

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

TABLE OF CONTENTS

	VOLUME 34 AUGUST 1996 NUMBE	R4
1		
	Advanced Problems and Solutions Edited by Raymond E. Whitney	379
	Elementary Problems and Solutions Edited by Stanley Rabinowitz	373
	P-Latin Matrices and Pascal's Triangle Modulo a Prime Valery V. Karachik	362
	On Sequences Related to Expansions of Real Numbers E. Vantieghem	356
	On the Sums of Digits of Fibonacci Numbers David C. Terr	349
	Polynomials Associated with Generalized Morgan-Voyce Polynomials	342
	Sixth International Conference Proceedings	341
	Some Interesting Subsequences of the Fibonacci and Lucas Pseudoprimes Paul S. Bruckman	332
	On a Binomial Sum for the Fibonacci and Related Numbers	326
	A Ten Point FFT Calculation Which Features the Golden Ratio	323
	On the Limit of Generalized Golden Numbers	320
	Recurrence Sequences and Nörlund-Euler Polynomials Wang Tianming and Zhang Zhizheng	314
	Author and Title Index for Sale	313
	Fibonacci Partitions Neville Robbins	306
	On the Stability of Certain Lucas Sequences Modulo 2 ^k	298
	Book Announcement: Fibonacci Entry Points and Periods for Primes 100,003 through 415,993 A Monograph by Daniel C. Fielder and Paul S. Bruckman	297
	GCD and LCM Power Matrices Shen Ze Chun	290

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.sdstate.edu/~wcsc/http/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, SAN-TA 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.

> ©1996 by The Fibonacci Association All rights reserved, including rights to this journal issue as a whole and, except where otherwise noted, rights to each individual contribution.

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 University, Durham, NC 27708-0251 BART GODDARD, East Texas State University, Commerce, TX 75429-3011 HENRY W. GOULD, West Virginia University, Morgantown, WV 26506-0001 HEIKO HARBORTH, Tech. Univ. Carolo Wilhelmina, Braunschweig, Germany A.F. HORADAM, University of New England, Armidale, N.S.W. 2351, Australia CLARK KIMBERLING, University of Evansville, Evansville, IN 47722-0001 STEVE LIGH, Southeastern Louisiana University, Hammond, LA 70402 RICHARD MOLLIN, University of Calgary, Calgary T2N 1N4, Alberta, Canada GARY L. MULLEN, The Pennsylvania State University, University Park, PA 16802-6401 HAROLD G. NIEDERREITER, Institute for Info. Proc., A-1010, Vienna, Austria 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

GCD AND LCM POWER MATRICES

Shen Ze Chun

An-Gang Engineering College, Anshan, P.R. China, 114001 (Submitted October 1994)

1. INTRODUCTION

Let $S = \{x_1, x_2, ..., x_n\}$ be a set of distinct positive integers. By (x_i, x_j) and $[x_i, x_j]$, we denote the greatest common divisor (GCD) and the least common multiple (LCM) of x_i and x_j , respectively.

The matrix (S) (resp. [S]) having (x_i, x_j) (resp. $[x_i, x_j]$) as its *i*, *j*-entry is called the GCD (resp. LCM) matrix defined on S.

A set is called factor-closed if it contains every divisor of each of its members. A set S is gcd-closed if $(x_i, x_j) \in S$ for any i and j $(1 \le i, j \le n)$.

Smith [6] and Beslin and Ligh [3] discussed (S) and det(S), the determinant of (S). They proved that det(S) = $\phi(x_1) \dots \phi(x_n)$, where ϕ is Euler's totient, if S is factor-closed. Beslin and Ligh [4] gave a formula for det(S) when S is gcd-closed.

Smith [6] and Beslin [2] considered the LCM matrix [S] when S is factor-closed. In 1992, Boueque and Ligh [1] gave a formula for det[S] when S is gcd-closed. They also obtained formulas for $(S)^{-1}$ and $[S]^{-1}$, the inverses of (S) and [S].

Let r be a real number. The matrix $(S^r) = (a_{ij})$, where $a_{ij} = (x_i, x_j)^r$, is called the GCD power matrix defined on S; the matrix $[S^r] = (b_{ij})$, where $b_{ij} = [x_i, x_j]^r$, is called the LCM power matrix defined on S.

In this paper the results mentioned above are generalized by giving formulas for (S^r) , $[S^r]$, det (S^r) , and det $[S^r]$ on factor-closed sets and gcd-closed sets, respectively. Making use of the Möbius matrix, which is a generalization of the Möbius function μ , we shall give the inverse matrices of (S^r) and $[S^r]$.

All known results about (S) and [S] are just the particular cases of the theory of (S^r) and $[S^r]$ on condition that r = 1.

One of the problems raised by Beslin [2] are solved. Some conjectures are put forward.

2. JORDAN'S TOTIENT

For any positive integer *n* and real *r*, we define

$$J_r(n) = n^r \prod_{p|n} \left(1 - \frac{1}{p^r}\right).$$

The function J_r is usually called *Jordan's totient*.

Theorem 1: If $n \ge 1$ and r is real, then

$$\sum_{d|n} J_r(d) = n^r .$$
(2.1)

290

AUG.

Proof: By the definition of J_r , when $n = p_1^{a_1} \dots p_k^{a_k}$,

$$J_r(n) = n^r \left(1 - \frac{1}{p_1^r} \right) \dots \left(1 - \frac{1}{p_k^r} \right) = n^r \sum_{d|n} \frac{\mu(d)}{d^r} = \sum_{d|n} \mu(d) \left(\frac{n}{d} \right)^r.$$
(2.2)

Equation (2.2) and the Möbius inversion formula give (2.1). \Box

3. MÖBIUS MATRICES

Let
$$S = \{x_1, ..., x_n\}$$
 be ordered by $x_1 < x_2 < \cdots < x_n$. We define $U = (u_{ij})$, where

$$u_{ij} = \begin{cases} 1 & \text{if } x_i | x_j, \\ 0 & \text{otherwise.} \end{cases}$$
(3.1)

Our purpose is to find $M = (\mu_{ij}) = U^{-1}$. As S is ordered, U is an upper triangular matrix. It is well known that the inverse of an upper triangular matrix is also an upper triangular matrix. Hence,

$$\mu_{ij} = \mu(x_i, x_j) = 0, \text{ if } i > j \ (i.e., x_i > x_j).$$
(3.2)

Since $M = U^{-1}$, we have $\sum_{k=1}^{n} u_{ik} u_{kj} = \delta_{ij}$. Using (3.1),

$$\sum_{x_k|x_j}^{n} \mu(x_i, x_k) = \delta_{ij}.$$
 (3.3)

When i = j, by (3.2) and (3.3), we have

$$\mu(x_i, x_i) = 1 \quad (i = 1, 2, ..., n). \tag{3.4}$$

When i < j, by (3.3), we have

$$\mu_{ij} = \mu(x_i, x_j) = -\sum_{\substack{x_k \mid x_j \\ x_k < x_i}} \mu(x_i, x_k).$$
(3.5)

Theorem 2: Function $\mu(x, y)$ is multiplicative.

Proof: $\mu(x, y)$ may be written as $\mu(p_1^{a_1} \dots p_s^{a_s}, p_1^{b_1} \dots p_s^{b_s})$, where $a_i \ge 0$, $b_i \ge 0$, but $a_i + b_i > 0$, $i = 1, 2, \dots, s$. First, for any $a_i \ge 0$ ($i = 1, 2, \dots, s$), by (3.2) and (3.4), we have

$$\mu(p_1^{a_1} \dots p_s^{a_s}, 1) = \mu(p_1^{a_1}, 1) \dots \mu(p_s^{a_s}, 1).$$
(3.6)

Next, we make an inductive hypothesis:

$$\mu(p_1^{a_1} \dots p_s^{a_s}, p_1^{i_1} \dots p_s^{i_s}) = \mu(p_1^{a_1}, p_1^{i_1}) \dots \mu(p_s^{a_s}, p_s^{i_s}),$$
(3.7)

for $(0, ..., 0) \le (i_1, ..., i_s) < (b_1, ..., b_s)$, which may be abbreviated $(0) \le (i) < (b)$.

Note that $(i_1, \ldots, i_s) = (b_1, \ldots, b_s)$ means $i_k = b_k$, $k = 1, 2, \ldots, s$; $(i_1, \ldots, i_s) < (b_1, \ldots, b_s)$ means $i_k \le b_k$, and there exists at least a t such that $i_t < b_t$ $(1 \le t \le s)$.

When $(a) \neq (b)$, by (3.5) and (3.7), we have

1996]

GCD AND LCM POWER MATRICES

$$\begin{split} \mu(p_1^{a_1} \dots p_s^{a_s}, \ p_1^{b_1} \dots p_s^{b_s}) &= -\sum_{(0) \le (i) < (b)} \mu(p_1^{a_1} \dots p_s^{a_s}, \ p_1^{i_1} \dots p_s^{i_s}) \\ &= -\sum_{(0) \le (i) < (b)} \mu(p_1^{a_1}, p_1^{i_1}) \cdots (p_s^{a_s}, p_s^{i_s}) \\ &= \left[\binom{s}{s} (-1)^s + \binom{s}{s-1} (-1)^{s-1} + \dots + \binom{s}{1} (-1)^1 \right] \mu(p_1^{a_1}, p_1^{b_1}) \cdots (p_s^{a_s}, p_s^{b_s}) \\ &= -[(1-1)^s - 1] \mu(p_1^{a_1}, p_1^{b_1}) \cdots (p_s^{a_s}, p_s^{b_s}) \\ &= \mu(p_1^{a_1}, p_1^{b_1}) \cdots (p_s^{a_s}, p_s^{b_s}). \end{split}$$

In summing, we consider all combinatorial possibilities of $0 \le i_k < b_k$ and $i_k = b_k$ satisfying $(0) \le (i) < (b)$; also,

$$\sum_{0 \le i_k < b_k} \mu(p_k^{a_k}, p_k^{i_k}) = -\mu(p_k^{a_k}, p_k^{b_k})$$

has been used.

When (a) = (b), by (3.4), we have

$$\mu(p_1^{a_1} \dots p_s^{a_s}, p_1^{b_1} \dots p_s^{b_s}) = 1 = \mu(p_1^{a_1}, p_1^{b_1}) \dots \mu(p_s^{a_s}, p_s^{b_s}). \quad \Box$$

Theorem 3: The generalized Möbius function

$$u(x, y) = \begin{cases} (-1)^s & \text{if } \frac{y}{x} = p_1 \dots p_s, \ s > 0, \\ 1 & \text{if } x = y, \\ 0 & \text{otherwise.} \end{cases}$$

Proof: Let p be a prime. By (3.2), (3.4), and (3.5),

$$\mu(p^m, p^n) = 0, \text{ if } m > n; \quad \mu(p^m, p^m) = 1;$$

$$\mu(p^m, p^{m+1}) = -\mu(p^m, p^m) = -1.$$

When $k \ge 2$, we have

$$\mu(p^{m}, p^{m+k}) = -\sum_{0 \le i < k} \mu(p^{m}, p^{m+i})$$
$$= -\sum_{0 \le i < k-1} \mu(p^{m}, p^{m+i}) - \mu(p^{m}, p^{m+k-1})$$
$$= \mu(p^{m}, p^{m+k-1}) - \mu(p^{m}, p^{m+k-1}) = 0.$$

These results and Theorem 2 complete the proof. \Box

4. GCD POWER MATRICES ON FACTOR-CLOSED SETS

Let $S = \{x_1, x_2, ..., x_n\}$ be an ordered set of distinct positive integers, and $\overline{S} = \{y_1, y_2, ..., y_m\}$, which is ordered by $y_1 < y_2 < \cdots < y_m$, be a minimal factor-closed set containing S. We call \overline{S} the factor-closed closure of S.

Theorem 4: Let $S = \{x_1, ..., x_n\}$ be an ordered set of distinct positive integers, and $\overline{S} = \{y_1, ..., y_m\}$ the factor-closed closure of S. Then the GCD power matrix on S, i.e.,

292

$$(S^r) = E^T G_r E, (4.1)$$

where

$$G_r = \text{diag}(J_r(y_1), ..., J_r(y_m)),$$
 (4.2)

$$E = (e_{ij}), \quad e_{ij} = \begin{cases} 1 & \text{if } y_i | x_j, \\ 0 & \text{otherwise.} \end{cases}$$
(4.3)

Proof: By (2.1), we have

$$(E^{t}G_{r}E)_{ij} = \sum_{k=1}^{m} e_{ki}J_{r}(y_{k})e_{kj} = \sum_{\substack{y_{k} \mid x_{i} \\ y_{k} \mid x_{j}}} J_{r}(y_{k}) = \sum_{\substack{y_{k} \mid (x_{i}, x_{j}) \\ y_{k} \mid x_{j}}} J_{r}(y_{k})$$
$$= \sum_{d \mid (x_{i}, x_{j})} J_{r}(d) = (x_{i}, x_{j})^{r} = (S^{r})_{ij}.. \quad \Box$$

Theorem 5: Let S be factor-closed, then we have

$$\det(S^r) = J_r(x_1) \dots J_r(x_n). \tag{4.4}$$

Proof: When S is factor-closed, $S = \overline{S}$, and the matrix E is equal to U, which is defined as (3.1), and is a triangular matrix with the diagonal (1, 1, ..., 1). We have

$$\det(S^r) = (\det U)^2 \det G_r = \det G_r = J_r(x_1) \dots J_r(x_n). \quad \Box$$

When S is arbitrary, $det(S^r)$ can be calculated by the Cauchy-Binet formula [8]. We omit this here for succinctness.

Remark 1: Letting r = 1 in (4.4), we obtain the well-known results of Smith [6] and of Beslin and Ligh [3]:

$$\det(S) = J_1(x_1) \dots J_1(x_n) = \phi(x_1) \dots \phi(x_n).$$

Remark 2: By (4.1), we have the reciprocal GCD power matrix

$$(S^{-r}) = E^T G_{-r} E \,. \tag{4.5}$$

Hence, if S is factor-closed, we have

$$\det(S^{-r}) = J_{-r}(x_1) \dots J_{-r}(x_n), \tag{4.6}$$

$$\det(S^{-1}) = J_{-1}(x_1) \dots J_{-1}(x_n). \tag{4.7}$$

In fact, (4.7) is exactly Corollary 1 of Beslin [2]. It is evident that the function g(n) introduced by Beslin in [2] and by Bourque and Ligh in [1] is none other than Jordan's totient function $J_{-1}(n)$.

5. LCM POWER MATRICES ON FACTOR-CLOSED SETS

In this section, we shall turn our attention to the LCM power matrix.

Theorem 6: Let S and \overline{S} be defined as in Theorem 4. Then we have the LCM power matrix

$$[S^r] = D_r E^T G_{-r} E D_r, \tag{5.1}$$

1996]

where

$$D_r = \text{diag}(x_1^r, ..., x_n^r), \tag{5.2}$$

 G_{-r} and E are defined by (4.2) and (4.3).

Proof: By (4.5), we have

$$(D_{r}E^{T}G_{-r}ED_{r})_{ij} = (D_{r}(S^{-r})D_{r})_{ij} = x_{i}^{r}(S^{-r})_{ij}x_{j}^{r}$$
$$= \frac{x_{i}^{r}x_{j}^{r}}{(x_{i}, x_{j})^{r}} = [x_{i}, x_{j}]^{r} = [S^{r}]_{ij}. \quad \Box$$

Theorem 7: If S is factor-closed, then the determinant

$$det[S^{r}] = x_{1}^{2r} \dots x_{n}^{2r} J_{-r}(x_{1}) \dots J_{-r}(x_{n})$$

= $J_{r}(x_{1}) \dots J_{r}(x_{n}) \pi_{r}(x_{1}) \dots \pi_{r}(x_{n}),$ (5.3)

where π_r is multiplicative and for the prime power p^m , $\pi_r(p^m) = -p^r$.

Proof: By (5.1) and the fact that E = U, we have

det[
$$S^r$$
] = $\prod_{i=1}^n x_i^{2r} J_{-r}(s_i)$ and $x_i^{2r} J_{-r}(x_i) = J_r(x_i) \pi_r(x_i)$.

This completes the proof. \Box

Remark 3: Letting r = 1 in (5.3), we shall have Corollary 3 of Beslin [2] immediately.

On the basis of (4.4) and (5.3), we have

Theorem 8: If S is factor-closed, then

$$\frac{\det[S^r]}{\det(S^r)} = \prod_{i=1}^n \pi_r(x_i), \tag{5.4}$$

$$\frac{\det[S]}{\det(S)} = \prod_{i=1}^{n} \pi(x_i), \tag{5.5}$$

where $\pi(n)$ is multiplicative, and $\pi(p^k) = -p$, for the prime power p^k .

Remark 4: By (5.4) and (5.5), we know that [S] and $[S^r]$ are not positive definite.

Remark 5: Let $\omega(x)$ denote the number of distinct prime factors of x, and $\Omega = \omega(x_1) + \dots + \omega(x_n)$. By Theorem 8, we know that det[S] and det[S^r] are positive, if Ω is even; they are negative if Ω is odd, for factor-closed S. This solves the second of the problems put forward by Beslin in [2].

6. INVERSES OF (S') AND [S'] ON FACTOR-CLOSED SETS

In Section 3, we obtained $M = (\mu(x_1, x_j)) = U^{-1}$. Now we shall give $(S^r)^{-1}$ and $[S^r]^{-1}$, the inverses of (S^r) and $[S^r]$, respectively.

[AUG.

GCD AND LCM POWER MATRICES

Theorem 9: Let S be factor-closed, then $(S^r)^{-1} = (a_{ij})$ and $[S^r]^{-1} = (b_{ij})$, where

$$a_{ij} = \sum_{[x_i, x_j] \mid x_k} \frac{\mu(x_i, x_k) \mu(x_j, x_k)}{J_r(x_k)};$$
(6.1)

$$b_{ij} = \sum_{[x_i, x_j]|x_k} \left(\frac{x_k}{x_i}\right)^r \left(\frac{x_k}{x_j}\right)^r \frac{\mu(x_i, x_k)\mu(x_j, x_k)}{J_r(x_k)\pi_r(x_k)}.$$
(6.2)

Proof: When S is factor-closed, we have E = U. By (4.1),

$$a_{ij} = (U^{-1}G_r^{-1}(U^{-1})^T)_{ij} = (MG_r^{-1}M^T)_{ij}$$

= $\sum_{k=1}^n \mu_{ik} (J_r(x_k))^{-1} \mu_{jk} = \sum_{[x_i, x_j] \mid x_k} \frac{\mu(x_i, x_k)\mu(x_j, x_k)}{J_r(x_k)}.$

By (5.2), we have

$$\begin{split} b_{ij} &= (D_r^{-1}U^{-1}G_{-r}^{-1}(U^{-1})^T D_r^{-1})_{ij} = (D_r^{-1}MG_{-r}^{-1}M^T D_r^{-1})_{ij} \\ &= \sum_{k=1}^n x_i^{-r} \mu_{ik} (J_{-r}(x_k))^{-1} \mu_{jk} x_j^{-r} = \frac{1}{x_i^r x_j^r} \sum_{\substack{x_i \mid x_k \\ x_j \mid x_k}} \frac{\mu(x_i, x_k) \mu(x_j, x_k)}{J_{-r}(x_k)} \\ &= \sum_{[x_i, x_j] \mid x_k} \left(\frac{x_k}{x_i} \right)^r \left(\frac{x_k}{x_j} \right)^r \frac{\mu(x_i, x_k) \mu(x_j, x_k)}{J_r(x_k) \pi_r(x_k)}. \quad \Box \end{split}$$

Remark 6: Theorem 9 is a generalization of Theorems 1 and 2 of Bourque and Ligh [1].

7. (S') AND [S'] ON GCD-CLOSED SETS

Let $\alpha_r(x_i)$, i = 1, 2, ..., n, be defined by

$$\alpha_r(x_i) = \sum_{\substack{d \mid x_i \\ d \nmid x_i \\ x_i < x_i}} J_r(d).$$
(7.1)

Using the principle of cross-classification [7] and (2.1), we can prove

Theorem 10: Let $S = \{x_1, x_2, ..., x_n\}$ be ordered by $x_1 < x_2 < \cdots < x_n$ and let $\alpha_r(x_i)$ be defined by (7.1). Then

$$\alpha_r(x_i) = x_i^r - \sum_{1 \le j < 1} (x_j, x_i)^r + \sum_{1 \le j < k < i} (x_j, x_k, x_i)^r - \dots + (-1)^{i-1} (x_1, x_2, \dots, x_i)^r, \quad i = 1, \dots, n.$$
(7.2)

Theorem 11: Let S be gcd-closed, then

$$(S^r) = U^T A_r U, \tag{7.3}$$

$$[S^r] = D_r U^T A_{-r} U D_r, \tag{7.4}$$

where $A_r = \text{diag}(\alpha_r(x_1), \dots, \alpha_r(x_n))$, U and D_r are defined in (3.1) and (5.2), respectively.

1996]

Proof: The proof of (7.3) is simple. We shall prove only (7.4).

$$(D_{r}U^{T}A_{-r}UD_{r})_{ij} = \sum_{k=1}^{n} x_{i}^{r}u_{ki}\alpha_{-r}(x_{k})u_{kj}x_{j}^{r} = x_{i}^{r}x_{j}^{r}\sum_{\substack{x_{k}\mid x_{i}\\x_{k}\mid x_{j}}} \alpha_{-r}(x_{k})$$
$$= x_{i}^{r}x_{j}^{r}\sum_{\substack{x_{k}\mid(x_{i},x_{j})\\x_{k}
$$= x_{i}^{r}x_{j}^{r}/(x_{i},x_{j})^{r} = [x_{i},x_{j}]^{r} = [S^{r}]_{ij}. \quad \Box$$$$

On the basis of Theorem 11, it is easy to prove

Theorem 12: Let *S* be gcd-closed, then

$$\det(S^r) = \prod_{i=1}^n \alpha_r(x_i), \tag{7.5}$$

$$\det[S^r] = \prod_{i=1}^n x_i^{2r} \alpha_{-r}(x_i).$$
(7.6)

Remark 7: Letting r = 1, equation (7.5) becomes Corollary 1 of Beslin and Ligh [4] and equation (7.6) becomes Theorem 5 of Bourque and Ligh [1].

8. INVERSES OF (S') AND [S'] ON GCD-CLOSED SETS

When S is gcd-closed, the inverse matrices $(S^r)^{-1}$ and $[S^r]^{-1}$ can be derived easily from Theorem 11. For future reference, we present the formulas without proof.

Theorem 13: Let S be gcd-closed, then

$$(S^r)^{-1} = (c_{ij})$$
 and $[S^r]^{-1} = (d_{ij})$,

where

.

$$c_{ij} = \sum_{[x_i, x_j] | x_k} \frac{\mu(x_i, x_k) \mu(x_j, x_k)}{\alpha_r(x_k)},$$
(8.1)

$$d_{ij} = \frac{1}{x_i^r x_j^r} \sum_{[x_i, x_j] \mid x_k} \frac{\mu(x_i, x_k) \mu(x_j, x_k)}{\alpha_{-r}(x_k)}.$$
(8.2)

Remark 8: We make the following conjectures, which are similar to the conjecture of Bourque and Ligh [1]:

- 1. If S is gcd-closed and $r \neq 0$, the LCM power matrix $[S^r]$ is invertible.
- 2. Let $S = \{x_1, x_2, ..., x_n\}$ be an ordered set of distinct positive integers and $r \neq 0$, then

$$\frac{1}{x_n^r} - \sum_{1 \le i < n} \frac{1}{(x_i, x_n)^r} + \sum_{1 \le i < j < n} \frac{1}{(x_1, x_j, x_n)^r} - \dots + (-1)^{n-1} \frac{1}{(x_1, x_2, \dots, x_n)^r} \neq 0$$

296

GCD AND LCM POWER MATRICES

3. Let $A = \{a_1, a_2, \dots, a_n\}$ be a set of distinct positive integers and $a_i > 1$ $(i = 1, \dots, n), r \neq 0$, then

$$1 - \sum_{1 \le i \le n} a_i^r + \sum_{1 \le i < j \le n} [a_i, a_j]^r - \dots + (-1)^n [a_1, \dots, a_n]^r \neq 0.$$

REFERENCES

- 1. K. Bourque S. Ligh. "On GCD and LCM Matrices." *Linear Algebra Appl.* 174 (1992):65-74.
- 2. S. Beslin. "Reciprocal GCD Matrices and LCM Matrices." *The Fibonacci Quarterly* 29.3 (1991):271-74.
- 3. S. Beslin & S. Ligh. "Greatest Common Divisor Matrices." *Linear Algebra Appl.* **118** (1989): 69-75.
- 4. S. Beslin & S. Ligh. "GCD-Closed Sets and the Determinants of GCD Matrices." The Fibonacci Quarterly 30.2 (1992):157-60.
- 5. Z. Li. "The Determinants of GCD Matrices." Linear Algebra Appl. 134 (1990):137-43.
- 6. H. J. S. Smith. "On the Value of a Certain Arithmetical Determinant." *Proc. London Math.* Soc. 7 (1875-1876):208-12.
- 7. T. M. Apospol. Introduction to Analytic Number Theory. New York: Springer-Verlag, 1976.
- 8. R. A. Horn & C. R. Johnson. *Matrix Analysis*. Cambridge: Cambridge University Press, 1985.

AMS Classification Numbers: 15A36, 15A15, 11C20

*** *** ***

FIBONACCI ENTRY POINTS AND PERIODS FOR PRIMES 100,003 THROUGH 415,993

A Monograph

by Daniel C. Fielder and Paul S. Bruckman Members, The Fibonacci Association

In 1965, Brother Alfred Brousseau, under the auspices of The Fibonacci Association, compiled a twovolume set of Fibonacci entry points and related data for the primes 2 through 99,907. This set is currently available from The Fibonacci Association as advertised on the back cover of *The Fibonacci Quarterly*. Thirty years later, this new monograph complements, extends, and triples the volume of Brother Alfred's work with 118 table pages of Fibonacci entry-points for the primes 100,003 through 415,993.

In addition to the tables, the monograph includes 14 pages of theory and facts on entry points and their periods and a complete listing with explanations of the *Mathematica* programs use to generate the tables. As a bonus for people who must calculate Fibonacci and Lucas numbers of all sizes, instructions are available for "stand-alone" application of a fast and powerful Fibonacci number program which outclasses the stock Fibonacci programs found in *Mathematica*. The Fibonacci portion of this program appears through the kindness of its originator, Dr. Roman Maeder, of ETH, Zürich, Switzerland.

The price of the book is \$20.00; it can be purchased from the Subscription Manager of *The Fibonacci Quarterly* whose address appears on the inside front cover of the journal.

ON THE STABILITY OF CERTAIN LUCAS SEQUENCES MODULO 2^k

Walter Carlip and Eliot Jacobson

Ohio University, Athens, OH 45701 (Submitted February 1995)

1. INTRODUCTION

Let $\{u_i | i \in \mathbb{N}\}$ be the two-term recurrence sequence defined by $u_0 = 0$, $u_1 = 1$, and $u_i = au_{i-1} + bu_{i-2}$ for all $i \ge 2$, where a and b are fixed integers. Let m be an integer and consider the corresponding sequence $\{\overline{u}_i\}$, where $\overline{u}_i \in \mathbb{Z} / m\mathbb{Z}$ is obtained via the natural projection $\mathbb{Z} \to \mathbb{Z} / m\mathbb{Z}$.

It is well known that $\{\overline{u}_i\}$ is eventually periodic and, if b is relatively prime to m, such a sequence is purely periodic (see, e.g., [3] or [10]). We will designate by $\lambda(m) = \lambda_{a,b}(m)$ the length of the (shortest) period of $\{\overline{u}_i\}$, and for each $r \in \mathbb{Z}$, we define $\nu(m, r) = \nu_{a,b}(m, r)$ to be the number of occurrences of the residue r (mod m) in one such period. We also define $\Omega(m) = \Omega_{a,b}(m) = \{\nu_{a,b}(m, r) | r \in \mathbb{Z}\}$.

The sequence $\{u_i\}$ is said to be *uniformly distributed* modulo *m* if each residue modulo *m* appears an equal number of times in each period, that is, if $|\Omega(m)| = 1$. The sequence $\{u_i\}$ is said to be *stable* modulo the prime *p* if there is a positive integer *N* such that $\Omega(p^k) = \Omega(p^N)$ for all $k \ge N$. If *N* is the least such integer, we say that stability *begins* at *N*.

Interest in the stability of two-term recurrence sequences developed from the investigation of the uniform distribution of the Fibonacci sequence. A flurry of papers in the early 1970s culminated in the complete characterization of those integers modulo which a two-term recurrence sequence is uniformly distributed. A thorough exposition can be found in [5].

The subject lay dormant until the ground-breaking work of Schinzel [7], who classified the sets $\Omega_{a,1}(p)$ for odd primes p. Pihko extended Schinzel's work to cover some additional two-term recurrence sequences in [6], and Somer explored and extended Schinzel's work in [8] and [9]. In 1992, Jacobson [4] investigated the distribution of the Fibonacci sequence modulo powers of 2 and discovered that the Fibonacci sequence is stable modulo 2. He used this stability to compute $v_{1,1}(2^k, r)$, for all $k \in \mathbb{N}$ and $r \in \mathbb{Z}$.

In the present work we explicitly compute $v_{a,b}(2^k, r)$ for all $k \ge 5$ and all integers r, whenever a is odd and $b \equiv 1 \pmod{16}$. We will show that $\{u_i\}$ is stable in this case, and that Jacobson's result for the Fibonacci sequence is archetypal for this situation.

Theorem 1.1: Assume that a is odd and $b \equiv 1 \pmod{16}$. Then, for all $k \ge 5$,

 $\nu(2^{k}, r) = \begin{cases} 1 & \text{if } r \equiv 3 \pmod{4}, \\ 2 & \text{if } r \equiv 0 \pmod{8}, \\ 3 & \text{if } r \equiv 1 \pmod{4}, \\ 8 & \text{if } r \equiv a^{2} + b \pmod{32}, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$

Corollary 1.2: Assume that a is odd and $b \equiv 1 \pmod{16}$. Then $\{u_i\}$ is stable modulo 2, with stability beginning at N = 5, and $\Omega_{a,b}(2^k) = \{0, 1, 2, 3, 8\}$ for all $k \ge 5$.

The reader may wonder if stability also occurs for other choices of the parameters a and b. In fact it does, though the proofs are considerably more delicate. Table 1 gives the value of N at which stability begins for a given pair (a, b). In [2] we proved that $\{u_i\}$ is stable when $b \equiv 5 \pmod{8}$, and in [1] we dealt with the case $b \equiv 3 \pmod{4}$, in which stability apparently occurs less frequently.

												a								
		1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37
	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
	3			4	4	4	4					4	4	4	4					4
	5	5	4	4	7	6	4	4	5	5	4	4	6	8	4	4	5	5	4	4
	7	5	4	5	4	6	7	4	6		4	· 6		5	5	4	4	5	4	5
	9																			
	11		4		4	4		4			4		4	4		4			4	
	13	4	5	7	4	4	6	5	4	4	5	6	4	4	9	5	4	4	5	8
h	15	6	3	3	6	5	3	3	5	8	3	3	5	7	3	3	8	7	3	3
0	17	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
	19			4	4	4	4					4	4	4	4					4
	21	7	4	4	5	5	4	4	6	6	4	4	5	5	4	4	11	8	4	4
	23	5	5	4		5	4	6		6	7	4	4	6	4	5	4	5	5	4
	25																			
	27		4		4	4		4			4		4	4		4			4	
	29	4	6	5	4	4	5	9	4	4	7	5	4	4	5	6	4	4	6	5
	31	7	3	3	4	4	3	3	8	6	3	3	4	4	3	3	2		3	3

TABLE 1. Smallest k for which $\Omega_{a,b}(2^k) = \Omega_{a,b}(2^{k+t})$ for all $t \ge 0$

A missing entry in Table 1 corresponds to a case that we have not yet resolved (but conjecture to be unstable). In particular, as of this writing, the stability of $\{u_i\}$ when $b \equiv 9 \pmod{16}$ is undetermined.

2. PRELIMINARY LEMMAS

In this section we present a few lemmas required for the proof of Theorem 1.1. Throughout this section, assume that a is odd and that $b \equiv 1 \pmod{16}$. As usual, $\{u_i\}$ will denote a two-term recurrence sequence defined by $u_0 = 0$, $u_1 = 1$, and $u_i = au_{i-1} + bu_{i-2}$ for all $i \ge 2$.

The following lemma summarizes some well-known facts about two-term recurrences. The routine induction proofs of each part are left to the reader.

Lemma 2.1: For all $m \ge 1$ and $n \ge 0$,

- (a) $u_{m+n} = bu_{m-1}u_n + u_m u_{n+1}$,
- (b) $u_{2n+1} = b(u_n)^2 + (u_{n+1})^2$,
- (c) $u_{2n} = 2u_n u_{n+1} a(u_n)^2$, and
- (d) u_n divides u_{nm} .

Although the next lemma is stated only for $b \equiv 1 \pmod{16}$, analogs exist for all odd b. The interested reader is invited to discover these congruences.

Lemma 2.2: For all $k \ge 5$,

(a)
$$u_{3\cdot 2^{k-3}} \equiv \begin{cases} 2^{k-1} \pmod{2^{k+1}} & \text{if } a \equiv 1 \pmod{8} \text{ or } a \equiv 3 \pmod{8}, \\ 3 \cdot 2^{k-1} \pmod{2^{k+1}} & \text{if } a \equiv 5 \pmod{8} \text{ or } a \equiv 7 \pmod{8}, \end{cases}$$

and

(b)
$$u_{3\cdot 2^{k-3}+1} \equiv \begin{cases} 1+2^{k-2} \pmod{2^k} & \text{if } a \equiv 1 \pmod{8} \text{ or } a \equiv 7 \pmod{8}, \\ 1+3\cdot 2^{k-2} \pmod{2^k} & \text{if } a \equiv 3 \pmod{8} \text{ or } a \equiv 5 \pmod{8}. \end{cases}$$

Proof: We will prove the results for $a \equiv 1 \pmod{8}$ and leave the analogous proofs when $a \equiv 3, 5, \text{ or } 7 \pmod{8}$ to the reader. To this end, assume that $a \equiv 1 \pmod{8}$. We prove (a) and (b) simultaneously by induction on k. The base step, when k = 5, can be checked by explicit computation. Since there are only a finite number of two-term recurrence sequences modulo 2^5 and 2^6 , this computation is finite, and we leave it to the reader to verify the result.

Now assume that (a) and (b) are true for some $k \ge 5$. Since $k \ge 5$, it follows that $2k - 4 \ge k + 1$ and $2k - 2 \ge k + 1$. Therefore, by Lemma 2.1 and the induction hypothesis,

$$u_{3\cdot 2^{k-2}+1} = u_{2(3\cdot 2^{k-3})+1} = b(u_{3\cdot 2^{k-3}})^2 + (u_{3\cdot 2^{k-3}+1})^2$$

$$\equiv b(2^{k-1})^2 + (1+2^{k-2})^2 \pmod{2^{k+1}}$$

$$\equiv b \cdot 2^{2k-2} + 1 + 2^{k-1} + 2^{2k-4} \pmod{2^{k+1}}$$

$$\equiv 1 + 2^{k-1} \pmod{2^{k+1}},$$

as desired.

Now write $u_{32^{k-3}+1} = 1 + 2^{k-2} + 2^k v$ for some integer v. Since $k \ge 4$, it follows that $2k - 2 \ge k + 2$ and, therefore, by Lemma 2.1 and the induction hypothesis,

$$u_{3\cdot 2^{k-2}} = u_{2(3\cdot 2^{k-3})} = 2(u_{3\cdot 2^{k-3}}u_{3\cdot 2^{k-3}+1}) - a(u_{3\cdot 2^{k-3}})^2$$

= $(2 \cdot 2^{k-1}) \cdot (1 + 2^{k-2} + 2^k v) - a(2^{k-1})^2 \pmod{2^{k+2}}$
= $2^k (1 + 2^{k-2}) \pmod{2^{k+2}}$
= $2^k \pmod{2^{k+2}}$,

as desired. This completes the induction and, hence, the proof of the lemma for $a \equiv 1 \pmod{8}$. \Box

Clearly the residue classes of u_n modulo 2, 4, and 8 depend only upon the residue classes of a and b. These classes will be required below. They may be computed directly, and we list them here for convenience.

Reduction of $\{u_i\}$ modulo 2 yields

$$0, 1, 1, 0, 1, \dots$$
 for all odd *a* and *b*. (2.1)

Since $b \equiv 1 \pmod{4}$, reduction of $\{u_i\}$ modulo 4 yields

0, 1, 1, 2, 3, 1, 0, 1, ... if
$$a \equiv 1 \pmod{4}$$
,
0, 1, 3, 2, 1, 1, 0, 1, ... if $a \equiv 3 \pmod{4}$.
(2.2)

300

AUG.

Finally, since $b \equiv 1 \pmod{8}$, reduction of $\{u_i\}$ modulo 8 yields

0, 1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, 0, 1, ... if
$$a \equiv 1 \pmod{8}$$
,
0, 1, 3, 2, 1, 5, 0, 5, 7, 2, 5, 1, 0, 1, ... if $a \equiv 3 \pmod{8}$,
0, 1, 5, 2, 7, 5, 0, 5, 1, 2, 3, 1, 0, 1, ... if $a \equiv 5 \pmod{8}$,
0, 1, 7, 2, 5, 5, 0, 5, 3, 2, 1, 1, 0, 1, ... if $a \equiv 7 \pmod{8}$.
(2.3)

In the next lemma we examine the periods of two-term recurrence sequences defined by our parameters a and b.

Lemma 2.3: If $b \equiv 1 \pmod{16}$ and a is odd, then $\lambda(2^k) = 3 \cdot 2^{k-1}$ for all $k \ge 5$.

Proof: Fix an integer k such that $k \ge 5$. By Lemma 2.2, $u_{32^{k-1}} \equiv 0 \pmod{2^k}$ and $u_{32^{k-1}+1} \equiv 1 \pmod{2^k}$. Hence, $\lambda(2^k)$ divides $3 \cdot 2^{k-1}$. But, by Lemma 2.2, $u_{32^{k-2}+1} \equiv 1 + 2^{k-1} \pmod{2^k}$ (in all cases) so that $\lambda(2^k)$ does not divide $3 \cdot 2^{k-2}$. Since, by (2.2), $u_{2^{k-1}} \neq 0 \pmod{4}$, it follows that $u_{2^{k-1}} \neq 0 \pmod{2^k}$ and, hence, $\lambda(2^k)$ does not divide 2^{k-1} . It now follows that $\lambda(2^k) = 3 \cdot 2^{k-1}$. \Box

We now derive four lemmas that are key to the proof of Theorem 1.1.

Lemma 2.4: Assume that $k \ge 5$. If $n \ge 0$ and $n \ne 0 \pmod{3}$, then $u_{n+3,2^{k-2}} \equiv u_n + 2^{k-1} \pmod{2^k}$.

Proof: Note that by (2.1) u_n is even if and only if 3|n; hence, the hypothesis that $n \neq 0 \pmod{3}$ implies that u_n is odd. Therefore, by Lemmas 2.1 and 2.2,

$$u_{n+3\cdot 2^{k-2}} = bu_{n-1}u_{3\cdot 2^{k-2}} + u_nu_{3\cdot 2^{k-2}+1}$$

$$\equiv bu_{n-2} \cdot 0 + u_nu_{3\cdot 2^{k-2}+1} \pmod{2^k}$$

$$\equiv u_n(1+2^{k-1}) \pmod{2^k}$$

$$\equiv u_n + 2^{k-1} \pmod{2^k},$$

as desired. \Box

Lemma 2.5: Assume that $k \ge 5$. If $n \ge 0$ and $n \equiv 0 \pmod{6}$, then $u_{n+3,2^{k-3}} \equiv u_n + 2^{k-1} \pmod{2^k}$.

Proof: By Lemma 2.2 we can write $u_{3\cdot 2^{k-3}+1} \equiv 1 + \ell \cdot 2^{k-2} \pmod{2^k}$ for some odd integer ℓ . Then

$$u_{n+3\cdot2^{k-3}} = bu_{n-1}u_{3\cdot2^{k-3}} + u_nu_{3\cdot2^{k-3}+1}$$

= $bu_{n-1}\cdot2^{k-1} + u_n(1+\ell\cdot2^{k-2}) \pmod{2^k}.$

Since both b and u_{n-1} are odd, $bu_{n-1} \cdot 2^{k-1} \equiv 2^{k-1} \pmod{2^k}$. Moreover, by (2.2), $u_6 \equiv 0 \pmod{4}$ 4) and, by Lemma 2.2, u_6 divides u_n , so $u_n \equiv 0 \pmod{4}$. Consequently, $u_n(1+\ell \cdot 2^{k-2}) \equiv u_n \pmod{2^k}$. Thus, $u_{n+2,2^{k-3}} \equiv u_n + 2^{k-1} \pmod{2^k}$, as desired. \Box

We also need a lemma similar to Lemmas 2.4 and 2.5 to cover the case in which $n \equiv 3 \pmod{6}$. 6). This will require a little more work.

Lemma 2.6: Assume that $k \ge 6$. If $n \ge 0$ and $n \equiv 3 \pmod{6}$, then $u_{n+3,2^{k-4}} \equiv u_n + 2^{k-1} \pmod{2^k}$.

1996]

Proof: Note that, by (2.3), $u_n \equiv 2 \pmod{8}$ whenever $n \equiv 3 \pmod{6}$. By Lemma 2.2 and the hypothesis that $k \ge 6$, we can find integers ℓ and m such that

$$u_{3,2^{k-4}+1} = 1 + \ell \cdot 2^{k-3} + m \cdot 2^{k-1},$$

where ℓ is determined by the class of *a* modulo 8. Also, by Lemma 2.2, there is an odd integer *v* such that

$$u_{3,2^{k-4}} \equiv v \cdot 2^{k-2} \pmod{2^k},$$

where v is also determined by the class of a modulo 8. Moreover, note that (2.2) implies that $u_{n-1} \equiv a \pmod{4}$ and recall that $b \equiv 1 \pmod{16}$. Combining these congruences, we obtain

$$u_{n+3\cdot2^{k-4}} = u_{3\cdot2^{k-4}+1}u_n + bu_{3\cdot2^{k-4}}u_{n-1}$$

$$\equiv (1 + \ell \cdot 2^{k-3} + m \cdot 2^{k-1})u_n + b \cdot v \cdot 2^{k-2}u_{n-1} \pmod{2^k}$$

$$\equiv u_n + \ell \cdot 2^{k-2} + av2^{k-2} \pmod{2^k}$$

$$\equiv u_n + (\ell + av)2^{k-2} \pmod{2^k}.$$

We now compute:

a (mod 8)	l	v	$\ell + av \pmod{4}$
1	1	1	$2 \equiv 2 \pmod{4}$
3	3	1	$6 \equiv 2 \pmod{4}$
5	3	3	$18 \equiv 2 \pmod{4}$
7	1	3	$22 \equiv 2 \pmod{4}$

In each case $\ell + av \equiv 2 \pmod{4}$; therefore, $u_{n+3,2^{k-4}} \equiv u_n + 2^{k-1} \pmod{2^k}$, as desired. \Box

Finally, we require an easy generalization of Lemma 2.6.

Lemma 2.7: Assume that $n \ge 0$ and $s \ge 0$. If $n \equiv 3 \pmod{6}$ and $k \ge 6$, then $u_{n+3s\cdot 2^{k-4}} \equiv u_n + s \cdot 2^{k-1} \pmod{2^k}$.

Proof: Proceed by induction on s. If s = 0, the result is trivial. Fix $s \ge 0$ and assume the lemma is true for this value of s. Then

$$u_{n+3\cdot 2^{k-4}(s+1)} = u_{n+3\cdot 2^{k-4}+3s2^{k-4}}.$$

Observe that $n + 3 \cdot 2^{k-4} \equiv n \equiv 3 \pmod{6}$, so by Lemma 2.6 and the induction hypothesis,

$$u_{n+3\cdot 2^{k-4}(s+1)} \equiv u_{n+3\cdot 2^{k-4}} + s \cdot 2^{k-1} \pmod{2^k}$$
$$\equiv u_n + 2^{k-1} + s \cdot 2^{k-1} \pmod{2^k}$$
$$\equiv u_n + 2^{k-1}(s+1) \pmod{2^k},$$

as desired. \Box

302

3. PROOF OF THE MAIN THEOREM

In this section we prove Theorem 1.1.

Proof of Theorem 1.1

First, note that, by Lemma 2.3, $\lambda(2^k) = 3 \cdot 2^{k-1}$. In particular, $\lambda(2^{k+1}) = 2 \cdot \lambda(2^k)$.

Now, proceed by induction on k. For k = 5 and k = 6, there are only a finite number of sequences to examine (corresponding to $b \in \{1, 17, 33, 49\}$ and $a \in \{1, 3, 5, 7, ..., 61, 63\}$). Direct computation (perhaps with the assistance of a computer) establishes the theorem in these cases.

Assume that $k \ge 6$ and that Theorem 1.1 is true for this k.

Step 1. If $r \equiv 3 \pmod{4}$, then $v(2^{k+1}, r) \ge 1$.

Proof: By the induction hypothesis, $v(2^{k+1}, r) = 1$, so there exists an integer n with $u_n \equiv r \pmod{2^k}$. Since r is odd, (2.1) implies that $n \neq 0 \pmod{3}$. Now, either $u_n \equiv r \pmod{2^{k+1}}$ or $u_n \equiv r + 2^k \pmod{2^{k+1}}$. In the latter case, Lemma 2.4 implies that $u_{n+3\cdot 2^{k-1}} \equiv u_n + 2^k \equiv r \pmod{2^{k+1}}$. Thus, $v(2^{k+1}, r) \ge 1$, as desired. \Box

Step 2. If $r \equiv 1 \pmod{4}$, then $v(2^{k+1}, r) \ge 3$.

Proof: By the induction hypothesis, $v(2^k, r) = 3$. Pick indices $0 < n_1 < n_2 < n_3 < 3 \cdot 2^{k-1}$ such that $u_{n_1} \equiv u_{n_2} \equiv u_{n_3} \equiv r \pmod{2^k}$.

By Lemma 2.4, $u_{n_i+3\cdot 2^{k-1}} \equiv u_{n_i} + 2^k \pmod{2^{k+1}}$. Also, for each *i*, either $u_{n_i} \equiv r \pmod{2^{k+1}}$ or $u_{n_i} \equiv r + 2^k \pmod{2^{k+1}}$. Hence, for each *i*,

$$u_{n_i} \equiv r \pmod{2^{k+1}}$$
 or $u_{n_i+3\cdot 2^{k-1}} \equiv r \pmod{2^{k+1}}$.

For each *i*, let $m_i \in \{n_i, n_i + 3 \cdot 2^{k-1}\}$ be the index that satisfies $u_{m_i} \equiv r \pmod{2^{k+1}}$. Then the indices m_1, m_2 , and m_3 are congruent modulo $3 \cdot 2^{k-1}$ to n_1, n_2 , and n_3 , respectively. Furthermore, by Lemma 2.3, $\lambda(2^{k+1}) = 3 \cdot 2^k$. Thus, the indices m_1, m_2 , and m_3 are distinct and satisfy $0 < m_i < \lambda(2^{k+1})$. It follows that $v(2^{k+1}, r) \ge 3$, as desired. \Box

Step 3. If $r \equiv 0 \pmod{8}$, then $v(2^{k+1}, r) \ge 2$.

Proof: By the induction hypothesis $v(2^k, r) = 2$. Hence, we can find integers n_1 and n_2 such that $0 < n_1 < n_2 < 3 \cdot 2^{k-1}$ and $u_{n_1} \equiv u_{n_2} \equiv r \pmod{2^k}$. Now $u_{n_1} \equiv 0 \pmod{4}$, so (2.2) implies that $n_1 \equiv n_2 \equiv 0 \pmod{6}$. By Lemma 2.5, $u_{n_1+3\cdot 2^{k-2}} \equiv u_{n_1} \pmod{2^k}$. It follows that $n_2 = n_1 + 3\cdot 2^{k-2}$.

Now, either $u_{n_1} \equiv r \pmod{2^{k+1}}$ or $u_{n_1} \equiv r + 2^k \pmod{2^{k+1}}$. If $u_{n_1} \equiv r \pmod{2^{k+1}}$, then, by Lemma 2.5, $u_{n_1} \equiv u_{n_1+3\cdot2^{k-1}} \equiv r \pmod{2^{k+1}}$ and, hence, $v(2^{k+1}, r) \ge 2$. On the other hand, if $u_{n_1} \equiv r + 2^k \pmod{2^{k+1}}$, then, by Lemma 2.5, $u_{n_2} \equiv u_{n_1+3\cdot2^{k-2}} \equiv u_{n_1} + 2^k \equiv r \pmod{2^{k+1}}$. Therefore, $u_{n_2} \equiv u_{n_1+3\cdot2^{k-1}} \equiv r \pmod{2^{k+1}}$. Thus, $v(2^{k+1}, r) \ge 2$ in this case as well. \Box

Step 4. If $r \equiv a^2 + b \pmod{32}$, then $v(2^{k+1}, r) \ge 8$.

1996]

Proof: By the induction hypothesis, $v(2^k, r) = 8$. Choose *n* such that $u_n \equiv r \pmod{2^k}$. By hypothesis, $b \equiv 1 \pmod{16}$, and *a* is odd. Therefore, $a^2 \equiv 1 \pmod{8}$ and $r \equiv a^2 + b \equiv 2 \pmod{8}$. It follows from (2.3) that $n \equiv 3 \pmod{6}$. Hence, Lemma 2.7 yields

$$u_{n+3s\cdot 2^{k-4}} \equiv \begin{cases} u_n \pmod{2^k} & \text{if } s \text{ is even,} \\ u_n + 2^k \pmod{2^k} & \text{if } s \text{ is odd.} \end{cases}$$

By Lemma 2.3, $\lambda(2^k) = 3 \cdot 2^{k-1}$. It follows that

$$u_{n+3s\cdot 2^{k-4}} \equiv \begin{cases} r \pmod{2^k} & \text{if } s \in \{0, 2, 4, 6\}, \\ r+2^{k-1} \pmod{2^k} & \text{if } s \in \{1, 3, 5, 7\}, \end{cases}$$

with all indices $n + 3s \cdot 2^{k-4}$ occurring within one period.

Since, by the induction hypothesis, $v(2^k, r) = 8$, we can now conclude that there are indices n_1 and n_2 such that $0 < n_1 < n_2 < 3 \cdot 2^{k-1}$ with $n_2 - n_1 < 3 \cdot 2^{k-4}$ and $u_{n_1} \equiv u_{n_2} \equiv r \pmod{2^k}$. As usual, for $i = \{1, 2\}$, either $u_{n_i} \equiv r \pmod{2^{k+1}}$ or $u_{n_i} \equiv r + 2^k \pmod{2^{k+1}}$, and in the second case, Lemma 2.6 implies that $u_{n_i+3\cdot 2^{k-3}} \equiv r \pmod{2^{k+1}}$. Hence, there are subscripts m_1 and m_2 such that $u_{m_1} \equiv u_{m_2} \equiv r \pmod{2^{k+1}}$ and $m_i \equiv n_i \pmod{3 \cdot 2^{k-3}}$.

Consider the set $\Gamma = \{m_i + 3s \cdot 2^{k-2} | 0 \le s \le 3 \text{ and } 1 \le i \le 2\}$. By Lemma 2.7, $u_m \equiv r \pmod{2^{k+1}}$ for $m \in \Gamma$. Since $\lambda(2^{k+1}) = 3 \cdot 2^k$, it suffices to show that the elements of Γ are incongruent modulo $3 \cdot 2^k$.

If $m_i + 3s \cdot 2^{k-2} \equiv m_i + 3t \cdot 2^{k-2} \pmod{3 \cdot 2^k}$ (for some s and t such that $0 \le s, t \le 3$), then $3(s-t) \cdot 2^{k-2} \equiv 0 \pmod{3 \cdot 2^k}$ and, therefore, $s \equiv t \pmod{4}$. Thus s = t.

Moreover, if $m_1 + 3s \cdot 2^{k-2} \equiv m_2 + 3t \cdot 2^{k-2} \pmod{3 \cdot 2^k}$, then $m_i \equiv m_2 \pmod{3 \cdot 2^{k-2}}$ and, hence, $n_1 \equiv m_1 \equiv m_2 \equiv n_2 \pmod{3 \cdot 2^{k-3}}$, which contradicts the choice of n_1 and n_2 to satisfy $n_2 - n_1 < 3 \cdot 2^{k-4}$ and $n_1 \neq n_2$.

It follows that the eight elements of Γ are distinct modulo $\lambda(2^{k+1})$ and, consequently, $\nu(2^{k+1}, r) \ge 8$. \Box

Step 5. Conclusion

Proof: We have established that $v(2^{k+1}, r) \ge v(2^k, r)$ in each case of Lemma 1.1 for which $v(2^k, r) > 0$. Now observe:

$$\begin{aligned} \lambda(2^{k+1}) &= 3 \cdot 2^k \\ &= \sum_{r=0}^{2^{k+1}-1} v(2^{k+1}, r) \\ &\geq \sum_{r\equiv 3 \pmod{4}} v(2^{k+1}, r) + \sum_{r\equiv 1 \pmod{4}} v(2^{k+1}, r) + \sum_{r\equiv 0 \pmod{8}} v(2^{k+1}, r) + \sum_{r\equiv a^2 + b \pmod{32}} v(2^{k+1}, r) \\ &\geq \frac{1}{4} \cdot 2^{k+1} \cdot 1 + \frac{1}{4} \cdot 2^{k+1} \cdot 3 + \frac{1}{8} \cdot 2^{k+1} \cdot 2 + \frac{1}{32} \cdot 2^{k+1} \cdot 8 \\ &= 2^{k-1} + 3 \cdot 2^{k-1} + 2^{k-1} + 2^{k-1} = 3 \cdot 2^k = \lambda(2^{k+1}). \end{aligned}$$

AUG.

It follows that all of the inequalities obtained in Steps 1-4 above are equalities. This shows that $v(2^{k+1}, r) = v(2^k, r)$ for all $r \in \mathbb{Z}$, and completes the induction and the proof of Theorem 1.1. \Box

Remark 3.1: As mentioned above, the techniques described in this paper may be extended to show stability of two-term recurrence sequences determined by other values of the parameters a and b. Originally, this work contained delicate arguments to handle a number of other such cases. Because subsequently developed methods have shown that only the case that $b \equiv 1 \pmod{16}$ needs to be singled out in this way, we leave the extension of this "direct approach" to the reader. We would like to thank the referee for suggesting this lighter approach to the presentation.

REFERENCES

- W. Carlip & E. Jacobson. "A Criterion for Stability of Two-Term Recurrence Sequences Modulo 2^k." J. Finite Fields (submitted).
- 2. W. Carlip & E. Jacobson. "Unbounded Stability of Two-Term Recurrence Sequences Modulo 2^k." Acta. Arith. (to appear).
- 3. R. D. Carmichael. "On Sequences of Integers Defined by Recurrence Relations." Quart. J. Pure and Appl. Math. 48 (1920):343-72.
- 4. Eliot T. Jacobson. "Distribution of the Fibonacci Numbers Mod 2^k." The Fibonacci Quarterly **30.3** (1992):211-15.
- 5. Wladyslaw Narkiewicz. Uniform Distribution of Sequences of Integers in Residue Classes. Lecture Notes in Mathematics, Vol. 1087. New York: Springer-Verlag, 1984.
- 6. Jukka Pihko. "A Note on a Theorem of Schinzel." *The Fibonacci Quarterly* **29.4** (1991): 333-38.
- A. Schinzel. "Special Lucas Sequences, Including the Fibonacci Sequence, Modulo a Prime." In A Tribute to Paul Erdös, pp. 349-57. Ed. A. Baker, B. Bollobás, and A. Hajnal. Cambridge: Cambridge University Press, 1990.
- 8. Lawrence Somer. "Distribution of Residues of Certain Second-Order Linear Recurrences Modulo *p*." In *Applications of Fibonacci Numbers*, pp. 311-24. Ed. A. N. Phillipou, A. F. Horadam, and G. E. Bergum. Dordrecht: Kluwer, 1988.
- 9. Lawrence Somer. "Distribution of Residues of Certain Second-Order Linear Recurrences Modulo *p*—II." *The Fibonacci Quarterly* **29:1** (1991):72-78.
- 10. D. D. Wall. "Fibonacci Series Modulo m." Amer. Math. Monthly 67 (1960):525-32.

AMS Classification Numbers: 11B39, 11B50, 11B37

** ** **

Neville Robbins

Mathematics Department, San Francisco State University, San Francisco, CA 94132 e-mail: robbins@math.sfsu.edu (Submitted October 1994)

INTRODUCTION

Let $\{u_n\}$ be a strictly increasing sequence of natural numbers, so that $u_n \ge n$ for all n. Let

$$g(z) = \prod_{n \ge 1} (1 - z^{u_n}).$$
 (1)

If |z| < 1, then

$$\left|\sum_{n\geq 1} z^{u_n}\right| \leq \sum_{n\geq 1} |z^{u_n}| = \sum_{n\geq 1} |z|^{u_n} \leq \sum_{n\geq 1} |z|^n = \frac{|z|}{1-|z|},$$

so the product in (1) converges absolutely to an analytic function without zeros on compact subsets of the unit disk. Let g(z) have a Maclaurin series representation given by

$$g(z) = \sum_{n \ge 0} a_n z^n$$
 (2)

Let

$$f(z) = 1/g(z)$$
. (3)

Then f(z) is also an analytic function without zeros on compact subsets of the unit disk. We have

$$f(z) = \prod_{n \ge 1} (1 - z^{u_n})^{-1} = \sum_{n \ge 0} U_n z^n \quad (\text{with } U_0 = 1).$$
(4)

Definition 1: Let r(n), $r_E(n)$, $r_0(n)$ denote, respectively, the number of partitions of n into distinct parts, evenly many distinct parts, oddly many distinct parts from $\{u_n\}$. Let $r(0) = r_E(0) = 1$, $r_0(0) = 0$. If $a_n = r_E(n) - r_0(n)$, then U_n is the number of partitions of n all of whose parts belong to $\{u_n\}$, that is, f(z) is the generating function for $\{u_n\}$. Since f(z) * g(z) = 1, we obtain the recurrence relation:

$$\sum_{k=0}^{n} a_{n-k} U_k = 0 \quad \text{(for } n \ge 1\text{)}.$$
(5)

This provides a way to determine the U_n , once the a_n are known. Now Definition 1 implies that

$$r_0(n) = r(n) - r_F(n); (6)$$

hence,

$$a_n = 2r_E(n) - r(n). \tag{7}$$

Our original problem, namely, to determine U_n , has been reduced to determining the r(n) and $r_E(n)$.

Several researchers have investigated the case where $\{u_n\}$ is the Fibonacci sequence. If we let $u_n = F_n$, as was done by Verner E. Hoggatt, Jr., & S. L. Basin [3], then an anomaly arises: since $F_1 = F_2 = 1$, it follows that 1 may occur twice as a summand in a partition of *n* into "distinct"

306

Fibonacci summands. We therefore prefer to let $u_n = F_{n+1}$, since the Fibonacci sequence is strictly increasing for $n \ge 2$. This is the approach taken by Klarner [4] and Carlitz [1]. Our algorithm for computing r(n) is simpler and apparently more efficient than that of Carlitz.

Definition 2: The trivial partition of *n* consists of just *n* itself.

We shall use the following well-known properties of Fibonacci numbers:

$$F_m = F_{m-1} + F_{m-2}, (8)$$

$$\sum_{k=1}^{m} F_k = F_{m+2} - 1,$$
(9)

$$\sum_{k=1}^{m} F_{2k} = F_{2m+1} - 1, \tag{10}$$

$$\sum_{k=2}^{m} F_{2k-1} = F_{2m} - 1, \tag{11}$$

Zeckendorf's Theorem (see [5]). (12)

Every natural number n has a unique representation:

$$n=\sum_{k=2}^r c_k F_k\,,$$

where $c_r = 1$, each $c_k = 0$ or 1, and $c_{k-1}c_k = 0$ for all k such that $3 \le k \le r$. Following Ferns [2], we call this the *minimal Fibonacci representation* of n.

More generally, if we drop the requirement that $c_{k-1}c_k = 0$, we obtain what will be called a Fibonacci representation of n. The c_k are called the digits of the representation. Now r(n) denotes the number of distinct Fibonacci representations of n.

THE MAIN THEOREMS

Theorem 1: $r(F_m) = \lfloor \frac{1}{2}m \rfloor$ if $m \ge 2$.

Proof: (Induction on *m*) Since $r(F_2) = r(1) = 1 = \lfloor \frac{1}{2}(2) \rfloor$ and $r(F_3) = r(2) = 1 = \lfloor \frac{1}{2}(3) \rfloor$, Theorem 1 holds for m = 2, 3. Now suppose $m \ge 4$. Every nontrivial partition of F_m into distinct Fibonacci parts must include F_{m-1} as a part, since (9) implies that $\sum_{k=2}^{m-2} F_k = F_m - 2 < F_m$. Therefore, by (8), every nontrivial partition of F_m into distinct Fibonacci parts consists of F_{m-1} , plus the summands in such a partition of F_{m-2} . Therefore, $r(F_m) = 1 + r(F_{m-2})$ if $m \ge 4$. (The "1" in this formula corresponds to the trivial partition of F_m .) By the induction hypothesis, $r(F_{m-2}) = \lfloor \frac{1}{2}(m-2) \rfloor$. Thus, $r(F_m) = 1 + \lfloor \frac{1}{2}(m-2) \rfloor = \lfloor \frac{1}{2}m \rfloor$.

Remark: Essentially the same proof of Theorem 1 appears in [1] and [3].

Theorem 2: $r_E(F_m) = [\frac{1}{4}m]$ if $m \ge 2$.

Proof: (Induction on m) Since $r_E(F_2) = r_E(1) = 0 = [\frac{1}{4}(2)]$ and $r_E(F_3) = r_E(2) = 0 = [\frac{1}{4}(3)]$, Theorem 2 holds for m = 2, 3. Now suppose $m \ge 4$. As in the proof of Theorem 1, any partition of F_m into evenly many distinct Fibonacci parts must include F_{m-1} as a part, plus the summands in

1996]

a partition of F_{m-2} into oddly many distinct Fibonacci parts. That is, $r_E(F_m) = r_0(F_{m-2})$. But (6), Theorem 1, and the induction hypothesis imply that $r_0(F_{m-2}) = r(F_{m-2}) - r_E(F_{m-2}) = [\frac{1}{2}(m-2)] - [\frac{1}{4}(m-2)] = [\frac{1}{4}m]$.

Theorem 3: Let $a(n) = a_n$. Then

$$a(F_m) = \begin{cases} 0 & \text{if } m \equiv 0, 1 \pmod{4}, \\ -1 & \text{if } m \equiv 2, 3 \pmod{4}. \end{cases}$$

Proof: From (7) and from Theorems 1 and 2, we have $a(F_m) = 2[\frac{1}{4}m] = [\frac{1}{2}m]$, from which the conclusion follows.

Having settled the case where *n* is a Fibonacci number, let us now consider the case where *n* is not a Fibonacci number. In the minimal Fibonacci representation, let $n = F_{k_1} + F_{k_2} + \cdots + F_{k_r}$, where $r \ge 2$, $k_r \ge 2$, and $k_i - k_{i+1} \ge 2$ for all *i* with $1 \le i \le r - 1$. Let $n_0 = n$, $n_i = n_{i-1} - F_{k_i}$ for $1 \le i \le r$. In particular, $n_1 = n - F_{k_1}$, $n_{r-1} = F_{k_r}$, $n_r = 0$. Given any Fibonacci representation of *n*, define the *initial segment* as the first $k_1 - k_2$ digits, while the *terminal segment* consists of the remaining digits. In the minimal Fibonacci representation of *n*, the initial segment consists of a 1 followed by $k_1 - k_2 - 1$ 0's, while the terminal segment starts with 10. Fibonacci representations of *n* may be obtained as follows:

Type I: Arbitrary combinations of Fibonacci representations of the integers corresponding to the initial and terminal segments in the minimal Fibonacci representation of *n*;

Type II: Suppose that in a nonminimal Fibonacci representation of n the initial segment ends in 10 while the terminal segment starts with 0. If this 100 block, which is partly in the initial segment and partly in the terminal segment, is replaced by 011, a new Fibonacci representation of n is obtained.

Lemma 1: Every Fibonacci representation of *n* that includes F_{k_1} as a part has an initial segment which agrees with that of the minimal Fibonacci representation.

Proof: If *n* has a Fibonacci representation that includes F_{k_1} as a part but differs from the minimal Fibonacci representation, then $n = F_{k_1} + F_j + \cdots$, where $j > k_2$. But $n \le F_{k_1} + F_{k_2} + F_{k_2-2} + F_{k_2-4} + \cdots \le F_{k_1} + F_{k_2+1} - 1$ by (10) and (11). Now $F_{k_1} + F_j \le n \le F_{k_1} + F_{k_2+1}$, which implies $F_j < F_{k_2+1}$; hence, $j \le k_2$, an impossibility.

Lemma 2: Let $\bar{r}(n)$ be the number of Fibonacci representations of n that do not include F_{k_1} as a part. Then $\bar{r}(n) = r(n) - r(n_1)$.

Proof: If n is a Fibonacci number, then the conclusion follows from Definitions 1 and 2. Otherwise, by hypothesis, $r(n) - \bar{r}(n)$ is the number of Fibonacci representations of n that do include F_{k_1} as a part. By Lemma 1, the initial segment of such a representation is unique, and consists of a 1 followed by $k_1 - k_2 - 1$ 0's. Since the terminal segment is unrestricted, the number of such Type I representations is $1 * r(n_1) = r(n_1)$. Type II representations are excluded here, since they can only arise when the initial segment has a nonminimal representation. Therefore, we have: $r(n) - \bar{r}(n) = r(n_1)$, from which the conclusion follows.

Lemma 3: Let $\bar{r}_E(n)$ denote the number of partitions of *n* into evenly many distinct Fibonacci numbers, not including F_{k_1} as a part. Then $\bar{r}_E(n) = r_E(n) - r_0(n_1)$.

Proof: The proof of Lemma 3 is similar to that of Lemma 2, and is therefore omitted.

Theorem 4:
$$r(n) = \begin{cases} \frac{1}{2}(k_1 - k_2 + 1)r(n_1) & \text{if } k_1 - k_2 \text{ is odd,} \\ (1 + \frac{1}{2}(k_1 - k_2))r(n_1) - r(n_2) & \text{if } k_1 - k_2 \text{ is even.} \end{cases}$$

Proof: Let $m = k_1$, $h = k_2$. Recall that the initial segment of the minimal Fibonacci representation of n consists of a 1 followed by m-h-1 0's. Viewed by itself, this initial segment corresponds to the minimal Fibonacci representation of F_{m-h+1} . By Theorem 1, the number of Fibonacci representations of the initial segment is $r(F_{m-h+1}) = [\frac{1}{2}(m-h+1)]$. The number of Fibonacci representations of the terminal segment is by definition $r(n_1)$. Therefore, the number of Type I Fibonacci representations of n is $[\frac{1}{2}(m-h+1)]r(n_1)$.

If m-h is odd, then the initial segment in the minimal Fibonacci representation of n consists of a 1 followed by evenly many 0's. Therefore, each Fibonacci representation of F_{m-h+1} (the integer corresponding to the initial segment) ends in 00 or 11. Thus, Type II Fibonacci representations of n cannot arise, so that $r(n) = [\frac{1}{2}(m-h+1)]r(n_1) = \frac{1}{2}(m-h+1)r(n_1)$.

If m-h is even, then the initial segment in the minimal Fibonacci representation of n consists of a 1 followed by oddly many 0's. Therefore, F_{m-h+1} is a unique Fibonacci representation ending in 10. By Lemma 2, the integer corresponding to the terminal segment, namely n_1 , has $\bar{r}(n_1) = r(n_1) - r(n_2)$ Fibonacci representations that start with digit 0. Thus, we have $r(n_1) - r(n_2)$ Type II Fibonacci representations of n. Therefore, $r(n_1) = [\frac{1}{2}(m-h+1)]r(n_1) + r(n_1) - r(n_2)$. Similifying, we get $r(n) = (1 + \frac{1}{2}(m-h))r(n_1) - r(n_2)$.

Theorem 5:

- (a) If $k_1 k_2 \equiv 3 \pmod{4}$, then $r_E(n) = \frac{1}{4}(k_1 k_2 + 1)r(n_1)$.
- (b) If $k_1 k_2 \equiv 1 \pmod{4}$, then $r_E(n) = \frac{1}{4}(k_1 k_2 + 3)r(n_1) r_E(n_1)$.

(c) If $k_1 - k_2 \equiv 2 \pmod{4}$, then $r_E(n) = \frac{1}{4}(k_1 - k_2 + 2)r(n_1) + r_E(n_2) - r(n_2)$.

(d) If $k_1 - k_2 \equiv 0 \pmod{4}$, then $r_E(n) = (1 + \frac{1}{4}(k_1 - k_2))r(n_1) - r_E(n_1) - r_E(n_2)$.

Proof: Let $m = k_1$, $h = k_2$. Let b(n) and c(n) denote, respectively, the numbers of Type I and Type II representations of n as a sum of evenly many distinct Fibonacci numbers, so that $r_E(n) = b(n) + c(n)$. A Fibonacci representation of n has evenly many parts if and only if the number of 1's in the initial segment has the same parity as the number of 1's in the terminal segment. Thus,

$$b(n) = r_E(F_{m-h+1})r_E(n_1) + r_0(F_{m-h+1})r_0(n_1)$$

= $[\frac{1}{4}(m-h+1)]r_E(n_1) + ([\frac{1}{2}(m-h+1)] - [\frac{1}{4}(m-h+1)])(r(n_1) - r_E(n_1))$
= $([\frac{1}{2}(m-h+1)] - [\frac{1}{4}(m-h+1)])r(n_1) + (2[\frac{1}{4}(m-h+1)] - [\frac{1}{2}(m-h+1)])r_E(n_1).$

If $m-h \equiv 0$ or 3 (mod 4), then $\left[\frac{1}{2}(m-h+1)\right] = 2\left[\frac{1}{4}(m-h+1)\right]$, so $b(n) = \left[\frac{1}{4}(m-h+1)\right]r(n_1)$.

If $m-h \equiv 1 \text{ or } 2 \pmod{4}$, then $[\frac{1}{2}(m-h+1)] = 1 + 2[\frac{1}{4}(m-h+1)]$, so $b(n) = (1 + [\frac{1}{4}(m-h+1)])r(n_1) - r_E(n_1)$.

1996]

If m-h is odd, then, as in the proof of Theorem 4, no Type II Fibonacci representations of n can occur, that is, c(n) = 0. Upon simplifying, we obtain:

- (a) If $m-h \equiv 3 \pmod{4}$, then $r_E(n) = \frac{1}{4}(m-h+1)r(n_1)$;
- (b) If $m-h \equiv 1 \pmod{4}$, then $r_E(n) = \frac{1}{4}(m-h+3)r(n_1) r_E(n_1)$.

If m-h; is even, then, as in the proof of Theorem 4, the integer corresponding to the initial segment has a unique Fibonacci representation ending in 10, so that Type II Fibonacci representations of n do occur. A Type II Fibonacci representation will have evenly many 1's if and only if the number of 1's in the initial and terminal segments differ in parity.

If $m-h \equiv 2 \pmod{4}$, then the unique Fibonacci representation of the integer corresponding to the initial segment that ends in 10 has an odd number of 1's. Therefore,

 $c(n) = \overline{r_E}(n_1) = r_E(n_1) - r_0(n_2).$

Thus,

$$\begin{aligned} r_E(n) &= b(n) + c(n) \\ &= (1 + [\frac{1}{4}(m-h+1)])r(n_1) - r_E(n_1) + r_E(n_1) - r_0(n_2) \\ &= \frac{1}{4}(m-h+2)r(n_1) + r_E(n_2) - r(n_2). \end{aligned}$$

This proves (c).

If $m - h \equiv 0 \pmod{4}$, then the unique Fibonacci representation of the integer corresponding to the initial segment that ends in 10 has an even number of 1's. Therefore,

$$c(n) = \overline{r}_0(n_1) = \overline{r}(n_1) - \overline{r}_E(n_1)$$

= $r(n_1) - r(n_2) - (r_E(n_1) - r_0(n_2))$
= $r(n_1) - r_E(n_1) - r_E(n_2).$

But $b(n) = [\frac{1}{4}(m-h+1)]r(n_1) = \frac{1}{4}(m-h)r(n_1)$, so

$$r_{E}(n) = b(n) + c(n) = (1 + \frac{1}{4}(m-h))r(n_{1}) - r_{E}(n_{2}).$$

This proves (d).

Theorem 6: If *n* is not a Fibonacci number, then

$$a(n) = \begin{cases} -a(n_1) - a(n_2) & \text{if } k_1 - k_2 \equiv 0 \pmod{4}, \\ -a(n_1) & \text{if } k_1 - k_2 \equiv 1 \pmod{4}, \\ a(n_2) & \text{if } k_1 - k_2 \equiv 2 \pmod{4}, \\ 0 & \text{if } k_1 - k_2 \equiv 3 \pmod{4}. \end{cases}$$

Proof: This follows from (7) and from Theorems 4 and 5.

Theorem 7: $a(n) = \begin{cases} 0 & \text{if } r(n) \text{ is even,} \\ \pm 1 & \text{if } r(n) \text{ is odd.} \end{cases}$

Proof: If n is a Fibonacci number, then the conclusion follows from Theorems 1 and 3. If n is not a Fibonacci number, then we will use induction. Note that (7) implies $a(n) \equiv r(n) \pmod{2}$. Therefore, it suffices to show that $|a(n)| \le 1$. By Theorem 6 and the induction hypothesis, this

is true, except possibly when $k_1 - k_2 \equiv 0 \pmod{4}$. In this case, we have $a(n) = -a(n_1) - a(n_2)$. Again by Theorem 6 we have:

 $a(n_1) = \begin{cases} -a(n_2) - a(n_3) & \text{if } k_2 - k_3 \equiv 0 \pmod{4}, \\ -a(n_2) & \text{if } k_2 - k_3 \equiv 1 \pmod{4}, \\ a(n_3) & \text{if } k_2 - k_3 \equiv 2 \pmod{4}, \\ 0 & \text{if } k_2 - k_3 \equiv 3 \pmod{4}. \end{cases}$

Therefore, we have

$$a(n) = \begin{cases} a(n_3) & \text{if } k_2 - k_3 \equiv 0 \pmod{4}, \\ 0 & \text{if } k_2 - k_3 \equiv 1 \pmod{4}, \\ -a(n_2) - a(n_3) & \text{if } k_2 - k_3 \equiv 2 \pmod{4}, \\ -a(n_2) & \text{if } k_2 - k_3 \equiv 3 \pmod{4}. \end{cases}$$

Thus, $|a(n)| \le 1$ except, possibly, when $k_2 - k_3 \equiv 2 \pmod{4}$. In the latter case, we evaluate $a(n_2)$ using Theorem 6. We then see that $|a(n)| \le 1$ except, possibly, when $k_3 - k_4 \equiv 2 \pmod{4}$, in which case $a(n) = -a(n_3) - a(n_4)$. If |a(n)| > 1, then we would have an infinite sequence: $n > n_1 > n_2 > n_3 > \cdots$. This is impossible, so we must have $|a(n)| \le 1$ for all n.

Theorem 8: r(n) = 1 if and only if $n = F_m - 1$ for some $m \ge 2$; if so, then

$$a(n) = \begin{cases} 1 & \text{if } m \equiv 1, 2 \pmod{4}, \\ -1 & \text{if } m \equiv 0, 3 \pmod{4}. \end{cases}$$

Proof: First, suppose that $n = F_m - 1$. By (10) and (11), we have

$$n = \sum_{k=1}^{\lfloor \frac{1}{2}m-1 \rfloor} F_{m+1-2k}$$

This is the minimal Fibonacci representation of n (since the condition $c_{j-1}c_j = 0$ holds) and consists of alternating 1's and 0's. Since no two consecutive 0's appear, this Fibonacci representation is also maximal; hence, is unique, that is, r(n) = 1. Conversely, if r(n) = 1, then the unique Fibonacci representation of n cannot contain consecutive 0's, and thus must consist of alternating 1's and 0's. Therefore, for some m, we have $n = F_{m-1} + F_{m-3} + F_{m-5} + \cdots$. Now (10) and (11) imply $n = F_m - 1$. If m = 4j + 1 or 4j + 2 for some j, then the unique Fibonacci representation of n has 2j summands. Thus, a(n) = 1 if $m \equiv 1, 2 \pmod{4}$. On the other hand, if m = 4j or 4j - 1, then the unique Fibonacci representation of n has 2j - 1 summands. Therefore, a(n) = -1 if $m = 0, 3 \pmod{4}$.

Theorem 9: There are arbitrarily long sequences of integers n such that a(n) = 0.

Proof: If $F_m + F_{m-3} \le n \le F_m + F_{m-2} - 1$, then the minimal Fibonacci representation of n is $n = F_m + F_{m-3} + \cdots$. Therefore, Theorem 6 implies that a(n) = 0. The number of integers satisfying the above inequality is $F_{m-2} - F_{m-3} = F_{m-4}$. For any given h, we can find $m \ge 6$ such that $F_{m-4} \ge h$. Thus, we are done.

Remark: With a little additional effort, one can also show that $a(F_m + F_{m-3} - 1) = 0$.

n	r(n)	a(n)	U(n)	n	r(n)	a(n)	U(n)
1	1	-1	1	51	3	1	4017
$\overline{2}$	ī	$-\overline{1}$	2	52	4	ō	4367
3	2	0	3	53	4	0	4737
4	1	1	4	54	1	1	5134
3	2	0	6	55	5	-1	5564
6	2	0	8	56	4	0	6016
7	1	1	10	57	4	0	6504
8	3	-1	14	58	7	1	7025
9	2	0	17	59	3	-1	7575
10	2	0	22	60	6	0	8171
11	3	1	27	61	6	0	8791
12	1	-1	33	62	3	-1	9466
13	3	-1	41	63	8	0	10183
14	3	1	49	64	5	1	10936
15	2	0	59	65	5	1	11744
16	4	0	71	66	7	-1	12599
17	2	0	83	67	2	0	13502
18	3	1	99	68	6	0	14471
19	3	-1	115	69	6	0	15486
20	1	-1	134	70	4	0	16568
21	4	0	157	71	8	0	177.15
22	3	1	180	72	4	0	18921
23	3	1	208	73	6	0	20207
24	5	-1	239	74	6	0	21559
25	2	0	272	75	2	0	22987
26	4	0	312	76	7	1	24506
27	4	0	353	77	5	-1	26094
28	2	0	400	78	5	-1	27782
29	5	1	453	79	8	0	29558
30	3	-1	509	80	3	I	31425
31	3	-1	573	81	6	0	33405
32	4	0	642	82	6	0	35478
33	1	1	717	83	3	1	37664
34	4	0	803	84		-1	39973
35	4	0	892	85	4	0	42386
30	5	1	993	86	4	0	44939
3/	0	0	1102	8/	1	1	4/613
20	5	-1	1219	88	1	1	50421
39	5	-1	1350	89	5	-1	55384
40	2	1	1489	90	3	1	50725
41	6	0	1040	91	4	0	62154
42	- 1	0	1000	92	0	0	66727
43	4	0	1965	93	4	1	70402
45	6	0	2170	05	7	1	70492 74400
46	2	0 0	2500	95	2	_1	78512
47	5	1	2854	97	9	-1	82871
48	5	_1	3113	97	6	0	87383
49	ĩ	_1	3393	99	6	0	92122
50	6	Ō	3697	100	9	-1	97075

Using (5) as well as Theorems 3, 4, and 6, one can compute r(n), a(n), and U(n) for any n. Table 1 lists the results of these computations for $1 \le n \le 100$.

TABLE 1

ACKNOWLEDGMENT

I wish to thank David Terr for his assistance in using Mathematica to compute the U_n and for many valuable discussions.

312

.

REFERENCES

- 1. L. Carlitz. "Fibonacci Representations." The Fibonacci Quarterly 6.4 (1968):193-220.
- 2. H. H. Ferns. "On the Representation of Integers as Sums of Distinct Fibonacci Numbers." *The Fibonacci Quarterly* **3.1** (1965):21-30.
- 3. V. E. Hoggatt, Jr., & S. L. Basin. "Representations by Complete Sequences—Part I." *The Fibonacci Quarterly* **1.3** (1963):1-14.
- 4. D. Klarner. "Partitions of N into Distinct Fibonacci Numbers." *The Fibonacci Quarterly* **6.4** (1968):235-43.
- 5. C. G. Lekkerkerker. "Voorstelling van natuurlyke getallen door een som van Fibonacci." *Simon Stevin* **29** (1951-1952):190-95.

AMS Classification Numbers: 11B39, 11P81

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.

RECURRENCE SEQUENCES AND NÖRLUND-EULER POLYNOMIALS

Wang Tianming

Institute of Math. Sciences, Dalian University of Technology, Dalian, 116024, China

Zhang Zhizheng

Department of Math., Luoyang Teachers' College, Luoyang, 471022, China (Submitted October 1994)

1. It is well known that a general linear sequence $S_n(p,q)$ (n = 0, 1, 2, ...) of order 2 is defined by the law of recurrence,

$$S_n(p,q) = pS_{n-1}(p,q) - qS_{n-2}(p,q),$$

with S_0 , S_1 , p, and q arbitrary, provided that $\Delta = p^2 - 4q > 0$, see [1].

In particular, if $S_0 = 0$ and $S_1 = 1$ or if $S_0 = 2$ and $S_1 = p$, we have generalized Fibonacci and Lucas sequences, respectively, in symbols $U_n(p,q)$ and $V_n(p,q)$.

By the roots $x_1 > x_2$ of the generating equation $x^2 - px + q = 0$, it is proved that

$$U_n(p,q) = \frac{x_1^n - x_2^n}{x_1 - x_2} \quad \text{and} \quad V_n(p,q) = x_1^n + x_2^n;$$
(1)

moreover, the general term of the recurrence sequence $S_n(p,q)$ is expressed as a sum of the general terms of generalized Fibonacci and Lucas sequences by the formula

$$S_n(p,q) = \left(S_1 - \frac{1}{2}pS_0\right) U_n(p,q) + \frac{1}{2}S_0V_n(p,q).$$
(2)

We assume

$$S_0 = \omega,$$

$$S_1 = \frac{1}{2}p\omega + \left(x - \frac{1}{2}\omega\right)\Delta^{\frac{1}{2}}$$

and, according to (1) and (2), we deduce

$$S_n(x; p,q) = \left(x - \frac{1}{2}\omega\right)\Delta^{\frac{1}{2}} \cdot U_n(p,q) + \frac{1}{2}\omega V_n(p,q)$$
(3)

and

314

$$S_n(x; p,q) = xx_1^n + (\omega - x)x_2^n.$$
 (4)

From this point on, we shall use the brief notation U_n, V_n , and $S_n(x)$ to denote $U_n(p,q), V_n(p,q)$, and $S_n(x; p,q)$, respectively.

2. From (3), we have

$$S_n^m(x) + S_n^m(\omega - x) = \frac{1}{2^{m-1}} \sum_{r=0}^{\left[\frac{m}{2}\right]} {m \brack 2r} \Delta^r U_n^{2r} V_n^{m-2r} (2x - \omega)^{2r},$$
(5)

[AUG,

and from (4), we have

$$S_n^m(x) + S_n^m(\omega - x) = \sum_{r=0}^m \begin{bmatrix} m \\ r \end{bmatrix} [x_1^{nr} x_2^{n(m-r)} + x_1^{n(m-r)} x_2^{nr}] x^r (\omega - x)^{m-r}$$
$$= \sum_{r=0}^m \begin{bmatrix} m \\ r \end{bmatrix} q^{nr} [x_1^{n(m-2r)} + x_2^{n(m-2r)}] x^r (\omega - x)^{m-r}.$$

Then we have

$$S_{n}^{2m}(x) + S_{n}^{2m}(\omega - x)$$

$$= \sum_{r=0}^{m} \begin{bmatrix} 2m \\ r \end{bmatrix} q^{nr} [x_{1}^{2n(m-r)} + x_{2}^{2n(m-r)}] x^{r}(\omega - x)^{2m-r} + \sum_{s=0}^{m-1} \begin{bmatrix} 2m \\ s \end{bmatrix} q^{ns} [x_{1}^{2n(m-s)} + x_{2}^{2n(m-s)}] x^{2m-s}(\omega - x)^{s}$$

$$= 2 \begin{bmatrix} 2m \\ m \end{bmatrix} q^{mn} x^{m}(\omega - x)^{m} + \sum_{r=0}^{m-1} \begin{bmatrix} 2m \\ r \end{bmatrix} q^{nr} [x_{1}^{2n(m-r)} + x_{2}^{2n(m-r)}] [x^{r}(\omega - x)^{2m-r} + x^{2m-r}(\omega - x)^{r}]$$

$$= 2 \begin{bmatrix} 2m \\ m \end{bmatrix} q^{mn} x^{m}(\omega - x)^{m} + \sum_{r=0}^{m-1} \begin{bmatrix} 2m \\ r \end{bmatrix} q^{nr} V_{2n(m-r)} [x^{r}(\omega - x)^{2m-r} + x^{2m-r}(\omega - x)^{r}].$$
(6)

Similarly, we have the analogous formula

$$S_n^{2m+1}(x) + S_n^{2m+1}(\omega - x) = \sum_{r=0}^m \begin{bmatrix} 2m+1\\r \end{bmatrix} q^{nr} V_{n(2m-2r+1)} [x^r(\omega - x)^{2m-r+1} + x^{2m-r+1}(\omega - x)^r].$$
(7)

We now have the difference formulas

$$S_n^m(x) - S_n^m(\omega - x) = \frac{\Delta^{\frac{1}{2}}}{2^{m-1}} \sum_{r=0}^{\left[\frac{m-1}{2}\right]} {m \choose 2r+1} \Delta^r U_n^{2r+1} V^{m-2r-1} \omega^{m-2r-1} (2x - \omega)^{2r+1},$$
(8)

and

$$S_n^m(x) - S_n^m(\omega - r) = \Delta^{\frac{1}{2}} \sum_{r=0}^{\left[\frac{m-1}{2}\right]} {m \choose r} q^{nr} U_{n(m-2r)} [x^{m-r}(\omega - x)^r - x^r(\omega - x)^{m-r}].$$
(9)

We shall end this section by giving the generating functions

$$\sum_{r=0}^{\infty} \frac{t^r}{r!} U_{nr} = \frac{1}{\Delta^{\frac{1}{2}}} \left(\exp(tx_1^n) - \exp(tx_2^n) \right)$$
(10)

and

$$\sum_{r=0}^{\infty} \frac{t^r}{r!} V_{nr} = \exp(tx_1^n) + \exp(tx_2^n).$$
(11)

3. First, we recall the Nörlund-Euler polynomials $E_n^{(k)}(x|\omega,...,\omega_k)$ defined by the generating expansion (see [2], [6]):

$$\sum_{r=0}^{\infty} E_r^{(k)}(x|\omega,...,\omega_k) \frac{t^r}{r!} = \frac{2^k e^{xt}}{(e^{\omega_1 t} + 1) \cdots (e^{\omega_k t} + 1)}.$$
(12)

1996]

In particular, the Nörlund-Euler numbers of order k are given by

$$E_n^{(k)}[\omega_1,\ldots,\omega_k] = 2^n E_n^{(k)} \left(\frac{\omega_1 + \cdots + \omega_k}{2} \big| \omega_1,\ldots,\omega_k \right).$$

If $\omega_1 = \cdots = \omega_k = 1$, then $E_n^{(k)}[1, 1, \dots, 1] = E_n^{(k)}$ (the Euler numbers of order k, see [3]), and we note that

$$E_n^{(k)}(\omega_1 + \dots + \omega_k - x | \omega_1, \dots, \omega_k) = (-1)^n E_n^{(k)}(x | \omega_1, \dots, \omega_k).$$
(13)

From (12), replacing t by $\Delta^{\frac{1}{2}}U_n t$, we have

$$\sum_{r=0}^{\infty} \frac{(\Delta^{\frac{1}{2}} U_n t)^r}{r!} E_r^{(k)}(x | \omega_1, \dots, \omega_k) = \frac{2^k e^{x \Delta^{\frac{1}{2}} U_n t}}{\left(e^{\omega_1 \Delta^{\frac{1}{2}} U_n t} + 1\right) \cdots \left(e^{\omega_k \Delta^{\frac{1}{2}} U_n t} + 1\right)}$$
$$= \frac{2^k}{\left(e^{\omega_1 t x_1^n} + e^{\omega_1 t x_2^n}\right) \cdots \left(e^{\omega_k t x_1^n} + e^{\omega_k t x_2^n}\right)} e^{t S_n(x)};$$

therefore,

$$\left(e^{\omega_{1}tx_{1}^{n}}+e^{\omega_{1}tx_{2}^{n}}\right)\cdots\left(e^{\omega_{k}tx_{1}^{n}}+e^{\omega_{k}tx_{2}^{n}}\right)\sum_{r=0}^{\infty}\frac{\left(\Delta^{\frac{1}{2}}U_{n}t\right)^{r}}{r!}E_{r}^{(k)}(x|\omega_{1},...,\omega_{k})=2^{k}e^{tS_{n}(x)}$$

Using (11), we obtain

$$\sum_{r_1=0}^{\infty} \frac{\omega_1^{r_1} t^{r_1}}{r_1!} V_{nr_1} \cdots \sum_{r_k=0}^{\infty} \frac{\omega_k^{r_k} t^{r_k}}{r_k!} V_{nr_k} \sum_{r=0}^{\infty} \frac{(\Delta^{\frac{1}{2}} U_n t)^r}{r!} E_r^{(k)}(x | \omega_1, \dots, \omega_k) = 2^k e^{tS_n(x)}$$

i.e.,

$$\left[\sum_{r=0}^{\infty} \left(\sum_{r_1+\dots+r_k=r} \frac{\omega_1^{r_1} V_{nr_1}}{r_1!} \cdots \frac{\omega_k^{r_k} V_{nr_k}}{r_k!}\right) t^r \right]_{r=0}^{\infty} \frac{(\Delta^{\frac{1}{2}} U_n t)^r}{r!} E_r^{(k)}(x | \omega_1, \dots, \omega_k) = 2^k e^{tS_n(x)}$$

Expanding the product, figuring in the first member, into a power series of t, and comparing with the expansion of the second member, we find

$$\sum_{r=0}^{m} \begin{bmatrix} m \\ r \end{bmatrix} \Delta^{\frac{r}{2}} U_n^r E_r^{(k)}(x | \omega_1, \dots, \omega_k) (m-r)! \sum_{r_1 + \dots + r_k = m-r} \frac{\omega_1^{r_1} V_{nr_1}}{r_1!} \cdots \frac{\omega_k^{r_k} V_{nr_k}}{r_k!} = 2^k S_n^m(x).$$
(14)

And if we replace x by $\omega_1 + \cdots + \omega_k - x$ in (14), and using (13), we have

$$\sum_{r=0}^{m} \begin{bmatrix} m \\ r \end{bmatrix} \Delta^{\frac{r}{2}} U_{n}^{r} (-1)^{r} E_{r}^{(k)} (x | \omega_{1}, ..., \omega_{k}) (m-r)! \sum_{r_{1} + \cdots + r_{k} = m-r} \frac{\omega_{1}^{r_{1}} V_{nr_{1}}}{r_{1}!} \cdots \frac{\omega_{k}^{r_{k}} v_{nr_{k}}}{r_{k}!}$$

$$= 2^{k} S_{n}^{m} (\omega_{1} + \cdots + \omega_{k} - x).$$
(15)

Taking (14) + (15), and using $\omega_1 + \cdots + \omega_k$ to replace ω in (5), (6), and (7), we obtain

[AUG.

$$\sum_{r=0}^{\left[\frac{m}{2}\right]} \sum_{r=0}^{m} \left[2r\right] \Delta^{r} U_{n}^{2r} E_{2r}^{(k)}(x | \omega_{1}, ..., \omega_{k})(m-2r)! \sum_{r_{1}+...+r_{k}=m-2r} \frac{\omega_{1}^{r_{1}} V_{m_{1}}}{r_{1}!} ... \frac{\omega_{k}^{r_{k}} V_{m_{k}}}{r_{k}!}$$

$$= \frac{1}{2^{m-k}} \sum_{r=0}^{\left[\frac{m}{2}\right]} \left[2r\right] \Delta^{r} U_{n}^{2r} V_{n}^{m-2r} (\omega_{1}+...+\omega_{k})^{m-2r} (2x-(\omega_{1}+...+\omega_{k}))^{2r}$$

$$= (1+(-1)^{m}) 2^{k-1} \left[\frac{m}{m/2}\right] q^{mn/2} (x(\omega_{1}+...+\omega_{k}-x))^{m/2} + 2^{k-1} \sum_{r=0}^{\left[\frac{m-1}{2}\right]} \left[\frac{m}{r}\right] q^{nr}$$

$$\cdot V_{n(m-2r)} [x^{r} (\omega_{1}+...+\omega_{k}-x)^{m-r} + x^{m-r} (\omega_{1}+...+\omega_{k}-x)^{r}].$$

$$(16)$$

Taking (14) – (15), and using $\omega_1 + \cdots + \omega_k$ to replace ω in (8) and (9), we get

$$\sum_{r=0}^{\left[\frac{m-1}{2}\right]} \left[2r+1 \right] \Delta^{r} U_{n}^{2r+1} E_{2r+1}^{(k)}(x | \omega_{1}, ..., \omega_{k})(m-2r-1)! \sum_{r_{1}+\dots+r_{k}=m-2r-1} \left(\frac{\omega_{1}^{r_{1}} V_{mr_{1}}}{r_{1}!} \cdots \frac{\omega_{k}^{r_{k}} V_{mr_{k}}}{r_{k}!} \right)$$

$$= \frac{1}{2^{m-k}} \sum_{r=0}^{\left[\frac{m-1}{2}\right]} \left[2r+1 \right] \Delta^{r} U_{n}^{2r+1} V_{n}^{m-2r-1} (\omega_{1}+\dots+\omega_{k})^{m-2r-1} (2x-(\omega_{1}+\dots+\omega_{k}))^{2r+1}$$

$$= 2^{k-1} \sum_{r=0}^{\left[\frac{m-1}{2}\right]} \left[m \atop r \right] q^{mr} U_{n(m-2r)} [x^{m-r} (\omega_{1}+\dots+\omega_{k}-x)^{r} - x^{r} (\omega_{1}+\dots+\omega_{k}-x)^{m-r}].$$
(18)

4. If we take $x = \frac{\omega_1 + \dots + \omega_k}{2}$ in (16), then

$$\sum_{r=0}^{\left[\frac{m}{2}\right]} \left[\sum_{2r}^{m} \right] \Delta^{r} U_{n}^{2r} \frac{1}{2^{2r}} E_{2r}^{(k)} [\omega_{1}, ..., \omega_{k}] (m-2r)! \sum_{r_{1}+\cdots+r_{k}=m-2r} \frac{\omega_{1}^{r_{1}} V_{nr_{1}}}{r_{1}!} \cdots \frac{\omega_{k}^{r_{k}} v_{nr_{k}}}{r_{k}!}$$

$$= \frac{1}{2^{m-k}} (\omega_{1} + \dots + \omega_{k})^{m} V_{n}^{m}.$$
(20)

Now, setting $\omega_1 = \cdots = \omega_k = 1$ in (20), we have

$$\sum_{r=0}^{\left[\frac{m}{2}\right]} \left[\frac{m}{2r} \right] \Delta^{r} U_{n}^{2r} \frac{E_{2r}^{(k)}}{2^{2r}} (m-2r)! \sum_{r_{1}+\dots+r_{k}=m-2r} \frac{V_{nr_{1}}}{r_{1}!} \cdots \frac{V_{nr_{k}}}{r_{k}!} = \frac{1}{2^{m-k}} k^{m} V_{n}^{m}.$$
(21)

Again, if we take k = 1, then

$$\sum_{r=0}^{\left[\frac{m}{2}\right]} \left[\sum_{r=0}^{m} \right] \Delta^{r} U_{n}^{2r} \frac{E_{2r}}{2^{2r}} V_{n(m-2r)} = \frac{1}{2^{m-1}} V_{n}^{m}.$$
(22)

If we set k = 1 in (18), we obtain

1996]

RECURRENCE SEQUENCES AND NÖRLUND-EULER POLYNOMIALS

$$\sum_{r=0}^{\left[\frac{m-1}{2}\right]} \begin{bmatrix} m\\2r+1 \end{bmatrix} \Delta^{r} U_{n}^{2r+1}(x|\omega_{1}) V_{n(m-2r-1)} \omega_{1}^{m-2r-1} = \frac{1}{2^{m-1}} \sum_{r=0}^{\left[\frac{m-1}{2}\right]} \begin{bmatrix} m\\2r+1 \end{bmatrix} \Delta^{r} U_{n}^{2r+1} V_{n}^{m-2r-1} \omega_{1}^{m-2r-1} (2x-\omega_{1})^{2r+1}.$$
(23)

Now, taking $\omega_1 = 1$ and x = 0 or $x = \frac{1}{3}$, and using the following relations (see [1]),

$$E_{n-1}(0) = 2(1-2^n)\frac{B_n}{n},$$
$$E_{2n-1}\left(\frac{1}{3}\right) = (2^{2n}-1)\left(\frac{1}{3^{2n}-1}\right)\frac{B_{2n}}{2n},$$

where B_n is a Bernoulli number, we have

$$\sum_{r=0}^{\left\lfloor\frac{m-1}{2}\right\rfloor} \begin{bmatrix} m\\2r+1 \end{bmatrix} \Delta^{r} U_{n}^{2r+1} \frac{1}{r+1} (2^{2r+2}-1) B_{2r+2} V_{n(m-2r-1)}$$

$$= \frac{1}{2^{m-1}} \sum_{r=0}^{\left\lfloor\frac{m-1}{2}\right\rfloor} \begin{bmatrix} m\\2r+1 \end{bmatrix} \Delta^{r} U_{n}^{2r+1} V_{n}^{m-2r-1},$$
(24)

and

$$\sum_{r=0}^{\left[\frac{m-1}{2}\right]} \left[{m \atop 2r+1} \right] \Delta^{r} U_{n}^{2r+1} (2^{2r+2}-1) \left(1 - \frac{1}{3^{2r+1}} \right) \frac{B_{2r+2}}{2r+2} V_{n(m-2r-1)}$$

$$= \frac{1}{2^{m-1}} \sum_{r=0}^{\left[\frac{m-1}{2}\right]} \left[{m \atop 2r+1} \right] \Delta^{r} U_{n}^{2r+1} V_{n}^{m-2r-1} \frac{1}{3^{2r+1}}.$$
(25)

Assuming p = 1 and q = -1, we have the so-called Fibonacci and Lucas sequences

 $U_n = F_n$ and $V_n = L_n$,

respectively. And from (22), (24), and (25), it follows that

$$\sum_{r=0}^{\left\lfloor\frac{m}{2}\right\rfloor} \begin{bmatrix}m\\2r\end{bmatrix} 5^r F_n^{2r} \frac{E_{2r}}{2^{2r}} L_{n(m-2r)} = \frac{1}{2^{m-1}} L_n^m,$$
(26)

$$\sum_{r=0}^{\left\lfloor\frac{m-1}{2}\right\rfloor} \left[2r + 1 \right] 5^{r} F_{n}^{2r+1} \frac{1}{r+1} (2^{2r+2} - 1) B_{2r+2} L_{n(m-2r-1)}$$

$$= \frac{1}{2^{m-1}} \sum_{r=0}^{\left\lfloor\frac{m-1}{2}\right\rfloor} \left[2r + 1 \right] 5^{r} F_{n}^{2r+1} L_{n}^{m-2r-1},$$
(27)

and

[AUG.

RECURRENCE SEQUENCES AND NÖRLUND-EULER POLYNOMIALS

$$\sum_{r=0}^{\left[\frac{m-1}{2}\right]} \left[2r + 1 \right] 5^{r} F_{n}^{2r+1} (2^{2r+2} - 1) \left(1 - \frac{1}{3^{2r+1}} \right) \frac{B_{2r+2}}{2r+2} L_{n(m-2r-1)}$$

$$= \frac{1}{2^{m-1}} \sum_{r=0}^{\left[\frac{m-1}{2}\right]} \left[2r + 1 \right] 5^{r} F_{n}^{2r+1} L_{n}^{(m-2r-1)} \frac{1}{3^{2r+1}},$$
(28)

where (26) is a generalization of P. F. Byrd's result (see [5]):

$$\sum_{r=0}^{\lfloor \frac{m}{2} \rfloor} 5^r \begin{bmatrix} m \\ 2r \end{bmatrix} B_{2r} F_n^{2r} F_{n(m-2r)} = \frac{m}{2} F_n L_{n(m-1)}.$$

ACKNOWLEDGMENT

The authors wish to thank the referees for their patience and for suggestions that significantly improved the appearance of this paper.

REFERENCES

- 1. L. Toscano. "Recurring Sequences and Bernoulli-Euler Polynomials." J. Comb. Inform. & System Sci. 4 (1979):303-08.
- 2. L. Carlitz. "Eulerian Numbers and Polynomials of Higher Order." *Duke Math. J.* 27 (1960): 401-23.
- 3. L. C. Hsu. "Finding Some Strange Identities via Faa di Bruno's Formula." J. Math. Research & Exposition 13 (1993):159-65.
- 4. R. P. Kelisky. "On Formulas Involving Both the Bernoulli and Fibonacci Numbers." *Scripta Math.* 23 (1957):27-35.
- 5. P. F. Byrd. "Relations between Euler and Lucas Numbers." *The Fibonacci Quarterly* **13.2** (1975):111-14.
- 6. N. E. Nörlund. Vorlesungen ober differenzenrechung. Berlin, 1924.
- 7. Zhang Zhizheng. "Recurrence Sequences and Bernoulli Polynomials of Higher Order." *The Fibonacci Quarterly* **33.4** (1995):359-62.

AMS Classification Numbers: 11B39, 11B37

* * *

1996]

ON THE LIMIT OF GENERALIZED GOLDEN NUMBERS

Hongquan Yu, Yi Wang, and Mingfeng He

Dalian University of Technology, Dalian 116024, China (Submitted November 1994)

1. INTRODUCTION

In this paper we discuss the asymptotic behavior of maximal real roots of generalized Fibonacci polynomials defined recursively by

$$G_{n+2}(x) = xG_{n+1}(x) + G_n(x), \tag{1}$$

for $n \ge 0$, with $G_0(x) = -a$, $G_1(x) = x - a$, where a is a real number.

Very recently, G. A. Moore [2] considered, among other things, the limiting behavior of the maximal real roots of $G_n(x)$ defined by (1), and with $G_0(x) = -1$, $G_1(x) = x - 1$. Let g_n denote the maximal real root of $G_n(x)$ which may be called "the generalized golden numbers" following [1]. G. Moore confirmed an implication of computer analysis that the odd-indexed subsequence of $\{g_n\}$ is monotonically increasing and convergent to 3/2 from below, while the even-indexed subsequence of $\{g_n\}$ is monotonically decreasing and convergent to 3/2 from above. Moreover, it was shown that $\{g_n\}$, n > 2, is a sequence of irrational numbers. He also guessed that this result may be generalized in the sense that there exists a real number taking the place of 3/2 for other kinds of Fibonacci polynomial sequences defined by (1) with given $G_0(x)$ and $G_1(x)$.

Here we generalize Moore's result by showing that, for Fibonacci polynomial sequences defined by (1) with $G_0(x) = -a$, $G_1(x) = x - a$, where a is a positive real number, a(a+2)/(a+1) is just the limit of the maximal real roots of $G_n(x)$.

It is noteworthy that the demonstration here is different from Moore's in that it does not rely on the previous knowledge of $\{G_n(x)\}$ on the limit point of g_n . In other words, we shall proceed here in a "deductive" rather than a "confirmative" way.

2. EXISTENCE OF $\{g_n\}$

Let $\{G_n(x)\}\$ be defined by (1) with $G_0(x) = -a$, $G_1(x) = x - a$, with a > 0. It can be checked easily by induction that each $G_n(x)$ is monic with degree *n* and constant term -a. Therefore, for each $n \ge 1$, $G_n(x)$ will tend to positive infinity for x large enough.

Note that $G_1(a) = 0$, $G_2(a) = -a < 0$, $G_3(a) = -a^2 = aG_2(a) < 0$, $G_4(a) = -a^3 - a \le aG_3(a) < 0$, by induction; suppose that $G_k(a) \le aG_{k-1}(a) < 0$ for $k \ge 2$. Then, from (1), $G_{k+1}(a) = aG_k(a) + G_{k-1}(a) < 0$, and the induction is completed. Therefore, for each $n \ge 1$, there exists at least one real root of $G_n(x)$ on $[a, +\infty)$ and, by definition, $g_n > a$.

On the other hand, it can be checked readily using the recursive relation (1) and by an induction argument that we have $G_n(x) > 0$ for $x \in [a+1, +\infty)$.

Therefore, each $G_n(x)$ $(n \ge 2)$ has at least one root on the interval [a, a+1). In particular, $g_n \in [a, a+1)$.

Lemma 2.1:^[2] If r is the maximal real root of a function f with positive leading coefficient, then f(x) > 0 for all $x \ge r$. Conversely, if f(x) > 0 for all $x \ge t$, then r < t. If f(s) < 0, then s < r.

320

Remark 2.2: If $a \ge 1$ is an integer, then a standard algebraic argument may be applied to show that the maximal real root of $G_n(x)$ is actually irrational.

3. THE MONOTONICITY OF $\{g_{2n-1}\}$ AND $\{g_{2n}\}$

To illustrate the monotonicity of $\{g_{2n-1}\}$ and $\{g_{2n}\}$, we need a formula of [2] which may be verified by induction.

Formula 3.1: $G_{n+k}(g_n) = (-1)^{k+1} G_{n-k}(g_n)$ for $n \ge k$.

Proposition 3.2: $\{g_{2n-1}\}\$ is a monotonically increasing sequence and $\{g_{2n}\}\$ is a monotonically decreasing sequence. Moreover, $g_{2n-1} < g_{2n}$.

Proof:

<u>Odd-Indexed Sequence</u>. It can be checked readily that $G_3(a) = -a^2 < 0$; thus, $g_3 > a = g_1$. Assume that, by induction, $g_1 < g_3 < \cdots < g_{2k-3} < g_{2k-1}$. Then, by Lemma 2.1, $G_{2k-3}(g_{2k-1}) > G_{2k-3}(g_{2k-3}) = 0$. Using Formula 3.1, we get

$$G_{2k+1}(g_{2k-1}) = G_{(2k-1)+2}(g_{2k-1}) = (-1)^3 G_{(2k-1)-2}(g_{2k-1}) < 0.$$

It follows from Lemma 2.1 that G_{2k+1} has a real root greater than g_{2k-1} , and thus $g_{2k-1} < g_{2k+1}$.

Even-Indexed Sequence. Using recursive formula (1), one obtains

$$g_{2k+1}(g_{2k-1}) = g_{2k-1}G_{2k}(g_{2k-1}) + G_{2k-1}(g_{2k-1}) = g_{2k-1}G_{2k}(g_{2k-1}).$$

Since $g_{2k-1} < g_{2k}$, it follows from Lemma 2.1 that $G_{2k-1}(g_{2k}) > 0$, thus $G_{2k-2}(g_{2k}) < 0$, and it follows from Lemma 2.1 again that $g_{2k} < g_{2k-2}$. \Box

4. THE CONVERGENCE OF g_{2n-1} AND g_{2n}

It is known now that $\{g_{2n-1}\}\$ is monotonically increasing, bounded above by a+1, and $\{g_{2n}\}\$ is monotonically decreasing, bounded below by a. Thus, limits exist for both of the sequences. Denote by $g_{\text{odd}} =: \lim_{n \to \infty} g_{2n-1}, g_{\text{even}} =: \lim_{n \to \infty} g_{2n}$. Then Proposition 3.2 implies $g_{\text{odd}} \leq g_{\text{even}}$. Our aim here is to show that $g_{\text{odd}} = g_{\text{even}}$, which is included in the following theorem.

Theorem 4.1: Both $\{g_{2n-1}\}$ and $\{g_{2n}\}$ converge to $\xi = a(a+2)/(a+1)$ when n tends to infinity.

Remark 4.2: If a is an integer, then, from Proposition 3.2, g_n is a sequence of irrationals that converges to a rational number a(a+2)/(a+1). This reduces to Moore's result in [2] when a = 1.

Proof: Since $G_n(x)$ may be expressed in terms of roots of its characteristic equation as

$$G_n(x) = C_1(x)\lambda_1(x)^n + C_2(x)\lambda_2(x)^n,$$
(2)

where

$$\lambda_1(x) = \frac{x + \sqrt{x^2 + 4}}{2} > \lambda_2(x) = \frac{x - \sqrt{x^2 + 4}}{2}, \qquad (3)$$

and

1996]

$$C_{1}(x) = \left[2(x-a) + ax - a\sqrt{x^{2}+4}\right] / 2\sqrt{x^{2}+4},$$

$$C_{2}(x) = \left[-2(x-a) - ax - a\sqrt{x^{2}+4}\right] / 2\sqrt{x^{2}+4}.$$
(4)

It is seen readily that $\lambda_1(x) \ge \lambda_1(a) > 1$, $|\lambda_2(x)| = 1/\lambda_1(x) \le 1/\lambda_1(a)$ for $x \in [a, a+1]$. Therefore, $\lim_{n\to\infty} \lambda_1(x)^n = +\infty$, $\lim_{n\to\infty} \lambda_2(x)^n = 0$ uniformly for $x \in [a, a+1]$.

Now, setting n = 2k - 1 and $x = g_{2k-1}$ in (2), we obtain

$$C_1(g_{2k-1})\lambda_1(g_{2k-1})^{2k-1}+C_2(g_{2k-1})\lambda_2(g_{2k-1})^{2k-1}=0.$$

Since $C_1(x)$ and $C_2(x)$ are continuous on the interval [a, a+1], this implies that $|C_1(x)|$ and $|C_2(x)|$ are bounded below and above on [a, a+1]. Therefore, we have

$$\lim_{k \to \infty} C_1(g_{2k-1}) = C_1(g_{odd}) = 0,$$

and it follows that $g_{\text{odd}} = \lim_{k \to \infty} g_{2k-1} = a(a+2)/(a+1)$ by the continuity of $C_1(x)$.

On the other hand, by taking n = 2k in (2), a similar argument can be applied to show that $g_{\text{even}} = a(a+2)/(a+1)$. \Box

Note that $\lim_{n\to\infty} g_n = 1$ if and only if $a = (\sqrt{5} - 1)/2$, the original golden number.

In conclusion, we remark that it may be shown easily that the maximal real root of $G'_n(x)$, denoted by g'_n , also exists on the interval (a, a+1) for $n \ge 4$. It seems, from numerical analysis, that the sequence $\{g'_n\}$ is monotonically increasing and converges to $\xi = a(a+2)/(a+1)$. This implication deserves further exposition.

REFERENCES

- 1. G. Moore. "A Fibonacci Polynomial Sequence Defined by Multidimensional Continued Fractions; and Higher-Order Golden Ratios." *The Fibonacci Quarterly* **31.4** (1993):354-64.
- 2. G. A. Moore. "The Limit of the Golden Numbers Is 3/2." *The Fibonacci Quarterly* 32.3 (1993):211-17.

AMS Classification Numbers: 11B39, 11B37

$\diamond \diamond \diamond$
A TEN POINT FFT CALCULATION WHICH FEATURES THE GOLDEN RATIO

J. M. H. Peters

The Liverpool John Moores University, Byrom Street, Liverpool L3 3AF, UK (Submitted November 1994)

1. INTRODUCTION

One version of a discrete Fourier transform pair based on N equally spaced sample points is

$$\bar{x}_m = \sum_{n=0}^{N-1} x_n e^{-\frac{2\pi j m n}{N}}, \qquad s_m = \frac{1}{N} \sum_{n=0}^{N-1} \bar{x}_n e^{\frac{2\pi j m n}{N}}, \qquad (1)$$

where $x_m = f(mT): m = 0, 1, 2, ..., N-1$ for a given temporal function f(t) of appropriate form, where T is the sampling interval in the time domain.

2. EXAMPLE

James et al., in [1], consider the function

$$F(t) = \begin{cases} t: & 0 \le t \le \frac{1}{2}, \\ 1 - t: & \frac{1}{2} \le t \le 1, \\ 0: & t > 1, \end{cases}$$

with N = 10 and T = 1/5 sec, for which the discrete Fourier transform, computed according to (1), reduces to

$$\overline{x}_m = \frac{\left(e^{-\frac{\pi j m}{5}} + 2\left(e^{-\frac{2\pi j m}{5}} + e^{-\frac{3\pi j m}{5}}\right) + e^{-\frac{4\pi j m}{5}}\right)}{5}.$$

3. MATRIX FORMULATION

It is especially interesting, however, to give a ten point FFT analysis, where the complex exponentials are tenth roots of unity that involve the golden ratio $\tau = (1 + \sqrt{5})/2$, which itself is the positive root of the quadratic equation $\tau^2 - \tau - 1 = 0$. By expressing results initially in terms of τ , rather than decimal numbers, we are able to appreciate deeper symmetries in the FFT.

By writing $\omega = e^{-\frac{\pi i}{5}} = \frac{1}{2} \left(\tau - j \sqrt{\sqrt{5} / \tau} \right)$, a tenth root of unity, the matrix representation of the first of (1) is as shown in (3) below, where the various powers of ω are, with asterisks denoting complex conjugates:

$$\omega^{0} = 1, \ \omega = \frac{(\tau - j\alpha)}{2}, \ \omega^{2} = \frac{(1/\tau - j\alpha)}{2}, \ \omega^{3} = \frac{-(1/\tau + j\alpha)}{2} = -\omega^{*2},$$
$$\omega^{4} = \frac{-(\tau + j\alpha)}{2} = -\omega^{*}, \ \omega^{5} = -1, \ \omega^{6} = \frac{-(\tau - j\alpha)}{2} = \omega^{*4},$$

1996]

A TEN POINT FFT CALCULATION WHICH FEATURES THE GOLDEN RATIO

$$\omega^{7} = \frac{-(1/\tau - j\alpha)}{2} = \omega^{*3}, \ \omega^{8} = \frac{(1/\tau + j\alpha)}{2} = \omega^{*2}, \ \omega^{9} = \frac{(\tau + j\alpha)}{2} = \omega^{*},$$
(2)

where $\alpha = \sqrt{\sqrt{5} / \tau}$, see [2],

4. FACTORIZATION

To factor the matrix in (3), we adopt the approach used in [1], noting first that $N = 10 = 2 \times 5$ is composite, with factors $r_1 = 2$ and $r_2 = 5$. Putting

$$n = 2n_1 + n_0; \quad n_0 = 0, 1; \quad n_1 = 0, 1, 2, 3, 4, m = 5m_1 + m_1; \quad m_0 = 0, 1, 2, 3, 4; \quad m_1 = 0, 1,$$

we can write the simultaneous system (3) as

$$\overline{x}_{5m_1+m_0} = \sum_{n_0=0}^{1} \left(\sum_{n_1=0}^{4} x_{2n_1+n_0} \omega^{2n_1m_0} \right) \omega^{(5m_1+m_0)n_0}.$$
(4)

Setting

$$\xi_{m_0 n_0} = \sum_{n_1=0}^{4} x_{2n_1+n_0} \omega^{2n_1 m_0} : n_0 = 0, 1; \ m_0 = 0, 1, 2, 3, 4,$$
(5)

then leads to a set of simultaneous equations, summarized in matrix form by

$$\begin{bmatrix} \xi_{00} \\ \xi_{01} \\ \xi_{10} \\ \xi_{10} \\ \xi_{11} \\ \xi_{20} \\ \xi_{21} \\ \xi_{30} \\ \xi_{31} \\ \xi_{30} \\ \xi_{31} \\ \xi_{40} \\ \xi_{41} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & \omega^2 & 0 & \omega^4 & 0 & \omega^6 & 0 & \omega^8 & 0 \\ 0 & 1 & 0 & \omega^2 & 0 & \omega^4 & 0 & \omega^6 & 0 & \omega^8 \\ 1 & 0 & \omega^4 & 0 & \omega^8 & 0 & \omega^2 & 0 & \omega^6 & 0 \\ 0 & 1 & 0 & \omega^4 & 0 & \omega^8 & 0 & \omega^2 & 0 & \omega^6 \\ 1 & 0 & \omega^6 & 0 & \omega^2 & 0 & \omega^8 & 0 & \omega^4 & 0 \\ 1 & 0 & \omega^6 & 0 & \omega^2 & 0 & \omega^8 & 0 & \omega^4 & 0 \\ 1 & 0 & \omega^8 & 0 & \omega^6 & 0 & \omega^4 & 0 & \omega^2 & 0 \\ 0 & 1 & 0 & \omega^8 & 0 & \omega^6 & 0 & \omega^4 & 0 & \omega^2 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \end{bmatrix} .$$

(6)

(3)

324

[AUG.

5. SOLUTIONS

Inserting the appropriate powers of ω , summarized in (2), into the linear system (6), leads to the following results:

$$\begin{aligned} \xi_{00} &= 3/5 = \xi_{01}, \\ \xi_{20} &= \frac{\left(-\tau^2 - j\sqrt{\sqrt{5}/\tau^5}\right)}{10}, \\ \xi_{20} &= \frac{\left(-\tau^2 - j\sqrt{\sqrt{5}/\tau^5}\right)}{10}, \\ \xi_{21} &= \frac{\left(-\frac{1}{\tau} - j\sqrt{\sqrt{5}/\tau}\right)}{5}, \\ \xi_{31} &= \frac{\left(-\frac{1}{\tau} + j\sqrt{\sqrt{5}/\tau}\right)}{5} = \overline{\xi}_{21}, \\ \xi_{40} &= \frac{\left(-\frac{1}{\tau^2} + j\sqrt{\sqrt{5}\tau^5}\right)}{10} = \overline{\xi}_{10}, \\ \xi_{41} &= \frac{\left(\tau + j\sqrt{\sqrt{5}\tau}\right)}{5} = \overline{\xi}_{11}. \end{aligned}$$

Returning to the system (4) we see that, with (5), we can write

$$\overline{x}_{5m_1+m_0} = \sum_{n_0=0}^{1} \xi_{m_0n_0} \omega^{(5m_1+m_0)n_0} : m_0 = 0, 1, 2, 3, 4; m_1 = 0, 1.$$

6. NUMERICAL RESULTS

Expansion leads to

$$\begin{split} \overline{x}_0 &= \xi_{00} + \xi_{01} = 6/5 = 1.2, \\ \overline{x}_1 &= \xi_{10} + \xi_{11}\omega = -j\sqrt{\sqrt{5}\tau^5}/5 = -j0.9959593, \\ \overline{x}_2 &= \xi_{20} + \xi_{21}\omega^2 = -\tau^2/5 = -0.5236068, \\ \overline{x}_3 &= \xi_{30} + \xi_{31}\omega^3 = j\sqrt{\sqrt{5}/t^5} = j0.0898055, \\ \overline{x}_4 &= \xi_{40} + \xi_{41}\omega^4 = -(1/\tau^2)/5 = -0.076392, \\ \overline{x}_5 &= \xi_{00} + \xi_{01}\omega^5 = 0, \\ \overline{x}_6 &= \xi_{10} + \xi_{11}\omega^6 = \overline{x}_4^* = -(1/\tau^2)/5 = -0.076392, \\ \overline{x}_7 &= \xi_{20} + \xi_{21}\omega^7 = \overline{x}_3^* = -j\sqrt{\sqrt{5}/\tau^5} = -j0.0898055, \\ \overline{x}_8 &= \xi_{30} + \xi_{31}\omega^8 = \overline{x}_2^* = -\tau^5/5 = -0.5236068, \\ \overline{x}_9 &= \xi_{40} + \xi_{41}\omega^9 = \overline{x}_1^* = j\sqrt{\sqrt{5}t^5}/5 = j0.9959593. \end{split}$$

Multiplying each of these by T = 0.2 gives James et al.'s final results (see [1]).

REFERENCES

- 1. G. James et al. Advanced Modern Engineering Mathematics. New York: Addison-Wesley, 1993.
- 2. Marjorie Bicknell & Verner E. Hoggatt, Jr. (eds.). *A Primer for the Fibonacci Numbers*, pp. 74-75. Santa Clara, CA: The Fibonacci Association, 1972.

AMS Classification Numbers: 11B39, 15A23, 65T20

** ** **

ON A BINOMIAL SUM FOR THE FIBONACCI AND RELATED NUMBERS

Pentti Haukkanen

Department of Mathematical Sciences, University of Tampere, P.O. Box 607, FIN-33101 Tampere, Finland (Submitted November 1994)

1. INTRODUCTION

Let u and v be nonzero integers, and let r be an integer. It is well known that

$$F_{un+r} = \sum_{k=0}^{n} \binom{n}{k} t^{n-k} s^{k} F_{vk+r}, \quad n = 0, 1, 2, ...,$$
(1)

if and only if

$$s = F_u / F_v, \quad t = (-1)^u F_{v-u} / F_v.$$
 (2)

This result originates with Carlitz [2], and was recently interpreted via exponential generating functions (or egfs) by Prodinger [7]. The purpose of this paper is to show that the egf method is also an efficient tool in deriving similar results for the Lucas numbers L_n , the Pell numbers P_n , and the Pell-Lucas numbers R_n .

The egf of a sequence $\{a_n\}$ is defined by

$$\hat{a}(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}$$

The product of the egfs of $\{a_n\}$ and $\{b_n\}$ generates the binomial convolution of $\{a_n\}$ and $\{b_n\}$:

$$\hat{a}(x)\hat{b}(x) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \binom{n}{k} a_{n-k} b_k \right) \frac{x^n}{n!}.$$
(3)

The right side of (1) is thus the binomial convolution of the sequences $\{t^n\}$ and $\{s^n F_{\nu n+r}\}$. The egf of the geometric progression $\{t^n\}$ is e^{tx} .

The proofs of this note are based on the following two lemmas.

Lemma 1: Let λ_1 and λ_2 be given distinct complex numbers, and let c_1 and c_2 be given nonzero *distinct* complex numbers. Then

$$c_1 e^{\lambda_1 x} + c_2 e^{\lambda_2 x} = c_1 e^{\mu_1 x} + c_2 e^{\mu_2 x}$$

if and only if

$$\mu_1 = \lambda_1$$
 and $\mu_2 = \lambda_2$.

Lemma 2: Let λ_1 and λ_2 be given distinct complex numbers, and let c be a given nonzero complex number. Then

$$ce^{\lambda_1 x} + ce^{\lambda_2 x} = ce^{\mu_1 x} + ce^{\mu_2 x}$$

[AUG.

if and only if either

or

$$\mu_1 = \lambda_1$$
 and $\mu_2 = \lambda_2$
 $\mu_1 = \lambda_2$ and $\mu_2 = \lambda_1$.

The lemmas follow from the linear independence of the functions $e^{\lambda x}$.

Lemma 1 is needed for the Fibonacci and the Pell numbers, and for the Lucas and the Pell-Lucas numbers in the case $r \neq 0$, while Lemma 2 is needed for the Lucas and the Pell-Lucas numbers in the case r = 0. We do not consider Fibonacci numbers here, since the egf method is applied to them in [7].

For a general account on egf's we refer to [4], and for egf's of Fibonacci and Lucas sequences we refer to [3], [5], and [6].

2. ON THE LUCAS NUMBERS

Let the negative index Fibonacci and Lucas numbers be defined by $F_{-n} = (-1)^{n+1}F_n$ and $L_{-n} = (-1)^n L_n$ $(n \ge 0)$. Let $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. The well-known Binet form of the Lucas numbers is $L_n = \alpha^n + \beta^n$. Thus, it is easy to see that

$$\hat{L}(x) = e^{\alpha x} + e^{\beta x}$$

We now state the promised binomial results for the Lucas numbers. We distinguish two cases: $r \neq 0$ and r = 0.

Theorem 1: Let u and v be nonzero integers, and let r be a nonzero integer. Then

$$L_{un+r} = \sum_{k=0}^{n} \binom{n}{k} t^{n-k} s^{k} L_{vk+r}, \quad n = 0, 1, 2, ...,$$
(4)

if and only if

$$s = F_u / F_v, \quad t = (-1)^u F_{v-u} / F_v.$$
 (5)

Proof: In terms of the egfs, (4) can be written as

$$\alpha^{r}e^{\alpha^{u}x} + \beta^{r}e^{\beta^{u}x} = e^{tx}(\alpha^{r}e^{\alpha^{v}sx} + \beta^{r}e^{\beta^{v}sx}), \qquad (6)$$

where the right side comes from the property (3). Since $r \neq 0$, we have $\alpha^r \neq \beta^r$. Thus, by Lemma 1, (6) holds if and only if

$$\alpha^{u} = t + \alpha^{v} s, \quad \beta^{u} = t + \beta^{v} s, \tag{7}$$

that is,

$$s = \frac{\alpha^u - \beta^u}{\alpha^v - \beta^v} = \frac{F_u}{F_v}, \text{ and } t = \alpha^u - \alpha^v \frac{\alpha^u - \beta^u}{\alpha^v - \beta^v} = (-1)^u \frac{F_{v-u}}{F_v},$$

where the last equality follows from the property $\alpha\beta = -1$. This completes the proof of Theorem 1.

Remark: Note that (5) is equivalent to (2).

1996]

Theorem 2: Let u and v be nonzero integers (and r = 0). Then

$$L_{un} = \sum_{k=0}^{n} {n \choose k} t^{n-k} s^{k} L_{\nu k}, \quad n = 0, 1, 2, ...,$$
(8)

if and only if either (5) holds or

$$s = -F_u / F_v, \quad t = F_{u+v} / F_v.$$
 (9)

Proof: In terms of the egfs, (8) can be written as

$$e^{\alpha^{u}x} + e^{\beta^{u}x} = e^{tx}(e^{\alpha^{v}sx} + e^{\beta^{v}sx}),$$
(10)

where the right side comes from property (3). By Lemma 2, (10) holds if and only if either (7) holds or

$$\alpha^{u} = t + \beta^{v} s, \quad \beta^{u} = t + \alpha^{v} s. \tag{11}$$

By the proof of Theorem 1, (7) is equivalent to (5). On the other hand, (11) holds if and only if

$$s = \frac{\beta^u - \alpha^u}{\alpha^v - \beta^v} = \frac{-F_u}{F_v}$$
, and $t = \alpha^u - \beta^v \frac{\beta^u - \alpha^u}{\alpha^v - \beta^v} = \frac{F_{u+v}}{F_v}$.

This completes the proof of Theorem 2.

Corollary 1: If u and v are nonzero integers and r is an integer, then

$$F_{\nu}^{n}L_{un+r} = \sum_{k=0}^{n} \binom{n}{k} (-1)^{u(n-k)} F_{\nu-u}^{n-k} F_{u}^{k} L_{\nu k+r}$$

$$F_{\nu}^{n}L_{un} = \sum_{k=0}^{n} \binom{n}{k} F_{u+\nu}^{n-k} (-1)^{k} F_{u}^{k} L_{\nu k}.$$

Corollary 2: If u is a nonzero integer and r is an integer, then

$$L_{un+r} = \sum_{k=0}^{n} \binom{n}{k} F_{u-1}^{n-k} F_{u}^{k} L_{k+r},$$
$$L_{un} = \sum_{k=0}^{n} \binom{n}{k} F_{u+1}^{n-k} (-1)^{k} F_{u}^{k} L_{k}.$$

Corollary 3: If *r* is an integer, then

$$L_{2n+r} = \sum_{k=0}^{n} \binom{n}{k} L_{k+r},$$
$$L_{2n} = \sum_{k=0}^{n} \binom{n}{k} 2^{n-k} (-1)^{k} L_{k}.$$

Corollary 1 follows from Theorems 1 and 2. Corollary 2 is Corollary 1 with v = 1, and Corollary 3 is Corollary 2 with u = 2. Note that the first identities in Corollaries 1-3 also hold for r = 0, cf. equation (5) in Theorem 2.

AUG.

3. ON THE PELL NUMBERS

The Pell numbers P_n are defined by

$$P_0 = 0, P_1 = 1, P_n = 2P_{n-1} + P_{n-2}, \quad n = 2, 3, ...,$$

 $P_{-n} = (-1)^{n+1}P_n, \quad n = 1, 2,$

The well-known Binet form of the Pell numbers is

$$P_n = \frac{a^n - b^n}{a - b},$$

where $a = 1 + \sqrt{2}$, $b = 1 - \sqrt{2}$, that is, where a and b are the roots of the equation $y^2 = 2y + 1$, see, e.g., [1]. Note that a + b = 2, ab = -1, and $a - b = 2\sqrt{2}$. Using the Binet form, it is easy to see that

$$\hat{P}(x) = \frac{1}{2\sqrt{2}} \left(e^{ax} - e^{bx} \right).$$

The Pell numbers have many properties similar to those of the Fibonacci numbers. We here point out that a property analogous to that given in (1) and (2) holds for the Pell numbers. As in the case of the Fibonacci numbers, we need not distinguish the cases $r \neq 0$ and r = 0 here.

Theorem 3: Let u and v be nonzero integers, and let r be an integer. Then

$$P_{un+r} = \sum_{k=0}^{n} \binom{n}{k} t^{n-k} s^{k} P_{vk+r}, \quad n = 0, 1, 2, ...,$$
(12)

if and only if

$$s = P_u / P_v, \quad t = (-1)^u P_{v-u} / P_v.$$
 (13)

Proof: In terms of the egf's, (12) is

$$\frac{1}{2\sqrt{2}}(a^{r}e^{a^{u}x}-b^{r}e^{b^{u}x})=e^{tx}\frac{1}{2\sqrt{2}}(a^{r}e^{a^{v}sx}-b^{r}e^{b^{v}sx}).$$
(14)

Since $a^r \neq -b^r$ for all r, we may apply Lemma 1. Thus (14) holds if and only if

$$a^{\mu} = t + a^{\nu}s, \quad b^{\mu} = t + b^{\nu}s,$$
 (15)

which can be shown to hold if and only if (13) holds; cf. the proof of (5). The last equality in (13) follows from the property ab = -1. This completes the proof of Theorem 3.

Corollary 4: If u and v are nonzero integers and r is an integer, then

$$P_{\nu}^{n}P_{un+r} = \sum_{k=0}^{n} \binom{n}{k} (-1)^{u(n-k)} P_{\nu-u}^{n-k} P_{u}^{k} P_{\nu k+r}.$$

Corollary 5: If u is a nonzero integer and r is an integer, then

$$P_{un+r} = \sum_{k=0}^{n} \binom{n}{k} P_{u-1}^{n-k} P_{u}^{k} P_{k+r}.$$

1996]

Corollary 6: If r is an integer, then

$$P_{2n+r} = \sum_{k=0}^{n} \binom{n}{k} 2^k P_{k+r}.$$

4. ON THE PELL-LUCAS NUMBERS

The numbers R_n are defined by

$$R_0 = 2, R_1 = 2, R_n = 2R_{n-1} + R_{n-2}, n = 2, 3, ...,$$

 $R_{-n} = (-1)^n R_n, n = 1, 2,$

These numbers are associated with the Pell numbers in a way similar to that in which the Lucas numbers are associated with the Fibonacci numbers, see, e.g., [1]. Therefore, we refer to the numbers R_n as the Pell-Lucas numbers. The Pell-Lucas numbers have the Binet form $R_n = a^n + b^n$, where a and b are as in Section 3. Thus,

$$\hat{R}(x) = e^{ax} + e^{bx}$$

The Pell-Lucas numbers possess the properties of the Lucas numbers given in Theorems 1 and 2. We state these properties in Theorems 4 and 5. The proofs of Theorems 4 and 5 are similar to those of Theorems 1 and 2, and are omitted for brevity.

Theorem 4: Let u and v be nonzero integers, and let r be nonzero integer. Then

$$R_{un+r} = \sum_{k=0}^{n} \binom{n}{k} t^{n-k} s^{k} R_{vk+r}, \quad n = 0, 1, 2, ...,$$
(16)

if and only if

$$s = P_u / P_v, \quad t = (-1)^u P_{v-u} / P_v. \tag{17}$$

Remark: Note that (17) is equivalent to (13).

Theorem 5: Let u and v be nonzero integers (and r = 0). Then

$$R_{un} = \sum_{k=0}^{n} \binom{n}{k} t^{n-k} s^k R_{vk}, \quad n = 0, 1, 2, ...,$$
(18)

if and only if either (17) holds or

 $s = -P_{\mu} / P_{\nu}, \quad t = P_{\mu+\nu} / P_{\nu}.$ (19)

5. REMARK

It may be worth recalling that the egf method is, of course, also a very efficient tool in deriving other binomial identities. We mention here two such identities, namely,

$$\sum_{k=0}^{n} \binom{n}{k} F_{uk+r} L_{u(n-k)+r} = 2^{n} F_{un+2r}, \qquad (20)$$

and

330

AUG.

$$\sum_{k=0}^{n} \binom{n}{k} P_{uk+r} R_{u(n-k)+r} = 2^{n} P_{un+2r}.$$
(21)

The left side of (20) can be written in terms of egfs as

$$\frac{1}{\sqrt{5}}(\alpha^r e^{\alpha^u x} - \beta^r e^{\beta^u x})(\alpha^r e^{\alpha^u x} + \beta^r e^{\beta^u x})$$

and the right side as

$$\frac{1}{\sqrt{5}}(\alpha^{2r}e^{\alpha^{u}2x}-\beta^{2r}e^{\beta^{u}2x}).$$

It is clear that these two egfs are equal; hence, (20) holds. The proof of (21) is similar.

For further examples, reference is made to [3], [5], and [6].

REFERENCES

- 1. M. Bicknell. "A Primer on the Pell Sequence and Related Sequences." *The Fibonacci Quarterly* **13.4** (1975):345-49.
- L. Carlitz. "Some Classes of Fibonacci Sums." The Fibonacci Quarterly 16.5 (1978):411-26.
- C. A. Church & M. Bicknell. "Exponential Generating Functions for Fibonacci Identities." *The Fibonacci Quarterly* 11.3 (1973):275-81.
- 4. R. L. Graham, D. E. Knuth, & O. Patashnik. Concrete Mathematics: A Foundation for Computer Science. Reading, Mass.: Addison-Wesley, 1989.
- 5. R. T. Hansen. "General Identities for Linear Fibonacci and Lucas Summations." The Fibonacci Quarterly 16.2 (1978):121-28.
- R. T. Hansen. "Exponential Generation of Basic Linear Identities." In A Collection of Manuscripts Related to the Fibonacci Sequence: 18th Anniversary Volume, pp. 61-65. Ed. V. E. Hoggatt, Jr., & Marjorie Bicknell-Johnson. Santa Clara, Calif.: The Fibonacci Association, 1980.
- 7. H. Prodinger. "Some Information about the Binomial Transform." *The Fibonacci Quarterly* **32.5** (1994):412-15.

AMS Classification Numbers: 11B39, 11B65

SOME INTERESTING SUBSEQUENCES OF THE FIBONACCI AND LUCAS PSEUDOPRIMES

Paul S. Bruckman

13 Webster Ave., Highwood, IL 60040 (Submitted December 1994)

1. INTRODUCTION

In this paper, certain interesting sequences of positive integers are investigated. As will be demonstrated, these are subsequences of the Fibonacci and Lucas pseudoprimes, as they have been defined in the author's previous papers ([2], [3], [4], [9]). Indeed, it will be shown that the elements of two of these subsequences are strong Lucas pseudoprimes and Euler-Lucas pseudoprimes.

The secondary aim of this paper is to partially unify some of the more significant results previously obtained by other authors regarding such pseudoprimes.

Throughout this paper, lower-case letters represent integers, usually positive (unless otherwise indicated); the letters p, q, q_1 , and r represent primes.

In Section 2, the definitions and properties required to prove our main results are given. These are readily accessible in the standard literature and are presented with minimal commentary.

A brief historical summary of some of the more relevant findings of previous researchers is presented in Section 3.

Section 4 sets forth the main results, including proofs, and Section 5 consists of concluding remarks.

2. DEFINITIONS AND PROPERTIES

The Jacobi symbol is defined in any elementary number theory text, where it is customarily expressed as a product of Legendre symbols in its definition. As a consequence of such definition, the Jacobi symbol assumes certain values (either +1 or -1) dependent on the residue class of its arguments. We take a slightly different approach and simply define the Jacobi symbol in terms of this residue class. The arguments are restricted to the values that are relevant to the topic of this paper.

Definition 2.1 The Jacobi symbol $\left(\frac{u}{n}\right)$ is defined as follows for u = -1, -3, or 5, and for the indicated values of n:

(a) $\left(\frac{-1}{n}\right) = (-1)^{\frac{1}{2}(n-1)} = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4}, \\ -1 & \text{if } n \equiv -1 \pmod{4}; \end{cases}$ (b) $\left(\frac{-3}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{6}, \\ -1 & \text{if } n \equiv -1 \pmod{6}; \end{cases}$

(c)
$$\left(\frac{5}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{10}, \\ -1 & \text{if } n \equiv \pm 3 \pmod{10}. \end{cases}$$

AUG.

For brevity, we also write ε_n for $(\frac{5}{n})$. Note that if n = p, an odd prime, the Jacobi symbol coincides with the Legendre symbol. The symbol $(\frac{u}{n})$ is undefined for values of *n* not indicated above.

Definition 2.2: Given any integer u, the Fibonacci entry-point of u, denoted by Z(u), is the smallest positive integer z such that $u|F_z$. If Z(p) = m, we say that p is a primitive prime divisor (p.p.d.) of F_m .

Note: A classical result of Carmichael states that F_u has a p.p.d. for all $u \neq 1, 2, 6$, or 12.

Definition 2.3:

(a) Given any integer u, the Fibonacci period (mod u), denoted by k(u), is the smallest positive integer k such that $F_{n+k} \equiv F_n \pmod{u}$ for all integers n.

(b) The Lucas period (mod u), denoted by $\overline{k}(u)$, is the smallest positive integer \overline{k} such that $L_{n+\overline{k}} \equiv L_n \pmod{u}$ for all integers n.

Definition 2.4: The strong Lucas pseudoprimes (denoted SLPP's) are those composite u with gcd(u, 10) = 1, $u - \varepsilon_u = d \cdot 2^s$, $s \ge 1$, d being odd, such that either:

- (a) $u|F_d$, or
- (b) $u | L_{d,2^t}$ for some t with $0 \le t < s$.

Let U denote the set of SLPP's.

Definition 2.5: The Euler-Lucas pseudoprimes (denoted ELPP's) are those composite u with gcd(u, 10) = 1 such that either

- (a) $u|F_{\frac{1}{2}(u-\varepsilon_u)}$ when $\left(\frac{-1}{u}\right) = 1$, or
- **(b)** $u|L_{\frac{1}{2}(u-\varepsilon_u)}$ when $(\frac{-1}{u}) = -1$.

Let *V* denote the set of ELPP's.

Definition 2.6: The Fibonacci pseudoprimes (denoted FPP's) are those composite u with gcd(u, 10) = 1 such that $u|F_{u-\varepsilon_u}$. Let X denote the set of FPP's.

Definition 2.7: The Lucas pseudoprimes (denoted LPP's) are those composite u such that $L_u \equiv 1 \pmod{u}$. Let Y denote the set of LPP's.

Definition 2.8: The Fibonacci-Lucas pseudoprimes (denoted FLPP's) are those u that are both FPP's and LPP's. Let $W = X \cap Y$ denote the set of FLPP's.

Comment: As we will later indicate, the sets V and W are identical. For the time being, however, we will maintain the distinction between these two sets.

In addition to the pseudoprimes defined above, there are other related pseudoprimes that have been studied by previous authors. Since these are only of peripheral interest to the topic of this paper, we merely mention these in passing. For example, Rotkiewicz [16], [17] and Baillie &

1996]

Wagstaff [1] discuss sequences of psuedoprimes u that (for the Fibonacci and Lucas sequences in particular) satisfy either of the following relations, given that gcd(u, 10) = 1:

$$F_u \equiv \varepsilon_u \pmod{u}; \tag{2.1}$$

$$L_{u-\varepsilon_u} \equiv 2\varepsilon_u \pmod{u}. \tag{2.2}$$

It may be shown that if u satisfies any *two* of the relations given in Definitions 2.6, 2.7, or in (2.1) and (2.2), the other two relations are implied.

We next introduce the special sequences that are of interest to the topic of this paper.

Definition 2.9: Define the following ratios for any arbitrary prime p (except as indicated), and for e = 0, 1, 2, ...

(a)
$$A_e(p) = F_{p^{e+1}} / F_{p^e}, \ p \neq 5; \ A_e(5) = F_{5^{e+1}} / 5F_{5^e};$$

(b)
$$B_e(p) = L_{p^{e+1}} / L_{p^e}, \ p \neq 2;$$

(c)
$$C_e(p) = F_{2 \cdot p^{e+1}} / F_{2 \cdot p^e}, \ p \neq 2, 5; \ C_e(5) = F_{2 \cdot 5^{e+1}} / 5F_{2 \cdot 5^e}$$

Note that $C_e(p) = A_e(p) \cdot B_e(p)$ for all odd p. Where no confusion is likely to arise, we omit the argument p and/or the subscript e. Clearly, A, B, and C are positive integers in all cases.

Next, we indicate some relevant properties.

Properties 2.1:

- (a) Z(u)|v iff $u|F_{v}$;
- **(b)** $Z(p)|(p-\varepsilon_p);$

(c)
$$Z(u) = \underset{p^e \parallel u}{\text{LCM}} \{Z(p^e)\};$$

- (d) $Z(p^e) = p^f Z(p)$ for some f with $0 \le f < e$;
- (e) for all odd p, Z(p) is even iff $p|L_u$ for some u.

Properties 2.2:

(d)

(a)
$$k(u) = \begin{cases} k(u) & \text{if } 5 \nmid u, \\ 5 \overline{k}(u) & \text{if } 5 \mid u; \end{cases}$$

(b)
$$k(u) = \operatorname{LCM}_{p^e \parallel u} \{k(p^e)\};$$

(c) $\bar{k}(p^e) = p^f \bar{k}(p)$ for some f with $0 \le f < e$ (for odd primes p, f is the same as in Property 2.1(d);

if
$$p \neq 2, 5$$
, $\overline{k}(p) = \begin{cases} Z(p) & \text{if } Z(p) \equiv 2 \pmod{4}, \\ 2Z(p) & \text{if } 4 | Z(p), \\ 4Z(p) & \text{if } Z(p) \text{ is odd.} \end{cases}$

Note: Properties 2.2(b)-(d) for the Lucas period also apply to the Fibonacci period k(u); however, scant use of this fact will be made here.

AUG.

Properties 2.3: We assume $p \neq 2, 5$ and write $p' = \frac{1}{2}(p-1)$, $m = p^e$, $\varepsilon = \varepsilon_p$. In (e) and (f) below, we assume gcd(n, 10) = 1 and write $t = \frac{1}{2}(n - \varepsilon_n)$.

(a) $A = (-1)^{p'} \left(1 + \sum_{j=1}^{p'} (-1)^j L_{2mj} \right);$

(b)
$$B = 1 + \sum_{j=1}^{p} L_{2mj};$$

- (c) $C = 1 + \sum_{j=1}^{p'} L_{4mj};$
- (d) $L_{2mp+\varepsilon} = -\varepsilon + 5F_{mp+\varepsilon}F_{mp} = \varepsilon + L_{mp+\varepsilon}L_{mp};$
- (e) $L_t^2 5L_tF_{t+\varepsilon_n} + 5F_{t+\varepsilon_n}^2 = (-1)^t + \varepsilon_n$;
- (f) $L_{t+\varepsilon_n}^2 5L_{t+\varepsilon_n}F_t + 5F_t^2 = (-1)^t$.

The derivations of Properties 2.3 involve elementary identities and are omitted. We will return to these definitions and properties in Section 4. First, however, we give a brief overview of some of the more significant results.

3. HISTORICAL SUMMARY

The use of the term "pseudoprime" in the preceding section stems from the fact that the defining relations are satisfied when u = p (with $p \neq 2, 5$ in all but Definition 2.7). The author's papers [2], [3], [4] may be referred to for comments regarding the merit of adopting the nomenclature employed in Definitions 2.6-2.8, since other nomenclature is used by other authors. Some of the prior findings of other authors have been mentioned in the author's papers (op.cit.); for the sake of continuity, we reiterate these findings below.

In a 1955 paper by Duparc [12], apparently the first proof that X, Y, and W are infinite sets is given. In particular, Duparc showed that $F_{2p} \in X$ for all p > 5. This result was independently rediscovered by E. Lehmer in a 1964 paper [14]. Using a different method, Parberry [15] showed that X is infinite; specifically, Parberry showed that if gcd(n, 30) = 1 and $n \in X$, then $F_n \in X$ [from which it follows necessarily that $gcd(F_n, 30) = 1$]. In a 1986 paper [13], Kiss, Phong, and Lieuwens showed that W is infinite; of course, this implies that X and Y are infinite. In a recent paper [2], the author proved that the "LPP" counterpart of Parberry's result holds, namely that if $n \in Y$ and gcd(n, 6) = 1, then $L_n \in Y$ [from which it follows necessarily that $gcd(L_n, 6) = 1$]. This is an independent proof that Y is infinite.

It is also known that all LPP's are odd. Apparently the first proof of this result was given by White, Hunt, and Dresel in 1977 paper [18]. Other independent proofs of this result were subsequently given by Di Porto [10] and by the author [3].

Many other interesting properties (or apparent properties) may be given, but we will restrict our discussion to those properties that are more or less relevant to the topic of this paper and, in particular, to the ratios introduced in Definition 2.9. Di Porto and Filipponi observed, and later proved in a 1988 paper [11], that if L_{2^e} is composite, it is a LPP. In a recently submitted problem for this journal [6], the author proves a generalization of such a result; this is indicated below in (3.1).

Other observations made recently by the author have been submitted to this journal as proposed problems (viz. [7], [8]) and are indicated below:

If
$$A_e(2)$$
 is composite, then $A_e(2) \in W$; (3.1)

If
$$e \ge 1$$
 and $A_e(3)[B_e(3)]$ is composite, then $A_e(3)[(B_e(3)] \in W;$ (3.2)

$$C_e(3) \in (X - Y); \tag{3.3}$$

If
$$A_e(5)[B_e(5)]$$
 is composite, then $A_e(5)[B_e(5)] \in W$; (3.4)

$$C_e(5) \in (X - Y).$$
 (3.5)

In fact, even stronger results are true, although we will not prove these here; namely, $A_e(p) \in U$, if p = 2, 3, 5, and $B_e(p) \in U$, if p = 3, 5.

The results indicated in (3.1)-(3.5) were obtained initially, suggesting the generalizations that are indicated in Section 4 (for p > 5).

Note that there is no definition of $B_e(2)$ in Definition 2.9(b), since $L_{2^e} \nmid L_{2^{e+1}}$. Also, there is no definition of $C_e(2)$, since this would be essentially the same as for $A_e(2)$ (by virtue of the identity $F_{2n} = F_n L_n$).

The result of (3.2) excludes the case e = 0, since $L_3 = 4$ is composite but is neither a FPP nor a LPP. Also, note the extra factor of 5 in the denominator of the definitions of $A_e(5)$ and $C_e(5)$; this is a consequence of the special role played by the number 5 in the Fibonacci and Lucas sequences.

Therefore, for one reason or another, the primes 2, 3, and 5 require special treatment. This is not the case for p > 5; in the remainder of this paper we will assume p > 5.

It is worthwhile to reiterate the notation introduced in the prologue to Properties 2.3, since we will use this frequently:

$$\varepsilon = \varepsilon_p, \ m = p^e, \ e = 0, 1, \dots$$
(3.6)

We will also write mp for p^{e+1} , for brevity. Note also that gcd(A, B) = 1, AB = C, and that A, B, and C are all relatively prime to 30.

4. MAIN RESULTS

We will make frequent use of the definitions and properties introduced in Section 2, often without specific reference thereto. Our main results are Theorems 4.1 and 4.2 (with their corollaries).

Theorem 4.1:

(a) If A is composite, then $A \in U$;

(b) If B is composite, then $B \in U$.

Corollary 4.1:

- (a) If A is composite, then $A \in W$;
- (b) If B is composite, then $B \in W$.

Corollary 4.2:

- (a) If F_p is composite, then $F_p \in W$;
- (b) If L_p is composite, then $L_p \in W$.

Our proof of the theorems requires several preliminary results, indicated in this section as lemmas.

Lemma 4.1: Z(A) = mp; Z(B) = Z(C) = 2mp.

Proof: From Definition 2.9 and from Carmichael's result (see Note after Definition 2.2), it follows that Z(q) = mp for some q with $q|F_{mp}$. Also, $q \nmid F_m$, since $Z(q) \nmid m$. Then $q \mid A$. Indeed, Z(r) = mp for all prime r with $r \mid F_{mp}, r \nmid F_m$. Then Z(A) = mp.

Using Property 2.1(e), we argue similarly that Z(B) = 2mp. Then, since C = AB, Z(C) = LCM(mp, 2mp) = 2mp.

Lemma 4.2: $A \equiv \varepsilon_p, B \equiv 1, C \equiv \varepsilon_p \pmod{mp}$.

Proof: This follows directly from Theorem 1 of a recent paper by Young [19], along with the observation that C = AB.

Lemma 4.3: $A \equiv \varepsilon_A, B \equiv \varepsilon_B, C \equiv \varepsilon_C \pmod{mp}$.

Proof: Since Z(q) = mp for all q | A, we have $mp | (q - \varepsilon_q)$ or $q \equiv \varepsilon_q \pmod{mp}$. If $A = \prod q^f$, then $A \equiv \prod (\varepsilon_q)^f \equiv \prod \varepsilon_{q^f} \equiv \varepsilon_A \pmod{mp}$. Likewise, $B = \varepsilon_B \pmod{mp}$. Also, $C = AB \equiv \varepsilon_A \varepsilon_B \equiv \varepsilon_C \pmod{mp}$.

Combining the results of Lemmas 4.2 and 4.3, we obtain

Lemma 4.4: $\varepsilon_A = \varepsilon_C = \varepsilon_p$; $\varepsilon_B = 1$.

Henceforth, we use the symbol ε interchangeably to denote ε_A , ε_C , or ε_p ; however, $\varepsilon_B = 1$ in all cases.

Lemma 4.5: $\bar{k}(A) = \bar{k}(C) = 4mp; \ \bar{k}(B) = 2mp$.

Proof: Let q be the same as in the proof of Lemma 4.1. Then, since Z(q) = mp is odd, it follows from Property 2.2(d) that $\overline{k}(q) = 4mp$ for all q|A; thus, $\overline{k}(A) = 4mp$. But, $\overline{k}(q_1) = 2mp = Z(q_1)$ for all $q_1|B$, since $2mp \equiv 2 \pmod{4}$. Then $\overline{k}(B) = 2mp$ and $\overline{k}(C) = \text{LCM}(4mp, 2mp) = 4mp$.

Proof of Theorem 4.1: Since gcd(A, 10) = 1, Lemma 4.3 implies that $A - \varepsilon = 2^s \cdot d$ for some $s \ge 1$ and odd d, such that Z(A) = mp|d. Then $A|F_d$, which shows that $A \in U$ if A is composite [using Definition 2.4(a)].

Similarly, $B-1=2^{s_1} \cdot d_1$ for some $s_1 \ge 1$, odd d_1 , such that $Z(B) = 2mp|2d_1$. Since $mp|d_1$ and d_1 is odd, we have $L_{mp}|L_{d_1}$. Also, $B|L_{mp}$, and so $B|L_{d_1}$. By Definition 2.4(b), $B \in U$, provided B is composite. The proof is complete.

1996]

To prove Corollary 4.1, we invoke Theorem 3 of a 1980 paper by Baillie and Wagstaff [1], which implies that all SLPP's are ELPP's, i.e., that $U \subseteq V$. Also, certain results due to Rotkiewicz (see [16], [17]) imply that all ELPP's are FLPP's, i.e., that $V \subseteq W$. Then $U \subseteq W$, which together with Theorem 4.1 implies Corollary 4.1. Corollary 4.2 is a special case of this (with e = 0); this result was obtained by the author in a recent paper [4].

As mentioned after Definition 2.8, the author shows (in a problem [5] submitted to this journal) that the sets V and W are actually identical. In light of this, no further explicit mention of the set of ELPP's (V) will be made.

The corresponding theorem dealing with the ratio C is somewhat more involved. As was the case for A and B, we require some preliminary results. We introduce the following notation:

$$\theta = \begin{cases} 1 & \text{if } e \text{ is even,} \\ 0 & \text{if } e \text{ is odd.} \end{cases}$$
(4.1)

Lemma 4.6: $m \equiv p^{\theta} \pmod{12}$.

Proof: Since $p \equiv \pm 1 \pmod{6}$, then $m \equiv 1$ if e is even, $m \equiv p$ if e is odd (mod 12).

Note that $\overline{k}(20) = \text{LCM}(\overline{k}(4), \overline{k}(5)) = \text{LCM}(6, 4) = 12$ and $k(20) = 5 \cdot 12 = 60$. To characterize *B* (mod 20), it suffices to consider all residues *p* (mod 12), since *B* involves Lucas numbers. However, to characterize *A* and *C* (mod 20), we must consider all residues *p* (mod 60), since *A* and *C* involve Fibonacci numbers. From Lemma 4.6, it follows that $L_{2mj} \equiv L_{2jp}\theta$ (mod 20), for all *j*. Then Properties 2.3(a)-(c) imply the following

Lemma 4.7: $A_e \equiv A_{\theta}, B_e \equiv B_{\theta}, C_e \equiv C_{\theta} \pmod{20}$

Using any standard table of F_u and L_u for $1 \le u \le 60$, along with quadratic reciprocity, we next form Table 1 below.

TA	BL	Æ	1	
LA	DL	JL.	1	

p (mod 60)	$\left(\frac{5}{p}\right)$	$\left(\frac{-3}{p}\right)$	<i>p</i> ² (mod 60)	$F_{p^2} \pmod{20}$	$L_{p^2} \pmod{20}$	$A_0 \equiv A_1 \\ \equiv F_p \pmod{20}$	$B_0 \equiv B_1 \\ \equiv L_p \pmod{20}$	$C_0 \equiv C_1 \\ \equiv F_{2p} \pmod{20}$
1	1	1	1	1	1	1	1	1
7	-1	1	-11	9	1	-7	9	-3
11	1	-1	1	1	1	9	-1	-9
13	-1	1	-11	9	1	-7	1	-7
17	-1	-1	-11	9	1	-3	-9	7
19	1	1	1	1	1	1	9	9
23	-1	-1	-11	9	1	-3	-1	3
29	1	-1	1	1	1	9	-9	-1
-29	1	1	1	1	1	9	9	1
-23	-1	1	-11	9	1	-3	1	-3
-19	1	-1	1	1	1	1	-9	-9
-17	-1	1	-11	9	1	-3	9	-7
-13	-1	-1	-11	9	1	-7	-1	7
-11	1	1	1	1	1	9	1	9
-7	-1	-1	-11	9	1	-7	-9	3
-1	1	-1	1	1	1	1	-1	-1

As we may readily verify, using Table 1, $A_0 \equiv A_1 \equiv F_p$, $B_0 \equiv B_1 \equiv L_p$, $C_0 \equiv C_1 \equiv F_{2p} \pmod{20}$. Then $(F_p)^2 \equiv F_{p^2}$, $(L_p)^2 \equiv L_{p^2}$, and $(F_{2p})^2 \equiv F_{2p^2} \pmod{20}$, from which we obtain

[AUG.

Lemma 4.8: $A_e \equiv A_0, B_e \equiv B_0, C_e \equiv C_0 \pmod{20}$.

From Lemma 4.8, and by inspection of the entries in Table 1, we obtain the following lemma.

Lemma 4.9: $C \equiv \left(\frac{-3}{p}\right) \pmod{4}$.

We are now ready to state the main theorem regarding C.

Theorem 4.2: $C \in (X - Y)$, unless $p \equiv 1$ or 19 (mod 30), in which case $C \in W$.

Proof: We may suppose that A and B are composite. The following proof needs some modification if either A or B is prime. Since $A \in X$ and $B \in X$, we see that $Z(A) = mp|(A - \varepsilon)$, Z(B) = 2mp|(B-1). Since $C - \varepsilon = AB - \varepsilon = (A - \varepsilon)(B - 1) + (A - \varepsilon) + \varepsilon(B - 1)$, then $mp|(C - \varepsilon)$. Since mp is odd and $C - \varepsilon$ is even, we have $Z(C) = 2mp|(C - \varepsilon)$. C = AB is necessarily composite, so $C \in X$.

From Lemmas 4.3, 4.4, and 4.9, we see that

$$C \equiv \begin{cases} \varepsilon \pmod{4mp} & \text{if } \varepsilon = \left(\frac{-3}{p}\right), \\ \varepsilon + 2mp \pmod{4mp} & \text{if } \varepsilon = -\left(\frac{-3}{p}\right). \end{cases}$$
(*)

Then, from Lemma 4.5, we obtain

$$L_{C} \equiv \begin{cases} L_{\varepsilon} \equiv \varepsilon \pmod{C}, & \text{if } \varepsilon = \left(\frac{-3}{p}\right), \\ L_{2mp+\varepsilon} \pmod{C}, & \text{if } \varepsilon = -\left(\frac{-3}{p}\right). \end{cases}$$
(**)

Now $A|F_{mp}$ and $B|L_{mp}$, clearly. Property 2.3(d) implies that $L_{2mp+\varepsilon} \equiv -\varepsilon \pmod{A}$, while $L_{2mp+\varepsilon} \equiv \varepsilon \pmod{B}$. Since C = AB, we see that $L_{2mp+\varepsilon} \neq 1 \pmod{C}$. Then (**) implies that $L_C \equiv 1 \pmod{C}$ iff $\varepsilon = (-3/p) = 1$. By reference to Table 1, this occurs precisely when $p \equiv 1, 19, -29$, or $-11 \pmod{60}$, i.e., when $p \equiv 1$ or 19 (mod 30). Thus, $C \in Y$ iff $p \equiv 1$ or 19 (mod 30), which completes the proof.

For the special case in which e = 0, we obtain the following corollary.

Corollary 4.3: $F_{2p} \in (X - Y)$, unless $p \equiv 1$ or 19 (mod 30), in which case $F_{2p} \in W$.

This result extends that of Duparc [12] (and of Lehmer [14]) mentioned in Section 3.

Theorem 4.2 cannot be improved, in the sense that $C \notin U$ when $p \equiv 1$ or 19 (mod 30). To see this, first suppose $p \equiv 1$ or 19 (mod 30), so that $\varepsilon = 1$. Since $C \in X$, by Theorem 4.2, we see that Z(C) = 2mp|(C-1). Letting $C-1=2^sd$, where $s \ge 1$ and d is odd, then 2mp|2d. Thus, $C|F_{2mp}|F_{2d}$. In order for $C \in U$, it is necessary that either $C|F_d$ or $C|L_d$. However, $A|F_d$ and $B|L_d$. Since gcd(A, B) = 1, it is impossible for either $C|F_d$ or $C|L_d$. Therefore, $C \notin U$, as claimed.

5. CONCLUSION

No attempt has been made to generalize the results of this paper so as to apply to more general second-order sequences. The author is content to confine his investigation to the Fibonacci and Lucas sequences and to leave such generalizations to others. It is apparent, however, that any such generalizations are easily suggested by the results of this paper.

Many other areas of research are suggested for the various pseudoprimes discussed in Section 2, in some cases leading to fascinating, difficult, and as yet unanswered questions. In recent years, due to the application of LPP's to the area of primality testing and public key crytography, there has been a tendency to shift the focus of investigation on LPP's. As this brief overview has attempted to indicate, however, there are areas of theoretical interest encompassing *all* of the pseudoprimes defined here.

ACKNOWLEDGMENT

The author gratefully acknowledges the helpful suggestions of the anonymous referee, who provided some references that were previously unknown to the author, strengthened the results so as to involve SLPP's and ELPP's, and provided proofs of some of these results.

REFERENCES

- 1. R. Baillie & S. Wagstaff, Jr. "Lucas Pseudoprimes." Math. of Comp. 35.152 (1980):1391-1417.
- 2. P. S. Bruckman. "On the Infinitude of Lucas Pseudoprimes." *The Fibonacci Quarterly* **32.2** (1994):153-54.
- 3. P. S. Bruckman. "Lucas Pseudoprimes are Odd." *The Fibonacci Quarterly* **32.2** (1994): 155-57.
- 4. P. S. Bruckman. "On a Conjecture of Di Porto and Filipponi." *The Fibonacci Quarterly* **32.2** (1994):158-59.
- 5. P. S. Bruckman. Problem H-496. The Fibonacci Quarterly 33.2 (1995):187.
- 6. P. S. Bruckman. Problem H-498. The Fibonacci Quarterly 33.2 (1995):187.
- 7. P. S. Bruckman. Problem H-499. The Fibonacci Quarterly.33.4 (1995):378.
- 8. P. S. Bruckman. Problem H-501. The Fibonacci Quarterly.33.4 (1995):379.
- 9. P. S. Bruckman. "A Characterization of Quadratfrei Lucas Pseudoprimes." *Pi Mu Epsilon Journal* **10.3** (1994-1999):207-11.
- 10. A. Di Porto. "Nonexistence of Even Fibonacci Pseudoprimes of the 1st Kind." *The Fibonacci Quarterly* **31.2** (1993):173-77.
- A. Di Porto & P. Filipponi. "A Probabilistic Primality Test Based on the Properties of Certain Generalized Lucas Numbers." In *Lecture Notes in Computer Science* 330:211-13. Ed. C. G. Günther. Berlin: Springer-Verlag, 1988.
- H. J. A. Duparc. "On Almost Primes of the Second Order." Rapport ZW, 1955-013, pp. 1-13. Math. Center, Amsterdam, 1955.
- P. Kiss, B. M. Phong, & E. Lieuwens. "On Lucas Pseudoprimes Which Are Products of s Primes." In *Fibonacci Numbers and Their Applications* 1:131-39. Ed. A. N. Philippou, G. E. Bergum, & A. F. Horadam. Dordrecht: Reidel, 1986.
- 14. E. Lehmer. "On the Infinitude of Fibonacci Pseudoprimes." *The Fibonacci Quarterly* **2.3** (1964):229-30.

- 15. E. A. Parberry. "On Primes and Pseudo-Primes Related to the Fibonacci Sequence." *The Fibonacci Quarterly* **8.1** (1970):49-60.
- 16. A. Rotkiewicz. "On the Pseudoprimes with Respect to the Lucas Sequences." Bull. Acad. Polon. Sci. Ser. Math. Astr. Phys. 21.9 (1973):793-97.
- 17. A. Rotkiewicz. "Problems on Fibonacci Numbers and Their Generalizations." In *Fibonacci Numbers and Their Applications* 1:241-55. Ed. A. N. Philippou, G. E. Bergum, & A. F. Horadam. Dordrecht: Reidel, 1986.
- 18. D. J. White, J. N. Hunt, & L. A. G. Dresel. "Uniform Huffman Sequences Do Not Exist." Bull. London Math. Soc. 9 (1977):193-98.
- 19. P. T. Young. "p-Adic Congruences for Generalized Fibonacci Sequences." The Fibonacci Quarterly 32.1 (1994):2-10.

AMS Classification Numbers: 11A07, 11B39, 11B50

*** *** ***

APPLICATIONS OF FIBONACCI NUMBERS

VOLUME 6

New Publication

Proceedings of The Sixth International Research Conference on Fibonacci Numbers and Their Applications, Washington State University, Pullman, Washington, USA, July 18-22, 1994

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

This volume contains a selection of papers presented at the Sixth International Research Conference on Fibonacci Numbers and Their Applications. The topics covered include number patterns, linear recurriences, 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:

1996, 560 pp. ISBN 0-7923-3956-8 Hardbound Dfl. 345.00 / £155.00 / US\$240.00

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 DordrechtP.O. Box 358, Accord StationThe NetherlandsHingham, MA 02018-0358, U.S.A.

Volumes 1-5 can also be purchased by writing to the same addresses.

POLYNOMIALS ASSOCIATED WITH GENERALIZED MORGAN-VOYCE POLYNOMIALS

A. F. Horadam

The University of New England, Armidale, Australia 2351 (Submitted December 1994)

1. PROLOGUE

André-Jeannin [1] recently defined a polynomial sequence $\{P_n^{(r)}(x)\}$, where r is a real number, by the recurrence

$$P_n^{(r)}(x) = (x+2)P_{n-1}^{(r)}(x) - P_{n-2}^{(r)}(x) \quad (n \ge 2)$$
(1.1)

with

$$P_0^{(r)}(x) = 1, \quad P_1^{(r)}(x) = x + r + 1.$$
 (1.2)

Furthermore [1], a sequence of integers $\{a_{n,k}^{(r)}\}$ exists for which

$$P_n^{(r)}(x) = \sum_{k=0}^n a_{n,k}^{(r)} x^k, \qquad (1.3)$$

where

$$a_{n,n}^{(r)} = 1 \quad (n \ge 0).$$
 (1.4)

He also proved [1] the crucial formula $(n \ge 0, k \ge 0)$

$$a_{n,k}^{(r)} = \binom{n+k}{2k} + r\binom{n+k}{2k+1}$$
(1.5)

and the recurrence

$$a_{n,k}^{(r)} = 2a_{n-1,k}^{(r)} - a_{n-2,k}^{(r)} + a_{n-1,k-1}^{(r)} \quad (n \ge 2, k \ge 1).$$
(1.6)

Simple instances of $P_n^{(r)}(x)$ are [1], with slightly varied notation,

$$P_{n-1}^{(0)}(x) = b_n(x) \quad (n \ge 1)$$
(1.7)

and

$$P_{n-1}^{(1)}(x) = B_n(x) \quad (n \ge 1), \tag{1.8}$$

where $b_n(x)$ and $B_n(x)$ are the well-known Morgan-Voyce polynomials [4]. (Please see [1] for other references to $b_n(x)$ and $B_n(x)$.)

It is the purpose of this short paper to give a brief account of a closely related sequence of polynomials $\{Q_n^{(r)}(x)\}$ with particular emphasis on the case r = 0. Necessarily, a formula corresponding to (1.5) will have to be discovered.

For ready comparison and contrast with the contents of [1], it seems desirable to present this material in a partially similar way. Before proceeding, however, we need to add the following items of information.

AUG.

Lemma 1: $a_{n,k}^{(1)} - a_{n-2,k}^{(1)} = a_{n,k}^{(0)} + a_{n-1,k}^{(0)}$ $(n \ge 2)$. Proof: $\binom{n+k}{2k} + \binom{n+k}{2k+1} = \binom{n+k+1}{2k+1}$ by Pascal's Theorem, i.e., $\binom{n+k}{2k} + \binom{n+k-1}{2k} + \binom{n+k-1}{2k+1} = \binom{n+k+1}{2k+1}$ by Pascal's Theorem, i.e., $\binom{n+k}{2k} + \binom{n+k-1}{2k} = \binom{n+k+1}{2k+1} - \binom{n+k-1}{2k+1}$.

Use (1.5) for r = 0, r = 1, and the Lemma follows by Pascal's Theorem.

When r = 2 in (1.1), then $P_{n-1}^{(2)}(x)$ is found to be

$$P_{n-1}^{(2)}(x) = c_n(x) = \frac{b_{n+1}(x) - b_{n-1}(x)}{x} \quad (n \ge 1),$$
(1.9)

where $c_n(x)$ —given in terms of Morgan-Voyce polynomials—has been introduced independently by me is a paper currently being written in which it is also demonstrated that

$$c_{n+1}(x) - c_n(x) = C_n(x), \qquad (1.10)$$

in which $C_n(x)$ is to be defined in (2.11).

2. THE POLYNOMIALS $\{Q_n^{(r)}(x)\}$

Define, as in (1.1), a polynomial sequence $\{Q_n^{(r)}(x)\}$ recursively by

$$Q_n^{(r)}(x) = (x+2)Q_{n-1}^{(r)}(x) - Q_{n-2}^{(r)}(x) \quad (n \ge 2)$$
(2.1)

with

$$Q_0^{(r)}(x) = 2, \quad Q_1^{(r)}(x) = x + r + 2.$$
 (2.2)

Then a sequence of integers $\{b_{n,k}^{(r)}\}$ exists such that

$$Q_n^{(r)}(x) = \sum_{k=0}^n b_{n,k}^{(r)} x^k, \qquad (2.3)$$

where

$$b_{n,n}^{(r)} = \begin{cases} 1 & (n \ge 1), \\ 2 & (n = 0). \end{cases}$$
(2.4)

Now $b_{n,0}^{(r)} = Q_n^{(r)}(0)$. By (2.1) and (2.2),

$$b_{n,0}^{(r)} = 2b_{n-1,0}^{(r)} - b_{n-2,0}^{(r)} \quad (n \ge 2)$$
(2.5)

with

$$\begin{cases} b_{0,0}^{(r)} = 2, \\ b_{1,0}^{(r)} = 2 + r & \text{by } (2.2). \end{cases}$$
(2.6)

1996]

Following [1], we deduce that $(n \ge 0)$

$$b_{n,0}^{(r)} = 2 + nr, \qquad (2.7)$$

whence

$$b_{n,0}^{(0)} = 2 \tag{2.8}$$

and

$$b_{n,0}^{(1)} = 2 + n. \tag{2.9}$$

Comparison of coefficients of x^k in (1.1) leads to the recurrence $(n \ge 2, k \ge 1)$

$$b_{n,k}^{(r)} = 2b_{n-1,k}^{(r)} + b_{n-1,k-1}^{(r)} - b_{n-2,k}^{(r)}.$$
(2.10)

Table 1 displays a triangular arrangement of the coefficients $b_{n,k}^{(r)}$. This ought to be compared with the (preferably extended) table in [1] for the coefficients $a_{n,k}^{(r)}$.

TABLE 1. Coefficients $b_{n,k}^{(r)}$ of $Q_n^{(r)}(x)$

n^{k}	0	1	2	3	4	5	0 • 0
0	2						••••
1	2 <i>+r</i>	1					•••
2	2 + 2r	4 + r	1				•••
3	2 + 3r	9 + 4 <i>r</i>	6+r	1			•••
4	2+4 <i>r</i>	16+10 <i>r</i>	20 + 6r	8+ <i>r</i>	1		•••
5	2 + 5r	25 + 20r	50+21r	35+8r	10+ <i>r</i>	1	•••
•••	•••	•••	• • •	•••		•••	•••

Next, we introduce the important symbolism

$$Q_n^{(0)}(x) = C_n(x).$$
 (2.11)

Using Table 1, we may now write out the expressions for $C_0(x)$, $C_1(x)$, $C_2(x)$, $C_3(x)$,.... Some properties of $C_n(x)$, especially in relation to Lucas polynomials, appear in [2].

3. CONNECTION BETWEEN $\{P_n^{(r)}(x)\}$ AND $\{Q_n^{(r)}(x)\}$

Inherent in the nature of the laws of formation of $\{P_n^{(r)}(x)\}$ and $\{Q_n^{(r)}(x)\}$ —namely, (1.1), (1.2), (2.1), and (2.2)—is the inevitably close connection between $a_{n,k}^{(r)}$ and $b_{n,k}^{(r)}$.

Typically, for example,

$$\begin{cases} b_{5,2}^{(r)} = 50 + 21r &= (35 + 21r) + 15 = a_{5,2}^{(r)} + a_{4,2}^{(0)} \\ b_{6,3}^{(r)} = 112 + 36r &= (84 + 36r) + 28 = a_{6,3}^{(r)} + a_{5,3}^{(0)}. \end{cases}$$
(3.1)

These illustrations suggest the nature of the constant (for which r = 0) by which $b_{n,k}^{(r)}$ exceeds $a_{n,k}^{(r)}$. It is $a_{n-1,k}^{(0)}$.

AUG.

Theorem 1: $b_{n,k}^{(r)} = a_{n,k}^{(r)} + a_{n-1,k}^{(0)}$ $(n \ge 1)$

$$= \binom{n+k}{2k} + \binom{n-1+k}{2k} + r\binom{n+k}{2k+1}$$
 by (1.5)

Proof: Follow the inductive proof in [1] for $a_{n,k}^{(r)}$, using the binomial coefficients and (2.10). The occurrence of the middle (extra) binomial term causes no complication.

[Alternatively: Subtract (1.6) from (2.10) and use induction.]

Combine the first two binomial coefficients in Theorem 1 to derive

Corollary 1:
$$b_{n,k}^{(r)} = \frac{n}{k} \binom{n-1+k}{2k-1} + r\binom{n+k}{2k+1}.$$

Multiply both sides of Theorem 1 by x^k and sum. Immediately, from (1.3) and (2.3), we infer the fundamental polynomial property associating $Q_n^{(r)}(x)$ with $P_n^{(r)}(x)$.

Theorem 2:
$$Q_n^{(r)}(x) = P_n^{(r)}(x) + P_{n-1}^{(0)}(x) \quad (n \ge 1)$$

Fixing r = 0 in Theorem 2 and using (1.7) and (2.11), we deduce

$$C_n(x) = b_{n+1}(x) + b_n(x).$$
(3.2)

Evaluating in Theorem 2 when x = 1 produces a nice specialization. Already [1] we know that, for Fibonacci numbers,

$$P_n^{(r)}(1) = F_{2n+1} + rF_{2n}.$$
(3.3)

Application of (3.3) enables us to get the following two useful subsidiary results for Fibonacci and Lucas numbers from Theorem 2 when x = 1.

Corollary 2:
$$Q_n^{(r)}(1) = L_{2n} + rF_{2n}$$
.
Proof: $Q_n^{(r)}(1) = P_n^{(r)}(1) + P_{n-1}^{(0)}(1)$ by Theorem 2
 $= F_{2n+1} + rF_{2n} + F_{2n-1}$ by (3.3)
 $= L_{2n} + rF_{2n}$.

Corollary 3:
$$Q_n^{(2u+1)}(1) = 2P_n^{(u)}(1)$$
.
Proof: $Q_n^{(2u+1)}(1) = F_{2n+1} + (2u+1)F_{2n} + F_{2n-1}$ as in Corollary 2 ($r = 2u+1$, odd)
 $= 2(F_{2n+1} + uF_{2n})$
 $= 2P_n^{(u)}(1)$ by (3.3).

Thus,

$$Q_n^{(1)}(1) = 2P_n^{(0)}(1) = 2F_{2n+1} = 2b_{n+1},$$
(3.4)

$$Q_n^{(3)}(1) = 2P_{n}^{(1)}(1) = 2F_{2n+2} = 2B_{n+1},$$
(3.5)

$$Q_n^{(5)}(1) = 2P_n^{(2)}(1) = 2L_{2n+1} = 2c_{n+1}.$$
(3.6)

1996]

Conventional symbolism $b_n(1) = b_n$,... has been employed in (3.4)-(3.6). Even superscript values of r in Corollary 2 do not, in general, appear to produce neat or interesting simplifications. However, by Corollary 2, (2.11), and [2], we do know that

$$Q_n^{(0)}(1) = C_n = L_{2n}.$$
 (3.7)

Worth recording in passing is

$$Q_n^{(2)}(1) = F_{2n+3} = b_{n+2}.$$
(3.8)

4. CONNECTION BETWEEN $Q_n^{(0)}(x)$ AND $B_n(x)$

Lastly, the link between our polynomials and the Morgan-Voyce polynomial $B_n(x)$ is described.

Theorem 3: $Q_n^{(0)}(x) = B_{n+1}(x) - B_{n-1}(x)$.

Proof:
$$Q_n^{(0)}(x) = \sum_{k=0}^n b_{n,k}^{(0)} x^k$$
 by (2.3) $(r = 0)$ (i)
 $= \sum_{k=0}^n (a_{n,k}^{(0)} + a_{n-1,k}^{(0)})$ by Theorem 1 $(r = 0)$
 $= \sum_{k=0}^n (a_{n,k}^{(1)} - a_{n-2,k}^{(1)})$ by Lemma 1
 $= P_n^{(1)}(x) - P_{n-2}^{(1)}(x)$ by (1.3)
 $= B_{n+1}(x) - B_{n-1}(x)$ by (1.8).
Corollary 4: $C_n(x) = B_{n+1}(x) - B_{n-1}(x)$ by (2.11), Theorem 3

$$=\sum_{k=0}^{n-1} \frac{n}{k} \binom{n-1+k}{2k-1} x^{k} + 2 + x^{n} \quad \text{by (i), (2.4), (2.8), (2.11), Corollary 1.}$$

The property embodied in Corollary 4 means that $B_n(x)$ and $C_n(x)$ form another pair of cognate polynomials which can be incorporated into the synthesis [3], to which all the theory therein applies, e.g.,

$$B_n(x)C_n(x) = B_{2n}(x), (4.1)$$

$$\frac{d}{dx}C_n(x) = nB_n(x). \tag{4.2}$$

5. CHEBYSHEV POLYNOMIALS

Polynomials $P_n^{(r)}(x)$ are shown [1] to be related to $U_n(x)$, the Chebyshev polynomials of the second kind. In particular, with an adjusted subscript notation,

$$B_n(x) = \frac{\sin nt}{\sin t} = U_n\left(\frac{x+2}{2}\right),\tag{5.1}$$

[AUG.

where

$$x + 2 = 2\cos t$$
. (5.2)

Now, by Theorem 3, Corollary 4, and (5.2),

$$Q_n^{(0)}(x) = C_n(x) = B_{n+1}(x) - B_{n-1}(x)$$

= $\frac{\sin(n+1)t - \sin(n-1)t}{\sin t}$
= $2\cos nt$ (5.3)

$$=2T_n\left(\frac{x+2}{2}\right),\tag{5.4}$$

where $T_n(x)$ are the Chebyshev polynomials of the first kind.

More generally, we construct the law relating $Q_n^{(r)}(x)$ to the two types of Chebyshev polynomials. Needed for this is a pair of known results involving Chebyshev polynomials (our notation):

$$P_n^{(r)}(x) = U_{n+1}\left(\frac{x+2}{2}\right) + (r-1)U_n\left(\frac{x+2}{2}\right) \text{ by [1]};$$
 (5.5)

$$2T_n(x) = U_{n+1}(x) - U_{n-1}(x).$$
(5.6)

Theorem 4:
$$Q_n^{(r)}(x) = 2T_n\left(\frac{x+2}{2}\right) + rU_n\left(\frac{x+2}{2}\right).$$

Proof:
$$Q_n^{(r)}(x) = P_n^{(r)}(x) + P_{n-1}^{(0)}(x)$$
 by Theorem 2 $(n \ge 1)$
 $= U_{n+1}\left(\frac{x+2}{2}\right) + (r-1)U_n\left(\frac{x+2}{2}\right) + U_n\left(\frac{x+2}{2}\right) - U_{n-1}\left(\frac{x+2}{2}\right)$ by (5.5)
 $= U_{n+1}\left(\frac{x+2}{2}\right) - U_{n-1}\left(\frac{x+2}{2}\right) + rU_n\left(\frac{x+2}{2}\right)$
 $= 2T_n\left(\frac{x+2}{2}\right) + rU_n\left(\frac{x+2}{2}\right)$ by (5.6).

Zeros

Zeros x_k (k = 1, 2, ..., n) of $C_n(x) = Q_n^{(0)}(x)$ are, by (5.4), tied to the zeros of $T_n(\frac{x+2}{2})$. Thus,

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

implying

$$x_k = -4\sin^2\left(\frac{2k-1}{2n}\cdot\frac{\pi}{2}\right) \quad (k = 1, 2, ..., n).$$
 (5.7)

For instance, the 3 zeros of $C_3(x) \left[= 2T_3\left(\frac{x+2}{2}\right) \right] = x^3 + 6x^2 + 9x + 2 = (x+2)(x^2 + 4x + 1)$ are

1996]

$$x_k = -4\sin^2\left(\frac{\pi}{12}\right), -4\sin^2\left(\frac{\pi}{4}\right) = -2, -4\sin^2\left(\frac{5\pi}{12}\right) \quad (k = 1, 2, 3).$$

Zeros of $P_n^{(r)}(x)$ (r = 0, 1, 2, ..., n) are given in [1].

EPILOGUE

Together with the Morgan-Voyce polynomials $b_n(x)$ and $B_n(x)$, the polynomials $c_n(x)$ and $C_n(x)$ constitute an appealing quartet of polynomial relationships which form the subject of my paper alluded to following (1.9). Here, they exhibit a nice simplicity amid complexity, a cohesion and unity amid diversity.

REFERENCES

- 1. R. André-Jeannin. "A Generalization of Morgan-Voyce Polynomials." *The Fibonacci Quarterly* **32.3** (1994):228-31.
- 2. R. André-Jeannin. "A Note on a General Class of Polynomials, Part II." *The Fibonacci Quarterly* **33.4** (1995):341-51.
- 3. A. F. Horadam. "A Synthesis of Certain Polynomial Sequences." In Applications of Fibonacci Numbers 6 (in press).
- 4. A. M. Morgan-Voyce. "Ladder Networks Analysis Using Fibonacci Numbers." *I.R.E. Transactions Circuit Theory* **6.3** (1959):321-22.

AMS Classification Number: 11B39

ON THE SUMS OF DIGITS OF FIBONACCI NUMBERS

David C. Terr

Department of Mathematics, University of California at Berkeley, Berkeley, CA 94720 (Submitted December 1994)

1. INTRODUCTION

The problem of determining which integers k are equal to the sum of the digits of F_k was first brought to my attention at the Fibonacci Conference in Pullman, Washington, this summer (1994). Professor Dan Fielder presented this as an open problem, having obtained all solutions for $k \leq 2000$. There seemed to be fairly many solutions in base 10, and it was not clear whether there were infinitely many. Shortly after hearing the problem, it occurred to me why there were so many solutions. If one assumes that the digits F_k are independently uniformly randomly distributed, then one expects S(k), the sum of the digits of F_k , to be approximately $\frac{9}{2}k\log_{10}\alpha$, where $\alpha = \frac{1}{2}(1+\sqrt{5}) \approx 1.61803$ is the golden mean. Since $\frac{9}{2}\log_{10}\alpha \approx 0.94044$, we expect $S(k) \approx$ 0.94044k. Since this is close to k, we expect many solutions to S(k) = k, at least for reasonably small k. However, as k gets large, we expect S(k)/k to deviate from 0.94044 by less and less. Thus, it appears that, for some integer n_0 , the ratio S(k)/k never gets as large as 1 for $k > n_0$, so S(k) = k has no solutions for $k > n_0$, and thus has finitely many solutions. In this paper, I present two closely related probabilistic models to predict the number of solutions. More generally, they predict N(b, n), the number of solutions to S(k, b) = k for $k \le n$, where S(k, b) is the sum of the digits of F_k in base b [thus, S(k; 10) = S(k)]. Let N(b) denote the total number of solutions in base b [thus, $N(b; n) \rightarrow N(b)$ as $n \rightarrow \infty$]. Both models predict finite values of N(b) for each base b. In the simpler model, N(10) is estimated to be 18.24 ± 3.86 , compared with the actual value N(10; 20000) = 20.

2. THE NAIVE MODEL

In this model I assume that the digits of F_k are independently uniformly randomly distributed among $\{0, 1, ..., b-1\}$ for each positive integer k and each fixed base $b \ge 4$. [It is fairly easy to prove that the only solutions to S(k; b) = k are 0 and 1 when b = 2 or 3. The proof involves showing that, for all sufficiently large k, we have $(b-1)(1+\log_b F_k) < k$.] Now let $\alpha = \frac{1}{2}(1+\sqrt{5})$ and $\beta = \frac{1}{2}(1-\sqrt{5})$. Then

$$F_k = \frac{\alpha^k - \beta^k}{\sqrt{5}} = \frac{\alpha^k}{\sqrt{5}} + o(1) \text{ for } k \to \infty.$$

The number of digits of F_k in base *b* is approximately the base-*b* logarithm of this number, $k \log_b \alpha - \log_b \sqrt{5} \approx k \log_b \alpha = k\gamma$, where $\gamma = \log_b \alpha$ and I neglect terms of order 1. In this model, the expected value of each digit of F_k is $\frac{1}{2}(b-1)$ and the standard deviation (SD) is $\sqrt{\frac{1}{12}(b^2-1)}$ (see [2], pp. 80-86). Therefore, the expected value of S(k; b) is approximately $\overline{S} = \frac{k}{2}(b-1)\gamma$ and the SD is approximately $\sigma = \sqrt{\frac{k}{12}(b^2-1)\gamma}$. Let $\mathcal{P}_1(k; \ell)$ denote the probability that $\widetilde{S}(k; b) = \ell$, where $\widetilde{S}(k; b)$ is distributed as the sum $Y_{k,1} + Y_{k,2} + \cdots + Y_{k,[k\gamma]}$, the $Y_{k,j}$ being independent random variables, each uniformly distributed over $\{0, 1, \dots, b-1\}$. According to the

1996]

central limit theorem ([2], pp. 165-77), if k is reasonably large, the probability distribution is approximately Gaussian, so

$$\mathcal{P}_1(k;\ell) \approx \frac{1}{\sigma\sqrt{2\pi}} \exp\left[\frac{-(\overline{S}-\ell)^2}{2\sigma^2}\right] = \sqrt{\frac{6}{k\pi\gamma(b^2-1)}} \exp\left[\frac{-6\left(k\gamma(\frac{b-1}{2})-\ell\right)^2}{k\gamma(b^2-1)}\right]$$

Let $\mathcal{P}_1(k) = \mathcal{P}_1(k; k)$; this is the estimated percentage of Fibonacci numbers $F_{k'}$ for k' near k whose base-b digits sum to the index k'. We have $\mathcal{P}_1(k) \approx Ae^{-Bk} / \sqrt{k}$, where

$$A = \sqrt{\frac{6}{\pi \gamma (b^2 - 1)}} \quad \text{and} \quad B = \frac{6(\gamma (\frac{b-1}{2}) - 1)^2}{\gamma (b^2 - 1)}$$

Incidentally, it is clear that the only solutions k for which $F_k < b$ are those for which $F_k = k$, namely 0, 1, and possibly 5 (if b > 5). We might as well put in these solutions by hand. Thus, in the model, we only calculate $\mathcal{P}_1(k)$ for k for which $F_k \ge b$ and add N_0 to the final result upon summing the probabilities, where $N_0 = 3$ if b > 5, otherwise $N_0 = 2$. Thus, our estimate for N(b; n) in this model is

$$N_1(b;n) = N_0 + \sum_{\substack{k \le n \\ F_k \ge b}} \mathcal{P}_1(k) \approx N_0 + \sum_{\substack{k \le n \\ F_k \ge b}} \frac{Ae^{-Bk}}{\sqrt{k}}$$

and the standard deviation of this estimate is [assuming that the S(k, b) are uncorrelated for different values of k]

$$\Delta_1(b;n) = \sqrt{\sum_{\substack{k \le n \\ F_k \ge b}} \mathcal{P}_1(k)(1-\mathcal{P}_1(k))} \approx \sqrt{\sum_{\substack{k \le n \\ F_k \ge b}} \frac{Ae^{-Bk}(\sqrt{k}-Ae^{-Bk})}{k}$$

This model gives good results for some bases, but not all. The next model is an improvement which seems to yield accurate results for all bases.

3. THE IMPROVED MODEL

In this model, I still assume that the digits of F_n are uniformly distributed over $\{0, 1, ..., b-1\}$, but with one restriction, namely, their sum modulo b-1. It is well known that the sum of the base-10 digits of a number a is congruent to $a \mod 9$. In general, the same applies to the sum of the digits in base $b \mod b-1$. Thus, we have the restriction $S(k; b) \equiv F_k \pmod{b-1}$. In particular, k cannot be a solution to S(k; b) = k unless $k \equiv F_k \pmod{b-1}$. This latter equation is not too difficult to solve. Upon solving it, we end up with a restriction of the form

$$k \mod q \in S. \tag{1}$$

Here, q = [b-1, p], where p = per(b-1) is the period of the Fibonacci sequence modulo b-1 and S is a specified subset of $\{0, 1, ..., q-1\}$. If k does not satisfy the above condition, it need not be considered, since the sum of its digits cannot equal F_n . On the other hand, if k does satisfy the condition, we know that the sum of its digits is congruent to F_n modulo b-1. In the improved model, we take this restriction into account and otherwise assume a uniform random distribution

of digits in F_n . In analogy to $\tilde{S}(k; b)$, let $\hat{S}(k; b)$ be distributed as the sum $Y_{k,1} + \cdots + Y_{k,\lfloor k\gamma \rfloor}$, the $Y_{k,j}$ being random variables uniformly distributed over 0, 1, ..., b-1 and independent except for the restriction that $Y_{k,1} + \cdots + Y_{k,\lfloor k\gamma \rfloor} \equiv F_k \pmod{b-1}$. We now estimate the probability $\mathcal{P}_2(k)$ that $\hat{S}(k; b) = k$ to be b-1 times our earlier estimate in the case where k satisfies (1) and zero otherwise, i.e.,

$$\mathcal{P}_{2}(k) = \begin{cases} (b-1)\mathcal{P}_{1}(k) & k \mod q \in S, \\ 0 & k \mod q \notin S. \end{cases}$$

Thus, in this model, the expectation and SD of N(b; n) are approximately

$$N_2(b;n) = N_0 + \sum_{\substack{k \le n \\ F_k \ge b}} \mathcal{P}_2(k) \approx N_0 + (b-1) \sum_{\substack{k \le n \\ F_k \ge b \\ k \mod q \in S}} \frac{Ae^{-bk}}{\sqrt{k}}$$

and

$$\Delta_2(b;n) = \sqrt{\sum_{\substack{k \le n \\ F_k \ge b}} \mathcal{P}_2(k)(1-\mathcal{P}_2(k))} \approx \sqrt{(b-1)\sum_{\substack{k \le n \\ F_k \ge b \\ k \bmod q \in S}} \frac{Ae^{-Bk}(\sqrt{k}-Ae^{-Bk})}{k}$$

As an example of how to calculate S, consider b = 8. In this case, p = per(7) = 16 and q = [7, 16] = 112. To determine S, we first tabulate k mod 16 and $F_k \mod 7$ for each congruence class of k mod 16. Next, below the line, we tabulate the unique solutions modulo 112 to the congruences $x \equiv k \pmod{16}$ and $x \equiv F_k \pmod{7}$. Since (16, 7) = 1, by the Chinese Remainder Theorem, each of these solutions exists and is unique.

<i>k</i> mod 16	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
$F_k \mod 7$	0	1	1	2	3	5	1	6	0	6	6	5	4	2	6	1	
<i>k</i> mod 112	0	1	50	51	52	5	22	55	56	41	90	75	60	93	62	15	

Thus, $S = \{0, 1, 5, 15, 22, 41, 50, 51, 52, 55, 56, 60, 62, 75, 90, 93\}$. Note that, in this example, the pair of congruences $k \equiv j \pmod{p}$ and $k \equiv F_j \mod b - 1$ has a solution mod q for every integer $j \mod p$. This is because, in this example, b - 1 = 7 and p = 16 are coprime. In general, this is not the case. For example, for b = 10, we get p = 24, which is not coprime to b - 1 = 9. Thus, if we constructed a similar table for b = 10, we would expect to get some simultaneous congruences without solutions. This is in fact the case, i.e., the pair of congruences $k \equiv 2 \pmod{24}$ and $k \equiv F_2 = 1 \pmod{9}$ has no solutions. We expect only one-third (eight) of them to have a solution, since (9, 24) = 3. In fact, we do get eight. For b = 10, we find $S = \{0, 1, 5, 10, 31, 35, 36, 62\}$ and q = 72.

One might wonder by about how much $N_1(k; b)$ and $N_2(k; b)$ differ. To first order, they differ by a multiplicative factor depending on b, i.e., $N_2(b; n) \approx M(b)N_1(b; n)$. Recall that in going from the first model to the second, we selected s out of every q congruence classes modulo q, where s = #S. Also, we multiplied the corresponding probabilities by b-1. Thus, M(b) = (b-1)s/q. For some bases, M(b) = 1, so the predictions of both models are essentially the same. This is true in particular whenever b-1 and p are coprime, and also in some other cases, like b = 10. However, there are other bases for which $M(b) \neq 1$; in fact, the difference can be quite

1996]

large! For instance, for b = 11, we find p = q = 60 and s = 14, hence $M(11) = 10 \times 14/60 = 7/3$, which is greater than 2. Thus, for b = 11, the second model predicts over twice as many solutions to S(k; 11) = k as the first model. In this case, as we will see, the second model agrees well with the known data; the first does not.

4. COMPARISON OF MODELS WITH "EXPERIMENT"

Every good scientist knows that the best way to test a model or theory is to see how well its predictions agree with experimental data. In this case, my "experiment" was a computer program I wrote and ran on my Macintosh LCII to determine S(k; b) given $k \le 20000$ and $b \le 20$. Incidentally, it is not necessary to calculate the Fibonacci numbers directly, only to store the digits in an array. Also, only two Fibonacci arrays need to be stored at one time. Nevertheless, trying to compute for k > 20000 presented memory problems, at least for the method I used. Still, this turned out to be sufficient for determining with high certainty all solutions to S(k; b) = kexcept for b = 11.

Here I present all the solutions I found for $4 \le b \le 20$ and $k \le n$.

b=4, n=1000:	0	1						
b=5, n=1000:	0	1						
b=6, n=1000:	0	1	5	9	15	35		
b=7, n=1000:	0	1	5	7	11	12	53	
b=8, n=1000:	0	1	5	22	41			
b=9, n=5000:	0	1	5	29	77	149	312	
b=10, n=20000:	0 175 540	1 180 946	5 216 1188	10 251 2222	31 252	35 360	62 494	72 504
b=11, n=20000:	$0 \\ 61 \\ 269 \\ 617$	1 90 353 629	5 97 355 630	13 169 385 653	41 185 397 713	53 193 437 750	55 215 481 769	60 265 493 780
	889 1405 1769	905 1435 1793	960 1501 1913	1013 1620 1981	1025 1650 2125	1045 1657 2153	1205 1705 2280	1320 1735 2297
	2389 2610 3055 3721	2413 2633 3155 3749	2460 2730 3209 3757	2465 2749 3360 3761	2509 2845 3475 3840	2533 2893 3485 3865	2549 2915 3521 3929	2609 3041 3641 3941
	4075 5489 6373	4273 5490 6401	4301 5700 6581	4650 5917 6593	4937 6169 6701	5195 6253 6750	5209 6335 6941	5435 6361 7021
	7349 8017 9120	7577 8215 9133	7595 8341 9181	7693 8495 9269	7740 8737 9277	7805 8861 9535	7873 8970 9541	8009 8995 9737
	9935 12029 14381	9953 12175 14550	10297 12353 14935	10609 12461 15055	10789 12565 15115	10855 12805 15289	11317 12893 15637	11809 13855 15709
	17941 18990	10789 17993 19135	10837 18193 19140	17065 18257 19375	17237 18421 19453	17605 18515 19657	17681 18733 19873	17873 18865

ON THE SUMS OF DIGITS OF FIBONACCI NUMBERS

b=12, n=20000:	0	1	5	13	14	89	96	123
	221	387	419	550	648	749	866	892
	1105	2037						
b=13, n=5000:	0	1	5	12	24	25	36	48
	53	72	73	132	156	173	197	437
	444	485	696	769	773			
b=14, n=3000:	0	1	5	8	11	27	34	181
	192	194						
b=15, n=2000:	0	1	5					
h = 16 n = 2000	0	1	5	10	60	101		
0 = 10, n = 2000.	0	1	0	10	00	101		
b=17, n=1000:	0	1	5					
b=18, n=1000:	0	1	5	60				
b=19, n=1000:	0	1	5	31	36			
b=20, n=1000:	0	1	5	21	22			

Next, I tabulated $N_1(b; n) \pm \Delta_1(b; n)$, $N_2(b; n) \pm \Delta_2(b; n)$, N(b; n), $(\frac{b-1}{2})\log_b \alpha$, and M(b) for the above pairs (b, n). Note how N(b; n) increases as $(\frac{b-1}{2})\log_b \alpha$ approaches 1.

b	n	$N_1(b;n)\pm \Delta_1(b;n)$	$N_2(b;n)\pm\Delta_2(b;n)$	N(b;n)	$(\frac{b-1}{2})\log_b \alpha$	M(b)
4	1000	2.25 ± 0.49	2.43 ± 0.61	2	0.52068	1.00
5	1000	2.67 ± 0.79	2.76 ± 0.72	2	0.59799	1.00
6	1000	4.17 ± 1.05	5.04 ± 1.25	6	0.67142	2.00
7	1000	5.10 ± 1.41	6.18 ± 1.42	7	0.74188	1.50
8	1000	6.61 ± 1.85	5.84 ± 1.47	5	0.80995	1.00
9	5000	9.40 ± 2.48	8.57 ± 2.09	7	0.87604	1.00
10	20000	18.24 ± 3.86	17.77 ± 3.46	20	0.94044	1.00
11	20000	79.71 ± 8.72	180.95 ± 12.82	183	1.00340	2.33
12	20000	17.03 ± 3.71	17.01 ± 3.28	18	1.06510	1.00
13	5000	9.71 ± 2.56	15.73 ± 3.08	21	1.12566	2.00
14	3000	7.15 ± 2.01	8.22 ± 1.62	10	1.18522	1.00
15	2000	5.93 ± 1.69	4.70 ± 1.19	3	1.24387	1.00
16	2000	5.21 ± 1.47	7.16 ± 1.62	6	1.30170	2.00
17	1000	4.75 ± 1.31	3.94 ± 0.90	3	1.35877	1.00
18	1000	4.42 ± 1.18	4.69 ± 1.06	4	1.41515	1.00
19	1000	4.10 ± 1.08	4.12 ± 0.95	5	1.47088	1.50
20	1000	4.01 ± 1.00	4.54 ± 0.97	5	1.52601	1.00

As one can see, the first model does not make accurate predictions for each base. In particular, its predictions for bases 11 and 13 are off by roughly 12 and 4.5 standard deviations, respectively. On the other hand, the second model seems to agree well with the known data for each base. For 12 out of 17 bases, its predictions are correct within one SD, and all 17 predictions are correct within two SD's. (The largest deviation, found for b = 13, is -1.71 SD's.) Furthermore, there does not seem to be a directional bias of the model. Eight out of 17 of the predicted values are too high; the other 9 are too low. Thus, the second model looks good.

5. PREDICTING THE UNKNOWN

With this in mind, we can use the second model to make predictions for which we are unable to calculate at present. In particular, we can estimate N(11), the total number of solutions to S(k, 11) = k in base 11, as well as the value of the largest one. We can also estimate the probability that we missed some solutions in each of the other bases we looked at. For these bases, I was careful to calculate out to large enough n so that these probabilities should be very small.

I calculated $N_2(11; n) \pm \Delta_2(11; n)$ for $200000 \le n \le 4000000$ in intervals of 200000. Here are the results:

	n	$N_2($	(11; n)	$\pm \Delta_{2}$	$_{2}(11; n)$
--	---	--------	---------	------------------	---------------

200000	490.38 ± 21.70
400000	595.89 ± 24.00
600000	641.02 ± 24.93
800000	662.32 ± 25.35
1000000	672.83 ± 25.56
1200000	678.16 ± 25.66
1400000	680.91 ± 25.71
1600000	682.34 ± 25.74
1800000	683.10 ± 25.76
2000000	683.50 ± 25.77
2200000	683.72 ± 25.77
2400000	683.83 ± 25.77
2600000	683.89 ± 25.77
2800000	683.93 ± 25.77
3000000	683.94 ± 25.77
3200000	683.95 ± 25.77
3400000	683.96 ± 25.77
3600000	683.96 ± 25.77
3800000	683.96 ± 25.77
4000000	683.97 ± 25.77

As can be seen, the results converge rapidly for large n. Let N'(b; n) denote the estimated number of solutions to S(k; b) = k for k > n. Then we have

$$N'(b; n) = \sum_{\substack{k > n \\ k \bmod q \in S}} \frac{Ae^{-Bk}}{\sqrt{k}} \approx M(b) \sum_{k > n} \frac{Ae^{-Bk}}{\sqrt{k}} \approx \frac{M(b)A}{\sqrt{B}} \int_{Bn}^{\infty} \frac{e^{-x}dx}{\sqrt{x}}$$
$$\approx M(b)A \sqrt{\frac{\pi}{B}} \operatorname{erfc} \sqrt{Bn} \approx \frac{M(b)A}{B\sqrt{n}} e^{-Bn},$$

where I make the change of variables $y = \sqrt{x}$ in the integral to get the error function term. In the last step, I use an asymptotic expansion of erfc [1].

I next tabulated N'(b,n) for the pairs (b,n) used, except for b=11, where I used n=14000000, the largest n for which I have estimated N(b, n). Since N' is much less than 1 in each case, the values of N' listed are the approximate probabilities that there is a solution to S(k; b) = k for k > n. I also tabulated the corresponding values of A, B, and M(b). Note that for every base less than 20, except 11, N'(b; n) is less than 10^{-6} ; in fact, the sums of these entries is roughly 10⁻⁶. Thus, if this model is accurate, there is about one chance in a million that I have missed any solutions in these bases. Also, note that the table of estimates of $N_2(11; n)$ can be used to estimate the largest solution to S(k; 11) = k.

[AUG.

ON THE SUMS OF DIGITS OF FIBONACCI NUMBERS

b	n	Α	B	M(b)	N'(b;n)
4	1000	0.606	2.65×10^{-1}	1.000	7.6×10^{-117}
5	1000	0.516	1.35×10^{-1}	1.000	2.5×10^{-60}
6	1000	0.451	6.89×10^{-2}	2.000	4.7×10^{-31}
7	1000	0.401	$3.37 imes 10^{-2}$	1.500	$1.3 imes 10^{-15}$
8	1000	0.362	1.49×10^{-2}	1.000	2.7×10^{-7}
9	5000	0.330	$5.26 imes 10^{-3}$	1.000	$2.3 imes 10^{-12}$
10	20000	0.304	1.03×10^{-3}	1.000	$2.4 imes 10^{-9}$
11	4000000	0.282	2.89×10^{-6}	2.333	1.1×10^{-3}
12	20000	0.263	9.18×10^{-4}	1.000	2.1×10^{-9}
13	5000	0.246	3.01×10^{-3}	2.000	6.8×10^{-7}
14	3000	0.232	$5.79 imes 10^{-3}$	1.000	1.6×10^{-8}
15	2000	0.219	8.97×10^{-3}	1.000	7.2×10^{-9}
16	2000	0.208	1.23×10^{-2}	2.000	1.7×10^{-11}
17	1000	0.198	1.58×10^{-2}	1.000	5.5×10^{-8}
18	1000	0.188	1.92×10^{-2}	1.000	1.4×10^{-9}
19	1000	0.180	2.26×10^{-2}	2.000	5.2×10^{-11}
20	1000	0.172	2.59×10^{-2}	1.000	1.1×10^{-12}

Suppose one wishes to find *n* such that there is a 50% chance that there are no solutions larger than *n*. According to Poisson statistics, this happens when the $N_2(11; n) = \ln 2 \approx 0.69$. By interpolating in the previous table, we see that this occurs when $n \approx 1.9 \times 10^6$; this is roughly the value we can expect for the largest solution. Calculating S(k; 11) for k up to 2.8×10^6 yields a 96% probability of finding all the solutions, and going up to 4×10^6 yields a 99.9% probability of finding them all. Perhaps someone will do this calculation in the near future.

ACKNOWLEDGMENTS

I would like to give special thanks to my advisor, H. W. Lenstra, Jr., for helping me with this paper. In particular, he made me aware of the need for congruence relations in finding solutions to S(k, b) = k.

REFERENCES

- 1. M. Abramowitz & I. A. Stegun. *Handbook of Mathematical Functions*. 9th ed. New York: Dover Publications, 1970.
- 2. H. J. Larson. Statistics: An Introduction. New York, London: Wiley, 1975.

AMS Classification Numbers: 11A63, 11B39, 60F99

** ** **

1996]

ON SEQUENCES RELATED TO EXPANSIONS OF REAL NUMBERS

E. Vantieghem

Leeuwerikenstraat 96, B-3001 Heverlee (Leuven), Belgium (Submitted December 1994)

1. INTRODUCTION

We intend to study some sequences of real numbers which are obtained as follows: take a natural number N and a real number α and form the sequence $s(N, \alpha) = (a_0, a_1, a_2, ..., a_k, ...)$, where the numbers a_i are defined by

$$a_{0} = \alpha,$$

$$a_{n} = \begin{cases} 2a_{n-1} & \text{if } 2a_{n-1} < N+n, \\ 2a_{n-1} - (N+n) & \text{otherwise.} \end{cases}$$
(1)

The sequences arise from certain nonstandard expansions of real numbers that are discussed in Section 3.

It is very easy to study these sequences by computer. This is what we did, and which led us to the following

Conjecture 1: When α is an integer $\in [0, N+2)$, the sequence $s(N, \alpha)$ will end in a sequence of zeros.

We verified the truth of this statement for all $N \le 2\,000\,000$.

In the next section we shall show that there is also some "probabilistic" evidence for this conjecture. In Section 3 we shall see that the conjecture has some "heuristic evidence." Finally, we shall conclude with a discussion of some other aspects of the problem.

2. PROBABILISTIC EVIDENCE

Consider a sequence $s(N, \alpha) = (a_0, a_1, a_2, ..., a_k, ...)$, where N is a natural number ≥ 2 and $\alpha = a_0 \in (0, N+2]$ and where the a_k are obtained by the relations (1).

If $\alpha < 0$, then $a_k = 2^k \alpha$; if $\alpha = N + 2 + \beta$ ($\beta \ge 0$), then $a_k = N + k + 2 + 2^k$ for all k. Thus, the behavior of $s(N, \alpha)$ is "sufficiently known" for such α .

If $0 \le a < N+2$, then it is easy to show that every a_k is in [0, N+k+2).

Indeed, this is obvious when k = 0. Suppose it is true for some $k \ge 0$. Then

- when $a_{k+1} = 2a_k$, we have $a_{k+1} < N + k + 1 < N + k + 3$,
- when $a_{k+1} = 2a_k N k 1$, then $a_{k+1} \le 2(N + k + 2) N k 1 = N + k + 3$.

Therefore, our assumption follows by induction.

Now, let α be an *integer* in (0, N+2). Then it is easy to verify that a_k will be in the interval [0, N+k) as soon as $k \ge 2$. Further, we obviously have

$$a_k \equiv 2a_{k-1} \mod(N+k) \quad \forall k \ge 1,$$

356

AUG.

whence a_k will be even as soon as N+k is (k > 0). Thus, $a_k = 0$ (smallest k) implies N+k even. It is also not difficult to see that we can restrict our attention to sequences with even N = 2M, so that in the *n*-tuple $(a_2, a_4, ..., a_{2n})$ the a_{2i} are even integers in the interval [0, N+2i). If they would behave like "random," the probability that **none** of them equals 0 is easy to compute.

Indeed, the total number of *n*-tuples $(b_1, b_2, ..., b_n)$ with $b_i \in N \cap [0, 2M + 2i)$, b_i even, is equal to the product $(M+1) \cdot (M+2) \cdots \cdot (M+n)$, while the total number of such *n*-tuples where no b_i is zero equals $M \cdot (M+1) \cdots \cdot (M+n-1)$. Thus, the chance for such an *n*-tuple not to contain 0 is

$$\frac{M(M+1)\cdot(M+n-1)}{(M+1)(M+2)\cdots(M+n)} = \frac{M}{M+n}.$$

Clearly, this number tends to 0 if *n* tends to infinity.

We include a small table in which the reader may find some numerical results concerning the "randomness" of the a_i .

N	\bar{l}_N	\bar{l}'_N
100	925.9	693.9
200	5902.3	2016.5
300	9999.3	2307.2
500	9993.6	8802.7
1000	10610.8	5701.3
2000	7389.8	50789.5
4000	11885.0	69030.1
8000	551313	95802.9

Here, l_N is the arithmetic mean of the numbers l_{α} that are defined as the smallest number k for which a_k is 0 ($\alpha = 1, 2, ..., N-1$).

The number l'_N is the arithmetic mean of 1000 numbers l'_N , which has the same meaning as the l_i but where the a_k are chosen at random in [0, N+k). Note that the l'_i will vary from one time to another. The reader who wishes to verify these numbers will probably not find the same ones.

3. SOME NONSTANDARD EXPANSION OF NUMBERS

First, note that a necessary condition for the sequences $s(N, \alpha)$ to end in a string of zeros is that α is a *rational number* with denominator of the form 2^t , for some $t \in \mathbb{N}$. Indeed, the equality $a_k = 0$ (for some $k \in \mathbb{N}_0$) implies $a_k = 2a_{k-1} - N - k$, which means that a_{k-1} is a rational number with denominator 2. From this it follows immediately that a_{k-2} must be a rational number with denominator 4. Continuing this proves our assertion.

In what follows, we shall discuss an "expansion of real numbers" that is (in some way) similar to what is known as "binary expansion."

Theorem 1: Every real number α in the interval [0, 2] can be written as an infinite sum

$$\alpha = \sum_{1}^{\infty} \delta_k \frac{k}{2^k}, \text{ where the } \delta_k \text{ are 0 or 1.}$$
 (2)

1996]

This is a special case of a more general theorem of Brown [1] that reads as follows:

If $\{r_i\}$ is a non-increasing sequence of real numbers with $\lim r_i = 0$ and $\{k_i\}$ is an arbitrary sequence of positive integers then every real number x in the interval $[0, \sum_{i=1}^{\infty} k_i r_i]$ can be expanded in the form $x = \sum_{i=1}^{\infty} \beta_i r_i$, where the β_i are integers satisfying $0 \le \beta_i \le k_i$, for all *i*, if and only if $r_p \le \sum_{i=p+1}^{\infty} k_i r_i$ for all $p \ge 1$.

The reader may verify that the conditions of this theorem are fulfilled when $r_i = i/2^i$, $k_i = 1$. However, to see the connection with the sequences mentioned in the introduction, it will be convenient to give a proof of this particular case.

Before doing so, notice that when the sum in (2) is *finite*, α will be a rational number with denominator of the form 2^t , $t \in \mathbb{N}_0$. About the converse, we state

Conjecture 2: Every rational number whose denominator is a power of 2 has a finite expansion (2).

We shall see that Conjecture 1 implies Conjecture 2. This implies that our numerical investigations provide a proof for the fact that every rational number in [0, 2] whose denominator is 2^t , $t \le 2\ 000\ 000$, can be expanded as a finite sum (2).

Proof of Theorem 1: Let us abbreviate the numbers $k/2^k$ as u_k . First, note that the series $\sum_{k=1}^{\infty} u_k$ converges to 2. This follows from the equality

$$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k \quad (x \in [0, 1])$$

which gives, after differentiation and multiplication by x_{i}

$$x \cdot \frac{1}{(1-x)^2} = \sum_{k=1}^{\infty} k x^k.$$

Taking x = 1/2 gives the desired result

It is also clear from this that any series of the form (2) converges.

Now let α be an arbitrary element of (0, 2) (the case $\alpha = 0$ or 2 is trivial). We define the numbers δ_k and the numbers B_k as follows:

If $\alpha \ge u_1 \ (=1/2)$, then $\delta_1 = 1$, else $\delta_1 = 0$; $B_1 = \alpha - \delta_1 u_1$. If $B_1 \ge u_2 \ (=2/2^2)$, then $\delta_2 = 1$, else $\delta_2 = 0$; $B_2 = B_1 - \delta_2 u_2$. If $B_2 \ge u_3 \ (=3/2^3)$, then $\delta_3 = 1$, else $\delta_3 = 0$; $B_3 = B_2 - \delta_3 u_3$

Our algorithm produces the digits δ_k by a so-called greedy expansion. It suffices to show that the sequence $(B_1, B_2, ...)$ has limit 0. To do so, put

$$a_0 = \alpha,$$

 $a_k = 2^k B_k \ (k = 1, 2, ...).$

Then it is clear that we have $a_{k+1} = 2a_k - \delta_{k+1}$ (k + 1), whence, by the definition of the δ_k :

$$a_{k+1} = \begin{cases} 2a_k & \text{if } < k+1, \\ 2a_k - (k+1) & \text{otherwise.} \end{cases}$$

AUG.
Since, previously, we noted that every a_k is in [0, k+2), we have $B_k \in [0, \frac{k+2}{2^k}]$, which completes the proof.

Note also that if **one** of the numbers B_i is zero, then so are all B_j when $j \ge i$; note further that the expansion is not "unique." To see this, define numbers η_k and numbers B'_k in the following way:

If
$$\alpha > u_1 (= 1/2)$$
, then $\eta_1 = 1$, else $\eta_1 = 0$; $B'_1 = \alpha - \eta_1 u_1$,
If $B'_1 > u_2 (= 2/2^2)$, then $\eta_2 = 0$; $B'_2 = B'_1 - \eta_2 u_2$,
If $B'_2 > u_3 (= 3/2^3)$, then $\eta_3 = 0$; $B'_3 = B'_2 - \eta_3 u_3$,

thus constructing a sequence B'_i of real numbers none of which will ever be zero.

The corresponding numbers a'_k (= $2^k B_k$) then satisfy a slightly different recursion, namely,

$$a'_{k+1} = \begin{cases} 2a'_k & \text{if } \le k+1, \\ 2a'_k - (k+1) & \text{otherwise,} \end{cases}$$

so that in this case a'_{k+1} might be in the interval $(0, k+3] \dots$

The proof of the theorem leads to the construction of a sequence s(N, a) with $a = \alpha$ and N = 0 as defined in the introduction.

Now, suppose $\alpha \in [0, 2]$ is a rational number of the form $k / 2^m$ with $k, m \in \mathbb{N}_0$. Then a_i is a rational number with denominator 2^{m-i} (i = 1, 2, ..., m) and will be an integer for i > m. From the proof, it is also clear that a_i is in the interval [0, 2+i). It is also easy to see that a_i is in the interval [0, 2+i). It is also easy to see that a_i is in the interval [0, i] when i > m + 1.

Thus, to see if every such α has a finite expression (2), it suffices to see if every series $s(N, \alpha)$ with N < m and α an integer in the range 1, 2, ..., N-1 will "end" in zeros. We took $N = 2\,000\,000$ and found $a_K = 0$ for some $K \le 4\,588\,298\,126$ (the computations took several hours on a fast PC).

Since the expansion (2) is not unique, it is possible that Conjecture 2 is true even if Conjecture 1 should prove false.

4. OTHER ANALOGS WITH BINARY EXPANSIONS

There is another analog of the expansion (2) with "binary expansions." Consider a number α such that the δ_k are *periodic*, i.e., there exists a nonzero natural number p such that

$$\delta_k = \delta_{p+k} \tag{3}$$

for all $k \in \mathbb{N}$. In such a case, we have

$$\alpha = \sum_{i=1}^{p} \delta_{i} \frac{i}{2^{i}} + \sum_{i=1}^{p} \delta_{i} \frac{p+i}{2^{p+i}} + \sum_{i=1}^{p} \delta_{i} \frac{2p+i}{2^{2p+i}} + \dots = \sum_{k=0}^{\infty} \left(\sum_{i=1}^{p} \delta_{i} \frac{kp+i}{2^{kp+i}} \right).$$

Theorem 2: α is a rational number.

Proof: Define the polynomial v(x) as $\sum_{i=1}^{p} \delta_i x^i$ and the real function $\varphi(x)$ as $\sum_{i=1}^{\infty} \delta_i x^i$. By the periodicity of the δ_i , we have

1996]

$$\varphi(x) = v(x) + x^p v(x) + x^{2p} v(x) + \dots = v(x) \frac{1}{1 - x^p}$$

Differentiation and multiplying with *x* gives

$$x\varphi'(x) = \sum_{i=1}^{\infty} \delta_i ix^i = \frac{x(1-x^p)v'(x) + v(x)px^p}{(1-x^p)^2}.$$

Putting x = 1/2 yields

$$\alpha = \frac{\nu'(1/2)2^{p-1}}{2^p - 1} + \frac{p2^p \nu(1/2)}{(2^p - 1)^2}.$$
(4)

It is easy to see that the numerators of the two fractions are both integers, which proves the theorem.

As to nonpure periodic expansions [this happens when the relations (3) are true for all $k \ge$ some *m*], it is not difficult to show that these α differ from some purely periodic number by a rational number with 2^m in the denominator.

It should be noted also that the pure periodic expansion of a number is in general **not** the one obtained by the greedy procedure explained in the proof of Theorem 1. For instance, if we take α to be 8/9, the sequence (δ_k) in Theorem 1 would be the nonpure periodic

$$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, \dots)$$

while we have the equality

$$\frac{8}{9} = \sum_{k=1}^{\infty} \frac{2k}{2^{2k}}$$

which is obviously pure periodic.

The converse of Theorem 2, however, is not true. This is seen by examining the second fraction in (4). Its numerator equals $\delta_1 2^{p-1} + \delta_2 2^{p-2} + \dots + \delta_p$, which can be **any** of the values 0, 1, 2, 3, ..., 2^{p-1} . However, this is not sufficient to cancel enough factors of the denominator to yield **any** prescribed denominator. For instance, the number 1/3 is never equal to any periodic expression (2).

This may be considered as a (weak) argument that Conjecture 1 could fail to be true.

Remark: The number 2 plays a special role in all of the preceding in the following way. Consider series of the form

$$\sum_{k=1}^{\infty} \delta_k k c^k \quad (c \in [0, 1))$$
(5)

where the δ_k are 0 or 1.

It is clear that such a series converges to a number of the interval [0, A]

$$A = \sum_{k=1}^{\infty} k c^{k} = \frac{c}{(1-c)^{2}}.$$

Using these notations, we can prove

Theorem 3: Every real number in the interval [0, A] can be expressed as a sum (5) if and only if $c \in [1/2, 1)$.

360

[AUG.

The proof is an immediate consequence of Brown's theorem applied to this case. Indeed, Brown's theorem states that every real number in the interval [0, A] is expressible as a sum (5) if and only if

$$pc^{p} \leq \sum_{k=p+1}^{\infty} kc^{k} = c^{p} \left(\sum_{i=1}^{\infty} (pc^{i} + ic^{i}) \right) = c^{p} \left(\frac{pc}{1-c} + \frac{c}{(1-c)^{2}} \right), \quad \forall p \in \mathbb{N}.$$

This is equivalent to $p(2c-1)(c-1) \le c$, $\forall p \in \mathbb{N}$, and this holds if and only if $c \in [1/2, 1)$. Q.E.D.

Therefore, extensions of our results when c is of the form $1/n, n \in \mathbb{N}, n > 2$ are not very likely to hold.

It is worthwhile to note that the number 2 has a similar role when looking at expansions of real numbers in the form

$$\sum_{k=1}^{\infty} \delta_k c^k \quad (c \in [0, 1)), \text{ where the } \delta_k \text{ are } 0 \text{ or } 1$$

(which includes binary expansions). In the same way as above, we obtain

Theorem 4: Every real number in the interval [0, A] can be expressed as a sum $\sum_{k=1}^{\infty} \delta_k c^k$ if and only if $c \in [1/2, 1)$.

This theorem has a surprising geometric interpretation. Consider for every infinite string

$$\delta = (\delta_1, \delta_2, \delta_3, \dots); \ \delta_i = 0 \text{ or } 1$$

a real function $\varphi_{\delta}(x)$ defined by

$$\varphi_{\delta}(x) = \sum_{k=1}^{\infty} \delta_k x^k, \ x \in [0,1].$$

Clearly, one has $0 \le \varphi_{\delta}(x) \le \frac{x}{1-x}$, $\forall x \in [0, 1)$. Now, by Theorem 4, every point of the unbounded set $\{(a, b) | 0.5 \le a < 1; 0 \le b \le \frac{a}{1-a}\}$ belongs to at least one curve $y = \varphi_{\delta}(x)$, while some points of the bounded region $\{(a, b) | 0 \le a < 0.5; 0 \le b \le \frac{a}{1-a}\}$ may fail to lie on any such curve. An example of such a point is $(1/3, \lambda)$, where λ is a positive real number less than 0.5, whole ternary expansion contains a two.

ACKNOWLEDGMENT

I wish to express my thanks to Professor J. Denef for his help with the presentation of this paper. I am also indebted to R. D. Guido Smets for his help with the computing.

REFERENCE

1. J. L. Brown, Jr. "On Generalized Bases for Real Numbers." *The Fibonacci Quarterly* 9.5 (1971):477-96, 525.

AMS Classification Numbers: 11B83, 11A67

*** *** ***

P-LATIN MATRICES AND PASCAL'S TRIANGLE MODULO A PRIME

Valery V. Karachik

Institute of Cybernetics of Acad. Sci. of Uzbekistan, 34, F. Hodzhaev St., Tashkent, 700143, Uzbekistan (Submitted December 1994)

INTRODUCTION

One of the more effective methods of counting residues modulo a prime in the rows of Pascal's triangle is a reduction of this problem to that of solving of certain systems of recurrence equations. This way was successfully employed by B. A. Bondarenko [1] in the investigation of this problem for various values of p and (only) for certain rows of Pascal's triangle. However, some characteristic properties of the matrices of these recurrent systems were noticed which led to the idea of p-latin matrices. This idea was formulated in more detail in [2], which also uses p-latin matrices in the investigation of other arithmetic triangles.

In this paper we consider a new application of the properties of p-latin matrices to the investigation of Pascal's triangle modulo a prime. Using a representation of the p-latin matrices in a convenient basis, we obtain the distribution of Pascal's triangle elements modulo a prime for an arbitrary row.

p-LATIN MATRICES

We note the definition of a p-latin matrix as given in [1] and [2]. A square matrix of order n is called a "latin square of order n" [3] if its elements take on n values in such a way that each value occurs only once in each column and row. A latin square of order n is called a "p-latin square of order n" if no diagonals except the main and secondary ones (the element indices are i and n-i+1 for $1 \le i \le n$) have equal elements. A p-latin square of order n is said to be a "normalized p-latin square of order n" if its first row has the form (1, 2, ..., n), and the main diagonal has the form (1, ..., 1).

We will construct such a matrix for any prime p.

Let us introduce the matrix $P = (j/i)_{i, j=\overline{1, p-1}}$ of order p-1 whose elements are to be understood as elements from the field \mathbb{Z}_p . (Here and later we use the notation $i, j = \overline{1, p-1}$ to mean $1 \le i \le p-1, 1 \le j \le p-1$.)

Example 1: For p = 7, the matrix P has the form:

<i>P</i> =	(1/1)	2/1	3/1	4/1	5/1	6/1	1	(1)	2	3	4	5	6)	ſ
	1/2	2/2	3/2	4/2	5/2	6/2	=	4	1	5	2	6	3	
	1/3	2/3	3/3	4/3	5/3	6/3		5	3	1	6	4	2	
	1/4	2/4	3/4	4/4	5/4	6/4		2	4	6	1	3	5	ŀ
	1/5	2/5	3/5	4/5	5/5	6/5		3	6	2	5	1	4	
	(1/6)	2/6	3/6	4/6	5/6	6/6		6	5	4	3	2	1)	

Theorem 1: If p is a prime number, then the matrix P is a normalized p-latin square.

[AUG.

Proof: It is obvious that elements of P occurring in the same row or column are distinct and belong to the multiplicative group of the field \mathbb{Z}_p . Thus the matrix P is a latin square.

Let j/i be one element of some diagonal that is parallel to the main diagonal. Then any other element of this diagonal has the form (j+s)/(i+s). Assume that these elements are equal; then is = js and therefore i = j, so in this case the element j/i has to occur on the main diagonal. There is an analogous situation with diagonals parallel to the secondary one. Hence P is a p-latin square. Since the first row of P has the form 1, 2, ..., p-1 and on the main diagonal there are only 1's, P is a normalized p-latin square.

Let us define the set of square matrices of order p-1 (called in [2] "normalized p-latin matrices"):

$$\mathbb{N}_p = \left\{ \left(c_{p_{i,j}} \right)_{i, j=\overline{1, p-1}} \middle| c_1, \dots, c_{p-1} \in \mathbb{C}, (p_{i,j}) = P \right\},\$$

where \mathbb{C} denotes the complex numbers.

Example 2: If p = 7, then, according to Example 1, the matrix

$\begin{pmatrix} c_1 \end{pmatrix}$	c_2	c_3	c_4	c_5	c_6
c_4	c_1	c_5	c_2	c_6	c_3
C_5	c_3	c_1	c_6	C_4	c_2
$ c_2 $	c_4	c_6	c_1	c_3	c_5
c_3	c_6	c_2	c_5	c_1	<i>C</i> ₄
C_6	c_5	c_4	c_3	c_2	c_1

belongs to \mathbb{N}_7 .

Though the idea of this set of matrices was contained in [1] and [2], their existence for any p was not made explicit.

Corollary 1: If $C, B \in \mathbb{N}_p$, then $CB \in \mathbb{N}_p$ and CB = BC.

Proof: In fact, if $C = (c_{i,j})$ and $B = (b_{i,j})$, then the equality

$$CB = \left(\sum_{k=1}^{p-1} c_{k/i} b_{j/k}\right)_{i, j=\overline{1, p-1}} = \left(\sum_{s=1}^{p-1} c_s b_{j/(is)}\right)_{i, j=\overline{1, p-1}},$$

where all indices are in \mathbb{Z}_p , holds. Therefore, if we denote by a_k the sum $\sum_{s=1}^{p-1} c_s b_{k/s}$, then we will have $CB = (a_{j/i})_{i, j=\overline{1, p-1}}$; hence $CB \in \mathbb{N}_p$. Moreover, in the same way, we can establish

$$BC = \left(\sum_{s=1}^{p-1} b_s c_{js/i}\right)_{i, j=\overline{1, p-1}} = (a_{j/i})_{i, j=\overline{1, p-1}},$$

with the aid of the equality

$$a_k = \sum_{s=1}^{p-1} b_s c_{k/s}.$$

Hence CB = BC, which was to be proved.

We develop the properties of these matrices from \mathbb{N}_p in what follows.

Let us denote by $\Delta^{(1)}$ the Pascal triangle modulo a prime p and let C(n,m) be an arbitrary element. Let us also denote by $\Delta_s^{(1)}$ the triangle containing only the first s rows of $\Delta^{(1)}$. Now consider the triangle $\Delta^{(k)} \equiv k\Delta^{(1)}$, whose elements $C_k(n,m)$ are defined by the expression $C_k(n,m) = kC(n,m) \pmod{p}$ and denote by $\Delta_s^{(k)}$ the triangle containing only the first s rows of $\Delta^{(k)}$. It is clear that $\Delta_s^{(k)} = k\Delta_s^{(1)}$.

Definition: The triangle with *sm* rows arising from $\Delta_s^{(k)}$ by replacing its elements $C(n, \ell)$ by the triangles $\Delta_m^{(C(n,\ell))}$ and filling in free places by 0 is denoted by $\Delta_s^{(k)} * \Delta_m$.

Example 3: For p = 5, the triangles $\Delta_4^{(1)}$ and $\Delta_3^{(k)}$ have the form

$$\Delta_{4}^{(1)} = \frac{1}{1 \cdot 2 \cdot 1}, \quad \Delta_{3}^{(1)} = \frac{1}{1 \cdot 2 \cdot 1}, \quad \Delta_{3}^{(2)} = \frac{2}{2 \cdot 2}, \quad \Delta_{3}^{(3)} = \frac{3}{3 \cdot 3}, \quad \Delta_{4}^{(3)} = \frac{3}{3 \cdot 1}, \quad \Delta_{4}^{(2)} = \frac{2}{2 \cdot 4}, \quad \Delta_{4}^{(3)} = \frac{3}{3 \cdot 1}, \quad \Delta_{4}^$$

1

and therefore we obtain:

$$\Delta_{4}^{(1)} * \Delta_{3} \equiv \frac{\Delta_{3}^{(1)} \quad \Delta_{3}^{(1)}}{\Delta_{3}^{(1)} \quad \Delta_{3}^{(2)} \quad \Delta_{3}^{(1)}} = \frac{\begin{array}{c} 1 & 1 \\ 1 & 2 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 2 & 1 & 1 & 2 & 1 \\ 1 & 0 & 0 & 2 & 0 & 0 & 1 \\ 1 & 1 & 0 & 2 & 2 & 0 & 1 & 1 \\ 1 & 1 & 0 & 2 & 2 & 0 & 1 & 1 \\ 1 & 1 & 0 & 2 & 2 & 0 & 1 & 1 \\ 1 & 0 & 0 & 3 & 0 & 0 & 3 & 0 & 0 & 1 \\ 1 & 1 & 0 & 3 & 0 & 3 & 3 & 0 & 0 & 1 \\ 1 & 1 & 0 & 3 & 0 & 3 & 3 & 0 & 0 & 1 \\ 1 & 1 & 0 & 3 & 0 & 3 & 3 & 0 & 0 & 1 \\ 1 & 2 & 1 & 3 & 1 & 3 & 3 & 1 & 3 & 1 & 2 & 1 \end{array}$$

This leads to the principal fractal property of Pascal's triangle.

Theorem 2: For any $n, m \in \mathbb{N}$ and each $k = \overline{1, p-1}$, the equality $\Delta_m^{(k)} * \Delta_{p^n} = \Delta_{mp^n}^{(k)}$ holds. The proof of this theorem is lengthy but not difficult and is given in [4].

This result allows us to reduce an investigation of $\Delta^{(1)}$ to the investigation of $\Delta_p^{(k)}$ for $k = \overline{1, p-1}$. The details will be given in Theorem 3.

Let $B_k, 1 \le k \le p-1$, be the matrix of order p-1, any element $b_{i,j}$ of which is the number of elements equal to j in the k^{th} row of the triangle $\Delta_p^{(i)}$. Denote by $g_s^{(k)}(n, p)$ the number of elements equal to s modulo p in the n^{th} row of the triangle $\Delta_p^{(k)}$.

Theorem 3: If $n = (a_r, ..., a_0)_p$ is the *p*-ary representation of *n*, then

$$g_s^{(k)}(n, p) = (B_{a_r} \dots B_{a_0})_{k,s}.$$
 (1)

364

AUG.

Proof: Using Theorem 2, we can write the equality

$$\Delta_{p^{r+1}}^{(1)} = \Delta_p^{(1)} * \Delta_{p^r}$$

which means that the n^{th} row of $\Delta_{p^{r+1}}^{(1)}$ is found in the a_r^{th} row of $\Delta_p^{(1)}$, which consists of the triangles $\Delta_{p^r}^{(k)}$, $1 \le k \le p-1$ (see Example 3). If we set $n_{(k)} \equiv (a_{r-k}, ..., a_0)$, then the following vector equality will hold:

$$(g_s^{(k)}(n, p))_{k=\overline{1, p-1}} = B_{a_r}(g_s^{(k)}(n_{(1)}, p))_{k=\overline{1, p-1}}.$$

Continuing this process, we can obtain

$$(g_s^{(k)}(n, p))_{k=\overline{1, p-1}} = B_{a_r} \dots B_{a_i}(g_s^{(k)}(n_{(r)}, p))_{k=\overline{1, p-1}}$$

Since $n_{(r)} = a_0$ and $g_s^{(k)}(a_0, p) = (B_{a_0})_{s,k}$, we get (1). This completes the proof.

Using Theorem 3, we can reduce counting the $g_s^{(1)}(n, p)$, where $s = \overline{1, p-1}$, to finding a product of the matrices B_k .

Theorem 4: $B_k \in \mathbb{N}_p$.

Proof: Let $b_1^{(k)}, \ldots, b_{p-1}^{(k)}$ be the elements of the first row of B_k . We will prove the equality

$$B_{k} = \left(b_{p_{i,j}}^{(k)}\right)_{i, \ j = \overline{1, \ p-1}}.$$
(2)

We can define the addition of the triangles $\Delta_p^{(k)}$ as the same operation between corresponding elements of $\Delta_p^{(k)}$ in \mathbb{Z}_p . For example, the following equality

$$\sum_{k=1}^{s} \Delta_{p}^{(1)} = \Delta_{p}^{(s)}$$
(3)

holds. If we denote the elements of matrix B_k by $b_{i,j}^{(k)}$, then, using (3) and the definition of $b_{i,j}^{(k)}$, we can write $b_{l,j}^{(k)} = b_{s,js}^{(k)}$ for each $s = \overline{1, p-1}$. Thus, $b_{i,j}^{(k)} = b_{l,j/i}^{(k)}$, and hence (2) holds. The proof is complete.

Let n_i be the number of elements equal to *i* in the *p*-ary representation of *n* in the form $n = (a_r, ..., a_0)_p$. By (1), using Corollary 1, we can find

$$g_{s}^{(k)}(n,p) = \left(\prod_{i=1}^{p-1} B_{i}^{n_{i}}\right)_{k,s}.$$
(4)

Here the matrix B_0 is absent because $B_0 = \text{diag}(1, ..., 1) \equiv E$. Now, to calculate the value of $g_s^{(k)}(n, p)$, we have to investigate the further properties of the matrices in \mathbb{N}_p .

PROPERTIES OF THE MATRICES FROM N_n

It is true that \mathbb{N}_p is just a subspace of the linear space of square matrices of order p-1. Moreover, we have

Corollary 2: $\text{Dim} \mathbb{N}_p = p - 1$ and

$$B \in \mathbb{N}_p \Longrightarrow B = \sum_{k=1}^{p-1} b_k I_k, \tag{5}$$

where $I_k \in \mathbb{N}_p$ and $I_k = (\delta_{ki, j})_{i, j = \overline{1, p-1}}$.

Here $\delta_{i,j}$ is Kronecker's symbol and all indices are to be understood as elements from \mathbb{Z}_p . Proof of this property can be obtained directly from the definition of \mathbb{N}_p .

Let us verify that the matrices I_k possess the property $I_k I_m = I_{km}$. In fact

$$I_k I_m = \left(\sum_{s=1}^{p-1} \delta_{ki,s} \,\delta_{ms,j}\right)_{i, j=\overline{1, p-1}},$$

and consequently the element of the matrix $I_k I_m$ with the indices *i* and *j* does not vanish if there exists an *s* so that ki = s and ms = j. Hence j = mki, and therefore $I_k I_m = (\delta_{mki,j})_{i, j=\overline{1, p-1}} = I_{km}$.

Let v be the root of the equation $x^{p-1} = 1$ in the field \mathbb{Z}_p , such that for each $k = \overline{1, p-2}$ the inequality $v^k \neq 1$ holds. For what follows, it will be convenient to introduce the matrices $J_k = (I_v)^k$. If we set $c_k = b_{v^k}$, then (5) can be written in the form

$$B = \sum_{k=1}^{p-1} c_k J_k \,. \tag{6}$$

Corollary 3: If μ is an eigenvalue of B, then there is a root of the equation $z^{p-1} = 1$ in \mathbb{C} , which we denote as λ , such that

İ

$$\mu = \sum_{k=1}^{p-1} c_k \lambda^k \,. \tag{7}$$

Proof: Let *a* be some vector from \mathbb{C}^{p-1} and

$$b=\sum_{k=1}^{p-1}\lambda^{-k}J_ka.$$

Then, employing the equality $J_s b = \lambda^s b$ and carrying this out for each s = 1, p-1, we can write

$$Bb = \sum_{k=1}^{p-1} c_k J_k b = \sum_{k=1}^{p-1} c_k \lambda^k b = \mu b,$$

i.e., μ is an eigenvalue of *B*. Now it remains to prove that formula (7) gives us all eigenvalues of *B*. We will complete this after Corollary 6.

As a consequence of Corollary 3, we note that the matrices I_k , and hence the matrices J_k , are nonsingular matrices, and $\forall k$, det $I_k = \det J_k = 1$. Indeed, since all eigenvalues of J_k are the roots of the equation $x^{p-1} = 1$ (we denote them by λ_i), then we have

$$\det J_k = \prod_{i=1}^{p-1} \lambda_i^k = \mu^k,$$

where $\mu = \lambda_1 \dots \lambda_{p-1}$. Using the equality $\sum_{k=1}^{p-1} k = 0 \pmod{p}$, we get $\mu = 1$, and hence det $J_k = 1$.

366

AUG.

As another interesting property of the matrices I_k we note that they are orthogonal matrices, namely, $I_k I_k^* = E$, where $(a_{i,j})^* = (\overline{a}_{j,i})$ and the bar denotes complex conjugation. This immediately follows from the equality

$$I_k^* = \left(\delta_{i,jk}\right)_{i,j=\overline{1,p-1}} = I_{1/k}$$

Obviously, the matrices J_k possess the same property, but by the equality $J_k J_s = J_{k+s}$ we have

$$J_k^* = J_k^{-1} = J_{p-k-1} \tag{8}$$

for each $k = \overline{1, p-2}$. Since $J_{p-1} = E$, we have $J_{p-1}^* = J_{p-1}$.

Corollary 4: Let B be in \mathbb{N}_p and be written in the form (6), then

$$B^* = \sum_{k=1}^{p-2} \overline{c}_{p-k-1} J_k + \overline{c}_{p-1} J_{p-1} .$$

Proof: In fact, using (8), we immediately obtain

$$B^* = \sum_{k=1}^{p-2} \overline{c}_k J_k^* + \overline{c}_{p-1} J_{p-1}^* = \sum_{k=1}^{p-2} \overline{c}_k J_{p-k-1} + \overline{c}_{p-1} J_{p-1};$$

hence Corollary 4 is true.

Let us introduce the matrices S_i for $i = \overline{1, p-1}$ in the form

$$S_i = \frac{1}{(p-1)} \sum_{k=1}^{p-1} \lambda_i^{-k} J_k \,. \tag{9}$$

Here, as before, λ_i is one of the roots of the equation $x^{p-1} = 1$ in \mathbb{C} . It is clear that, for each $i = \overline{1, p-1}$, the matrices S_i belong to \mathbb{N}_p .

Let λ be a primitive root of the equation $x^{p-1} = 1$, i.e., for each $k = \overline{1, p-2}$, we have $\lambda^k \neq 1$. Therefore, in formula (9), we can assume that $\lambda_i = \lambda^i$.

Theorem 5: The following equalities,

$$S_i S_j = \delta_{i,j} S_i \tag{10}$$

are true for all $i, j = \overline{1, p-1}$.

Proof: Consider the left-hand side of (10). After some calculation, we get

$$S_i S_j = \frac{1}{(p-1)^2} \left[\sum_{\ell=0}^{p-2} \lambda_j^{-\ell} J_\ell \sum_{k=0}^{\ell} \lambda_{i-j}^{-k} + \sum_{\ell=p-1}^{2(p-2)} \lambda_j^{-\ell} J_\ell \sum_{k=\ell-p+2}^{p-2} \lambda_{i-j}^{-k} \right],$$

whence

$$S_i S_j = \frac{1}{(p-1)^2} \left[\sum_{\ell=0}^{p-2} \lambda_j^{-\ell} J_\ell \sum_{k=0}^{\ell} \lambda_{i-j}^{-k} + \sum_{\ell=0}^{p-3} \lambda_j^{-\ell} J_\ell \sum_{k=\ell+1}^{p-2} \lambda_{i-j}^{-k} \right];$$

hence

$$S_i S_j = \frac{1}{(p-1)^2} \sum_{\ell=0}^{p-2} \lambda_j^{-\ell} J_\ell \sum_{k=0}^{p-2} \lambda_{i-j}^{-k} .$$

Let us examine this equality. Employing the identity $\lambda_{i-j} = \lambda_i / \lambda_j$, where $\lambda_i \neq \lambda_j$ (for $i \neq j$), we obtain

$$\sum_{k=0}^{p-2} \lambda_{i-j}^{-k} = (\lambda_{i-j}^{1-p} - 1) / (\lambda_{i-j}^{-1} - 1) = 0.$$

Hence (10) holds for $i \neq j$. Further, at i = j, we have

$$\sum_{k=0}^{p-2} \lambda_{i-j}^{-k} = p - 1;$$
(11)

consequently, $S_i^2 = S_i$, and the proof is complete.

The matrices S_i are Hermitian, i.e., they possess the property $S_i = S_i^*$. In fact, for $i = \overline{1, p-1}$, we have

$$S_i^* = \frac{1}{(p-1)} \sum_{k=1}^{p-1} \lambda_i^k J_k^* = \frac{1}{(p-1)} \sum_{k=1}^{p-1} \lambda_i^{k-p+1} J_{p-k-1} = S_i$$

Let us denote the transposed matrix $A = (a_{i,j})_{i,j=\overline{1,p-1}}$ by $A' = (a_{j,i})_{i,j=\overline{1,p-1}}$. Then we have $S'_i = S_{p-i-1}$ for $i = \overline{1, p-2}$. This can be proved in the same way as the previous result, but we need to keep in mind that $J_k^* = J_k'$ and $\overline{\lambda}_i = \lambda_{p-i-1}$.

Theorem 6: The equalities

$$J_{k} = \sum_{i=1}^{p-1} \lambda_{i}^{k} S_{i}, \ k = \overline{1, p-1},$$
(12)

which are converse to (9), are true.

Proof: Employing (9)-(11) and making some transformations, we get

$$\sum_{i=1}^{p-1} \lambda_i S_i = \sum_{k=1}^{p-1} \left\lfloor \frac{1}{(p-1)} \sum_{i=1}^{p-1} \lambda_i^{1-k} \right\rfloor J_k = \sum_{k=1}^{p-1} \delta_{k,1} J_k.$$

Therefore, (12) is true for k = 1. For the completion of the proof, it suffices to note that $J_k = J_1^k$ and to make use of (10).

Now we must note that the matrix S_{p-1} consists only of 1's in each place; hence $S'_{p-1} = S_{p-1}$. This is clear from the following equalities,

$$S_{p-1} = \sum_{k=1}^{p-1} J_k = \sum_{k=1}^{p-1} I_k = \left(\sum_{k=1}^{p-1} \delta_{ki,j} J_k\right)_{i,j=\overline{1,p-1}}$$

if we bear in mind that, for $i, j = \overline{1, p-1}, \sum_{k=1}^{p-1} \delta_{ki,j} = 1$.

Corollary 5: Let $B \in \mathbb{N}_p$, then

$$B = \sum_{i=1}^{p-1} \mu_i S_i, \text{ where } \mu_i \text{ are the eigenvalues of } B.$$
(13)

AUG.

The proof of this Corollary can be obtained without difficulty from (6) by using Theorem 6 and equality (7).

Using the basis $S_1, ..., S_{p-1}$, we can easily find the product of matrices from \mathbb{N}_p . To illustrate this statement we prove

Theorem 7: Let $\mu_1^{(i)}, \dots, \mu_{p-1}^{(i)}$ be the eigenvalues of the matrices B_i from Theorem 3. If we set

$$\sigma_j = \prod_{i=1}^{p-1} (\mu_j^{(i)})^{n_i}, \tag{14}$$

then the equality

$$g_s^{(k)}(n,p) = \left(\sum_{i=1}^{p-1} \sigma_i S_i\right)_{k,s}$$
(15)

is true.

Proof: It is readily seen that, making use of (13) and Theorem 5, we can obtain

$$B_i^{n_i} = \sum_{j=1}^{p-1} (\mu_j^{(i)}) > S_j$$

Therefore, equality (4) transforms to (15), and the proof is complete.

Note that we can also write σ_i in the form $\sigma_i = \mu_i^{(a_r)} \dots \mu_i^{(a_0)}$.

Corollary 6: Any eigenvector b_i of the matrix B corresponding to the eigenvalue μ_i can be written in the form

$$b_i = \sum_{(j)} S_j c_j, \tag{16}$$

where $c_j \in \mathbb{C}^{p-1}$ and the summation is taken over *j* satisfying the condition $\mu_j = \mu_i$.

Proof: Let b_i be the eigenvector of the matrix *B* corresponding to the eigenvalue μ_i . Operating on the equality $Bb_i = \mu_i b_i$ by the matrix S_s , using (13) and Theorem 5, we obtain $\mu_s S_s b_i = \mu_i S_s b_i$. If $\mu_i \neq \mu_s$ here, then $S_s b_i = 0$. Now, if we make use of the identity $E = S_1 + \dots + S_{p-1}$, which easily follows from Corollary 5 for B = E, then we get $b_i = (\sum_{(i)} S_i) b_i$.

In addition, if $c \in \mathbb{C}^{p-1}$, then, using the equality $BS_i c = \mu_i S_i c$, we can say that the vectors of the form $S_i c$ are the eigenvectors corresponding to the eigenvalue μ_i . Thus (16) is true, and the proof is complete.

Conclusion of the Proof of Corollary 3: Let us take $c \in \mathbb{C}^{p-1}$ so that $\forall k, S_k c \neq 0$. This is possible, for example, with c = (1, 0, ..., 0). We saw above that the vector $c_k = S_k c$ is the eigenvector of the matrix *B* corresponding to the eigenvalue μ_k determined from (7) at $\lambda = \lambda_k$. We claim that the vectors c_k ($k = \overline{1, p-1}$) are linearly independent. In fact, if there are $\delta_1, ..., \delta_{p-1} \in \mathbb{C}$ not all zero and such that $\delta_1 c_1 + \cdots + \delta_{p-1} c_{p-1} = 0$, then operating on this equality by S_k , we obtain $\delta_k c_k = 0$ or $\delta_k = 0$ for $k = \overline{1, p-1}$, which is a contradiction. Thus, the vectors c_k for $k = \overline{1, p-1}$ are the basis in \mathbb{C}^{p-1} , and so there are no other eigenvalues of *B*. Thus, the proof is complete.

Corollary 7: If $\mu_i \neq 0$ for each $i = \overline{1, p-1}$, then the matrix B has an inverse defined by the equality

$$B^{-1} = \sum_{i=1}^{p-1} \mu_i^{-1} S_i \; .$$

To prove this statement, it is sufficient to use the identity $E = S_1 + \dots + S_{p-1}$ again, and to employ Theorem 5.

Now we apply the properties obtained of the matrices from \mathbb{N}_p to counting $g_s^{(k)}(n, p)$ for p = 7. It should be pointed out that in [5] this problem was considered for p = 3 and p = 5.

COUNTING $g_s^{(k)}(n,7)$

To count the value of $g_s^{(k)}(n, p)$ we need, according to Theorem 7, to examine the triangles $\Delta_7^{(k)}$ for $k = \overline{1, 6}$. The triangle $\Delta_7^{(1)}$ has the form:

$1 \\ 1 \\ 1 \\ 1$	
121	
1331	
14641	
153351	
61616	1

If we multiply each element of $\Delta_7^{(1)}$ by k in \mathbb{Z}_p , we will obtain the triangle $\Delta_7^{(k)}$. For example, $\Delta_7^{(3)}$ has the form:

3	
33	
3 6 3	
3223	
35453	
3 1 2 2 1 3	
3 4 3 4 3 4	3

Now we need to find the matrices B_k for $k = \overline{1, 6}$. Let us take, for instance, the 4th rows of triangles $\Delta_7^{(k)}$, which give us the matrix B_4 . The 4th row of triangle $\Delta_7^{(1)}$ has the form (1, 4, 6, 4, 1). Since the numbers 1 and 4 occur twice and the number 6 occurs once there, the first row of B_4 has the form (2, 0, 0, 2, 0, 1). If we want to count the third row of B_4 now, we must take the 4th row of triangle $\Delta_7^{(3)}$, which gives us what we desire, i.e., (0, 0, 2, 1, 2, 0). Thus, we can count all the matrices B_k for $k = \overline{1, 6}$. To write our calculation, we make use of the matrices J_k ($k = \overline{1, 6}$). So let us find the matrix J_1 . In our case, we have $\nu = 3$ because, for each $k = \overline{1, 5}$, the inequality $3^k \neq 1 \pmod{7}$ is correct. Therefore,

$$J_1 = I_3 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

[AUG.

Now we can write

$$\begin{array}{ll} B_0=J_6, & B_1=2J_6, & B_2=J_2+2J_6, & B_3=2J_1+2J_6, \\ B_4=J_3+2J_4+2J_6, & B_5=2J_1+2J_5+2J_6, & B_6=3J_3+4J_6. \end{array}$$

Let us assume that the number k is contained in the record of $(n)_7$ a total of n_k times. Using the notation of Theorem 7 and formulas (6) and (7), and keeping in mind that $\lambda_k = \exp(ik\pi/3)$ (here, $i^2 = -1$), we obtain, for each $k = \overline{1, 6}$,

$$\mu_k^{(1)} = 2, \quad \mu_k^{(2)} = \lambda_k^2 + 2, \quad \mu_k^{(3)} = 2\lambda_k + 2, \quad \mu_k^{(4)} = \lambda_k^3 + 2\lambda_k^4 + 2,$$

$$\mu_k^{(5)} = 2(\lambda_k + \lambda_k^5 + 1), \quad \mu_k^{(6)} = 3\lambda_k^3 + 4.$$

Whence, by (14),

$$\sigma_{1} = 2^{n_{1}-n_{2}} (3+i\sqrt{3})^{n_{2}+n_{3}} (-i\sqrt{3})^{n_{4}} 4^{n_{5}},$$

$$\sigma_{2} = 2^{n_{1}-n_{2}} (3-i\sqrt{3})^{n_{2}} (1+i\sqrt{3})^{n_{3}} (2+i\sqrt{3})^{n_{4}} (2\lambda_{2}+2\lambda_{4}+2)^{n_{5}} 7^{n_{6}},$$

$$\sigma_{3} = (-1)^{n_{5}} 2^{n_{1}+n_{5}} 3^{n_{2}+n_{4}} (2\lambda_{3}+2)^{n_{3}}, \quad \sigma_{6} = 2^{n_{1}} 3^{n_{2}} 4^{n_{3}} 5^{n_{4}} 6^{n_{5}} 7^{n_{6}},$$

$$\sigma_{4} = \overline{\sigma}_{2}, \quad \sigma_{5} = \overline{\sigma}_{1},$$

$$(17)$$

where the bar denotes the complex conjugate. To make use of (15), we need the matrices S_k $(k = \overline{1, 6})$. According to (9), the matrices S_1 and S_2 have the form

$$S_{1} = \frac{1}{6} \begin{pmatrix} 1 & \overline{\lambda}_{2} & \overline{\lambda}_{1} & \underline{\lambda}_{2} & \lambda_{1} & -1 \\ \lambda_{2} & 1 & \lambda_{1} & \overline{\lambda}_{2} & -1 & \overline{\lambda}_{1} \\ \lambda_{1} & \overline{\lambda}_{1} & 1 & -1 & \underline{\lambda}_{2} & \overline{\lambda}_{2} \\ \overline{\lambda}_{2} & \lambda_{2} & -1 & 1 & \overline{\lambda}_{1} & \lambda_{1} \\ \overline{\lambda}_{1} & -1 & \overline{\lambda}_{2} & \underline{\lambda}_{1} & 1 & \lambda_{2} \\ -1 & \lambda_{1} & \lambda_{2} & \overline{\lambda}_{1} & \overline{\lambda}_{2} & 1 \end{pmatrix}, \qquad S_{2} = \frac{1}{6} \begin{pmatrix} 1 & \lambda_{2} & \overline{\lambda}_{2} & \overline{\lambda}_{2} & \lambda_{2} & 1 \\ \overline{\lambda}_{2} & 1 & \lambda_{2} & \lambda_{2} & 1 & \overline{\lambda}_{2} \\ \lambda_{2} & \overline{\lambda}_{2} & 1 & 1 & \overline{\lambda}_{2} & \lambda_{2} \\ \lambda_{2} & \overline{\lambda}_{2} & 1 & 1 & \overline{\lambda}_{2} & \lambda_{2} \\ \overline{\lambda}_{2} & 1 & \lambda_{2} & \overline{\lambda}_{2} & 1 & \overline{\lambda}_{2} \\ 1 & \lambda_{2} & \overline{\lambda}_{2} & \overline{\lambda}_{2} & 1 & 2 \end{pmatrix}.$$

If we denote the k^{th} row of S_3 by $(S_3)_k$, then we have

$$(S_3)_1 = (S_3)_2 = -(S_3)_3 = (S_3)_4 = -(S_3)_5 = -(S_3)_6$$

= 1/6(1,1,-1,1,-1,-1).

Also, from the general properties of S_j , we find $S_4 = S'_2$, $S_5 = S'_1$, $S_6 = (1)_{i,j=\overline{1,6}}$. Now, from (15), keeping in mind (17), we can obtain what we required, i.e.,

$$g_{1}^{(1)}(n,7) = 1/6[2 \operatorname{Re}(\sigma_{1} + \sigma_{2}) + \sigma_{3} + \sigma_{6}],$$

$$g_{2}^{(1)}(n,7) = 1/6[2 \operatorname{Re}(\lambda_{4}\sigma_{1} + \lambda_{2}\sigma_{2}) + \sigma_{3} + \sigma_{6}],$$

$$g_{3}^{(1)}(n,7) = 1/6[2 \operatorname{Re}(\lambda_{5}\sigma_{1} + \lambda_{4}\sigma_{2}) - \sigma_{3} + \sigma_{6}],$$

$$g_{4}^{(1)}(n,7) = 1/6[2 \operatorname{Re}(\lambda_{2}\sigma_{1} + \lambda_{4}\sigma_{2}) + \sigma_{3} + \sigma_{6}],$$

$$g_{5}^{(1)}(n,7) = 1/6[2 \operatorname{Re}(\lambda_{1}\sigma_{1} + \lambda_{2}\sigma_{2}) - \sigma_{3} + \sigma_{6}],$$

$$g_{6}^{(1)}(n,7) = 1/6[2 \operatorname{Re}(-\sigma_{1} + \sigma_{2}) - \sigma_{3} + \sigma_{6}].$$
(18)

P-LATIN MATRICES AND PASCAL'S TRIANGLE MODULO A PRIME

Since $2\lambda_2 + 2\lambda_4 + 2 = 0$ and $2\lambda_3 + 2 = 0$, we know the equalities obtained are true only if $n_3 = n_5 = 0$. When $n_3 \neq 0$ and $n_5 = 0$, we must assume that $\sigma_3 = 0$ in (18), but when $n_5 \neq 0$ and $n_3 = 0$, we must assume that $\sigma_2 = 0$. Finally, if $n_3 \neq 0$ and $n_5 \neq 0$, then $\sigma_2 = \sigma_3 = 0$. In all other cases except those indicated above, we must make use of (17).

CONCLUSION

We note here two simple properties of $g_s^{(k)}(n, p)$. Consider two rows of Pascal's triangle with numbers $(n)_p$ and $(m)_p$. First, if $(n)_p$ and $(m)_p$ contain the same figures excepting zero, then $g_s^{(k)}(n, p) = g_s^{(k)}(m, p)$ for each k and s. Second, if $(n)_p$ contains 1 ℓ more than $(m)_p$, then $g_s^{(k)}(n, p) = 2^{\ell} g_s^{(k)}(m, p)$ for each k and s. The latter follows from (4) because $B_1 = 2E$ for each $\Delta_p^{(1)}$.

ACKNOWLEDGMENT

I wish to thank Professor Boris Bondarenko for his interest and helpful criticism and the anonymous referee for many valuable comments.

REFERENCES

- 1. B. A. Bondarenko. *Generalized Pascal Triangles and Pyramids: Their Fractals, Graphs and Applications* (trans. from Russian; ed. R. C. Bollinger). Santa Clara, Calif.: The Fibonacci Association, 1993.
- 2. B. A. Bondarenko. "Normalizovannye *p*-latinskie kvadraty i algorithmy ih primenenija k zada-cham raspredelenija elementov po modulju *p* v ariphmeticheskih strukturah." *Voprosy vichislitelnoj i priklandnoj matematiki* 91 (1991):61-80. (Tashkent, RISO AN RUz.)
- 3. J. Dénes & A. D. Keedwell. *Latin Squares and Their Applications*. Budapest: Akad. Kiadó, 1974.
- 4. V. V. Karachik. "O nekotorhy svojstvah *p*-latinskih matriz i ih primenenii." *Voprosy vichislitelnoj i prikladnoj matematiki* 95 (1993):49-60. (Tashkent, RISO AN RUz.)
- 5. E. Hexel & H. Sachs. "Counting Residues Modulo a Prime in Pascal's Triangle." *Indian J Math.* 20.2 (1978):91-105.

AMS Classification Numbers: 11B65, 11B50, 11C20

** ** **

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. Although this Elementary Problem section does not insist on original problems, we do ask that proposers 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

$$\begin{split} F_{n+2} &= F_{n+1} + F_n, \ F_0 = 0, \ F_1 = 1; \\ L_{n+2} &= L_{n+1} + L_n, \ L_0 = 2, \ L_1 = 1. \end{split}$$

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-814 Proposed by M. N. Deshpande, Institute of Science, Nagpur, India

Show that for each positive integer *n*, there exists a constant C_n such that $F_{2n+2i}F_{2i} - C_n$ and $F_{2n+2i+1}F_{2i+1} - C_n$ are both perfect squares for all positive integers *i*.

B-815 Proposed by Paul S. Bruckman, Highwood, IL

Let $K(a, b, c) = a^3 + b^3 + c^3 - 3abc$. Show that if x_1, x_2, x_3, y_1, y_2 , and y_3 are integers, then there exist integers z_1, z_2 , and z_3 such that

$$K(x_1, x_2, x_3) \cdot K(y_1, y_2, y_3) = K(z_1, z_2, z_3)$$

B-816 Proposed by Mohammad K. Azarian, University of Evansville, Evansville, IN

Let *i*, *j*, and *k* be any three positive integers. Show that

$$\frac{F_j F_k}{F_i + F_i F_j F_k} + \frac{F_k F_i}{F_j + F_i F_j F_k} + \frac{F_i F_j}{F_k + F_i F_j F_k} < 2.$$

B-817 Proposed by Kung-Wei Yang, Western Michigan University, Kalamazoo, MI Show that

$$\sqrt[k]{\sum_{i=0}^{k} \binom{k}{i} F_{ni-1}F_{n(k-i)+1} - \sum_{j=1}^{k-1} \binom{k}{j} F_{nj}F_{n(k-j)}}$$

is an integer for all positive integers k and n.

B-818 Proposed by L. C. Hsu, Dalian University of Technology, Dalian, China

Let $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$. Find a closed form for

$$\sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} H_{2k}.$$

<u>B-819</u> Proposed by David Zeitlin, Minneapolis, MN

Find integers a, b, c, and d (with 1 < a < b < c < d) that make the following an identity:

$$P_n = P_{n-a} + 444P_{n-b} + P_{n-c} + P_{n-d},$$

where P_n is the Pell sequence, defined by $P_{n+2} = 2P_{n+1} + P_n$, for $n \ge 0$, with $P_0 = 0$, $P_1 = 1$.

NOTE: The Elementary Problems Column is in need of more *easy*, yet elegant and nonroutine problems.

SOLUTIONS

Generalizing a Pell Congruence

<u>B-787</u> Proposed by H.-J. Seiffert, Berlin, Germany (Vol. 33, no. 2, May 1995)

For $n \ge 0$ and k > 0, it is known that F_{kn} / F_k and P_{kn} / P_k are integers. Show that these two integers are congruent modulo $R_k - L_k$.

[Note: P_n and $R_n = 2Q_n$ are the Pell and Pell-Lucas numbers, respectively, defined by $P_{n+2} = 2P_{n+1} + P_n$, $P_0 = 0$, $P_1 = 1$ and $Q_{n+2} = 2Q_{n+1} + Q_n$, $Q_0 = 1$, $Q_1 = 1$.]

Solution by Lawrence Somer, Catholic University of America, Washington, DC

We will prove the following more general result. Let $\langle A_n \rangle_{n=0}^{\infty}$ and $\langle C_n \rangle_{n=0}^{\infty}$ denote two secondorder linear recurrences satisfying the respective recursion relations

$$A_{n+2} = aA_{n+1} - bA_n, \qquad A_0 = 0, \quad A_1 = 1,$$

$$C_{n+2} = cC_{n+1} - bC_n, \qquad C_0 = 0, \quad C_1 = 1,$$

where a, b, and c are nonzero integers. We assume that $\langle A_n \rangle$ and $\langle C_n \rangle$ are both nondegenerate second-order linear recurrences with $A_n \neq 0$ and $C_n \neq 0$ for any $n \ge 1$.

Let $\langle B_n \rangle$ be a sequence satisfying the same recursion relation as $\langle A_n \rangle$ but having initial terms $B_0 = 2$ and $B_1 = a$. Let $\langle D_n \rangle$ be a sequence satisfying the same recursion relation as $\langle C_n \rangle$ but having initial terms $C_0 = 2$ and $C_1 = c$. Then, for $n \ge 0$ and k > 0, we have that A_{kn} / A_k and C_{kn} / C_k are integers and

$$A_{kn} / A_k \equiv C_{kn} / C_k \pmod{B_k - D_k}.$$
(1)

Proof: We first note that it is well known that A_{kn} / A_k and C_{kn} / C_k are integers, since $A_k C_k \neq 0$. It was proven ([1], p. 437) that, for a fixed $k \ge 1$, both $\langle A_{kn} / A_k \rangle_{n=0}^{\infty}$ and $\langle C_{kn} / C_k \rangle_{n=0}^{\infty}$ are second-order linear recurrences satisfying the recursion relations

$$r_{n+2} = B_k r_{n+1} - b^k r_n \tag{2}$$

and

$$s_{n+2} = D_k s_{n+1} - b^k s_n, (3)$$

374

AUG.

respectively. To establish our result, it suffices to show that (1) holds for k fixed and n varying over the nonnegative integers. We proceed by induction:

$$A_{k \cdot 0} / A_k = 0 \equiv C_{k \cdot 0} / C_k = 0 \pmod{B_k - D_k};$$

$$A_{k \cdot 1} / A_k = 1 \equiv C_{k \cdot 1} / C_k = 1 \pmod{B_k - D_k}.$$

Assume the result holds up to n. By (2) and (3),

$$A_{k(n+1)} / A_k = B_k A_{kn} / A_k - b^k A_{k(n-1)} / A_k$$
(4)

and

$$C_{k(n+1)} / C_k = D_k C_{kn} / C_k - b^k C_{k(n-1)} / C_k.$$
⁽⁵⁾

Clearly $B_k \equiv D_k \pmod{B_k - D_k}$. Moreover, by our induction hypothesis, $A_{kn} / A_k \equiv C_{kn} / C_k$ and $A_{k(n-1)} / A_k \equiv C_{k(n-1)} / C_k \pmod{B_k - D_k}$. It now follows from (4) and (5) that $A_{k(n+1)} / A_k \equiv C_{k(n+1)} / C_k \pmod{B_k - D_k}$. The result now follows by induction.

If a = 2, b = -1, and c = 1, we get the original problem.

Reference

1. D. H. Lehmer. "An Extended Theory of Lucas' Functions." Annals of Mathematics (2) 31 (1930):419-48.

Also solved by Paul S. Bruckman, Andrej Dujella, Pentti Haukkanen, Norbert Jensen, Dorka O. Popova, Tony Shannon, and the proposer.

Asymptotic Analysis

B-788 Proposed by Russell Jay Hendel, University of Louisville, Louisville, KY (Vol. 33, no. 2, May 1995)

- (a) Let $G_n = F_{n^2}$. Prove that $G_{n+1} \sim L_{2n+1}G_n$.
- (b) Find the error term. More specifically, find a constant C such that $G_{n+1} \sim L_{2n+1}G_n + CG_{n-1}$.

Solution by H.-J. Seiffert, Berlin, Germany

We shall prove that, for all positive integers n, $G_{n+1} = L_{2n+1}G_n + \beta^2 G_{n-1} - \beta^{(n-1)^2}$. Since $\lim_{n\to\infty} \beta^{(n-1)^2} = 0$, this is much more than is asked for in the proposal. In particular, the constant of part (b) is $C = \beta^2 = (3 - \sqrt{5})/2$.

Using the Binet formulas, we obtain

$$\begin{split} \sqrt{5}(G_{n+1} - L_{2n+1}G_n - \beta^2 G_{n-1}) &= \sqrt{5} \Big(F_{(n+1)^2} - L_{2n+1}F_{n^2} - \beta^2 F_{(n-1)^2} \Big) \\ &= \alpha^{(n+1)^2} - \beta^{(n+1)^2} - (\alpha^{2n+1} + \beta^{2n+1})(\alpha^{n^2} - \beta^{n^2}) \\ &- \beta^2 \big(\alpha^{(n-1)^2} - \beta^{(n-1)^2} \big) \\ &= \alpha^{2n+1}\beta^{n^2} - \beta^{2n+1}\alpha^{n^2} - \beta^2 \alpha^{(n-1)^2} + \beta^2 \beta^{(n-1)^2} \\ &= -\beta^{n^2 - 2n - 1} + \alpha^{n^2 - 2n - 1} - \alpha^{(n-1)^2 - 2} + \beta^2 \beta^{(n-1)^2} \\ &= \beta^{(n-1)^2} \big(\beta^2 - 1/\beta^2 \big) = -\sqrt{5}\beta^{(n-1)^2}, \end{split}$$

where we have used that $\alpha\beta = -1$. This proves the desired equation.

Also solved by Paul S. Bruckman, Andrej Dujella, Russell Jay Hendel, Norbert Jensen, Can. A. Minh, Tony Shannon, and the proposer.

Differential Equation Involving Lucas Polynomials

<u>B-789</u> Proposed by Richard André-Jeannin, Longwy, France (Vol. 33, no. 2, May 1995)

The Lucas polynomials, $L_n(x)$, are defined by $L_0 = 2$, $L_1 = x$, and $L_n = xL_{n-1} + L_{n-2}$, for $n \ge 2$.

Find a differential equation satisfied by $L_n^{(k)}$, the k^{th} derivative of $L_n(x)$, where k is a non-negative integer.

Solution by Andrej Dujella, University of Zagreb, Croatia

The Binet form for $L_n(x)$ is

$$L_n(x) = \left(\frac{x + \sqrt{x^2 + 4}}{2}\right)^n + \left(\frac{x - \sqrt{x^2 + 4}}{2}\right)^n.$$

Take the derivative of both sides to get $L'_n(x) = nF_n(x)$.

Combining this with the relation $L_n^2(x) - (x^2 + 4)F_n^2(x) = 4(-1)^n$, we get the differential equation for $L_n(x)$:

$$(x^{2}+4)L_{n}''(x)+xL_{n}'-n^{2}L_{n}(x)=0.$$

Taking the derivative k times gives $(x^2 + 4)L_n^{(k+2)}(x) + (2k+1)xL_n^{(k+1)} - (n^2 - k^2)L_n^{(k)} = 0$. Hence, the function $L_n^{(k)}$ satisfies the differential equation

$$(x^{2}+4)y''+(2k+1)xy'-(n^{2}-k^{2})y=0.$$

Also solved by Paul S. Bruckman, Charles K. Cook, Russell Jay Hendel, Can. A. Minh, Igor O. Popov, H.-J. Seiffert, Tony Shannon, M. N. S. Swamy, and the proposer.

Even Inequality

<u>B-790</u> Proposed by H.-J. Seiffert, Berlin, Germany (Vol. 33, no. 4, August 1995)

Find the largest constant c such that $F_{n+1}^2 > cF_{2n}$ for all even positive integers n.

Solution by L. A. G. Dresel, Reading, England

When *n* is even, the Binet forms give

$$\frac{F_{n+1}^2}{F_{2n}} = \frac{(\alpha^{n+1} - \beta^{n+1})^2}{\sqrt{5}(\alpha^{2n} - \beta^{2n})} = \frac{\alpha^2}{\sqrt{5}} \frac{(1 + \beta^{2n+2})^2}{(1 - \beta^{4n})},$$

and since $0 < \beta^2 < 1$, we see that, for all positive even n, $F_{n+1}^2 / F_{2n} > \alpha^2 / \sqrt{5}$. As $n \to \infty$, we have $F_{n+1}^2 / F_{2n} \to \alpha^2 / \sqrt{5}$. It follows that $c = \alpha^2 / \sqrt{5} = (5 + 3\sqrt{5}) / 10$ is the largest constant such that $F_{n+1}^2 > cF_{2n}$ for all positive even integers n.

Remark: In a similar manner, we can prove the corresponding result for all odd integers *n*: $F_{n+1}^2 < (\alpha^2 / \sqrt{5})F_{2n}$, and that $\alpha^2 / \sqrt{5}$ is the smallest constant for which this is true.

[AUG.

Also solved by Charles Ashbacher, Michel A. Ballieu, Paul S. Bruckman, Charles K. Cook, Andrej Dujella, Russell Euler, C. Georghiou, Russell Jay Hendel, Hans Kappus, Carl Libis, Dorka O. Popova, Bob Prielipp, Lawrence Somer, and the proposer.

Divisibility by 18

<u>B-791</u> Proposed by Andrew Cusumano, Great Neck, NY (Vol. 33, no. 4, August 1995)

Prove that, for all n, $F_{n+11} + F_{n+7} + 8F_{n+5} + F_{n+3} + 2F_n$ is divisible by 18.

Solution by H.-J. Seiffert, Berlin, Germany

Let $c_0, c_1, ..., c_m$ be arbitrary integers. We shall prove that all sums $S_n = \sum_{k=0}^m c_k F_{n+k}$, where *n* is an integer, are divisible by $gcd(S_0, S_1)$, provided that S_0 and S_1 are not both zero.

It is clear that $S_{n+2} = S_{n+1} + S_n$ for all integers *n*. It follows that $S_n = S_0 F_{n-1} + S_1 F_n$ for all integers *n*. The claim follows.

The expression considered in this proposal is such an S_n . Here, $S_0 = 144$ and $S_1 = 234$. The conclusion follows from the fact that gcd(144, 234) = 18.

Haukkanen found the same generalization as Seiffert. Many solvers also came up with the explicit formula $F_{n+11} + F_{n+7} + 8F_{n+5} + F_{n+3} + 2F_n = 18F_{n+6}$ which makes the result obvious.

Also solved by Charles Ashbacher, Michel A. Ballieu, Glenn Bookhout, Paul S. Bruckman, David M. Burton, Charles K. Cook, Leonard A. G. Dresel, Andrej Dujella, Russell Euler, C. Georghiou, Pentti Haukkanen, Russell Jay Hendel, Joseph J. Koštál, Carl Libis, Can. A. Minh, Bob Prielipp, Don Redmond, R. P. Sealy, Sahib Singh, and the proposer.

Reciprocal Sum

B-792 Proposed by Paul S. Bruckman, Edmonds, WA (Vol. 33, no. 4, August 1995)

Let the sequence $\langle a_n \rangle$ be defined by the recurrence $a_{n+1} = a_n^2 - a_n + 1$, n > 0, where the initial term, a_1 , is an arbitrary real number larger than 1. Express $\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \cdots$ in terms of a_1 .

Solution by Hans Kappus, Rodersdorf, Switzerland

The sum in question is $S = 1/(a_1 - 1)$.

Proof: For
$$n > 0$$
, let $S_n = \sum_{k=1}^n \frac{1}{a_k}$. The recurrence $a_{k+1} = a_k^2 - a_k + 1$ is equivalent to

$$\frac{1}{a_k} = \frac{1}{a_k - 1} - \frac{1}{a_{k+1} - 1}.$$

Thus, S_n is unmasked as a telescoping sum. Hence,

$$S_n = \frac{1}{a_1 - 1} - \frac{1}{a_{n+1} - 1}.$$

Since it is clear that $\lim_{n\to\infty} a_n = \infty$, the result follows.

Also solved by Andrej Dujella, C. Georghiou, Russell Jay Hendel, Joseph J. Koštál, H.-J. Seiffert, and the proposer.

1996]

A Congruence for $2^n L_n$

<u>B-793</u> Proposed by Wray Brady, Jalisco, Mexico (Vol. 33, no. 4, August 1995)

Show that $2^n L_n \equiv 2 \pmod{5}$ for all positive integers *n*.

Solution 1 by Can. A. Minh, University of California at Berkeley, Berkeley, CA

The proof is by complete induction on *n*. The result is clearly true for n = 1 and n = 2. Suppose the assertion holds for $1 \le m < n$; we show it holds for *n*. We have $2^n L_n = 2^n (L_{n-1} + L_{n-2}) = 2(2^{n-1}L_{n-1}) + 2^2(2^{n-2}L_{n-2}) \equiv 2 \cdot 2 \pmod{5} = 12 \pmod{5} \equiv 2 \pmod{5}$, and we are done.

Solution 2 by H.-J. Seiffert, Berlin, Germany

From the well-known identities [see Problem B-660, this Quarterly 29.1 (1991):86],

$$2^{n}L_{n} = 2\sum_{i=0}^{\lfloor n/2 \rfloor} {n \choose 2i} 5^{i}$$
 and $2^{n}F_{n} = 2\sum_{i=1}^{\lfloor (n+1)/2 \rfloor} {n \choose 2i-1} 5^{i-1}$,

it obviously follows that, for all nonnegative integers n,

 $2^{n}L_{n} \equiv 2 \pmod{10}$ and $2^{n}F_{n} \equiv 2n \pmod{10}$.

Also solved by Charles Ashbacher, Glenn Bookhout, Paul S. Bruckman, David M. Burton, Charles K. Cook, Leonard A. G. Dresel, Andrej Dujella, Russell Euler, C. Georghiou, Russell Jay Hendel, Hans Kappus, Joseph J. Koštál, Carl Libis, Dorka O. Popova, Bob Prielipp, R. P. Sealy, Sahib Singh, Lawrence Somer, and the proposer.

Exponential Inequality

<u>B-794</u> Proposed by Zdravko F. Starc, Vršac, Yugoslavia (Vol. 33, no. 4, August 1995)

For x a real number and n a positive integer, prove that

$$S_n = \left(\frac{F_2}{F_1}\right)^x + \left(\frac{F_3}{F_2}\right)^x + \dots + \left(\frac{F_{n+1}}{F_n}\right)^x \ge n + x \ln F_{n+1}.$$

Solution by C. Georghiou, University of Patras, Greece

From the Arithmetic-Geometric Mean Inequality, we get $S_n \ge n \left(\frac{F_{n+1}}{F_1}\right)^{x/n} = n \exp\left(\frac{x}{n} \ln F_{n+1}\right) \ge n + x \ln F_{n+1}$, where we have used the inequality $e^y \ge 1 + y$, valid for $y \ge 0$.

Also solved by Paul S. Bruckman, Leonard A. G. Dresel, Andrej Dujella, Russell Euler, Hans Kappus, Joseph J. Koštál, Bob Prielipp, H.-J. Seiffert, and the proposer.

Addenda: The following were inadvertantly omitted as solvers of problems presented in previous issues of this Quarterly: Mohammad K. Azarian solved B-780; Andrej Dujella solved B-782–B-783; Russell J. Hendel solved B-785–B-786; Harris Kwong solved B-780–B-781 and B-784–B-785; Igor O. Popov solved B-784 and B-786; R. P. Sealy solved B-778–780 and B-784–B-785.

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-513 Proposed by Paul S. Bruckman, Salmiya, Kuwait

Define the following quantities:

$$A = \sum_{n \ge 0} \frac{1}{(n!)^2}, \ B = \sum_{n \ge 0} \frac{1}{n!(n+1)!}, \ C = \sum_{n \ge 0} \frac{(2n)!}{(n!)^4}, \ D = \sum_{n \ge 0} \frac{(2n+2)!}{n!((n+1)!)^2(n+2)!}.$$

Prove that $A^2D = B^2C$.

H-514 Proposed by Juan Pla, Paris, France

1. Let (L_n) be the generalized Lucas sequence of the recursion $U_{n+2} - 2aU_{n+1} + U_n = 0$ with a real such that a > 1. Prove that

$$\lim_{n \to +\infty} \frac{L_2 L_{2^2} L_{2^3} \cdots L_{2^n}}{L_{2^{n+1}}} = \frac{1}{4} \frac{1}{a \sqrt{a^2 - 1}}.$$

2. Show that the above expression has a limit when (L_n) is the *classical* Lucas sequence.

H-515 Proposed by Paul S. Bruckman, Salmiya, Kuwait

For all primes $p \neq 2, 5$, let Z(p) denote the entry-point of p in the Fibonacci sequence. It is known that $Z(p) | (p - (\frac{5}{p}))$. Let $a(p) = (p - (\frac{5}{p}))/Z(p), q = \frac{1}{2}(p - (\frac{5}{p}))$. Prove that if $p \equiv 1$ or 9 (mod 20) then

$$F_{q+1} \equiv (-1)^{\frac{1}{2}(q+a(p))} \pmod{p}.$$
 (*)

H-516 Proposed by Paul S. Bruckman, Edmonds, WA

Given p an odd prime, let $\overline{k}(p)$ denote the Lucas period (mod p), that is, $\overline{k}(p)$ is the smallest positive integer m = m(p) such that $L_{m+n} \equiv L_n \pmod{p}$ for all integers n.

Prove the following:

- (a) Let u = u(p) denote the smallest positive integer such that $\alpha^u \equiv \beta^u \equiv 1 \pmod{p}$. Then $u = m = \overline{k}(p)$.
- (b) $\overline{k}(p)$ is even for all (odd) p.

1996]

(c)
$$p \equiv 1 \pmod{k(p)}$$
 iff $p = 5 \text{ or } p \equiv \pm 1 \pmod{10}$.

(d) $p \equiv -1 + \frac{1}{2}\overline{k}(p) \pmod{\overline{k}(p)}$ iff p = 5 or $p \equiv \pm 3 \pmod{10}$.

<u>H-508</u> Proposed by H.-J. Seiffert, Berlin, Germany (Corrected)

Define the Fibonacci polynomials by $F_0(x) = 0$, $F_1(x) = 1$, $F_n(x) = xF_{n-1}(x) + F_{n-2}(x)$, for $n \ge 2$. Show that, for all complex numbers x and y and all positive integers n,

$$F_n(x)F_n(y) = n\sum_{k=0}^{n-1} \frac{1}{k+1} {\binom{n+k}{2k+1}} (x+y)^k F_{k+1} {\binom{xy-4}{x+y}}.$$
 (1)

As special cases of (1), obtain the following identities:

$$F_n(x)F_n(x+1) = n\sum_{k=0}^{n-1} \frac{(-1)^{n-k+1}}{k+1} \binom{n+k}{2k+1} F_{k+1}(x^2+x+4);$$
(2)

$$F_n(x)F_n(4/x) = n \sum_{k=0}^{\left[\frac{n-1}{2}\right]} \frac{1}{2k+1} \binom{n+2k}{4k+1} \left(\frac{x^2+4}{x}\right)^{2k}, \ x \neq 0;$$
(3)

$$F_n(x)^2 = n \sum_{k=0}^{n-1} \frac{(-1)^{n-k+1}}{k+1} \binom{n+k}{2k+1} (x^2+4)^k;$$
(4)

$$F_n(x)^2 = n \sum_{k=0}^{n-1} \frac{1}{k+1} {\binom{n+k}{2k+1}} \frac{x^{2k+2} - (-4)^{k+1}}{x^2 + 4};$$
(5)

$$F_{2n-1}(x) = (2n-1)\sum_{k=0}^{2n-2} \frac{(-1)^k}{k+1} \binom{2n+k-1}{2k+1} x^k F_{k+1}(4/x).$$
(6)

SOLUTIONS

Recurring Theme

<u>H-497</u> Proposed by Mohammad K. Azarian, University of Evansville, Evansville, IN (Vol. 33, no. 2, May 1995)

Solve the recurrence relation

$$\sum_{i=0}^{k} \left(\prod_{j=0}^{k} \frac{x_{n-j}}{x_{n-i}} \right)^{r} + \left(\prod_{t=0}^{k} x_{n-t} \right)^{r} = 0,$$

where r is any nonzero real number, $n > k \ge 1$, and $x_m \ne 0$ for all m.

Solution by the proposer

First, we note that

$$\sum_{i=0}^{k} \left(\prod_{j=0}^{k} \frac{x_{n-j}}{x_{n-i}} \right)^{r} + \left(\prod_{t=0}^{k} x_{n-t} \right)^{r} = (x_{n} x_{n-1} \cdots x_{n-k})^{r} \left(\sum_{i=0}^{k} \left(\frac{1}{x_{n-i}} \right)^{r(k+1)} + 1 \right) = 0.$$

380

[AUG.

Now, using the fact that $(x_n x_{n-1} \cdots x_{n-k})^r \neq 0$ and making the substitution

$$u_{n-i} = \left(\frac{1}{x_{n-i}}\right)^{r(k+1)}, \quad i = 0, 1, 2, \dots, k,$$

we obtain the following nonhomogeneous recurrence relation of order k:

$$u_n + u_{n-1} + u_{n-2} + \dots + u_{n-k} = -1.$$
 (1)

Next, the general solution to (1) has the form $u_n = u_n^{(h)} + u_n^{(p)}$, where $u_n^{(p)}$ is a particular solution to (1) and $u_n^{(h)}$ is the general solution to the homogeneous recurrence relation

$$u_n + u_{n-1} + u_{n-2} + \dots + u_{n-k} = 0.$$
⁽²⁾

We know that $u_n^{(p)}$ must be a constant A. Thus, substituting A in (1), we obtain $u_n^{(p)} = \frac{-1}{k+1}$. To find $u_n^{(h)}$, we note that the characteristic equation associated with (2) is

$$\lambda^k + \lambda^{k-1} + \lambda^{k-2} + \dots + \lambda + 1 = 0.$$
(3)

Hence, using the fact that $\lambda^{k+1} - 1 = (\lambda - 1)(\lambda^k + \lambda^{k-1} + \lambda^{k-2} + \dots + \lambda + 1)$, the roots of (3) are k distinct complex roots of unity:

$$\lambda_m = \cos \frac{2m\pi}{k+1} + i \sin \frac{2m\pi}{k+1}, \ m = 1, 2, ..., k.$$

But, since λ_m is the complex conjugate of λ_{k+1-m} when k is odd, $\lambda_{\frac{k+1}{2}} = -1$. Thus, if k is odd and $k \ge 3$ [if k = 1, then $u_n^{(h)} = C(-1)^n$], then

$$u_n^{(h)} = C(-1)^n + \sum_{m=1}^{\frac{k-2}{2}} (A_m \cos(n\theta_m) + B_m \sin(n\theta_m)),$$

where C, A_m , and B_m are constants and $\theta_m = \tan^{-1}(\tan \frac{2m\pi}{k+1})$. If k is even, then

$$u_n^{(h)} = \sum_{m=1}^{\frac{k}{2}} (A_m \cos(n\theta_m) + B_m \sin(n\theta_m)),$$

where A_m , B_m , and θ_m are as above. Therefore, the general solution to the given recurrence relation is

$$x_n = (u_n)^{-\frac{1}{r(k+1)}} = (u_n^{(h)} + u_n^{(p)})^{-\frac{1}{r(k+1)}}.$$

Also solved by A. Dujella and P. Bruckman.

Pseudo Primes

<u>H-498</u> Proposed by Paul S. Bruckman, Edmonds, WA (Vol. 33, no. 2, May 1995)

Let $u = u_e = L_{2^e}$, e = 2, 3, ... Show that if u is composite it is both a Fibonacci pseudoprime (FPP) and a Lucas pseudoprime (LPP). Specifically, show that $u \equiv 7 \pmod{10}$, $F_{u+1} \equiv 0 \pmod{u}$, and $L_u \equiv 1 \pmod{u}$.

Solution by L. A. G. Dresel, Reading, England

For convenience of writing subscripts, let $E = 2^e$ so that $u_e = L_E$ and

$$u_{e+1} = L_{2E} = (L_E)^2 - 2 = (u_e)^2 - 2.$$
⁽¹⁾

Now make the inductive hypothesis that, for some $e \ge 2$,

$$u_e \equiv 7 \pmod{10}.$$

Then (1) gives $u_{e+1} = (u_e)^2 - 2 \equiv 49 - 2 \equiv 7 \pmod{10}$ and, since $u_2 = L_4 = 7$, the congruence (2) is proved for all $e \ge 2$.

Next, make the inductive hypothesis that, for some $e \ge 2$,

 $u_e = h2^{e+1} - 1$, where *h* is an *odd* integer. (3)

Then

$$u_{e+1} = (u_e)^2 - 2 = (h2^{e+1} - 1)^2 - 2$$
$$= (h^2 2^e - h)2^{e+2} - 1,$$

where $(h^2 2^e - h)$ is again an odd integer, since h is odd. But $u_2 = 2^3 - 1$, and therefore (3) is proved for all $e \ge 2$. It follows that u_e is always odd.

Now, since $u = u_e = L_E$, we have $L_E \equiv 0 \pmod{u}$ and, similarly, $F_{2E} = F_E L_E \equiv 0 \pmod{u}$. Furthermore, (3) shows that u + 1 = 2hE is a multiple of 2E, and it follows that $F_{u+1} \equiv 0 \pmod{u}$.

Next, $\frac{1}{2}(u+1) = hE$ is an odd multiple of E, so that L_{hE} is divisible by L_E and $L_{hE} \equiv 0$ (mod u). Thus, $L_{u+1} = L_{2hE} = (L_{hE})^2 - 2 \equiv -2 \pmod{u}$. From the identities $L_{u+2} + L_u = 5F_{u+1}$ and $L_{u+2} - L_u = L_{u+1}$, we have $2L_u = 5F_{u+1} - L_{u+1} \equiv 2 \pmod{u}$, giving $L_u \equiv 1 \pmod{u}$, since u is odd.

Remark: Another proof of $L_u \equiv 1 \pmod{u}$, also based on formula (3) above, was given by A. Di Porto and P. Filipponi in their article "A Probabilistic Primality Test Based on the Properties of Certain Generalized Lucas Numbers" in *Lecture Notes in Computer Science* **330** (1988):211-223.

Also solved by A. Dujella, H.-J. Seiffert, and the proposer.

FPP's and LPP's

<u>H-499</u> Proposed by Paul S. Bruckman, Edmonds, WA (Vol. 33, no. 3, August 1995)

Given n a natural number, n is a *Lucas pseudoprime* (LPP) if it is composite and satisfies the following congruence:

$$L_n \equiv 1 \pmod{n}. \tag{1}$$

If gcd(n, 10) = 1, the Jacobi symbol $(5/n) = \varepsilon_n$ is given by the following:

$$\varepsilon_n = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{10}, \\ -1 & \text{if } n \equiv \pm 3 \pmod{10}. \end{cases}$$

Given gcd(n, 10) = 1, n is a Fibonacci pseudoprime (FPP) if it is composite and satisfies the following congruence:

[AUG.

$$F_{n-\varepsilon_n} \equiv 0 \pmod{n}.$$
 (2)

Define the following sequences for e = 1, 2, ...:

$$u = u_e = F_{3^{e+1}} / F_{3^e}; (3)$$

$$v = v_e = L_{3^{e+1}} / L_{3^e}; (4)$$

$$w = w_e = F_{23^{e+1}} / F_{23^e} = uv.$$
 (5)

Prove the following for all $e \ge 1$: (i) u is a FPP and a LPP, provided it is composite; (ii) same statement for v; (iii) w is a FPP but not a LPP.

Solution by H.-J. Seiffert, Berlin, Germany

We need the additional easily verifiable equations:

$$F_{3k} = 5F_k^3 + 3(-1)^k F_k, (6)$$

$$L_{3k} = L_k^3 - 3(-1)^k L_k, \tag{7}$$

$$L_{2k} = L_k^2 - 2(-1)^k = 5F_k^2 + 2(-1)^k,$$
(8)

where k is any integer, and the following propositions.

Proposition 1: If n is a composite positive integer such that gcd(n, 10) = 1, then n is a FPP and a LPP if and only if $F_{\frac{1}{2}(n-\varepsilon_n)} \equiv 0 \pmod{n}$ if $n \equiv 1 \pmod{4}$, and $L_{\frac{1}{2}(n-\varepsilon_n)} \equiv 0 \pmod{n}$ if $n \equiv 3 \pmod{4}$.

Proof: This is just the result of H-496.

Proposition 2: If e is a positive integer, then $\frac{1}{2}L_{2,2^e}$ is an odd positive integer divisible by 3^{e+1} .

Proof: This is true for e = 1, since $\frac{1}{2}L_6 = 9$. Suppose that the statement holds for $e, e \in N$. Then we have $\frac{1}{2}L_{2\cdot 3^e} = 3^{e+1}m$, where *m* is an odd positive integer. Equation (7) with $k = 2 \cdot 3^e$ gives

$$\frac{1}{2}L_{2\cdot3^{e+1}} = \frac{1}{2}\left(L_{2\cdot3^{e}}^{3} - 3L_{2\cdot3^{e}}\right) = 3^{e+2}m(4\cdot3^{2e+1}m^{2} - 1),$$

showing that the statement holds for e + 1. This completes the induction proof. Q.E.D.

Proposition 3: If k and n are nonnegative integers, then we have $gcd(L_k, L_{2kn}) \in \{1, 2\}$.

Proof: From $L_{2kn} = L_k L_{k(2n-1)} - (-1)^k L_{2k(n-1)}$, it follows that

$$gcd(L_k, L_{2kn}) \in \{gcd(L_k, L_{2k}), gcd(L_k, L_0)\}.$$

Since $L_{2k} = L_k^2 - 2(-1)^k$ and $L_0 = 2$, the desired result follows. Q.E.D.

Now we are able to prove the statements of the present proposal. From (6)-(8), we obtain

$$u_e + 1 = 5F_{3^e}^2 - 2 = L_{23^e} = L_{3^e}^2 + 2 = v_e - 1, \ e \in N.$$
(9)

Since F_{3^e} , $e \in N$, is even, it follows that $u = u_e \equiv -3 \pmod{10}$, $u \equiv 1 \pmod{4}$, $v = v_e \equiv -1 \pmod{10}$, and $v \equiv 3 \pmod{4}$, so that $\varepsilon_u = -1$ and $\varepsilon_v = 1$. Using Proposition 2, equations (9), and

1996]

ADVANCED PROBLEMS AND SOLUTIONS

the well-known divisibility properties of the Fibonacci and Lucas numbers, we conclude that $F_{3^{e+1}} | F_{\frac{1}{2}(u+1)}$ and $L_{3^{e+1}} | L_{\frac{1}{2}(v-1)}$, which imply $F_{\frac{1}{2}(u+1)} \equiv 0 \pmod{u}$ and $L_{\frac{1}{2}(v-1)} \equiv 0 \pmod{v}$. Applying Proposition 1, we see that u is a FPP and a LPP if it is composite, and that v is a FPP and a LPP if it is composite. This solves (i) and (ii).

From what has been proved above, we have $w = uv \equiv 3 \pmod{4}$, $w \equiv 3 \pmod{10}$, $\varepsilon_w = -1$, $w + 1 = u(u+2) + 1 = (u+1)^2$, and

$$F_{u+1} \equiv 0 \pmod{u}$$
 and $F_{u+1} = F_{v-1} \equiv 0 \pmod{v}$. (10)

We note that (10) remains valid if u or v is a prime. Since gcd(u, v) = gcd(u, u+2) = gcd(u, 2) = 1and since $F_{u+1} | F_{(u+1)^2} = F_{w+1}$, from (10) we obtain $F_{w+1} \equiv 0 \pmod{w}$. Thus, w is a FPP, since it is composite. However, w is not a LPP. This can be seen as follows. Assume, by way of contradiction, that w is a LPP. Then, since w is a FPP as shown above, we would have $L_{\frac{1}{2}(w+1)} \equiv 0 \pmod{w}$, by Proposition 1. It then would follows that

$$v|\gcd(L_{\frac{1}{2}(\nu-1)}, L_{\frac{1}{2}(\nu+1)}) = \gcd(L_{\frac{1}{2}(\nu+1)}, L_{\frac{1}{2}(\nu+1)^2})$$

However, $\frac{1}{2}(u+1)^2$ is an even multiple of $\frac{1}{2}(u+1)$; thus, by Proposition 3, we have $v \in \{1, 2\}$. Clearly, this is a contradiction, since v is obviously greater than 2. Hence, w cannot be a LPP. This solves (iii).

Also solved by L. A. G. Dresel and the proposer.

Belated Acknowledgment: C. Georghiou solved H-486.

SUSTAINING MEMBERS

*H.L. Alder G.L. Alexanderson P. G. Anderson S. Ando R. Andre-Jeannin *J. Arkin C. Ashbacher M.K. Azarian N. Balasubramania J.G. Bergart G. Bergum G. Berzsenyi * M. Bicknell-Johnson P.S. Bruckman M.F. Bryn G.D. Chakerian C. Chouteau C.K. Cook M.J. DeBruin M.J. DeLeon J. De Kerf

L.A.G. Dresel U. Dudley M. Faccio D.R. Farmer D.C. Fielder P. Filipponi C.P. Flynn Fondazione Ugo Bordoni Anthony Gioia M.F. Goode *H.W. Gould P. Hagis, Jr. H. Harborth P. Haukkanen * A.P. Hillman * A.F. Horadam Y. Horibe F.T. Howard R.J. Howell J.P. Jones

R.E. Kennedy C.H. Kimberling Y.H.H. Kwong J. Lahr B. Landman L.H. Lange * C.T. Long G. Lord * J. Maxwell F.U. Mendizabal J.L. Miller M.G. Monzingo J.F. Morrison S.A. Obaid S. Palsson J. Pla A. Prince S. Rabinowitz S. Sato J.A. Schumaker

A.G. Shannon L.W. Shapiro J.R. Siler L. Somer P. Spears W.R. Spickerman Paul K. Stockmeyer J. Suck M.N.S. Swamy *D. Thoro J.C. Turner T.P. Vaughan J.N. Vitale M. Waddill J.E. Walton W.A. Webb G.E. Weekly D.L. Wells R.E. Whitney **B.E.** Williams * Charter Members

INSTITUTIONAL MEMBERS

CALIFORNIA STATE UNIVERSITY SACRAMENTO Sacramento, California

ETH-BIBLIOTHEK Zurich, Switzerland

CHALMERS UNIVERSITY OF TECHNOLOGY AND UNIVERSITY OF GOTEBORG *Goteborg, Sweden*

GONZAGA UNIVERSITY Spokane, Washington

HOWELL ENGINEERING COMPANY Bryn Mawr, California

INDIANA UNIVERSITY Bloomington, Indiana

KLEPCO, INC. Sparks, Nevada

KOBENHAVNS UNIVERSITY Matematisk Institut Copenhagen, Denmark

LAURENTIAN UNIVERSITY Sudbury, Ontario, Canada MATHEMATISCHES FORSCHUNGS INSTITUT Lorenzenhof, Germany

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 1-6. 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.

Fibonacci Entry Points and Periods for Primes 100,003 through 415,993 by Daniel C. Fielder and Paul S. Bruckman.

Please write to the Fibonacci Association, Santa Clara University, Santa Clara, CA 95053, U.S.A., for more information and current prices.