The Fibonacci Quarterly

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

TABLE OF CONTENTS

VOLUME 38 JUNE-JULY 2000 NUMBER 3

PURPOSE

The primary function of **THE FIBONACCI QUARTERLY** is to serve as a focal point for widespread interest in the Fibonacci and related numbers, especially with respect to new results, research proposals, challenging problems, and innovative proofs of old ideas.

EDITORIAL POLICY

THE FIBONACCI QUARTERLY seeks articles that are intelligible yet stimulating to its readers, most of whom are university teachers and students. These articles should be lively and well motivated, with new ideas that develop enthusiasm for number sequences or the exploration of number facts. Illustrations and tables should be wisely used to clarify the ideas of the manuscript. Unanswered questions are encouraged, and a complete list of references is absolutely necessary.

SUBMITTING AN ARTICLE

Articles should be submitted using the format of articles in any current issues of **THE FIBONACCI QUARTERLY.** They should be typewritten or reproduced typewritten copies, that are clearly readable, double spaced with wide margins and on only one side of the paper. The full name and address of the author must appear at the beginning of the paper directly under the title. Illustrations should be carefully drawn in India ink on separate sheets of bond paper or vellum, approximately twice the size they are to appear in print. Since the Fibonacci Association has adopted $F_1 = F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$, $n \geq 2$ and $L_1 = 1$, $L_2 = 3$, $L_{n+1} = L_n + L_{n-1}$, $n \geq 2$ as the standard definitions for The Fibonacci and Lucas sequences, these definitions ***should not*** be a part of future papers. However, the notations ***must*** be used. One to three ***complete*** A.M.S. classification numbers ***must*** be given directly after references or on the bottom of the last page. **Papers not satisfying all of these criteria will be returned.** See the new worldwide web page at:

http://www.sdstate.edu/~wcsc/http/fibhome.html

for additional instructions.

Two copies of the manuscript should be submitted to: **CURTIS COOPER, DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, CENTRAL MISSOURI STATE UNIVERSITY, WARRENSBURG, MO 64093-5045.**

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.

The journal will now accept articles via electronic services. However, electronic manuscripts must be submitted using the typesetting mathematical wordprocessor AMS-TeX. Submitting manuscripts using AMS-TeX will speed up the refereeing process. AMS-TeX can be downloaded from the internet via the homepage of the American Mathematical Society.

SUBSCRIPTIONS, ADDRESS CHANGE, AND REPRINT INFORMATION

Address all subscription correspondence, including notification of address change, to: **PATTY SOLSAA, SUBSCRIPTIONS MANAGER, THE FIBONACCI ASSOCIATION, P.O. BOX 320, AURORA, SD 57002-0320. E-mail: solsaap@itctel.com.**

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 $40 for Regular Membership, $50 for Library, $50 for Sustaining Membership, and $80 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 **BELL & HOWELL INFORMATION & LEARNING, 300 NORTH ZEEB ROAD, P.O. BOX 1346, ANN ARBOR, MI 48106-1346.** Reprints can also be purchased from **BELL & HOWELL** at the same address.

The Fibonacci Quarterly

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

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

ON p-ADIC COMPLEMENTARY THEOREMS BETWEEN PASCAL'S TRIANGLE AND THE MODIFIED PASCAL TRIANGLE*

Shiro Ando
5-29-10 Honda Kokubunji-shi, Tokyo 185-0011, Japan

Daihachiro Sato
Department of mathematics and Statistics, University of Regina, Regina, Saskatchewan, S4S 0A2, Canada
(Submitted July 1996-Final Revision January 2000)

1. INTRODUCTION

For any entry X inside Pascal's triangle, there are six entries next to and surrounding X which form a hexagon $A_1A_2A_3A_4A_5A_6$ (taken counterclockwise in this order).

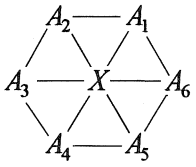


FIGURE 1

H. W. Gould [3] conjectured that an equal GCD property of the values of the binomial coefficients, namely

$$\mathrm{GCD}(A_1, A_3, A_5) = \mathrm{GCD}(A_2, A_4, A_6),$$

is true for all choices of the central entry X on Pascal's triangle. Gould called this conjecture a Star of David equality.

This equality was proved p-adically first by A. P. Hillman and V. E. Hoggatt, Jr. [4], and then by many others. A simple non-p-acid proof for the Star of David equality is given by S. Hitotumatu and D. Sato [5].

It is clear that an analogous equal LCM property for the Star of David configuration, namely

$$\mathrm{LCM}(A_1, A_3, A_5) = \mathrm{LCM}(A_2, A_4, A_6),$$

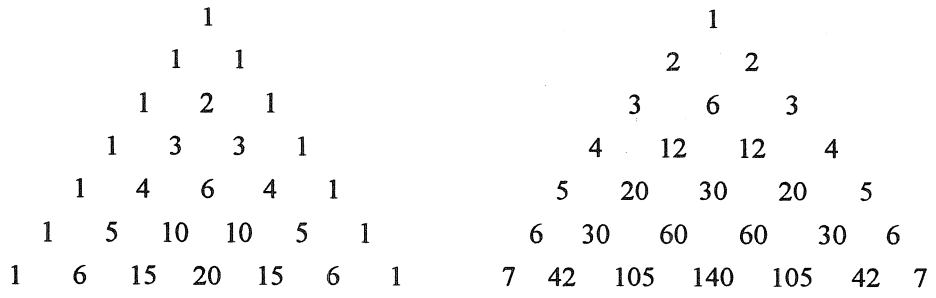
does not hold on Pascal's triangle.

In order to obtain an analogous LCM equality for two triplets $\{A_1, A_3, A_5\}$ and $\{A_2, A_4, A_6\}$, S. Ando [1] proposed a modified number array that has modified binomial coefficients $X' = (n+1)!/k!(n-k)!$ as its entries instead of binomial coefficients $X = n!/k!(n-k)!$ and called it the modified Pascal triangle. The beginning parts of Pascal's triangle and the modified Pascal triangle corresponding to $0 \le n \le 6$ are shown in Figure 2.

This modified Pascal triangle consists of the reciprocals of the entries on the harmonic triangle of Leibniz which has been studied by G. W. Leibniz as a method of summing up an infinite telescopic sequence.

---

* The content of this paper was presented to The Fibonacci Association under the title "On p-adic Duality between Pascal's Triangle and the Harmonic Triangle I" at the Seventh International Research Conference on Fibonacci Numbers and Their Applications held at the Technische Universität in Graz, Austria, on July 15-19, 1996.



(a) Pascal's Triangle $\Delta(B)$ **(b) Modified Pascal Triangle $\Delta(M)$**

FIGURE 2

On the modified Pascal triangle, the equal LCM property of the new Star of David configuration, namely

$$\mathrm{LCM}(A_1', A_3', A_5') = \mathrm{LCM}(A_2', A_4', A_6'),$$

always holds, no matter where we take the center X'.

While the equal LCM property holds on this modified Pascal triangle, it is easy to see that the equal GCD property of two triplets $\{A_1', A_3', A_5'\}$ and $\{A_2', A_4', A_6'\}$, namely

$$\mathrm{GCD}(A_1', A_3', A_5') = \mathrm{GCD}(A_2', A_4', A_6'),$$

no longer holds there.

Moreover, we studied in [2] a necessary and sufficient condition that rays of a star configuration on Pascal's triangle or on the modified Pascal triangle cover its center with respect to GCD and LCM. We do not want to repeat the results here, but the conditions for GCD and LCM on Pascal's triangle correspond to those for LCM and GCD on the modified Pascal triangle, respectively, although on the modified Pascal triangle we have to take the reflection of configurations on Pascal's triangle with respect to the horizontal line (see item (i) of Section 2 and the Corollary in Section 4).

The purpose of this paper is to clarify the reason why such a phenomenon occurs between these triangular arrays of numbers by showing a p-adic complementary relation of binomial coefficients and modified binomial coefficients.

2. DEFINITIONS, NOTATIONS, AND CLARIFICATIONS

(a) We denote the value of binomial coefficients as

$$X = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

for $0 \le k \le n$. The triangular array of binomial coefficients is Pascal's triangle, which we denote by $\Delta(B)$.

(b) We call

$$\left\{ {n \atop k} \right\} = \frac{(n+1)!}{k!(n-k)!} = (n+1)\binom{n}{k}$$

the modified binomial coefficients, and we refer to a similar triangular array of these coefficients as the modified Pascal triangle, which we denote by $\Delta(M)$.

(c) Given a prime number p and an integer y, the additive p-adic valuation of y, denoted by $\beta = v_p(y)$, is the largest β such that p^β divides y.

Let the symbols $\binom{n}{k}$ and $\{{}^{n}_{k}\}$ represent both their numerical values and their positions on $\Delta(B)$ and $\Delta(M)$, respectively. The inequality $0 \le k \le n$ is assumed throughout the arguments.

(d) The set of both triangular arrays of nonnegative integers defined in (a) and (b) is denoted by $\Delta(T)$. Thus, $\Delta(T) = \{\Delta(B), \Delta(M)\}$, and $Y \in \Delta(T)$ means that Y is one of these two triangular arrays.

(e) A finite subset C of $Y \in \Delta(T)$ is called a configuration on Y.

(f) We introduce an equivalence relation to the set of all the configurations on Y such that two configurations on Y are equivalent to each other if and only if one is obtained by a parallel translation of the other. Then an equivalence class of the set of all configurations on Y by this equivalence relation is called a translatable configuration on Y. Unless otherwise stated, we simply call it a configuration C even if it is actually referring to the translatable configuration to which the configuration C belongs. There will not be a danger of misinterpretation since we are discussing only the GCD and LCM properties that hold on C independent of the location of C on Y.

(g) Let S_1 and S_2 be two nonempty finite subsets of $Y \in \Delta(T)$ and put $C = S_1 \cup S_2$. Then C is a configuration on Y. We do not claim $S_1 \cap S_2 = \phi$.

If the equality

$$\mathrm{GCD}(S_1) = \mathrm{GCD}(S_2) \tag{1}$$

holds independent of the location of C on Y, we call (1) a GCD equality on Y. In the case $S_1 = \{A_1, A_3, A_5\}$ and $S_2 = \{A_2, A_4, A_6\}$, (1) turns out to be the original Star of David equality. In the same manner, if

$$\mathrm{LCM}(S_1) = \mathrm{LCM}(S_2) \tag{2}$$

holds instead of (1), we call (2) a LCM equality in Y.

(h) The central symmetric axis of $Y \in \Delta(T)$ is the straight line of entries with $n = 2k$, where $k = 0, 1, 2, \ldots$, on Y. Any line of entries that is parallel to it on y is called a vertical line of Y. Y is supposed to be placed in the traditional way so that these lines are vertical. A set of entries with $n =$ constant on Y is called a horizontal line of Y. It is perpendicular to a vertical line of Y.

(i) We consider a group $K = \{I, V, H, R\}$ of transformations that operate on the configuration C on Y. I is the identity transformation by which each entry in C stays unchanged. V is the vertical reflection of C by which each entry in C moves to its symmetrical point with respect to a vertical line. H is the horizontal reflection of C by which each entry in C moves to its symmetrical point with respect to a horizontal line. R is a 180° rotation about a point X by which each entry in C moves to its symmetrical point with respect to X. X is not always a point in C, but sometimes is a midpoint of two entries on Y.

Notice that each transformation in K operates on C, not on Y, and we do not have to locate the reflection axis or the center of symmetry since we assume that configuration C on which each element of K operates is translatable.

(j) Group K is Klein's four group with unit I, and its elements satisfy the relations

$$V^2 = H^2 = R^2 = I, \quad VH = HV = R, \quad VR = RV = H, \quad HR = RH = V.$$

The images of a configuration C under the transformations V, H, and R are also called a vertical (or right-left) reflection of C, a horizontal (or upside-down) reflection of C and a 180° rotation of C, and are denoted by $V(C)$, $H(C)$, and $R(C)$, respectively.

3. p-ADIC COMPLEMENTARY THEOREM BETWEEN BINOMIAL AND MODIFIED BINOMIAL COEFFICIENTS

First, we will write a preparatory lemma concerning binomial coefficients.

Lemma 1: Let p be a given prime number and r be a nonnegative integer. Then we have

$$v_p\left(\binom{p^r-1}{k}\right) = 0$$

for $0 \le k \le p^r - 1$, and

$$v_p\left(\binom{2p^r-1}{k}\right) = 0$$

for $0 \le k \le 2p^r - 1$.

Proof: Both equalities are special cases of Theorem 8 in C. T. Long [6]. Notice that, for $p = 2$, the second equality is reduced to the first one.

Now, we will show our main result.

Theorem 1: Let p be a prime number and r be a nonnegative integer. Then, for any integers m, n, h, and k satisfying

$$m+n = 2p^r - 2, \quad h+k = p^r - 1, \quad 0 \le k \le n \text{ and } 0 \le h \le m, \tag{3}$$

we have

$$v_p\left(\binom{m}{h}\right) + v_p\left(\left\{{n \atop k}\right\}\right) = r. \tag{4}$$

Proof: Using given conditions (3) and Lemma 1, we can easily show that

$$v_p\left(\binom{m}{h}\right) + v_p\left(\left\{{n \atop k}\right\}\right) = v_p\left(\binom{m}{h}\left\{{n \atop k}\right\}\right) = v_p\left(\frac{m!}{h!(m-h)!} \times \frac{(n+1)!}{k!(n-k)!}\right)$$

$$= v_p\left(\frac{(h+k+1)\times(m+n+1)!}{(h+k+1)!(m+n-h-k)!} \times \frac{(h+k)!}{h!k!} \times \frac{(m+n-h-k)!}{(m-h)!(n-k)!} \div \frac{(m+n+1)!}{m!(n+1)!}\right)$$

$$= v_p(h+k+1) + v_p\left(\binom{m+n+1}{h+k+1}\right) + v_p\left(\binom{h+p}{h}\right) + v_p\left(\binom{m+n-h-k}{m-h}\right) - v_p\left(\binom{m+n+1}{m}\right)$$

$$= v_p(p^r) + v_p\left(\binom{2p^r-1}{h+k+1}\right) + v_p\left(\binom{p^r-1}{h}\right) + v_p\left(\binom{p^r-1}{m-h}\right) - v_p\left(\binom{2p^r-1}{m}\right)$$

$$= r + 0 + 0 + 0 - 0 = r.$$

4. GCD-LCM DUALITY BETWEEN PASCAL'S TRIANGLE AND THE MODIFIED PASCAL TRIANGLE

As an application of the p-adic complementary theorem between the binomial coefficients and the modified binomial coefficients that was established in the previous section, we now prove a duality between Pascal's triangle $\Delta(B)$ and the modified Pascal triangle $\Delta(M)$ concerning the GCD and the LCM.

Let S_1 and S_2 be two nonempty finite subsets of $\Delta(B)$ and put $C = S_1 \cup S_2$. Then C is a configuration in $\Delta(B)$. First, we assume that

$$\mathrm{GCD}(S_1) = \mathrm{GCD}(S_2) \tag{5}$$

holds independent of the location of C in $\Delta(B)$.

Define $\min\{v_p(S)\}$ to be $\min\{v_p(A) \mid A \in S\}$. Then the GCD equality (5) is equivalent to

$$\min\{v_p(S_1)\} = \min\{v_p(S_2)\} \text{ for all primes } p. \tag{6}$$

Let R be a 180° rotation about a point X defined in item (i) in Section 2. Since we are discussing the translatable properties of the configurations, we can take any point X such that, for any entry $A \in \Delta(B)$, $R(A)$ is also an entry of $\Delta(B)$ as long as $R(A) \in \Delta(B)$.

We overlap two triangles $\Delta(B)$ and $\Delta(M)$ in such a way that $\binom{n}{k}$ and $\left\{{n \atop k}\right\}$ fall on the same point. Then a configuration C in $\Delta(B)$ is also considered to be one in $\Delta(M)$, which is geometrically the same as C in $\Delta(B)$ although they are different as sets of integers. If $R(C) \subset \Delta(M)$, we put $C' = R(C)$. Then $C' = S_1' \cup S_2'$, where $S_1' = R(S_1)$ and $S_2' = R(S_2)$ are subsets of C'.

Let p be an arbitrary, but fixed prime. If we take the midpoint of

$$\binom{0}{0} \text{ and } \binom{2p'-2}{p'-1},$$

where r is a sufficiently large positive integer, as the center X of rotation R, then the configuration C corresponding to C' by R is contained in $\Delta(B)$. Any entry $A' \in C'$ and the corresponding entry $A \in C$ satisfies condition (3) of Theorem 1 if we let

$$A = \binom{m}{h} \text{ and } A' = \left\{{n \atop k}\right\}.$$

Therefore, we have $v_p(A) + v_p(A') = r$ by Theorem 1, so that

$$\min\{v_p(S)\} + \max\{v_p(S')\} = r \tag{7}$$

for any $S' \in C'$ and corresponding $S \in C$.

Since we assume the GCD equality (5) on $\Delta(B)$, equality (6) holds so that, using (7), we have

$$\max\{v_p(S_1')\} = \max\{v_p(S_2')\} \text{ for all primes } p, \tag{8}$$

which is equivalent to

$$\mathrm{LCM}(S_1') = \mathrm{LCM}(S_2'). \tag{9}$$

Thus, (9) holds independent of the location of C' on $\Delta(M)$.

In a similar manner, we can prove that if (9) holds independent of the location of C' on $\Delta(M)$, then (5) holds independent of the location of C' on $\Delta(B)$. If we exchange min and max in

(6), (7), and (8), then GCD and LCM in (5) and (9) must be exchanged. Summarizing these arguments, we have the following results.

Theorem 2: Let $C = S_1 \cup S_2$ be a configuration on $\Delta(B)$ and $C' = S_1' \cup S_2'$ be the configuration on $\Delta(M)$ corresponding to C by a 180° rotation R about a point X. Then GCD equality (5) holds independent of the location of C on $\Delta(B)$ if and only if LCM equality (9) holds independent of the location of $C' = R(C)$ on $\Delta(M)$. Similarly, the LCM equality holds for C on $\Delta(B)$ if and only if the corresponding GCD equality for C' holds on $\Delta(M)$.

Corollary: Let $C = S_1 \cup S_2$ be as above and C'' be the configuration on $\Delta(M)$ corresponding to C by horizontal reflection H with respect to a horizontal line. If we put $H(S_1) = S_1''$, $H(S_2) = S_2''$, then $C'' = S_1'' \cup S_2''$. GCD equality (5) holds independent of the location of C on $\Delta(B)$ if and only if LCM equality $\mathrm{LCM}(S_1'') = \mathrm{LCM}(S_2'')$ holds independent of the location of $C'' = H(C)$ on $\Delta(M)$. Similarly, the LCM equality holds for C on $\Delta(B)$ if and only if the corresponding GCD equality for C'' holds on $\Delta(M)$.

Proof: A horizontal reflection H can be expressed as $H = RV$ by a vertical reflection V and a 180° rotation R. If we remember that the equality

$$\binom{n}{n-k} = \binom{n}{k}$$

holds for nonnegative integers n, k with $k \le n$, it is clear that a GCD equality or an LCM equality holds for C if and only if it holds for $V(C)$. Combining this fact with Theorem 2, we have the stated conclusion.

5. p-ADIC COMPLEMENTARY THEOREMS BETWEEN GENERALIZED BINOMIAL COEFFICIENTS AND GENERALIZED MODIFIED BINOMIAL COEFFICIENTS WHICH ARE DEFINED BY A STRONG DIVISIBILITY SEQUENCE

A sequence of integers $A = \{a_n\} = \{a_1, a_2, a_3, \ldots\}$ is called a strong divisibility sequence if $(a_k, a_h) = a_{(k,h)}$ for every k, $h = 1, 2, 3, \ldots$, where (a_k, a_h) and (k, h) are the greatest common divisors of the two numbers.

The sequence of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ and the sequence of Fibonacci numbers $F = \{F_1, F_2, F_3, \ldots\}$ are two examples of strong divisibility sequences.

For any strong divisibility sequence $A = \{a_n\}$, if we generalize the binomial coefficients $\binom{n}{k}$ and modified binomial coefficients $\left\{{n \atop k}\right\}$ by replacing n and k in 2(a) and 2(b) by a_n and a_k throughout, then we have A-binomial coefficients

$$\binom{n}{k}_A = \frac{a_1 a_2 \ldots a_n}{(a_1 a_2 \ldots a_k)(a_1 a_2 \ldots a_{n-k})}$$

and A-modified binomial coefficients

$$\left\{{n \atop k}\right\}_A = \frac{a_1 a_2 \ldots a_n a_{n+1}}{(a_1 a_2 \ldots a_k)(a_1 a_2 \ldots a_{n-k})} = a_{n+1}\binom{n}{k}_A.$$

It is not difficult to obtain generalizations of the p-adic complementary theorem and the GCD-LCM duality theorem between analogous two-dimensional number arrays of A-binomial

coefficients and A-modified binomial coefficients, both of which are defined by the same strong divisibility sequence $A = \{a_n\}$.

Those generalizations, other extensions, and their applications will be reported in subsequent papers in due course.

REFERENCES

1. S. Ando. "A Triangular Array with Hexagon Property, Dual to Pascal's Triangle." In *Applications of Fibonacci Numbers* **2:**61-67. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1988.
2. S. Ando & D. Sato. "A Necessary and Sufficient Condition that Rays of a Star Configuration on Pascal's Triangle Cover Its Center with Respect to GCD and LCM." In *Applications of Fibonacci Numbers* **5:**11-36. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1993.
3. H. W. Gould. "A New Greatest Common Divisor Property of the Binomial Coefficients." *The Fibonacci Quarterly* **10.6** (1972):579-84, 628.
4. A. P. Hillman & V. E. Hoggatt, Jr. "A Proof of Gould's Pascal Hexagon Conjecture." *The Fibonacci Quarterly* **10.6** (1972):565-68, 598.
5. S. Hitotumatu & D. Sato. "The Star of David Theorem (I)." *The Fibonacci Quarterly* **13.1** (1975):70.
6. C. T. Long. "Some Divisibility Properties of Pascal's Triangle." *The Fibonacci Quarterly* **19.3** (1981):257-63.

AMS Classification Numbers: 11B65, 11A05, 05A10

❖❖❖

A NUMBER THEORETIC FUNCTION ARISING FROM CONTINUED FRACTIONS

H. C. Williams
University of Manitoba, Department of Computer Science
Winnipeg, Manitoba R3T 2N2 Canada
(*Submitted June 1998*)

1. INTRODUCTION

Let a, b be integers with $b > 0$. If we perform the Euclidean algorithm to find (a, b), the greatest common divisor of a and b, we get

$$\begin{array}{rcll} a & = & q_0 b + r_0 & (0 \le r_0 < b) \\ b & = & q_1 r_0 + r_1 & (0 \le r_1 < r_0) \\ r_0 & = & q_2 r_1 + r_2 & (0 \le r_2 < r_1) \\ \cdots & & \cdots & \cdots \end{array}$$

until we finally find the least $n \ge 0$ such that $r_n = 0$. Note that for this value of n we get $q_n > 1$. We will define $E(a, b)$ to be this value n. We now let a, q be any pair of coprime integers with $q > 0$ and set $\omega = \omega(a, q)$ to be the multiplicative order of a modulo q; that is, ω is the least positive value of m such that $a^m \equiv 1 \pmod{q}$. We define the number theoretic function $W(a, q)$ by

$$W(a, q) = 2\sum_{i=1}^{\omega} \lfloor E(a^i, q)/2 \rfloor. \tag{1.1}$$

We next let N be any positive non-square integer and define

$$v(N) = (\sigma - 1 + \sqrt{N})/\sigma,$$

where

$$\sigma = \begin{cases} 2 & \text{when } N \equiv 1 \pmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

Now consider

$$N = (\sigma(qra^n + \mu(a^k + \lambda)/q)/2)^2 - \sigma^2 \mu\lambda a^n r,$$

where $\mu, \lambda \in \{1, -1\}$, $qr \mid a^k + \lambda$, $(n, k) = 1$, $n > k \ge 1$, and

$$\sigma = \begin{cases} 1 & \text{if } 2 \mid qra^n + \mu(a^k + \lambda)/q, \\ 2 & \text{if } 2 \nmid qra^n + \mu(a^k + \lambda)/q. \end{cases}$$

It was shown in Williams [16] that $W(a, q)$ is a very important function for determining *a priori* the period length $p(N)$ of the simple continued fraction expansion of $v(N)$. For example, in the simple case of $r = \mu = -\lambda = 1$, we get

$$p(N) = 2n + k + kW(a, q)/\omega(a, q).$$

Indeed, as shown in Mollin and Williams [6], we get the simple continued fraction expansion for $v(N)$ as

$$v(N) = \langle q_0, \overline{q_1, q_2, \ldots, q_p} \rangle,$$

where we can actually provide formulas for q_i $(i = 0, 1, 2, \ldots, p = p(N))$ in terms of q, a, n, k. In order to do this, we first need to define for $1 \le j \le n-1$ the symbols:

$$\lambda_j = jk - \lfloor kj/n \rfloor n,$$
$$\varepsilon_j = \lfloor (j+1)k/n \rfloor - \lfloor jk/n \rfloor,$$
$$\rho_j = k - n + \lambda_j,$$
$$m_j = \begin{cases} 2\lfloor E(a^i, q)/2 \rfloor + 1 & \text{when } \varepsilon_j = 1, \\ 1 & \text{when } \varepsilon_j = 0, \end{cases}$$

and $\psi(i)$, where $\psi(1) = 3$ and $\psi(j+1) = \psi(j) + \varepsilon_j m_j + 2$. With these in mind we get

$$q_0 = (qa^n + (a^k - 1)/q)/2 + (\sigma - 1)/\sigma,$$
$$q_1 = q,\ q_2 = qa^{n-k},$$
$$q_{\psi(j)} = \begin{cases} qa^{\lambda_j} & \text{when } \varepsilon_j = 0, \\ qa^{\lambda_j} + (a^{\rho_j} - \gamma_j)/q & \text{when } \varepsilon_j = 1. \end{cases}$$

Also, if $\varepsilon_j = 0$, then $q_{\psi(j)+1} = qa^{n-k-\lambda_j}$, and if $\varepsilon_j = 1$, then

$$q_{\psi(j)+i} = \begin{cases} b_{i,j} & \text{for } 1 \le i \le m_j, \\ qa^{2n-k-\lambda_j} + (a^{n-\lambda_j} - \delta_i)/q & \text{for } i = m_j + 1. \end{cases}$$

Here,

$$a^{\rho_j}/q = \langle b_{0,j}, b_{1,j}, \ldots, b_{m_j,j} \rangle,$$

$$\gamma_j \equiv a^{\rho_j} \pmod{q},\ \delta_j \equiv a^{n-\lambda_j} \pmod{q}, \text{ and } 0 < \gamma_j,\ \delta_j < q.$$

We have $p(N) = 2 + \psi(n-1) = 2n + k + kW(a, q)/\omega(a, q)$.

Some properties of $W(a, q)$ were developed by Mollin and Williams [7]; for example,

$$W(a, q) = 4 \sum_{i=1}^{(\omega-1)/2} \lfloor E(a^i, q)/2 \rfloor \quad \text{when } 2 \nmid \omega \tag{1.2}$$

and

$$W(a, q) = 4 \sum_{i=1}^{\omega/2-1} \lfloor E(a^i, q)/2 \rfloor + 2\lfloor E(a^{\omega/2}, q)/2 \rfloor \quad \text{when } 2 \mid \omega. \tag{1.3}$$

Thus, if ω is odd, we always have $4 \mid W(a, q)$, but if ω is even, the value of $W(a, q)$ is always even, of course, but its value modulo 4 is determined by $2\lfloor E(a^{\omega/2}, q)/2 \rfloor$. In the simple case of $a^{\omega/2} \equiv -1 \pmod{q}$, we have $E(a^{\omega/2}, q) = 2$, but we see that $\omega(29, 35) = 2$ and $E(29, 35) = 4$. Thus, it appears that $W(a, q) \equiv 2, 0 \pmod 4$ when $2 \mid \omega$. This raises the question of exactly what values can be assumed by $W(a, q)$. In this paper we will find values that can be assumed by $W(a, q)$ when $\omega = 1, 2, 3, 4, 6$. In particular, we show that if $\omega = 2$ or $\omega = 3$ then $W(a, q)$ can assume all possible positive values that are allowable under the above conditions, i.e., $W(a, q)/2$ or $W(a, q)/4$ can be any given positive integer when $\omega = 2$ or $\omega = 3$, respectively. We will then apply our results to the problem of determining values of N such that the period of the continued fraction expansion of $\nu(N)$ has a cyclic structure.

Bernstein [1], [2] seems to have been the first individual to examine the cycle structure of periodic continued fractions to any great extent. He developed a rather complicated definition of a cycle, which resulted from his investigation of the continued fraction expansion of $\sqrt{N}$ for certain parametric families of values of N. However, Nyberg [9], Shanks [11], [12], Yamomoto [18], and Hendy [4] had essentially discovered cycle structures for certain $\sqrt{N}$ or $\nu(N)$ earlier. For example, a result of Hendy is that if $N = (qa^n + (a-1)/q)^2 + 4a^n$, where $a \equiv 1 \pmod{q}$ and $2 \mid qa^n + (a-1)/q$, then

$$\nu(N) = \langle q_0, \overline{q_1, q_2, \ldots, q_p} \rangle,$$

where

$$q_0 = (qa^n + (a-1)/q + 1)/2, \quad q_{2i+1} = qa^i, \quad q_{2i+2} = qa^{n-i-1}$$

for $i = 0, 1, 2, \ldots, n-1$, $q_p = 2q_0 - 1$, $p = p(N) = 2n+1$. Bernstein considered pairs like $\{qa^i, aq^{n-i-1}\}$ $(i = 0, 1, 2, \ldots, n-1)$ to be cycles in the period $q_1, q_2, \ldots, q_p$ of the continued fraction expansion of $\nu(N)$. For the purpose of this paper we will provide a somewhat more restrictive definition of cycles than that of Bernstein.

Let $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_k \subseteq \mathbb{Z}$ and $\mathcal{P} = \mathcal{P}_1 \times \mathcal{P}_2 \times \cdots \times \mathcal{P}_k$ be infinite. Let F be some function defined on $\mathcal{P}$ such that $F : \mathcal{P} \to \mathbb{Z}$ and let

$$\begin{aligned} \mathcal{N} = \{\nu(N) \mid N = F(p_1, p_2, \ldots, p_k), \\ (p_1, p_2, \ldots, p_k) \in \mathcal{P},\ N > 0, \\ N \text{ not a perfect square}\}. \end{aligned}$$

We say that the simple continued fraction expansions of the values of $\nu(N)$ in the family $\mathcal{N}$ have *the structure of cycles of length* c if the periodic part $q_1, q_2, \ldots, q_p$ $(p = p(N))$ of these continued fractions can, for some fixed value of $b \geq 0$, be given by

$$q_{ic+j+b} = f_j(i, p_1, p_2, \ldots, p_k) \quad (i = 0, 1, 2, \ldots, t-1),$$

where $p(N) \equiv b \pmod{c}$, $t \geq 2$, and f_j $(j = 0, 1, 2, \ldots, c-1)$ are c fixed functions such that

$$f_j : \{0, 1, 2, \ldots, t-1\} \times \mathcal{P} \to \mathbb{Z}.$$

A *cycle* in the period of the continued fraction of $\nu(N) \in \mathcal{N}$ is any set

$$\{f_j(i, p_1, p_2, \ldots, p_k) \mid j = 0, 1, 2, \ldots, c-1\}.$$

The restriction that $t \geq 2$ ensures that there are at least two cycles in the period; otherwise, all continued fractions could be considered to have a cycle structure. In the case of Hendy's example, we get $b = 1$, $c = 2$, $f_0(i, a, q, n) = qa^i$, $f_1(i, a, q, n) = qa^{n-i-1}$.

In the families considered by Nyberg, Shanks, Yamomoto, and Hendy, the values of c are either 2 or 6, but Bernstein discovered families for which $c = 4, 5, 6, 8, 10, 11, 12$. Later, his results were extended by Williams [15] and Halter-Koch [3], but no new values of c were found except for $c = 3$. Bernstein expressed surprise that cycles with c as large as 12 exist, but we will show here that even under our more restrictive definition of cycle structure there always exist infinite families $\mathcal{N}$ such that any $\nu(N) \in \mathcal{N}$ has the structure of cycles of length c for any preselected value of $c > 0$.

2. SOME PRELIMINARY RESULTS

In order to determine values for $W(a, q)$, we must find values of a, q such that $a^{\omega} = 1 \pmod{q}$ for a given ω and such that we can predict the values of $E(a^i, q)$. We will do this by making use of some elementary properties of the continued fraction expansion of quadratic irrationals. In developing the material in this action, it is assumed that the reader is familiar with basic results concerning continued fractions which can be found in Perron [10] and Mollin [5] or Stephens and Williams [13], [14], and Williams and Wunderlich [17].

Consider the continued fraction $\langle q_0, q_1, \ldots, q_n, \ldots\rangle$. For a fixed i and j, define $A_{j,i}$ and $B_{j,i}$ by

$$A_{j+1,i} = q_{j+i+1}A_{j,i} + A_{j-1,i},$$
$$B_{j+1,i} = q_{j+i+1}B_{j,i} + B_{j-1,i},$$

where $A_{-2,i} = 0$, $A_{-1,i} = 1$, $B_{-2,i} = 1$, $B_{-1,i} = 0$. Then

$$\frac{A_{j,i}}{B_{j,i}} = \langle q_i, q_{i+1}, \ldots, q_{i+j}\rangle, \tag{2.1}$$

$$\frac{B_{j,i}}{B_{j,i-1}} = \langle q_{i+j}, q_{i+j-1}, \ldots, q_{i+1}\rangle, \tag{2.2}$$

and

$$A_{j,i}B_{j-1,i} - A_{j-1,i}B_{j,i} = (-1)^{j+1}. \tag{2.3}$$

Put $A_j = A_{j,0}$, $B_j = B_{j,0}$. If P, Q, $D \in \mathbb{Z}$, $\phi = (P + \sqrt{D})/Q$, where D is any positive non-square integer and $Q \mid D - P^2$, we put $P_0 = P$, $Q_0 = Q$, $\phi_0 = \phi$, $q_0 = \lfloor \phi_0 \rfloor$. Compute P_n, Q_n, ϕ_n, q_n recursively by $P_n = q_{n-1}Q_{n-1} - P_{n-1}$, $Q_n = (D - P_n^2)/Q_{n-1}$, $\phi_n = (P_n + \sqrt{D})/Q_n$, $q_n = \lfloor \phi_n \rfloor$, and define

$$\begin{aligned} G_{j,i} &= Q_i A_{j,i} - P_i B_{j,i}, \\ G_j &= G_{j,0}. \end{aligned} \tag{2.4}$$

Then ϕ_0 can be written in a continued fraction as $\phi_0 = \langle q_0, q_1, \ldots, q_{n-1}, \phi_n\rangle$ and, in general, ϕ_i can be written as $\phi_i = \langle q_i, q_{i+1}, \ldots, q_{n-1}, \phi_n\rangle$. If we define $\theta_k = \prod_{i=1}^{k-1} \phi_i^{-1}$, then

$$\theta_k = (-1)^{k-1}(A_{k-2} - \phi B_{k-2}) = (-1)^{k-1}(G_{k-2} - \sqrt{D}B_{k-2})/Q_0. \tag{2.5}$$

Denote by $N(\alpha)$ the norm of α. Since

$$N(\theta_k) = (-1)^{k-1}Q_{k-1}/Q_0, \tag{2.6}$$

we can show that

$$\begin{aligned} \frac{G_{j,i} + \sqrt{D}B_{j,i}}{Q_{j+i+1}} &= \prod_{k=i+1}^{j+i+1}(P_k + \sqrt{D})/Q_k \\ &= (-1)^i(G_{i-1} - \sqrt{D}B_{i-1})(G_{i+j} + \sqrt{D}B_{i+j})/(Q_0Q_{i+j+1}); \end{aligned}$$

hence,

$$G_{j,i} + \sqrt{D}B_{j,i} = (-1)^i(G_{i-1} - \sqrt{D}B_{i-1})(G_{i+j} + \sqrt{D}B_{i+j})/Q_0. \tag{2.7}$$

Since $\phi_i = \langle q_i, q_{i+1}, \ldots, q_{i+j}, \phi_{i+j+1}\rangle$, we get

$$\phi_i = \frac{\phi_{i+j+1}A_{j,i} + A_{j-1,i}}{\phi_{i+j+1}B_{j,i} + B_{j-1,i}};$$

on equating rational and irrational parts, we find that

$$\begin{aligned} G_{j,i} &= P_{i+j+1}B_{j,i} + Q_{i+j+1}B_{j-1,i}, \\ DB_{j,i} &= P_{i+j+1}G_{j,i} + Q_{i+j+1}G_{j-1,i}. \end{aligned} \tag{2.8}$$

Let Q_0 be selected such that $Q_0 \mid 2D$. Since $G_i \equiv -P_0B_i \pmod{Q_0}$ for any $i \geq -2$, we get

$$(G_n - \sqrt{D}B_n)(G_m - \sqrt{D}B_m) = G_nG_m + DB_nB_m - (G_nB_m + G_mB_n)\sqrt{D} \equiv 0 \pmod{Q_0};$$

therefore, $(G_n - \sqrt{D}B_n)(G_m - \sqrt{D}B_m)/Q_0 \in \mathbb{Z}[\sqrt{D}]$ for $n, m \geq -2$. Now let $X, Y \in \mathbb{Z}$ and put $m = N(X + \sqrt{D}Y)$. We have the following theorem.

Theorem 2.1: Let $U, T \in \mathbb{Z}$ such that $U + \sqrt{D}T = (G_{i-1} - \sqrt{D}B_{i-1})^2(X + \sqrt{D}Y)/Q_0$ $(i \geq 0)$; then $S = (U + P_iT)/Q_i \in \mathbb{Z}$ and $S^2 \equiv m \pmod{T}$.

Proof: Put

$$\begin{aligned} R + \sqrt{D}S &= -(G_{i-2} - \sqrt{D}B_{i-2})(G_{i-1} - \sqrt{D}B_{i-1})(X + \sqrt{D}Y)/Q_0, \\ R' + \sqrt{D}S' &= (G_{i-2} - \sqrt{D}B_{i-2})^2(X + \sqrt{D}Y)/Q_0, \end{aligned}$$

where $R, S, R', S' \in \mathbb{Z}$. We get

$$\frac{R + \sqrt{D}S}{U + \sqrt{D}T} = -\frac{G_{i-2} - \sqrt{D}B_{i-2}}{G_{i-1} - \sqrt{D}B_{i-1}} = \frac{R' + \sqrt{D}S'}{R + \sqrt{D}S}. \tag{2.9}$$

Now, by (2.5),

$$-\frac{G_{i-2} - \sqrt{D}B_{i-2}}{G_{i-1} - \sqrt{D}B_{i-1}} = \frac{P_i + \sqrt{D}}{Q_i};$$

hence, by equating rational and irrational parts in (2.9), we get $U + P_iT = Q_iS$, $UP_i + TD = Q_iR$, $R + P_iS = Q_iS'$. It follows that

$$Q_i^2S' = UP_i + TD + P_i(U + P_iT) = 2P_iQ_iS + Q_iQ_{i-1}T$$

and

$$S' = (2P_iS + Q_{i-1}T)/Q_i.$$

By (2.6), we have $U^2 - DT^2 = Q_i^2m$; therefore, $(Q_iS - P_iT)^2 - DT^2 = Q_i^2m$, which can be written as $S^2 - TS' = m$. □

We next consider the special cases of $m = 1, -1, -3$. As before, we let P_0, Q_0 be selected such that $Q_0 \mid 2D$ and $Q_0 \mid D - P_0^2$. Denote by π the period length of the continued fraction expansion of $\phi_0 = (P_0 + \sqrt{D})/Q_0$. We know (see, e.g., [13]) that there must exist some minimal $h > 0$ such that either $P_h = P_{h+1}$ or $Q_h = Q_{h+1}$; in the former case, we get $\pi = 2h$ and in the latter, $\pi = 2h + 1$. If $n \equiv h \pmod{\pi}$, put

$$X + Y\sqrt{D} = (G_{n-1} + \sqrt{D}B_{n-1})^2/(Q_0Q_h) \tag{2.10}$$

when $\pi = 2h$, and put

$$X + Y\sqrt{D} = (P_{h+1} + \sqrt{D})(G_{n-1} + \sqrt{D}B_{n-1})^2/(Q_0Q_hQ_{h+1}) \tag{2.11}$$

when $\pi = 2h+1$. It is well known (see, e.g., [10]) that

$$N(X+Y\sqrt{D}) = (-1)^{\pi}. \tag{2.12}$$

From results in Mollin, van der Poorten, and Williams [8], we know that if the Diophantine equation $x^2 - Dy^2 = -3$ is solvable for $x, y \in \mathbb{Z}$, then we must get $Q_{h+1} = P_{h+1} + Q_h$ for some choice of Q_0, where $Q_0 \mid 2D$. We will assume that Q_0 has been so selected. Let $n \equiv h \pmod{\pi}$, then if

$$X + Y\sqrt{D} = (2Q_h - Q_{h+1} + 2\sqrt{D})(G_n + \sqrt{D}B_n)^2 / (Q_0 Q_{h+1}^2), \tag{2.13}$$

we have $X, Y \in \mathbb{Z}$ and

$$N(X+Y\sqrt{D}) = -3. \tag{2.14}$$

If, for example, we have X, Y given by (2.13), we get

$$\begin{aligned} U + \sqrt{D}T &= (G_{i-1} - \sqrt{D}B_{i-1})^2 (X + Y\sqrt{D}) / Q_0 \\ &= ((G_{n-i,i} + \sqrt{D}B_{n-i,i}) / Q_{h+1})^2 (2Q_h - Q_{h+1} + 2\sqrt{D}) \end{aligned}$$

by (2.7). It can be verified after some manipulation involving the identities in (2.8) and the condition $Q_{h+1} = P_{h+1} + Q_h$ that

$$\begin{aligned} U &= 2G_{n-i,i}B_{n-i,i} + G_{n-i,i}B_{n-i-1,i} + G_{n-i-1,i}B_{n-i,i} + 2G_{n-i-1,i}B_{n-i-1,i}, \\ T &= 2(B_{n-i,i}^2 + B_{n-i,i}B_{n-i-1,i} + B_{n-i-1,i}^2). \end{aligned} \tag{2.15}$$

On using (2.4) and (2.3), we get

$$\begin{aligned} S &= (U + P_i T) / Q_i \\ &= 2A_{n-i,i}B_{n-i,i} + A_{n-i,i}B_{n-i-1,i} + A_{n-i-1,i}B_{n-i,i} + 2A_{n-i-1,i}B_{n-i-1,i} \\ &= 2(A_{n-i,i}B_{n-i,i} + A_{n-i-1,i}B_{n-i,i} + A_{n-i-1,i}B_{n-i-1,i}) + (-1)^{n-i+1}. \end{aligned} \tag{2.16}$$

Similarly, we get

$$\begin{aligned} T &= B_{n-i-1,i}B_{n-i,i} + B_{n-i-2,i}B_{n-i-1,i}, \\ S &= B_{n-i-1,i}A_{n-i,i} + B_{n-i-2,i}A_{n-i-1,i}, \end{aligned} \tag{2.17}$$

when X, Y are given by (2.10), and

$$\begin{aligned} T &= B_{n-i,i}^2 + B_{n-i-1,i}^2, \\ S &= A_{n-i,i}B_{n-i,i} + A_{n-i-1,i}B_{n-i-1,i}, \end{aligned} \tag{2.18}$$

when X, Y are given by (2.11).

3. VALUES ASSUMED BY $W(a, q)$

We now need to find a, q such that we can easily compute $E(a^i, q)$ for $i = 1, 2, \ldots, \lfloor \omega / 2 \rfloor$. We first note that $E(a, q) = 1$ if and only if $q \mid a$, and $E(a, q) = 1$ if and only if $a \equiv 1 \pmod{q}$; thus, $W(a, q) = 0$ whenever $\omega = 1$ and $W(a, q) \neq 0$ whenever $\omega > 1$. Indeed, the story concerning the values that $W(a, q)$ can assume when $\omega = 2$ is very different from that when $\omega = 1$. For let T and S be given by (2.17). We have $S^2 \equiv 1 \pmod{T}$ by Theorem 2.1, and

$$\frac{S}{T} = \frac{(B_{n-i-1,i} / B_{n-i-2,i})A_{n-i,i} + A_{n-i-1,i}}{(B_{n-i-1,i} / B_{n-i-2,i})B_{n-i,i} + B_{n-i-1,i}}$$

$$= \langle q_i, q_{i+1}, \cdots, q_n,\ B_{n-i-1,i} / B_{n-i-2,i} \rangle$$
$$= \langle q_i, q_{i+1}, \cdots, q_n,\ q_{n-1}, q_{n-2}, \cdots, q_{i+1} \rangle$$

by (2.1) and (2.2). Thus, $E(S,t) = 2n - 2i - 1 - \chi_{i+1}$, where χ_j is defined by

$$\chi_j = \begin{cases} 0 & \text{when } q_j > 1, \\ 1 & \text{when } q_j = 1. \end{cases}$$

Thus, if $q = T$ and $a \equiv S \pmod{q}$, then

$$W(a,q) = 2\lfloor E(a,q)/2 \rfloor = 2(n-i-1).$$

It is evident that if we put $n = k\pi + h$ then, for any given positive integer x, we can find k, i such that $W(a,q) = 2x$ when $\omega = 2$. Hence, $W(a,q)$ can assume all possible even positive values when $\omega = 2$.

We next consider the case of $\omega = 4$. We let T and S be given by (2.18); we have $S^2 \equiv -1 \pmod{T}$ and

$$\frac{S}{T} = \frac{(B_{n-i,i} / B_{n-i-1,i}) A_{n-i,i} + A_{n-i-1,i}}{(B_{n-i,i} / B_{n-i-1,i}) B_{n-i,i} + B_{n-i-1,i}}$$
$$= \langle q_1, q_{i+1}, \cdots, q_n,\ q_n, q_{n-1}, \cdots, q_{i+1} \rangle.$$

Hence, $E(S,T) = 2n - 2i - \chi_{i+1}$. On putting $q = T$ and $a \equiv S \pmod{q}$, we get

$$W(a,q) = 4\lfloor E(S,T)/2 \rfloor + 2 = 4(n - i - \chi_{i+1}) + 2.$$

For $D = (4fc^2 + c + f)^2 + 4fc + 1$, we get $\sqrt{D} = \langle b, \overline{2c, 2c, 2b} \rangle$ with $b = 4fc^2 + c + f$. In this case, we have $h = 1$, $\pi = 3$, $n = 3r + 1$, $\chi_j = 0$ for all j; hence, $W(a,q) = 4(3r + 1 - i) + 2$. Thus, given any positive $x \equiv 2 \pmod{4}$, we can find values of a, q such that $\omega(a,q) = 4$ and $W(a,q) = x$.

The case of $\omega = 3$ is a little more difficult. We let T and S be given by (2.15) and (2.16) and note that $S^2 \equiv -3 \pmod{T}$. Thus, since $2 \| T$, we have $S \equiv 1 \pmod{2}$ and

$$((S-1)/2)^2 + (S-1)/2 + 1 \equiv 0 \pmod{T/2};$$

it follows that

$$((S-1)/2)^3 \equiv 1 \pmod{T/2}$$

and $\omega((S-1)/2, T) = 3$. Let $n \equiv h \pmod{\pi}$ and put $q_n' = q_n + 1 - \eta$, $q_n'' = q_n + \eta$, where $\eta \in \{0, 1\}$. Then

$$\langle q_i, q_{i+1}, \cdots, q_{n-1}, q_n' \rangle = \frac{A_{n-i,i} + (1-\eta) A_{n-i-1,i}}{B_{n-i,i} + (1-\eta) B_{n-i-1,i}},$$

$$\langle q_n'', q_{n-1}, q_{n-2}, \cdots, q_{i+1} \rangle = q_n'' + \frac{B_{n-i-2,i}}{B_{n-i-1,i}} = \frac{B_{n-i,i}}{B_{n-i-1,i}} + \eta;$$

hence

$$(T/2)\langle q_i, q_{i+1}, \cdots, q_{n-1}, q_n', q_n'', q_{n-1}, \cdots, q_{i+1} \rangle$$
$$= A_{n-i,i} B_{n-i,i} + A_{n-i-1,i} B_{n-i,i} + A_{n-i-1,i} B_{n-i-1,i} + \eta(-1)^{n-i+1}$$
$$= (S + (-1)^{n-i+1}(2\eta - 1))/2$$

by (2.3) and (2.16). Putting $2\eta - 1 = (-1)^{n-i}$, we get

$$\frac{(S-1)/2}{T/2} = \langle q_i, q_{i+1}, \cdots, q_{n-1}, q_n', q_n'', q_{n-1}, \cdots, q_{i+1} \rangle$$

and $E((S-1)/2, T/2) = 2n - 2i - \chi_{i+1}$. If we put $q = T/2$ and $a \equiv (S-1)/2 \pmod{q}$, we see by (1.2) that

$$W(a, q) = 4\lfloor E(a, q)/2 \rfloor = 4(n - i - \chi_{i+1}).$$

We should also observe that, since $Q_{h+1} = Q_h + P_{h+1}$, we have $D = P_{h+1}^2 + P_{h+1}Q_h + Q_h^2$ and $\sqrt{D} < P_{h+1} + Q_h$. It follows that $q_{h+1} = 1$, $P_{h+2} = Q_{h+1} - P_{h+1} = Q_h$, and $Q_{h+2} = P_{h+1}$; hence, $Q_{h+1} = Q_{h+2} + P_{h+2}$. By the symmetry rules $Q_{\pi-i} = Q_i$ and $P_{\pi-i} = P_{i+1}$, we get $Q_{\pi-h-1} = P_{\pi-h-1} + Q_{\pi-h-2}$. Thus, we can replace h by $\pi - h - 2$ and still have $Q_{h+1} = Q_h + P_{h+1}$. It follows that $n - i - \chi_{i+1}$ can be $\equiv h - i - \chi_{i+1}$ or $\equiv -h - 2 - i - \chi_{i+1} \pmod{\pi}$. For example, in the simple case of $D = 21$, $P_0 = 0$, $Q_0 = 1$, we get

$$\sqrt{21} = \langle 4, \overline{1, 1, 2, 1, 1, 8} \rangle$$

with $Q_1 = Q_0 + P_1$ and $Q_5 = Q_4 + P_5$. We have $\pi = 6$ and $n = 6m$ or $n = 6m + 4$, $\chi_1 = 1$, $\chi_2 = 1$, $\chi_3 = 0$, $\chi_4 = 1$, $\chi_5 = 1$, $\chi_6 = 0$. The values of $n - i - \chi_{i+1}$ can be $6m - 1$, $6m - 2$, $6m - 4$, $6m - 5$, $6m - 3$, $6m - 6$, where in the last case $m > 1$; that is, $n - i - \chi_{i+1}$ can take on any positive integral value and therefore $W(a, q)/4$ can take on any positive integral value.

For T, S given by (2.15), (2.16), we also have

$$((S+1)/2)^2 - (S+1)/2 + 1 \equiv 0 \pmod{T/2};$$

hence, $((S+1)/2)^6 \equiv 1 \pmod{T/2}$ and $((S+1)/2)^3 \equiv -1$, $((S+1)/2)^2 \not\equiv 1$, $(S+1)/2 \not\equiv 1 \pmod{T/2}$. We get $\omega((S+1)/2, T/2) = 6$ and

$$W(a, q) = 4\lfloor E(a, q)/2 \rfloor + 4\lfloor E(a^2, q)/2 \rfloor + 2$$

by (1.3) when $q = T/2$ and $a \equiv (S+1)/2 \pmod{T/2}$. Since $a^2 \equiv (S-1)/2 \pmod{T/2}$, the continued fraction expansion for a/q and a^2/q are identical except that the values of q_n' and q_n'' are interchanged. We get

$$W(a, q) = 8(n - i - \chi_{i+1}) + 2$$

and $W(a, q)$ can therefore assume any positive value which is 2 (mod 8), but these need not be the only values that $W(a, q)$ is capable of assuming when $\omega = 6$.

4. CYCLE STRUCTURES

We will now use our earlier results to establish the existence of cycle structures of arbitrary length in the continued fraction period of $\nu(N)$ for $N = (\sigma(qa^n + (a^k - 1)/q))^2 + \sigma^2 a^n$ with certain values of a, q, n, k. We put $n = sk + 1$ $(s \geq 1)$, $k = \omega t$, where $\omega = \omega(a, q)$. Then

$$p(N) = 2(sk + 1) + \omega t + tW = tc + 2,$$

where $W = W(a, q)$ and $c = (2s + 1)\omega + W$.

Let j be any nonnegative integer $\leq n - 1 = sk = \omega st$, and suppose $j = us + r$ $(1 \leq r \leq s)$. We get $kj = un + \omega tr - u$ and $0 < \omega tr - u < \omega st + 1 = n$; thus, $\lambda_j = \omega tr - u < (s-1)\omega t + 1$ when $r < s$. It follows that $\lambda_j < n - k$ if $r < s$; hence, by Lemma 4.5 of [6], $\varepsilon_j = 0$ if $r < s$ or, equivalently, $\varepsilon_j = 0$ if $s \nmid j$. If $s \mid j$, then $r = s$ and $u = j/s - 1 \leq k - 1$. In this case,

$$\lambda_j = \omega rt - u \geq \omega st - (k-1) = (s-1)\omega t + 1 = n - k;$$

thus, $\varepsilon_j = 1$ if and only if $s \mid j$.

We next assume that $j + gs\omega \leq n-1$. We get $k(j+gs\omega) = n(u+\omega g) - u - \omega g + \omega rt$. Now, $\omega rt \leq \omega st = n-1$ and $\omega st \geq j + gs\omega$ or $\omega t \geq u + g\omega + r/s$; hence, $u + g\omega < \omega tr < n$ and

$$\lfloor k(j+gs\omega)/n \rfloor = u + \omega g.$$

It follows that

$$\lambda_{j+gs\omega} = \lambda_j - g\omega.$$

If $j = gs\omega + is$, then $\lambda_j \equiv \lambda_{is} \equiv -i+1 \pmod{\omega}$ and $\rho_j \equiv -i \pmod{\omega}$.

Consider

$$\begin{aligned}\Psi(g) &= \psi((g+1)s\omega + 1) - \psi(gs\omega + 1) \\ &= \sum_{j=gs\omega+1}^{(g+1)s\omega} \psi(j+1) - \psi(j) = \sum_{j=gs\omega+1}^{(g+1)s\omega} (\varepsilon_j m_j + 2) \\ &= 2s\omega + \sum_{i=1}^{\omega} m_{gs\omega+is} = 2s\omega + \omega + W = c,\end{aligned}$$

a value independent of the value of g as long as $(g+1)s\omega \leq n-1 = st\omega$ or $g+1 \leq t$. From this, we can easily establish by induction that $\psi(gs\omega+1) = gc+3$, and since $\varepsilon_j = \varepsilon_{gs\omega+j}$, $m_j = m_{gs\omega+j}$, we can use induction to show that $\psi(gs\omega + j) = gc + \psi(j)$ whenever $g+1 \leq t$ and $j \leq \omega s$.

We now see that the continued fraction expansion of $\nu(N)$ given in Section 1 with $n = sk+1$ $(s \geq 1)$ has

$$\begin{aligned}q_0 &= (qa^n + (a^k - 1)/q)/2 + (\sigma - 1)/\sigma, \\ q_1 &= q_1, \quad q_2 = qa^{n-k}.\end{aligned}$$

If $0 \leq g \leq t-1$, $1 \leq h \leq s\omega$, then

$$q_{\psi(h)+gc} = \begin{cases} qa^{\lambda_h - g\omega} & \text{when } s \nmid h, \\ qa^{\lambda_h - g\omega} + (a^{k-n+\lambda_h - g\omega} - \delta_h)/q & \text{when } s \mid h; \end{cases}$$

furthermore, when $s \nmid h$,

$$q_{\psi(h)+gc+1} = qa^{n-k-\lambda_h + g\omega},$$

and when $s \mid h$,

$$g_{\psi(h)+gc+i} = \begin{cases} b_{i,h} & \text{when } 1 \leq i \leq m_h, \\ qa^{2n-k-\lambda_h+g\omega} + (a^{n-g\omega-\lambda_h} - \delta_h)/q & \text{when } i = m_k + 1, \end{cases}$$

where

$$a^{\rho_h}/q = \langle b_{0,h}, b_{1,h}, \ldots, b_{m_h,h} \rangle.$$

That is, there are c functions $f_j(g,a,q,n,k)$ $(j = 0, 1, 2, \ldots, c-1)$ such that

$$q_{gc+j+3} = f_j(g,a,q,n,k)$$

for $g = 0, 1, \ldots, t-1$. This means that the period of $\nu(N)$ has t cycles of length $c = (2s+1)\omega + W(a,q)$ whenever $n = sk+1 > 1$.

We next show that, given any positive integer c, we can find s, a, q such that

$$c = (2s+1)\omega(a,q) + W(a,q).$$

When c is odd, this is very easy because $W = 0$ whenever $\omega = 1$; thus, we need only put $s = (c-1)/2$, $a = mq+1$. For example, if we have $c = 7$ (a cycle length not previously known), we can put $s = 3, k = t, n = 3k+1, a \equiv 1 \pmod{q}$ and

$$f_0(g,a,q,k) = qa^{k-g}, \quad f_1(g,a,q,k) = qa^{k+g+1},$$
$$f_2(g,a,q,k) = qa^{2k-g}, \quad f_3(g,a,q,k) = qa^{g+1},$$
$$f_4(g,a,q,k) = aq^{3k-g} + (a^{k-g-1}-1)/q,$$
$$f_5(g,a,q,k) = q, \quad f_6(g,a,q,k) = qa^{2k+g+2} + (a^{g+1}-1)/q.$$

We get for $N = (qa^{3k+1} + (a^k - 1)/q)^2 + 4a^{3k+1}$ $(2 \mid a)$ that the periodic part of the continued fraction expansion of $\nu(N)$ is given by $q_{7g+j+3} = f_j(g,a,q,k)$ for $g = 0, 1, 2, \ldots, k-1$.

It is also easy to handle this problem when c is even. Since $2 \mid W(a,q)$, we must have $2 \mid W$. If we put $\omega = 2$, we get $c = 2(2s+1) + W(a,q)$, but we can find a, q such that $W(a,q) = c - 2(2s+1)$ for any $s \geq 1$ such that $c - 2(2s+1) > 0$. Thus, if $c \geq 8$, we can always produce by this technique cycles of length c. We have already seen that examples exist of cycles of length 2, 4, 6.

When, in the case of odd c, we put $\omega = 1$, we are compelled to make s large in order to produce a large cycle length. We can also do this in another way by using $\omega = 3$. In this case, we have $c = 3(2s+1) + W$. Thus, we can keep s small and try to find $W = c - 3(2s+1)$. For example, consider the case of $c = 13$; we put $s = 1$ and must find a, q such that $W(a,q) = 4$. If we use $D = 21, i = 5, n = 6$, we get $n - i - \chi_{i+1} = 1$ and $(S-1)/T = \langle 1, 9, 8 \rangle$. Hence, $(S-1)/2 = 81$ and $T/2 = 73$; and if $a \equiv 8 \pmod{73}$, $q = 73$, we get $\omega(a,q) = 4$. It follows that if $2 \mid a$ and $a \equiv 8 \pmod{73}$, then $\nu(N)$, where

$$N = (73a^{3t+1} + (a^{3t} - 1)/73)^2 + 4a^{3t+1}$$

has a cycle length of 13. This cycle is given by $q_{13g+j+3} = f_j(g,a,t)$, where

$$f_0(g,a,t) = 73a^{3t-3g} + (a^{3t-1-3g} - 64)/73,$$
$$f_1(g,a,t) = 1, \quad f_2(g,a,t) = 7, \quad f_3(g,a,t) = 9,$$
$$f_4(g,a,t) = 73a^{3g+2} + (a^{3g+1} - 8)/73,$$
$$f_5(g,a,t) = 73a^{3t-3g-1} + (a^{3t-3g-2} - 8)/73,$$
$$f_6(g,a,t) = 9, \quad f_7(g,a,t) = 7, \quad f_8(g,a,t) = 1,$$
$$f_9(g,a,t) = 73a^{3g+3} + (a^{3g+2} - 64)/73,$$
$$f_{10}(g,a,t) = 73a^{3t-3g-2} + (a^{3t-3g-3} - 1)/73,$$
$$f_{11}(g,a,t) = 73, \quad f_{12}(g,a,t) = 73a^{3g+4} + (a^{3g+3} - 1)/73.$$

A more extreme example is provided by putting $i = 0$, $n = 12$. We get $n - i - \chi_{i+1} = 11$, $\eta = 1$,

$$(S-1)/T = \langle 4,1,1,2,1,1,8,1,1,2,1,1,8,9,1,1,2,1,1,8,1,1,2,2 \rangle$$
$$= 664670164/1450042921.$$

Thus, if

$$N = (1450042921a^{6t+1} + (a^{3t} - 1)/1450042921)^2 + 4a^{6t+1},$$

where $a \equiv 84498480 \pmod{1450042921}$ and $2 \mid a$, then $v(N)$ has a cycle structure with cycle length

$$c = W + (2s+1)\omega = 44 + 15 = 59.$$

REFERENCES

1. L. Bernstein. "Fundamental Units and Cycles." *J. Number Theory* **8** (1976):446-91.
2. L. Bernstein. "Fundamental Units and Cycles in the Period of Real Quadratic Fields, Part II." *Pacific J. Math.* **63** (1976):63-78.
3. F. Halter-Koch. "Einige periodische Kettenbruchentwicklungen und Grundeinheiten quadratischer Ordnung." *Abh. Math. Sem. Univ. Hamburg* **59** (1989):157-69.
4. M. D. Hendy. "Applications of a Continued Fraction Algorithm to Some Class Number Problems." *Math. Comp.* **28** (1974):267-77.
5. R. A. Mollin. *Quadratics*. Boca Raton: CRC Press, 1996.
6. R. A. Mollin & H. C. Williams. "Consecutive Powers in Continued Fractions." *Acta Arith.* **61** (1992):233-64.
7. R. A. Mollin & H. C. Williams. "On the Period Length of Some Special Continued Fractions." *Sém. Théorie des Nombres de Bordeaux* **4** (1992):19-42.
8. R. A. Mollin, A. J. van der Poorten, & H. C. Williams. "Halfway to a Solution of $x^2 - Dy^2 = -3^n$." *J. de Théorie des Nombres* **6** (1994):421-59.
9. M. Nyberg. "Culminating and Almost Culminating Continued Fractions." *Norsk. Mat. Tidsskr.* **31** (1949):95-99.
10. O. Perron. *Die Lehre von der Kettenbrüchen*. Stuttgart: Teubner, 1977.
11. D. Shanks. "On Gauss's Class Number Problems." *Math. Comp.* **23** (1969):151-63.
12. D. Shanks. "Class Number: A Theory of Factorization and Genera." In *Proc. Sympos Pure Math 20*, pp. 415-40. Providence, RI: American Mathematical Society, 1971.
13. A. J. Stephens & H. C. Williams. "Some Computational Results on a Problem Concerning Powerful Numbers." *Math. Comp.* **50** (1988):619-32.
14. A. J. Stephens & H. C. Williams. "Computation of Real Quadratic Fields with Class Number One." *Math. Comp.* **51** (1988):809-24.
15. H. C. Williams. "A Note on the Period Length of the Continued Fraction Expansion of Certain $\sqrt{D}$." *Utilitas Math.* **28** (1985):201-09.
16. H. C. Williams. Some Generalizations of the S_n Sequence of Shanks." *Acta. Arith.* **69** (1995):199-215.
17. H. C. Williams & M. C. Wunderlich. "On the Parallel Generation of the Residues for the Continued Fraction Factoring Algorithm." *Math. Comp.* **177** (1987):405-23.
18. Y. Yamomoto. "Real Quadratic Fields with Large Fundamental Units." *Osaka J. Math.* **8** (1971):261-70.

AMS Classification Number: 11A55

❖❖❖

UNIQUENESS OF REPRESENTATIONS BY MORGAN-VOYCE NUMBERS

A. F. Horadam
The University of New England, Armidale, Australia 2351
(Submitted June 1998)

1. MORGAN-VOYCE NUMBERS

Consider the recurrence

$$X_{n+2} = 3X_{n+1} - X_n \tag{1.1}$$

with

$$X_0 = a, \ X_1 = b \ (a, b \text{ integers}). \tag{1.2}$$

Morgan-Voyce numbers B_n, b_n, and their related numbers C_n, c_n are then generated according to the following scheme in which F_n, L_n symbolize the n^{th} Fibonacci and n^{th} Lucas numbers, respectively:

	X_n	a	b	$X_n = F_m, L_m$
(B)	B_n	0	1	F_{2n}
(b)	b_n	1	1	F_{2n-1}
(C)	C_n	2	3	L_{2n}
(c)	c_n	−1	1	L_{2n-1}

(1.3)

Readers are encouraged to determine the first few members of each of these sequences. In particular, $\{B_n\} = 0, 1, 3, 8, 21, 55, \ldots$.

The sets of numbers (1.3) are special cases of the corresponding sets of polynomials $B_n(x)$, $b_n(x)$, $C_n(x)$, $c_n(x)$ [2] when $x = 1$.

2. REPRESENTATIONS BY B_n

Next, consider the representation of positive integers N by means of B_n:

$$N = \sum_{i=1}^{n} \alpha_i \beta_i \quad (\alpha_i = 0, 1, 2). \tag{2.1}$$

Of special interest is the case as in [3] in which all the α_i in (2.1) are 1, giving rise to the numbers 1, 4, 12, 33, ..., i.e.,

$$\sum_{i=1}^{n} B_i = F_{2n+1} - 1. \tag{2.2}$$

A *minimal representation* is indicated in the abbreviated table (Table 1) in which an empty space signifies 0 (zero). This table has already appeared in [3]. An essential feature of this representation proved in [3] is that no two successive terms in the summation have coefficient 2.

TABLE 1. Minimal Representation for $\{B_n\}$: $n = 1, 2, 3, 4$

N	B_1	B_2	B_3	B_4	N	B_1	B_2	B_3	B_4	N	B_1	B_2	B_3	B_4
	1	3	8	21		1	3	8	21		1	3	8	21
1	1				13	2	1	1		24		1		1
2	2				14		2	1		25	1	1		1
3		1			15	1	2	1		26	2	1		1
4	1	1			16			2		27		2		1
5	2	1			17	1		2		28	1	2		1
6		2			18	2		2		29			1	1
7	1	2			19		1	2		30	1		1	1
8			1		20	1	1	2		31	2		1	1
9	1		1		21				1	32		1	1	1
10	2		1		22	1			1	33	1	1	1	1
11		1	1		23	2			1	34	2	1	1	1
12	1	1	1							35		2	1	1

Is this representation unique?

Write S_k for the set of digits 0, 1, 2 of length k in the representation. Let

$$\begin{cases} N_k^{\min} = \text{the smallest integer in } S_k, \\ N_k^{\max} = \text{the largest integer in } S_k, \\ R_k = \text{the range of integers in } S_k, \\ I_k = \text{the number of integers in } S_k. \end{cases} \tag{2.3}$$

Then we readily construct the following scheme (Table 2).

TABLE 2. B_n Representation Summary

k	S_k	R_k	$N_k^{\min}$	$N_k^{\max}$	I_k
1	S_1	1, 2	B_1	$B_2 - 1$	$2 = F_3$
2	S_2	3, ..., 7	B_2	$B_3 - 1$	$5 = F_5$
3	S_3	8, ..., 20	B_3	$B_4 - 1$	$13 = F_7$
4	S_4	21, ..., 54	B_4	$B_5 - 1$	$34 = F_9$
⋮	⋮	⋮	⋮	⋮	⋮
k	S_k	$F_{2k}, \ldots, F_{2k+2} - 1$	$B_k = F_{2k}$	$B_{k+1} - 1 = F_{2k+2} - 1$	F_{2k+1}

Clearly, $I_k = N_k^{\max} - N_k^{\min} + 1 = F_{2k+2} - F_{2k} = F_{2k+1}$.
In each block of length k in Table 1,

$$\begin{cases} \text{the smallest number is necessarily } (0, 0, 0, \ldots, 1), \text{ and} \\ \text{the largest number is necessarily } (0, 0, 0, \ldots, 2). \end{cases} \tag{2.4}$$

Lemma 1: $B_n \le N \le B_{n+1} - 1$.

E.g., $B_8 (= 987) \le N = 1000 \le B_9 - 1 (= 2583)$.

Lemma 2: k is uniquely determined by N.

E.g., $N = 1000 \Rightarrow k = 5$.

Combining the above information, we deduce that

Theorem 1: Every positive integer N has a unique representation of the form

$$N = \sum_{i=1}^{\infty} \alpha_i B_i,$$

where [3] two successive values α_i, α_{i+1} cannot both be 2.

The distinctive pattern fixed in Tables 1 and 2 determines the uniqueness of the representation.

A tabular schedule similar to that in Table 1 (but suppressed here for the sake of brevity) ought now to be constructed for maximal representations by B_n. The embargo on the appearance of two successive coefficients in the summation with the value 2, as in the enunciation of Theorem 1, naturally does not apply for maximality. A fixed pattern of the coefficients emerges in the tabulation of maximal representations for B_n, leading to the conviction that the maximal representation is unique. Where this situation differs from that, say, for Pell numbers [1], is that, while (2.2) in which all coefficients are 1 is there common to both minimal and maximal representations, other summations here are common to both which do not belong to (2.2), e.g., $5 = 2B_1 + B_2$. Also see [3] in this context.

3. OTHER REPRESENTATIONS

(i) C_n (lacunary)

Coming now to the companion number set $\{C_n\} = 2, 3, 7, 18, 47, \ldots$ to $\{B_n\}$, i.e., (1.3)(C), we find that the even tenor of our progress is disrupted. For a start, $C_0 = 2$, $C_1 = 3$, so that there is no possible representation of 1 (unity). Thus, any representation is necessarily *lacunary*. It is no good appealing to C_{-1} as an accommodating adjunct to the set $\{C_n\}$ since $C_{-1} = 3$ (indeed, $C_{-n} = C_n$).

Because of this hiatus, there is also no member in the pattern of the minimal representation of, say, 8 though it can be represented maximally as $8 = 2C_0 + 2C_1$, in which there occur two successive coefficients equal to 2. Except for the lacuna at $N = 1$, the potentially fixed minimal pattern is negated in a regular way at $C_n = 1$, $n \geq 2$. The nature of the representation is therefore hybrid.

(ii) b_n

Turning now to the Morgan-Voyce numbers $\{b_n\}$: 1, 2, 5, 13, 34, ..., we encounter a similar set of circumstances to those for $\{B_n\}$. Arguments paralleling those employed in the previous section are likewise applicable to this context. Analogously to Table 1, a *minimal representation* table may be constructed (an entertaining and instructive pastime). As for B_n, the proscription of two successive coefficients equal to 2 in a minimal representation applies here also.

For comparison with the Table 2 Summary for B_n, we here append a Summary (Table 3) for b_n, in which non-capital symbols correspond to the capital symbols specified in (2.3).

TABLE 3. b_n Representation Summary

k	s_k	r_k	$n_k^{\min}$	$n_k^{\max}$	i_k
1	s_1	1	b_1	b_2-1	F_2
2	s_2	$2,\ldots,4$	b_2	b_3-1	F_4
3	s_3	$5,\ldots,12$	b_3	b_4-1	F_6
4	s_4	$13,\ldots,33$	b_4	b_5-1	F_8
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
k	s_k	$F_{2k-1},\ldots,F_{2k+1}-1$	b_k	$b_{k+1}-1$	F_{2k}

Observe that, by (1.3), $i_k=(b_{k+1}-1)-(b_k)+1=b_{k+1}-b_k=F_{2k+1}-F_{2k-1}=F_{2k}$. Uniqueness of the minimal representation is determined by the fixedness of the pattern.

(iii) c_n

Some initial comfort is offered here by the fact that $1=c_1$, $2=2c_1$. But to represent the number 3, we need to revert to the subterfuge of including $-1=c_{-1}$ ($c_{-n}=c_n$ in fact) in our set $\{c_n\}$. This implies that a representation exists which is non-lacunary. There is a purposefulness about the coefficients which then suggests minimality and uniqueness.

4. CONCLUDING OBSERVATIONS

Write

$$\mathcal{B}_n=\sum_{i=1}^{n}B_i\ (2.2),\quad \mathbf{b}_n=\sum_{i=1}^{n}b_i,\quad \mathcal{C}_n=\sum_{i=0}^{n-1}C_i,\quad \mathbf{c}_n=\sum_{i=1}^{n}c_i.$$

Then we discover the following schedule (cf. (1.3)):

	Fibonacci Equivalence	Recurrence Relation
$\mathcal{B}_n$	$F_{2n+1}-1$	$\mathcal{B}_{n+2}=3\mathcal{B}_{n+1}-\mathcal{B}_n-1$
$\mathbf{b}_n$	F_{2n}	$\mathbf{b}_{n+2}=3\mathbf{b}_{n+1}-\mathbf{b}_n$
$\mathcal{C}_n$	$L_{2n+1}-1$	$\mathcal{C}_{n+2}=3\mathcal{C}_{n+1}-\mathcal{C}_n-1$
$\mathbf{c}_n$	$L_{2n}-2$	$\mathbf{c}_{n+2}=3\mathbf{c}_{n+1}-\mathbf{c}_n+2$

Aspects of $\mathcal{B}_n$ and $\mathcal{C}_n$ are discussed in [3], while features of $\mathbf{b}_n$ and $\mathbf{c}_n$ are analyzed in [4].

Peripherally of import to this paper, but also to provide some publicity for the concept, we mention *Brahmagupta polynomials* [5] which relate to $B_n(x)$ and $b_n(x)$ [5], and to $C_n(x)$ and $c_n(x)$ [4]. Historical information on Brahmagupta and his mathematics is given in some detail in [6].

REFERENCES

1. A. F. Horadam. "Minmax Sequences for Pell Numbers." In *Applications of Fibonacci Numbers* **6**:231-49. Ed. G. E. Bergum, A. N. Philippou, & A. F. Horadam. Dordrecht: Kluwer, 1996.
2. A. F. Horadam. "New Aspects of Morgan-Voyce Polynomials." In *Applications of Fibonacci Numbers* **7**:161-76. Ed. G. E. Bergum, A. N. Philippou, & A. F. Horadam. Dordrecht: Kluwer, 1998.

3. A. F. Horadam. "Unit Coefficients Sums for Certain Morgan-Voyce Numbers." *Notes on Number Theory and Discrete Mathematics* **3.3** (1997):117-27.
4. A. F. Horadam.. "Representation Grids for Certain Morgan-Voyce Numbers." *The Fibonacci Quarterly* **37.4** (1999):320-25.
5. E. R. Suryanarayan. "The Brahmagupta Polynomials." *The Fibonacci Quarterly* **34.3** (1996):30-39.
6. A. Weil. *Number Theory: An Approach Through History: From Hammurapi to Legendre*. Boston: Birkhäuser, 1984.

AMS Classification Number: 11B37

❖❖❖

Announcement

NINTH INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS

July 17-July 22, 2000

Institut Supérieur de Technologie
Grand Duché de Luxembourg

LOCAL COMMITTEE

J. Lahr, Chairman
R. André-Jeannin
M. Malvetti
C. Molitor-Braun
M. Oberweis
P. Schroeder

INTERNATIONAL COMMITTEE

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

LOCAL INFORMATION

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

PROFESSOR JOSEPH LAHR
Institut Supérior de Technologie
6, rue R. Coudenhove-Kalergi
L-1359 Luxembourg
e-mail: joseph.lahr@ist.lu
Fax: (00352) 432124 Phone: (00352) 420101-1

CALL FOR PAPERS

Papers on all branches of mathematics and science related to the Fibonacci numbers, number theoretic facts as well as recurrences and their generalizations are welcome. Abstracts, which should be sent in duplicate to F. T. Howard at the address below, are due by June 1, 2000. An abstract should be at most one page in length (preferably half a page) and should contain the author's name and address. New results are especially desirable; however, abstracts on work in progress or results already accepted for publication will be considered. Manuscripts should *not* be submitted. Questions about the conference should be directed to:

PROFESSOR F. T. HOWARD
Wake Forest University
Box 7388 Reynolda Station
Winston-Salem, NC 27109 (U.S.A.)
e-mail: howard@mthcsc.wfu.edu

OBTAINING NEW DIVIDING FORMULAS $n|Q(n)$ FROM THE KNOWN ONES

Bau-Sen Du
Institute of Mathematics, Academia Sinica, Taipei, Taiwan, 11529, R.O.C.
e-mail: mabsdu@sinica.edu.tw
(Submitted July 1998-Final Revision April 1999)

1. INTRODUCTION

In [8], Lin introduced a well-known result (i.e., Theorem 3.1) from discrete dynamical systems theory (which he called "iterated maps") concerning the number of period-n points. As applications, Lin computed the number $N(n)$ of period-n points of the maps $B(\mu, x)$ for some suitably chosen μ and obtained some interesting dividing formulas $n|N(n)$ (i.e., formulas (4.23) in [8]) which had already been obtained in [6, Theorem 3] from different maps. As mentioned in [8], each iterated map contributes an $N(n)$ and, hence, *in principle*, infinitely many $N(n)$ can be obtained. However, in practice, to actually compute $N(n)$ is not so easy as was demonstrated in [8]. Lin did not mention how to compute explicit formulas for $N(n)$ other than the one for the special maps $B(\mu, x)$, where the method he used does not seem to apply to other maps easily. In this note, we want to point out that a simple systematic way of constructing functions $Q(n)$ such that $n|Q(n)$ has already been introduced in [2]-[7] (see also [9]) for a large class of *continuous* maps from a compact interval into itself and examples of various $Q(n)$ can also be found in [4]-[7]. Furthermore, we want to present a few methods (Theorems 1-3) from discrete dynamical systems theory of obtaining new functions $Q(n)$ from the known ones so that many more $Q(n)$ can be constructed (see, e.g., Theorem 4). Finally, in [8], Lin only considered the numbers of period-n points for iterated maps. He did not mention the numbers of *symmetric* period-$(2n)$ points. Therefore, we also include such examples in Theorem 5.

2. SOME DEFINITIONS

Since our main results are taken from discrete dynamical systems theory, we shall use the notations commonly used there (see also [4]-[7]). For completeness, we include the definitions of $\Phi_i(\phi, n)$, $i = 1, 2$, below. Let $\phi(n)$ be an integer-valued function defined on the set of all positive integers. If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, where the p_i's are distinct prime numbers, r and the k_i's are positive integers, we let $\Phi_1(\phi, 1) = \phi(1)$ and let

$$\Phi_1(\phi, n) = \phi(n) - \sum_{i=1}^{r} \phi\left(\frac{n}{p_i}\right) + \sum_{i_1<i_2} \phi\left(\frac{n}{p_{i_1}p_{i_2}}\right) - \sum_{i_1<i_2<i_3} \phi\left(\frac{n}{p_{i_1}p_{i_2}p_{i_3}}\right)$$
$$+ \cdots + (-1)^r \phi\left(\frac{n}{p_1 p_2 \cdots p_r}\right),$$

where the summation $\sum_{i_1<i_2<\cdots<i_j}$ is taken over all integers $i_1, i_2, \ldots, i_j$ with $1 \le i_1 < i_2 < \cdots < i_j \le r$. If $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, where the p_i's are distinct odd prime numbers and $k_0 \ge 0, r \ge 1$, and the k_i's ≥ 1 are integers, we let

$$\Phi_2(\phi, n) = \phi(n) - \sum_{i=1}^{r} \phi\left(\frac{n}{p_i}\right) + \sum_{i_1<i_2} \phi\left(\frac{n}{p_{i_1}p_{i_2}}\right) - \sum_{i_1<i_2<i_3} \phi\left(\frac{n}{p_{i_1}p_{i_2}p_{i_3}}\right)$$
$$+ \cdots + (-1)^r \phi\left(\frac{n}{p_1 p_2 \cdots p_r}\right).$$

If $n = 2^k$, where $k \geq 0$ is an integer, we let $\Phi_2(\phi, n) = \phi(n) - 1$.

3. MAIN RESULTS

Let S be a nonempty set and let f be a function from S into itself. *In the sequel*, for every positive integer n, we let $\phi_f(n)$ denote the number (if finite) of distinct solutions of the equation $f^n(x) = x$ in S, where f^n denotes the n^{th} iterate of $f: f_1 = f$ and $f^n = f \circ f^{n-1}$ for $n > 1$. By standard inclusion-exclusion arguments, it is easy to see that, for each positive integer n, $\Phi_1(\phi_f, n)$ is the number of periodic points of f with least period n. On the other hand, if S contains the origin and g is an odd function from S into itself, we let $\psi_g(n)$ denote the number (if finite) of distinct solutions of the equation $g^n(x) = -x$. In this case, if $g^n(y) = -y$, then $g^{kn}(y) = (g^n)^k(y) = -y$ for every odd integer $k \geq 1$ and $g^{mn}(y) = (g^n)^m(y) = y$ for every even integer $m \geq 1$. So, it is again easy to see, by the same inclusion-exclusion arguments, that $\Phi_2(\psi_g, n)$ is the number of symmetric periodic points (i.e., periodic points whose orbits are symmetric with respect to the origin) of g with least period $2n$. Consequently, we have $\Phi_1(\phi_f, n) \equiv 0 \pmod{n}$ and $\Phi_2(\psi_g, n) \equiv 0 \pmod{2n}$ for all positive integers n. Therefore, by letting $Q(n) = \Phi_1(\phi_f, n)$ or $Q(n) = \Phi_2(\psi_g, n)$, we obtain that $n \mid Q(n)$ for all positive integers n. In the following, we shall present a few methods (Theorems 1-3) from discrete dynamical systems theory of obtaining new functions $Q(n)$ from the known ones so that many more $Q(n)$ can be constructed.

Since $\Phi_1(\phi, n)$ is linear in ϕ [note that $\Phi_2(\psi, n)$ is not linear in ψ because of its definition on $n = 2^k$], we easily obtain the following result.

Theorem 1: Let φ_i, $i = 1, 2$, be integer-valued functions defined on the set of all positive integers. If, for all positive integers n, $\Phi_1(\varphi_1, n) \equiv 0 \pmod{n}$ and $\Phi_1(\varphi_2, n) \equiv 0 \pmod{n}$, then, for any fixed integers k and m, $\Phi_1(k\varphi_1 + m\varphi_2, n) = k\Phi_1(\varphi_1, n) + m\Phi_1(\varphi_2, n) \equiv 0 \pmod{n}$ for all positive integers n.

Let f and f_i, $1 \leq i \leq j$, be functions from S into itself and let $(\prod_{i=1}^{j} \phi_{f_i})(n) = \prod_{i=1}^{j} \phi_{f_i}(n)$ for all positive integers n. If h is a function from S into itself defined by $h(x) = f^k(x)$, then, since $h^n(y) = y$ if and only if $f^{kn}(y) = y$, we obtain that $\phi_h(n) = \phi_f(kn)$. On the other hand, if H is a function from the Cartesian product set S^j into itself defined by $H(x_1, x_2, \ldots, x_j) = (f_1(x_1), f_2(x_2), \ldots, f_j(x_j))$, then, since $(y_1, y_2, \ldots, y_j) = H^n(y_1, y_2, \ldots, y_j) = (f_1^n(y_1), f_2^n(y_2), \ldots, f_j^n(y_j))$ if and only if $y_i = f_i^n(y_i)$ for all $1 \leq i \leq j$, we obtain that $\phi_H(n) = (\prod_{i=1}^{j} \phi_{f_i})(n)$. If S contains the origin and all f and f_i, $1 \leq i \leq j$, are also odd functions, then so are h (when k is odd) and H. Arguments similar to the above also show that $\psi_H(n) = (\prod_{i=1}^{j} \psi_{f_i})(n) = \prod_{i=1}^{j} \psi_{f_i}(n)$. Therefore, we obtain the following results.

Theorem 2: Let f and f_i, $1 \le i \le j$, be functions from S into itself. Then the following hold:

(a) For any fixed positive integer k, let $\varphi_k(n) = \phi_f(kn)$. Then $\Phi_1(\varphi_k, n) \equiv 0 \pmod{n}$ for all positive integers n.

(b) $\Phi_1(\prod_{i=1}^{j} \phi_{f_i}, n) \equiv 0 \pmod{n}$ for all positive integers n.

Theorem 3: Assume that the set S contains the origin and let g and g_i, $1 \le i \le j$, be odd functions from S into itself. Then the following hold:

(a) For any fixed odd integer $k > 0$, let $\psi_k(n) = \psi_g(kn)$. Then $\Phi_2(\psi_k, n) \equiv 0 \pmod{2n}$ for all positive integers n.

(b) $\Phi_2(\prod_{i=1}^{j} \psi_{g_i}, n) \equiv 0 \pmod{2n}$ for all positive integers n.

Remark: Note that in Theorem 1 we only require φ_i to satisfy $\Phi_1(\varphi_i, n) \equiv 0 \pmod{n}$, while in Theorems 2 and 3 we require them to be the numbers of (symmetric, respectively) periodic points of all periods for some (odd, respectively) maps. It would be interesting to know if these stronger requirements in Theorems 2 and 3 can be loosened.

4. SOME EXAMPLES

In [6] we show that, for any fixed integer $j \ge 2$, if $\varphi_j(n) = 2^n - 1$ for $1 \le n \le j$ and $\varphi_j(n) = \sum_{i=1}^{j} \varphi_j(n-i)$ for $j < n$, then φ_j satisfies the congruence identities $\Phi_1(\varphi_j, n) \equiv 0 \pmod{n}$ for all positive integers n. Since the constant functions also satisfy the same congruence identities, it follows from Theorem 1 that, for any fixed integers j, k, and m with $j \ge 2$, if $\phi_{j,k,m}(n) = m\varphi_j(n) + k$ for all positive integers n, then $\Phi_1(\phi_{j,k,m}, n) \equiv 0 \pmod{n}$ for all positive integers n. Since it is easy to see that $\phi_{j,k,m}$ also satisfies the recursive formula $\phi_{j,k,m}(n) = m(2^n - 1) + k$ for $1 \le n \le j$ and $\phi_{j,k,m}(n) = \left(\sum_{i=1}^{j} \phi_{j,k,m}(n-i)\right) - (j-1)k$ for $j < n$, we have the following result.

Theorem 4: For any fixed integers j, k, and m with $j \ge 2$, let

$$\phi_{j,k,m}(n) = \begin{cases} m(2^n - 1) + k, & \text{for } 1 \le n \le j, \\ \left(\sum_{i=1}^{j} \phi_{j,k,m}(n-i)\right) - (j-1)k, & \text{for } j < n. \end{cases}$$

Then $\Phi_1(\phi_{j,k,m}, n) \equiv 0 \pmod{n}$ for all positive integers n.

The following is an example of $\Phi_2(\psi, n) \equiv 0 \pmod{2n}$. For other examples see [5] and [7]. By Theorem 3 above, many more examples can be generated easily from these known ones.

Theorem 5: Let $j \ge 2$ be a fixed integer and let $g_j(x)$ be the continuous map from $[-j, j]$ onto itself defined by

$$g_j(x) = \begin{cases} x+1, & \text{for } -j \le x \le -2, \\ j, & \text{for } x = -1, \\ -j, & \text{for } x = 1, \\ x-1, & \text{for } 2 \le x \le j, \\ \text{linear}, & \text{on each of the intervals } [-2,-1], [-1,1], [1,2]. \end{cases}$$

We let $\phi_j(n)$ be defined by

$$\phi_j(n) = \begin{cases} 3^n - 2, & \text{for } 1 \le n \le j, \\ 3^n - 2 - 4n \cdot 3^{n-j-1}, & \text{for } j+1 \le n \le 2j-1, \\ \sum_{i=1}^{j}(2i-1)\phi_j(n-i) + \sum_{i=j+1}^{2j-1}(4j-2i-1)\phi_j(n-i), & \text{for } 2j \le n. \end{cases}$$

We also let $\psi_j(n)$ be defined by

$$\psi_j(n) = \begin{cases} 3^n, & \text{for } 1 \le n \le j-1, \\ 3^j - 2j, & \text{for } n = j, \\ 3^n - 4n \cdot 3^{n-j-1}, & \text{for } j+1 \le n \le 2j-1, \\ \sum_{i=1}^{j}(2i-1)\psi_j(n-i) + \sum_{i=j+1}^{2j-1}(4j-2i-1)\psi_j(n-i), & \text{for } 2j \le n. \end{cases}$$

Then, for any integer $j \ge 2$, the following hold:

(a) For any positive integer n, $\phi_j(n)$ is the number of distinct solutions of the equation $g_j^n(x) = x$ in $[-j, j]$. Consequently, $\Phi_1(\phi_j, n) \equiv 0 \pmod{n}$ for all positive integers n.

(b) For any positive integer n, $\psi_j(n)$ is the number of distinct solutions of the equation $g_j^n(x) = -x$ in $[-j, j]$. Consequently $\Phi_2(\psi_j, n) \equiv 0 \pmod{2n}$ for all positive integers n.

Remark: Numerical computations suggest that the functions $\psi_j(n)$ in Theorem 5 also satisfy $\Phi_1(\psi_j, n) \equiv 0 \pmod{n}$ for all positive integers n. However, we are unable to verify this.

5. OUTLINE OF THE PROOF OF THEOREM 5

The proof of Theorem 5 is based on the method of symbolic representations which is simple and easy to use. For a description of this method, we refer the reader to, say, Section 2 of [6]. Here we only give an outline of the proof. We shall also use the terminology introduced there. In the following, we shall assume that $j > 2$. The case $j = 2$ can be proved similarly.

Lemma 6: Under g_j, we have:

$$\begin{cases} (-j)1 \to (-(j-1))(-(j-2)) \cdots (-3)(-2)(-1)j(-j), \\ 1(-j) \to (-j)j(-1)(-2)(-3) \cdots (-(j-2))(-(j-1)), \\ (i-1)i \to i(i+1) \text{ and } i(i-1) \to (i+1)i, \text{ for } -(j-2) \le i \le -2, \\ (-2)(-1) \to (-1)j \text{ and } (-1)(-2) \to j(-1), \\ (-j)j \to (-(j-1))(-(j-2)) \cdots (-3)(-2)(-1)j(-j)123 \cdots (j-2)(j-1), \\ j(-j) \to (j-1)(j-2) \cdots 321(-j)j(-1)(-2)(-3) \cdots (-(j-2))(-(j-1)), \\ 12 \to (-j)1 \text{ and } 21 \to 1(-j), \\ i(i+1) \to (i-1)i \text{ and } (i+1)i \to i(i-1) \text{ for } 2 \le i \le j-2, \\ j(-1) \to (j-1)(j-2) \cdots 321(-j)j, \\ (-1)j \to j(-j)123 \cdots (j-2)(j-1). \end{cases}$$

In the following, when we say the representation for $y = g_j^n(x)$, we mean the representation obtained, following the procedure as described in Section 2 of [6], by applying Lemma 6 to the representation $(-(j-1))(-(j-2)) \cdots (-3)(-2)(-1)j(-j)123 \cdots (j-2)(j-1)$ for $y = g_j(x)$ successively until we get to the one for $y = g_j^n(x)$.

For every positive integer n and all integers k, i with $-(j-1) \le k \le j-1$ and $-(j-1) \le i \le j-1$, let $a_{n,k,i,j}$ denote the number of uv's and vu's in the representation for $y = g_j^n(x)$ whose corresponding x-coordinates are in the interval $[s_k, t_k]$, where

$$[s_k, t_k] = \begin{cases} [k-1, k], & \text{for } -(j-1) \le k \le -1, \\ [-1, 1], & \text{for } k = 0, \\ [k, k+1], & \text{for } 1 \le k \le j-1, \end{cases} \quad \text{and} \quad uv = \begin{cases} (-j)1, & \text{for } i = -(j-1), \\ (i-1)i, & \text{for } -(j-2) \le i \le -1, \\ (-j)j, & \text{for } i = 0, \\ i(i+1), & \text{for } 1 \le i \le j-2, \\ j(-1), & \text{for } i = j-1. \end{cases}$$

We also define $c_{n,j}$ and $d_{n,j}$ by letting

$$c_{n,j} = \sum_{k=-(j-1)}^{j-1} a_{n,k,k,j} + \sum_{k=1}^{j-1} (a_{n,-k,0,j} + a_{n,k,0,j}) + \sum_{k=0}^{j-2} (a_{n,-k,-(j-1),j} + a_{n,k,j-1,j})$$

and

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

It is easy to see that, for every positive integer n, $c_{n,j}$ is the number of distinct solutions of the equation $g_j^n(x) = x$ and $d_{n,j}$ is the number of distinct solutions of the equation $g_j^n(x) = -x$.

Now, from Lemma 6 above, we find that these sequences $\langle a_{n,k,i,j} \rangle$ can be computed recursively.

Lemma 7: For every positive integer n and all integers k with $-(j-1) \le k \le j-1$, we have

$$\begin{cases} a_{n+1,k,-(j-1),j} = a_{n,k,0,j} + a_{n,k,1,j} + a_{n,k,j-1,j}, & \\ a_{n+1,k,-(j-2),j} = a_{n,k,0,j} + a_{n,k,-(j-1),j}, & \\ a_{n+1,k,i,j} = a_{n,k,i-1,j} + a_{n,k,0,j} + a_{n,k,-(j-1),j}, & -(j-3) \le i \le -1, \\ a_{n+1,k,0,j} = a_{n,k,-(j-1),j} + a_{n,k,0,j} + a_{n,k,j-1,j}, & \\ a_{n+1,k,i,j} = a_{n,k,0,j} + a_{n,k,i+1,j} + a_{n,k,j-1,j}, & 1 \le i \le j-3, \\ a_{n+1,k,j-2,j} = a_{n,k,0,j} + a_{n,k,j-1,j}, & \\ a_{n+1,k,j-1,j} = a_{n,k,-(j-1),j} + a_{n,k,-1,j} + a_{n,k,0,j}. & \end{cases}$$

The initial values of $a_{n,k,i,j}$ can be found easily as follows:

$$\begin{cases} a_{1,k,k+1,j} = 1, & \text{for } -(j-1) \le k \le -2, \\ a_{1,-1,j-1,j} = 1, & \\ a_{1,0,0,j} = 1, & \\ a_{1,1,-(j-1),j} = 1, & \\ a_{1,k,k-1,j} = 1, & \text{for } 2 \le k \le j-1, \\ a_{1,k,i,j} = 0, & \text{elsewhere.} \end{cases}$$

Since the initial values of the $a_{n,k,i,j}$'s are known, it follows from Lemma 7, by direct but somewhat tedious computations for n ranging from 1 to $2j$, that we can find explicit expressions (omitted) for the sequences $\langle a_{n,k,i,j} \rangle$, $-(j-1) \le k \le j-1$, $-(j-1) \le i \le j-1$, $1 \le n \le 2j$, and from there we obtain the following two results:

(a) $c_{m,j} = \phi_j(m)$ and $d_{m,j} = \psi_j(m)$ for $1 \le m \le 2j-1$.

(b) $a_{2j,k,i,j} = \sum_{m=1}^{j}(2m-1)a_{2j-m,k,i,j} + \sum_{m=j+1}^{2j-1}(4j-2m-1)a_{2j-m,k,i,j}$
for all $-(j-1) \le k \le j-1$, $-(j-1) \le i \le j-1$.

Since, for fixed integers k and i with $-(j-1) \le k \le j-1$, $-(j-1) \le i \le j-1$, $a_{n,k,i,j}$ is a linear combination of $a_{n-1,k,m,j}$, $-(j-1) \le m \le j-1$, it follows from part (b) above that

$$a_{n,k,i,j} = \sum_{m=1}^{j}(2m-1)a_{n-m,k,i,j} + \sum_{m=j+1}^{2j-1}(4j-2m-1)a_{n-m,k,i,j} \quad \text{for all } n \ge 2j.$$

Since both $c_{n,j}$ and $d_{n,j}$ are linear combinations of the $a_{n,k,i,j}$'s, we obtain that

$$c_{n,j} = \sum_{m=1}^{j}(2m-1)c_{n-m,j} + \sum_{m=j+1}^{2j-1}(4j-2m-1)c_{n-m,j},$$

and

$$d_{n,j} = \sum_{m=1}^{j}(2m-1)d_{n-m,j} + \sum_{m=j+1}^{2j-1}(4j-2m-1)d_{n-m,j}$$

for all $n \ge 2j$. This completes the proof of Theorem 5.

ACKNOWLEDGMENTS

The author is very indebted to Professor Peter Jau-Shyong Shiue and the anonymous referee for their many valuable suggestions that led to a more desirable presentation of this paper.

REFERENCES

1. Paul S. Bruckman. "Problem H-517." *The Fibonacci Quarterly* **34.5** (1996):473.
2. Bau-Sen Du. "Almost All Points Are Eventually Periodic with Minimal Period 3." *Bull. Inst. Math. Acad. Sinica* **12** (1984):405-11.
3. Bau-Sen Du. "Topological Entropy and Chaos of Interval Maps." In *Nonlinear Analysis: Theory, Methods & Applications* **11** (1987):105-14.
4. Bau-Sen Du. "The Minimal Number of Periodic Orbits of Periods Guaranteed in Sharkovskii's Theorem." *Bull. Austral. Math. Soc.* **31** (1985):89-103. Corrigendum, *ibid.* **32** (1985): 159.
5. Bau-Sen Du. "Symmetric Periodic Orbits of Continuous Odd Functions on the Interval." *Bull. Inst. Math. Acad. Sinica* **16** (1988):1-48.
6. Bau-Sen Du. "A Simple Method Which Generates Infinitely Many Congruence Identities." *The Fibonacci Quarterly* **27.2** (1989):116-24.
7. Bau-Sen Du. "Congruence Identities Arising from Dynamical Systems." *Appl. Math. Letters* **12** (1999):115-19.
8. Chyi-Lung Lin. "Obtaining Dividing Formulas $n|Q(n)$ from Iterated Maps." *The Fibonacci Quarterly* **36.2** (1998):118-24.
9. Fa-Gen Xie & Bai-Lin Hao. "Counting the Number of Periods in One-Dimensional Maps with Multiple Critical Points." *Phys.* A **202** (1994):237-63.

AMS Classification Numbers: 11A07, 11B50

❖❖❖

ON THE FIBONACCI NUMBERS AND THE DEDEKIND SUMS

Zhang Wenpeng and Yi Yuan
The Research Center for Science, Xi'an Jiaotong University,
Xi'an, Shaanxi, Peoples Republic of China
(Submitted July 1998-Final Revision April 1999)

1. INTRODUCTION

As usual, the Fibonacci sequence $F=(F_n)$ is defined by $F_0=0$, $F_1=1$, and by the second-order linear recurrence sequence $F_{n+2}=F_{n+1}+F_n$ for $n\geq 0$. This sequence has many important properties, and it has been investigated by many authors. In this paper we shall attempt to study the distribution problem of Dedekind sums for Fibonacci numbers and obtain some interesting results. For convenience, we first introduce the definition of the Dedekind sum $S(h,q)$. For a positive integer q and an arbitrary integer h, we define

$$S(h,q)=\sum_{a=1}^{q}\left(\left(\frac{a}{q}\right)\right)\left(\left(\frac{ah}{q}\right)\right),$$

where
$$((x))=\begin{cases}x-[x]-\frac{1}{2} & \text{if } x \text{ is not an integer;}\\ 0 & \text{if } x \text{ is an integer.}\end{cases}$$

The various arithmetical properties of $S(h,k)$ can be found in [3], [4], and [6]. About Dedekind sums and uniform distribution, Myerson [5] and Zheng [7] have obtained some meaningful conclusions. However, it seems that no one has yet studied the mean value distribution of $S(F_n,F_{n+1})$, at least we have not found expressions such as $\sum S(F_n,F_{n+1})$ in the literature. The main purpose of this paper is to study the mean value distribution of $S(F_n,F_{n+1})$ and present a sharper asymptotic formula. That is, we shall prove the following main theorem.

Theorem: Let m be a positive integer, then we have

$$\sum_{n=1}^{m}S(F_n,F_{n+1})=-\frac{(\sqrt{5}-1)^2}{48}m+C(m)+O\left(\frac{1}{\alpha^{2m}}\right),$$

where $\alpha=\frac{1+\sqrt{5}}{2}$, $C(m)$ is a constant depending only on the parity of m, i.e.,

$$C(m)=\begin{cases}\frac{1}{12}\sum_{n=1}^{\infty}\frac{1}{F_{2n}F_{2n+1}}+\frac{1}{12}\sum_{n=1}^{\infty}\frac{\left(\frac{1}{\alpha}\right)^{n+1}}{F_n} & \text{if } m \text{ is an even number;}\\ \frac{1}{12}\sum_{n=1}^{\infty}\frac{1}{F_{2n+1}F_{2n+2}}+\frac{1}{12}\sum_{n=1}^{\infty}\frac{\left(\frac{1}{\alpha}\right)^{n+1}}{F_n} & \text{if } m \text{ is an odd number.}\end{cases}$$

2. SOME LEMMAS

To complete the proof of the theorem, we need the following two lemmas.

Lemma 1: Let m be a positive integer, then we have

$$S(F_m,F_{m+1})+\frac{F_{m-1}}{12F_{m+1}}=\frac{1}{12}\left[\frac{1}{F_mF_{m+1}}-\frac{1}{F_{m-1}F_m}+\cdots+(-1)^{m-2}\frac{1}{F_2F_3}\right].$$

Proof: It is clear that $(F_m, F_{m+1}) = 1$, $m = 1, 2, 3, \ldots$, so, from the reciprocity formula of Dedekind sums (see [2] or [3]), we get

$$S(F_m, F_{m+1}) + S(F_{m+1}, F_m) = \frac{F_m^2 + F_{m+1}^2 + 1}{12F_mF_{m+1}} - \frac{1}{4}. \tag{1}$$

By the recursion relationship $F_{m+1} = F_m + F_{m-1}$ for $m > 0$, we have $S(F_{m+1}, F_m) = S(F_{m-1}, F_m)$. Thus,

$$S(F_m, F_{m+1}) + S(F_{m-1}, F_m) = \frac{F_m^2 + F_{m+1}^2 + 1}{12F_mF_{m+1}} - \frac{1}{4} = \frac{1}{12}\left(\frac{F_m}{F_{m+1}} + \frac{F_{m+1}}{F_m} + \frac{1}{F_mF_{m+1}}\right) - \frac{1}{4}$$

$$= \frac{1}{12}\left(\frac{F_{m-1}}{F_m} + \frac{F_m}{F_{m+1}} + \frac{1}{F_mF_{m+1}}\right) - \frac{1}{6} = \frac{1}{12F_mF_{m+1}} - \frac{F_{m-1}}{12F_{m+1}} - \frac{F_{m-2}}{12F_m},$$

so that

$$S(F_m, F_{m+1}) + \frac{F_{m-1}}{12F_{m+1}} = \frac{1}{12F_mF_{m+1}} - \left[S(F_{m-1}, F_m) + \frac{F_{m-2}}{12F_m}\right]$$

$$= \frac{1}{12F_mF_{m+1}} - \frac{1}{12F_{m-1}F_m} + \left[S(F_{m-2}, F_{m-1}) + \frac{F_{m-3}}{12F_{m-1}}\right] = \cdots$$

$$= \frac{1}{12F_mF_{m+1}} - \frac{1}{12F_{m-1}F_m} + \frac{1}{12F_{m-2}F_{m-1}} - \cdots - (-1)^{m-2}\left[S(F_1, F_2) + \frac{F_0}{12F_2}\right].$$

It is clear that $S(F_1, F_2) = S(1, 1) = 0$ and $F_0 = 0$, so we obtain

$$S(F_m, F_{m+1}) + \frac{F_{m-1}}{12F_{m+1}} = \frac{1}{12F_mF_{m+1}} - \frac{1}{12F_{m-1}F_m} + \cdots + (-1)^{m-2}\frac{1}{12F_2F_3}.$$

This concludes the proof of Lemma 1.

Lemma 2: Let m be a positive integer, then we have

$$\sum_{n=1}^{m} \frac{F_n}{F_{n+1}} = \frac{\sqrt{5}-1}{2}m + \sum_{n=1}^{\infty} \frac{\left(\frac{1}{\alpha}\right)^{n+1}}{F_{n+1}} + O\left(\frac{1}{\alpha^{2m}}\right),$$

where $\alpha = \frac{1+\sqrt{5}}{2}$.

Proof: From the second recursion relationship for F_n, we can easily deduce that

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) \quad \text{and} \quad \alpha F_m = F_{m+1} + \left(\frac{1}{\alpha}\right)^m.$$

From these identities, we get

$$\sum_{n=1}^{m} \frac{F_n}{F_{n+1}} = \frac{1}{\alpha}\sum_{n=1}^{m} \frac{\alpha F_n}{F_{n+1}} = \frac{1}{\alpha}\sum_{n=1}^{m} \frac{F_{n+1} + \left(\frac{1}{\alpha}\right)^n}{F_{n+1}}$$

$$= \frac{1}{\alpha}m + \sum_{n=1}^{m} \frac{\left(\frac{1}{\alpha}\right)^{n+1}}{F_{n+1}} = \frac{\sqrt{5}-1}{2}m + \sum_{n=1}^{\infty} \frac{\left(\frac{1}{\alpha}\right)^{n+1}}{F_{n+1}} + O\left(\frac{1}{\alpha^{2m}}\right).$$

This completes the proof of Lemma 2.

3. PROOF OF THE THEOREM

In this section we shall complete the proof of the theorem. First, let m be a positive integer, then from (1) we have

$$S(F_m, F_{m+1}) + S(F_{m+1}, F_m) = \frac{1}{12}\left(\frac{F_{m+1}}{F_m} + \frac{F_m}{F_{m+1}} + \frac{1}{F_m F_{m+1}}\right) - \frac{1}{4}$$

or

$$S(F_m, F_{m+1}) + S(F_{m-1}, F_m) = \frac{1}{12}\left(\frac{F_{m-1}}{F_m} + \frac{F_m}{F_{m+1}} + \frac{1}{F_m F_{m+1}}\right) - \frac{1}{6}$$

and

$$\sum_{n=1}^{m}[S(F_n, F_{n+1}) + S(F_{n-1}, F_n)] = \frac{1}{12}\sum_{n=1}^{m}\left[\frac{F_n}{F_{n+1}} + \frac{F_{n-1}}{F_n} + \frac{1}{F_n F_{n+1}}\right] - \frac{m}{6}.$$

Noting that

$$S(F_0, F_1) = S(0, 1) = 0 \quad \text{and} \quad F_0 = 0$$

so that

$$2\sum_{n=1}^{m} S(F_n, F_{n+1}) - S(F_m, F_{m+1}) = \frac{1}{12}\sum_{n=2}^{m}\frac{F_{n-1}}{F_n} + \frac{1}{12}\sum_{n=1}^{m}\frac{F_n}{F_{n+1}} + \frac{1}{12}\sum_{n=1}^{m}\frac{1}{F_n F_{n+1}} - \frac{m}{6};$$

hence,

$$2\sum_{n=1}^{m} S(F_n, F_{n+1}) = S(F_m, F_{m+1}) + \frac{1}{12}\frac{F_{m-1}}{F_{m+1}} + \frac{1}{6}\sum_{n=1}^{m}\frac{1}{F_{n+1}} + \frac{1}{12}\sum_{n=1}^{m}\frac{F_n}{F_n F_{n+1}} - \frac{2m+1}{12}. \tag{2}$$

Applying (2), Lemma 1, and Lemma 2, we obtain

$$2\sum_{n=1}^{m} S(F_n, F_{n+1}) = \frac{1}{12}\left[\frac{1}{F_m F_{m+1}} - \frac{1}{F_{m-1}F_m} + \cdots + (-1)^{m-2}\frac{1}{F_2 F_3}\right]$$
$$+ \frac{1}{6}\left[\frac{\sqrt{5}-1}{2}m + \sum_{n=1}^{\infty}\frac{\left(\frac{1}{\alpha}\right)^{n+1}}{F_{n+1}} + O\left(\frac{1}{\alpha^{2m}}\right)\right] + \frac{1}{12}\sum_{n=1}^{m}\frac{1}{F_n F_{n+1}} - \frac{2m+1}{12}.$$

If m is an even number, then from the above we have

$$\sum_{n=1}^{m} S(F_n, F_{n+1}) = \frac{\sqrt{5}-3}{24}m + \frac{1}{12}\sum_{n=1}^{m/2}\frac{1}{F_{2n}F_{2n+1}} + \frac{1}{12}\sum_{n=1}^{\infty}\frac{\left(\frac{1}{\alpha}\right)^{n+1}}{F_{n+1}} + O\left(\frac{1}{\alpha^{2m}}\right)$$
$$= -\frac{(\sqrt{5}-1)^2}{48}m + \frac{1}{12}\sum_{n=1}^{\infty}\frac{1}{F_{2n}F_{2n+1}} + \frac{1}{12}\sum_{n=1}^{\infty}\frac{\left(\frac{1}{\alpha}\right)^{n+1}}{F_{n+1}} + O\left(\frac{1}{\alpha^{2m}}\right).$$

If m is an odd number, then

$$\sum_{n=1}^{m} S(F_n, F_{n+1}) = \frac{\sqrt{5}-3}{24}m + \frac{1}{12}\sum_{n=1}^{(m-1)/2}\frac{1}{F_{2n+1}F_{2n+2}} + \frac{1}{12}\sum_{n=1}^{\infty}\frac{\left(\frac{1}{\alpha}\right)^{n+1}}{F_{n+1}} + O\left(\frac{1}{\alpha^{2m}}\right)$$
$$= -\frac{(\sqrt{5}-1)^2}{48}m + \frac{1}{12}\sum_{n=1}^{\infty}\frac{1}{F_{2n+1}F_{2n+2}} + \frac{1}{12}\sum_{n=1}^{\infty}\frac{\left(\frac{1}{\alpha}\right)^{n+1}}{F_{n+1}} + O\left(\frac{1}{\alpha^{2m}}\right).$$

This completes the proof of the theorem.

ACKNOWLEDGMENTS

The authors express their gratitude to the anonymous referee for very helpful and detailed comments.

REFERENCES

1. Tom M. Apostol. *Introduction to Analytic Number Theory.* New York: Springer-Verlag, 1976.
2. Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory.* New York: Springer-Verlag, 1976.
3. L. Carlitz. "The Reciprocity Theorem for Dedekind Sums." *Pacific J. Math.* **3** (1953):523-27.
4. L. J. Mordell. "The Reciprocity Formula for Dedekind Sums." *Amer. J. Math.* **73** (1951): 593-98.
5. G. Myerson. "Dedekind Sums and Uniform Distribution." *J. Number Theory* **28** (1991): 1803-07.
6. H. Rademacher. "On the Transformation of $\log \eta(\tau)$." *J. Indian Math. Soc.* **19** (1955):25-30.
7. Z. Zheng. "Dedekind Sums and Uniform Distribution (mod 1)." *Acta Mathematica Sinica* **11** (1995):62-67.

AMS Classification Numbers: 11B37, 11B39

❖❖❖

RESIDUES OF GENERALIZED BINOMIAL COEFFICIENTS MODULO A PRIME

John M. Holte
Dept. of Math. and Computer Science, Gustavus Adolphus College, St. Peter MN 56082
(Submitted August 1998-Final Revision April 1999)

1. INTRODUCTION

A remarkable theorem of E. Lucas [10] provides a simple way to compute the binomial coefficient $\binom{N}{m}$ modulo a prime p in terms of the binomial coefficients of the base-p digits of N and m: If $N = \sum N_j p^j$ and $m = \sum m_j p^j$, where $0 \le N_j,\ m_j < p$, then

$$\binom{N}{m} \equiv \prod \binom{N_j}{m_j} \pmod{p}.$$

This paper will generalize the following alternative version of Lucas's theorem: Let

$$B(m,n) = \binom{m+n}{m} = \frac{(m+n)!}{m!n!};$$

then

$$B(m,n) \equiv B(m \div p, n \div p) B(m \bmod p, n \bmod p) \pmod{p},$$

where $m \div p$ is the integer quotient of m by p, and $m \bmod p$ is the remainder. It follows that if $m = \sum m_j p^j$ and $n = \sum n_j p^j$, where $0 \le m_j,\ n_j < p$, then

$$B(m,n) \equiv \prod B(m_j, n_j) \pmod{p}.$$

As a corollary, $p \mid B(m,n)$ if and only if $m_j + n_j \ge p$ for some j.

This theorem also implies that the residues of Pascal's triangle modulo p have a self-similar structure; see, e.g., [12], [2], [4], [5], [9], [17], and [1]. For example, if $p = 3$, then $[B(m,n) \bmod p]$ for $0 \le m,\ n < 9$ is given as follows:

$$\begin{bmatrix} 1&1&1&1&1&1&1&1&1 \\ 1&2&0&1&2&0&1&2&0 \\ 1&0&0&1&0&0&1&0&0 \\ 1&1&1&2&2&2&0&0&0 \\ 1&2&0&2&1&0&0&0&0 \\ 1&0&0&2&0&0&0&0&0 \\ 1&1&1&0&0&0&0&0&0 \\ 1&2&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0 \end{bmatrix} \equiv \begin{bmatrix} \mathbf{1B} & \mathbf{1B} & \mathbf{1B} \\ \mathbf{1B} & \mathbf{2B} & \mathbf{0B} \\ \mathbf{1B} & \mathbf{0B} & \mathbf{0B} \end{bmatrix} \pmod{p},$$

where

$$\mathbf{B} = \begin{bmatrix} 1&1&1 \\ 1&2&3 \\ 1&3&6 \end{bmatrix} \equiv \begin{bmatrix} 1&1&1 \\ 1&2&0 \\ 1&0&0 \end{bmatrix} \pmod{p},$$

so this matrix is the tensor (or Kronecker) product $\mathbf{B} \otimes \mathbf{B}$ mod p. Generally, as noted in [11], modulo p we have that $[B(m,n) \bmod p]$ for $0 \le m,\ n < p^k$ will be $\mathbf{B}^{\otimes k}$, the k-fold tensor product of $\mathbf{B} = [B(i,j) \bmod p]$, where $0 \le i,\ j < p$. Note that matrix indices start at index pair (0, 0).

Generalized binomial coefficients are defined corresponding to a given sequence $\langle u_n \rangle$ by replacing $n!$ by the product of u_1 through u_n. This paper uses recurrence-relation techniques to deduce generalizations of Lucas's theorem for generalized binomial coefficients based on a sequence generated by a second-order recurrence relation (see Theorems 1 and 3). One resulting generalization is equivalent to the theorem (Theorem 4 below) obtained by Wells [13] by an intricate analysis. The new approach to the proof clarifies and explains the complexities of Wells's formula.

2. THE UNDERLYING SEQUENCE $\langle u_n \rangle$

Definition 1: Let $a, b \in \mathbb{Z}$. Let p be a prime. Define the sequence $\langle u_n \rangle$ recursively as follows:

$$u_0 = 0;\ u_1 = 1;\ u_n = au_{n-1} + bu_{n-2} \text{ for } n = 2, 3, 4, \ldots$$

(or $u_1 = 1;\ u_2 = a;\ u_n = au_{n-1} + bu_{n-2}$ for $n = 3, 4, 5, \ldots$).

For example, when $a = 2$ and $b = -1$, then $u_n = n$; when $a = 1 + q$ and $b = -q$, then $u_n = 1 + q + q^2 + \cdots + q^{n-1}$; and when $a = 1$ and $b = 1$, then $u_n = F_n$, the n^{th} Fibonacci number.

Definition 2: Let r denote the rank of apparition of p; thus, $r = \min\{n \in \mathbb{N} : u_n \equiv 0 \pmod{p}\}$. Let t denote the (least) period of $\langle u_n \bmod p \rangle$, if it exists. Let $s = t/r$.

From now on, consider the prime p and the integers a and b fixed, and assume a and b are not both zero. We shall usually assume that $p \nmid b$. If $p \mid b$, then $u_n \equiv a^{n-1} \pmod{p}$, and so either $p \mid a$ and $u_n \equiv 0 \pmod{p}$ for $n \geq 2$ while $u_1 = 1$ so that t is undefined, or $p \nmid a$ and $r = \infty$. In any case, the recurrence relation $u_n \equiv au_{n-1} + bu_{n-2} \pmod{p}$ defines a transformation

$$\begin{bmatrix} u_{n+1} \\ u_n \end{bmatrix} \equiv \begin{bmatrix} a & b \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u_n \\ u_{n-1} \end{bmatrix} \pmod{p}$$

mapping $\{0, \ldots, p-1\}^2$ to itself. If $p \nmid b$, then the transformation is invertible, and consequently it must be periodic with period $t \leq p^2$, and, since $u_0 = 0$ and 0 repeats, $r \leq t$.

The following basic addition formula, which appears, e.g., in [7], may be proved by induction.

Lemma 1 (Extended Recurrence): For $m \geq 1$ and $n \geq 0$, $u_{m+n} = u_m u_{n+1} + bu_{m-1}u_n$.

Many basic properties of the sequence $\langle u_n \rangle$ follow immediately from this lemma.

Corollary 0: Let $z = \min\{n \in \mathbb{N} : u_n = 0\}$. Then $z > 1$, and if $z < \infty$, then $\{n \in \mathbb{N} : u_n = 0\} = \{z, 2z, 3z, \ldots\}$.

Proof: If $z < \infty$, Lemma 1 implies that $u_{kz+n} = u_{kz}u_{n+1} + bu_{kz-1}u_n$, from which the conclusion easily follows by induction if $b \neq 0$. If $b = 0$, then $u_n = a^{n-1}$ for $n > 0$, where $a \neq 0$ (by the assumption above), so $z = \infty$. □

Corollary 1: If $p \nmid b$, then $\{n \in \mathbb{N} : u_n \equiv 0 \pmod{p}\} = \{r, 2r, 3r, \ldots\}$.

Corollary 2: If $p \nmid b$, then s (defined as t/r) is an integer.

Corollary 3: If $r < \infty$, then, for $k = 1, 2, 3, \ldots$, $bu_{kr-1} \equiv u_{kr+1} \equiv u_{r+1}^k \pmod{p}$.

Corollary 4: If $p \nmid b$, then $u_1 = 1, u_{r+1}, u_{2r+1}, \ldots, u_{(s-1)r+1}$—or, equivalently, u_{r+1}^k for $0 \leq k < s$—are all distinct modulo p.

Corollary 5: If $p \nmid b$, then the sequence $\langle u_{r+1}^n \mod p \rangle_{n=0}^{\infty}$ has period s: $u_{r+1}^n \equiv u_{r+1}^{n \bmod s} \pmod{p}$.

Corollary 6: If $p \nmid b$, then $s \mid p-1$.

Definition 3: The *rank of apparition* of k, denoted $r(k)$, is the least index n for which k divides u_n: $r(k) = \min\{n \in \mathbb{N} : k \mid u_n\}$. (If k does not divide any u_n, then $r(k) = \infty$.) Note that $r = r(p)$.

Definition 4: The sequence $\langle u_n \rangle$ is regularly divisible by p if, for every positive integer i, $\{n \in \mathbb{N} : p^i \mid u_n\} = \{kr(p^i) : k \in \mathbb{N}\}$.

Corollary 7 (Wells): If $p \nmid b$, then the sequence $\langle u_n \rangle$ is regularly divisible by p.

3. GENERALIZED BINOMIAL COEFFICIENTS

Definition 5: Given $\langle u_n \rangle$, define the generalized, or bracket, factorial $[n]!$ for $n = 0, 1, 2, \ldots$ by

$$[n]! = \prod_{j=1}^{n} u_j .$$

For $m \geq 0$ and $n \geq 0$, define the generalized binomial coefficient $C(m, n)$ by

$$C(m,n) = \begin{bmatrix} m+n \\ m \end{bmatrix} = \frac{[m+n]!}{[m]![n]!}.$$

If some factors are zero, then it is to be understood that zeros in the numerator and denominator are to be canceled in pairs. By Corollary 0, if there are some zero factors u_j, their indices j are multiples of some $z > 1$. so the number of zero factors in the numerator will either equal the number in the denominator or exceed it by 1.

When $a = 2$ and $b = -1$, then $u_n = n$ and the generalized binomial coefficients become the ordinary binomial coefficients: $C(m, n) = B(m, n)$. When $a = 1 + q$ and $b = -q$, then $u_n = 1 + q + q^2 + \cdots + q^{n-1}$ and the generalized binomial coefficients are the Gauss q-binomial coefficients. When $a = 1$ and $b = 1$, then $u_n = F_n$ and the generalized binomial coefficients become the Fibonomial coefficients.

Obviously, the generalized binomial coefficients are symmetric: $C(m, n) = C(n, m)$. Also, they satisfy the following *boundary conditions*:

$$C(m, 0) = 1 \text{ and } C(0, n) = 1 \text{ for } m \geq 0,\ n \geq 0.$$

Lemma 2 (Basic Recurrence): For $m \geq 1$, $n \geq 1$, $C(m, n) = u_{m+1} C(m, n-1) + b u_{n-1} C(m-1, n)$.

Proof:

$$\begin{aligned} & u_{m+1} C(m, n-1) + b u_{n-1} C(m-1, n) \\ &= \frac{u_{m+1}[m+n-1]! u_n}{[m]![n-1]! u_n} + \frac{u_m b u_{n-1}[m-1+n]!}{u_m [m-1]![n]!} \\ &= \frac{[m+n-1]!(u_{m+1}u_n + b u_m u_{n-1})}{[m]![n]!} = C(m, n), \end{aligned}$$

because $u_n u_{m+1} + b u_{n-1} u_m = u_{n+m}$, by Lemma 1. □

Corollary: If a and b are integers, then the generalized binomial coefficients are all integers.

4. GENERALIZED BINOMIAL COEFFICIENTS MODULO p

When $p|b$, the generalized binomial coefficients modulo p are very simple. If $p|b$, then $u_n \equiv a^{n-1} \pmod{p}$, and by Lemma 2, $C(m,n) \equiv u_{m+1}C(m,n-1) \pmod{p}$. Also, $C(m,0) = 1$ for $m \geq 0$. Therefore, for $m, n \geq 0$,

$$\text{if } p \mid b, \text{ then } C(m,n) \equiv a^{mn} \pmod{p}.$$

Here $0^0 \equiv 1$.

When $p\nmid b$, the pattern of the residues is more complex. There may be a self-similar pattern, as in the case of binomial coefficients presented above. But the pattern may be more complicated. For example, see Table 1 for the layout of Fibonomial coefficients modulo 3.

When $p\nmid b$, a formula for the mod-p residues of $C(m,n)$ may be derived in three steps: (1) Show that $C(m,n) \equiv 0 \pmod{p}$ when $m \bmod r + n \bmod r \geq r$; (2) find a recurrence for $C'(m,n)$, defined as $C(mr,nr)$, and solve it; and (3) complete the solution by using the basic recurrence relation in Lemma 2. This procedure parallels and extends that given in [6], which may be consulted for further details.

Notation: If $r < \infty$, then, for each nonnegative integer n, let

$$n_0 = n \bmod r,$$
$$n' = n \div r,$$
$$n^* = n \bmod t,$$
$$n'' = n^* \div r = n' \bmod s.$$

Lemma 3: If $p\nmid b$, then $C(m,n) \equiv 0 \pmod{p}$ when $m_0 + n_0 \geq r$.

Proof: This result is a consequence of Knuth and Wilf's generalization of Kummer's theorem: According to [8], $C(m,n)$ will be divisible by p if there is a carry across the radix point when m/r and n/r are added in base p; this happens when $m_0 + n_0 \geq r$. □

Lemma 4 (r-Step Recurrence): If $p\nmid b$, then, for every $m \geq 1$ and $n \geq 1$,

$$C(mr,nr) \equiv u_{r+1}^{mr}C(mr,(n-1)r) + u_{r+1}^{nr}C((m-1)r,nr) \pmod{p}.$$

Proof: For $h = 1, 2, \ldots, r-1$, we have, by Lemma 2,

$$\begin{aligned} &C(mr,(n-1)r+h) \\ &\equiv u_{mr+1}C(mr,(n-1)r+h-1) + bu_{(n-1)r+h-1}C((m-1)r+r-1,(n-1)r+h) \\ &\equiv u_{mr+1}C(mr,(n-1)r+h-1) \pmod{p}, \end{aligned}$$

because $C((m-1)r+r-1,(n-1)r+h) \equiv 0$, by Lemma 3. Together with Corollary 3, this implies that

$$C(mr,(n-1)r+r-1) \equiv u_{r+1}^{m(r-1)}C(mr,(n-1)r) \pmod{p}. \tag{1}$$

Similarly,

$$C((m-1)r+r-1,nr) \equiv u_{r+1}^{n(r-1)}C((m-1)r,nr) \pmod{p}. \tag{2}$$

Again by Lemma 2, $C(mr,nr) \equiv u_{mr+1}C(mr,nr-1) + bu_{nr-1}C(mr-1,nr) \pmod{p}$. Equations (1) and (2) and Corollary 3 transform this result into the desired conclusion. □

TABLE 1. The Fibonomial Coefficients Modulo 3

```
1111 1111 1111 1111 1111 1111 1111 1111 1111
1120 2210 1120 2210 1120 2210 1120 2210 1120
1200 1200 1200 1200 1200 1200 1200 1200 1200
1000 2000 1000 2000 1000 2000 1000 2000 1000

1212 2121 0000 1212 2121 0000 1212 2121 0000
1220 1220 0000 2110 2110 0000 1220 1220 0000
1100 2200 0000 1100 2200 0000 1100 2200 0000
1000 1000 0000 2000 2000 0000 1000 1000 0000

1111 0000 0000 1111 0000 0000 1111 0000 0000
1120 0000 0000 2210 0000 0000 1120 0000 0000
1200 0000 0000 1200 0000 0000 1200 0000 0000
1000 0000 0000 2000 0000 0000 1000 0000 0000

1212 1212 1212 2121 2121 2121 0000 0000 0000
1220 2110 1220 1220 2110 1220 0000 0000 0000
1100 1100 1100 2200 2200 2200 0000 0000 0000
1000 2000 1000 1000 2000 1000 0000 0000 0000

1111 2222 0000 2222 1111 0000 0000 0000 0000
1120 1120 0000 1120 1120 0000 0000 0000 0000
1200 2100 0000 2100 1200 0000 0000 0000 0000
1000 1000 0000 1000 1000 0000 0000 0000 0000

1212 0000 0000 2121 0000 0000 0000 0000 0000
1220 0000 0000 1220 0000 0000 0000 0000 0000
1100 0000 0000 2200 0000 0000 0000 0000 0000
1000 0000 0000 1000 0000 0000 0000 0000 0000

1111 1111 1111 0000 0000 0000 0000 0000 0000
1120 2210 1120 0000 0000 0000 0000 0000 0000
1200 1200 1200 0000 0000 0000 0000 0000 0000
1000 2000 1000 0000 0000 0000 0000 0000 0000

1212 2121 0000 0000 0000 0000 0000 0000 0000
1220 1220 0000 0000 0000 0000 0000 0000 0000
1100 2200 0000 0000 0000 0000 0000 0000 0000
1000 1000 0000 0000 0000 0000 0000 0000 0000

1111 0000 0000 0000 0000 0000 0000 0000 0000
1120 0000 0000 0000 0000 0000 0000 0000 0000
1200 0000 0000 0000 0000 0000 0000 0000 0000
1000 0000 0000 0000 0000 0000 0000 0000 0000
```

Introduce $C'(m,n) = C(mr, nr)$. By Lemma 4,

$$C'(m,n) \equiv u_{r+1}^{rm} C'(m-1,n) + u_{r+1}^{rn} C'(m-1,n) \pmod{p}. \tag{3}$$

Also

$$C'(m,0) \equiv 1 \text{ and } C'(0,n) \equiv 1 \pmod{p} \text{ for } m,n \geq 0. \tag{4}$$

One may check that the unique solution of congruence (3) satisfying the boundary conditions (4) is given by the following formula. This step involves the Pascal triangle rule,

$$B(m,n) = B(m,n-1) + B(m-1,n).$$

Lemma 5: If $p \nmid b$, then, for every $m \geq 0$ and $n \geq 0$, $C(mr,nr) \equiv B(m,n) u_{r+1}^{rmn} \pmod{p}$.

Definition 6: For $i, j \geq 0$ and for $0 \leq k, l < r$, let $A_{i,j}(k, l)$ denote the solution of the modulo-p recurrence relation

$$A_{i,j}(k,l) \equiv u_{ir+k+1}A_{i,j}(k,l-1) + bu_{jr+l-1}A_{i,j}(k-1,l)$$

for $0 \leq k, l < r$ together with the boundary conditions $A_{i,j}(k,-1) \equiv 0 \pmod{p}$ for $1 \leq k < r$ and $A_{i,j}(-1,l) \equiv 0 \pmod{p}$ for $1 \leq l < r$ and $A_{i,j}(0,0) \equiv 1 \pmod{p}$.

If $(i, j) = (m', n')$ and $(k, l) = (m_0, n_0)$, and if the final boundary condition in this definition were $A_{m',n'}(0,0) \equiv C(m'r, n'r)$, then these would be the congruences satisfied by $C(m'r + m_0, n'r + n_0)$ for $0 \leq m_0, n_0 < r$. Because $u_{m'r+m_0+1} \equiv u_{m''r+m_0+1} \pmod{p}$ where $m'' = m' \bmod s$, and similarly for $u_{n'r+n_0-1}$, these congruences imply that

$$A_{m',n'}(m_0,n_0) \equiv A_{m'',n''}(m_0,n_0) \pmod{p}. \tag{5}$$

and so $C(m, n) \bmod p$ is given as follows.

Lemma 6: If $p \nmid b$, then, for $m \geq 0$ and $n \geq 0$, $C(m,n) \equiv C(m'r, n'r)A_{m'',n''}(m_0,n_0) \pmod{p}$.

Definition 7: If $r < \infty$, then, for $i, j \geq 0$ and $0 \leq k, l < r$, define $H_{i,j}(k,l) = u_{r+1}^{ri}A_{i,j}(k,l)$. By Corollary 5 and equation (5), $H_{m',n'}(m_0,n_0) \equiv H_{m'',n''}(m_0,n_0) \pmod{p}$.

5. THE PATTERN OF THE RESIDUES

Recall that $n_0 = n \bmod r$, $n' = n \div r$, $n^* = n \bmod t$, and $n'' = n' \bmod s$, where r is the rank of apparition of the prime p in $\langle u_n \rangle$, t is the period of $\langle u_n \bmod p \rangle$, and $s = t/r$. Lemmas 5 and 6 yield the following formula.

Theorem 1: If $p \nmid b$, then, for $m, n \geq 0$, $C(m,n) \equiv B(m',n')H_{m'',n''}(m_0,n_0) \pmod{p}$.

This result simplifies nicely when $s = 1$. Then $m'' = n'' = 0$, and $H_{0,0}(m_0,n_0) \equiv C(m_0,n_0) \pmod{p}$ for $0 \leq m_0, n_0 < r$. Thus, in this case, as in the Pascal "triangle" case, the pattern of residues exhibits self-similarity upon scaling by p.

Corollary: If $p \nmid b$ and $s = 1$, then, for $m, n \geq 0$, $C(m,n) \equiv B(m',n')C(m_0,n_0) \pmod{p}$ or, letting $\mathbf{B}$ denote the matrix $[B(i,j)]$ with $0 \leq i, j < p$, and $\mathbf{C}_k = [C(m,n)]$ with $0 \leq m, n < rp^k$, we have $\mathbf{C}_k \equiv \mathbf{B}^{\otimes k} \otimes \mathbf{C}_0 \pmod{p}$.

Example 1: q-Binomial Coefficients. Take $u_n = \sum_{k=0}^{n-1} q^k$ to obtain the q-binomial coefficients. If $p \mid q$, then $u_n \equiv 1$ for $n \geq 1$, so $C(m,n) \equiv 1 \pmod{p}$ for $m, n \geq 0$. So assume $p \nmid q$. Then $1 + q + \cdots + q^{r-1} = u_r \equiv 0 \pmod{p}$, so $q^r - 1 = qu_r - u_r \equiv 0 \pmod{p}$, whence $u_{r+1} = u_r + q^r \equiv 0 + 1 \equiv 1 \pmod{p}$. Thus, $(u_r, u_{r+1}) \equiv (u_0, u_1)$, and so the period, t, equals r, and so $s = 1$. Therefore, the corollary covers the case of q-binomial coefficients when $p \nmid q$, yielding a result given originally by Fray [3].

For a numerical example, take $q = 2$ and $p = 5$. Then $u_1 = 1$, $u_2 = 3$, $u_3 = 7$, $u_4 = 15$, $u_5 = 31$, ..., whence $r = 4$ and

$$\mathbf{C}_0 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 7 & 15 \\ 1 & 7 & 35 & 155 \\ 1 & 15 & 155 & 1395 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 0 \\ 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \pmod{5},$$

so

$$\mathbf{C}_1 \equiv \mathbf{B} \otimes \mathbf{C}_0 \equiv \begin{bmatrix} 1\mathbf{C}_0 & 1\mathbf{C}_0 & 1\mathbf{C}_0 & 1\mathbf{C}_0 & 1\mathbf{C}_0 \\ 1\mathbf{C}_0 & 2\mathbf{C}_0 & 3\mathbf{C}_0 & 4\mathbf{C}_0 & 0\mathbf{C}_0 \\ 1\mathbf{C}_0 & 3\mathbf{C}_0 & 1\mathbf{C}_0 & 0\mathbf{C}_0 & 0\mathbf{C}_0 \\ 1\mathbf{C}_0 & 4\mathbf{C}_0 & 0\mathbf{C}_0 & 0\mathbf{C}_0 & 0\mathbf{C}_0 \\ 1\mathbf{C}_0 & 0\mathbf{C}_0 & 0\mathbf{C}_0 & 0\mathbf{C}_0 & 0\mathbf{C}_0 \end{bmatrix} \pmod 5.$$

Individual residues may be calculated easily by the Corollary to Theorem 1. For example,

$$C(222, 161) \equiv B(55, 40)C(2, 1) \equiv B(2, 1)B(1, 3)B(0, 0)C(2, 1) \equiv 3 \cdot 4 \cdot 1 \cdot 2 \equiv 4 \pmod 5.$$

Example 2: Fibonomial Coefficients Modulo p. Let $a = b = 1$ so that $u_n = F_n$ and, for illustration, let $p = 3$. Then $r = 4$, $t = 8$, and $s = 2$. The initial part of the table of Fibonomial coefficients modulo 3 were given in Table 1 above. Submatrices of the Fibonomial coefficients modulo 3 are shown in Table 2.

TABLE 2. Submatrices of the Fibonomial Coefficients Modulo 3

$$\begin{bmatrix} 1\mathbf{H}_{0,0} & 1\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & 1\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & 1\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & 1\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & \cdots \\ 1\mathbf{H}_{1,0} & 2\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 1\mathbf{H}_{1,1} & 2\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 1\mathbf{H}_{1,0} & 2\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & \cdots \\ 1\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 1\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & \cdots \\ 1\mathbf{H}_{1,0} & 1\mathbf{H}_{1,1} & 1\mathbf{H}_{1,0} & 2\mathbf{H}_{1,1} & 2\mathbf{H}_{1,0} & 2\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & \cdots \\ 1\mathbf{H}_{0,0} & 2\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 2\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & \cdots \\ 1\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 2\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & \cdots \\ 1\mathbf{H}_{0,0} & 1\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & \cdots \\ 1\mathbf{H}_{1,0} & 2\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & \cdots \\ 1\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots \end{bmatrix}$$

By Definition 7,

$$\mathbf{H}_{0,0} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 0 \\ 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}; \quad \mathbf{H}_{0,1} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{bmatrix}; \quad \mathbf{H}_{1,0} = \begin{bmatrix} 1 & 2 & 1 & 2 \\ 1 & 2 & 2 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}; \quad \mathbf{H}_{1,1} = \begin{bmatrix} 1 & 2 & 1 & 2 \\ 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{bmatrix}.$$

Wells [16] also gives a formula for these residues, one that is a special case of her Theorem 4, given below, and she provides a detailed description of the pattern of these sub-matrices from a "triangular" perspective.

Modulo $p = 2$, the Fibonacci sequence has $r = t = 3$, so $s = 1$ and, in accordance with the corollary, the Fibonomial coefficients modulo 2 exhibit a pattern similar to that of the binomial coefficients, but with a different $\mathbf{C}_0$. Wells [15] presents the equivalent of this result in an interesting context. The pattern of Fibonomial coefficients modulo any prime is treated in [6].

Theorem 1 and the Examples show that the infinite matrix $[C(i, j) \bmod p]$ may be partitioned into $r \times r$ submatrices which form basic, natural "tiling units." The pattern of the residues is obtained by superimposing the self-similar array of binomial coefficients modulo p upon the

doubly periodic "tiling" of the plane by "hidden" $r \times r$ $\mathbf{H}$ matrices. The binomial structure is self-similar upon scaling by the factor p. The $r \times r$ tiling structure has period s both horizontally and vertically, and so the period is t at the element level.

When $s = 1$, there are $p-1$ different nonzero $r \times r$ submatrices, one for each nonzero residue value of $B(m', n') \bmod p$ times $\mathbf{C}_0$. In the general case, by Corollary 4, there are also $s \cdot s$ different $H_{m'',n''}$-matrices. This suggests that there may be $(p-1)s^2$ different nonzero "tiles." In the case of the Fibonomial coefficients modulo 3, the exhibited matrix shows these seven submatrices:

$$1\mathbf{H}_{0,0},\ 1\mathbf{H}_{0,1},\ 1\mathbf{H}_{1,0},\ 1\mathbf{H}_{1,1},\ 2\mathbf{H}_{0,1},\ 2\mathbf{H}_{1,0},\ 2\mathbf{H}_{1,1}.$$

The missing case, $2\mathbf{H}_{0,0}$, must be sought farther out. The places of the missing $2\mathbf{H}_{0,0}$ are (5, 11), (11, 5), (5, 13), (13, 5)... in Table 2.

Theorem 2: Assume $p \nmid b$. The number of different nonzero $r \times r$ submatrices of the infinite matrix $[C(i, j) \bmod p]$ is $(p-1)s^2$.

Proof: The proof is trivial for $s = 1$, so assume $s > 1$. First, we verify that the tiles $\rho\mathbf{H}_{\mu,\nu}$ are distinct for different (ρ, μ, ν)'s with $1 \le \rho < p$ and $0 \le \mu,\ \nu < s$. By Definition 6 and Corollary 3, $A_{\mu,\nu}(0, 0) \equiv 1$, $A_{\mu,\nu}(0, 1) \equiv u_{\mu r+1} \equiv u_{r+1}^{\mu}$, and $A_{\mu,\nu}(1, 0) \equiv b u_{\nu r-1} \equiv u_{r+1}^{\nu} \pmod p$, so by Definition 7, $H_{\mu,\nu}(0, 0) \equiv u_{r+1}^{r\mu\nu}$, $H_{\mu,\nu}(0, 1) \equiv u_{r+1}^{r\mu\nu+\mu}$, and $H_{\mu,\nu}(1, 0) \equiv u_{r+1}^{r\mu\nu+\nu} \pmod p$. Note that $p \nmid u_{r+1}$. If $\rho\mathbf{H}_{\mu,\nu} \equiv \tilde{\rho}\mathbf{H}_{\tilde{\mu},\tilde{\nu}} \pmod p$, where $1 \le \rho,\ \tilde{\rho} < p$, and $0 \le \mu, \nu,\ \tilde{\mu}, \tilde{\nu} < s$, or $\mathbf{H}_{\mu,\nu} \equiv \rho_1\mathbf{H}_{\tilde{\mu},\tilde{\nu}} \pmod p$, where $\rho_1 \equiv \rho^{-1}\tilde{\rho}$, then $u_{r+1}^{r\mu\nu} \equiv \rho_1 u_{r+1}^{r\tilde{\mu}\tilde{\nu}}$, $u_{r+1}^{r\mu\nu+\mu} \equiv \rho_1 u_{r+1}^{r\tilde{\mu}\tilde{\nu}+\tilde{\mu}}$, and $u_{r+1}^{r\mu\nu+\nu} \equiv \rho_1 u_{r+1}^{r\tilde{\mu}\tilde{\nu}+\tilde{\nu}} \pmod p$, so $u_{r+1}^{\mu} \equiv u_{r+1}^{\tilde{\mu}}$ and $u_{r+1}^{\nu} \equiv u_{r+1}^{\tilde{\nu}} \pmod p$, whence, by Corollary 4, $\mu = \tilde{\mu}$ and $\nu = \tilde{\nu}$, and therefore going back one finds $\rho_1 \equiv 1$, i.e., $\rho = \tilde{\rho}$. This proves that the mapping $(\rho, \mu, \nu) \mapsto \rho\mathbf{H}_{\mu,\nu}$ is one to one.

It remains to show that, given (ρ, μ, ν) with $1 \le \rho < p$ and $0 \le \mu,\ \nu < s$, one can find (m, n) such that $B(m', n') \equiv \rho \pmod p$ and $m'' = \mu$ and $n'' = \nu$. Let $m = r(1 + ip)$ and $n = r(\rho - 1 + jp^2)$, choosing i and j so that $i \equiv \mu - 1 \pmod s$, $j = \nu - (\rho - 1) \pmod s$, and $0 \le i,\ j < p$. Since $p \equiv 1$ and $p^2 \equiv 1 \pmod s$, by Corollary 6, we have

$$m'' = (m \div r) \bmod s = (1 + ip) \bmod s = (1 + i) \bmod s = \mu,$$

$$n'' = (\rho - 1 + jp^2) \bmod s = (\rho - 1 + j) \bmod s = \nu,$$

and, by Lucas's theorem,

$$B(m', n') \equiv B(0, j)B(i, 0)B(1, \rho - 1) \equiv \rho \pmod p.$$

(Modification of this construction can yield infinitely many occurrences of each possible tile.). □

6. GENERALIZATION OF LUCAS'S THEOREM

Using Theorem 1, one may express $H_{m'',n''}(m_0, n_0)$ in terms of $C(m, n)$ for small values of (m, n). The tricky part is to work around the cases when $B(m', n') \equiv 0 \pmod p$. Here is one approach.

Given (m, n), let $\mu = m^*$ and $\nu = n^* + \lambda t$, where λ will be chosen later. By Theorem 1,

$$C(\mu, \nu) \equiv B(\mu', \nu')H_{\mu'',\nu''}(\mu_0, \nu_0) \pmod p. \tag{6}$$

Now,

$$\begin{aligned}
&\mu_0 = m^* \bmod r = (m \bmod t) \bmod r = m \bmod r = m_0,\\
&\mu' = m^* \div r = m'',\\
&\mu'' = \mu' \bmod s = m'' \bmod s = m'',\\
&\nu_0 = (n^* + \lambda t) \bmod r = n^* \bmod r = n_0,\\
&\nu' = (n^* + \lambda t) \div r = (n \bmod t) \div r + \lambda s = n'' + \lambda s, \text{ and}\\
&\nu'' = ((n^* + \lambda t) \bmod t) \div r = n^* \pmod t \div r = n^* \div r = n''.
\end{aligned} \tag{7}$$

Thus, equation (6) becomes $C(m^*, n^* + \lambda t) \equiv B(m'', n'' + \lambda s) H_{m'',n''}(m_0, n_0) \pmod p$. Now, if λ is chosen so that $p \nmid B(m'', n'' + \lambda s)$, then

$$H_{m'',n''}(m_0, n_0) \equiv B(m'', n'' + \lambda s)^{-1} C(m^*, n^* + \lambda t) \pmod p. \tag{8}$$

Theorem 3: Assume $p \nmid b$. Let $\lambda = \max\{0, m'' + n'' - (p-1)\}$. Then

$$C(m, n) \equiv B(m', n') B(m'', n'' + \lambda s)^{-1} C(m^*, n^* + \lambda t) \pmod p.$$

Proof: By Corollary 6, $s \mid p-1$. If $s < p-1$, then actually $s < (p-1)/2$, so $m'' + n'' < p-1$, whence $\lambda = 0$ and $p \nmid B(m'', n'' + \lambda s)$. If $s = p-1$ and $m'' + n'' < p$, then again we have $\lambda = 0$ and $p \nmid B(m'', n'' + \lambda s)$. Assume that $s = p-1$ and $m'' + n'' \geq p$. Now $n'' + \lambda s = n'' + \lambda(p-1) = \lambda p + (n'' - \lambda)$ and $0 \leq n'' - \lambda < p-1$. By Lucas's theorem, $B(m'', n'' + \lambda s) \equiv B(0, \lambda) B(m'', n'' - \lambda) \pmod p$, and this is not congruent to 0 as long as $m'' + n'' - \lambda \leq p-1$. Therefore, $\lambda = m'' + n'' - (p-1)$ is actually the *minimum* value that works. Now, in every case, equation (8) and Theorem 1 imply the desired conclusion. □

Thus, except when $s = p-1$ and $m'' + n'' \geq p$, the residue $C(m, n) \bmod p$ is given by this simple, symmetric expression:

$$C(m, n) \equiv B(m', n') B(m'', n'')^{-1} C(m^*, n^*) \pmod p.$$

Example 3: Consider the Fibonomial coefficient $C(6, 29) \bmod 3$. It appears in the 7th row and 30th column of Table 1. Since $u_n = F_n$ and $p = 3$, then $r = 4$, $t = 8$, and $s = 2$. Let $m = 6$ and $n = 29$. Then $m_0 = 2$, $m' = 1$, $m^* = 6$, and $m'' = 1$, while $n_0 = 1$, $n' = 7$, $n^* = 5$, and $n'' = 1$. Here $m'' + n'' - (p-1) = 1 + 1 - 2 = 0$, so $\lambda = 0$. Now

$$B(m', n') = B(1, 7) = B(1, 2 \times 3 + 1) \equiv B(0, 2) B(1, 1) \equiv 2 \pmod 3,$$
$$B(m'', n'' + \lambda s) = B(1, 1) = 2 \text{ and } 2^{-1} \equiv 2 \pmod 3,$$

and

$$C(m^*, n^* + \lambda t) = C(6, 5) \equiv 2 \pmod 3$$

so

$$C(m, n) \equiv B(m', n') B(m'', n'')^{-1} C(m^*, n^*) \equiv 2 \cdot 2 \cdot 2 \equiv 2 \pmod 3.$$

Theorem 3 may also be used to go back and extend Lemma 4 to a full r-step recurrence formula. The result is stated in the following tidy formula.

Corollary: If $p \nmid b$, then for $m, n \geq r$,

$$C(m, n) \equiv u_{r+1}^m C(m, n-r) + u_{r+1}^n C(m-r, n) \pmod p.$$

In terms of the $r \times r$ matrices $\mathbb{G}_{i,j} := [C(ir+h, jr+k)]$, where $0 \le h,\ k < r$, and $i, j \ge 0$, and the diagonal matrix $\mathbb{D} = diag\{u_{r+1}^0, u_{r+1}^1, \ldots, u_{r+1}^{r-1}\}$, the conclusion of the corollary may be rewritten as

$$\mathbb{G}_{i,j} \equiv u_{r+1}^{ir}\mathbb{D}\mathbb{G}_{i,j-1} + u_{r+1}^{jr}\mathbb{G}_{i-1,j}\mathbb{D} \pmod{p}.$$

For binomial coefficients, $u_{r+1} = p+1 \equiv 1 \pmod{p}$ and $\mathbb{D} = \mathbb{I}$, so $\mathbb{G}_{i,j} \equiv \mathbb{G}_{i,j-1} + \mathbb{G}_{i-1,j} \pmod{p}$, the $p \times p$ generalization of the Pascal triangle rule noted by Long [9]. For Fibonomial coefficients modulo 2, $u_{r+1} = F_4 \equiv 1 \pmod 2$ and again $\mathbb{D} = \mathbb{I}$, so $\mathbb{G}_{i,j} \equiv \mathbb{G}_{i,j-1} + \mathbb{G}_{i-1,j} \pmod 2$, as noted by Wells [15]. For Fibonomial coefficients modulo 3, which were considered in Example 2, $u_{r+1} = F_5 \equiv 2 \pmod 3$ and $\mathbb{D} \equiv \text{diag}\{1, 2, 1, 2\}$, so that $\mathbb{G}_{i,j} \equiv \mathbb{D}\mathbb{G}_{i,j-1} + \mathbb{G}_{i-1,j}\mathbb{D} \pmod 3$, which the reader may see illustrated in Table 2. [Note first that $\mathbb{D}\mathbb{H}_{i,j} \equiv \mathbb{H}_{i,j\pm1}$ and $\mathbb{H}_{i,j}\mathbb{D} \equiv \mathbb{H}_{i\pm1,j} \pmod 3$.]

7. WELLS'S THEOREM

By means of a bit of translation, Theorem 3 may be transformed into Wells's theorem. Let $N = m+n$ and, correspondingly, $N_0 = N \bmod r$, $N' = N \div r$, and $N'' = N' \bmod s$. Then,

$$C(m, n) = \begin{bmatrix} N \\ m \end{bmatrix}$$

and

$$B(m', n') = \binom{N'}{m'}.$$

Let $N' = \sum_{j\ge1} N_j p^{j-1}$ and $m' = \sum_{j\ge1} m_j p^{j-1}$ be the base-p representations of N' and m'. By the original Lucas theorem,

$$\binom{N'}{m'} \equiv \prod_{j\ge1} \binom{N_j}{m_j} \pmod{p}.$$

The result of Wells [14] is as follows.

Theorem 4 (Wells): If $p \nmid b$, then, for $N'' \ge m''$,

$$\begin{bmatrix} N \\ m \end{bmatrix} \equiv \binom{N''}{m''}^{-1} \prod_{j\ge1} \binom{N_j}{m_j} \begin{bmatrix} Nr + N_0 \\ m''r + m_0 \end{bmatrix} \pmod{p}$$

and, for $N'' < m''$,

$$\begin{bmatrix} N \\ m \end{bmatrix} \equiv \begin{cases} \binom{s+N''}{m''}^{-1} \prod_{j\ge1} \binom{N_j}{m_j} \begin{bmatrix} t+N''r+N_0 \\ m''r+m_0 \end{bmatrix} \pmod{p} & \text{if } s < p-1, \\ \binom{s}{m''}^{-1} \prod_{j\ge1} \binom{N_j}{m_j} \begin{bmatrix} (N''+1)t+N''r+N_0 \\ m''r+m_0 \end{bmatrix} \pmod{p} & \text{if } s = p-1, \end{cases}$$

where $N_0 = N \bmod r$, $N' = N \div r$, and $N'' = N' \bmod s$.

Proof: Let $n = N - m$. First, assume that $m_0 + n_0 \ge r$. Then $\begin{bmatrix} N \\ m \end{bmatrix} = C(m, n) \equiv 0 \pmod{p}$, by Lemma 3. Also, $N_0 = m_0 + n_0 - r$, so, for $Kr = N''r$, $t + N''r$, or $(N''+1)t + N''r$, we have

$$\begin{bmatrix} Kr + N_0 \\ m''r + m_0 \end{bmatrix} = C(m''r + m_0, (K-1-m)r + n_0) \equiv 0 \pmod{p},$$

again by Lemma 3, and so all congruences in the theorem's conclusion reduce to $0 \equiv 0$ when $m_0 + n_0 \geq r$. Next, assume $m_0 + n_0 < r$. Theorem 3 and the theorem of Lucas imply that

$$\begin{bmatrix} N \\ m \end{bmatrix} \equiv \binom{m'' + n'' + \lambda s}{m''}^{-1} \prod_{j \geq 1} \binom{N_j}{m_j} \begin{bmatrix} m^* + n^* + \lambda t \\ m^* \end{bmatrix} \pmod{p},$$

where $\lambda = \max\{0, m'' + n'' - (p-1)\}$. Refer to the mixed-radix addition

$$\begin{array}{r} m = m'''t + m''r + m_0 \\ +\ n = n'''t\ + n''r + n_0 \\ \hline N = N'''t + N''r + N_0 \end{array}$$

where $0 \leq m_0, n_0,\ N_0 < r,\ 0 \leq m'', n'',\ N'' < s$, and $0 \leq m''', n''',\ N''' < \infty$. Since $m_0 + n_0 < r$, there is no carry out of the rightmost column. If $N'' \geq m''$, then $m'' + n'' = N'' < s \leq p-1$, so $\lambda = 0$ and $m'' + n'' + \lambda s = N''$ and $m^* + n^* + \lambda t = m''r + m_0 + n''r + n_0 = N''r + N_0$, so the first formula is correct. Now assume $N'' < m''$. Then there is a carry out of the second column, so $N'' = m'' + n'' - s$. If $s < p-1$, then $m'' + n'' < 2s < p-1$, so $\lambda = 0$ and $m'' + n'' + \lambda s = s + N'' + 0$ and $m^* + n^* + \lambda t = m''r + m_0 + n''r + n_0 = (s + N'')r + (m_0 + n_0) = t + N''r + N_0$, and the formula for this case follows. Finally, if $s = p-1$, then $\lambda = m'' + n'' - (p-1) = N''$ and $m'' + n'' + \lambda s = s + N'' + N''s = s + N''(1+s) = p - 1 + N''p$, whence

$$\binom{m'' + n'' + \lambda s}{m''} \equiv \binom{p-1}{m''}\binom{N''}{0} \equiv \binom{s}{m''}$$

and

$$m^* + n^* + \lambda t = N''r + N_0 + 1t + N''t,$$

and the final case follows. □

Example 4: Let us find the value of the Fibonomial coefficient $\begin{bmatrix} 35 \\ 6 \end{bmatrix}$ modulo 3. This is equivalent to Example 3. Here $p = 3$, $r = 4$, $t = 8$, and $s = 2$. Corresponding to $m = 6$, we have $m_0 = 2$, $m' = 1$, and $m'' = 1$. Similarly, for $N = 35$, we have $N_0 = 3$, $N' = 8$, and $N'' = 0$. Also, $m_1 = 1$, $m_2 = 0$, $N_1 = 2$, and $N_2 = 2$. Here $N'' < m''$ and $s = p-1$, so

$$\begin{aligned} \begin{bmatrix} N \\ m \end{bmatrix} &\equiv \binom{s}{m''}^{-1}\binom{N_1}{m_1}\binom{N_2}{m_2}\begin{bmatrix} (N''+1)t + N''r + N_0 \\ m''r + m_0 \end{bmatrix} \\ &\equiv \binom{2}{1}^{-1}\binom{2}{1}\binom{2}{0}\begin{bmatrix} (0+1)8 + 0\cdot 4 + 3 \\ 1\cdot 4 + 2 \end{bmatrix} \\ &\equiv 2\cdot 2\cdot 1\cdot 2 \equiv 2 \pmod 3. \end{aligned}$$

This result is consistent, of course, with the calculation based on Theorem 3.

REFERENCES

1. Boris A. Bondarenko. *Generalized Pascal Triangles and Pyramids: Their Fractals, Graphs and Applications*. Trans. Richard C. Bollinger. Santa Clara, CA: The Fibonacci Association, 1993.
2. W. Antony Broomhead. "Pascal (mod p)." *Mathematical Gazette* **56** (1972):268-71.

3. Robert D. Fray. "Congruence Properties of Ordinary and q-Binomial Coefficients." *Duke Math. J.* **34** (1967):467-80.
4. Heiko von Harborth. "Über die Teilbarkeit im Pascal-Dreieck." *Mathematisch-physikalische Semesterberichte* **22** (1975):13-21.
5. Erhard Hexel & Horst Sachs. "Counting Residues Modulo a Prime in Pascal's Triangle." *Indian J. of Math.* **20** (1978):91-105.
6. John M. Holte. "A Lucas-Type Theorem for Fibonomial-Coefficient Residues." *The Fibonacci Quarterly* **32.1** (1994):60-68.
7. P. Horak & L. Skula. "A Characterization of the Second-Order Strong Divisibility Sequences." *The Fibonacci Quarterly* **23.2** (1985):126-32.
8. D. E. Knuth & H. S. Wilf. "The Power of a Prime that Divides a Generalized Binomial Coefficient." *J. reine angew. Math.* **396** (1989):212-19.
9. Calvin T. Long. "Pascal's Triangle Modulo p." *The Fibonacci Quarterly* **19.5** (1981):458-63.
10. E. Lucas. "Théorie des fonctions numériques simplement périodiques." *Amer. J. Math.* **1** (1878):184-240.
11. Marko Razpet. "On Divisibility of Binomial Coefficients." *Discrete Math.* **135** (1994):377-79.
12. J. B. Roberts. "On Binomial Coefficient Residues." *Canadian J. of Math.* **9** (1957):363-70.
13. Diana L. Wells. "Lucas' Theorem for Generalized Binomial Coefficients." *AMS Abstracts* **14** (1993):32.
14. Diana L. Wells. "Lucas' Theorem for Generalized Binomial Coefficients." Preprint.
15. Diana L. Wells. "The Fibonacci and Lucas Triangles Modulo 2." *The Fibonacci Quarterly* **32.2** (1994):111-23.
16. Diana L. Wells. "Residue Counts Modulo Three for the Fibonacci Triangle." In *Applications of the Fibonacci Numbers* **6:**521-36. Dordrecht: Kluwer, 1996.
17. S. Wolfram. "Geometry of Binomial Coefficients." *Amer. Math. Monthly* **92** (1984):566-71.

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

❖❖❖

GENERALIZED JACOBSTHAL POLYNOMIALS

Gospava B. Djordjević
Department of Mathematics, University of Niš, 16000 Leskovac, Yugoslavia
(Submitted August 1998-Final Revision March 1999)

1. INTRODUCTION

In this paper we study two classes of polynomials: the generalized Jacobsthal polynomials $\{J_{n,m}(x)\}$ and the generalized Jacobsthal-Lucas polynomials $\{j_{n,m}(x)\}$ defined, respectively, by

$$J_{n,m}(x) = J_{n-1,m}(x) + 2xJ_{n-m,m}(x), \quad n \geq m, \tag{1.1}$$

with $J_{0,m}(x) = 0$, $J_{n,m}(x) = 1$, $n = 1, 2, \ldots, m-1$, and

$$j_{n,m}(x) = j_{n-1,m}(x) + 2xj_{n-m,m}(x), \quad n \geq m, \tag{1.2}$$

with $j_{0,m}(x) = 2$, $j_{n,m}(x) = 1$, $n = 1, 2, \ldots, m-1$. In this paper we call these polynomials the generalized Jacobsthal polynomials.

The polynomials $J_{n,2}(x)$ and $j_{n,2}(x)$ are studied in [4].

For $m = 2$ and $x = 1$, we get the Jacobsthal numbers $\{J_{n,2}(1)\}$ and Jacobsthal-Lucas numbers $\{j_{n,2}(1)\}$, which are studied in [3].

Here we shall prove the list of characteristic properties of the polynomials $\{J_{n,m}(x)\}$ and $\{j_{n,m}(x)\}$. Also, we are going to introduce two classes of polynomials: $\{F_{n,m}(x)\}$ and $\{f_{n,m}(x)\}$. For $m = 2$, these polynomials are studied in [4]. Namely, we are going to exhibit some basic properties of the polynomials $\{J_{n,m}(x)\}$, $\{j_{n,m}(x)\}$, $\{F_{n,m}(x)\}$, and $\{f_{n,m}(x)\}$, to generalize the properties of the corresponding polynomials in [4].

2. POLYNOMIALS $J_{n,m}(x)$ AND $j_{n,m}(x)$

Using (1.1) and (1.2), we find the first $m+3$-members of the sequences $\{J_{n,m}(x)\}$ and $\{j_{n,m}(x)\}$, which are given in Table 1.

TABLE 1

n	$J_{n,m}(x)$	$\cdots$	$j_{n,m}(x)$	$\cdots$
0	0	$\cdots$	2	$\cdots$
1	1	$\cdots$	1	$\cdots$
2	1	$\cdots$	1	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$m-1$	1	$\cdots$	1	$\cdots$
m	1	$\cdots$	$1+4x$	$\cdots$
$m+1$	$1+2x$	$\cdots$	$1+6x$	$\cdots$
$m+2$	$1+4x$	$\cdots$	$1+8x$	$\cdots$
$m+3$	$1+6x$	$\cdots$	$1+10x$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Using the standard method, we find that the polynomials $\{J_{n,m}(x)\}$ have the following generating function,

$$F(x,t) = (1-t-2xt^m)^{-1} = \sum_{n=1}^{+\infty} J_{n,m}(x)t^{n-1}, \tag{2.1}$$

and the polynomials $\{j_{n,m}(x)\}$ have the generating function

$$G(x,t) = (1+4xt^{m-1})(1-t-2xt^m)^{-1} = \sum_{n=1}^{+\infty} j_{n,m}(x)t^{n-1}. \tag{2.2}$$

From (2.1) and (2.2), we get the following explicit representations:

$$J_{n,m}(x) = \sum_{k=0}^{[(n-1)/m]} \binom{n-1-(m-1)k}{k} (2x)^k; \tag{2.3}$$

$$j_{n,m}(x) = \sum_{k=0}^{[n/m]} \frac{n-(m-2)k}{n-(m-1)k} \binom{n-(m-1)k}{k} (2x)^k. \tag{2.4}$$

For $m=2$ in (2.3) and (2.4), we get the known polynomials $\{J_n(x)\}$ and $\{j_n(x)\}$ (see [4]), respectively.

We can prove the following theorem.

Theorem 2.1: The polynomials $J_{n,m}(x)$ and $j_{n,m}(x)$ satisfy the following equalities, where the superscript (k) denotes the k^{th} derivative with respect to x:

$$j_{n,m}(x) = J_{n,m}(x) + 4xJ_{n+1-m,m}(x); \tag{2.5}$$

$$J^{(k)}_{n,m}(x) = J^{(k)}_{n-1,m}(x) + 2^k J^{(k-1)}_{n-m,m}(x) + 2xJ^{(k)}_{n-m,m}(x), \quad k \geq 1; \tag{2.6}$$

$$j^{(k)}_{n,m}(x) = J^{(k)}_{n,m}(x) + 4kJ^{(k-1)}_{n+1-m,m}(x) + 4xJ^{(k)}_{n+1-m,m}(x); \tag{2.7}$$

$$j^{(k)}_{n,m}(x) = j^{(k)}_{n-1,m}(x) + 2^k j^{(k-1)}_{n-m,m}(x) + 2xj^{(k)}_{n-m,m}(x), \quad k \geq 1; \tag{2.8}$$

$$\sum_{i=0}^{n} J^{(k)}_{i,m}(x)J^{(s)}_{n-i,m}(x) = \left(2t^{m-1}(k+s+1)\binom{k+s}{k}\right)^{-1} J^{(k+s+1)}_{n,m}(x); \tag{2.9}$$

$$\sum_{i=0}^{n} J^{(k)}_{i,m}(x)j^{(s)}_{n-i,m}(x) = \frac{2t^{-m}-t^{1-m}}{2(k+s+1)\binom{k+s}{k}} J^{(k+s+1)}_{n,m}(x); \tag{2.10}$$

$$\sum_{i=0}^{n} j^{(k)}_{i,m}(x)j^{(s)}_{n-i,m}(x) = \frac{(2-t)^2}{2t^{m+1}(k+s+1)\binom{k+s}{k}} J^{(k+s+1)}_{n,m}(x); \tag{2.11}$$

$$\sum_{i=1}^{n} J_{i,m}(x) = \frac{J_{n+m,m}(x)-1}{2x}; \tag{2.12}$$

$$\sum_{i=1}^{n} j_{i,m}(x) = \frac{j_{n+m,m}(x)-1}{2x}. \tag{2.13}$$

Proof: From Table 1, we can see that (2.5) is true.

To prove the relations (2.6), (2.7), and (2.8), we will use (1.1), (2.5), and (1.2), respectively. Namely, differentiating (1.1), (2.5), and (1.2) k times with respect to x, we obtain equalities (2.6), (2.7), and (2.8), respectively.

From (2.1), we get

$$\frac{\partial^k F(x,t)}{\partial x^k} = \frac{2^k k! t^{mk}}{(1-t-2xt^m)^{k+1}} = \sum_{n=1}^{+\infty} J_{n,m}^{(k)}(x) t^{n-1}. \tag{1}$$

From (2.2), we get

$$\frac{\partial^s G(x,t)}{\partial x^s} = \frac{2^s s!(2-t) t^{ms-1}}{(1-t-2xt^m)^{s+1}} = \sum_{n=1}^{+\infty} j_{n,m}^{(s)}(x) t^{n-1}. \tag{2}$$

Using (1), we obtain

$$\frac{\partial^k F(x,t)}{\partial x^k} \cdot \frac{\partial^s F(x,t)}{\partial x^s} = \frac{2^{k+s} k! s! t^{m(k+s)}}{(1-t-2xt^m)^{k+s+2}}.$$

Since

$$\frac{\partial^k F(x,t)}{\partial x^k} \cdot \frac{\partial^s F(x,t)}{\partial x^s} = \sum_{n=2}^{\infty} \sum_{i=0}^{n} J_{n-i,m}^{(k)}(x) J_{i,m}^{(s)}(x) t^{n-2},$$

we have

$$\begin{aligned} \sum_{n=1}^{\infty} \sum_{i=0}^{n} J_{n-i,m}^{(k)}(x) J_{i,m}^{(s)}(x) t^{n-1} &= \frac{2^{k+s} k! s! t^{mk+ms+1}}{(1-t-2xt^m)^{k+s+2}} \quad \text{[by (1)]} \\ &= \frac{2^{k+s+1}(k+s+1)! k! s! t^{m(k+s+1)}}{2(k+s+1)! t^{m-1}(1-t-2xt^m)^{k+s+2}} \\ &= \frac{k! s!}{2(k+s+1)! t^{m-1}} \sum_{n=1}^{\infty} J_{n,m}^{(k+s+1)}(x) t^{n-1}. \end{aligned}$$

By the last equalities, we find

$$\sum_{i=0}^{n} J_{i,m}^{(k)}(x) J_{n-i,m}^{(s)}(x) = \left(2t^{m-1}(k+s+1)\binom{k+s}{k}\right)^{-1} J_{n,m}^{(k+s+1)}(x),$$

which is the desired equality (2.9).

In a similar way, from

$$\frac{\partial^k F(x,t)}{\partial x^k} \cdot \frac{\partial^s G(x,t)}{\partial x^s} = \frac{2^{k+s} k! s!(2-t) t^{mk+ms-1}}{(1-t-2xt^m)^{k+s+2}} \quad \text{[by (1) and (2)]},$$

we get (2.10):

$$\sum_{i=0}^{n} J_{i,m}^{(k)}(x) j_{n-i,m}^{(s)}(x) = \frac{2t^{-m} - t^{1-m}}{2(k+s+1)\binom{k+s}{k}} J_{n,m}^{(k+s+1)}(x).$$

Again, from (2), we get the equality (2.11). Using the recurrence relations (1.1) and (1.2), we can prove equalities (2.12) and (2.13), respectively.

Corollary 2.1: For $m = 1$, $m = 2$, and $m = 3$, we obtain (see [4]):

$$\begin{aligned} J_{n,1}(x) &= D_n(x), & j_{n,1}(x) &= d_n(x), \\ J_{n,2}(x) &= J_n(x), & j_{n,2}(x) &= j_n(x), \\ J_{n,3}(x) &= R_n(x), & j_{n,3}(x) &= r_n(x). \end{aligned}$$

Corollary 2.2: For $s = 0$ in (2.9) and for $k = 0$ in (2.10), we have

$$\sum_{i=0}^{n} J_{i,m}^{(k)}(x) J_{n-i,m}(x) = (2t^{m-1}(k+1))^{-1} J_{n,m}^{(k+1)}(x),$$

and

$$\sum_{i=0}^{n} j_{i,m}^{(s)}(x) J_{n-i,m}(x) = \frac{2t^{-m} - t^{1-m}}{2(s+1)} J_{n,m}^{(s+1)}(x),$$

where $J_{n,m}^{(0)}(x) \equiv J_{n,m}(x)$.

3. POLYNOMIALS $F_{n,m}(x)$ AND $f_{n,m}(x)$

First, we are going to introduce the polynomials $\{F_{n,m}(x)\}$ and $\{f_{n,m}(x)\}$ by

$$F_{n,m}(x) = F_{n-1,m}(x) + 2xF_{n-m,m}(x) + 3, \quad n \geq m, \tag{3.1}$$

with $F_{0,m}(x) = 0$, $F_{n,m}(x) = 1$, $n = 1, 2, \ldots, m-1$, and

$$f_{n,m}(x) = f_{n-1,m}(x) + 2xf_{n-m,m}(x) + 5, \quad n \geq m, \tag{3.2}$$

with $f_{0,m}(x) = 0$, $f_{n,m}(x) = 1$, $n = 1, 2, \ldots, m-1$. So, by (3.1), we find the first $m+2$-members of the sequence $\{F_{n,m}(x)\}$:

$$F_{0,m}(x) = 0, \quad F_{1,m}(x) = 1, \ldots, F_{m-1,m}(x) = 1,$$
$$F_{m,m}(x) = 4, \quad F_{m+1,m}(x) = 7 + 2x, \quad F_{m+2,m}(x) = 10 + 4x.$$

By (3.2), we find:

$$f_{0,m}(x) = 0, \quad f_{1,m}(x) = 1, \ldots, f_{m-1,m}(x) = 1,$$
$$f_{m,m}(x) = 6, \quad f_{m+1,m}(x) = 11 + 2x, \quad f_{m+2,m}(x) = 16 + 4x.$$

For $m = 2$, the polynomials $\{F_{n,m}(x)\}$ and $\{f_{n,m}(x)\}$ are studied in [4].

Theorem 3.1: The polynomials $F_{n,m}(x)$ and $f_{n,m}(x)$ have, respectively, the following explicit representations:

$$F_{n-1+m,m}(x) = J_{n-1+m,m}(x) + 3\sum_{r=0}^{[n/m]} \binom{n-(m-1)r}{r+1} (2x)^r; \tag{3.3}$$

$$f_{n-1+m,m}(x) = J_{n-1+m,m}(x) + 5\sum_{r=0}^{[n/m]} \binom{n-(m-1)r}{r+1} (2x)^r. \tag{3.4}$$

Proof: From (1.1) and (3.1), we see that (3.3) is true for $n = 1$. Suppose that (3.3) is true for n, i.e.,

$$F_{n-1+m,m}(x) = J_{n-1+m,m}(x) + 3\sum_{r=0}^{[n/m]} \binom{n-(m-1)r}{r+1} (2x)^r.$$

Then

$$\begin{aligned} F_{n+m,m}(x) &= F_{n-1+m,m}(x) + 2xF_{n,m}(x) + 3 \\ &= J_{n-1+m,m}(x) + 3\sum_{r=0}^{[n/m]} \binom{n-(m-1)r}{r+1} (2x)r \\ &\quad + 2x\left(J_{n,m}(x) + 3\sum_{r=0}^{[(n-m+1)/m]} \binom{n+1-m-(m-1)r}{r+1} (2x)^r \right) + 3 \end{aligned}$$

$$= J_{n+m,m}(x) + 3\sum_{r=0}^{[(n+1)/m]} \binom{n+1-(m-1)r}{r+1} (2x)^r.$$

By induction on n, we conclude that (3.3) is true for all n.

Similarly, we can prove that equality (3.4) is true for all n.

The polynomials $F_{n,2}(x)$ and $f_{n,2}(x)$ are studied in [4].

Theorem 3.2: The polynomials $\{F_{n,m}(x)\}$ and $\{f_{n,m}(x)\}$ satisfy the following relations:

$$2xF_{n,m}(x) = J_{n+m,m}(x) + 2J_{n+1,m}(x) - 2x\sum_{i=1}^{m-2} J_{n-i,m}(x) - 3; \tag{3.5}$$

$$2xf_{n,m}(x) = J_{n+m,m}(x) + 4J_{n+1,m}(x) - 2x\sum_{i=1}^{m-2} J_{n-i,m}(x) - 5. \tag{3.6}$$

Proof: From (1.1) and (1.2), we see that (3.5) is true for $n = 0, 1, \ldots$. Assume (3.5) is true for $n = k$, i.e.,

$$2xF_{k,m}(x) = J_{k+m,m}(x) + 2J_{k+1,m}(x) - 2x\sum_{i=1}^{m-2} J_{k-i,m}(x) - 3.$$

Then

$$\begin{aligned} F_{k+1,m}(x) &= F_{k,m}(x) + 2xF_{k+1-m,m}(x) + 3 \quad \text{[by (3.1)]} \\ &= \frac{J_{k+m,m}(x) + 2J_{k+1,m}(x) - 2x\sum_{i=1}^{m-2} J_{k-i,m}(x) - 3}{2x} \\ &\quad + 2x\frac{J_{k+1,m}(x) + 2J_{k+2-m,m}(x) - 2x\sum_{i=0}^{m-2} J_{k+1-m-i,m}(x) - 3}{2x} + 3 \\ &= \frac{J_{k+1+m,m}(x) + 2J_{k+2,m}(x) - 2x\sum_{i=0}^{m-2} J_{k+1-i,m}(x) - 3}{2x}. \end{aligned}$$

By induction on n, we conclude that (3.5) is true for all n. In a similar way, we can prove that (3.6) is true for all n.

From (3.5) and (3.6), we get

$$f_{n,m}(x) - F_{n,m}(x) = \frac{J_{n+1,m}(x) - 1}{x}.$$

For $m = 2$ in the last equality, we obtain the known equality (6.11) in [4].

REFERENCES

1. Verner E. Hoggatt, Jr., & Marjorie Bicknell-Johnson. "Convolution Arrays for Jacobsthal and Fibonacci Polynomials." *The Fibonacci Quarterly* **16.5** (1978):385-402.
2. A. F. Horadam. "Jacobsthal and Pell Curves." *The Fibonacci Quarterly* **26.1** (1988):77-83.
3. A. F. Horadam. "Jacobsthal Representation Numbers." *The Fibonacci Quarterly* **34.1** (1996): 40-53.
4. A. F. Horadam. "Jacobsthal Representation Polynomials." *The Fibonacci Quarterly* **35.2** (1997):137-48.

AMS Classification Numbers: 11B39, 26A24, 11B83

❖❖❖

CONDITIONS FOR THE EXISTENCE OF GENERALIZED FIBONACCI PRIMITIVE ROOTS

Hua-Chieh Li
Department of Mathematics, National Tsing Hua University
Hsinchu, Taiwan 30043, Republic of China
(Submitted August 1998-Final Revision October 1998)

1. INTRODUCTION

Consider sequences of integers $\{U_n\}_{n=0}^{\infty}$ defined by $U_n = aU_{n-1} + bU_{n-2}$ for all integers $n \geq 2$, where $U_0 = 0$, $U_1 = 1$, a and b are given integers. We call these sequences generalized Fibonacci sequences with parameters a and b. In the case where $a = b = 1$, the sequence $\{U_n\}_{n=0}^{\infty}$ is called the Fibonacci sequence, and we denote its terms by $F_0, F_1, \ldots$.

The polynomial $f(x) = x^2 - ax - b$ with discriminant $D = a^2 + 4b$ is called the characteristic polynomial of the sequence $\{U_n\}_{n=0}^{\infty}$. Suppose that $f(x) = 0$ has two distinct solutions α and β. Then we can express U_n in the *Binet form*,

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

This and its relative $V_n = \alpha^n + \beta^n$ are known as *Lucas functions* as well and have a rich history. Please see the pioneering work of the late D. Lehmer [2] for more detail. Let p be a prime number. If $x = g$ satisfies the congruence $f(x) = x^2 - ax - b \equiv 0 \pmod{p}$, then by setting $W_0 = 1$, $W_1 = g$, and $W_n = aW_{n-1} + bW_{n-2}$, we have that $W_n \equiv g^n \pmod{p}$. We have given particular attention to those cases having the longest possible cycles, i.e., the number g being a primitive root modulo p; these are the most important cases in practical applications of the theory. We call g a generalized Fibonacci primitive root modulo p with parameters a and b if g is a root of $x^2 - ax - b \equiv 0 \pmod{p}$ and g is a primitive root modulo p. In particular, in the case $a = b = 1$, we call g a Fibonacci primitive root.

Fibonacci primitive roots modulo p have an extensive literature (see, e.g., [1], [3], [4], [7], [8], and [9]). For generalized Fibonacci primitive roots modulo p, R. A. Mollin [5] dealt with the case $a = 1$ and B. M. Phong [6] dealt with the case $b = \pm 1$. Mollin's work was the first to introduce the notion of a generalized Fibonacci primitive root based upon the pioneering work of the last D. Shanks [8]. In this paper we consider even more general cases, i.e., with arbitrary a and b. Our main theorem generalizes the results of Mollin and Phong.

2. NOTATIONS AND PRELIMINARY RESULTS

Let $\{U_n\}_{n=0}^{\infty}$ be the generalized Fibonacci sequence with parameters a and b. In this section we always suppose that b is relatively prime to m and suppose that $x^2 - ax - b \equiv 0 \pmod{m}$ has two distinct solutions modulo m.

For convenience, we introduce some notations:

(1) Let α be an integer relatively prime to m. Denote $\mathrm{ord}_m(\alpha)$ the least positive integer x such that $\alpha^x \equiv 1 \pmod{m}$.

(2) $k(m)$ is called the period of the sequence $\{U_n\}_{n=0}^{\infty}$ modulo m if it is the smallest positive integer for which $U_{k(m)} \equiv 0 \pmod{m}$ and $U_{k(m)+1} \equiv 1 \pmod{m}$.

(3) $[x, y]$ is the least common multiple of x and y.

(4) For an odd prime p, (β/p) denotes the Legendre symbol; i.e., $(\beta/p) = 1$ if and only if $y^2 \equiv \beta \pmod{p}$ is solvable.

We now state some elementary results that will be useful later.

Suppose that α and β are distinct solutions to $x^2 - ax - b \equiv 0 \pmod{m}$. Let $l = [\text{ord}_m(\alpha), \text{ord}_m(\beta)]$. Since $\alpha\beta \equiv -b \pmod{m}$, we have that $1 \equiv (\alpha\beta)^l \equiv (-b)^l \pmod{m}$. This implies that

$$\text{ord}_m(-b) \mid [\text{ord}_m(\alpha), \text{ord}_m(\beta)].$$

By a similar argument, we have that

$$\text{ord}_m(\alpha) \mid [\text{ord}_m(-b), \text{ord}_m(\beta)]$$

and

$$\text{ord}_m(\beta) \mid [\text{ord}_m(\alpha), \text{ord}_m(-b)].$$

In particular, if $\text{ord}_m(-b) \mid \text{ord}_m(\alpha)$, then $\text{ord}_m(\beta) \mid \text{ord}_m(\alpha)$ and vice versa. We have the following lemma.

Lemma 2.1: Let α and β be the two distinct solutions to $x^2 - ax - b \equiv 0 \pmod{m}$. Suppose that $\text{ord}_m(-b) \mid \text{ord}_m(\alpha)$. Then we have $\text{ord}_m(\beta) \mid \text{ord}_m(\alpha)$. Furthermore, $\text{ord}_m(\beta) = \text{ord}_m(\alpha)$ if and only if $\text{ord}_m(-b) \mid \text{ord}_m(\beta)$.

Lemma 2.2: Let α and β be the two distinct solutions to $x^2 - ax - b \equiv 0 \pmod{m}$ and let $k(m)$ be the period of the generalized Fibonacci sequence with parameters a and b modulo m. Then

$$k(m) = [\text{ord}_m(\alpha), \text{ord}_m(\beta)].$$

Proof: Since α and β are the two distinct solutions to $x^2 - ax - b \equiv 0 \pmod{m}$,

$$\alpha^n \equiv a\alpha^{n-1} + b\alpha^{n-2} \pmod{m} \quad \text{and} \quad \beta^n \equiv a\beta^{n-1} + b\beta^{n-2} \pmod{m}.$$

Consider the sequence $\{A_n\}_{n=0}^{\infty}$, where $A_n - b\alpha U_{n-2} + \alpha^2 U_{n-1}$. Since $\{A_n\}_{n=0}^{\infty}$ and $\{\alpha^n\}_{n=0}^{\infty}$ both satisfy the same recurrence relation modulo m and $A_2 \equiv \alpha^2$, $A_3 \equiv \alpha^3 \pmod{m}$. Therefore, we have that $A_n \equiv \alpha^n \pmod{m}$ for all $n \geq 2$. Thus, $\alpha^n \equiv b\alpha U_{n-2} + \alpha^2 U_{n-1} \pmod{m}$ and, similarly, we have $\beta^n \equiv b\beta U_{n-2} + \beta^2 U_{n-1} \pmod{m}$. This tells us that if $k(m)$ is the period of the generalized Fibonacci sequence modulo m then

$$\alpha^{k(m)+2} \equiv b\alpha U_{k(m)} + \alpha^2 U_{k(m)+1} \pmod{m}.$$

Hence, $\text{ord}_m(\alpha) \mid k(m)$ and $\text{ord}_m(\beta) \mid k(m)$. On the other hand, consider the Binet form

$$U_n \equiv \frac{\alpha^n - \beta^n}{\alpha - \beta} \pmod{m}.$$

Let $l = [\text{ord}_m(\alpha), \text{ord}_m(\beta)]$. $\alpha^l - \beta^l \equiv 0 \pmod{m}$ and $\alpha^{l+1} - \beta^{l+1} \equiv \alpha - \beta \pmod{m}$. This implies that $U_l \equiv 0 \pmod{m}$ and $U_{l+1} \equiv 1 \pmod{m}$. Thus, $k(m) \mid [\text{ord}_m(\alpha), \text{ord}_m(\beta)]$. □

3. GENERALIZED FIBONACCI PRIMITIVE ROOTS MODULO p

The conditions for the existence of Fibonacci primitive roots modulo p and their properties were studied by several authors. In this section we will generalize their results to generalized Fibonacci primitive roots. Again $\{U_n\}_{n=0}^{\infty}$ is the generalized Fibonacci sequence with parameters a and b. For completeness, we begin with special cases. Since the argument is quite straightforward, we omit the proofs.

Proposition 3.1: Let p be an odd prime and let $\{U_n\}_{n=0}^{\infty}$ be the generalized Fibonacci sequence with parameters a and b.

(1) Suppose that $p \mid b$ but $p \nmid a$. Then there exists a generalized Fibonacci primitive root for $\{U_n\}_{n=0}^{\infty}$ modulo p if and only if $z = p$ is the least integer greater than 1 such that $U_z \equiv 1 \pmod{p}$. Moreover, in this case, a is the unique generalized Fibonacci primitive root for $\{U_n\}_{n=0}^{\infty}$ modulo p.

(2) Suppose that $p \mid a^2 + 4b$. Then there exists a generalized Fibonacci primitive root for $\{U_n\}_{n=0}^{\infty}$ modulo p if and only if $k(p) = p(p-1)$. Moreover, in this case, $\alpha \equiv a/2 \pmod{p}$ is the unique generalized Fibonacci primitive root for $\{U_n\}_{n=0}^{\infty}$ modulo p.

For the remainder of this section we assume that p is an odd prime with $(D/p) = 1$, where $D = a^2 + 4b$ and $p \nmid b$.

In the Fibonacci case, $\{F_n\}_{n=0}^{\infty}$ possesses a Fibonacci primitive root modulo p if and only if the period of $\{F_n\}_{n=0}^{\infty}$ modulo p equals $p-1$ (for results on Fibonacci primitive roots, we refer to [6]). This is not always true for generalized Fibonacci primitive roots. We have the following example.

Example: Let $a = 1, b = 2$, and $p = 7$. $\{U_n\}_{n=0}^{\infty} \equiv \{0, 1, 1, 3, 5, 4, 0, 1, \ldots\} \pmod{7}$. The period of $\{U_n\}_{n=0}^{\infty}$ modulo p is $p-1$. $x \equiv 2$ and 6 (mod 7) are distinct roots to $x^2 - x - 2 \equiv 0 \pmod{7}$ but neither 2 nor 6 is a primitive root modulo 7. Hence, there is no generalized Fibonacci primitive root modulo 7 for $\{U_n\}_{n=0}^{\infty}$ with parameters 1 and 2.

However, by Lemma 2.2, there is no generalized Fibonacci primitive root modulo p if $k(p) \neq p-1$.

Lemma 3.2: Let α and β be two distinct roots of $x^2 - ax - b \equiv 0 \pmod{p}$. Then there exists a generalized Fibonacci primitive root modulo p for $\{U_n\}_{n=0}^{\infty}$ with parameters a and b if and only if $k(p) = p-1$ and either $\operatorname{ord}_p(-b) \mid \operatorname{ord}_p(\alpha)$ or $\operatorname{ord}_p(-b) \mid \operatorname{ord}_p(\beta)$.

Proof: Suppose that α is a primitive root modulo p. Then $\operatorname{ord}_p(-b) \mid \operatorname{ord}_p(\alpha)$ by Euler's theorem, and $k(p) = p-1$ by Lemma 2.2. Conversely, suppose that $\operatorname{ord}_p(-b) \mid \operatorname{ord}_p(\alpha)$. Then $\operatorname{ord}_p(\beta) \mid \operatorname{ord}_p(\alpha)$ by Lemma 2.1, and hence $k(p) = \operatorname{ord}_p(\alpha)$ by Lemma 2.2. By the assumption, $k(p) = p-1$, and our proof is complete. □

Theorem 3.3: Suppose that $\operatorname{ord}_p(-b) = q$, where q is a prime power of 1. Then there exists a generalized Fibonacci root modulo p for $\{U_n\}_{n=0}^{\infty}$ with parameters a and b if and only if $k(p) = p-1$.

Proof: Let α and β be two distinct roots of $x^2 - ax - b \equiv 0 \pmod{p}$. Since $q = \operatorname{ord}_p(-b) \mid [\operatorname{ord}_p(\alpha), \operatorname{ord}_p(\beta)]$ and q is a prime power, this implies $\operatorname{ord}_p(-b) \mid \operatorname{ord}_p(\alpha)$ or $\operatorname{ord}_p(-b) \mid \operatorname{ord}_p(\beta)$. By Lemma 3.2, our claim follows. □

Example: Consider the Fibonacci sequence. Since $b=1$, $\text{ord}_p(-b)=2$. We have that there exists a Fibonacci primitive root modulo p if and only if the period of the Fibonacci sequence modulo p is $p-1$.

Naturally, we ask if anything more can be said about the existence of generalized Fibonacci primitive roots modulo p with parameters a and b, for $\text{ord}_p(-b)$ not a prime power. The following example shows that nothing more can be said in this case.

Example:

(1) We have that $a=1$, $b=2$, and $p=7$. $\text{ord}_7(-2)=2\cdot 3$, and there is no generalized Fibonacci primitive root modulo 7 with parameters 1 and 2.

(2) Let $a=-1$, $b=2$, and $p=7$.Then $\{U_n\}_{n=0}^{\infty}\equiv\{0,1,6,3,2,4,0,1,\ldots\}\pmod 7$. The period of $\{U_n\}_{n=0}^{\infty}$ modulo p is $p-1$, and $x\equiv 5$ and $1 \pmod 7$ are distinct roots of $x^2-x-2\equiv 0 \pmod 7$. 5 is a primitive root modulo 7. Hence, there is a general-ized Fibonacci primitive root modulo 7 for $\{U_n\}_{n=0}^{\infty}$ with parameters -1 and 2.

Suppose that $\text{ord}_p(-b)=q$. Let α and β be two distinct roots of $x^2-ax-b\equiv 0 \pmod p$. Let $\text{ord}_p(\alpha)=n_1$ and let $\text{ord}_p(\beta)=n_2$. Suppose that $q\mid n_1$. Then, by Lemma 2.1, we have that $n_2\mid n_1$. Moreover, since $(\alpha)^{qn_2}\equiv(\alpha\beta)^{qn_2}\equiv(-b)^{qn_2}\equiv 1 \pmod p$, we have that $n_2\mid n_1$ and $n_1\mid qn_2$.

Theorem 3.4: Suppose that $\text{ord}_p(-b)=q$ (hence $q\mid p-1$), where q is a prime power. Suppose also that the period of the generalized Fibonacci sequence with parameters a and b modulo p is $p-1$. Then we have the following:

(1) Suppose that $q^2\mid p-1$. Then there exist two distinct general Fibonacci primitive roots modulo p with parameters a and b.

(2) Suppose that $q\nmid(p-1)/2$. Then there exists exactly one generalized Fibonacci primitive root modulo p with parameters a and b.

Proof:

(1) Let α and β be two distinct roots of $x^2-ax-b\equiv 0 \pmod p$. By Theorem 3.3, the assumption implies that either α or β is a primitive root modulo p; let us say that α is a primitive root. By Lemma 2.1, $q\mid\text{ord}_p(\beta)$ if and only if β is a primitive root modulo p. Suppose that $q\nmid\text{ord}_p(\beta)$. By the assumption $q^2\mid p-1$, it follows that $p-1\nmid q\,\text{ord}_p(\beta)$. This contradicts the argument above which says that $\text{ord}_p(\alpha)=p-1\mid q\,\text{ord}_p(\beta)$. Therefore, β is also a primitive root modulo p.

(2) $\text{ord}_p(-b)\nmid(p-1)/2$ is equivalent to $(-b/p)=-1$. Since $\alpha\beta=-b$, it is impossible that $(\alpha/p)=-1$ and $(\beta/p)=-1$. Our claim follows. □

Remark: Theorems 3.3 and 3.4 generalize Phong ([6], Theorem 1). In his case, $b=1$, and hence $\text{ord}_p(-b)=2$. Therefore, suppose $k(p)=p-1$. $p\equiv 1 \pmod 4$ (i.e., $4\mid p-1$) implies the existence of two distinct generalized Fibonacci primitive roots modulo p, and $p\equiv -1 \pmod 4$ (i.e., $2\nmid(p-1)/2$) implies the existence of exactly one generalized Fibonacci primitive root modulo p.

Suppose that $q^2\nmid p-1$. There may be two or only one generalized Fibonacci primitive root modulo p. Our next example illustrates these cases.

Example:

(1) Consider $a=1, b=2$, and $p=11$. $\text{ord}_p(-b)=5$ and $5^2 \nmid p-1$. $\{U_n\}_{n=0}^{\infty} \equiv \{0, 1, 1, 3, 5, 0, 10, 10, 8, 6, 0, 1, \ldots\} \pmod{11}$. The period $\{U_n\}_{n=0}^{\infty}$ modulo p is $p-1$, and $x \equiv 2$ and $-1 \pmod{11}$ are distinct roots of $x^2 - x - 2 \equiv 0 \pmod{11}$. 2 is a primitive root modulo 11 and -1 is not a primitive root modulo 11. Hence, there is a generalized Fibonacci primitive root modulo 11 for $\{U_n\}_{n=0}^{\infty}$ with parameters 1 and 2.

(2) Consider $a=-1$, $b=6$, and $p=11$. $\text{ord}_p(-b)=5$ and $5^2 \nmid p-1$. $\{U_n\}_{n=0}^{\infty} \equiv \{0, 1, 10, 7, 9, 0, 10, 1, 4, 2, 0, 1, \ldots\} \pmod{11}$. The period $\{U_n\}_{n=0}^{\infty}$ modulo p is $p-1$, and $x \equiv 2$ and $8 \pmod 7$ are distinct roots of $x^2 + x - 6 \equiv 0 \pmod{11}$. Both 2 and 8 are primitive roots modulo 11. Hence, there are two generalized Fibonacci primitive roots modulo 11 for $\{U_n\}_{n=0}^{\infty}$ with parameters -1 and 6.

4. SOME INTERESTING EXAMPLES

In [8], D. Shanks asked whether there exist infinitely many primes possessing Fibonacci primitive roots. For generalized Fibonacci primitive roots similar questions can be asked. In [4], Mays proved that if $p=60k-1$ and $q=30k-1$ are both prime, then there exists a Fibonacci primitive root modulo p. Phong (see [6], Corollary 3) generalized Mays' result for a generalized Fibonacci sequence with parameters a and $b=1$, which says that if a is an integer and both q and $p=2q+1$ are primes with $(D/p)=1$, where $D=a^2+4$, then there exists exactly one generalized Fibonacci primitive root modulo p with parameters a and $b=1$. Mollin (see [5], Theorem 1), following Mays' method, proved the following: Suppose that $p>b>2$ and $(D/p)=1$, where $D=4b+1$ and $p=2q+1$ is a prime with q an odd prime. Furthermore, suppose that b has order q modulo p. Then there exists a generalized Fibonacci primitive root modulo p with parameters $a=1$ and b. Our next theorem generalizes Phong and Mollin's results.

Theorem 4.1: Suppose that $p=2q+1$ is a prime with q an odd prime and suppose that $(D/p)=1$, where $D=a^2+4b$. Furthermore, suppose that $1+a-b \not\equiv 0 \pmod p$ and $\text{ord}_p(b)=1$ or q. Then there exists exactly one generalized Fibonacci primitive root modulo p with parameters a and b.

Proof: Suppose that $\text{ord}_p(-b)=q$. Then $b^q \equiv -1 \pmod p$. This contradicts our assumption that $\text{ord}_p(b)=1$ or q. Our assumption also says that $\text{ord}_p(-b) \neq 1$, because otherwise $\text{ord}_p(b)=2$. Therefore, the possible order for $-b$ modulo p is 2 or $2q$. Let α and β be two distinct roots of $x^2 - ax - b \equiv 0 \pmod p$. Since $\text{ord}_p(-b) \mid [\text{ord}_p(\alpha), \text{ord}_p(\beta)]$, this implies that either $\text{ord}_p(\alpha)$ is even or $\text{ord}_p(\beta)$ is even; say that $\text{ord}_p(\alpha)$ is even. Now, since -1 is not a root of $x^2 - ax - b \equiv 0 \pmod p$, by the assumption, it follows that $\text{ord}_p(\alpha) = 2q = p-1$, and by the same reasoning as in Theorem 3.4(2), there exists exactly one generalized Fibonacci primitive root modulo p.

Remark: Suppose that $p=2q+1$ is a prime with q an odd prime and suppose that $(D/p)=1$, where $D=a^2+4b$. Furthermore, suppose that $1+a-b \not\equiv 0 \pmod p$ and $b \not\equiv -1 \pmod p$. Let α and β be two roots of $x^2 - ax - b \equiv 0 \pmod p$. Then Theorem 4.1 says that among α, β, and $-\alpha\beta$ there exists one primitive root modulo p. Unfortunately, we do not know whether or not there exist infinitely many such p.

In [10], Wall asked whether, for a Fibonacci sequence, $k(p) = k(p^2)$ is always impossible; up to now, this is still an open question. According to Williams [11], $k(p) \neq k(p^2)$ for every odd prime p less than 10^9. Our next proposition states that, for a generalized Fibonacci sequence, it is possible that $k(p) = k(p^2)$.

Proposition 4.2: For any odd prime p, there exists a generalized Fibonacci sequence with parameters a and b such that $k(p) = k(p^2)$.

Proof: For any odd prime p, choose $\alpha \not\equiv 0 \pmod{p}$ and $\beta \not\equiv 0 \pmod{p}$ such that $\alpha \not\equiv \beta \pmod{p}$. By Hensel's lemma, there exist $\alpha' \equiv \alpha \pmod{p}$ and $\beta' \equiv \beta \pmod{p}$ such that $\text{ord}_{p^2}(\alpha') = \text{ord}_p(\alpha)$ and $\text{ord}_{p^2}(\beta') = \text{ord}_p(\beta)$. Choose $a = \alpha' + \beta'$ and $b = -\alpha'\beta'$. Consider the generalized Fibonacci sequence $\{U_n\}_{n=0}^{\infty}$ with parameters a and b. Then, by Lemma 2.2,

$$k(p) = [\text{ord}_p(\alpha'), \text{ord}_p(\beta')] = [\text{ord}_{p^2}(\alpha'), \text{ord}_{p^2}(\beta')] = k(p^2). \quad \square$$

Example: For $p = 5$, consider $\alpha = 2$ and $\beta = 1$. We have that $\text{ord}_{25}(7) = \text{ord}_5(2) = 4$ and $\text{ord}_{25}(1) = \text{ord}_5(1) = 1$. Let $a = 7 + 1 = 8$ and $b = -7$. Then $\{U_n\}_{n=0}^{\infty} \equiv \{0, 1, 3, 2, 0, 1, \ldots\} \pmod{5}$ and $\{U_n\}_{n=0}^{\infty} \equiv \{0, 1, 8, 7, 0, 1, \ldots\} \pmod{25}$.

ACKNOWLEDGMENT

The author would like to express his appreciation to the anonymous referee for making valuable suggestions regarding the presentation of this paper.

REFERENCES

1. P. Kiss & B. M. Phong. "On the Connection between the Rank of Apparition of a Prime p in the Fibonacci Sequence and the Fibonacci Primitive Roots." *The Fibonacci Quarterly* **15.4** (1977):347-49.
2. D. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. of Math.* **31** (1930):419-48.
3. M. J. DeLeon. "Fibonacci Primitive Roots and Period of the Fibonacci Numbers Modulo p." *The Fibonacci Quarterly* **15.4** (1977):353-55.
4. M. E. Mays. "A Note on Fibonacci Primitive Roots." *The Fibonacci Quarterly* **20.2** (1982): 111.
5. R. A. Mollin. "Generalized Fibonacci Primitive Roots and Class Numbers of Real Quadratic Fields." *The Fibonacci Quarterly* **24.1** (1986):46-53.
6. B. M. Phong. "Lucas Primitive Roots." *The Fibonacci Quarterly* **29.1** (1991):66-71.
7. D. Shanks. *Solved and Unsolved Problems in Number Theory*. 2nd ed. New York: Chelsea, 1978.
8. D. Shanks. "Fibonacci Primitive Roots." *The Fibonacci Quarterly* **10.2** (1972):162-68.
9. D. Shanks & L. Taylor. "An Observation on Fibonacci Primitive Roots." *The Fibonacci Quarterly* **11.2** (1973):159-60.
10. D. D. Wall. "Fibonacci Series Modulo m." *Amer. Math. Monthly* **67** (1960):525-32.
11. H. C. Williams. "A Note on the Fibonacci Quotient $F_{p-\varepsilon}/p$." *Canad. Math. Bull.* **25** (1982): 366-70.

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

❖❖❖

FAMILIES OF SOLUTIONS OF A CUBIC DIOPHANTINE EQUATION

Marc Chamberland
Department of Mathematics and Computer Science, Grinnell College, Grinnell, IA 50112
E-mail: chamberl@math.grin.edu
(Submitted August 1998-Final Revision February 1999)

This study started with an unusual advertisement which appeared (January 6, 1996) in *The Globe and Mail*, Canada's national newspaper. Vivikanand Kadarnauth (of Toronto) presented the "first few cases" in a family of solutions to the "cubic version of the Pythagorean equation"

$$a^3+b^3+c^3=d^3 \tag{1}$$

as

$$4^3+5^3+3^3=6^3,\ 4^3+17^3+22^3=25^3,$$
$$16^3+23^3+41^3=44^3,\ 16^3+47^3+108^3=111^3,$$
$$64^3+107^3+405^3=408^3,\ 64^3+155^3+664^3=667^3.$$

Mr. Kadarnauth then asked the reader to find the general pattern. Some of the patterns indicate that the general solution is

$$(a,b,c,d)=(2^{2m},2\cdot 2^{2m}-3\cdot 2^m+3,2^{3m}-2\cdot 2^{2m}+3\cdot 2^m-3,2^{3m}-2\cdot 2^{2m}+3\cdot 2^m)$$

and

$$(a,b,c,d)=(2^{2m},2\cdot 2^{2m}+3\cdot 2^m+3,2^{3m}+2\cdot 2^{2m}+3\cdot 2^m,2^{3m}+2\cdot 2^{2m}+3\cdot 2^m+3),$$

where m varies over the positive integers. One may generalize this by replacing 2^m with x, thus yielding the one-parameter polynomial families of solutions

$$(a,b,c,d)=(x^2,2x^2-3x+3,x^3-2x^2+3x-3,x^3-2x^2+3x) \tag{2}$$

and

$$(a,b,c,d)=(x^2,2x^2+3x+3,x^3+2x^2+3x,x^3+2x^2+3x+3). \tag{3}$$

The second family (3) is equivalent to (2). This is seen by replacing x with $-x$ in (2) and re-arranging the terms, since $a^3+b^3+c^3=d^3$ implies $a^3+b^3+(-d)^3=(-c)^3$. By letting $x=v/u$ in (3) and multiplying by u^3 gives the family of solutions listed by Jandasek (see [3], p. 559):

$$(a,b,c,d)=(uv^2,3u^2v+2uv^2+v^3,3u^3+3u^2v+2uv^2,3u^3+3u^2v+2uv^2+v^3). \tag{4}$$

The cubic Diophantine equation (1) has been studied for over 400 years. In 1591, P. Bungus (see [3], p. 550) found the smallest positive solution mentioned above, namely

$$4^3+5^3+3^3=6^3, \tag{5}$$

the same year that Vieta found a family of solutions. (Perelman writes on page 139 in [7]: "It is said that [equation (5)] highly intrigued Plato.") Almost 200 years later, Euler (see [3], p. 552) found that the general **rational** solution to equation (1) may be represented (see [6], p. 292) as

$$\begin{aligned}(a,b,c,d) = (&\sigma(-(\xi-3\eta)(\xi^2+3\eta^2)+1),\\ &\sigma((\xi^2+3\eta^2)^2-(\xi+3\eta)),\\ &\sigma((\xi+3\eta)(\xi^2+3\eta^2)-1),\\ &\sigma((\xi^2+3\eta^2)^2-(\xi-3\eta))),\end{aligned} \tag{6}$$

where σ, ξ, and η are rationals. The variable σ is simply a scaling factor reflecting the homogeneity of equation (1). Ramanujan [2] also gave a general solution as

$$(a,b,c,d) = (\alpha+\lambda^2\gamma, \lambda\beta+\gamma, -\lambda\alpha-\gamma, \beta+\lambda^2\gamma) \tag{7}$$

whenever $\alpha^2+\alpha\beta+\beta^2 = 3\lambda\gamma^2$ (Ramanujan's result was slightly pre-dated by a very similar general solution due to Schwering (see [3], p. 557).)

Despite these results, however, there is no known formula characterizing the **integral** solutions to equation (1). In this light, considering various families of solutions is of value. This paper categorizes and extends various families of solutions to equation (1). Many of the results may be found in Dickson [3] and Barbeau [1].

There are many other one-parameter families of solutions to equation (1) besides (2) and (3). Examples are:

$$\begin{aligned}(a,b,c,d) = ((2x-1)(2x^3-6x^2-1), (x+1)(5x^3-9x^2+3x-1),\\ 3x(x+1)(x^2-x+1), 3x(2x-1)(x^2-x+1));\end{aligned} \tag{8}$$

$$(a,b,c,d) = (x^3+1, 2x^3-1, x(x^3-2), x(x^3+1)); \tag{9}$$

$$(a,b,c,d) = (3x^2, 6x^2\pm 3x+1, 3x(3x^2\pm 2x+1), c+1). \tag{10}$$

As before, one may let x be a rational number v/u and multiply through by an appropriate power of u to obtain a two-parameter family of **integral** solutions.

A strikingly dissimilar one-parameter family of solutions is due to Ramanujan. Letting

$$\frac{1+53x+9x^2}{1-82x-82x^2+x^3} = \sum_{n\geq 0} a_n x^n,$$

$$\frac{2-26x-12x^2}{1-82x-82x^2+x^3} = \sum_{n\geq 0} b_n x^n,$$

$$\frac{2+8x-10x^2}{1-82x-82x^2+x^3} = \sum_{n\geq 0} c_n x^n,$$

yields

$$a_n^3+b_n^3 = c_n^3+(-1)^n.$$

This result produces "near misses" when considering Fermat's Last Theorem. Hirschhorn [4] has observed that Ramanujan's solutions are contained in

$$(a,b,c,d) = (u^2+7uv-9v^2, -u^2+9uv+v^2, 2u^2-4uv+12v^2, 2u^2+10v^2). \tag{11}$$

Some authors have given two-parameter families of solutions to equation (1) that could have been generated from a one-parameter solutions (as we have done earlier). Examples are:

$$(a,b,c,d) = (3u^2+5uv-5v^2, 4u^2-4uv+6v^2, 5u^2-5uv-3v^2, 6u^2-4uv+4v^2); \tag{12}$$

$$(a,b,c,d) = (3u^2+16uv-7v^2,\ 6u^2-4uv+14v^2,\ -3u^2+16uv+7v^2,\ 6u^2+4uv+14v^2). \tag{13}$$

Two-parameter solutions of (1) which do not arise from one-parameter solutions are not so plentiful. Ramanujan (see [1], pp. 35, 48) discovered

$$\begin{aligned}(a,b,c,d) = (&u^7-3(v+1)u^4+(3v^2+6v+2)u,\ 2u^6-3(2v+1)u^3+3v^2+3v+1,\\ &u^6-3v^2-3v-1,\ u^7-3vu^4+(3v^2-1)u).\end{aligned} \tag{14}$$

In comparing the different families of solutions previously mentioned, one notices that the coefficients in the solution represented by (12) are the same as the values in equation (5). This generalizes to

Theorem 1: If

$$a^3+b^3+c^3 = d^3 \tag{15}$$

and

$$c(c^3-a^2) = b(d^2-b^2), \tag{16}$$

then

$$(ax^2+cx-c)^3+(bx^2-bx+d)^3+(cx^2-cx-a)^3 = (dx^2-bx+b)^3.$$

This theorem may be proved directly by expansion. It shows that a one-parameter family of solutions may sometimes be constructed from one solution. The next theorem shows exactly where Theorem 1 applies.

Theorem 2: The only solutions of equations (15)-(16) are:

(a) (trivial) solutions of the form $(a,b,c,d) = (a,b,-a,b)$;

(b) (scaled) solutions of the one-parameter system represented by (9), namely

$$(a,b,c,d) = (1+u^3,\ u^4-2u,\ 2u^3-1,\ u^4+u).$$

Proof: Substituting Euler's general solution (6) of (15) into (16) gives (after dividing by σ^3)

$$0 = 36\eta^2(\xi-\eta)(\xi^2+3\eta^2-1)(\xi^4+6\xi^2\eta^2+\xi^2+9\eta^4+3\eta^2+1).$$

If $\eta = 0$ or $\xi^2+3\eta^2-1 = 0$, one falls into the first class of solutions. The only other possibility is if $\xi = \eta$, which yields

$$(a,b,c,d) = (8\eta^3+1,\ 16\eta^4-4\eta,\ 16\eta^3-1,\ 16\eta^4+2\eta).$$

Setting $u = 2\eta$ shows that this case falls into the second class of solutions. □

Note that the second class of solutions is the same as (9). This solution is due to Vieta. Combining Theorems 1 and 2 generates a new two-parameter family of solutions to (1), namely

$$\begin{aligned}(a,b,c,d) = (&((1+u^3)x^2+(2u^3-1)(x-1),\ (u^4-2u)x(x-1)+u^4+u,\\ &(2u^3-1)x(x-1)-u^3-1,\ (u^4+u)x^2-(u^4-2u)(x-1)).\end{aligned} \tag{17}$$

ACKNOWLEDGMENT

I would like to thank the anonymous referee for helpful comments which improved the presentation of this paper.

REFERENCES

1. E. J. Barbeau. *Power Play*. Washington, D.C.: MAA, 1997.
2. B. C. Berndt & S. Bhargava. "Ramanujan—for Lowbrows." *Amer. Math. Monthly* **100.7** (1993):644-656.
3. L. E. Dickson. *History of the Theory of Numbers*. Vol. 2. Washington, D. C.: Carnegie Institution of Washington, 1919-1923.
4. M. D. Hirschhorn. "An Amazing Identity of Ramanujan." *Math. Mag.* **68.3** (1995):199-201.
5. M. D. Hirschhorn. "A Proof in the Spirit of Zeilberger of An Amazing Identity of Ramanujan." *Math. Mag.* **69.4** (1996):267-69.
6. H. L. Keng. *Introduction to Number Theory*. New York: Springer, 1982.
7. Y. I. Perelman. *Algebra Can Be Fun*. Moscow: Mir Publishers, 1979.

AMS Classification Number: 11D25

❖❖❖

NEW PROBLEM WEB SITE

Readers of *The Fibonacci Quarterly* will be pleased to know that many of its problems can now be searched electronically (at no charge) on the World Wide Web at

http://problems.math.umr.edu

Over 20,000 problems from 38 journals and 21 contests are referenced by the site, which was developed by Stanley Rabinowitz's MathPro Press. Ample hosting space for the site was generously provided by the Department of Mathematics and Statistics at the University of Missouri-Rolla, through Leon M. Hall, Chair.

Problem statements are included in most cases, along with proposers, solvers (whose solutions were published), and other relevant bibliographic information. Difficulty and subject matter vary widely; almost any mathematical topic can be found.

The site is being operated on a volunteer basis. Anyone who can donate journal issues or their time is encouraged to do so. For further information, write to:

Mr. Mark Bowron
Director of Operations, MathPro Press
P.O. Box 713
Westford, MA 01886 USA
bowron@my-deja.com

ALTERNATING SUMS OF FOURTH POWERS OF FIBONACCI AND LUCAS NUMBERS

R. S. Melham
School of Mathematical Sciences, University of Technology, Sydney
PO Box 123, Broadway, NSW 2007 Australia
(Submitted August 1998-Final Revision December 1998)

1. INTRODUCTION

The Fibonacci and Lucas numbers are defined for all integers n as

$$\begin{cases} F_{n+1} = F_n + F_{n-1}, & F_1 = F_2 = 1, \\ L_{n+1} = L_n + L_{n-1}, & L_1 = 1, L_2 = 3. \end{cases}$$

Their Binet forms are $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ and $L_n = \alpha^n + \beta^n$, where α and β are the roots of $x^2 - x - 1 = 0$.

Inspired by the well-known sum

$$\sum_{k=1}^{n} F_k^2 = F_n F_{n+1}, \tag{1.1}$$

Clary and Hemenway [2] obtained factored closed-form expressions for all sums of the form $\sum_{k=1}^{n} F_{mk}^3$, where m is an integer. For example, they discovered

$$\sum_{k=1}^{n} F_{2k}^3 = \begin{cases} \frac{1}{4} F_n^2 L_{n+1}^2 F_{n-1} L_{n+2} & \text{if } n \text{ is even}, \\ \frac{1}{4} L_n^2 F_{n+1}^2 L_{n-1} F_{n+2} & \text{if } n \text{ is odd}, \end{cases} \tag{1.2}$$

and

$$\sum_{k=1}^{n} F_{4k}^3 = \frac{1}{8} F_{2n}^2 F_{2n+2}^2 (L_{4n+2} + 6). \tag{1.3}$$

Motivated by the results of Clary and Hemenway, we turned to fourth powers to see if similar factorizations could be obtained. In the case of nonalternating sums, we could find nothing to compare with the beautiful formulas of Clary and Hemenway. However, by experimenting with many numerical examples, we found the most interesting results when we considered alternating sums. We present these results in Section 3, and indicate our method of proof in Section 4. As noted in [2], once such identities are discovered, it is usually a comparatively routine matter to prove them. However, to assist us in the proofs, we have discovered a number of striking sums that involve the Lucas numbers, and we present these in Section 2.

2. PRELIMINARY RESULTS

We require the following results.

$$F_{n+k} + F_{n-k} = F_n L_k, \quad k \text{ even}, \tag{2.1}$$

$$F_{n+k} + F_{n-k} = L_n F_k, \quad k \text{ odd}, \tag{2.2}$$

$$F_{n+k} - F_{n-k} = F_n L_k, \quad k \text{ odd}, \tag{2.3}$$

$$F_{n+k} - F_{n-k} = L_n F_k, \qquad k \text{ even}, \tag{2.4}$$

$$L_{n+k} + L_{n-k} = L_n L_k, \qquad k \text{ even}, \tag{2.5}$$

$$L_{n+k} + L_{n-k} = 5F_n F_k, \qquad k \text{ odd}, \tag{2.6}$$

$$L_{n+k} - L_{n-k} = L_n L_k, \qquad k \text{ odd}, \tag{2.7}$$

$$L_{n+k} - L_{n-k} = 5F_n F_k, \qquad k \text{ even}, \tag{2.8}$$

$$L_{2m} - 2 = L_m^2, \qquad m \text{ odd}, \tag{2.9}$$

$$L_{2m} + 2 = L_m^2, \qquad m \text{ even}, \tag{2.10}$$

$$L_{2m} + (-1)^{m+1} 2 = 5F_m^2. \tag{2.11}$$

Identities (2.1)-(2.8) appear as (5)-(12) in Bergum and Hoggatt [1], while (2.9)-(2.11) can be proved with the aid of the Binet forms for F_n and L_n.

Throughout this paper $m \neq 0$ is an integer. To assist in our proofs, we also make use of four sums which involve Lucas numbers with even subscripts. If m is odd, we have

$$\sum_{k=1}^{n} L_{2mk} = \begin{cases} \dfrac{5F_{mn}F_{m(n+1)}}{L_m}, & n \text{ even}, \\ \dfrac{L_{mn}L_{m(n+1)}}{L_m}, & n \text{ odd}, \end{cases} \tag{2.12}$$

and

$$\sum_{k=0}^{n} L_{2mk} = \begin{cases} \dfrac{L_{mn}L_{m(n+1)}}{L_m}, & n \text{ even}, \\ \dfrac{5F_{mn}F_{m(n+1)}}{L_m}, & n \text{ odd}. \end{cases} \tag{2.13}$$

On the right sides of (2.12) and (2.13), the even and odd cases are reversed. Equally surprising, we have found that for m even

$$\sum_{k=1}^{n} (-1)^k L_{2mk} = \begin{cases} \dfrac{5F_{mn}F_{m(n+1)}}{L_m}, & n \text{ even}, \\ -\dfrac{L_{mn}L_{m(n+1)}}{L_m}, & n \text{ odd}, \end{cases} \tag{2.14}$$

and

$$\sum_{k=0}^{n} (-1)^k L_{2mk} = \begin{cases} \dfrac{L_{mn}L_{m(n+1)}}{L_m}, & n \text{ even}, \\ -\dfrac{5F_{mn}F_{m(n+1)}}{L_m}, & n \text{ odd}. \end{cases} \tag{2.15}$$

The proofs of (2.12)-(2.15) are similar. We illustrate the method by proving (2.13).

Proof of (2.13): Expressing L_{2mk} in Binet form and summing the resulting geometric progressions, we obtain

$$\begin{aligned}\sum_{k=0}^{n} L_{2mk} &= \frac{\alpha^{2mn+2m}-1}{\alpha^{2m}-1}+\frac{\beta^{2mn+2m}-1}{\beta^{2m}-1}\\ &= \frac{L_{2mn+2m}-L_{2mn}+L_{2m}-2}{L_{2m}-2}\\ &= \frac{L_{(2mn+m)+m}-L_{(2mn+m)-m}+L_m^2}{L_m^2} \qquad \text{[by (2.9)]}\\ &= \frac{L_{2mn+m}L_m+L_m^2}{L_m^2} \qquad \text{[by (2.7)]}\\ &= \frac{L_{(mn+m)+mn}+L_{(mn+m)-mn}}{L_m}.\end{aligned}$$

Since m is odd, (2.13) follows from (2.5) and (2.6). □

3. THE MAIN RESULTS

We now present our main results. If m is even, then

$$\sum_{k=1}^{n}(-1)^k F_{mk}^4 = \frac{(-1)^n F_{mn}F_{m(n+1)}[L_mL_{mn}L_{m(n+1)}-4L_{2m}]}{5L_mL_{2m}}, \tag{3.1}$$

$$\sum_{k=1}^{n}(-1)^k L_{mk}^4 = \frac{5F_{mn}F_{m(n+1)}[L_mL_{mn}L_{m(n+1)}+4L_{2m}]}{L_mL_{2m}}, \quad n \text{ even}, \tag{3.2}$$

$$\sum_{k=0}^{n}(-1)^k L_{mk}^4 = -\frac{5F_{mn}F_{m(n+1)}[L_mL_{mn}L_{m(n+1)}+4L_{2m}]}{L_mL_{2m}}, \quad n \text{ odd}. \tag{3.3}$$

We mention that (3.2) and (3.3) can be combined in a single sum as

$$\sum_{k=1}^{n}(-1)^k L_{mk}^4 = \frac{(-1)^n 5F_{mn}F_{m(n+1)}[L_mL_{mn}L_{m(n+1)}+4L_{2m}]}{L_mL_{2m}} - 8(1+(-1)^{n+1}).$$

On the other hand, if m is odd, then

$$\sum_{k=1}^{n}(-1)^k F_{mk}^4 = \frac{(-1)^n F_{mn}F_{m(n+1)}[L_mL_{mn}L_{m(n+1)}+4(-1)^{n+1}L_{2m}]}{5L_mL_{2m}}, \tag{3.4}$$

$$\sum_{k=1}^{n}(-1)^k L_{mk}^4 = \frac{5F_{mn}F_{m(n+1)}[L_mL_{mn}L_{m(n+1)}+4L_{2m}]}{L_mL_{2m}}, \quad n \text{ even}, \tag{3.5}$$

$$\sum_{k=0}^{n}(-1)^k L_{mk}^4 = -\frac{5F_{mn}F_{m(n+1)}[L_mL_{mn}L_{m(n+1)}-4L_{2m}]}{L_mL_{2m}}, \quad n \text{ odd}. \tag{3.6}$$

As before, (3.5) and (3.6) can be expressed as a single sum, but we choose to write them separately in order to present the right sides in factored form. This is the reason for the appearance of the zero lower limit.

4. THE METHOD OF PROOF

To illustrate the method, we prove (3.4). First, let n be even. In what follows, we note that since m is odd and $\alpha\beta = -1$, then $(\alpha\beta)^{mk} = (-1)^k$. Now

$$\begin{aligned}\sum_{k=1}^{n}(-1)^k F_{mk}^4 &= \frac{1}{25}\sum_{k=1}^{n}(-1)^k(\alpha^{mk}-\beta^{mk})^4\\ &= \frac{1}{25}\sum_{k=1}^{n}(-1)^k(L_{4mk}-4(-1)^k L_{2mk}+6)\\ &= \frac{1}{25}\sum_{k=1}^{n}((-1)^k L_{4mk}-4L_{2mk}+6(-1)^k)\\ &= \frac{1}{25}\sum_{k=1}^{n}((-1)^k L_{4mk}-4L_{2mk}), \text{ since } n \text{ is even.}\end{aligned}$$

With the use of (2.12) and (2.14), this becomes

$$\begin{aligned}\frac{1}{25}\left[\frac{5F_{2mn}F_{2m(n+1)}}{L_{2m}}-\frac{20F_{mn}F_{m(n+1)}}{L_m}\right] &= \frac{1}{5}\left[\frac{F_{mn}L_{mn}F_{m(n+1)}L_{m(n+1)}}{L_{2m}}-\frac{4F_{mn}F_{m(n+1)}}{L_m}\right]\\ &= \frac{F_{mn}F_{m(n+1)}[L_mL_{mn}L_{m(n+1)}-4L_{2m}]}{5L_mL_{2m}}.\end{aligned}$$

If n is odd, then we have

$$\begin{aligned}\sum_{k=1}^{n}(-1)^k F_{mk}^4 &= \sum_{k=0}^{n}(-1)^k F_{mk}^4 \quad (\text{since } F_0 = 0)\\ &= \frac{1}{25}\sum_{k=0}^{n}((-1)^k L_{4mk}-4L_{2mk}+6(-1)^k)\\ &= \frac{1}{25}\sum_{k=0}^{n}((-1)^k L_{4mk}-4L_{2mk}), \text{ since } n \text{ is odd.}\end{aligned}$$

With the aid of (2.13) and (2.15), this sum becomes

$$\begin{aligned}\frac{1}{25}\left[\frac{-5F_{2mn}F_{2m(n+1)}}{L_{2m}}-\frac{20F_{mn}F_{m(n+1)}}{L_m}\right] &= -\frac{1}{5}\left[\frac{F_{mn}L_{mn}F_{m(n+1)}L_{m(n+1)}}{L_{2m}}+\frac{4F_{mn}F_{m(n+1)}}{L_m}\right]\\ &= -\frac{F_{mn}F_{m(n+1)}[L_mL_{mn}L_{m(n+1)}+4L_{2m}]}{5L_mL_{2m}},\end{aligned}$$

and this completes the proof. □

We remark that the proof of (3.1) is similar since the parities of n must be considered separately, but the proofs of the other results in Section 3 are more straightforward.

5. CONCLUSION

During the course of our investigation we discovered two further pairs of sums similar in character to (2.12)-(2.15) which we include here. If m is odd, then

$$\sum_{k=1}^{n}(-1)^k L_{2mk} = \frac{(-1)^n F_{mn} L_{m(n+1)}}{F_m}, \tag{5.1}$$

and

$$\sum_{k=0}^{n}(-1)^k L_{2mk} = \frac{(-1)^n L_{mn} F_{m(n+1)}}{F_m}. \tag{5.2}$$

If m is even, then

$$\sum_{k=1}^{n} L_{2mk} = \frac{F_{mn} L_{m(n+1)}}{F_m}, \tag{5.3}$$

and

$$\sum_{k=0}^{n} L_{2mk} = \frac{L_{mn} F_{m(n+1)}}{F_m}. \tag{5.4}$$

The Lucas counterpart of (1.1), which appears as I_4 in [3], is

$$\sum_{k=1}^{n} L_k^2 = L_n L_{n+1} - 2 = L_n L_{n+1} - L_0 L_1. \tag{5.5}$$

The right side of (5.5) suggests the notation $[L_j L_{j+1}]_0^n$.

We now make an observation about identity (3.4) and its Lucas counterpart. We have found that for $m = 1$ they can be expressed as

$$\sum_{k=1}^{n}(-1)^k F_k^4 = \frac{(-1)^n}{3} F_{n-2} F_n F_{n+1} F_{n+3}, \tag{5.6}$$

and

$$\sum_{k=1}^{n}(-1)^k L_k^4 = \left[\frac{(-1)^j}{3} L_{j-2} L_j L_{j+1} L_{j+3}\right]_0^n. \tag{5.7}$$

They can be proved quite effectively using the method outlined on page 135 of [2]. We illustrate by proving (5.7).

Let l_n denote the sum on the left side of (5.7), and let $r_n = \frac{(-1)^n}{3} L_{n-2} L_n L_{n+1} L_{n+3}$. Then

$$r_n - r_{n-1} = \frac{(-1)^n}{3} L_n (L_{n-2} L_{n+1} L_{n+3} + L_{n-3} L_{n-1} L_{n+2}). \tag{5.8}$$

Now, by using the recurrence satisfied by the Lucas numbers, we express L_{n-2}, L_{n+3}, L_{n-3}, L_{n-1}, and L_{n+2} in terms of L_n and L_{n+1}, and substitute in (5.8) to obtain

$$r_n - r_{n-1} = l_n - l_{n-1} = \frac{(-1)^n}{3} L_n^4.$$

Thus, $l_n - r_n = -r_0$, and this proves (5.7).

To conclude, we mention that for p real the sequences $\{U_n\}$ and $\{V_n\}$ defined for all integers n by

$$\begin{cases} U_n = pU_{n-1} + U_{n-2}, & U_0 = 0,\ U_1 = 1, \\ V_n = pV_{n-1} + V_{n-2}, & V_0 = 2,\ V_1 = p, \end{cases}$$

generalize the Fibonacci and Lucas numbers, respectively. Identities (2.12)-(2.15), together with the results in Section 3, and (5.1)-(5.4) translate immediately to U_n and V_n. The reason is that if

we replace F_n by U_n, L_n by V_n, and 5 by p^2+4, then U_n and V_n satisfy (2.1)-(2.11), upon which all our proofs are based. For example, if m is odd, (3.4) and (3.5) become, respectively,

$$\sum_{k=1}^{n}(-1)^k U_{mk}^4 = \frac{(-1)^n U_{mn}U_{m(n+1)}[V_m V_{mn}V_{m(n+1)} + 4(-1)^{n+1}V_{2m}]}{(p^2+4)V_m V_{2m}}, \tag{5.9}$$

and

$$\sum_{k=1}^{n}(-1)^k V_{mk}^4 = \frac{(p^2+4)U_{mn}U_{m(n+1)}[V_m V_{mn}V_{m(n+1)} + 4V_{2m}]}{V_m V_{2m}}, \quad n \text{ even}. \tag{5.10}$$

REFERENCES

1. G. E. Bergum & V. E. Hoggatt, Jr. "Sums and Products for Recurring Sequences." *The Fibonacci Quarterly* **13.2** (1975):115-20.
2. S. Clary & P. D. Hemenway. "On Sums of Cubes of Fibonacci Numbers." In *Applications of Fibonacci Numbers* **5:**123-36. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1993.
3. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers.* Boston: Houghton Mifflin, 1969; rpt. The Fibonacci Association, Santa Clara, CA, 1979.

AMS Classification Numbers: 11B39, 11B37

❖❖❖

COMPLETION OF NUMERICAL VALUES OF GENERALIZED MORGAN-VOYCE AND RELATED POLYNOMIALS

A. F. Horadam
The University of New England, Armidale, Australia 2351
(Submittted August 1998-Final Revision February 1999)

1. MOTIVATION

Two recent publications [2], [3] examined some of the properties of the related polynomial sequences $\{R_n^{(r,u)}(x)\}$ and $\{S_n^{(r,u)}(x)\}$ defined recursively by

$$R_n^{(r,u)}(x) = (x+2)R_{n-1}^{(r,u)}(x) - R_{n-2}^{(r,u)}(x) \quad (n \geq 2), \tag{1.1}$$

$$S_n^{(r,u)}(x) = (x+2)S_{n-1}^{(r,u)}(x) + S_{n-2}^{(r,u)}(x) \quad (n \geq 2). \tag{1.2}$$

with identical initial conditions

$$R_0(x) = u, \quad R_1(x) = x + r + u, \tag{1.3}$$

$$S_0(x) = u, \quad S_1(x) = x + r + u. \tag{1.4}$$

Papers [2] and [3] dealt only with the five values of the subscript pairs, and the notation, indicated immediately below:

$R_n^{(r,u)}(x)$	r	u	$S_n^{(r,u)}(x)$
$xB_n(x)$	0	0	$x\mathcal{B}_n(x)$
$b_{n+1}(x)$	0	1	$\mathbf{c}_{n+1}(x)$
$C_n(x)$	0	2	$\mathcal{C}_n(x)$
$B_{n+1}(x)$	1	1	$\mathcal{B}_{n+1}(x)$
$c_{n+1}(x)$	2	1	$\mathbf{b}_{n+1}(x)$

(1.5)

where $B_n(x)$, $b_n(x)$, $C_n(x)$, and $c_n(x)$ in the R-column are the *Morgan-Voyce polynomials* specified by the following tabulation (a, b being initial conditions for $n = 0, 1$, respectively)

$R_n^{(r,u)}(x)$	a	b
$B_n(x)$	0	1
$b_n(x)$	1	1
$C_n(x)$	2	$2+x$
$c_n(x)$	−1	1

(1.6)

and $\mathcal{B}_n(x)$, $\mathbf{b}_n(x)$, $\mathcal{C}_n(x)$, and $\mathbf{c}_n(x)$ in the S-column are the corresponding polynomials (the *quasi-Morgan-Voyce polynomials*) relating to $S_n^{(r,u)}(x)$.

Let us now examine the consequence of considering the remaining $3^2 - 5 = 4$ superscript pairs

$$(r, u) = (1, 0), (2, 0), (1, 2), (2, 2). \tag{1.7}$$

Readers are encouraged to construct sets of polynomial expressions for $R_n^{(r,u)}(x)$ and $S_n^{(r,u)}(x)$ for the cases listed in (1.7). Particular usage is made of these polynomials when $x = 1$.

Conventions: Write

$$\left.\begin{array}{ll} (i) & R_n^{(r,u)}(1) \equiv R_n^{(r,u)}, \text{ so } B_n(1) \equiv B_n, \ldots, \\ (ii) & S_n^{(r,u)}(1) \equiv S_n^{(r,u)}, \text{ so } \mathcal{B}_n(1) \equiv \mathcal{B}_n, \ldots . \end{array}\right\} \tag{1.8}$$

Observe that by (1.2), (1.5), and (1.8),

$$\mathcal{R}_n = 3\mathcal{B}_{n-1} + \mathcal{R}_n. \tag{1.9}$$

2. REFERENCE DATA

It is known from [1] that

$$b_n(x) = B_n(x) - B_{n-1}(x), \tag{2.1}$$

$$c_n(x) = B_n(x) + B_{n-1}(x), \tag{2.2}$$

$$C_n(x) = B_{n+1}(x) - B_{n-1}(x), \tag{2.3}$$

while (see [3])

$$\mathbf{b}_n(x) = \mathcal{B}_n(x) + \mathcal{B}_{n+1}(x), \tag{2.4}$$

$$\mathbf{c}_n(x) = \mathcal{B}_n(x) - \mathcal{B}_{n-1}(x), \tag{2.5}$$

$$\mathcal{C}_n(x) = \mathcal{B}_{n+1}(x) + \mathcal{B}_{n-1}(x). \tag{2.6}$$

Moreover (see [1]),

$$B_n = F_{2n}, \tag{2.7}$$

$$b_n = F_{2n-1}, \tag{2.8}$$

$$C_n = L_{2n}, \tag{2.9}$$

$$c_n = L_{2n-1}, \tag{2.10}$$

where F_n and L_n are the n^{th} Fibonacci and Lucas numbers, respectively. For basic information on F_n and L_n, one might consult [4].

Fibonacci and *Lucas polynomials* are defined recursively by

$$F_n(x) = xF_{n-1}(x) + F_{n-2}(x), \quad F_0(x) = 0, \ F_1(x) = 1; \tag{2.11}$$

$$L_n(x) = xL_{n-1}(x) + L_{n-2}(x), \quad L_0(x) = 2, \ L_1(x) = x. \tag{2.12}$$

Particular Cases:

$$x = 1: \quad F_n(1) = F_n, \ L_n(1) = L_n; \tag{2.13}$$

$$x = 2: \quad F_n(2) = P_n, \ L_n(2) = Q_n \tag{2.14}$$

(the n^{th} *Pell* and *Pell-Lucas numbers*, respectively);

$$x = 3: \quad \{F_n(3)\} \equiv \{0, 1, 3, 10, 33, 109, \ldots\} = \{\mathcal{R}_n\}, \tag{2.15}$$

$$\{L_n(3)\} \equiv \{2, 3, 11, 36, 119, 393, \ldots\} = \{\mathcal{C}_n\}, \tag{2.16}$$

as one may readily verify.

Keep in mind the recurrence ($x = 3$ in (2.11))

$$F_n(3) = 3F_{n-1}(3) + F_{n-2}(3). \tag{2.17}$$

Knowledge of the facts from [1]

$$b_n = B_n - B_{n-1}, \tag{2.18}$$

$$c_n = B_n + B_{n-1}, \tag{2.19}$$

and from [3]

$$\mathbf{b}_n = \mathcal{B}_n + \mathcal{B}_{n-1}, \tag{2.20}$$

$$\mathbf{c}_n = \mathcal{B}_n - \mathcal{B}_{n-1}, \tag{2.21}$$

is applicable to the "crossing" correspondence *vis-à-vis* b_n and $\mathbf{c}_n$, and c_n and $\mathbf{b}_n$ in relation to + and − in (2.18)-(2.21), which appears schematically in [3, (4.33)].

Two Useful Theorems:

I. $$R_n^{(r,u)}(x) = P_n^{(r)}(x) + (u-1)b_n(x) \quad \text{[2, Theorem 1]}, \tag{2.22}$$

in which

$$P_n^{(0)}(x) = b_{n+1}(x), \tag{2.23}$$

$$P_n^{(1)}(x) = B_{n+1}(x), \tag{2.24}$$

$$P_n^{(2)}(x) = c_{n+1}(x). \tag{2.25}$$

From (2.23)-(2.25) were derived the results for $R_n^{(r,u)}(x)$ in (1.5).

II. $$S_n^{(r,u)}(x) = (x+r+u)\mathcal{B}_n(x) + u\mathcal{B}_{n-1}(x) \quad \text{[3, (4.14)]}. \tag{2.26}$$

3. NUMERICAL COMPLETION

A critical elementary question to ask is: Considering the basic property $B_n = R_n^{(0,0)} = F_{2n}$, derived from (1.5), (1.8), and (2.7), what number plays the corresponding role in $\mathcal{B}_n = S_n^{(0,0)}$?

$S_n^{(0,0)}$

Comparison of (1.9) and (2.17) quickly reveals that

$$S_n^{(0,0)} = F_n(3) \; (= \mathcal{B}_n) \tag{3.1}$$

since both relevant sequences have initial conditions 0, 1 at $n = 0, 1$. Therefore, we would expect $F_n(3) = \mathcal{B}_n$ could effect a role for $S_n^{(r,u)}(x)$ analogous to $F_{2n} = \mathcal{B}_n = R_n^{(0,0)}$ for $R_n^{(r,u)}(x)$. Then it remains for us to discover whether our expectations are fully realized.

$R_n^{(r,u)}$

Values of $R_n^{(r,u)}$ in (1.5) and (1.8) are known (see [2]), so we need only to enquire into the corresponding situation appropriate to (1.7).

Pairs of values of (r, u) in (1.7) with $x = 1$ now lead by (2.22), (2.24), (2.25), and (2.7)-(2.10), to

$$R_n^{(1,0)} = P_n^{(1)} - b_n = B_{n+1} - b_n = 2F_{2n}, \tag{3.2}$$

$$R_n^{(2,0)} = P_n^{(2)} - b_n = c_{n+1} - b_n = 3F_{2n}, \tag{3.3}$$

$$R_n^{(1,2)} = P_n^{(1)} + b_n = B_{n+1} + b_n = 2F_{2n+1}, \tag{3.4}$$

$$R_n^{(2,2)} = P_n^{(2)} + b_n = c_{n+1} + c_n = F_{2n+3}. \tag{3.5}$$

$S_n^{(r,u)}$

Pairs of values of (r, u) in (1.5) with $x = 1$ disclose that by (2.26), (3.1), (2.17), and (1.5),

$$S_n^{(0,1)} = 2\mathcal{B}_n + \mathcal{B}_{n-1} = F_{n+1}(3) - F_n(3) \; (= \mathbf{c}_{n+1}), \tag{3.6}$$

$$S_n^{(0,2)} = 3\mathcal{B}_n + 2\mathcal{B}_{n-1} = F_{n+1}(3) + F_{n-1}(3) = L_n(3) = \mathcal{C}_n, \tag{3.7}$$

$$S_n^{(1,1)} = 3\mathcal{B}_n + \mathcal{B}_{n-1} = \mathcal{B}_{n+1} = F_{n+1}(3), \tag{3.8}$$

$$S_n^{(2,1)} = 4\mathcal{B}_n + \mathcal{B}_{n-1} = F_{n+1}(3) + F_n(3) = \mathbf{b}_{n+1}. \tag{3.9}$$

Turning next to (1.7), we determine by (2.26), (3.1), and (2.17) that

$$S_n^{(1,0)} = 2\mathcal{B}_n = 2F_n(3), \tag{3.10}$$

$$S_n^{(2,0)} = 3\mathcal{B}_n = 3F_n(3), \tag{3.11}$$

$$S_n^{(1,2)} = 2(2\mathcal{B}_n + \mathcal{B}_{n-1}) = 2(F_{n+1}(3) - F_n(3)), \tag{3.12}$$

$$S_n^{(2,2)} = 5\mathcal{B}_n + 2\mathcal{B}_{n-1} = 2F_{n+1}(3) - F_n(3). \tag{3.13}$$

Proofs of all the numerical properties stated above are quite straightforward, as the reader may readily verify.

4. SUMMARY AND CONCLUSION

Assembling together all the $2 \times 3^2 = 18$ exhibited superscript values of r, u in $R_n^{(r,u)}$ and $S_n^{(r,u)}$ for convenience and visual comparison, we have the following attractive compact correlation pattern, which thus completes our objective.

TABLE 1. $R_n^{(r,u)}$ and $S_n^{(r,u)}$ for $r, u = 0, 1, 2$

r, u	$R_n^{(r,u)}$	$S_n^{(r,u)}$
00	$F_{2n}\ (= B_n)$	$F_n\ (3)\ (= \mathcal{B}_n)$
01	F_{2n+1}	$F_{n+1}(3) - F_n(3)$
02	L_{2n}	$L_n(3)$
11	F_{2n+2}	$F_{n+1}(3)$
21	L_{2n+1}	$F_{n+1}(3) + F_n(3)$
10	$2F_{2n}$	$2F_n(3)$
20	$3F_{2n}$	$3F_n(3)$
12	$2F_{2n+1}$	$2F_{n+1}(3) - 2F_n(3)$
22	F_{2n+3}	$2F_{n+1}(3) - F_n(3)$

Thus, for example,

$$\frac{R_n^{(2,0)}}{R_n^{(1,0)}} = \frac{S_n^{(2,0)}}{S_n^{(1,0)}} = \frac{3}{2}.$$

REFERENCES

1. A. F. Horadam. "New Aspects of Morgan-Voyce Polynomials." In *Applications of Fibonacci Numbers* **7**:161-76. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1998.
2. A. F. Horadam. "A Composite of Morgan-Voyce Generalizations." *The Fibonacci Quarterly* **35.3** (1997):233-39.
3. A. F. Horadam. "Quasi Morgan-Voyce Polynomials and Pell Convolutions." In *Applications of Fibonacci Numbers* **8**:179-93. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1999.
4. S. Vajda. *Fibonacci and Lucas Numbers and the Golden Section: Theory and Applications.* Chichester: Horwood, 1989.

AMS Classification Numbers: 11B39

❖❖❖

A REMARK ON PARITY SEQUENCES

James H. Schmerl
Department of Mathematics, University of Connecticut, Storrs, CT 06269
(Submitted August 1998-Final Revision January 1999)

For an integer $n \geq 2$, let T_n be the unique set of positive integers such that:
(1) $1 \in T_n$;
(2) if $t > 1$, then $t \in T_n$ iff exactly one of $t-1$, $t-n$ is in T_n.

Condition (2) can be rephrased as

The Triple Criterion: If $t \neq 1$, then $|\{t-n, t-1, t\} \cap T_n| \in \{0, 2\}$.

If $n = 2$, then the set T_n is closely related to the Fibonacci sequence; specifically, $t \in T_2$ iff the t^{th} term of the Fibonacci sequence is odd.

We ask, for each n, which numbers are uniquely expressible as the sum of two distinct elements of T_n. In general, for any given n, one can determine exactly which numbers are uniquely expressible. If $n = 2$, it is easy to see that there are five such numbers: $3 = 1+2$, $5 = 1+4$, $7 = 2+5$, $8 = 1+7$, and $10 = 2+8$. If $n = 3$, then there are exactly eight uniquely expressible numbers: $3 = 1+2$, $4 = 1+3$, $5 = 2+3$, $6 = 1+5$, $7 = 2+5$, $8 = 3+5$, $9 = 1+8$, and $16 = 1+15$. If $n = 4$, then there are exactly five uniquely expressible numbers: $3 = 1+2$, $4 = 1+3$, $6 = 2+4$, $8 = 2+6$, and $16 = 4+12$. If $n \geq 3$, then $1, 2, 3 \in T_n$, so that 3 and 4 are uniquely expressible.

The principal theorem of this note answers this question for all other situations. Let U_n be the set of all integers which are uniquely expressible as the sum of two distinct elements of T_n. Thus, we have just observed that

$$U_2 = \{3, 5, 7, 8, 10\},\ U_3 = \{3, 4, 5, 6, 7, 8, 9, 16\}, \text{ and } U_4 = \{3, 4, 6, 8, 16\}.$$

The following principal theorem characterizes U_n for $n \geq 5$.

Theorem: Let $n \geq 5$. Then $U_n = \{3, 4, n^2 - n + 3, 2n^2 - 2n + 4\}$ if $n = 2^k + 1$ for some k, and $U_n = \{3, 4\}$ otherwise.

The remainder of this paper consists of two sections. The first contains a discussion of the motivation for the principal theorem, and the second contains its proof. The second section can be read independently of the first.

1. MOTIVATION

For an integer $n \geq 2$, let $f_1, f_2, f_3, \ldots$ be the sequence defined by the initial conditions

$$f_1 = f_2 = \cdots = f_n = 1$$

and the recurrence relation

$$f_{n+j} = f_j + f_{n+j-1}$$

for $j \geq 1$. If, in particular, $n = 2$, then the Fibonacci sequence has just been defined, and, as another example, if $n = 5$, then we get the sequence

$$1, 1, 1, 1, 1, 2, 3, 4, 5, 6, 8, 11, 15, 20, 26, 34, 45, 60, 80, 106, \ldots.$$

From this sequence, we define another sequence $t_1, t_2, t_3, \ldots$, which we will call the *n^{th} parity sequence*: we set $t_i = j$ iff the i^{th} odd term in the sequence $f_1, f_2, f_3, \ldots$ is f_j. For example, the 5^{th} parity sequence is

$$1, 2, 3, 4, 5, 7, 9, 12, 13, 17, 22, 23, 24, \ldots.$$

Then $T_n = \{t_1, t_2, t_3, \ldots\}$.

The principal theorem extends the result of [4] but in a somewhat disguised form. What is essentially proved in [4] is this theorem weakened by requiring that n be an even number, thereby eliminating any exceptional cases.

We next discuss some background for the result of [4] and, consequently, of the above theorem. For positive integers $u < v$, the *1-additive sequence based on u, v* is the sequence $s_1, s_2, s_3, \ldots$, where $s_1 = u$, $s_2 = v$, and s_{n+2} is the least $a > s_{n+1}$ for which there is a unique pair of integers i, j such that $1 \le i < j \le n+1$ and $a = s_i + s_j$. For example, the 1-additive sequence based on 1, 2 is the sequence

$$1, 2, 3, 4, 6, 8, 11, 13, 16, 18, 26, 28, \ldots,$$

which was introduced by Ulam [5]. This sequence is still not well understood, but it appears to have a quite erratic behavior. Other 1-additive sequences, such as the one based on 2, 3 also exhibit a similar erratic behavior. In contrast to this, the 1-additive sequence based on 2, v, where $v \ge 5$ is an odd number, has a much more predictable behavior.

Finch made the definition in [2] that the (increasing) sequence $s_1, s_2, s_3, \ldots$ is *regular* if there are positive integers m, p, and d such that whenever $i \ge m$, then $s_{i+p} = s_i + d$. (He refers to the least such p as the *period* of the sequence and to the least such d as the *fundamental difference*.) He observed in [2] that a 1-additive sequence having only finitely many even terms is regular. He then went on to make the conjecture, based on extensive numerical evidence, that for relatively prime $u < v$, the 1-additive sequence based on u, v has only finitely many even terms iff one of the following holds:

(i) $u = 2$ and $v \ge 5$ is odd;
(ii) $u = 4$ and $v \ge 5$ is odd;
(iii) $u = 5$ and $v = 6$;
(iv) $u \ge 6$ is even;
(v) $u \ge 7$ is odd and v is even.

For each of the cases (i)-(v), he made a conjecture as to what the finite sets are. For example, in (i) the set of even terms is $\{2, 2v+2\}$, and in (ii) the set is $\{4, 2v+4, 4v+4\}$ provided that $v \ne 2^m - 1$ for any $m \ge 3$. The conjecture for (i) was proved correct in [4], and for (ii) it was proved correct in [1] in the case $v \equiv 1 \pmod 4$. For (iii) the set is

$$\{6, 16, 26, 36, 80, 124, 144, 172, 184, 196, 238, 416, 448\},$$

and in this case the truth of the conjecture can be verified by direct computation.

Now suppose that $D = \{d_1, d_2, \ldots, d_k\}$ is a finite set of integers, where $d_1 < d_2 < \cdots < d_k$. Let us say for now that the sequence $t_1, t_2, t_3, \ldots$ is the *1-incremental sequence based on D* if $t_1 = 1$ and t_{n+1} is the least $a > t_n$ for which there is a unique pair of integers i, j such that $1 \le i \le n$, $1 \le j \le k$, and $a = t_i + d_j$. For example, the 1-incremental sequence based on $\{1, 5\}$ is

$$1, 2, 3, 4, 5, 7, 9, 12, 13, 17, 22, 23, 24, \ldots.$$

Notice that this sequence is identical to the 5^{th} parity sequence. In general, the n^{th} parity sequence is identical to the 1-incremental sequence based on $\{1, n\}$.

The connection between 1-incremental sequences and the regularity of 1-additive sequences, elaborating on Finch's observation [2], will be discussed next.

Consider the 1-additive sequence $s_1, s_2, s_3, \ldots$ based on u, v, where $u = 2d_1$ is even and v is odd. Suppose that $2d_1, 2d_2, \ldots, 2d_k$ are all the even terms that are no greater than $2(d_{k-1} + d_k)$ occurring in the 1-additive sequence, where $d_1 < d_2 < \cdots < d_k$. Let $t_1, t_2, t_3, \ldots$ be the 1-incremental sequence based on $D = \{d_1, d_2, \ldots, d_k\}$ and let $T = \{t_1, t_2, t_3, \ldots\}$. It is easy to check that

$$\{s_1, s_2, s_3, \ldots\} = \{2t + v - 2 : t \in T\} \cup \{2d_1, 2d_2, \ldots, 2d_k\}.$$

Now consider 1-additive sequences based on 2, v, where $v \geq 5$ is an odd integer. The result of [4] is thus seen to be equivalent to the principal theorem restricted to even $n \geq 6$. This leads naturally to the question that this theorem answers.

Every n^{th} parity sequence is regular. (In fact, it is obvious that every 1-incremental sequence is regular.) However, even a little more is true for these sequences (and for all 1-incremental sequences based on 2-element sets, as well). Let $P(n)$ be the period of the n^{th} parity sequence $t_1, t_2, t_3, \ldots$, and let $D(n)$ be the fundamental difference. Then, it follows from the Triple Criterion that, for each $i \geq 1$, $t_{i+P(n)} = t_i + D(n)$. Also $D(n)$ is the least $d > 1$ for which none of d, $d-1$, $d-2$, ..., $d-n+2$ is in T_n. Tabulation of $2D(n)$ and $P(n)$ for many even $n \geq 6$ can be found in [3].

2. THE PROOF

We will need an analysis of the $(2^k + 1)^{\text{th}}$ parity sequence. An analysis of the $(2^k)^{\text{th}}$ parity sequence was given in [4]. As a comparison, we summarize that analysis here.

Proposition 1 ([4]): Let $k \geq 1$ and let $n = 2^k$. Let $1 \leq t \leq 4n^2$ and suppose that $t = 2in + j$, where $0 \leq i < 2n$ and $1 \leq j \leq 2n$. Then:

(1) if $i < n$ and $j \leq n$, then $t \in T_{2n}$ iff $in + j \in T_n$;

(2) if $i < n$ and $j > n$, then $t \in T_{2n}$ iff $in + j - n \in T_n$;

(3) if $i \geq n$ and $j \leq n$, then $t \in T_{2n}$ iff $(i-n)n + j \in T_n$ and $j < n$;

(4) if $i \geq n$ and $j > n$, then $t \in T_{2n}$ iff $j = 2n$. □

The following notation from Section 1 will be used. Recall from Section 1 that, for each $n \geq 2$, there is $d \geq 1$ such that, for any $t \geq 1$, $t \in T_n$ iff $t + d \in T_n$. We let $D(n)$ be the least such d. Clearly, $D(n)$ is the least $d \geq 1$ such that $d+1$, $d+2$, $d+3$, ..., $d+n \in T_n$, and also it is the least $d \geq 1$ such that d, $d-1$, $d-2$, ..., $d-(n-2) \notin T_n$.

Using Proposition 1, we can easily prove by induction that, if $n = 2^k$, then the following hold: if $1 \leq i \leq n$, then $in \in T_n$; if $1 \leq j \leq n$, then $(n-1)j \in T_n$; if $i < n$ and $n - i \leq j < n$, then $in + j \notin T_n$. From this it follows that $n^2 - 1$ is the least $d \geq 1$ such that $\{d, d-1, d-2, \ldots, d-n+2\} \cap T_n = \emptyset$. Thus, $D(n) = 4^k - 1 = n^2 - 1$. It can also be shown that $P(n) = 3^k - 1$.

There is another way to characterize the elements of T_{2^k}. We introduce some notation. For nonnegative integers t and i, we let $b_i(t)$ be the i^{th} digit in the binary expansion of t. For example, since $37 = 1 + 4 + 32$, we get that $b_i(37) = 1$ if $i = 0, 2, 5$ and $b_i(37) = 0$ for all other nonnegative integers i.

Proposition 2: Suppose $k \geq 1$ and $n = 2^k$, and let $1 \leq t \leq n^2 = 2^{2k}$. Then $t \in T_n$ iff whenever $0 \leq r < k$, then $b_r(t) \cdot b_{k+r}(t) = 0$.

Proof: Let us first consider the special case of the proposition when $b_{k-1}(t) = 1$, $b_{2k-1}(t) = 0$, and $b_r(t) = 0$ for all $r < k-1$. Clearly, $b_r(t) \cdot b_{k+r}(t) = 0$ for all $r < k$. It is easily checked by induction on k that Proposition 1 implies that all such t are in T_n.

We now turn to the proof of the proposition in general. The proof is by induction on k. For $k = 1$, it is easily checked. Let $n = 2^k$; we will prove it for the case $2n = 2^{k+1}$. Let $1 \leq t \leq 4n^2$, and (as in Proposition 1) let $t = 2in + j$, where $0 \leq i < 2n$ and $1 \leq j \leq 2n$. The proof splits naturally into the same four cases as does Proposition 1. Since each one is routine, we will do just case (1), where $i < n$ and $j \leq n$. Notice that these restrictions on i and j are equivalent to the condition that $b_k(t-1) = b_{2k+1}(t-1) = 0$, and this condition splits into two subcases.

Subcase 1: $b_k(t) = b_{2k+1}(t) = 0$ and $b_r(t) = 1$ for some $r < k$. Since $b_k(t) = 0$, we need only be concerned with $b_r(t) \cdot b_{(k+1)+r}(t)$ for $r < k$. For such r, $b_r(t) = b_r(in + j)$ and $b_{(k+1)+r}(t) = b_{k+r}(in + j)$, so the result easily follows from the inductive hypothesis.

Subcase 2: $b_k(t) = 1$, $b_{2k+1}(t) = 0$, and $b_r(t) = 0$ for all $r < k$. But this is just the special case that was noted at the beginning of the proof. □

In ways analogous to those in Propositions 1 and 2, the sets T_{2^k+1} can be analyzed. This is done in Propositions 3 and 4, respectively.

Proposition 3: Let $k \geq 0$ and let $n = 2^k$. Let $1 \leq t \leq (2n+1)^2$ and suppose that $t = i(2n+1) + j$, where $0 \leq i \leq 2n$ and $1 \leq j \leq 2n+1$. Then:

(1) if $i \leq n$ and $j \leq n+1$, then $t \in T_{2n+1}$ iff $i(n+1) + j \in T_{n+1}$;

(2) if $i \leq n$ and $j > n+1$, then $t \in T_{2n+1}$ iff $i(n+1) + j - n \in T_{n+1}$ and $i \neq n$;

(3) if $i > n$ and $j \leq n+1$, then $t \in T_{2n+1}$ iff $(i-n)(n+1) + j \in T_{n+1}$;

(4) if $i > n$ and $j > n+1$, then $t \in T_{2n+1}$ iff $i = 2n$.

Proof: The proof is by induction on k. For $k = 0$, it is easily checked. Consider some $k > 0$, and assume, as the inductive hypothesis, that the proposition holds for all smaller values of k. Let $n = 2^k$, and let $t = i(2n+1) + j$, where $0 \leq i \leq 2n$ and $1 \leq j \leq 2n+1$. We proceed by induction on t. The proof splits naturally into four cases. Since each is routine, we will show only case (1), where $i \leq n$ and $j \leq n+1$. This case splits into three subcases.

Subcase 1: $i = 0$. Then $t = j$, and it is clear that $j \in T_{2n+1}$ and $j \in T_{n+1}$.

Subcase 2: $i > 0$ **and** $j > 1$. Then, using the Triple Criterion and the inductive hypothesis on t, we see that $t \in T_{2n+1}$ iff

$$t - 1 \in T_{2n+1} \Leftrightarrow t - (2n+1) \notin T_{2n+1}$$

iff

$$i(2n+1) + j - 1 \in T_{2n+1} \Leftrightarrow (i-1)(2n+1) + j \notin T_{2n+1}$$

iff

$$i(n+1) + j - 1 \in T_{n+1} \Leftrightarrow (i-1)(n+1) + j \notin T_{n+1}$$

iff

$$i(n+1) + j \in T_{n+1}.$$

Subcase 3: $i > 0$ and $j = 1$. Then, again using the Triple Criterion and the inductive hypothesis on t, we see that $t \in T_{2n+1}$ iff

$$t-1 \in T_{2n+1} \Leftrightarrow t-(2n+1) \notin T_{2n+1}$$

iff

$$(i-1)(2n+1)+(2n+1) \in T_{2n+1} \Leftrightarrow (i-1)(2n+1)+1 \notin T_{2n+1}$$

iff

$$i(n+1) \in T_{n+1} \Leftrightarrow (i-1)(n+1)+1 \notin T_{n+1}$$

iff

$$i(n+1)+1 \in T_{n+1}. \ \square$$

Proposition 4: Suppose $k \geq 1$ and $n = 2^k$, and let $2 \leq t \leq n^2+1$. Then $t \in T_{n+1}$ iff whenever $0 \leq r < k$, then $b_r(t-2) \geq b_{k+r}(t-2)$.

Proof: The proof is by induction on k. For small values of k, say $k = 1, 2$, it is easily checked. Let $n = 2^k$; we will prove it for the case $2n = 2^{k+1}$. Let $2 \leq t \leq 4n^2+1$, and (as in Proposition 3) let $t = i(2n+1)+j$, where $0 \leq i \leq 2n$ and $1 \leq j \leq 2n+1$. As $t \geq 2$, it is obvious that $2 \leq i+j$. The proof splits naturally into the same four cases as does Proposition 3. Since each one is routine, we will show just case (1), where $i \leq n$ and $j \leq n+1$. Thus, $2 \leq i+j \leq 2n+1 = 2^{k+1}+1$.

Subcase 1: $i+j < 2^k$. Since $t = i2^{k+1}+(i+j)$, where $2 \leq i+j < 2^k$, it is clear that $b_k(t-2) = b_{2k+1}(t-2) = 0$ and also that $b_r(t-2) = b_r(in+(i+j)-2)$ and $b_{k+(r+1)}(t-2) = b_{k+r}(in+(i+j)-2)$ for $r < k$. Therefore, from the inductive hypothesis,

$$t \in T_{2n+1} \Leftrightarrow i(n+1)+j \in T_{n+1} \Leftrightarrow b_r(i(n+1)+j-2) \geq b_{k+r}(i(n+1)+j-2)$$
$$\text{for } r < k \Leftrightarrow b_r(t-2) \geq b_{(k+1)+r}(t-2) \text{ for } r \leq k.$$

Subcase 2: $i+j = 2^k$. Then $b_0(t-2) = b_k(t-2) = b_{2k+1}(t-2) = 0$, and $b_r(t-2) = 1$ if $1 \leq r < k$. Also, $b_{k+1}(t-2) = 0$ iff i is even. Therefore, we have that $b_r(t-2) \geq b_{(k+1)+r}(t-2)$ whenever $0 \leq r \leq k$ iff i is even. On the other hand,

$$t \in T_{2n+1} \Leftrightarrow i(n+1)+j \in T_{n+1} \Leftrightarrow (i+1)n \in T_{n+1} \Leftrightarrow b_k((i+1)n-2) = 0 \Leftrightarrow i \text{ is even.}$$

Subcase 3: $i+j = 2^k+1$. Then $b_k(t-2) = b_{2k+1}(t-2) = 0$ and $b_r(t-2) = 1$ if $0 \leq r < k$. Thus, we have that $b_r(t-2) \geq b_{(k+1)+r}(t-2)$ whenever $0 \leq r \leq k$. On the other hand,

$$i2^{k+1}+2^k+1 \in T_{2n+1} \Leftrightarrow (i+1)n+1 \in T_{n+1},$$

which is the case since $b_r((i+1)n-1) = 1$ for all $r < k$.

Subcase 4: $2^k+2 \leq i+j < 2^{k+1}$. As in Subcase 1, it is clear that $b_k(t-2) = 1$ and also that $b_r(t-2) = b_r(in+(i+j)-2)$ and $b_{k+(r+1)}(t-2) = b_{k+r}(in+(i+j)-2)$ for $r < k$. Therefore, from the inductive hypothesis,

$$t \in T_{2n+1} \Leftrightarrow i(n+1)+j \in T_{n+1} \Leftrightarrow b_r(i(n+1)+j-2) \geq b_{k+r}(i(n+1)+j-2)$$
$$\text{for } r < k \Leftrightarrow b_r(t-2) \geq b_{(k+1)+r}(t-2) \text{ for } r \leq k.$$

Subcase 5: $i+j = 2^{k+1}$. (This subcase is similar to Subcase 2.) Then $b_0(t-2) = b_k(t-2) = 0$ and $b_r(t-2) = 1$ if $1 \leq r < k$. Also, $b_{k+1}(t-2) = 0$ iff i is even. Therefore, we have that $b_r(t-2) \geq b_{(k+1)+r}(t-2)$ whenever $0 \leq r \leq k$ iff i is even. On the other hand,

$$t \in T_{2n+1} \Leftrightarrow i(n+1)+j \in T_{n+1} \Leftrightarrow (i+1)n \in T_{n+1} \Leftrightarrow b_k((i+1)n-2)=0 \Leftrightarrow i \text{ is even.}$$

Subcase 6: $i+j=2^{k+1}+1$. Therefore, we have $i=n$, $j=n+1$, and $t=2^{2k+1}+2^{k+1}+1$. Then $b_r(t-2)=1$ for all $r \le k$. Thus, we have that $b_r(t-2) \ge b_{(k+1)+r}(t-2)$ whenever $0 \le r \le k$. On the other hand,

$$t \in T_{2n+1} \Leftrightarrow n(2n+1)+(n+1) \in T_{2n+1} \Leftrightarrow n(n+1)+(n+1)T_{n+1} \Leftrightarrow 2^{2k}+2^{k+1}+1 \in T_{n+1},$$

which is the case by the inductive hypothesis since $b_r(2^{2k}+2^{k+1}-1)=1$ for all $r<k$. □

Proposition 5: Suppose that $n \ge 2$ and $s=in+j$, where $0 \le i < n$ and $0 \le j < n$. Then:

(1) if $i < n-1$ and $j < n-i-1$, then $D(n)-s \notin T_n$;

(2) if $i < n$ and $j = n-i-1$, then $D(n)-s \in T_n$;

(3) if $i < n-1$ and $j = n-1$, then $D(n)-s \in T_n$.

Proof: The proof is by induction on s. We provide the details. We let $s=in+j$, where $0 \le i < n$ and either $0 \le j \le n-i-1$ or $j=n-1$. Suppose the proposition is true for all smaller values of s. Let $a=D(n)-s$, so a might be negative. We will determine whether or not $a \in T_n$ by seeing whether or not each of $a+n$ and $a+n-1$ is in T_n, and then use the Triple Criterion applied to $\{a, a+n-1, a+n\}$. To do so, it is necessary to know that $a+n \ne 1$. In each case, it will be clear that $a+n \ne 1$ since there will be b such that $a < b < a+n$ and $b \notin T_n$.

Case 1: $i=0$, $0 \le j < n-1$. Then $a+n=n+D(n)-j \in T_n$ since $n-j \in T_n$, and $a+n-1=n+D(n)-j-1 \in T_n$ since $n-j-1 \in T_n$. Therefore, $a \notin T_n$.

Case 2: $i=0$, $j=n-1$. Then $a+n=D(n)+1 \in T_n$ since $1 \in T_n$, and $a+n-1=D(n) \notin T_n$ by the inductive hypothesis. Therefore, $a \in T_n$.

Case 3: $0 < i < n-1$, $j=0$. Then $a+n=D(n)=(i-1)n \notin T_n$ and $a+n-1=D(n)-((i-1)n+1) \notin T_n$ by the inductive hypothesis. Therefore, $a \notin T_n$.

Case 4: $i=n-1$, $j=0$. Then $a+n=D(n)-(n-2)n \notin T_n$ and $a+n-1=D(n)-((n-2)n+1) \in T_n$ by the inductive hypothesis. Therefore, $a \in T_n$.

Case 5: $0 < i < n-1$, $0 < j < n-i-1$. Then $a+n=D(n)-((i-1)n+j) \notin T_n$ and $a+n-1=D(n)-((i-1)n+(j+1)) \notin T_n$ by the inductive hypothesis. Therefore, $a \notin T_n$.

Case 6: $0 < i < n-1$, $j=n-i-1$. Then $a+n=D(n)-((i-1)n+j) \notin T_n$ and $a+n-1=D(n)-((i-1)n+(j+1)) \in T_n$ by the inductive hypothesis. Therefore, $a \in T_n$.

Case 7: $0 < i < n-1$, $j=n-1$. Then $a+n=D(n)-((i-1)n+(n-1)) \in T_n$ and $a+n-1=D(n)-in \notin T_n$ by the inductive hypothesis. Therefore, $a \in T_n$. □

Two special instances of Proposition 5 will be used later on. If $i=1$, then (2) shows that $D(n)-2n+2 \in T_n$ and (3) shows that $D(n)-2n+1 \in T_n$.

Corollary 6: Let $n \ge 2$.

(1) Then $D(n) \ge n^2-n+1$.

(2) If $n=2^k+1$, then $D(n)=n^2-n+1$.

Proof: It follows from Proposition 5(2) (letting $i=n-1$, $j=0$) that $D(n)-(n-1)n \in T_n$, so that $D(n) \ge n^2-n+1$. For $n=2^k+1$, it follows from Proposition 4 that, if $n^2-n+2 \le t \le n^2+1$, then $t \in T_n$, so that $D(n) \le n^2-n+1$. □

It can be shown that, if $n = 2^k + 1$, then $P(n) = 3^k + 1$.

It follows that, if $n = 2^k + 1$, then $n^2 - n + 2 = 1 + D(n) \in T_n$ and $2n^2 - 2n + 3 = 1 + 2D(n) \in T_n$. We can now deduce a part of the principal theorem.

Corollary 7: Suppose $k \geq 1$ and $n = 2^k + 1$. Let $a, b \in T_n$ be such that $a < b$.

(1) If $a + b = n^2 - n + 3$, then $a = 1$ and $b = n^2 - n + 2$.

(2) If $a + b = 2n^2 - 2n + 4$, then $a = 1$ and $b = 2n^2 - 2n + 3$.

Proof: Let $a, b \in T_n$ such that $a < b$.

(1) Suppose $a + b = n^2 - n + 3$ but $a > 1$. Let $c = a - 2$, $d = b - 2$, and $e = c + d = n^2 - n - 1$. Then $b_{n-1}(e) = 1$ and, for $0 \leq i < 2^k = n - 1$, $b_i(e) = 1$ iff $i < 2^{k-1}$. Since $b \in T_n$ and $b \leq n^2 - n + 1$, it must be that $b \leq n^2 - 2n + 1$, so that $d \leq n^2 - 2n$. Therefore, there is $j < k$ such that $b_{k+j}(c) = 1$ and then, also, $b_j(d) = 1$. Consider some such j. Clearly, for each $i < k$, $b_i(c) \neq b_i(d)$. It is also clear that, if $k \leq i < 2k$, then $b_i(c) = b_i(d)$. But then $1 = b_{k+j}(c) = b_{k+j}(d) = b_j(d) \neq b_j(c)$, contradicting Proposition 4.

(2) Suppose $a + b = 2n^2 - 2n + 4$, but $a > 1$. Then $b \geq n^2 - n + 3$. Let $c = b - (n^2 - n + 1)$, so that $c \geq 2$, $c \in T_n$ by Corollary 6(2), and $a + c = n^2 - n + 3$. It follows from (1) that $a = c$, which is impossible because $a + c$ is odd. □

With the assistance of Proposition 3 or Proposition 4 we can, in general, determine a large initial segment of any n^{th} parity sequence.

Proposition 8: Let $k \geq 0$, $q \geq 1$,, $n = q2^k + 1$, and $m = 2^k + 1$. Suppose $1 \leq t \leq n(m-1)$, and let $t = in + j$, where $0 \leq i < m - 1$ and $1 \leq j \leq n$. Let $j = r2^k + s$, where $0 \leq r < q$ and $1 \leq s \leq m$. Then $t \in T_n$ iff $im + s \in T_m$.

Proof: The proof is a straightforward induction on t. □

Proof of the Theorem: Suppose that $n \geq 5$. As previously observed, $3, 4 \in U_n$. It follows from Corollary 7 that, if $n = 2^k + 1$, then $n^2 - n + 3$ and $2n^2 - 2n + 4$ are in U_n.

For the reverse inclusion, suppose that $a, b \in T_n$ are such that $a < b$, $a + b \geq 5$, and for no $a', b' \in T_n$ is it the case that $a \neq a' < b' \neq b$ and $a' + b' = a + b$.

We can assume that $a + b > 2n$. (For, as is easy to check, if $s \leq 2n$, then the number of pairs $a, b \in T_n$ such that $a < b$ and $a + b = s$ is $\left[\frac{1}{2}(s-1)\right]$ if $s \leq n$, is $\frac{1}{2}(n-1)$ if $s > n$ is odd, is $\frac{n}{2}$ if $s > n$ and n is even, and is $\frac{1}{2}(n-2)$ if $s > n$ is even and n is even.) Since $\{1, 2, 3, \ldots, n\} \subseteq T_n$ and since $\{a + b - 1, a + b - 2, a + b - 3, \ldots, a + b - n\} \cap T_n \neq \emptyset$, it must be that $1 \leq a \leq n$. Also, $b \leq 2D(n) + n$, as other-wise setting $a' = a + D(n)$ and $b' = b - D(n)$ yields a contradiction.

Now let $n = q2^k + 1$, where q is odd. We consider two cases.

$a = 1$: Then $\{b-1, b-2, b-3, \ldots, b-n+1\} \cap T_n = \emptyset$. Thus, $b = 1 + pD(n)$ for some $p \geq 1$, and also $p \leq 2$, as otherwise $a' = 1 + D(n)$, $b' = 1 + (p-1)D(n)$ would yield a contradiction. By Corollary 7, we can suppose that $q > 1$. Then, from Proposition 8, we get that $2^k + 1 \in T_n$ and, from Proposition 5, that $D(n) - 2^k + 1 \in T_n$. It follows from Corollary 6 that $D(n) - 2^k + 1 > 2^k + 1$. Thus, setting $a' = 2^k + 1$ and $b' = b - 2^k + 1$ yields a contradiction.

$1 < a \le n$: Then $\{a+b-i : 1 \le i \le n \text{ and } i \ne a\} \cap T_n = \emptyset$. Thus, Proposition 5 implies that $b = pD(n) - n + 1$ for some $p > 0$. Either $a+n \in T_n$ or $a+n-1 \in T_n$. Let a' be whichever one is in T_n, and let $b' = b - (a' - a)$. Then, by Proposition 5, $b' \in T_n$, thereby arriving at a contradiction. □

REFERENCES

1. J. Cassaigne & S. R. Finch. "A Class of 1-Additive Sequences and Quadratic Recurrences." *Experimental Math.* **4** (1995):49-60.
2. S. R. Finch. "Conjectures about *s*-Sequences." *The Fibonacci Quarterly* **29.2** (1991):209-214.
3. S. R. Finch. "Patterns in 1-Additive Sequences." *Experimental Math.* **1** (1992):57-63.
4. J. H. Schmerl & E. Spiegel. "The Regularity of Some 1-Additive Sequences." *J. Comb. Th.* Ser. A, **66** (1994):172-75.
5. S. M. Ulam. *Problems in Modern mathematics.* New York: Interscience, 1964.

AMS Classification Number: 11B13

❖❖❖

NEW ELEMENTARY PROBLEMS AND SOLUTIONS EDITORS AND SUBMISSION OF PROBLEMS AND SOLUTIONS

Starting May 1, 2000, all new problem proposals and corresponding solutions must be submitted to the Problems Editor:

Dr. Russ Euler
Department of Mathematics and Statistics
Northwest Missouri State University
800 University Drive
Maryville, MO 64468

Starting May 1, 2000, all solutions to others' proposals must be submitted to the Solutions Editor:

Dr. Jawad Sadek
Department of Mathematics and Statistics
Northwest Missouri State University
800 University Drive
Maryville, MO 64468

Guidelines for submission of problems and solutions are listed at the beginning of the Elementary Problems and Solutions section of each issue of *The Fibonacci Quarterly.*

COMPLETE AND REDUCED RESIDUE SYSTEMS OF SECOND-ORDER RECURRENCES MODULO p

Hua-Chieh Li
Department of Mathematics, National Tsing Hua University,
Hsinchu, Taiwan 30043, Republic of China
(Submitted August 1998-Final Revision June 1999)

1. INTRODUCTION

Fix a prime p. We say that a set S forms a complete residue system modulo p if, for all i such that $0 \le i \le p-1$, there exists $s \in S$ such that $s \equiv i \pmod{p}$. We say that a set S forms a reduced residue system modulo p if, for all i such that $1 \le i \le p-1$, there exists $s \in S$ such that $s \equiv i \pmod{p}$. In [9], Shah showed that, if p is a prime and $p \equiv 1, 9 \pmod{10}$, then the Fibonacci sequence does not form a complete residue system modulo p. For $p > 7$, Bruckner [2] proved this result for the remaining case. Thus, if p is a prime and $p > 7$, then the Fibonacci sequence $\{F_n\}$ has an incomplete system of residues modulo p. Somer [11] generalized these results by considering all linear recurrence sequences with parameters $(a, 1)$, i.e., linear recurrences of the form

$$u_n = au_{n-1} + u_{n-2}.$$

He proved that, if $p > 7$ and $p \not\equiv 1$ or $9 \pmod{20}$, then all recurrence sequences with parameters $(a, 1)$, for which $p \nmid a^2 + 4$, have an incomplete system of residues modulo p. For the remaining primes, this result has been proved by Schinzel in [8].

In this paper we obtain a unified theory of the structure of recurrence sequences by examining the ratios of recurrence sequences. We can apply our method to prove that, if $p > 7$, then all recurrence sequences with parameters $(a, 1)$, for which $p \nmid a^2 + 4$, have an incomplete system of residues modulo p. To explain our idea more clearly, we include our proof here. However, our idea is totally different from Schinzel's. Finally, we apply our method to determine for which primes p a second-order recurrence sequence forms a reduced residue system modulo p. Our main result is that, if $p > 17$ and $a^2 + 4$ is not a quadratic residue modulo p, then all the recurrence sequences with parameters $(a, 1)$ do not form a reduced residue system modulo p.

2. PRELIMINARIES AND CONVENTIONAL NOTATIONS

Given $a, b \in \mathbb{Z}$, we consider all the second-order linear recurrence sequences $\{u_n\}$ in $\mathbb{Z}$ satisfying $u_n = au_{n-1} + bu_{n-2}$. However, in this paper we exclude the case $u_n = 0$ for all $n \in \mathbb{Z}$. We also exclude the case in which $b \equiv 0 \pmod{p}$ since, in this case, $\{u_n\}$ is not purely periodic modulo p. We call the sequence $\{u_n\}$ a second-order recurrence sequence with parameters (a, b). In particu-lar, the sequence with $u_0 = 0$ and $u_1 = 1$ is called the generalized Fibonacci sequence and we denote it by $\{f_n\}$. The sequence with $u_0 = 2$ and $u_1 = a$ is called the generalized Lucas sequence and we denote it by $\{l_n\}$.

Definition: Let $\{u_n\}$ be a second-order linear recurrence sequence. Consider $r_n = (u_n, u_{n+1})$ as an element in the projective space $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. We call r_n the n^{th} ratio of $\{u_n\}$ modulo p and we call the sequence $\{r_n\}$ the ratio sequence of $\{u_n\}$ modulo p.

We say that two sequences $\{u_n\}$ and $\{u'_n\}$ which both satisfy the same recurrence relation are equivalent modulo p if there is $c \not\equiv 0 \pmod{p}$ and an integer s such that $u_{n+s} \equiv cu'_s \pmod{p}$ for all n. Let $\{r_n\}$ and $\{r'_n\}$ be the ratio sequences of $\{u_n\}$ and $\{u'_n\}$ modulo p, respectively. Then $\{u_n\}$ and $\{u'_n\}$ are equivalent modulo p if and only if there exist integers s and t such that $r_s = r'_t$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$.

Since $\{u_n\}$ is periodic modulo p, the ratio sequence $\{r_n\}$ of $\{u_n\}$ modulo p is also periodic. The least positive integer z such that $r_0 = r_z$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ is called the rank of $\{u_n\}$ modulo p. We remark that the rank of apparition of $\{f_n\}$ modulo p (i.e., the smallest positive integer z such that $f_z \equiv 0 \pmod{p}$), by our definition, equals the rank of $\{f_n\}$ modulo p.

For convenience, we introduce some notation:

(1) (β/p) denotes the Legendre symbol; i.e., for $p \nmid \beta$, $(\beta/p) = 1$ if $y^2 \equiv \beta \pmod{p}$ is solvable and $(\beta/p) = -1$ if $y^2 \equiv \beta \pmod{p}$ is not solvable.

(2) For an integer $m \not\equiv 0 \pmod{p}$, we denote m^{-1} to be the solution of $mx \equiv 1 \pmod{p}$.

(3) We denote the least positive integer t such that $d^t \equiv 1 \pmod{p}$ by $\mathrm{ord}_p(d)$.

Given a sequence $\{u_n\}$, there exists an $r \in \mathbb{Z}$ such that $\{u_n\}$ modulo p is equivalent to the sequence $\{u'_n\}$ modulo p with $u'_0 = 1$ and $u'_1 = r$. Therefore, without loss of generality, we only consider the sequence with $u_0 = 1$ and $u_1 = r$.

The following lemmas are not new. However, for some of the lemmas, we include proofs because these ideas will be used for the proof of our main theorems.

Lemma 2.1: Let $\{u_n\}$ be the recurrence sequence with parameters (a, b) and $u_0 = 1$, $u_1 = r$. Then the rank of $\{u_n\}$ modulo p equals the rank of $\{f_n\}$ modulo p if $r^2 - ar - b \not\equiv 0 \pmod{p}$.

Proof: Suppose the the rank of $\{u_n\}$ modulo p is t and the rank of $\{f_n\}$ modulo p is z. Since $u_n = bf_{n-1} + rf_n$, we have that $u_{z+1} \equiv rf_{z+1} \equiv ru_z \pmod{p}$ because $f_z \equiv 0 \pmod{p}$ and $bf_{z-1} \equiv f_{z+1} \pmod{p}$. This says that $(u_z, u_{z+1}) = (u_0, u_1)$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ and hence $t \mid z$. On the other hand, we have that $bf_t + rf_{t+1} \equiv r(bf_{t-1} + rf_t) \pmod{p}$ by the assumption that $u_{t+1} \equiv ru_t \pmod{p}$. Substituting $f_{t+1} = af_t + bf_{t-1}$, we have that $(r^2 - ar - b)f_t \equiv 0 \pmod{p}$. Therefore, $p \nmid r^2 - ar - b$ implies that $f_t \equiv 0 \pmod{p}$. This says that $z \mid t$. □

Lemma 2.2: Let p be an odd prime and let z be the rank of the generalized Fibonacci sequence with parameters (a, b) modulo p. Let $D = a^2 + 4b$. Then

(i) $z \mid p+1$ if $(D/p) = -1$,

(ii) $z = p$ if $p \mid D$,

(iii) $z \mid p-1$ if $(D/p) = 1$.

Proof: ***(i)*** Suppose that $(D/p) = -1$. Then $x^2 - ax - b \equiv 0 \pmod{p}$ has no solution. Thus, by Lemma 2.1, every recurrence sequence with parameters (a, b) has the same rank modulo p. Let t be the number of distinct equivalence classes of recurrence sequences of parameters (a, b) modulo p. Further, let $\{\{u_{i,n}\} \mid 1 \le i \le t\}$ be a representative of these equivalence classes and let $\{\{r_{i,n}\} \mid 1 \le i \le t\}$ be their ratio sequences in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, respectively. By definition, we then have $r_{i,s} \neq r_{i,\lambda}$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ for all $1 \le s \neq \lambda \le z$ and, if $i \neq j$, $\{r_{i,n}\}$ and $\{r_{j,n}\}$ are disjoint. Since, for

any $r \in \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, $(u_0, u_1) = r$ gives a sequence $\{u_n\}$, we have $\{r_{1,1}, \ldots, r_{1,z}\} \cup \cdots \cup \{r_{t,1}, \ldots, r_{t,z}\} = \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. It follows that $tz = p+1$ because the number of elements in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ is $p+1$.

(ii) For $p \mid D$, $x^2 - ax - b \equiv 0 \pmod{p}$ has a double root. By Lemma 2.1, the number of ratios that give the same rank as the generalized Fibonacci sequence does is $p+1-1 = p$. Our claim follows by a similar argument as in (i) above.

(iii) For $(D/p) = 1$, there exist two distinct solutions to $x^2 - ax - b \equiv 0 \pmod{p}$. Our claim follows by a similar argument as in (i) above. □

Remark: From the proof above, we have that the number of distinct equivalence classes of recurrence sequences with parameters (a, b) modulo p is $(p+1)/z$ (resp. $2+(p-1)/z$), if $(D/p) = -1$ (resp. $(D/p) = 1$).

Lemma 2.3: Let z be the rank of the generalized Fibonacci sequence with parameters (a, b) modulo p and let $D = a^2 + 4b$. Suppose that p is an odd prime such that $p \nmid D$. Then $(-b/p) = 1$ if and only if $z \left| \frac{p-(D/p)}{2} \right.$.

Proof: For the proof, please see Lehmer [5]. □

Lemma 2.4: Let $\{f_n\}$ be the generalized Fibonacci sequence with parameters (a, b) and let z be the rank and k be the period of $\{f_n\}$ modulo p, respectively. Let $z = 2^v z'$ and $\operatorname{ord}_p(-b) = 2^\mu h$, where z' and h are odd integers.

(i) If $v \neq \mu$, then $k = 2\operatorname{lcm}[z, \operatorname{ord}_p(-b)]$.

(ii) If $v = \mu > 0$, then $k = \operatorname{lcm}[z, \operatorname{ord}_p(-b)]$.

Proof: For the proof, please see Wyler [13]. □

In the following, we concentrate on recurrence sequences with parameters $(a, 1)$.

Lemma 2.5: Let $\{u_n\}$ and $\{u'_n\}$ be two recurrence sequences with parameters $(a, 1)$. Then $u_r u'_s + u_{r+1} u'_{s+1} = u_{r+1} u'_{s-1} + r_{r+2} u'_s$.

Proof: By the recurrence formula, we have that

$$u_{r+1} u'_{s-1} + u_{r+2} u'_s = u_{r+1}(u'_{s+1} - au'_s) + (au_{r+1} + u_r) u'_s = u_{r+1} u'_{s+1} + u_r u'_s. \quad \square$$

Lemma 2.6: Let z be the rank of apparition of the generalized Fibonacci sequence modulo p.

(i) $f_i f_{z-i-1} + f_{i+1} f_{z-i} \equiv 0 \pmod{p}$.

(ii) $f_{\lambda z - t} \equiv \begin{cases} f_{\lambda z + t} \pmod{p} & \text{if } t \text{ is odd,} \\ -f_{\lambda z + t} \pmod{p} & \text{if } t \text{ is even.} \end{cases}$

(iii) If z is even, then $f_{z/2 - t} \equiv \begin{cases} -f_{z/2 + t} \pmod{p} & \text{if } t \text{ is odd,} \\ f_{z/2 + t} \pmod{p} & \text{if } t \text{ is even.} \end{cases}$

Proof: ***(i)*** Since $1 f_{z-2} + a f_{z-1} = f_z \equiv 0 \pmod{p}$ and $f_1 = 1$, $f_2 = a$ by Lemma 2.5, we have that $f_2 f_{z-3} + f_3 f_{z-2} \equiv 0 \pmod{p}$. By induction, our claim follows.

(ii) Since $f_{\lambda z} \equiv 0 \pmod{p}$, we have that $f_{\lambda z} f_{\lambda z - 1} + f_{\lambda z + 1} f_{\lambda z} \equiv 0 \pmod{p}$. It follows from Lemma 2.5 that $f_{\lambda z + 1} f_{\lambda z - 2} + f_{\lambda z + 2} f_{\lambda z - 1} \equiv 0 \pmod{p}$. We have that $f_{\lambda z - 2} \equiv -f_{\lambda z + 2} \pmod{p}$ because $f_{\lambda z - 1} \equiv f_{\lambda z + 1} \pmod{p}$. By induction, our claim follows.

(iii) Substitute $i = z/2$ in (i). We have $f_{z/2}f_{z/2-1} + f_{z/2+1}f_{z/2} \equiv 0 \pmod{p}$. Since $f_{z/2} \not\equiv 0 \pmod{p}$, it follows that $f_{z/2-1} \equiv -f_{z/2+1} \pmod{p}$. By induction, our claim follows. □

Since $f_{z+1} \equiv f_{z+1}f_1 \pmod{p}$ and $f_z \equiv f_{z+1}f_0 \pmod{p}$, it follows that $f_{n+z} \equiv f_{z+1}f_n \pmod{p}$ for all n. Suppose that $\{u_n\}$ is a recurrence sequence with parameters $(a, 1)$. Then, as $u_n = u_0f_{n-1} + u_1f_n$, we also have $u_{n+z} \equiv f_{z+1}u_n \pmod{p}$ for all n and, hence, $u_{n+\lambda z} \equiv f_{z+1}^{\lambda}u_n \pmod{p}$.

Lemma 2.7: Let z be the rank of apparition of the generalized Fibonacci sequence modulo p. Then

(i) $l_{i-1}l_{z-i} + l_il_{z-i+1} \equiv 0 \pmod{p}$,

(ii) $l_{\lambda z-t} \equiv \begin{cases} -l_{\lambda z+t} \pmod{p} & \text{if } t \text{ is odd,} \\ l_{\lambda z+t} \pmod{p} & \text{if } t \text{ is even.} \end{cases}$

Proof: ***(i)*** Since z is the rank of $\{f_n\}$ modulo p, by the argument above it follows that $(l_z, l_{z+1}) = (l_0, l_1) = (2, a)$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. By the recurrence relation, we have that $(l_{z-1}, l_z) = (-a, 2)$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. Therefore, we have that $l_0l_{z-1} + l_1l_z \equiv 0 \pmod{p}$. By Lemma 2.5, it follows that $l_1l_{z-2} + l_2l_{z-1} \equiv 0 \pmod{p}$. By induction, our claim follows.

(ii) Since $l_{\lambda z-1} \equiv -l_{\lambda z+1} \pmod{p}$, we have that $l_{\lambda z}l_{\lambda z-1} + l_{\lambda z+1}l_{\lambda z} \equiv 0 \pmod{p}$. By Lemma 2.5 it follows that $l_{\lambda z+1}l_{\lambda z-2} + l_{\lambda z+2}l_{\lambda z-1} \equiv 0 \pmod{p}$. Therefore, $l_{\lambda z-2} \equiv l_{\lambda z+2} \pmod{p}$. By induction, our claim follows. □

3. COMPLETE RESIDUE SYSTEMS OF SECOND-ORDER RECURRENCES MODULO p

Somer [11] proved that, if $p > 7$, $p \mid a^2 + 4$, and $p \not\equiv 1$ or $9 \pmod{20}$, then all recurrence sequences with parameters $(a, 1)$ have an incomplete system of residues modulo p. In Theorem 3.3 we will improve Somer's results to all primes $p > 7$ by substantially extending the methods used in Somer's paper. As remarked earlier, Schinzel [8] proved this result by a different method.

We remark that, if $u_i \equiv 0 \pmod{p}$ for some i, then the recurrence sequence $\{u_n\}$ is equivalent to $\{f_n\}$ modulo p. Therefore, we only have to consider the sequence that is equivalent to the generalized Fibonacci sequence modulo p. Hence, we reduce our problem to considering whether or not $\{f_n\}$ forms a complete residue system modulo p.

First, we consider the case where $p \mid a^2 + 4$ and $x^2 - ax - 1 \equiv 0 \pmod{p}$ is solvable. In this case, it follows by Lemmas 2.2, 2.3, and 2.4 that the period of $\{f_n\}$ divides $p - 1$. Thus, the number of distinct residues of $\{f_n\}$ modulo p is less than p and we conclude that $\{f_n\}$ does not form a complete residue system modulo p.

Now we consider the case where $x^2 - ax - 1 \equiv 0 \pmod{p}$ is not solvable.

Lemma 3.1: Suppose that $x^2 - ax - 1 \equiv 0 \pmod{p}$ is not solvable. Let z be the rank of apparition of the generalized Fibonacci sequence modulo p. Consider all recurrence sequences with parameters $(a, 1)$ modulo p. Fix an integer e with $1 \le e < z$. Then, given an integer λ, up to the equivalence relation, there exists a unique $\{u_n\}$ and there exists a unique integer i depending on $\{u_n\}$ with $1 \le i \le z$ such that $u_{i+e} \equiv \lambda u_i \pmod{p}$.

Proof: Suppose $(u_i, u_{i+1}) = (1, r)$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. Then we see by induction that $(u_i, u_{i+e}) = (1, rf_e + f_{e-1})$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. Since $f_e \not\equiv 0 \pmod{p}$, for $1 \le e < z$, there exists a unique r modulo p

such that $rf_e + f_{e-1} \equiv \lambda \pmod{p}$. For the ratio $(1, r) \in \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, this gives a unique equivalence class of recurrence sequences modulo p. Let $\{u_n\}$ be a representative of such a class. Since there is no solution for $x^2 - ax - 1 \equiv 0 \pmod{p}$, the rank of $\{u_n\}$ modulo p is equal to z. Therefore, there exists a unique i with $1 \le i \le z$ such that $(u_i, u_{i+1}) = (1, r)$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. □

Example: We are particularly interested in the case $\lambda \equiv \pm 1 \pmod{p}$. Consider the recurrence sequences satisfying $u_n = 3u_{n-1} + u_{n-2}$ modulo $p = 7$. We have the generalized Fibonacci sequence

$$\{f_n\}_0^\infty \equiv \{0, 1, 3, 3, 5, 4, 3, 6, 0, 6, 4, 4, 2, 3, 4, 1, 0, \ldots\} \pmod{7}.$$

Since $z = 8 = p + 1$, every recurrence sequence with parameters (3, 1) is equivalent to $\{f_n\}$ modulo 7. For $e = 3$, we have $f_3 \equiv f_{3+3}$ and $f_2 \equiv -f_{2+3} \pmod{7}$. For $e = 5$, we have $f_5 \equiv f_{5+5}$ and $f_6 \equiv -f_{6+5} \pmod{7}$.

Since Somer has treated the case $p \equiv 3 \pmod{4}$ completely, in the following we only consider the case $p \equiv 1 \pmod{4}$.

For the case $p \equiv 1 \pmod{4}$, by Lemma 2.3, we have that $z \mid (p+1)/2$; hence, by Lemma 2.4, $k = 4z$. Thus, $k \ge p$ occurs only if $z = (p+1)/2$; hence, we have to consider only the case $z = (p+1)/2$. In this case, by the Remark following Lemma 2.2, there are exactly two distinct equivalence classes of recurrence sequences with parameters $(a, 1)$ modulo p. One is equivalent to $\{f_n\}$ modulo p and the other is equivalent to $\{l_n\}$ because of the following.

Lemma 3.2: Let $p \equiv 1 \pmod{4}$ be a prime such that $x^2 - ax - 1 \equiv 0 \pmod{p}$ is not solvable.

(i) The generalized Lucas sequence with parameters $(a, 1)$ is not equivalent to the generalized Fibonacci sequence with parameters $(a, 1)$ modulo p.

(ii) Let z be the rank of $\{f_n\}$ modulo p. Then, for every $t, \lambda \in \mathbb{Z}$, $l_t l_{z-t+\lambda} \equiv (-1)^\lambda l_{t-\lambda} l_{z-t} \pmod{p}$.

Proof: ***(i)*** For $\{f_n\}$, we have $f_n^2 - f_{n-1}f_{n+1} = (-1)^{n-1}$. Suppose that $\{u_n\}$ is equivalent to $\{f_n\}$ modulo p. Then there exist r and j such that $u_n \equiv r f_{n+j} \pmod{p}$ for all n. Thus, $u_n^2 - u_{n-1}u_{n+1} \equiv (-1)^{n+j-1} r^2 \pmod{p}$; hence, it is a quadratic residue modulo p for all n because -1 is a quadratic residue modulo p. On the other hand, $l_n^2 - l_{n-1}l_{n+1} = (-1)^n(a^2 + 4)$ which, by assumption, is not a quadratic residue modulo p. Our first claim follows.

(ii) Since $\{l_n\}$ is not equivalent to $\{f_n\}$ modulo p, it follows that $l_n \not\equiv 0 \pmod{p}$ for all n. By Lemma 2.7(i), we have that $l_t l_{t-1}^{-1} \equiv -l_{z-t} l_{z-t+1}^{-1}$, $l_{t-1} l_{t-2}^{-1} \equiv -l_{z-t+1} l_{z-t+2}^{-1}, \ldots \pmod{p}$. Multiplying on both sides, our proof is complete. □

From the proof above we know that, if $z = (p+1)/2$, then $\{u_n\}$ is equivalent to $\{f_n\}$ modulo p if and only if $u_n^2 - u_{n-1}u_{n+1}$ is a quadratic residue modulo p for all n.

By Lemma 2.6(ii), for each t with $1 \le t \le k = 2(p+1)$, we have that $f_t \equiv \pm f_i \pmod{p}$ for some i, where $1 \le i \le z = (p+1)/2$. Thus, if we can find one pair (i, j), where $1 \le i, j \le z - 1$, such that $f_i \equiv \pm f_j \pmod{p}$, then the number of distinct residues of $\{f_n\}$ modulo p is less than or equal to $2(z-2) + 1 = p - 2$ since $f_0 \equiv f_z \equiv 0 \pmod{p}$; hence, $\{f_n\}$ does not form a complete residue system modulo p. We only have to claim that there exists an odd integer e such that $1 \le e < (p+1)/2$ and $f_i \equiv \pm f_{i+e} \pmod{p}$ for some i such that $1 \le i \le z - 1$. This claim is sufficient because in this case, if $i + e > z$, then by Lemma 2.6(ii), we have that $f_i \equiv \pm f_{2z-(i+e)} \pmod{p}$ and $1 \le 2z - (i+e) < z$. (Notice that $2z - (i+e) - i$ is also odd.) Now, for a fixed odd integer e, consider the sequence $\{u_n\}$ such that $u_n = f_n - f_{n+e}$. Since e is odd, it follows by the Binet formulas that

$$u_n^2 - u_{n-1}u_{n+1} = (-1)^n(f_{e+1} + f_{e-1}) = (-1)^n l_e.$$

Since $p \equiv 1 \pmod 4$, it follows that there exists i with $1 \le i \le z-1$ such that $f_i \equiv f_{i+e} \pmod p$ if and only if $\{u_n\}$ is equivalent to $\{f_n\}$ modulo p if and only if l_e is a quadratic residue modulo p. Similarly, using the Binet formulas to show that, if $u'_n = f_n + f_{n+e}$, then $(u'_n)^2 - u'_{n-1}u'_{n+1} = (-1)^{n-1}l_e$, we find that there exists j such that $1 \le j \le z-1$ and such that $f_j \equiv -f_{j+e} \pmod p$ if and only if l_e is a quadratic residue modulo p. We remark that l_z is a quadratic residue modulo p since, for $e = z$, $u_0 = f_0 - f_z \equiv 0 \pmod p$.

Theorem 3.3: Let $\{f_n\}$ be the generalized Fibonacci sequence with parameters $(a, 1)$ and let p be a prime such that $p \equiv 1 \pmod 4$ and $(D/p) = -1$, where $D = a^2 + 4$. Then, for $p > 5$, $\{f_n\}$ does not form a complete residue system modulo p.

Proof: Assume that l_e is not a quadratic residue modulo p for all odd integers e such that $1 \le e < z$. We shall get a contradiction.

First, we consider the case $p \equiv 5 \pmod 8$. By substituting $i = (z-1)/2$ in Lemma 2.6(i) and $i = (z+1)/2$ in Lemma 2.7(i), we have that $l_{(z+1)/2}l_{(z-1)/2}^{-1}$ and $f_{(z+1)/2}f_{(z-1)/2}^{-1}$ are solutions to $x^2 \equiv -1 \pmod p$; hence, neither is a quadratic residue modulo p. Note that $l_0 = 2$ is not a quadratic residue modulo p, either. By assumption, $l_1 = a$ is not a quadratic residue modulo p. By Lemma 2.7(i), $l_1l_0^{-1} \equiv -l_{z-1}l_z^{-1} \pmod p$; hence, l_{z-1} is a quadratic residue modulo p. By the assumption $(l_{z-2}/p) = -1$, we have that $(l_2/p) = 1$ because $l_2l_1^{-1} \equiv -l_{z-2}l_{z-1}^{-1} \pmod p$. By induction, we have that $(l_i/p) = -1$ for odd i, but $(l_j/p) = 1$ for even j, where $1 \le i,\ j \le z-1$. This means that $l_tl_{t-1}^{-1}$ is not a quadratic residue modulo p for every t such that $2 \le t \le z-1$. Note that every element of $\{l_tl_{t-1}^{-1} \mid 2 \le t \le z-1\}$ is in a distinct residue class modulo p and that there are $z-2 = (p-3)/2$ of them. Because $\{l_n\}$ and $\{f_n\}$ are not equivalent modulo p, $\{l_tl_{t-1}^{-1} \mid 2 \le t \le z-1\}$ and $\{f_tf_{t-1}^{-1} \mid 2 \le t \le z-1\}$ are disjoint modulo p. It follows that among $\{f_tf_{t-1}^{-1} \mid 2 \le t \le z-1\}$ there is only one which is not a quadratic residue modulo p. But we know that neither $f_{(z+1)/2}f_{(z-1)/2}^{-1}$ nor $f_2f_1^{-1} = a = l_1$ is a quadratic residue modulo p. We get a contradiction because, by the assumption, $p > 5$, $(z+1)/2 = (p+3)/4 > 2$.

For the case $p \equiv 1 \pmod 8$, $l_{(z+1)/2}l_{(z-1)/2}^{-1}$ and $f_{(z+1)/2}f_{(z-1)/2}^{-1}$ are roots of $x^2 \equiv -1 \pmod p$; hence, both are quadratic residues modulo p. Note that $l_0 = 2$ is also a quadratic residue modulo p. By the same reasoning as above, we have that $(l_i/p) = -1$ for every integer i such that $1 \le i \le z-1$; hence, $l_tl_{t-1}^{-1}$ is a quadratic residue modulo p for every t such that $2 \le t \le z-1$. Therefore, among $\{f_tf_{t-1}^{-1} \mid 2 \le t \le z-1\}$, $f_{(z+1)/2}f_{(z-1)/2}^{-1}$ is the only quadratic residue modulo p. However, since $f_2 = a = l_1$ is not a quadratic residue modulo p, it follows that $f_4 = f_2l_2$ is a quadratic residue modulo p. Hence, one of $f_3f_2^{-1}$ or $f_4f_3^{-1}$ is a quadratic residue modulo p. We get a contradiction because, by the assumption, $p \ge 17$, $(z+1)/2 = (p+3)/4 > 4$. □

4. REDUCED RESIDUE SYSTEMS OF SECOND-ORDER RECURRENCES MODULO p

From the previous section, we conclude that, if $p > 7$ and $p \nmid a^2 + 4$, then every recurrence sequence $\{u_n\}$ with parameters $(a, 1)$ does not form a complete residue system modulo p.

It would be interesting to know whether or not the recurrence sequence $\{u_n\}$ forms a reduced residue system modulo p.

For the prime p such that $p \mid a^2+4$, since $z = p$, there are exactly two distinct equivalence classes modulo p. One is the equivalence class of $\{f_n\}$ modulo p and the other is the equivalence class of $\{v_n\}$ which satisfies $v_0 = 1$ and $v_1 = \alpha$, where α is the double root of $x^2 - ax - 1 \equiv 0 \pmod{p}$. We already know, by [3], [11], and [12], that $\{f_n\}$ forms a complete residue system modulo p. Moreover, $\{v_n\}$ also forms a reduced residue system modulo p if and only if α is a primitive root modulo p, since $v_n \equiv \alpha^n \pmod{p}$.

Definition: Let α be a root of $x^2 - ax - 1 \equiv 0 \pmod{p}$. We call α a generalized Fibonacci primitive root with parameters $(a, 1)$ modulo p if α is a primitive root modulo p. For the case $a = 1$, we call it a Fibonacci primitive root modulo p.

Brison [1], using Hermite's criterion for a permutation polynomial over a finite field (see [6]), proved that, for $p \geq 7$, a recurrence sequence $\{u_n\}$ with parameters $(1, 1)$ has the property that $\{u_1, u_2, \ldots, u_{p-1}\}$ is a reduced residue system modulo p if and only if $\{u_n\}$ is equivalent to the sequence $\{v_n\}$ modulo p, where $v_0 = 1$ and v_1 is a Fibonacci primitive root modulo p. Brison's method can be applied directly to recurrence sequences with parameters $(a, 1)$. Therefore, we have the following lemma.

Lemma 4.1: Let $p \geq 7$ be a prime. Then a recurrence sequence $\{u_n\}$ with parameters $(a, 1)$ has the property that $\{u_1, u_2, \ldots, u_{p-1}\}$ is a reduced residue system modulo p if and only if $u_2 u_1^{-1}$ modulo p is a generalized Fibonacci primitive root with parameters $(a, 1)$ modulo p.

For a prime $p \geq 7$ such that a^2+4 is a quadratic residue modulo p, the period of every recurrence sequence with parameters $(a, 1)$ modulo p divides $p-1$. Therefore, we rephrase Lemma 4.1 as follows.

Proposition 4.2: Let $p \geq 7$ be a prime such that a^2+4 is a quadratic residue modulo p. Then a recurrence sequence $\{u_n\}$ with parameters $(a, 1)$ forms a reduced residue system modulo p if and only if $u_2 u_1^{-1}$ modulo p is a generalized Fibonacci primitive root with parameters $(a, 1)$ modulo p.

Fibonacci primitive roots and related topics have an extensive literature. Here, we refer to Shanks [10] and Phong [7].

Lemma 4.1 does not answer our question for primes p such that a^2+4 is not a quadratic residue modulo p, because in this case the period of the recurrence sequence with parameters $(a, 1)$ modulo p may be greater than $p-1$. We have the following example.

Example: Consider the Lucas sequence $\{L_n\}$ (i.e., $L_0 = 2$, $L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$) modulo 13 and 17. We have that

$$\{L_n\}_{n=0}^{7} \equiv \{2, 1, 3, 4, 7, 11, 5, 3\} \pmod{13},$$

$$\{L_n\}_{n=14}^{21} \equiv \{11, 12, 10, 9, 6, 2, 8, 10\} \pmod{13},$$

and

$$\{L_n\}_{n=0}^{9} \equiv \{2, 1, 3, 4, 7, 11, 1, 12, 13, 8\} \pmod{17},$$

$$\{L_n\}_{n=18}^{27} \equiv \{15, 16, 14, 13, 10, 6, 16, 5, 4, 9\} \pmod{17}.$$

Therefore, the Lucas sequence forms a reduced residue system modulo 13 and 17.

We now claim that, for a prime $p>17$ such that a^2+4 is not a quadratic residue modulo p, every recurrence sequence with parameters $(a, 1)$ does not form a reduced residue system modulo p.

Let $\{u_n\}$ be a recurrence sequence with parameters $(a, 1)$. Since $u_n = u_0 f_{n-1} + u_1 f_n$, we have that the period of $\{u_n\}$ modulo p divides the period of $\{f_n\}$ modulo p. Therefore, as before, we only have to consider the cases where the rank of the generalized Fibonacci sequence modulo p is $(p+1)/2$ or $p+1$. If the rank is $p+1$, then, since every sequence is equivalent to $\{f_n\}$ modulo p, it follows that none of the recurrence sequences with parameters $(a, 1)$ forms a reduced residue system modulo p. For the case in which the rank is $(p+1)/2$, by Theorem 3.3, $\{f_n\}$ does not form a complete residue system modulo p. Therefore, we only have to consider the generalized Lucas sequence $\{l_n\}$ modulo p. By Lemma 2.7(ii), for every t with $1 \le t \le k = 2(p+1)$, we have that $l_t \equiv \pm l_i$ for some i, where $0 \le i \le z = (p+1)/2$. Thus, if we can find three distinct pairs (i, j) such that $0 \le i < j \le (p+1)/2$ and $l_i \equiv \pm l_j \pmod p$, then the number of distinct residues of $\{l_n\}$ modulo p is less than or equal to $2(z+1-3) = p-3$; hence, $\{l_n\}$ does not form a reduced residue system modulo p.

For a fixed odd integer e, consider the sequence $\{v_n\}$ such that $v_n = l_n - l_{n+e}$. Since e is odd, we see by the Binet formulas that $v_n^2 - v_{n-1}v_{n+1} = (-1)^{n-1}(a^2+4)l_e$. Since $z = (p+1)/2$, by Lemma 2.3, $p \equiv 1 \pmod 4$. Because a^2+4 is not a quadratic residue modulo p, it follows that there exists $0 \le i \le (p+1)/2$ such that $l_i \equiv l_{i+e} \pmod p$ if and only if $\{v_n\}$ is equivalent to $\{f_n\}$ modulo p if and only if l_e is not a quadratic residue modulo p. Similarly, by using the Binet formulas to show that, if $v'_n = l_n + l_{n+e}$, then $(v'_n)^2 - v'_{n-1}v'_{n+1} = (-1)^n(a^2+4)l_e$, we have that there exists j such that $0 \le j \le z$ and such that $l_j \equiv -l_{j+e} \pmod p$ if and only if l_e is not a quadratic residue modulo p. If there exist three distinct odd integers e such that $0 < e < z$ and l_e is not a quadratic residue modulo p, then, by the routine argument given in the last section, we can find three distinct pairs (i, j) such that $0 \le i < j \le z$ and $l_i \equiv \pm l_j \pmod p$.

Suppose that there are at most two odd integers e such that $0 < e < z$ and l_e is not a quadratic residue modulo p. Then, for p large enough, we claim this leads to a contradiction.

First, we consider the case $p \equiv 1 \pmod 8$. Recall that $z = (p+1)/2$ and l_z must be a quadratic residue modulo p. Since $l_0 = 2$ in this case, we have $(l_0/p) = (l_z/p) = 1$; hence, $(l_1/p) = (l_{z-1}/p)$ by Lemma 2.7(i). Again, by Lemma 2.7(i) and by induction, it follows that $(l_i/p) = (l_{z-1}/p)$ for all $0 \le i \le (z+1)/2$. Note that i is odd if and only if $z-i$ is even. By assumption, there are at most two odd integers e such that $0 < e < z$ and $(l_e/p) = -1$; hence, there are also at most two even integers e such that $0 < e < z$ and $(l_e/p) = -1$. Therefore, among $\{l_i l_{i-1}^{-1} \mid 1 \le i \le z\}$ modulo p, there are at most eight quadratic nonresidues modulo p. Hence, there are at least $(p+1)/2 - 8$ nonzero quadratic residues modulo p in $\{l_i l_{i-1}^{-1} \mid 1 \le i \le z\}$. Since $\{f_i f_{i-1}^{-1} \mid 1 < i < z\}$ and $\{l_i l_{i-1}^{-1} \mid 1 \le i \le z\}$ modulo p form a reduced residue system modulo p, we get a contradiction if we find eight nonzero quadratic residues modulo p among $\{f_i f_{i-1}^{-1} \mid 1 < i < z\}$. Let $s = (z+1)/2$. By Lemma 2.6(i), we have that $f_{s+i} f_{s+i-1}^{-1} \equiv -f_{s-i-1} f_{s-i}^{-1} \pmod p$. Therefore, for s large enough, if we can prove that there exist four integers i with $1 < i < s = (p+3)/4$ such that $f_i f_{i-1}^{-1}$ is a nonzero quadratic residue modulo p, then our claim follows. Recall that $f_{2n} = l_n f_n$. Suppose that e is odd and $(l_e/p) = 1$. Then we have $(f_e/p) = (f_{2e}/p)$ and, since e is odd, it follows that there exists i with $e < i \le 2e$ such that $(f_i/p) = (f_{i-1}/p)$. Thus, $f_i f_{i-1}^{-1}$ is a quadratic residue modulo p. Hence,

our strategy is finding s large enough so that we can find four positive odd integers $e(i)$ with $2e(i) < e(i+1)$ for $1 \le i \le 3$ and $2e(4) < s$ such that $(l_{e(i)} / p) = 1$ for all $1 \le i \le 4$. Since, by assumption, we have at most two odd integers e such that $(l_e / p) = -1$, the worst case is that $(l_1 / p) = (l_3 / p) = -1$. In this case, we can choose $e(1) = 5$, $e(2) = 11$, $e(3) = 23$, and $e(4) = 47$. Therefore, for $s > 94$ (i.e., $p > 373$), we get a contradiction.

Next we consider the case $p \equiv 5 \pmod 8$. Since $l_0 = 2$ in this case, we have that $(l_0 / p) = -(l_z / p) = -1$; hence, $(l_1 / p) = -(l_{z-1} / p)$ by Lemma 2.7(i). Again, by Lemma 2.7(i) and by induction, it follows that $(l_i / p) = -(l_{z-i} / p)$ for all $0 \le i \le (z+1)/2$. By assumption, there are at most two odd integers e such that $0 < e < z$ and $(l_e / p) = -1$; hence, there are at most two positive even integers e such that $0 < e < z$ and $(l_e / p) = 1$. Thus, among $\{l_i l_{i-1}^{-1} \mid 1 \le i \le z\}$ modulo p, there are at most eight quadratic residues modulo p, so there are at least $(p+1)/2 - 8$ quadratic nonresidues modulo p in $\{l_i l_{i-1}^{-1} \mid 1 \le i \le z\}$. Therefore, by the same argument as above for s large enough, if we can prove that there exist four integers i with $1 < i < s = (p+3)/4$ such that $f_i f_{i-1}^{-1}$ is a quadratic nonresidue modulo p, then our claim follows. Suppose that e is even and $(l_e / p) = -1$. Then we have $(f_e / p) = -(f_{2e} / p)$, and it follows that there exists an integer i with $e < i \le 2e$ such that $((f_i / p) = -(f_{i-1} / p)$. Thus, $f_i f_{i-1}^{-1}$ is a quadratic nonresidue modulo p. Hence, our strategy is finding s large enough so that we are able to discover four positive even integers $e(i)$ with $2e(i) \le e(i+1)$ for $1 \le i \le 3$ and $2e(4) < s$ such that $(l_{e(i)} / p) = -1$ for all $1 \le i \le 4$. The worst case is that $(l_2 / p) = (l_4 / p) = 1$. In this case, we can choose $e(1) = 6$, $e(2) = 12$, $e(3) = 24$, and $e(4) = 48$. Therefore, for $s > 96$ (i.e., $p > 381$), we get a contradiction.

We remark that, by more detailed investigation, the argument can be narrowed down to the case $s > 13$ (i.e., $p > 49$). However, in order to avoid this complication, we omit the proof here. For the cases $p = 29$, $p = 37$, and $p = 41$, by direct computation, we have that the generalized Lucas sequence with parameters $(a, 1)$ does not form a reduced residue system modulo p. Thus, we have the following theorem.

Theorem 4.3: Let p be a prime such that $a^2 + 4$ is not a quadratic residue modulo p. Then, for $p > 17$, every recurrence sequence $\{u_n\}$ with parameters $(a, 1)$ does not form a reduced residue system modulo p.

In conclusion, we remark that in [11] Somer mentions that, for a more general recurrence sequence (i.e., a recurrence with parameters (a, b), where $b \ne 1$) our results are not always true. The following proposition tells us that, given any prime p, there exists a generalized Fibonacci sequence that forms a complete residue system modulo p.

Proposition 4.4: Suppose that either $p = 2$ or that p is an odd prime, $-b$ is a primitive root modulo p, and $a^2 + 4b$ is not a quadratic residue modulo p. Then the generalized Fibonacci sequence $\{f_n\}$ with parameters (a, b) forms a complete residue system modulo p. Furthermore, every recurrence sequence with parameters (a, b) which is not equivalent to $\{f_n\}$ forms a reduced residue system modulo p.

Proof: The proposition is true by inspection for $p = 2$. Assume $p > 2$. Let z and k be the rank and period of $\{f_n\}$ modulo p, respectively. Since $a^2 + 4b$ is not a quadratic residue modulo p, then $z \mid p+1$ by Lemma 2.2. Furthermore, since $-b$ is not a quadratic residue modulo p, then $z \nmid (p+1)/2$ by Lemma 2.3. Suppose that $p \equiv 1 \pmod 4$. Then $z \equiv 2 \pmod 4$ and, by Theorem

2.4, it follows that $k = 2\gcd[z, p-1] = z(p-1)$. Suppose that $p \equiv 3 \pmod 4$. Then $z \equiv 0 \pmod 4$ and, by Theorem 2.4, it follows that $k = 2\gcd[z, p-1] = z(p-1)$. This shows that f_{z+1} is a primitive root modulo p in both cases. Since, for every recurrence sequence $\{u_n\}$ with parameters (a, b), $u_{\lambda z+1} \equiv f_{z+1}^{\lambda} u_1 \pmod p$, our proof is complete. □

Remark: Regarding the statement of Proposition 4.4, we note that, for any odd prime p, one can always find residues a and b modulo p such that $-b$ is a primitive root modulo p and $a^2 + 4b$ is a quadratic nonresidue modulo p. It was proved in [4] that, for a fixed residue b modulo p, one can always find a residue a such that $a^2 + 4b$ is a quadratic nonresidue modulo p.

ACKNOWLEDGMENT

The author would like to express his appreciation to the anonymous referee for making valuable suggestions and helpful comments that improved the presentation of this paper.

REFERENCES

1. O. J. Brison. "Complete Fibonacci Sequences in Finite Fields." *The Fibonacci Quarterly* **30.4** (1992):295-304.
2. G. Bruckner. "Fibonacci Sequence Modulo a Prime $p \equiv 3 \pmod 4$." *The Fibonacci Quarterly* **8.3** (1970):217-20.
3. R. T. Bumby. "A Distribution Property for Linear Recurrence of the Second Order." *Proc. Amer. Math. Soc.* **50** (1975):101-06.
4. G. Kowol. "On Strong Dickson Pseudoprimes." *Appl. Algebra Engrg. Comm. Comput.* **3** (1992):129-38.
5. D. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. of Math.* **31** (1930):419-48.
6. R. Lidl & H. Niederreiter. *Introduction to Finite Fields and Their Applications.* Cambridge: Cambridge University Press, 1991.
7. B. M. Phong. "Lucas Primitive Roots." *The Fibonacci Quarterly* **29.1** (1991):66-71.
8. A. Schinzel. "Special Lucas Sequences, Including the Fibonacci Sequence, Modulo a Prime." In *A Tribute to Paul Erdös*, pp. 349-57. Ed. A. Baker et al. Cambridge: Cambridge University Press, 1990.
9. A. P. Shah. "Fibonacci Sequence Modulo m." *The Fibonacci Quarterly* **6** (1968):139-41.
10. D. Shanks. *Solved and Unsolved Problems in Number Theory.* 2nd ed. New York: Chelsea, 1978.
11. L. Somer. "Primes Having an Incomplete System of Residues for a Class of Second-Order Recurrences." In *Applications of Fibonacci Numbers* **2**:113-41. Ed. A. N. Philippou et al. Dordrecht: Kluwer, 1988.
12. W. A. Webb & C. T. Long. "Distribution Modulo p^h of the General Linear Second-Order Recurrence." *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.*(8), **58.2** (1975):92-100.
13. O. Wyler. "On Second Order Recurrences. *Amer. Math. Monthly* **72** (1965):500-06.

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

❖❖❖

PHASED TILINGS AND GENERALIZED FIBONACCI IDENTITIES

Arthur T. Benjamin
Dept. of Mathematics, Harvey Mudd College, Claremont, CA 91711
benjamin@hmc.edu

Jennifer J. Quinn
Dept. of Mathematics, Occidental College, Los Angeles, CA 90041
jquinn@oxy.edu

Francis Edward Su
Dept. of Mathematics, Harvey Mudd College, Claremont, CA 91711
su@math.hmc.edu
(Submitted August 1998-Final Revision May 1999)

1. INTRODUCTION

Fibonacci numbers arise in the solution of many combinatorial problems. They count the number of binary sequences with no consecutive zeros, the number of sequences of 1's and 2's which sum to a given number, and the number of independent sets of a path graph. Similar interpretations exist for Lucas numbers. Using these interpretations, it is possible to provide combinatorial proofs that shed light on many interesting Fibonacci and Lucas identities (see [1], [3]). In this paper we extend the combinatorial approach to understand relationships among generalized Fibonacci numbers.

Given G_0 and G_1, *a generalized Fibonacci sequence* $G_0, G_1, G_2, \ldots$ is defined recursively by $G_n = G_{n-1} + G_{n-2}$ for $n \geq 2$. Two important special cases are the classical Fibonacci sequence F_n ($F_0 = 0$ and $F_1 = 1$) and the Lucas sequence L_n ($L_0 = 2$ and $L_1 = 1$).

These sequences satisfy numerous relationships. Many are documented in Vajda [6], where they are proved by algebraic means. Our goal is to *recount* these identities by combinatorial means. We introduce several combinatorial techniques which allow us to provide new proofs of nearly all the identities in [6] involving generalized Fibonacci numbers. We show that in the framework of *phased tilings*, these identities follow naturally as the tilings are counted, represented, and transformed in clever ways. These techniques are developed in the next several sections. In the final section, we discuss possible extensions.

2. COMBINATORIAL INTERPRETATION

Recall that F_{n+1} counts the number of sequences of 1's and 2's which sum to n. Equivalently, F_{n+1} counts the number of ways to tile a $1 \times n$ rectangle (called an *n-board* consisting of *cells* labeled $1, \ldots, n$) with 1×1 *squares* and 1×2 *dominoes*. For combinatorial convenience, we define $f_n = F_{n+1}$. Then f_n is the number of ways to tile an n-board with squares and dominoes.

When G_0 and G_1 are nonnegative integers, we shall obtain an analogous combinatorial interpretation of the generalized Fibonacci numbers G_n. Define a *phased n-tiling* to be a tiling of an n-board by squares and dominoes in which the last tile is distinguished in a certain way. Specifically, if the last tile is a domino, it can be assigned one of G_0 possible *phases*, and if the last tile is a square, it can be assigned one of G_1 possible phases. For example, when $G_0 = 5$ and $G_1 = 17$, there are $G_3 = 39$ phased tilings of length 3 as follows: There are 5 of the form (square, phased domino); 17 of the form (domino, phased square); and 17 of the form (square, square, phased

square). In general, let $g_0 = G_0$, $g_1 = G_1$, and, for $n \geq 2$, let g_n count the number of phased n-tilings. By conditioning on whether the first tile is a square or domino, we obtain the identity $g_n = g_{n-1} + g_{n-2}$ for $n \geq 2$. Hence, $g_n = G_n$, giving the desired interpretation.

This combinatorial definition can be extended to $n = 1$ and $n = 0$. Clearly G_1 counts the number of phased 1-tilings. It will be convenient to assign the "last" tile of a 0-board one of the G_0 domino phases.

Notice when there exists only one domino phase and only one square phase, we recover our original interpretation of f_n.

Previous interpretations of the Lucas numbers L_n (see [1], [4], [5]) counted the number of ways to tile a "circular" n-board by squares or dominoes. Since $L_0 = 2$ and $L_1 = 1$, a phased n-board tiling can end with a phase one domino, a phase two domino, or a phase one square. In all three cases, the corresponding circular n-board tiling arises by first gluing cells n and 1 together. Tilings that end in a phase two domino are then rotated one cell to obtain a circular tiling with a domino covering cells n and 1.

3. ELEMENTARY IDENTITIES

Before launching into more sophisticated techniques, we demonstrate how our combinatorial interpretation of G_n yields quick proofs of some basic identities. For instance, by conditioning on whether the last tile is a phased domino or a phased square, we immediately obtain, for $n \geq 2$, $G_n = G_0 f_{n-2} + G_1 f_{n-1}$.

More identities are obtained by conditioning on other events. Consider

Identity 1 [Vajda (33)]: $\sum_{k=0}^{n} G_k = G_{n+2} - G_1$.

The right-hand side of this equality counts all phased $(n+2)$-tilings containing at least one domino (there are G_1 phased tilings consisting of all squares). The left-hand side is obtained by conditioning on the position of the first domino. If the first domino covers cells $n-k+1$ and $n-k+2$ $(0 \leq k \leq n)$, then the preceding cells are covered by squares and the remaining cells can be covered G_k ways.

Similarly, there are $G_{2n} - G_0$ phased $2n$-tilings with at least one square. By conditioning on the position of the first square, we obtain

Identity 2 [Vajda (34)]: $\sum_{k=1}^{n} G_{2k-1} = G_{2n} - G_0$.

A phased $(2n+1)$-tiling must contain a first square, which leads to

Identity 3 [Vajda (35)]: $G_1 + \sum_{k=1}^{n} G_{2k} = G_{2n+1}$.

The G_1 term on the left-hand side counts those boards that begin with n dominoes followed by a phased square.

To prove

Identity 4 [Vajda (8)]: $G_{m+n} = f_m G_n + f_{m-1} G_{n-1}$,

we consider whether or not a phased $(m+n)$-tiling can be separated into an (unphased) m-tiling followed by a phased n-tiling. There are $f_m G_n$ tilings breakable at cell m. The unbreakable tilings must contain a domino covering cells m and $m+1$; the remaining board can be covered $f_{m-1}G_{n-1}$ ways.

4. BINOMIAL IDENTITIES

Vajda contains several identities involving generalized Fibonacci numbers and binomial coefficients. All of these are special cases of the following two identities.

Identity 5 [Vajda (46)]: $G_{n+p} = \sum_{i=0}^{p} \binom{p}{i} G_{n-i}$.

Identity 6 [Vajda (66)]: $G_{m+(t+1)p} = \sum_{i=0}^{p} \binom{p}{i} f_t^i f_{t-1}^{p-i} G_{m+i}$.

When $n \geq p$, Identity 5 counts phased $(n+p)$-tilings by conditioning on the number of dominoes that appear among the first p tiles. Given an initial segment of i dominoes and $p-i$ squares, $\binom{p}{i}$ counts the number of ways to select the i positions for the dominoes among the first p tiles. G_{n-i} counts the number of ways the remaining $n-i$ cells can be given a phased tiling.

Identity 6 can be seen as trying to break a phased $(m+(t+1)p)$-tiling into p unphased segments of length t followed by a phased remainder. The first segment consists of the tiles covering cells 1 through j_1, where $j_1 = t$ if the tiling is breakable at cell t and $j_1 = t+1$ otherwise. The next segment consists of the tiles covering cells j_1+1 through j_1+j_2, where $j_2 = t$ if the tiling is breakable at cell j_1+t and $j_2 = t+1$ otherwise. Continuing in this fashion, we decompose our phased tiling into p tiled segments of length t or $t+1$ followed by a phased remainder of length at least m. Since the length $t+1$ segments must end with a domino, the term $\binom{p}{i} f_t^i f_{t-1}^{p-i} G_{m+i}$ counts the number of phased $(m+(t+1)p)$-tilings with exactly i segments of length t.

5. SIMULTANEOUS TILINGS

Identities involving squares of generalized Fibonacci numbers suggest investigating pairs of phased tilings. The right-hand side of

Identity 7 [Vajda (39)]: $\sum_{i=1}^{2n} G_{i-1}G_i = G_{2n}^2 - G_0^2$

counts ordered pairs (A, B) of phased $2n$-tilings, where A or B contains at least one square. To interpret the left-hand side, we define the parameter k_X to be the first cell of the phased tiling X covered by a square. If X is all dominoes, we set k_X equal to infinity. Since, in this case, at least one square exists in (A, B), the minimum of k_A and k_B must be finite and odd. Let $k = \min\{k_A, k_B+1\}$. When k is odd, A and B have dominoes covering cells 1 through $k-1$ and A has a square covering cell k. Hence, the number of phased pairs (A, B) with odd k is $G_{2n-k}G_{2n-k+1}$. When k is even, A has dominoes covering cells 1 through k and B has dominoes covering cells 1 through $k-2$ with a square covering cell $k-1$. Hence, the number of phased pairs (A, B) with even k is also $G_{2n-k}G_{2n-k+1}$. Setting $i = 2n+1-k$ gives the desired identity.

Similarly, the next identity counts ordered pairs of phased $(2n+1)$-tilings that contain an unphased square. Conditioning on the first unphased square yields

Identity 8 [Vajda (41)]: $\sum_{i=2}^{2n+1} G_{i-1}G_i = G_{2n+1}^2 - G_1^2$.

In the same spirit, our next identity conditions on the location of the first domino in a pair of phased tilings.

Identity 9 [Vajda (43)]: $\sum_{i=1}^{n} G_{i-1}G_{i+2} = G_{n+1}^2 - G_1^2$.

The right-hand side counts the number of pairs (A, B) of phased $(n+1)$-tilings, where A or B contains at least one domino. Here we define the parameter ℓ_X to be the first cell of the phased tiling X covered by a domino. If X is all squares, we set ℓ_X equal to infinity. Let $\ell = \min\{\ell_A, \ell_B\}$. The number of phased $(n+1)$-tiling pairs (A, B), where the ℓ^{th} cell of A is covered by a domino is $G_{n-\ell}G_{n-\ell+2}$ and the number of such pairs where the ℓ^{th} cell of A is covered by a square is $G_{n-\ell+1}G_{n-\ell}$. This implies

$$\sum_{\ell=1}^{n} G_{n-\ell}(G_{n-\ell+2} + G_{n-\ell+1}) = G_{n+1}^2 - G_1^2$$

Substituting $G_{n-\ell+3}$ for $G_{n-\ell+2} + G_{n-\ell+1}$ and letting $i = n - \ell + 1$ yields the desired identity.

6. A TRANSFER PROCEDURE

The identities proved in this section all take advantage of the same technique. Before proceeding, we introduce helpful notation. For $m \geq 0$, define $\mathcal{G}_m$ to be the set of all phased m-tilings with G_0 domino phases and G_1 square phases. An element $A \in \mathcal{G}_m$ created from a sequence of e_1 dominoes, e_2 squares, e_3 dominoes, ..., and ending with a phased tile can be expressed uniquely as $A = d^{e_1}s^{e_2}d^{e_3}s^{e_4}\cdots d^{e_{t-1}}s^{e_t}p$, where p represents the phase of the last tile. All exponents are positive except that e_1 or e_t may be 0, and $2e_1 + e_2 + 2e_3 + e_4 + \cdots + 2e_{t-1} + e_t = m$. When $e_t = 0$, the last tile is a domino and $p \in \{1, \ldots, G_0\}$; when $e_t \geq 1$, the last tile is a square and $p \in \{1, \ldots, G_1\}$. Likewise, for $n \geq 0$, define $\mathcal{H}_n$ to be the set of all phased n-tilings with H_0 domino phases and H_1 square phases. Notice that the sizes of $\mathcal{G}_m$ and $\mathcal{H}_n$ are G_m and H_n, respectively.

We introduce a transfer procedure T to map an ordered pair $(A, B) \in \mathcal{G}_m \times \mathcal{H}_n$ to an ordered pair $(A', B') \in \mathcal{G}_{m-1} \times \mathcal{H}_{n+1}$, where $1 \leq m \leq n$. T has the effect of shrinking the smaller tiling and growing the larger tiling by one unit. For such a pair (A, B), define $k = \min\{k_A, k_B\}$, the first cell in A or B that is covered by a square. If the k^{th} cell of A is covered by a square and $1 \leq k \leq m-1$, then we transfer that square from A to the k^{th} cell of B. Formally, before the transfer, we have $A = d^{(k-1)/2}sa$, $B = d^{(k-1)/2}b$, where $a \in \mathcal{G}_{m-k}$, $b \in \mathcal{H}_{n-k+1}$. The transfer yields $A' = d^{(k-1)/2}a$, $B' = d^{(k-1)/2}sb$. If the k^{th} cell of A is covered by a domino and $1 \leq k \leq m-2$, then we exchange that domino with the square in the k^{th} cell of B. Formally, before the exchange, $A = d^{(k+1)/2}a$, $B = d^{(k-1)/2}sb$, where $a \in \mathcal{G}_{m-k-1}$, $b \in \mathcal{H}_{n-k}$. The exchange yields $A' = d^{(k-1)/2}sa$, $B' = d^{(k+1)/2}b$. We abbreviate this transformation by $T(A, B) = (A', B')$. Notice that our rules do not allow for a phased tile to be transferred or exchanged.

Lemma 1: For $1 \leq m \leq n$, T establishes an *almost* one-to-one correspondence between $\mathcal{G}_m \times \mathcal{H}_n$ and $\mathcal{G}_{m-1} \times \mathcal{H}_{n+1}$. The difference of their sizes satisfies

$$G_mH_n - G_{m-1}H_{n+1} = (-1)^m[G_0H_{n-m+2} - G_1H_{n-m+1}].$$

Proof: Notice that when T is defined, $T(A, B)$ has the same k value as (A, B), which makes T easy to reverse. It remains to enumerate $(A, B) \in \mathcal{G}_m \times \mathcal{H}_n$ for which T is undefined and $(A', B') \in \mathcal{G}_{m-1} \times \mathcal{H}_{n+1}$ that do not appear in the image of T.

When m is odd, T is undefined whenever $k = m$. Here $A = d^{(m-1)/2}a$, $B = d^{(m-1)/2}b$, where $a \in \mathcal{G}_1$, $b \in \mathcal{H}_{n-m+1}$. Hence, the domain of T contains $G_mH_n - G_1H_{n-m+1}$ elements. The elements of $\mathcal{G}_{m-1} \times \mathcal{H}_{n+1}$ that do not appear in the image of T have $k \geq m$ and are therefore of the form $A' = d^{(m-1)/2}p$, $B' = d^{(m-1)/2}b'$, where $p \in \{1, \ldots, G_0\}$, $b' \in \mathcal{H}_{n-m+2}$. Hence, the image of T consists of $G_{m-1}H_{n+1} - G_0H_{n-m+2}$ elements. Since T is one-to-one we have, when m is odd,

$$G_mH_n - G_1H_{n-m+1} = G_{m-1}H_{n+1} - G_0H_{n-m+2}.$$

When m is even, T is undefined whenever $k \geq m$ and sometimes undefined when $k = m-1$. Specifically, T is undefined when $A = d^{m/2}p$, $B = d^{(m-2)/2}b$, where $p \in \{1, \ldots, G_0\}$, $b \in \mathcal{H}_{n-m+2}$. Hence, the domain of T contains $G_mH_n - G_0H_{n-m+2}$ elements. The elements of $\mathcal{G}_{m-1} \times \mathcal{H}_{n+1}$ that do not appear in the image are of the form $A' = d^{(m-2)/2}a'$, $B' = d^{m/2}b'$, where $a' \in \mathcal{G}_1$, $b' \in \mathcal{H}_{n-m+1}$. Hence, the image of T consists of $G_{m-1}H_{n+1} - G_1H_{n-m+1}$ elements. Thus, when m is even, we have

$$G_mH_n - G_0H_{n-m+2} = G_{m-1}H_{n+1} - G_1H_{n-m+1}. \quad \square$$

We specialize Lemma 1 by setting $m = n$ and choosing the same initial conditions for $\mathcal{G}_n$ and $\mathcal{H}_n$ to obtain

Identity 10 [Vajda (28)]: $G_{n+1}G_{n-1} - G_n^2 = (-1)^n(G_1^2 - G_0G_2)$.

Alternately, setting $G_m = F_m$ and evaluating lemma 1 at $m+1$, we obtain

Identity 11 [Vajda (9)]: $H_{n-m} = (-1)^m(F_{m+1}H_n - F_mH_{n+1})$ for $0 \leq m \leq n$.

A slightly different transfer process is used to prove

Identity 12 [Vajda (10a)]: $G_{n+m} + (-1)^mG_{n-m} = L_mG_n$ for $0 \leq m \leq n$.

We construct an almost one-to-one correspondence from $\mathcal{L}_m \times \mathcal{G}_n$ to $\mathcal{G}_{m+n}$, where $\mathcal{L}_m$ denotes the set of Lucas tilings of length m. Let $(A, B) \in \mathcal{L}_m \times \mathcal{G}_n$. If A ends in a (phase 1) square or a phase 1 domino, then we simply append A to the front of B to create an $(m+n)$-tiling that is breakable at m. Otherwise, A ends in a phase 2 domino. In this case, before appending A to the front of B, we transfer a unit from B to A by a similar process. (If the first square occurs in B, then transfer it into the corresponding cell of A. Otherwise, the first square of A is exchanged with the corresponding domino in B.) This creates a tiling of $\mathcal{G}_{m+n}$ that is unbreakable at m. When m is even, the transfer is undefined for the G_{n-m} elements of $\mathcal{L}_m \times \mathcal{G}_n$, where A contains only dominoes, ending with a phase 2 domino, and B begins with $m/2$ dominoes. Otherwise, the transfer is one-to-one and onto $\mathcal{G}_{m+n}$. When m is odd, the transfer is always defined but misses the G_{n-m} elements of $\mathcal{G}_{m+n}$ that begin with m dominoes. Identity 12 follows.

A similar argument establishes

Identity 13 [Vajda (10b)]: $G_{n+m} - (-1)^mG_{n-m} = F_m(G_{n-1} + G_{n+1})$ for $0 \leq m \leq n$.

The transfer process T can be refined to allow us to shrink and grow pairs of phased tilings by more than one unit. Specifically, we construct an almost one-to-one correspondence between $\mathcal{G}_m \times \mathcal{H}_n$ and $\mathcal{G}_{m-h} \times \mathcal{H}_{n+h}$, where $1 \leq h \leq m-1 < n$. Let $\mathcal{F}_n$ denote the set of (unphased) n-tilings.

So $|\mathcal{F}_n| = f_n$. Given $(A, B) \in \mathcal{G}_m \times \mathcal{H}_n$, define a transfer process T_h as follows: if A is breakable at cell h, i.e., $A = a_1a_2$, where $a_1 \in \mathcal{F}_h$ and $a_2 \in \mathcal{G}_{m-h}$, then we append segment a_1 to the beginning of B. That is to say, $T_h(A, B) = (A', B')$, where $A' = a_2$ and $B' = a_1B$. If A is unbreakable at cell h, i.e., $A = a_1da_2$, where $a_1 \in \mathcal{F}_{h-1}$ and $a_2 = \mathcal{G}_{m-h-1}$, then let $(A'', B'') = T(da_2, B)$ and $(A', B') = (A'', a_1B'')$. Notice that B'', when defined, will necessarily begin with a domino and, therefore, B' will be unbreakable at h.

Discrepancies in T_h mapping $\mathcal{G}_m \times \mathcal{H}_n$ to $\mathcal{G}_{m-h} \times \mathcal{H}_{n+h}$, are proportional (by a factor of f_{h-1}) to the discrepancies in T mapping $\mathcal{G}_{m-h+1} \times \mathcal{H}_n$ to $\mathcal{G}_{m-h} \times \mathcal{H}_{n+1}$. Hence, for $1 \le h \le m-1$, Lemma 1 implies

$$G_mH_n - G_{m-h}H_{n+h} = (-1)^{m-h+1} f_{h-1}(G_0H_{n-m+h+1} - G_1H_{n-m+h}). \tag{1}$$

Notice that $f_{h-1}H_{n-m+h+1}$ counts the number of phased $(n-m+2h)$-tilings that are breakable at $h-1$. Hence, $f_{h-1}H_{n-m+h+1} = H_{n-m+2h} - f_{h-2}H_{n-m+h}$. Similarly, $f_{h-1}G_1 = G_h - f_{h-2}G_0$. So equation (1) can be rewritten as

$$G_mH_n - G_{m-h}H_{n+h} = (-1)^{m-h+1}(G_0H_{n-m+2h} - G_hH_{n-m+h}).$$

Reindexing, this is equivalent to

Identity 14 [Vajda (18)]: $G_{n+h}H_{n+k} - G_nH_{n+h+k} = (-1)^n(G_hH_k - G_0H_{h+k})$.

This identity is applied, directly or indirectly, by Vajda to obtain identities (19a) through (32).

7. BINARY SEQUENCES

There are identities involving generalized Fibonacci numbers and powers of 2. This leads us to investigate the relationship between binary sequences and Fibonacci tilings.

A binary sequence $x = x_1x_2\ldots x_n$ can be viewed as a set of instructions for creating a Fibonacci tiling of length less than or equal to n. Reading x from left to right, we interpret 1's and 01's as squares and dominoes, respectively. The construction halts on encountering a 00 or the end of the sequence. For example, 111010110101 represents the 12-tiling $s^3d^2sd^2$, 1110101110 represents the 9-tiling $s^3d^2s^2$, and 0111001011 represents the 4-tiling ds^2. Binary sequences that begin with 00 denote the 0-tiling.

Given n, tilings of length n and $n-1$ are represented uniquely by binary sequences of length n that end with a 1 or 0, respectively. For $k \le n-2$, a k-tiling is represented by 2^{n-k-2} binary sequences of length n since the first $k+2$ bits are determined by the k-tiling followed by 00; the remaining $n-(k+2)$ bits may be chosen freely. This yields the following identity:

$$f_n + f_{n-1} + \sum_{k=0}^{n-2} f_k 2^{n-k-2} = 2^n. \tag{2}$$

By dividing by 2^n, reindexing, and employing $f_{n+1} = f_n + f_{n-1}$, we obtain

Identity 15 [Vajda (37a)]: $\displaystyle\sum_{k=2}^{n} \frac{f_{k-2}}{2^k} = 1 - \frac{f_{n+1}}{2^n}$.

The same strategy can be applied to phased tilings. Here, for convenience, we assume the phase is determined by the first tile (rather than the last). The phased identity corresponding to equation (2) is

$$G_{n+1} + G_n + \sum_{k=0}^{n-1} G_k 2^{n-k-1} = 2^n (G_0 + G_1). \tag{3}$$

The right-hand side counts the number of ways to select a length n binary sequence x and a phase p. From this, we construct a length $n+1$ binary sequence. If p is a domino phase, construct the sequence $0x$; if p is a square phase, construct the sequence $1x$. Interpret this new $n+1$-sequence as a Fibonacci tiling in the manner discussed previously, and assign the tiling the phase p. By construction, the phase is compatible with the first tile. (Recall that empty tilings are assigned a domino phase.) A phased tiling of length $n+1$ or n has a unique (x, p) representation. For $0 \le k \le n-1$, a phased k-tiling has 2^{n-k-1} representations. This establishes equation (3). Dividing by 2^n gives

Identity 16 [Vajda (37)]: $\displaystyle\sum_{k=0}^{n-1} \frac{G_k}{2^{k+1}} = (G_0 + G_1) - \frac{G_{n+1} + G_n}{2^n}.$

8. DISCUSSION

The techniques presented in this paper are simple but powerful—counting phased tilings enables us to give visual interpretations to expressions involving generalized Fibonacci numbers. This approach facilitates a clearer understanding of existing identities, and can be extended in a number of ways.

For instance, by allowing tiles of length 3 or longer, we can give combinatorial interpretation to higher-order recurrences; however, the initial conditions do not work out so neatly, since the number of phases that the last tile admits do not correspond with the initial conditions of the recurrence.

Another possibility is to allow *every* square and domino to possess a number of phases, depending on its location. This leads to recurrences of the form $x_n = a_n x_{n-1} + b_n x_{n-2}$. The special case where $b_n = 1$ for all n provides a tiling interpretation of the numerators and denominators of simple finite continued fractions and is treated in [2].

ACKNOWLEDGMENT

The authors gratefully acknowledge the anonymous referee for many valuable suggestions.

REFERENCES

1. A. T. Benjamin & J. J. Quinn. "Recounting Fibonacci and Lucas Identities." *College Math. J.* **30.5** (1999):359-66.
2. A. T. Benjamin, J. J. Quinn, & F. E. Su. "Counting on Continued Fractions." *Math. Magazine* **73.2** (2000):98-104.
3. R. C. Brigham, R. M. Caron, P. Z. Chinn, & R. P. Grimaldi. "A Tiling Scheme for the Fibonacci Numbers." *J. Recreational Math.* **28.1** (1996-1997):10-16.
4. L. Comtet. *Advanced Combinatorics: The Art of Finite and Infinite Expansions.* Dordrecht: D. Reidel, 1974.
5. H. Prodinger & R. F. Tichy. "Fibonacci Numbers of Graphs." *The Fibonacci Quarterly* **20.1** (1982):16-21.
6. S. Vajda. *Fibonacci and Lucas Numbers, and the Golden Section.* New York: Wiley, 1989.

AMS Classification Numbers: 05A19, 11B39

❖❖❖

SUSTAINING MEMBERS

*H.L. Alder
G.L. Alexanderson
P. G. Anderson
S. Ando
R. Andre-Jeannin
D.C. Arney
J.G. Bergart
G. Bergum
*M. Bicknell-Johnson
M.W. Bowron
P.S. Bruckman
G.D. Chakerian
C. Chouteau
C.K. Cook
C. Cooper
M.J. DeBruin
M.J. DeLeon
J. De Kerf
E. Deutsch
L.A.G. Dresel
U. Dudley
M. Elia
L.G. Ericksen, Jr.
D.R. Farmer
D.C. Fielder
C.T. Flynn
E. Frost
N. Gauthier
*H.W. Gould
P. Hagis, Jr.
H. Harborth
J. Herrera
*A.P. Hillman
*A.F. Horadam
Y. Horibe
F.T. Howard
R.J. Howell
J.P. Jones
R.E. Kennedy
C.H. Kimberling
R. Knott
D.A. Krigens
Y.H.H. Kwong
J.C. Lagarias
J. Lahr
*C.T. Long
G. Lord
W.L. McDaniel
F.U. Mendizabal
M.G. Monzingo
S.A. Obaid
A. Prince
B.M. Romanic
S. Sato
J.A. Schumaker
H.J Seiffert
A.G. Shannon
L.W. Shapiro
J.R. Siler
L. Somer
P. Spears
W.R. Spickerman
P.K. Stockmeyer
D.R. Stone
I. Strazdins
J. Suck
M.N.S. Swamy
*D. Thoro
J.C. Turner
C. Vanden Eynden
T.P. Vaughan
J.N. Vitale
M.J. Wallace
J.E. Walton
W.A. Webb
R.E. Whitney
B.E. Williams

*Charter Members

INSTITUTIONAL MEMBERS

BIBLIOTECA DEL SEMINARIO MATHEMATICO
Padova, Italy

CALIFORNIA STATE UNIVERSITY
SACRAMENTO
Sacramento, California

CHALMERS UNIVERSITY OF TECHNOLOGY
AND UNIVERSITY OF GOTEBORG
Goteborg, Sweden

ETH-BIBLIOTHEK
Zurich, Switzerland

GONZAGA UNIVERSITY
Spokane, Washington

HOWELL ENGINEERING COMPANY
Yucaipa, California

KLEPCO, INC.
Sparks, Nevada

KOBENHAVNS UNIVERSITY
Matematisk Institut
Copenhagen, Denmark

MISSOURI SOUTHERN STATE COLLEGE
Joplin, Missouri

SAN JOSE STATE UNIVERSITY
San Jose, California

SANTA CLARA UNIVERSITY
Santa Clara, California

UNIVERSITY OF NEW ENGLAND
Armidale, N.S.W. Australia

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. $18.00

Fibonacci and Lucas Numbers by Verner E. Hoggatt, Jr. FA, 1972. $23.00

A Primer for the Fibonacci Numbers. Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1972. $32.00

Fibonacci's Problem Book, Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1974. $19.00

The Theory of Simply Periodic Numerical Functions by Edouard Lucas. Translated from the French by Sidney Kravitz. Edited by Douglas Lind. FA, 1969. $6.00

Linear Recursion and Fibonacci Sequences by Brother Alfred Brousseau. FA, 1971. $6.00

Fibonacci and Related Number Theoretic Tables. Edited by Brother Alfred Brousseau. FA, 1972. $30.00

Number Theory Tables. Edited by Brother Alfred Brousseau. FA, 1973. $39.00

Tables of Fibonacci Entry Points, Part One. Edited and annotated by Brother Alfred Brousseau. FA, 1965. $14.00

Tables of Fibonacci Entry Points, Part Two. Edited and annotated by Brother Alfred Brousseau. FA, 1965. $14.00

A Collection of Manuscripts Related to the Fibonacci Sequence—18th Anniversary Volume. Edited by Verner E. Hoggatt, Jr. and Marjorie Bicknell-Johnson. FA, 1980. $38.00

Applications of Fibonacci Numbers, Volumes 1-7. Edited by G.E. Bergum, A.F. Horadam and A.N. Philippou. Contact Kluwer Academic Publishers for price.

Applications of Fibonacci Numbers, Volume 8. Edited by F.T. Howard. Contact Kluwer Academic Publishers for price.

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. $37.00

Fibonacci Entry Points and Periods for Primes 100,003 through 415,993 by Daniel C. Fielder and Paul S. Bruckman. $20.00

Handling charges will be $4.00 for the first book and $1.00 for each additional book in the United States and Canada. For Foreign orders, the handling charge will be $8.00 for the first book and $3.00 for each additional book.

Please write to the Fibonacci Association, P.O. Box 320, Aurora, S.D. 57002-0320, U.S.A., for more information.