}z - (2n-3)\left[(x+p)z' + \binom{n+k-1}{1}z\right] - (2n-1)z = 0.$$

After some rearrangement, one can see that this equation is identical to  $E_{n,k}$ .

**Remark:** Using the formulation (2.7) of  $E_{n,k}$  and putting  $z = \frac{d^{n+k-1}}{dx^{n+k-1}} \Delta^{n-1/2}$ , one can write

$$\frac{d}{dx} \left[ \Delta^{k+1/2} \frac{d^{n+k}}{dx^{n+k}} \Delta^{n-1/2} \right] = (n^2 - k^2) \Delta^{k-1/2} \frac{d^{n+k-1}}{dx^{n+k-1}} \Delta^{n-1/2}. \tag{2.9}$$

Changing k to (-k-1) in (2.9), where  $n-k \ge 2$ , we obtain a formula that we shall need later:

$$\frac{d}{dx} \left[ \Delta^{-k-1/2} \frac{d^{n-k-1}}{dx^{n-k-1}} \Delta^{n-1/2} \right] = (n^2 - (k+1)^2) \Delta^{-k-3/2} \frac{d^{n-k-2}}{dx^{n-k-2}} \Delta^{n-1/2}.$$
 (2.10)

In particular, changing n to (n+1), and putting k = -1, we get

$$\frac{d}{dx} \left[ \Delta^{1/2} \frac{d^{n+1}}{dx^{n+1}} \Delta^{n+1/2} \right] = (n+1)^2 \Delta^{-1/2} \frac{d^n}{dx^n} \Delta^{n+1/2}, \quad n \ge 0.$$
 (2.11)

#### 3. PROOF OF THEOREM 2

In the proof of Theorem 2, we shall need the following well-known and readily proven result:

$$V_{n+1} = \frac{1}{2} [(x+p)V_n + \Delta U_n]. \tag{3.1}$$

By (1.8), formula (1.12) (resp. (1.13)) is clear if n = 1 (resp. n = 0 or n = 1). Supposing that (1.12) and (1.13) are true for  $n \ge 1$ , we get by (3.1) that

$$V_{n+1} = \frac{n!}{(2n!)} \Delta^{1/2} \left[ (x+p) \frac{d^n}{dx^n} \Delta^{n-1/2} + n \frac{d^{n-1}}{dx^{n-1}} \Delta^{n-1/2} \right].$$
 (3.2)

On the other hand, one can notice by (1.5) that

$$\frac{d^{n+1}}{dx^{n+1}} \Delta^{n+1/2} = \frac{d^n}{dx^n} \Big[ (2n+1)(x+p) \Delta^{n-1/2} \Big] 
= (2n+1) \Big[ (x+p) \frac{d^n}{dx^n} \Delta^{n-1/2} + n \frac{d^{n-1}}{dx^{n-1}} \Delta^{n-1/2} \Big].$$
(3.3)

From (3.2) and (3.3), we see that

$$V_{n+1} = \frac{n!}{(2n!)} \Delta^{1/2} \frac{1}{2n+1} \frac{d^{n+1}}{dx^{n+1}} \Delta^{n+1/2} = 2 \frac{(n+1)!}{(2n+2)!} \Delta^{1/2} \frac{d^{n+1}}{dx^{n+1}} \Delta^{n+1/2}, \tag{3.4}$$

which is the needed formula for  $V_{n+1}$ 

Now we see, by (2.3) and (3.4), that

$$U_{n+1} = \frac{1}{n+1} V'_{n+1} = 2 \frac{n!}{(2n+2)!} \frac{d}{dx} \left[ \Delta^{1/2} \frac{d^{n+1}}{dx^{n+1}} \Delta^{n+1/2} \right]$$

$$= 2 \frac{n!}{(2n+2)!} (n+1)^2 \Delta^{-1/2} \frac{d^n}{dx^n} \Delta^{n+1/2}, \text{ by (2.11)},$$

$$= 2(n+1) \frac{(n+1)!}{(2n+2)!} \Delta^{-1/2} \frac{d^n}{dx^n} \Delta^{n+1/2}.$$
(3.5)

This completes the proof of Theorem 2.

#### 4. PROOF OF THEOREM 3

We proceed by induction on k. By Theorem 2, statement (1.14) clearly holds for k = 0 and every  $n \ge 1$ . Supposing that (1.14) holds for  $k \ge 0$  and every  $n \ge k + 1$  we get, by (1.16),

$$U_n^{(k+1)} = \frac{d}{dx} U_n^{(k)} = \frac{c_{n,k+1}}{n} \frac{d}{dx} \left[ \Delta^{-k-1/2} \frac{d^{n-k-1}}{dx^{n-k-1}} \Delta^{n-1/2} \right],$$

and, by (2.10), we have at once that

$$U_n^{(k+1)} = \frac{c_{n, k+1}}{n} \left[ n^2 - (k+1)^2 \right] \Delta^{-k-3/2} \frac{d^{n-k-2}}{dx^{n-k-2}} \Delta^{n-1/2}, \quad n \ge k+2,$$

which is the needed formula for  $U_n^{(k+1)}$ 

On the other hand, statement (1.15) holds for k = 0, by Theorem 2. When  $k \ge 1$  we get, by (2.4) and (1.14) that

$$V_n^{(k)} = nU_n^{(k-1)} = c_{n,k} \Delta^{-k+1/2} \frac{d^{n-k}}{dx^{n-k}} \Delta^{n-1/2}, \quad n \ge k.$$

This completes the proof of Theorem 3.

# REFERENCES

- 1. R. André-Jeannin. "A Note on a General Class of Polynomials." *The Fibonacci Quarterly* **32.5** (1994):445-54.
- 2. R. André-Jeannin. "A Note on a General Class of Polynomials, Part II." *The Fibonacci Quarterly* **33.4** (1995):341-51.
- 3. P. Filipponi & A. F. Horadam. "Derivative Sequences of Fibonacci and Lucas Polynomials." In *Applications of Fibonacci Numbers* **4:**99-108. Ed. G. E. Bergum, A. N. Philippou, & A. F. Horadam. Dordrecht: Kluwer, 1991.
- 4. P. Filipponi & A. F. Horadam. "Second Derivative Sequences of Fibonacci and Lucas Polynomials." *The Fibonacci Quarterly* **31.3** (1993):194-204.
- 5. G. Ferri, M. Faccio, & A. D'Amico. "The DFF and DFFz Triangles and Their Mathematical Properties." In *Applications of Fibonacci Numbers* 5. Ed. A. N. Philippou, G. E. Bergum, & A. F. Horadam. Dordrecht: Kluwer, 1994.
- 6. A. F. Horadam & Br. J. M. Mahon. "Pell and Pell-Lucas Polynomials." *The Fibonacci Quarterly* 23.1 (1985):7-20.

1995] 457

- 7. A. F. Horadam. "Chebyschev and Fermat Polynomials for Diagonal Functions." *The Fibonacci Quarterly* **19.4** (1979):328-33.
- 8. J. Lahr. "Fibonacci and Lucas Numbers and the Morgan-Voyce Polynomials in Ladder Networks and in Electrical Line Theory." In *Applications of Fibonacci Numbers* (AU? Please check Volume No.), pp. 141-61. Ed. A. N. Philippou, G. E. Bergum, & A. F. Horadam. Dordrecht: Kluwer, 1986.
- 9. M. N. S. Swamy. "Properties of the Polynomials Defined by Morgan-Voyce." *The Fibonacci Quarterly* **4.1** (1966):73-81.
- 10. M. N. S. Swamy. "Further Properties of Morgan-Voyce Polynomials." *The Fibonacci Quarterly* **6.2** (1968):167-75.

AMS Classification Numbers: 11B39, 26A24, 11B83



# Author and Title Index

The AUTHOR, TITLE, KEY-WORD, ELEMENTARY PROBLEMS, and ADVANCED PROBLEMS indices for the first 30 volumes of *The Fibonacci Quarterly* have been completed by Dr. Charles K. Cook. Publication of the completed indices is on a 3.5-inch, high density disk. The price for a copyrighted version of the disk will be \$40.00 plus postage for non-subscribers, while subscribers to *The Fibonacci Quarterly* need only pay \$20.00 plus postage. For additional information, or to order a disk copy of the indices, write to:

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

The indices have been compiled using WORDPERFECT. Should you wish to order a copy of the indices for another wordprocessor or for a non-compatible IBM machine, please explain your situation to Dr. Cook when you place your order and he will try to accommodate you. DO NOT SEND PAYMENT WITH YOUR ORDER. You will be billed for the indices and postage by Dr. Cook when he sends you the disk. A star is used in the indices to indicate unsolved problems. Furthermore, Dr. Cook is working on a SUBJECT index and will also be classifying all articles by use of the AMS Classification Scheme. Those who purchase the indices will be given one free update of all indices when the SUBJECT index and the AMS Classification of all articles published in *The Fibonacci Quarterly* are completed.

458

# POLYNOMIAL DIVISIBILITY IN FINITE FIELDS, AND RECURRING SEQUENCES

# Odoardo Brugia and Piero Filipponi

Fondazione Ugo Bordoni, Via B. Castiglione 59, I-00142 Rome, Italy (Submitted May 1994)

#### 1. INTRODUCTION AND PRELIMINARIES

The theory of polynomials the coefficients of which belong to finite fields (e.g., see [4]) is a valid mathematical tool to face various problems arising in telecommunication engineering. For example, it plays a crucial role in the design of scramblers and descramblers, multilevel codecoders, linear shift-registers, etc., and in the analysis of their performances (e.g., see [1], [5]). It is sometimes necessary to fix our attention on special classes of these polynomials, such as *irreducible* and *primitive* polynomials [4], [5]. For example, for the sequence generated by a linear feedback shift register to be of maximal length, the characteristic polynomial of the register must be primitive [1], [2].

To seek irreducible polynomials or to factor reducible ones, it is useful to have at disposal criteria for the divisibility over the finite field GF(q) (q a prime or a power of a prime) of a polynomial f(x) by a polynomial g(x) of degree less than that of f(x). Some criteria for the divisibility over GF(2) are well known. As a minor instance, we have that: (i) if the coefficient of the zero-degree term of f(x) vanishes, then this polynomial is divisible by its term of lower degree; (ii) if the number of the nonzero coefficients is even, then f(x) is divisible by x+1.

Following the notation of Lidl [4], let  $f(x) \in GF(q)[x]$  and  $g(x) \in GF(q)[x]$  be two polynomials of arbitrary degree n and m (m < n), respectively,

$$f(x) = \sum_{k=0}^{n} a_k x^k, \ a_k \in GF(q), \ a_n \neq 0 \ (\text{mod } q),$$
 (1.1)

$$g(x) = x^m - \sum_{k=0}^{m-1} b_k x^k, \ m < n, \ b_k \ GF(q).$$
 (1.2)

The polynomial f(x) is divisible in GF(q) by g(x) if the remainder of f(x): g(x) is congruent to zero modulo q. In Section 2, criteria for this divisibility are established which involve the use of certain  $m^{th}$ -order recurring sequences. The ubiquitous Fibonacci numbers make their appearance in the case m = q = 2. In Section 3, three special cases are analyzed, the last of which turns out to be a useful tool for ascertaining the irreducibility or the primitivity of certain classes of polynomials.

Throughout this paper, all relations and algebraic manipulations are meant to be performed modulo q. This fact will be indicated explicitly only in the final results.

#### 2. THE MAIN RESULT

The (provisional) remainder  $f_i(x)$  obtained at the  $i^{th}$  step  $(0 \le i \le n - m + 1)$  of the long division f(x): g(x) has the form

$$f_i(x) = \sum_{j=0}^{n-i} r_j^{(i)} x^{n-i-j}, r_j^{(i)} \in GF(q).$$
 (2.1)

Obviously, the *actual* remainder of this division is  $f_{n-m+1}(x)$ . Moreover, we assume that  $f_0(x) = f(x)$ , which implies

$$r_i^{(0)} = a_{n-i} \ (j = 0, 1, ..., n).$$
 (2.2)

Since the term of  $(n-i-m)^{th}$ -degree of the quotient is given by  $r_0^{(i)}x^{n-i-m}$ , using the long division algorithm gives the  $(i+1)^{th}$  provisional remainder

$$f_{i+1}(x) = f_i(x) - r_0^{(i)} x^{n-i-m} g(x) = \sum_{j=0}^{n-i-1} \left( r_{j+1}^{(i)} + b_{m-j-1} r_0^{(i)} \right) x^{n-i-j-1}, \tag{2.3}$$

whereas, by definition (2.1), we can write

$$f_{i+1}(x) = \sum_{j=0}^{n-i-1} r_j^{(i+1)} x^{n-i-j-1}.$$
 (2.4)

By identifying the terms of the same degree in (2.3) and (2.4), the following system of n-i difference equations can be written

$$r_{j}^{(i+1)} = \begin{cases} r_{j+1}^{(i)} + b_{m-j-1} r_{0}^{(i)} & (0 \le j \le m-1), \\ r_{j+1}^{(i)} & (m \le j \le n-i-1), \end{cases}$$
(2.5)

the initial conditions of which are given by (2.2).

By (2.2), the second equation of (2.5) produces

$$r_{j}^{(1)} = r_{j+1}^{(0)} = a_{n-j-1},$$

$$r_{j}^{(2)} = r_{j+1}^{(1)} = r_{j+2}^{(0)} = a_{n-j-2},$$

$$r_{j}^{(3)} = r_{j+1}^{(2)} = r_{j+2}^{(1)} = r_{j+3}^{(0)} = a_{n-j-3},$$

$$...$$

$$r_{j}^{(i)} = r_{j+1}^{(i-1)} = \cdots = a_{n-j-i} \quad (m \le j \le n-i-1),$$

$$(2.6)$$

whence, as a special case,

$$r_m^{(i)} = a_{n-m-i}. (2.6')$$

The first equation of (2.5) produces the equations

$$\begin{split} r_{j}^{(i)} &= r_{j+1}^{(i-1)} + b_{m-j-1} r_{0}^{(i-1)}, \\ r_{j+1}^{(i-1)} &= r_{j+2}^{(i-2)} + b_{m-j-2} r_{0}^{(i-2)} \\ & \dots \\ r_{m-1}^{(i-m+j+1)} &= r_{m}^{(i-m+j)} + b_{0} r_{0}^{(i-m+j)}. \end{split}$$

Summing both sides of these equations and using (2.6') yields

$$r_j^{(i)} = r_m^{(i-m+j)} + \sum_{\ell=1}^{m-j} b_{m-j-\ell} r_0^{(i-\ell)} = a_{n-i-j} + \sum_{\ell=1}^{m-j} b_{m-j-\ell} r_0^{(i-\ell)} \quad (0 \le j \le m-1).$$
 (2.7)

460

For j = 0, (2.7) reduces to

$$r_0^{(i)} = a_{n-i} + \sum_{\ell=1}^m b_{m-\ell} r_0^{(i-\ell)}, \tag{2.8}$$

where  $r_0^{(i-\ell)} = 0$  if  $i < \ell$ , and (2.2) applies.

### Proposition 1:

$$r_0^{(i)} = \sum_{h=0}^{i} a_{n-h} Z_{i-h+1}, \tag{2.9}$$

where the integers  $Z_h$  obey the recurrence

$$Z_h = b_{m-1} Z_{h-1} + b_{m-2} Z_{h-2} + \dots + b_0 Z_{h-m}$$
 (2.10)

which is of  $m^{th}$ -order if  $b_0 \not\equiv 0 \pmod{q}$ , and has initial conditions

$$Z_h = 0 \text{ (for } -m+2 \le h \le 0) \text{ and } Z_1 = 1$$
 (2.11)

or, equivalently,

$$\begin{cases}
Z_1 = 1, \\
Z_2 = b_{m-1}Z_1, \\
Z_3 = b_{m-1}Z_2 + b_{m-2}Z_1, \\
... \\
Z_m = b_{m-1}Z_{m-1} + b_{m-2}Z_{m-2} + \dots + b_1Z_1.
\end{cases}$$
(2.11')

**Proof:** We shall prove that replacing the right-hand side of (2.9) in (2.8) yields an identity. In fact, this replacement gives the equation

$$\sum_{h=0}^{i} a_{n-h} Z_{i-h+1} = a_{n-i} + b_{m-1} \sum_{h=0}^{i-1} a_{n-h} Z_{i-h} + b_{m-2} \sum_{h=0}^{i-2} a_{n-h} Z_{i-h-1} + \dots + b_0 \sum_{h=0}^{i-m} a_{n-h} Z_{i-h-m+1}.$$
(2.12)

By reducing all summations in (2.12) to the same upper range indicator (namely, i-m), we can write

$$a_{n-i}Z_{1} + a_{n-i+1}Z_{2} + \dots + a_{n-i+m-1}Z_{m} + \sum_{h=0}^{i-m} a_{n-h}Z_{i-h+1}$$

$$= a_{n-i} + b_{m-1}(a_{n-i+1}Z_{1} + a_{n-i+2}Z_{2} + \dots + a_{n-i+m-1}Z_{m-1}) + b_{m-1}\sum_{h=0}^{i-m} a_{n-h}Z_{i-h}$$

$$+ b_{m-2}(a_{n-i+2}Z_{1} + \dots + a_{n-i+m-1}Z_{m-2}) + b_{m-2}\sum_{h=0}^{i-m} a_{n-h}Z_{i-h-1} + \dots$$

$$+ b_{1}(a_{n-i+m-1}Z_{1}) + b_{1}\sum_{h=0}^{i-m} a_{n-h}Z_{i-h-m+2} + b_{0}\sum_{h=0}^{i-m} a_{n-h}Z_{i-h-m+1}.$$

The above equation can be rewritten as

1995]

$$a_{n-i}(Z_1-1) + a_{n-i+1}(Z_2 - b_{m-1}Z_1) + \dots + a_{n-i+m-1}(Z_m - b_{m-1}Z_{m-1} - \dots - b_1Z_1) + \sum_{h=0}^{i-m} a_{n-h}(Z_{i-h+1} - b_{m-1}Z_{i-h} - b_{m-2}Z_{i-h-1} - \dots - b_0Z_{i-m-h+1}) = 0,$$

which, by (2.10) and (2.11') is identically satisfied. Q.E.D.

Recalling that the quantities  $r_j^{(n-m+1)}$  (j=0,1,...,m-1) are the coefficients of the remainder of f(x): g(x), it becomes patent that f(x) is divisible by g(x) iff  $r_j^{(n-m+1)} \equiv 0 \pmod{q}$  for all admissible values of j. By (2.9), after some simple manipulations, one can see that the condition  $r_0^{(n-m+1)} \equiv 0 \pmod{q}$  is satisfied if

$$\sum_{h=m-1}^{n} a_h Z_{h-m+2} \equiv 0 \pmod{q}. \tag{2.13}$$

By using the first equation of (2.5), we can get analogous conditions pertaining to  $r_j^{(n-m+1)}$  for  $1 \le j \le m-1$ . For example, letting j=0 in (2.5) yields

$$r_1^{(n-m+1)} = r_0^{(n-m+2)} - b_{m-1}r_0^{(n-m+1)} \equiv r_0^{(n-m+2)} \pmod{q}$$
 [by (2.13)],

whence, by (2.9), the condition  $r_1^{(n-m+1)} \equiv r_0^{(n-m+2)} \equiv 0 \pmod{q}$  is satisfied if

$$\sum_{h=m-2}^{n} a_h Z_{h-m+3} \equiv 0 \pmod{q}.$$
 (2.14)

Iterating this procedure for all values of j allows us to state our main result.

**Proposition 2 (main result):** The polynomial f(x) is divisible by the polynomial g(x) iff

$$\sum_{h=m-j-1}^{n} a_h Z_{h-m+j+2} \equiv 0 \pmod{q} \text{ for } j = 0, 1, ..., m-1.$$
 (2.15)

#### 3. SPECIAL CASES

For small values of m, or for special polynomials f(x), the divisibility conditions (2.15) simplify remarkably. In this section, three special cases are discussed in detail.

#### Case 1: m = 1

If m = 1, Proposition 2 tells us that f(x) is divisible by  $x - b_0$  [ $b_0 \neq 0 \pmod{q}$ ] iff

$$\sum_{h=0}^{n} a_h Z_{h+1} \equiv \sum_{h=0}^{n} a_h b_0^h \equiv 0 \pmod{q}, \tag{3.1}$$

since  $Z_h = b_0 Z_{h-1}$  with  $Z_1 = 1$  [see (2.10)-(2.11)] implies  $Z_h = b_0^{h-1}$ . The condition (3.1) agrees with the well-known fact (e.g., see [4], Theorem 1.64) that, if  $f(b_0) \equiv 0 \pmod{q}$ , then f(x) is divisible by  $x - b_0$  [cf. point (ii) in Section 1].

# Case 2: m = 2

If m = 2, Proposition 2 tells us that f(x) is divisible by  $x^2 - b_1 x - b_0$  [ $b_0 \not\equiv 0 \pmod{q}$ ] iff

$$\sum_{h=1-j}^{n} a_h Z_{h+j} \equiv 0 \pmod{q} \quad (j=0,1), \tag{3.2}$$

where the numbers  $Z_h$  are the generalized Fibonacci numbers  $W_h$  [more precisely, the numbers  $W_h(b_1, -b_0; 0, 1)$ ] which have been studied extensively over the past years (e.g., see [3] for background material). In particular, if q = 2, f(x) is divisible by  $x^2 - x - 1$  iff

$$\sum_{h=1-j}^{n} a_h F_{h+j} \equiv 0 \pmod{2} \quad (j=0,1), \tag{3.3}$$

where  $F_h$  denotes the  $h^{th}$  Fibonacci number. Taking into account that  $F_h$  is even iff  $h \equiv 0 \pmod{3}$ , conditions (3.2) can be rewritten as

$$\sum_{h=1}^{n} a_h \equiv \sum_{h=1}^{n} a_h \equiv 0 \pmod{2}.$$

$$h \not\equiv 0 \pmod{3} \quad h \not\equiv 2 \pmod{3}$$
(3.4)

Case 3:  $f(x) = x^n - 1$ 

If  $f(x) = x^n - 1$ , then Proposition 2 tells us that f(x) is divisible by g(x) iff

$$\begin{cases}
Z_{n-m+j+2} \equiv 0 \pmod{q} & (j=0,1,...,m-2), \\
Z_{n+1} \equiv Z_1 \equiv 1 \pmod{q}.
\end{cases}$$
(3.5)

When  $n = q^m - 1$  and m is a prime not less than q, the fulfillment of (3.5) implies that g(x) [ $b_0 \neq 0 \pmod{q}$ ] is *irreducible* (see [4], Theorem 3.20). Moreover, if q = 2 and n is a Mersenne prime, then g(x), beyond being irreducible, is *primitive* (see [4], Corollary 3.4).

The fulfillment of (3.5) can be checked out rapidly by means of the software implementation of an m-cell linear feedback shift register [2] having g(x) as its characteristic polynomial, and initial state [1, 0, 0, ..., 0]. Once this is made, one simply has to ascertain that the m terms  $Z_{n-m+2}, Z_{n-m+3}, ..., Z_{n+1}$  of the sequence  $\{Z_h\}$  generated by this device satisfy (3.5).

### **ACKNOWLEDGMENT**

This work has been carried out in the framework of an agreement between the Italian PT Administration (Istituto Superiore PT) and the Fondazione Ugo Bordoni.

#### REFERENCES

- 1. H. Beker & F. Piper. Cipher Systems. New York: Wiley, 1982.
- 2. S. W. Golomb. Shift Register Sequences. Laguna Hills, Calif.: Aegean Park Press, 1982.
- 3. A. F. Horadam. "Generalization of a Result of Morgado." *Portugaliae Mathematica* **44.2** (1987):131-36.
- 4. R. Lidl & H. Niederreiter. "Finite Fields." In *Encyclopedia of Mathematics and Its Applications*. Vol. 20. Ed. Gian-Carlo Rota. Reading, Mass.: Addison Wesley, 1983.
- 5. W. W. Peterson. Error-Correcting Codes. New York: Wiley, 1961.

AMS Classification Numbers: 12E05, 11B83, 11B39

\*\*\*

# SOME CONDITIONS FOR "ALL OR NONE" DIVISIBILITY OF A CLASS OF FIBONACCI-LIKE SEQUENCES

#### Juan Pla

315 rue de Belleville 75019 Paris, France (Submitted May 1994)

In reference [1], the following theorem has been proved:

**Theorem:** Let  $u_n$  be the general term of a given sequence of integers such that  $u_{n+1} = u_{n+1} + u_n$ , where  $u_0$  and  $u_1$  are arbitrary integers. Let x be an arbitrary integer other than -2, -1, 0 and 1. Let D be any divisor of  $x^2 + x - 1$  other than 1. Then the sequence  $w_n = xu_{n+1} - u_n$ , where  $n \ge 0$  is such that:

- (a) D divides every  $w_n$ ;
- (b) D divides no  $w_n$ .

The aim of this paper is to provide some precise conditions for the "all" situation.

**Theorem 1:** A necessary, but not sufficient, condition for the sequence with general term  $w_n = xu_{n+1} - u_n$  to display the "all" property relative to a given *prime* divisor p of  $x^2 + x - 1$  is that the distribution of the residues of  $(u_n)$  modulo p be either constant or periodic with period p-1.

### 1) Proof that the condition is necessary:

Let us define the transformation  $T_x(u_n)$ , for any n, by  $T_x(u_n) = xu_{n+1} - u_n$ . If  $(T_x(u_n))^{(m)}$  denotes the m<sup>th</sup> iterate of this transformation on  $(u_n)$ , it is quite easy to prove by induction that, for any n and m:

$$(T_x(u_n))^{(m)} = \sum_{k=0}^{k=m} (-1)^{m+k} \binom{m}{k} (x)^k u_{n+k}.$$

Put m = p in this formula. Since p is prime, the binomial coefficients are all divisible by p, except the two extreme ones ([2], p. 417). Therefore,

$$(T_x(u_n))^{(p)} \equiv x^p u_{n+p} + (-1)^p u_n \pmod{p}$$
.

Since no even number can divide  $x^2 + x - 1$ , p is always an odd prime, and therefore,

$$(T_x(u_n))^{(p)} \equiv x^p u_{n+p} - u_n \pmod{p}$$

for any n. But, since by construction  $(T_x(u_n))^{(p)}$  is a linear combination (with integral coefficients) of  $w_n$  terms all supposedly divisible by p, this entails

$$x^p u_{n+p} - u_n \equiv 0 \pmod{p}.$$

Since p is prime,  $x^p \equiv x \pmod{p}$ , and the previous congruence becomes

$$xu_{n+p} - u_n \equiv 0 \pmod{p}.$$

By hypothesis, for any n,  $xu_{n+1} - u_n \equiv 0 \pmod{p}$ . From the difference of the previous congruences, we obtain

$$x(u_{n+p}-u_{n+1})\equiv 0\pmod{p}.$$

Since p and x are relatively prime, this implies that, for any n,  $u_{n+p} - u_{n+1} \equiv 0 \pmod{p}$ , which proves the necessity of the condition stated above.

**Example:** In reference [1], we have seen that  $w_n = xL_{n+1} - L_n$  displays the property "all" for x = 2 and p = 5. Therefore, we must have, for any n,  $L_{n+5} - L_{n+1} \equiv 0 \pmod{5}$ , which property can easily be confirmed.

# 2) Proof that the condition is not sufficient:

To prove this, we shall find an appropriate counter-example deduced from the following lemma.

**Lemma:** For any x and any prime p dividing  $x^2 + x - 1$ , the sequence  $(w_n) = (xF_{n+1} - F_n)$  displays the "none" property.

Its demonstration is immediate, since  $w_0 = x$ , and p cannot divide x.

Now, for x = 7, we have  $x^2 + x - 1 = 55 = 5 * 11$ .

But we have  $F_{n+11} - F_{n+1} \equiv 0 \pmod{11}$  for n = 0 and n = 1. By using the fundamental recurrence property of the Fibonacci numbers, it is then easy to prove this property for any n. However, the above Lemma proves that it is not sufficient to imply the "all" property relative to p = 11.

**Theorem 2:** If, for a sequence  $w_n = xu_{n+1} - u_n$ , the "all" situation occurs for a nontrivial divisor D of  $x^2 + x - 1$ , then D divides the quantity  $(u_1)^2 - u_0 u_2$ .

**Proof:** By definition of D:  $x^2 + x - 1 \equiv 0 \pmod{D}$ . By multiplying both sides of this congruence by  $(u_1)^2$ , we obtain  $(xu_1)^2 + (xu_1)u_1 - (u_1)^2 \equiv 0 \pmod{D}$ . But since  $xu_1 \equiv u_0 \pmod{D}$ , this is equivalent to  $(u_0)^2 + u_0u_1 - (u_1)^2 \equiv 0 \pmod{D}$ . And since  $(u_1)^2 - u_0u_1 - (u_0)^2 = (u_1)^2 - u_0u_2$ , the proof is complete.

This property helps to sharply reduce the number of divisors possible for an "all" situation to occur. For instance, for  $u_n = L_n$ ,  $(u_1)^2 - u_0 u_2 = -5$ . Therefore, 5 is the only possible (positive) divisor of  $w_n = xL_{n+1} - L_n$  among those of  $x^2 + x - 1$ .

But this property of D is not sufficient to warrant the "all" situation, as shown by taking  $u_0 = -1$ ,  $u_1 = 4$ , and x = 4. In this case,  $x^2 + x - 1 = 19$ , so the only possible D is 19 and, on the other hand,  $(u_1)^2 - u_0 u_2 = 19$ . But since  $w_0 = 4u_1 - u_0 = 17$ , we are in the "none" situation.

#### REFERENCES

- 1. Juan Pla. "An 'All or None' Divisibility Property for a Class of Fibonacci-Like Sequences of Integers." *The Fibonacci Quarterly* **32.3** (1994):226-27.
- 2. Edouard Lucas. Théorie des Nombres. Paris, 1891; rpt. Paris: Jacques Gabay, 1991.

AMS Classification Numbers: 11B37, 11B39

\*\*\*

### **ELEMENTARY PROBLEMS AND SOLUTIONS**

# Edited by Stanley Rabinowitz

Please send all material for ELEMENTARY PROBLEMS AND SOLUTIONS to Dr. STANLEY RABINOWITZ; 12 VINE BROOK RD; WESTFORD, MA 01886-4212 USA. Correspondence may also be sent to the problem editor by electronic mail to Fibonacci@MathPro.com on Internet. All correspondence will be acknowledged.

Each solution should be on a separate sheet (or sheets) and must be received within six months of publication of the problem. Solutions typed in the format used below will be given preference. Proposers of problems should normally include solutions. Proposers should inform us of the history of the problem, if it is not original. A problem should not be submitted elsewhere while it is under consideration for publication in this column.

#### **BASIC FORMULAS**

The Fibonacci numbers  $F_n$  and the Lucas numbers  $L_n$  satisfy

$$F_{n+2} = F_{n+1} + F_n$$
,  $F_0 = 0$ ,  $F_1 = 1$ ;  
 $L_{n+2} = L_{n+1} + L_n$ ,  $L_0 = 2$ ,  $L_1 = 1$ .

Also, 
$$\alpha = (1 + \sqrt{5})/2$$
,  $\beta = (1 - \sqrt{5})/2$ ,  $F_n = (\alpha^n - \beta^n)/\sqrt{5}$ , and  $L_n = \alpha^n + \beta^n$ .

# PROBLEMS PROPOSED IN THIS ISSUE

B-796 Proposed by M. N. S. Swamy, St. Lambert, Quebec, Canada

Show that 
$$\frac{L_n^2 + L_{n+1}^2 + L_{n+2}^2 + \dots + L_{n+a}^2}{F_n^2 + F_{n+1}^2 + F_{n+2}^2 + \dots + F_{n+a}^2}$$
 is always an integer if  $a$  is odd.

**B797** Proposed by Andrew Cusumano, Great Neck, NY

Let  $\langle H_n \rangle$  be any sequence that satisfies the recurrence  $H_{n+2} = H_{n+1} + H_n$ . Prove that

$$7H_n \equiv H_{n+15} \pmod{10}.$$

**B-798** Proposed by Seung-Jin Bang, Ajou University, Suwon, Korea

Prove that, for *n* a positive integer,  $F_{s^n}$  is divisible by  $5^n$  but not by  $5^{n+1}$ .

**B-799** Proposed by David Zeitlin, Minneapolis, MN

Solve the recurrence  $A_{n+2} = 4A_{n+1} + A_n$ , for  $n \ge 0$ , with initial conditions  $A_0 = 1$  and  $A_1 = 4$ ; expressing your answer in terms of Fibonacci and/or Lucas numbers.

**B-800** Proposed by H.-J. Seiffert, Berlin, Germany

Define the Pell numbers by the recurrence  $P_n = 2P_{n-1} + P_{n-2}$ , for  $n \ge 2$ , with initial conditions  $P_0 = 0$  and  $P_1 = 1$ .

Show that, for all integers  $n \ge 4$ ,  $P_n < F_{k(n)}$  where  $k(n) = \lfloor (1 \ln + 2) / 6 \rfloor$ .

# **B-801** Proposed by Larry Taylor, Rego Park, NY

Let  $k \ge 2$  be an integer and let *n* be an odd integer. Prove that

(a) 
$$F_{2^k} \equiv 27 \cdot 7^k \pmod{40}$$
;

$$F_{-2^k} \equiv 7^k F_{16n} \pmod{40}.$$

### **SOLUTIONS**

# A Lucas Congruence

# <u>B-766</u> Proposed by R. André-Jeannin, Longwy, France (Vol. 32, no. 4, August 1994)

Let n be an even positive integer such that  $L_n \equiv 2 \pmod{p}$ , where p is an odd prime. Prove that  $L_{n+1} \equiv 1 \pmod{p}$ .

# Solution by Leonard A. G. Dresel, Reading, England

We start with the identity

$$5F_n^2 = L_n^2 - 4(-1)^n$$

which is identity (24) from [1]. If n is even and  $L_n \equiv 2 \pmod{p}$ , we have  $5F_n^2 \equiv 0 \pmod{p}$  and therefore  $5F_n \equiv 0 \pmod{p}$  since p is a prime. Applying the identity  $L_{n+1} + L_{n-1} = 5F_n$ , which is identity (5) from [1], and the definition  $L_{n+1} - L_{n-1} = L_n$ , we find  $2L_{n+1} = 5F_n + L_n \equiv 2 \pmod{p}$ . Since p is odd, this gives  $L_{n+1} \equiv 1 \pmod{p}$ .

#### Reference:

1. S. Vajda. Fibonacci & Lucas Numbers, and the Golden Section: Theory and Applications. Chichester, England: Ellis Horwood Ltd., 1989.

Also solved by Paul S. Bruckman, Herta T. Freitag, Norbert Jensen, Bob Prielipp, H.-J. Seiffert, Lawrence Somer, David C. Terr, and the proposer.

# **Mutual Admiration Fibonacci Society**

# B-767 Proposed by James L. Hein, Portland State University, Portland, OR (Vol. 32, no. 4, August 1994)

Consider the following two mutual recurrences:

$$G_1 = 1$$
;  $G_n = F_{n+1}G_{n-1} + F_nH_{n-2}$ ,  $n \ge 2$ ;

and

$$H_0 = 0$$
;  $H_n = F_{n+1}G_n + F_nH_{n-1}$ ,  $n \ge 1$ .

Prove that  $H_{n-1}$  and  $G_n$  are consecutive Fibonacci numbers for all  $n \ge 1$ .

### Solution by M. N. S. Swamy, Montreal, Canada

We see that  $G_n$  and  $H_{n-1}$  are consecutive Fibonacci numbers for n=1 and n=2 since  $G_1=F_1$ ,  $H_0=F_0$ , and  $G_2=F_3$ ,  $H_1=F_2$ . Assuming that  $G_n=F_{a_n}$  and  $H_{n-1}=F_{a_n-1}$ , where  $a_n=n(n+1)/2$ , we have

$$G_{n+1} = F_{n+2}F_{a_n} + F_{n+1}F_{a_n-1} = F_{n+1+a_n} = F_{a_{n+1}}, \label{eq:Gn+1}$$

where we have used identity (I<sub>26</sub>) from [1]:  $F_{j+1}F_{k+1} + F_jF_k = F_{j+k+1}$ . In the same way,

$$H_n = F_{n+1}F_{a_n} + F_nF_{a_n-1} = F_{n+a_n} = F_{a_{n+1}-1}$$

Hence, by induction, we have  $G_n = F_{a_n}$  and  $H_{n-1} = F_{a_{n-1}}$  for all n. Thus,  $G_n$  and  $H_{n-1}$  are consecutive Fibonacci numbers for all  $n \ge 1$ .

#### Reference:

1. Verner E. Hoggatt, Jr. Fibonacci and Lucas Numbers. Santa Clara, CA: The Fibonacci Association, 1979.

Also solved by Paul S. Bruckman, Charles K. Cook, Leonard A. G. Dresel, Steve Edwards, Herra T. Freitag, C. Georghiou, Norbert Jensen, Carl Libis, Bob Prielipp, Don Redmond, H.-J. Seiffert, Lawrence Somer, David Zeitlin, and the proposer.

# A Radical Approach to Fibonacci Numbers

# <u>B-768</u> Proposed by Juan Pla, Paris, France (Vol. 32, no. 4, August 1994)

Let  $u_n, v_n$ , and  $w_n$  be sequences defined by  $u_1 = 1/2, v_1 = \sqrt{2}$ , and  $w_1 = (1/2)\sqrt{3}$ ;  $u_{n+1} = u_n^2 + v_n^2 - w_n^2$ ,  $v_{n+1} = 2u_n v_n$ ,  $w_{n+1} = 2u_n w_n$ . Express  $u_n, v_n$ , and  $w_n$  in terms of Fibonacci and/or Lucas numbers.

# Solution by C. Georghiou, University of Patras, Greece

The answer is  $u_n = \frac{1}{2}L_m$ ,  $v_n = \sqrt{2}F_m$ , and  $w_n = \frac{1}{2}\sqrt{3}F_m$ , where  $m = 2^{n-1}$ . We prove this by induction. Evidently, it is true for n = 1. Assuming it is true for n, we have

$$u_{n+1} = \frac{1}{4}L_m^2 + 2F_m^2 - \frac{3}{4}F_m^2 = \frac{1}{4}(L_m^2 + 5F_m^2) = \frac{1}{2}L_{2m} = \frac{1}{2}L_{2m}^2,$$

where we have used the identity  $L_m^2 + 5F_m^2 = 2L_{2m}$ , which is identity (22) from [1]. We also have

$$v_{n+1} = \sqrt{2}L_m F_m = \sqrt{2}F_{2m} = \sqrt{2}F_{2^n}$$

and

$$w_{n+1} = \frac{1}{2}\sqrt{3}L_m F_m = \frac{1}{2}\sqrt{3}F_{2m} = \frac{1}{2}\sqrt{3}F_{2^n},$$

where we have used the identity  $L_m F_m = F_{2m}$ , which is identity (13) from [1]. The induction step is now complete.

#### Reference:

1. S. Vajda. Fibonacci & Lucas Numbers, and the Golden Section: Theory and Applications. Chichester, England: Ellis Horwood Ltd., 1989.

Also solved by Brian D. Beasley, Paul S. Bruckman, Charles K. Cook, Leonard A. G. Dresel, Steve Edwards, Herta T. Freitag, Norbert Jensen, Hans Kappus, Bob Prielipp, H.-J. Seiffert, David C. Terr, David Zeitlin, and the proposer.

# The Recurrence for $F_{3^n}$

# <u>B-769</u> Proposed by Piero Filipponi, Fond. U. Bordoni, Rome, Italy (Vol. 32, no. 4, August 1994)

Solve the recurrence  $a_{n+1} = 5a_n^3 - 3a_n$ ,  $n \ge 0$ , with initial condition  $a_0 = 1$ .

# Solution by David C. Terr, University of California, Berkeley

We claim that the solution is  $a_n = F_{3^n}$ . Clearly this holds for n = 0. Assume it holds for some nonnegative integer n. Then

$$a_{n+1} = 5a_n^3 - 3a_n = 5F_{3^n}^3 - 3F_{3^n}$$

$$= 5\left[\frac{1}{\sqrt{5^3}}(\alpha^{3^n} - \beta^{3^n})^3\right] - \frac{3}{\sqrt{5}}(\alpha^{3^n} - \beta^{3^n})$$

$$= \frac{1}{\sqrt{5}}(\alpha^{3^{n+1}} - \beta^{3^{n+1}} - 3(\alpha^{3^n} - \beta^{3^n})[(\alpha\beta)^{3^n} + 1])$$

$$= \frac{1}{\sqrt{5}}(\alpha^{3^{n+1}} - \beta^{3^{n+1}}) = F_{3^{n+1}},$$

where we have used the identity  $\alpha\beta = -1$ . Thus, by induction, our answer is correct for all non-negative integers n.

# Comment by Murray S. Klamkin, University of Alberta, Canada

The same problem appeared as Problem 1809 in *Crux Mathematicorum* **20** (1994):19-20. In the same issue, there was a proposal to solve the recurrence

$$P_{n+1} = 25P_n^5 - 25P_n^3 + 5P_n, P_0 = 1.$$

The solution, which appeared in **20** (1994):295-96, is  $P_n = F_{5^n}$ . Also, one can show that the solutions to the following recurrences

$$A_{n+1} = A_n^2 - 2,$$
  $A_1 = 3,$   
 $B_{n+1} = B_n^4 - 4B_n^2 + 2,$   $B_1 = 7,$   
 $C_{n+1} = C_n^6 - 6C_n^4 + 9C_n^2 - 2,$   $C_1 = 18,$ 

are given by  $A_n = L_{2^n}$ ,  $B_n = L_{4^n}$ , and  $C_n = L_{6^n}$ .

In the Crux Mathematicorum solution, it was shown that the solution to the recurrence  $p_0 = 1$ ,  $p_{n+1} = \frac{1}{\sqrt{5}} f_m(\sqrt{5}p_n)$ , m odd,  $m \ge 3$ , where f(x) is defined by  $f_0(x) = 2$ ,  $f_1(x) = x$ , and  $f_n(x) = x f_{n-1}(x) - f_{n-2}(x)$ , for  $n \ge 2$  is  $p_n = F_{m^n}$ . This reduces to our problem when m = 3.

Also solved by Michel A. Ballieu, Seung-Jin Bang, Brian D. Beasley, Paul S. Bruckman, Leonard A. G. Dresel, Steve Edwards, Herta T. Freitag, C. Georghiou, Norbert Jensen, Hans Kappus, Murray S. Klamkin, Bob Prielipp, H.-J. Seiffert, Lawrence Somer, Adam Stinchcombe, David Zeitlin, and the proposer.

# **Unit Digit Madness**

# B-770 Proposed by Andrew Cusumano, Great Neck, NY (Vol. 32, no. 4, August 1994)

Let U(x) denote the unit's digit of x when written in base 10. Let  $H_n$  be any generalized Fibonacci sequence that satisfies the recurrence  $H_n = H_{n-1} + H_{n-2}$ . Prove that, for all n,

1995]

$$\begin{split} &U(H_n+H_{n+4})=U(H_{n+47}), &U(H_n+H_{n+17})=U(H_{n+34}), \\ &U(H_n+H_{n+5})=U(H_{n+10}), &U(H_n+H_{n+19})=U(H_{n+41}), \\ &U(H_n+H_{n+7})=U(H_{n+53}), &U(H_n+H_{n+20})=U(H_{n+55}), \\ &U(H_n+H_{n+8})=U(H_{n+19}), &U(H_n+H_{n+23})=U(H_{n+37}), \\ &U(H_n+H_{n+11})=U(H_{n+49}), &U(H_n+H_{n+25})=U(H_{n+50}), \\ &U(H_n+H_{n+13})=U(H_{n+26}), &U(H_n+H_{n+28})=U(H_{n+59}), \\ &U(H_n+H_{n+16})=U(H_{n+23}), &U(H_n+H_{n+29})=U(H_{n+58}). \end{split}$$

# Solution by Paul S. Bruckman, Edmonds, WA

Essentially, the problem asks us to verify that  $H_n + H_{n+a} \equiv H_{n+b} \pmod{10}$ , for all n, where (a, b) is a specified pair of positive integers. Using the identity

$$H_n = F_n H_1 + F_{n-1} H_0$$

which is identity (8) of [1], we see that it suffices to prove that

$$F_n + F_{n+a} \equiv F_{n+b} \pmod{10}, \quad \text{for all } n. \tag{*}$$

Since  $F_m + F_{m+1} = F_{m+2}$ , we need only prove (\*) for n = 0 and n = 1, for then, by induction, (\*) would be true for all n. Thus, we need only show that  $U(F_a) = U(F_b)$  and  $U(1 + F_{a+1}) = U(F_{b+1})$  for the given a and b.

In each case, these are readily checked from the following table of  $U(F_n)$ , n = 1, 2, ..., 60:

#### Reference:

1. S. Vajda. Fibonacci & Lucas Numbers, and the Golden Section: Theory and Applications. Chichester, England: Ellis Horwood Ltd., 1989.

Also solved by Leonard A. G. Dresel, Herta T. Freitag, Norbert Jensen, Bob Prielipp, H.-J. Seiffert, David Zeitlin, and voluminous generalizations and correspondence by the proposer.

### **More Sums**

<u>B-771</u> Proposed by H.-J. Seiffert, Berlin, Germany (Vol. 32, no. 4, August 1994)

Show that

$$\sum_{n=1}^{\infty} \frac{(2n+1)F_n}{2^n n(n+1)} = \ln 4.$$

Solution by Don Redmond, Southern Illinois University, Carbondale, IL

We generalize this result somewhat.

Let r, t, and u be complex numbers such that |t/r| < 1 and |u/r| < 1. Define the sequence  $\langle P_n \rangle$  by  $P_n = ct^n + du^n$ , where c and d are arbitrary complex numbers. For |x| < 1, we know that

$$\sum_{n=1}^{\infty} \frac{x^n}{n} = \ln\left(\frac{1}{1-x}\right).$$

This is series 1.513 on page 44 of [1]. Since

$$\frac{2n+1}{n(n+1)} = \frac{1}{n} + \frac{1}{n+1},$$

we find that

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

Thus,

$$\sum_{n=1}^{\infty} \frac{2n+1}{r^n n(n+1)} P_n = \sum_{n=1}^{\infty} \frac{2n+1}{n(n+1)} \left[ c \left( \frac{t}{r} \right)^n + d \left( \frac{u}{r} \right)^n \right]$$

$$= c \sum_{n=1}^{\infty} \frac{2n+1}{n(n+1)} \left( \frac{t}{r} \right)^n + d \sum_{n=1}^{\infty} \frac{2n+1}{n(n+1)} \left( \frac{u}{r} \right)^n$$

$$= -c \left( 1 + \frac{r}{t} \right) \ln \left( 1 - \frac{t}{r} \right) - c - d \left( 1 + \frac{r}{u} \right) \ln \left( 1 - \frac{u}{r} \right) - d.$$

If  $t = \alpha$ ,  $u = \beta$ ,  $c = 1/\sqrt{5}$ ,  $d = -1/\sqrt{5}$ , and r = 2, we get

$$\sum_{n=1}^{\infty} \frac{(2n+1)}{2^n n(n+1)} F_n = \ln 4.$$

If  $t = \alpha$ ,  $u = \beta$ , c = 1, d = 1, and r = 2, we get

$$\sum_{n=1}^{\infty} \frac{(2n+1)}{2^n n(n+1)} L_n = -2 - \sqrt{5} \ln \left( \frac{7 - 3\sqrt{5}}{2} \right).$$

#### Reference:

1. I. S. Gradshteyn & I. M. Ryzhik. *Table of Integrals, Series, and Products*. San Diego, CA: Academic Press, 1980.

Also solved by Seung-Jin Bang, Glenn A. Bookhout, Wray Brady, Paul S. Bruckman, Leonard A. G. Dresel, Steve Edwards, C. Georghiou, Norbert Jensen, Hans Kappus, Murray S. Klamkin, Bob Prielipp, Adam Stinchcombe, David Zeitlin, and the proposer.

#### **ERRATA**

**B-746** (Feb. 1995, p. 87): It should be noted that the formula  $L_{3n} = L_n^3 + 3L_n$  is only valid for n odd.

B-754 (May 1995): Gauthier's formula on the bottom of page 184 should read

$$\sum_{k=1}^{n} x^{k} G_{sk+t} = \frac{(-1)^{s} x^{n+1} G_{sn+t} - x^{n} G_{x(n+1)+t} + G_{s+t} + (-1)^{s+1} x G_{t}}{1 - 2x (G_{s} + G_{s-1}) + (-1)^{s} x^{2}}.$$

**B-759** (Aug. 1995, p. 372): In the fourth line of the solution,  $tu^{n+1}(t/v)^j$  should be  $tv^{n+1}(t/v)^j$ .

\*\*\*

# 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-503 Proposed by Paul S. Bruckman, Edmonds, WA

Let  $\mathcal{G}$  be the set of functions  $F: \mathbb{C}^3 \to \mathbb{C}$  ( $\mathbb{C}$  is the complex plane) satisfying the following formal properties:

$$xyz F(x, x^3y, x^3y^2z) = F(x, y, z),$$
 (1)

$$F(x^{-1}, y, z^{-1}) = F(x, y, z).$$
(2)

Formally define the functions U and V as follows:

$$U(x, y, z) = \sum x^{n^3} y^{n^2} z^n$$
 (summed over all integers n); (3)

$$V(x, y, z) = \prod_{n=1}^{\infty} (1 - y^{2n} A(x)) (1 + x^{3n^2 - 3n + 1} y^{2n - 1} z) (1 + x^{-3n^2 + 3n - 1} y^{2n - 1} z^{-1}), \tag{4}$$

where

$$A(x) = \frac{\sum x^{3m} o_m}{\sum x^{3m} e_m} \quad \text{(summed over all integers } m\text{)},$$

$$o_m = \frac{1}{2}(1 - (-1)^m), \quad e_m = \frac{1}{2}(1 + (-1)^m).$$
 (6)

Show that, at least formally,

$$U \in \mathcal{G}, \quad V \in \mathcal{G};$$
 (7)

$$A(1) = 1, \tag{8}$$

$$U(1, y, z) = V(1, y, z). (9)$$

Prove or disprove that  $U(x, y, z) \equiv V(x, y, z)$  identically. Can U(x, y, z) be factored into an infinite product?

# H-504 Proposed by Z. W. Trzaska, Warsaw, Poland

Given a sequence of polynomials in complex variable  $z \in C$  defined recursively by

(i) 
$$R_{k+1}(z) = (3+z)R_k(z) - R_{k-1}(z), \quad k = 0, 1, 2, ...,$$

with  $R_0(z) = 1$  and  $R_1(z) = (1+z)R_0$ .

Prove that

(ii) 
$$R_k(0) = F_{2k+1}$$
,

where  $F_{\ell}$ ,  $\ell = 0, 1, 2, ...$ , denotes the  $\ell^{th}$  term of the Fibonacci sequence.

# H-505 Proposed by Juan Pla, Paris, France

Edouard Lucas once noted: "On ne connaît pas de formule simple pour la somme des cubes du binôme" [No simple formula is known for the sum of the cubes of the binomial coefficients] (see Edouard Lucas, *Théorie des Nombres*, Paris, 1891, p. 133, as reprinted by Jacques Gabay, Paris, 1991).

The following problem is designed to find *closed*, if not quite "simple," formulas for the sum of the cubes of all the coefficients of the binomial  $(1+x)^n$ .

1) Prove that

$$\sum_{n=0}^{p=n} {n \choose p}^3 = \frac{2^n}{4\pi^2} \int_0^{2\pi} \int_0^{2\pi} \{1 + \cos\varphi + \cos\theta + \cos(\varphi + \theta)\}^n d\theta d\varphi.$$

2) Prove that

$$\sum_{n=0}^{p=n} {n \choose p}^3 = \frac{8^n}{\pi^2} \int_0^{\pi} \int_0^{\pi} {\cos \varphi \cos \theta \cos (\varphi + \theta)}^n d\theta d\varphi.$$

### **SOLUTIONS**

#### Sum Problem

# H-489 Proposed by H.-J. Seiffert, Berlin, Germany (Vol. 32, no. 4, August 1994)

Define the sequences of Pell numbers and Pell-Lucas numbers by

$$P_0 = 0$$
,  $P_1 = 1$ ,  $P_{k+2} = 2P_{k+1} + P_k$ ,  
 $Q_0 = 2$ ,  $Q_1 = 2$ ,  $Q_{k+2} = 2Q_{k+1} + Q_k$ .

Show that

(a) 
$$\sum_{n=1}^{\infty} \frac{F_{2^n} Q_{2^n}}{8(L_{2^n} P_{2^n})^2 - 5(F_{2^n} Q_{2^n})^2} = \frac{1}{12},$$

(b) 
$$\sum_{n=1}^{\infty} \frac{L_{2^n} P_{2^n}}{8(L_{2^n} P_{2^n})^2 - 5(F_{2^n} Q_{2^n})^2} = \frac{8 - 3\sqrt{2}}{48}.$$

# Solution by Norbert Jensen, Kiel, Germany

Step (1): Solving the characteristic equation and determining the explicit formulas for  $(P_k)_{k \in \mathbb{N}_0}$  and  $(Q_k)_{k \in \mathbb{N}_0}$ , we obtain

$$P_k = \frac{1}{2\sqrt{2}} \left( (1 + \sqrt{2})^k - (1 - \sqrt{2})^k \right), \tag{1.1}$$

$$Q_k = (1 + \sqrt{2})^k + (1 - \sqrt{2})^k \quad \text{for all } k \in \mathbb{N}_0.$$
 (1.2)

Let  $\gamma := 1 + \sqrt{2}$ ,  $\delta := 1 - \sqrt{2}$ . As  $\gamma$  and  $\delta$  are the zeros of the characteristic polynomial, it follows that

$$\gamma \delta = -1 \text{ and } \gamma + \delta = 2.$$
 (1.3)

Since the sequences  $(\gamma^n)_{n\in\mathbb{N}_0}$  and  $(\delta^n)_{n\in\mathbb{N}_0}$  satisfy the same recursion as  $(P_k)_{k\in\mathbb{N}_0}$ , it follows by induction that

$$\gamma^n = P_n \gamma + P_{n-1} = P_n \sqrt{2} + (P_n + P_{n-1})$$
 (1.4)

[and 
$$\delta^n = P_n \delta + P_{n-1} = -P_n \sqrt{2} + (P_n + P_{n-1})$$
] for all  $n \in \mathbb{N}$ .

Calculation shows that

$$|\alpha/\gamma| = \alpha/\gamma < 1$$
. [Of course  $|\beta/\gamma| < 1$ .] (1.5)

**Step (2):** We need the following general identity: For all  $z \in \mathbb{R}$  such that |z| < 1, we have

$$\sum_{n=1}^{\infty} \frac{z^{2^n}}{1-z^{2^{n+1}}} = \frac{z^2}{1-z^2}.$$

**Proof:** The series  $\sum_{k=1}^{\infty} z^{2k}$  is absolutely convergent with limit  $\frac{z^2}{1-z^2}$ , provided |z| < 1. Hence, we can sum up the terms  $z^{2k}$  in arbitrary order without changing the limit or convergence. Now

$$\sum_{k=1}^{\infty} z^{2k} = \sum_{n=1}^{\infty} \sum_{m=0}^{\infty} z^{2^{n}(2m+1)} = \sum_{n=1}^{\infty} \sum_{m=0}^{\infty} z^{2^{n+1}m+2^{n}},$$

since, on the right side, each term  $z^{2k}$  appears exactly once for each positive integer  $k \in \mathbb{N}$ . Now, for each fixed  $n \in \mathbb{N}$ , we have

$$\sum_{m=0}^{\infty} z^{2^{n+1}m+2^n} = \frac{z^{2^n}}{1-z^{2^{n+1}}}.$$

Therefore,  $\sum_{n=1}^{\infty} \frac{z^{2^n}}{1-z^{2^{n+1}}}$  is convergent and

$$\sum_{n=1}^{\infty} \frac{z^{2^n}}{1 - z^{2^{n+1}}} = \sum_{n=1}^{\infty} \sum_{m=0}^{\infty} z^{2^n (2m+1)} = \sum_{k=1}^{\infty} z^{2k} = \frac{z^2}{1 - z^2}.$$

Q.E.D. Step (2).

**Step (3):** it is convenient to prove the following two identities:

$$\sqrt{8} \cdot L_{2^{n}} P_{2^{n}} - \sqrt{5} \cdot F_{2^{n}} Q_{2^{n}} = 2 \cdot \left(\frac{\gamma}{\alpha}\right)^{2^{n}} \left[1 - \left(\frac{\alpha}{\gamma}\right)^{2^{n+1}}\right], \tag{3.1}$$

$$\sqrt{8} \cdot L_{2^n} P_{2^n} + \sqrt{5} \cdot F_{2^n} Q_{2^n} = 2 \cdot \left(\frac{\gamma}{\beta}\right)^{2^n} \left[1 - \left(\frac{\beta}{\gamma}\right)^{2^{n+1}}\right]. \tag{3.2}$$

**Proof:** We have

$$\sqrt{8} \cdot L_{2^n} P_{2^n} = (\alpha^{2^n} + \beta^{2^n}) (\gamma^{2^n} - \delta^{2^n}) = (\alpha \gamma)^{2^n} - (\alpha \delta)^{2^n} + (\beta \gamma)^{2^n} - (\beta \delta)^{2^n}$$

and

$$\sqrt{5} \cdot F_{2^n} Q_{2^n} = (\alpha^{2^n} - \beta^{2^n}) (\gamma^{2^n} + \delta^{2^n}) = (\alpha \gamma)^{2^n} + (\alpha \delta)^{2^n} - (\beta \gamma)^{2^n} - (\beta \delta)^{2^n}.$$

Hence, using  $\alpha\beta = \gamma\delta = -1$ , we have

$$\sqrt{8} \cdot L_{2^{n}} P_{2^{n}} - \sqrt{5} \cdot F_{2^{n}} Q_{2^{n}} = 2 \cdot ((\beta \gamma)^{2^{n}} - (\alpha \delta)^{2^{n}}) = 2 \left(\frac{\gamma}{\alpha}\right)^{2^{n}} \left[1 - \left(\frac{\alpha}{\gamma}\right)^{2^{n+1}}\right].$$

This proves (3.1). Similarly, (3.2) is seen to be

$$\sqrt{8} \cdot L_{2^{n}} P_{2^{n}} + \sqrt{5} \cdot F_{2^{n}} Q_{2^{n}} = 2 \cdot \left( (\alpha \gamma)^{2^{n}} - (\beta \delta)^{2^{n}} \right) = 2 \left( \frac{\gamma}{\beta} \right)^{2^{n}} \left| 1 - \left( \frac{\beta}{\gamma} \right)^{2^{n+1}} \right|.$$

Q.E.D. Step (3).

**Step (4):** Replacing z in Step (2) by  $\alpha/\gamma$  and  $\beta/\gamma$ , respectively, we obtain the following identities, where all limits exist:

$$A := \sum_{n=1}^{\infty} \frac{1}{\sqrt{8} \cdot L_{2^{n}} P_{2^{n}} - \sqrt{5} \cdot F_{2^{n}} Q_{2^{n}}} = \sum_{n=1}^{\infty} \frac{1}{2} \frac{\left(\frac{\alpha}{\gamma}\right)^{2^{n}}}{1 - \left(\frac{\alpha}{\gamma}\right)^{2^{n+1}}} = \frac{1}{2} \frac{1}{2} \frac{\left(\frac{\alpha}{\gamma}\right)^{2}}{1 - \left(\frac{\alpha}{\gamma}\right)^{2}} = \frac{1}{2} \frac{\alpha^{2}}{\gamma^{2} - \alpha^{2}}.$$

$$B := \sum_{n=1}^{\infty} \frac{1}{\sqrt{8} \cdot L_{2^{n}} P_{2^{n}} + \sqrt{5} \cdot F_{2^{n}} Q_{2^{n}}} \stackrel{=}{=} \sum_{n=1}^{\infty} \frac{1}{2} \frac{\left(\frac{\beta}{\gamma}\right)^{2^{n}}}{1 - \left(\frac{\beta}{\gamma}\right)^{2^{n+1}}} \stackrel{=}{=} \frac{1}{2} \frac{1}{2} \frac{\left(\frac{\beta}{\gamma}\right)^{2}}{1 - \left(\frac{\beta}{\gamma}\right)^{2}} = \frac{1}{2} \frac{\beta^{2}}{\gamma^{2} - \beta^{2}}.$$

Step (5): Now, using the fact that linear combinations of converging sequences are convergent against the linear combinations of their limits, we obtain:

(a) 
$$\sum_{n=1}^{\infty} \frac{F_{2^n} Q_{2^n}}{8(L_{2^n} P_{2^n})^2 - 5(F_{2^n} Q_{2^n})^2} = \frac{1}{2\sqrt{5}} (A - B) = \frac{1}{\text{step (4)}} \frac{1}{4\sqrt{5}} \left[ \frac{\alpha^2}{\gamma^2 - \alpha^2} - \frac{\beta^2}{\gamma^2 - \beta^2} \right]$$
$$= \frac{1}{4\sqrt{5}} \cdot \frac{(\alpha^2 - \beta^2)(2\sqrt{2} + 3)}{6\sqrt{2} + 9} = \frac{F_2}{4 \cdot 3} = \frac{1}{12};$$

1995]

(b) 
$$\sum_{n=1}^{\infty} \frac{L_{2^{n}} P_{2^{n}}}{8(L_{2^{n}} P_{2^{n}})^{2} - 5(F_{2^{n}} Q_{2^{n}})^{2}} = \frac{1}{2\sqrt{8}} (A+B) \underset{\text{Step (4)}}{=} \frac{1}{4\sqrt{8}} \left[ \frac{\alpha^{2}}{\gamma^{2} - \alpha^{2}} + \frac{\beta^{2}}{\gamma^{2} - \beta^{2}} \right]$$

$$= \frac{1}{8\sqrt{2}} \cdot \frac{(\alpha^{2} + \beta^{2})\gamma^{2} - 2(\alpha^{2}\beta^{2})}{\gamma^{4} - (\alpha^{2} + \beta^{2})\gamma^{2} + \alpha^{2}\beta^{2}} = \frac{1}{8\sqrt{2}} \cdot \frac{3\gamma^{2} - 2}{\gamma^{4} - 3\gamma^{2} + 1}$$

$$= \frac{1}{8\sqrt{2}} \cdot \frac{3(P_{2}\sqrt{2} + (P_{2} + P_{1})) - 2}{P_{4}\sqrt{2} + P_{4} + P_{3} - 3(P_{2}\sqrt{2} + P_{2} + P_{1}) + 1} = \frac{1}{8\sqrt{2}} \cdot \frac{6\sqrt{2} + 7}{6\sqrt{2} + 9}$$

$$= \frac{6\sqrt{2} + 7}{8 \cdot 9\sqrt{2} + 8 \cdot 2 \cdot 6} = \frac{(6\sqrt{2} + 7)(-8 \cdot 9\sqrt{2} + 8 \cdot 2 \cdot 6)}{(8 \cdot 2 \cdot 6)^{2} - 2(8 \cdot 9)^{2}}$$

$$= \frac{(6\sqrt{2} + 7)(-3 \cdot \sqrt{2} + 4)}{8 \cdot 3(4^{2} - 2 \cdot 3^{2})} = \frac{-8 + 3\sqrt{2}}{-48} = \frac{8 - 3\sqrt{2}}{48}.$$

Q.E.D.

Also solved by P. Bruckman, B. Popov, and the proposer.

### **Just So Many**

# H-490 Proposed by A. Stuparu, Vâlcea, Romania (Vol. 32, no. 5, November 1994)

Prove that the equation S(x) = p, where p is a given prime number, has just  $2^{p-2}$  solutions, all of them in between p and p!. [S(n)] is the Smarandache Function: the smallest integer such that S(n)! is divisible by n.

# Solution by Paul S. Bruckman, Edmonds, WA

The stated conclusion is incorrect. The correct number of solutions of the equation S(x) = p is  $\tau((p-1)!)$ , not  $2^{p-2}$ ; here,  $\tau(n)$  is the counting function of the divisors of n.

If S(x) = p, then  $x \mid p!$ , but  $x \not\mid m!$  for all m < p. If q is any prime factor of x, then  $q \le p$ ; for, if q > p, then  $q \mid p!$ , an obvious contradiction. On the other hand, if *all* prime factors of x are less than p, then  $x \mid (p-1)!$ , another contradiction. Therefore,  $p \mid x$ . Since  $p^1 \mid p!$ , it follows that x = pr, where  $r \mid (p-1)!$ .

Conversely, if x = pr, where r|(p-1)!, then  $S(x) \ge p$ , since  $x \nmid m!$  for all m < p. Also,  $S(x) \le p$ , since  $x \mid p!$ . Consequently, S(x) = p.

We have proven the following proposition:

$$S(x) = p \quad \text{iff} \quad x = pr \quad \text{where} \quad r | (p-1)!. \tag{*}$$

It follows that the number of solutions of the equation S(x) = p is precisely  $\tau((p-1)!)$ . A brief table of the first few values of  $\tau((p-1)!)$  is on the following page along with values of  $2^{p-2}$ , for comparison.

p	(p - 1)	$\tau((p-1)!)$	$2^{p-2}$
2	1	1	1
3	$2^1$	2	2
5	$2^3 \cdot 3^1$	8	8
7	$2^4 \cdot 3^2 \cdot 5^1$	30	32
11	$2^8 \cdot 3^4 \cdot 5^2 \cdot 7^1$	270	512
13	$2^{10} \cdot 3^5 \cdot 5^2 \cdot 7^1 \cdot 11^1$	792	2048
17	$2^{15} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11^1 \cdot 13^1$	5376	32768
19	$2^{16} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11^1 \cdot 13^1 \cdot 17^1$	14688	131072

The proposer may have been misled by the coincidence that  $\tau((p-1)!) = 2^{p-2}$  for p = 2,3,5. However, since  $(p-1)! \sim (2\pi/p)^{1/2}(p/e)^p$  (using Stirling's formula), and since the average order of  $\tau(n)$  is log n (a well-known result of number theory), it follows that the average order of  $\tau((p-1)!)$  is asymptotic to  $p \log p$  (as  $p \to \infty$ ), which is much smaller than  $2^{p-2}$ . It should be mentioned that such average is taken over all  $n \le p$ , not merely primes. However,  $n \log n$  is certainly  $o(2^n)$  as  $n \to \infty$ .

Also solved by M. Ballieu, A. Dujella, N. Jensen, H.-J. Seiffert, and the proposer.

Late Acknowledgment: Paul S. Bruckman solved H-459.



#### **VOLUME INDEX**

- ABRAHAMS, Julia, "Varn Codes and Generalized Fibonacci Trees," 33(1):21-25.
- ANDO, Shiro, "On a System of Sequences Defined by a Recurrence Relation," 33(3):279-282; (coauthor: Teluhiko Hilano), "A Disjoint Covering of the Set of Natural Numbers Consisting of Sequences Defined by a Recurrence Whose Characteristic Equation Has a Pisot Number Root," 33(4):363-367.
- ANDRÉ-JEANNIN, Richard, "A Note on a General Class of Polynomials, Part II, 33(4):341-351; "Differential Properties of a General Class of Polynomials," 33(5):453-458.
- ATANASSOV, Krassimir T., "Remark on a New Direction for a Generalization of the Fibonacci Sequence," 33(3):249-250.
- **BALAKRISHNAN**, N. (coauthors: K. Balasubramanian & Roman Viveros), "Some Discrete Distributions Related to Extended Pasca! Triangles," 33(5):415-425.
- **BALASUBRAMANIAN**, K. (coauthors: Roman Viveros & N. Balakrishnan), "Some Discrete Distributions Related to Extended Pascal Triangles," 33(5):415-425.
- **BALKIN**, S. D. (coauthors: D. S. Cousins, C. K. Orr, & C. A. Reiter), "Short Periods of Continued Fraction Convergents Modulo *M*: A Generalization of the Fibonacci Case," 33(3):222-233.
- BIALEK, Krystyna, "A Note on Choudhry's Results," 33(2):179-180.
- **BICKNELL\_JOHNSON**, Marjorie (coauthor: David A. Englund), "Greatest Integer Identities for Generalized Fibonacci Sequences  $\{H_n\}$ , Where  $H_n = H_{n-1} + H_{n-2}$ ," 33(1):50-58; (coauthor: Duane DeTemple), "Visualizing Golden Ratio Sums with Tiling Patterns," 33(4):298-303.
- **BRACKEN**, Paul, "Dynamics of the Mapping  $f(x) = (x+1)^{-1}$ ," 33(4):357-358.
- **BRENTON**, Lawrence (coauthor: Mi-Kyung Joo), "On the System of Congruences  $\prod_{i\neq i} n_i \equiv 1 \mod n_i$ ," 33(3):258-267.
- **BROWN**, Tom C. (coauthor: Peter Jau-shyong Shiue), "Squares of Second-Order Linear Recurrence Sequences," 33(4):352-356.
- **BRUGIA**, Odoardo (coauthor: Piero Filipponi), "Polynomial Divisibility in Finite Fields, and Recurring Sequences," 33(5): 459-463.
- **BRUYN**, G. F. C., de., "Formulas for  $a + a^2 2^p + a^3 3^p + \dots + a^n n^p$ ," 33(2):98-103.
- CHUAN, Wai-Fong, "Generating Fibonacci Words," 33(2):104-112; "Extraction Property of the Golden Sequence," 33(2):113-122.
- COOK, Roger (coauthor: David Sharpe), "Sums of Arithmetic Progressions," 33(3):218-221.
- COOPER, Curtis (coauthor: Robert E. Kennedy), "Proof of a Result by Jarden by Generalizing a Proof by Carlitz," 33(4):304-310
- COUSINS, D. S. (coauthors: S. D. Balkin, C. K. Orr, & C. A. Reiter), "Short Periods of Continued Fraction Convergents Modulo M: A Generalization of the Fibonacci Case," 33(3):222-233.
- **CREECH**, R. L. (coauthors: W. R. Spickerman & R. N. Joyner), "On the (3, F) Generalizations of the Fibonacci Sequence," 33(1):9-12.
- **DeLEON**, Morris Jack, "Sequences Related to an Infinite Product Expansion for the Square Root and Cube Root Functions," 33(1):41-49.
- **DeTEMPLE**, Duane (coauthor: Marjorie Bicknell-Johnson), "Visualizing Golden Ratio Sums with Tiling Patterns," 33(4):298-
- **DIMITROV**, Vassil S. (coauthor: Borislav D. Donevsky), "Faster Multiplication of Medium Large Numbers Via the Zeckendorf Representation," 33(1):74-77.
- **DONEVSKY**, Borislav D. (coauthor: Vassil S. Dimitrov), "Faster Multiplication of Medium Large Numbers Via the Zeckendorf Representation," 33(1):74-77.
- DUBEAU, François (coauthor: Alain Pautasso), "On Triangular Rectangular Numbers," 33(3):244-248.
- **ENGLUND**, David A. (coauthor Marjorie Bicknell-Johnson), "On the (3, F) Generalizations of the Fibonacci Sequence," Sequences  $\{H_n\}$ , Where  $H_n = H_{n-1} + H_{n-2}$ ," 33(1):50-58.
- **FILIPPONI**, Piero, "Some Binomial Fibonacci Identities," 33(3):251-257; (coauthor: Renato Menicocci), "Some Probabilistic Aspects of the Terminal Digits of Fibonacci Numbers," 33(4):325-331; (coauthor: Alwyn F. Horadam), "Real Pell and Pell-Lucas Numbers with Real Subscripts," 33(5):398-406; (coauthor: Odoardo Brugia), "Polynomial Divisibility in Finite Fields, and Recurring Sequences," 33(5):459-463.
- GAMKRELIDZE, N. G., "On a Probabilistic Property of the Fibonacci Sequence," 33(2):147-152.
- GLASER, Herbert (coauthor: Gerd Schöffl), "Ducci-Sequences and Pascal's Triangle," 33(4):313-324.
- GLASSON, Alan R., "Remainder Formulas Involving Generalized Fibonacci and Lucas Polynomials," 33(3):268-272.
- GOLIC, Jovan Dj., "On Decimation of Linear Recurring Sequences," 33(5):407-411.
- GOULD, H. W., "Extensions of the Hermite G.C.D. Theorems for Binomial Coefficients," 33(5):386-391.
- HAHN, Sang Geun (coauthor: Jun Kyo Kim), "A Note on Multiplicative Partitions of Bipartite Numbers," 33(3):283-288.

#### VOLUME INDEX

**HENDEL**, Russell (coauthors: Edith H. Luchins, Paul Lemke & David Tuller), "Linear Recurrences in Difference Triangles," 33(5):441-452.

**HENZE**, Norbert, "The Distribution of Spaces on Lottery Tickets," 33(5):426-431.

**HILANO**, Teluhiko (coauthor: Shiro Ando), "A Disjoint Covering of the Set of Natural Numbers Consisting of Sequences Defined by a Recurrence Whose Characteristic Equation Has a Pisot Number Root," 33(4):363-367.

**HILTON**, Peter (coauthors: Jean Pedersen & Luc Vrancken), "On Certain Arithmetic Properties of Fibonacci and Lucas Numbers," 33(3):211-217.

HOPE, Peter, "Exponential Growth of Random Fibonacci Sequences," 33(2):164-168.

HORADAM, Alwyn F. (coauthor: Piero Filipponi), "Real Pell and Pell-Lucas Numbers with Real Subscripts," 33(5):398-406.

HSU, L. C., "A Difference-Operational Approach to the Möbius Inversion Formulas," 33(2):169-173.

**HSU**, Leetsch Charles (coauthors: Peter Jau-shyong Shiue & Yi Wang), "Notes on a Conjecture of Singmaster," 33(5):392-397. **IZOTOV**, Anatoly S., "A Note on Sierpinski Numbers," 33(3):206-207.

JENNINGS, Derek (coauthor: Ray Melham), "On the General Linear Recurrence Relation," 33(2):142-146.

**JOO**, Mi-Kyung (coauthor: Lawrence Brenton), "On the System of Congruences  $\prod_{i\neq i} n_i \equiv 1 \mod n_i$ ," 33(3):258-267.

**JOYNER**, R. N. (coauthors: R. L. Creech & W. R. Spickerman), "On the (3, F) Generalizations of the Fibonacci Sequence," 33(1):9-12.

**KENNEDY**, Robert E. (coauthor: Curtis Cooper), "Proof of a Result by Jarden by Generalizing a Proof by Carlitz," 33(3):304-310

KHAN, M. A. (coauthor: Y. H. Harris Kwong), "Some Invariant and Minimum Properties of Stirling Numbers of the Second Kind," 33(3):203-205.

KIM, Jun Kyo (coauthor: Sang Geun Hahn), "A Note on Multiplicative Partitions of Bipartite Numbers," 33(3):283-288.

**KIMBALL**, William A. (coauthor: William A. Webb), "A Congruence for Fibonomial Coefficients Modulo  $p^3$ ," 33(4):290-297

**KIMBERLING**, Clark, "The Zeckendorf Array Equals the Wythoff Array," 33(1):3-8; "Conjectures Concerning Irrational Numbers and Integers," 33(3):208-210.

**KNOPFMACHER**, Arnold (coauthor: M. E. Mays), "Pierce Expansions of Ratios of Fibonacci and Lucas Numbers and Polynomials," 33(2):153-163.

KONVALINA, John, "Roots of Unity and Circular Subsets without Consecutive Elements," 33(5):412-414.

**KWONG**, Y. H. Harris (coauthor: M. A. Khan), "Some Invariant and Minimum Properties of Stirling Numbers of the Second Kind," 33(3):203-205.

LEE, Gwang-Yeon (coauthor: Sang-Gu Lee), "A Note on Generalized Fibonacci Numbers," 33(3):273-278.

LEE, Sang-Gu (coauthor: Gwang-Yeon Lee), "A Note on Generalized Fibonacci Numbers," 33(3):273-278.

**LEMKE**, Paul (coauthors: Edith H. Luchins, Russell Hendel, & David Tuller), "Linear Recurrences in Difference Triangles," 33(5):441-452.

LENGYEL, T., "The Order of the Fibonacci and Lucas Numbers," 33(3):234-239.

LEWIS, Richard, "Antisocial Dinner Parties," 33(4):368-370.

**LIZHOU**, Guo (coauthor: Zhang Zhizheng), "Recurrence Sequences and Bernoulli Polynomials of Higher Order," 33(4):359-362.

**LUCHINS**, Edith H. (coauthors: Russell Hendel, Paul Lemke, & David Tuller), "Linear Recurrences in Difference Triangles," 33(5):441-452.

MAYS, M. E. (coauthor: Arnold Knopfmacher), "Pierce Expansions of Ratios of Fibonacci and Lucas Numbers and Polynomials," 33(2):153-163.

McDANIEL, Wayne L., "Diophantine Representation of Lucas Sequences," 33(1):59-63.

MELHAM, Ray (coauthor: Derek Jennings), "On the General Linear Recurrence Relation," 33(2):142-146.

MELHAM, R. S. (coauthor: A. G. Shannon), "Some Infinite Series Summations Using Power Series Evaluated at a Matrix," 33(1):13-20; "Inverse Trigonometric and Hyperbolic Summation Formulas Involving Generalized Fibonacci Numbers," 33(1):43-40; "Some Summation Identities Using Generalized Q-Matrices," 33(1):64-73; "A Generalization of the Catalan Identity and Some Consequences," 33(1):82-84; "Generalizations of Some Simple Congruences," 33(2):126-130; "A Generalization of a Result of D'Ocagne," 33(2):135-138; "On Reciprocal Sums of Chebyshev Related Sequences," 33(3):194-202

**MENICOCCI**, Renato (coauthor Piero Filipponi), "Some Probabilistic Aspects of the Terminal Digits of Fibonacci Numbers," 33(4):325-331.

MOREE, Pieter (coauthor: Hans Roskam), "On an Arithmetical Function Related to Euler's Totient and the Discriminator," 33(4):332-340.

ORR, C. K. (coauthors: S. D. Balkin, D. S. Cousins, & C. A. Reiter), "Short Periods of Continued Fraction Convergents Modulo M: A Generalization of the Fibonacci Case," 33(3):222-233.

PAUTASSO, Alain (coauthor: François Dubeau), "On Triangular Rectangular Numbers," 33(3):244-248.

**PEDERSEN**, Jean (coauthors: Peter Hilton & Luc Vrancken), "On Certain Arithmetic Properties of Fibonacci and Lucas Numbers," 33(3):211-217.

PLA, Juan, "Some Conditions for "All or None" Divisibility of a Class of Fibonacci-Like Sequences," 33(5):464-465.

#### VOLUME INDEX

PRODINGER, Helmut, "Geometric Distributions and Forbidden Subwords," 33(2):139-141.

**RABINOWITZ**, Stanley (Ed.), Elementary Problems and Solutions, 33(1):85-90; 33(2):181-186; 33(4):372-377; 33(5): 466-471.

**REITER**, A. (coauthors: S. D. Balkin, D. S. Cousins, & C. K. Orr), "Short Periods of Continued Fraction Convergents Modulo *M*: A Generalization of the Fibonacci Case," 33(3):222-233.

ROBBINS, Neville, "A Note Regarding Continued Fractions," 33(4):311-312.

ROSKAM, Hans (coauthor: Pieter Moree), "On an Arithmetical Function Related to Euler's Totient and the Discriminator," 33(4):332-340.

ROTKIEWICZ, A. (coauthor: K. Ziemak), "On Even Pseudoprimes," 33(2):123-125.

SCHÖFFL, Gerd (coauthor: Herbert Glaser), "Ducci-Sequences and Pascal's Triangle," 33(4):313-324.

SHANNON, A. G. (coauthor: R. S. Melham), "Some Infinite Series Summations Using Power Series Evaluated at a Matrix," 33(1):13-20; "Inverse Trigonometric and Hyperbolic Summation Formulas Involving Generalized Fibonacci Numbers," 33(1):43-40; "Some Summation Identities Using Generalized Q-Matrices," 33(1):64-73; "A Generalization of the Catalan Identity and Some Consequences," 33(1):82-84; "Generalizations of Some Simple Congruences," 33(2):126-130; "A Generalization of a Result of D'Ocagne," 33(2):135-138; "On Reciprocal Sums of Chebyshev Related Sequences," 33(3):194-202.

SHARPE, David (coauthor: Robert Cook), "Sums of Arithmetic Progressions," 33(3):218-221.

**SHI**, Xiquan, "Concerning the Recursive Sequence  $A_{n+k} = \sum_{i=1}^k a_i A_{n+i-1}^{\alpha_i}$ ," 33(3):240-243.

SHIUE, Peter Jau-shyong (coauthor: Tom C. Brown), "Squares of Second-Order Linear Recurrence Sequences," 33(4):352-356; (coauthors: Leetsch Charles Hsu & Yi Wang), "Notes on a Conjecture of Singmaster," 33(5):392-397.

SPICKERMAN, W. R. (coauthors: R. L. Creech & R. N. Joyner), "On the (3, F) Generalizations of the Fibonacci Sequence," 33(1):9-12.

SUBRAMANIAN, P. R., "Nonzero Zeros of the Hermite Polynomials Are Irrational," 33(2):131-134.

TULLER, David (coauthors: Edith H. Luchins, Russell Hendel, & Paul Lemke), "Linear Recurrences in Difference Triangles," 33(5):441-452.

VIVEROS, Roman (coauthors: K. Balasubramanian & N. Balakrishnan), "Some Discrete Distributions Related to Extended Pascal Triangles," 33(5):415-425.

VRANCKEN, Luc (coauthors: Peter Hilton & Jean Pedersen), "On Certain Arithmetic Properties of Fibonacci and Lucas Numbers," 33(3):211-217.

WANG, Jun, "On the k<sup>th</sup> Derivative Sequences of Fibonacci and Lucas Polynomials," 33(2):174-178; (coauthors: Leetsch Charles Hsu & Peter Jau-shyong Shiue), "Notes on a Conjecture of Singmaster," 33(5):392-397.

**WEBB**, William A. (coauthor: William A. Kimball), "A Congruence for Fibonomial Coefficients Modulo  $p^3$ ," 33(4):290-297.

WEBSTER, Roger, "A Combinatorial Problem with a Fibonacci Solution," 33(1):26-31.

WHITNEY, Raymond E. (Ed.), Advanced Problems and Solutions, 33(1):91-96, 33(2):187-192, 33(4):378-384, 472-477.

YOUNG, Anne Ludington, "The Switch, Subtract, Reorder Routine," 33(5):432-440.

YOUNG, Paul Thomas, "Quadratic Reciprocity Via Lucas Sequences," 33(1):78-81.

ZHIZHENG, Zhang (coauthor: Guo Lizhou), "Recurrence Sequences and Bernoulli Polynomials of Higher Order," 33(4):359-362

ZIEMAK, K. (coauthor: A. Rotkiewicz), "On Even Pseudoprimes," 33(2):123-125.

# SUSTAINING MEMBERS

*H.L. Alder	M.J. DeLeon	R.E. Kennedy	J.A. Schumaker
G.L. Alexanderson	J. De Kerf	C.H. Kimberling	A.G. Shannon
P.G. Anderson	L.A.G. Dresel	Y.H.H. Kwong	L.W. Shapiro
S. Ando	U. Dudley	J. Lahr	J.R. Siler
R. Andre-Jeannin	M. Faccio	J.C. Lagarias	D. Singmaster
*J. Arkin	D.R. Farmer	B. Landman	J. Sjoberg
C. Ashbacher	D.C. Fielder	L.H. Lange	L. Somer
M.K. Azarian	P. Filipponi	K.W. Lok	P. Spears
N. Balasubramania	Fondazione Ugo Bordoni	* C.T. Long	W.R. Spickerman
L. Bankoff	Emerson Frost	G. Lord	Paul K. Stockmeyer
J.G. Bergart	Anthony Gioia	* J. Maxwell	J. Suck
G. Bergum	*H.W. Gould	F.U. Mendizabal	M.N.S. Swamy
G. Berzsenyi	P. Hagis, Jr.	J.L. Miller	*D. Thoro
*M. Bicknell-Johnson	H. Harborth	M.G. Monzingo	J.C. Turner
P.S. Bruckman	P. Haukkanen	J.F. Morrison	T.P. Vaughan
M.F. Bryn	* A.P. Hillman	K. Nagasaka	J.N. Vitale
G.D. Chakerian	*A.F. Horadam	S.A. Obaid	M. Waddill
W.V. Chappelow	Y. Horibe	S. Palsson	*L.A. Walker
C. Chouteau	F.T. Howard	J. Pla	J.E. Walton
C.K. Cook	R.J. Howell	A. Prince	W.A. Webb
R.L. Creech	S. Howell	S. Rabinowitz	G.E. Weekly
J.W. Creely	J.P. Jones	I. Sadoveanu	R.E. Whitney
M.G. DeBruin	R.N. Joyner	S. Sato	B.E. Williams
		*	*Charter Members

# **INSTITUTIONAL MEMBERS**

CALIFORNIA STATE UNIVERSITY SACRAMENTO

Sacramento, California

CAREY VIGOR-ZIERK, M.D.

Santa Ana, California

ETH-BIBLIOTHEK

Zurich, Switzerland

**GONZAGA UNIVERSITY** 

Spokane, Washington

**HOLY NAME COLLEGE** 

Oakland, California

HOWELL ENGINEERING COMPANY

Bryn Mawr, California

INDIANA UNIVERSITY

Bloomington, Indiana

KLEPCO, INC.

Sparks, Nevada

LAURENTIAN UNIVERSITY

Sudbury, Ontario, Canada

MISSOURI SOUTHERN STATE COLLEGE

Joplin, Missouri

NATIONAL LIBRARY OF EDUCATION

Copenhagen, Denmark

SAN JOSE STATE UNIVERSITY

San Jose, California

SANTA CLARA UNIVERSITY

Santa Clara, California

UNIVERSITY OF NEW ENGLAND

Armidale, N.S.W. Australia

UNIVERSITY OF TECHNOLOGY

Sydney, N.S.W. Australia

WAKE FOREST UNIVERSITY

Winston-Salem, North Carolina

WASHINGTON STATE UNIVERSITY

Pullman, Washington

YESHIVA UNIVERSITY

New York, New York

JOVE STATISTICAL TYPING SERVICE 2088 Orestes Way Campbell, California 95008

# BOOKS AVAILABLE THROUGH THE FIBONACCI ASSOCIATION

Introduction to Fibonacci Discovery by Brother Alfred Brousseau. Fibonacci Association (FA), 1965.

Fibonacci and Lucas Numbers by Verner E. Hoggatt, Jr. FA, 1972.

- A Primer for the Fibonacci Numbers. Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1972.
- Fibonacci's Problem Book. Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1974.
- The Theory of Simply Periodic Numerical Functions by Edouard Lucas. Translated from the French by Sidney Kravitz. Edited by Douglas Lind. FA, 1969.
- Linear Recursion and Fibonacci Sequences by Brother Alfred Brousseau. FA, 1971.
- Fibonacci and Related Number Theoretic Tables. Edited by Brother Alfred Brousseau. FA, 1972.
- Number Theory Tables. Edited by Brother Alfred Brousseau. FA, 1973.
- Tables of Fibonacci Entry Points, Part One. Edited and annotated by Brother Alfred Brousseau. FA, 1965.
- Tables of Fibonacci Entry Points, Part Two. Edited and annotated by Brother Alfred Brousseau. FA, 1965.
- A Collection of Manuscripts Related to the Fibonacci Sequence—18th Anniversary Volume. Edited by Verner E. Hoggatt, Jr. and Marjorie Bicknell-Johnson. FA, 1980.
- Applications of Fibonacci Numbers, Volumes 1-5. Edited by G.E. Bergum, A.F. Horadam and A.N. Philippou
- Generalized Pascal Triangles and Pyramids Their Fractals, Graphs and Applications by Boris A. Bondarenko. Translated from the Russian and edited by Richard C. Bollinger, FA, 1993.

Please write to the Fibonacci Association, Santa Clara University, Santa Clara CA 95053, U.S.A., for more information and current prices.