The Fibonacci Quarterly

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

TABLE OF CONTENTS

VOLUME 36 JUNE-JULY 1998 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.**

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

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

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

The Fibonacci Quarterly

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

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

THE FIBONACCI TRIANGLE MODULO p

Brad Wilson
2030 State Street #5, Santa Barbara, CA 93105
(Submitted July 1996-Final Revision August 1997)

1. INTRODUCTION

Let $F_n! = F_nF_{n-1}\ldots F_2F_1$.

Definition: The Fibonacci coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_{\mathfrak{F}}$ is defined to be

$$\begin{bmatrix} n \\ k \end{bmatrix}_{\mathfrak{F}} = \frac{F_n!}{F_k!F_{n-k}!} = \frac{F_nF_{n-1}\ldots F_1}{(F_kF_{k-1}\ldots F_1)(F_{n-k}F_{n-k-1}\ldots F_1)}.$$

An important property of the Fibonacci coefficients from [4] is

$$\begin{bmatrix} k \\ \ell \end{bmatrix}_{\mathfrak{F}} = F_{\ell+1}\begin{bmatrix} k-1 \\ \ell \end{bmatrix}_{\mathfrak{F}} + F_{k-\ell-1}\begin{bmatrix} k-1 \\ \ell-1 \end{bmatrix}_{\mathfrak{F}}. \tag{1}$$

From the Fibonacci coefficients we form the Fibonacci triangle in much the same way as Pascal's triangle is formed from the binomial coefficients; namely, the Fibonacci triangle is formed by letting the k^{th} element of the n^{th} row be $\begin{bmatrix} n \\ k \end{bmatrix}_{\mathfrak{F}}$.

1
1 1
1 1 1
1 2 2 1
1 3 6 3 1
1 5 15 15 5 1

FIGURE 1. Rows 0 to 5 of the Fibonacci Triangle

The parity of the binomial coefficients and the iterative structure of Pascal's triangle have been the subject of many papers (see, e.g., [2], [3], [13]). More recently, the Fibonacci coefficients and the iterative structure of the Fibonacci triangle modulo 2 and 3 has been examined in [5], [11], and [12]. In this paper we extend the results of [11] and [12] from the Fibonacci coefficients and triangle modulo 2 and 3 to modulus p for p an odd prime.

For an odd prime p other than 5 and $i \geq 0$, define $r_i \in \mathbb{N}$ as the smallest number such that $p^i | F_{r_i}$. In particular, $r_0 = 1$ and r_1 is what is commonly called the rank of apparition of p. We will denote $\wp = \{r_0, r_1, \ldots\}$. It is well known that $r_i | r_{i+1}$ for all $i \in \mathbb{N}$, so any $n \in \mathbb{N}$ can be written uniquely as $n = n_k r_k + n_{k-1}r_{k-1} + \cdots + n_1 r_1 + n_0$ for $0 \leq n_i < \frac{r_{i+1}}{r_i}$. We call this the base $\wp$ representation of $n \in \mathbb{N}$.

Our main results are

Theorem 1: Let $r = \max_{i \geq 0} \frac{r_{i+1}}{r_i}$. The number of entries in the n^{th} row of the Fibonacci triangle not divisible by p is $2^{s_1}3^{s_2}4^{s_3}\ldots r^{s_{r-1}}$, where s_i is the number of i's in the base $\wp$ expansion of n.

Theorem 2: Let $p \neq 2, 5$ be a prime. There is the following connection between the Fibonacci and binomial coefficients modulo p:

$$\begin{bmatrix} nr_1 \\ kr_1 \end{bmatrix}_{\mathfrak{F}} \equiv \binom{n}{k} F_{r_1+1}^{k(n-k)r_1} \pmod{p}.$$

In particular, the triangle Δ_{F_p} formed by having $\left[\begin{smallmatrix} nr_1 \\ kr_1 \end{smallmatrix}\right]_{\mathfrak{F}} \pmod{p}$ as the k^{th} entry of the n^{th} row is Pascal's triangle modulo p if and only if r_1 is even.

Theorem 3: For $p \neq 2, 5$ a prime, we have

$$\begin{bmatrix} nr_1 + j \\ mr_1 + i \end{bmatrix}_{\mathfrak{F}} \equiv \binom{n}{m} \begin{bmatrix} j \\ i \end{bmatrix}_{\mathfrak{F}} F_{r_1+1}^{r_1 m(n-m)+i(n-m)+m(j-i)} \pmod{p}.$$

2. PRELIMINARY FACTS

Of fundamental importance in our investigation are the following two well-known facts (see [9]): First, if (a, b) denotes the greatest common divisor of two natural numbers, then

$$(F_n, F_m) = F_{(m,n)}. \tag{2}$$

Second,

$$F_{n+m} = F_n F_{m-1} + F_{n+1} F_m. \tag{3}$$

A sequence $\{A_j\}$ is said to be regularly divisible by $d \in \mathbb{N}$ if there exists $r(d) \in \mathbb{N}$ such that $d \mid A_j$ if and only if $r(d) \mid j$. A sequence is regularly divisible if it is regularly divisible for all $d \in \mathbb{N}$ (see [5]). From (2), we see that the sequence $\{F_n\}_{n=1}^{\infty}$ is regularly divisible. To simplify notation, for p our fixed prime and for $i \geq 0$, we let $r_i \in \mathbb{N}$ be the smallest number such that $p^i \mid F_{r_i}$. Notice that $r_0 = 1$ and r_1 is what is generally called the rank of apparition of p. Let $\wp = \{r_0, r_1 \ldots\}$. Since the Fibonacci sequence is regularly divisible $r_i \mid r_{i+1}$ so each $n \in \mathbb{N}$ can be written uniquely as $n = n_t r_t + n_{t-1} r_{t-1} + \cdots + n_1 r_1 + n_0$ with $0 \leq n_i < \frac{r_{i+1}}{r_i}$. We call this the base $\wp$ representation of n and denote it by $n = (n_t n_{t-1} \ldots n_1 n_0)_{\wp}$ (see [6]).

It is well known from [7] that for $i \geq 1$ we have

$$\frac{r_{i+1}}{r_i} = \begin{cases} 1 \\ \text{or} \\ p. \end{cases} \tag{4}$$

The following theorem was first shown in [5] in a different form. The introduction of the base $\wp$ allows us to state the theorem more succinctly. The theorem was given in this form in [10]. The proof is reproduced here with the permission of the first author of [10].

Kummer's Theorem for Generalized Binomial Coefficients: Let $\mathcal{A} = \{A_j\}_{j=1}^{\infty}$ be a sequence of positive integers. If $\mathcal{A}$ is regularly divisible by the powers of p, then the highest power of p that divides

$$\begin{bmatrix} m+n \\ m \end{bmatrix}_{\mathcal{A}} = \frac{A_{m+n} A_{m+n-1} \cdots A_{n+1}}{A_m A_{m-1} \cdots A_2 A_1}$$

is the number of carries that occur when the integers n and m are added in base $\wp$, where $\wp = \{r_j\}_{j=0}^{\infty}$ for r_j defined by $p^j \mid A_{r_j}$, $p^j \nmid A_r$ for $0 < r < r_j$.

Proof: By definition of r_i, A_{r_i} is the first element in $\mathcal{A}$ divisible by p^i. By regular divisibility of the sequence $\{A_j\}_{j=1}^{\infty}$, we see that $p^i \mid A_k$ if and only if $r_i \mid k$. This means the number of A_k, $k \leq n$ that are multiples of p^i is

$$\left\lfloor \frac{n}{r_i} \right\rfloor = \left\lfloor \frac{n_t r_t + \cdots + n_1 r_1 + n_0}{r_i} \right\rfloor = n_t \frac{r_t}{r_i} + \cdots + n_{i+1} \frac{r_{i+1}}{r_i} + n_i .$$

Now suppose, in base $\wp$, we have $m = m_t r_t + m_{t-1} r_{t-1} + \cdots + m_1 r_1 + m_0$ and $n = n_t r_t + n_{t-1} r_{t-1} + \cdots + n_1 r_1 + n_0$, where we allow some of the initial digits to be 0 so we may assume m and n are written with the same number of digits in base $\wp$. Counting the multiples of p^i in $\{A_1, A_2, \ldots, A_{m+n}\}$, $\{A_1, A_2, \ldots, A_m\}$, and $\{A_1, A_2, \ldots, A_n\}$, we see a carry at the i^{th} place,

$$(m_{i-1} r_{i-1} + \cdots + m_1 r_1 + m_0) + (n_{i-1} r_{i-1} + \cdots + n_1 r_1 + n_0) \geq r_i$$

occurs if and only if the number of multiples of p^i in $\{A_1, A_2, \ldots, A_{m+n}\}$ is one greater than the number of multiples of p^i in $\{A_1, A_2, \ldots, A_m\}$ plus the number of multiples of p^i in $\{A_1, A_2, \ldots, A_n\}$. Therefore, the number of carries is the highest power of p that divides $\left[{m+n \atop m} \right]_{\mathscr{A}}$. □

In particular, the theorem applies to the Fibonacci sequence: $\{\mathscr{A}_j\}_{j=1}^{\infty} = \{F_j\}_{j=1}^{\infty}$.

Corollary (Knuth and Wilf) [5]: The highest power of p that divides $\left[{m+n \atop n} \right]_{\mathscr{F}}$ is the number of carries that occur when the integers n and m are added in base $\wp$, where $\wp = \{r_j\}_{j=0}^{\infty}$ for r_j defined by $p^j \mid F_{r_j}$, $p^j \nmid F_r$ for $0 < r < r_j$.

3. CONGRUENCES FOR FIBONACCI NUMBERS AND COEFFICIENTS

In this section we give a series of lemmas about congruences of Fibonacci numbers and coefficients.

Lemma 1: For $i \geq 1$, $F_{nr_i+1} \equiv F_{nr_i-1} \equiv F_{r_i+1}^n \pmod{p^i}$.

Proof: Since $p^i \mid F_{nr_i}$, we have $F_{nr_i+1} = F_{nr_i} + F_{nr_i-1} \equiv F_{nr_i-1} \pmod{p^i}$, so we will switch freely between F_{nr_i+1} and F_{nr_i-1} modulo p^i throughout the rest of the article. Since $p^i \mid F_{r_i}$, $F_{r_i+1}^1 = F_{r_i} + F_{r_i-1} \equiv F_{1r_i-1} \pmod{p^i}$, so the lemma is true for $n = 1$. Assume $F_{kr_i-1} \equiv F_{r_i+1}^k \pmod{p^i}$. Using (3) with $n = kr_i$, $m = r_i + 1$ gives

$$F_{(k+1)r_i-1} \equiv F_{(k+1)r_i+1} \equiv F_{kr_i} F_{r_i} + F_{kr_i+1} F_{r_i+1} \equiv F_{kr_i+1} F_{r_i+1} \equiv F_{r_i+1}^{k+1} \pmod{p^i}. \quad \square$$

Lemma 2: For $i \geq 1$, $F_{nr_i} \equiv F_{r_i}(nF_{r_i+1}^{n-1}) \pmod{p^{2i}}$.

Proof: This is clearly true for $n = 1$. Now assume $F_{kr_i} \equiv F_{r_i}(kF_{r_i+1}^{k-1}) \pmod{p^{2i}}$. Then, using (3) with $n = kr_i - 1$, $m = r_i + 1$ gives

$$F_{(k+1)r_i} = F_{kr_i-1} F_{r_i} + F_{kr_i} F_{r_i+1} \equiv F_{r_i}(F_{kr_i-1} + kF_{r_i+1}^{k-1} F_{r_i+1}) \pmod{p^{2i}}. \tag{5}$$

Since Lemma 1 says $F_{kr_i-1} \equiv F_{r_i+1}^k \pmod{p^i}$, we get

$$F_{kr_i-1} + kF_{r_i+1}^{k-1} F_{r_i+1} \equiv F_{r_i+1}^k + kF_{r_i+1}^k \equiv (k+1)F_{r_i+1}^k \pmod{p^i}.$$

Since $p^i \mid F_{r_i}$, this congruence gives

$$F_{r_i}(F_{kr_i-1} + kF_{r_i+1}^{k-1} F_{r_i+1}) \equiv F_{r_i}(k+1)F_{r_i+1}^k \pmod{p^{2i}}.$$

This congruence together with (5) gives $F_{(k+1)r_i} \equiv F_{r_i}(k+1)F_{r_i+1}^k \pmod{p^{2i}}$. □

Lemma 3: For $0 \le j, \ell$ and $0 \le m \le r_1 - 1$, we have $F_{\ell r_1+m}F_{jr_1+1} \equiv F_{\ell r_1+1}F_{jr_1+m} \pmod{p}$.

Proof: For $m = 0$, both sides are congruent to 0 modulo p since $p|F_{\ell r_1}$ and $p|F_{jr_1}$. For $m = 1$, both sides are identical. Assume that $F_{\ell r_1+m}F_{jr_1+1} \equiv F_{\ell r_1+1}F_{jr_1+m} \pmod{p}$ for all $m < k \le r_1 - 1$ for some k. Using our induction hypothesis, $F_{jr_1+k} = F_{jr_1+(k-1)} + F_{jr_1+(k-2)}$, and $F_{\ell r_1+k} = F_{\ell r_1+(k-1)} + F_{\ell r_1+(k-2)}$, we get

$$\begin{aligned} F_{\ell r_1+k}F_{jr_1+1} &= F_{\ell r_1+(k-1)}F_{jr_1+1} + F_{\ell r_1+(k-2)}F_{jr_1+1} \\ &\equiv F_{\ell r_1+1}F_{jr_1+(k-1)} + F_{\ell r_1+1}F_{jr_1+(k-2)} = F_{\ell r_1+1}F_{jr_1+k} \pmod{p}. \ \square \end{aligned}$$

Note that alternate forms of Lemma 3 are

$$\frac{F_{\ell r_1+m}}{F_{\ell r_1+1}} \equiv \frac{F_{jr_1+m}}{F_{jr_1+1}} \pmod{p},$$

which will be used below in Lemma 6 and, for $m \neq 0$,

$$\frac{F_{\ell r_1+m}}{F_{jr_1+m}} \equiv \frac{F_{\ell r_1+1}}{F_{jr_1+1}} \pmod{p},$$

which we will use in Theorem 2 below.

Lemma 4: For $0 \le j, \ell$ we have

$$\frac{F_{\ell r_1+1}}{F_1} \equiv \frac{F_{(\ell+j)r_1+1}}{F_{jr_1+1}} \pmod{p}.$$

Proof: By (3) with $n = \ell r_1$, $m = jr_1 + 1$, we have

$$F_{(\ell+j)r_1+1} = F_{\ell r_1}F_{jr_1} + F_{\ell r_1+1}F_{jr_1+1} \equiv F_{\ell r_1+1}F_{jr_1+1} \pmod{p}.$$

Since F_{jr_1+1} is invertible modulo p, we may divide to put this in the form of the statement of the lemma. $\square$

Lemma 5: For $p \neq 2, 5$,

$$F_{r_1-1} \equiv \begin{cases} 1 \pmod{p} & \text{if } r_1 \equiv 2 \pmod{4}, \\ -1 \pmod{p} & \text{if } r_1 \equiv 0 \pmod{4}, \\ \text{an element of order 4} \pmod{p} & \text{if } r_1 \text{ is odd.} \end{cases}$$

Proof: From (3) with $n = a - 1$, $m = a$, we get $F_a^2 + F_{a-1}^2 = F_{2a-1}$. From (3) with $n = a$, $m = a + 1$, we get $F_a^2 + F_{a+1}^2 = F_{2a+1}$. If $r_1 = 2a$, then $F_{2a+1} = F_{2a} + F_{2a-1} \equiv F_{2a-1} \pmod{p}$, so

$$F_a^2 + F_{a-1}^2 = F_{2a-1} \equiv F_{2a+1} = F_a^2 + F_{a+1}^2 = 2F_a^2 + F_{a-1}^2 + 2F_aF_{a-1} \pmod{p},$$

where the last equality is found by expanding $F_{a+1}^2 = (F_a + F_{a-1})^2$. This means $0 \equiv F_a^2 + 2F_aF_{a-1} \pmod{p}$. Since $F_a \not\equiv 0 \pmod{p}$, we can factor it out to get $0 \equiv F_a + 2F_{a-1} \pmod{p}$ or, stated differently, $F_a \equiv -2F_{a-1} \pmod{p}$. Then $F_{a+1} = F_a + F_{a-1} \equiv -F_{a-1} \pmod{p}$. If $F_{a+k} \equiv (-1)^k F_{a-k} \pmod{p}$ for all $0 \le k < \ell \le a - 1$, then

$$F_{a+\ell} = F_{a+\ell-1} + F_{a+\ell-2} \equiv (-1)^{\ell-1}F_{a-\ell+1} + (-1)^{\ell-2}F_{a-\ell+2}$$
$$= (-1)^{\ell}(F_{a-(\ell-2)} - F_{a-(\ell-1)}) = (-1)^{\ell}F_{a-\ell} \pmod{p},$$

so

$$F_{r_1-1} = F_{a+(a-1)} \equiv (-1)^{a-1}F_{a-(a-1)} = (-1)^{a-1} \pmod{p}.$$

This means that if $r_1 \equiv 2 \pmod 4$, we have a odd, so $F_{r_1-1} \equiv 1 \pmod{p}$. If $r_1 \equiv 0 \pmod 4$, we have a even, so $F_{r_1-1} \equiv -1 \pmod{p}$.

Now assume that r_1 is odd. Since $F_{r_1} \equiv 0 \pmod{p}$, we get $F_{r_1-1} \equiv F_{r_1+1} \pmod{p}$. Assume $F_{r_1+k} \equiv (-1)^{k-1}F_{r_1-k} \pmod{p}$ for all $0 \le k < \ell \le r_1 - 1$. Then

$$F_{r_1+\ell} = F_{r_1+(\ell-1)} + F_{r_1+(\ell-2)} \equiv (-1)^{\ell-1}(F_{r_1-(\ell-2)} - F_{r_1-(\ell-1)})$$
$$\equiv (-1)^{\ell-1}F_{r_1-\ell} \pmod{p}.$$

Therefore, $F_{2r_1-1} = F_{r_1+(r_1-1)} \equiv (-1)^{r_1-2}F_{r_1-(r_1-1)} \equiv -1 \pmod{p}$. By (3) with $n = r_1 - 1$, $m = r_1$, we get

$$F_{2r_1-1} = F_{r_1}^2 + F_{r_1-1}^2 \equiv F_{r_1-1}^2 \pmod{p},$$

so $F_{r_1-1}^2 \equiv -1 \pmod{p}$, i.e., has order 4 modulo p. □

Lemma 6: For $0 \le i \le j < r_1$,

$$\begin{bmatrix} nr_1 + j \\ mr_1 + i \end{bmatrix}_{\mathfrak{F}} \equiv \begin{bmatrix} nr_1 \\ mr_1 \end{bmatrix}_{\mathfrak{F}} \begin{bmatrix} j \\ i \end{bmatrix}_{\mathfrak{F}} F_{(n-m)r_1-1}^{i} F_{mr_1-1}^{j-i} \pmod{p}.$$

Proof: This is clear for $i = 0 = j$. Assume true for all $0 \le i \le j < k < r_1$ for some k. Take $1 \le \ell \le k-1$. Then, by (1),

$$\begin{bmatrix} nr_1 + k \\ mr_1 + \ell \end{bmatrix}_{\mathfrak{F}} = F_{mr_1+\ell+1}\begin{bmatrix} nr_1 + k - 1 \\ mr_1 + \ell \end{bmatrix}_{\mathfrak{F}} + F_{(n-m)r_1+k-\ell-1}\begin{bmatrix} nr_1 + k - 1 \\ mr_1 + \ell - 1 \end{bmatrix}_{\mathfrak{F}}.$$

The induction hypothesis gives

$$\begin{bmatrix} nr_1 + k \\ mr_1 + \ell \end{bmatrix}_{\mathfrak{F}} \equiv F_{mr_1+\ell+1}\begin{bmatrix} nr_1 \\ mr_1 \end{bmatrix}_{\mathfrak{F}}\begin{bmatrix} k-1 \\ \ell \end{bmatrix}_{\mathfrak{F}} F_{(n-m)r_1-1}^{\ell} F_{mr_1-1}^{k-\ell-1} + F_{(n-m)r_1+k-\ell-1}\begin{bmatrix} nr_1 \\ mr_1 \end{bmatrix}_{\mathfrak{F}}\begin{bmatrix} k-1 \\ \ell-1 \end{bmatrix}_{\mathfrak{F}} F_{(n-m)r_1-1}^{\ell-1} F_{mr_1-1}^{k-\ell}$$
$$\equiv \begin{bmatrix} nr_1 \\ mr_1 \end{bmatrix}_{\mathfrak{F}} F_{(n-m)r_1-1}^{\ell} F_{mr_1-1}^{k-\ell}\left(\frac{F_{mr_1+\ell+1}}{F_{mr_1-1}}\begin{bmatrix} k-1 \\ \ell \end{bmatrix}_{\mathfrak{F}} + \frac{F_{(n-m)r_1+k-\ell-1}}{F_{(n-m)r_1-1}}\begin{bmatrix} k-1 \\ \ell-1 \end{bmatrix}_{\mathfrak{F}}\right) \pmod{p}.$$

Using Lemma 3, we find this is equivalent to

$$\begin{bmatrix} nr_1 + k \\ mr_1 + \ell \end{bmatrix}_{\mathfrak{F}} \equiv \begin{bmatrix} nr_1 \\ mr_1 \end{bmatrix}_{\mathfrak{F}} F_{(n-m)r_1-1}^{\ell} F_{mr_1-1}^{k-\ell}\left(\frac{F_{\ell+1}}{F_1}\begin{bmatrix} k-1 \\ \ell \end{bmatrix}_{\mathfrak{F}} + \frac{F_{k-\ell-1}}{F_1}\begin{bmatrix} k-1 \\ \ell-1 \end{bmatrix}_{\mathfrak{F}}\right) \pmod{p}.$$

By (1), we conclude that

$$\begin{bmatrix} nr_1 + k \\ mr_1 + \ell \end{bmatrix}_{\mathfrak{F}} \equiv \begin{bmatrix} nr_1 \\ mr_1 \end{bmatrix}_{\mathfrak{F}}\begin{bmatrix} k \\ \ell \end{bmatrix}_{\mathfrak{F}} F_{(n-m)r_1-1}^{\ell} F_{mr_1-1}^{k-\ell} \pmod{p}.$$

The cases $\ell = 0$ and $\ell = k$ are dealt with similarly. □

4. MAIN RESULTS

Theorem 1: Let $r = \max_{i\geq 0} \frac{r_{i+1}}{r_i}$. The number of entries in the n^{th} row of the Fibonacci triangle not divisible by p is $2^{s_1}3^{s_2}4^{s_3}\ldots r^{s_{r-1}}$, where s_i is the number of i's in the base $\wp$ expansion of n.

Proof: First, we note that the maximum exists. It is well known that $r_1 \leq p+1$. By (4), we know that $\frac{r_{i+1}}{r_i} \leq p$ for $i \geq 1$, so $r \leq p+1$.

By Kummer's Theorem for Generalized Binomial Coefficients, $p \nmid \left[\begin{matrix} n \\ k \end{matrix}\right]_{\mathfrak{F}}$ if and only if there is no carry when k and $n-k$ are added in base $\wp$. Let the base $\wp$ expansions of n and k be $n = (n_t \ldots n_2 n_1 n_0)_{\wp}$ and $k = (k_t \ldots k_2 k_1 k_0)_{\wp}$. Then there is no carry when adding k and $n-k$ in base $\wp$ if and only if $k_i \leq n_i$ for all i. For a fixed n, the number of such k is $\prod_i (n_i+1)$ since there are (n_i+1) possible values of k_i less than or equal to n_i. □

The iterative structure of Pascal's triangle modulo 2 has been studied extensively (see [13]). Recently, the iterative structure of the Fibonacci triangle modulo 2 has also been studied. In particular, a map between the Fibonacci triangle modulo 2 and Pascal's triangle modulo 2 was found in [11]. For all primes $p \neq 2, 5$ whose rank of apparition is even, we get an analogous result: a map between the Fibonacci triangle modulo p and Pascal's triangle modulo p. While the result for these primes is similar to the case $p = 2$, our method of proof is different and, in fact, breaks down for $p = 2$.

Theorem 2: Let $p \neq 2, 5$ be a prime. There is the following connection between the Fibonacci and binomial coefficients modulo p:

$$\left[\begin{matrix} nr_1 \\ kr_1 \end{matrix}\right]_{\mathfrak{F}} \equiv \binom{n}{k} F_{r_1+1}^{k(n-k)r_1} \pmod{p}.$$

In particular, the triangle Δ_{F_p} formed by having $\left[\begin{matrix} nr_1 \\ kr_1 \end{matrix}\right]_{\mathfrak{F}} \pmod{p}$ as the k^{th} entry of the n^{th} row is Pascal's triangle modulo p if and only if r_1 is even.

Proof: By definition

$$\left[\begin{matrix} nr_1 \\ kr_1 \end{matrix}\right]_{\mathfrak{F}} \equiv \frac{F_{nr_1} F_{nr_1-1} \cdots F_{(n-k)r_1+1}}{F_{kr_1} F_{kr_1-1} \cdots F_2 F_1}.$$

Separating the factors divisible by p from those not divisible by p, we get

$$\left[\begin{matrix} nr_1 \\ kr_1 \end{matrix}\right]_{\mathfrak{F}} \equiv \frac{F_{nr_1} F_{(n-1)r_1} \cdots F_{(n-k+1)r_1}}{F_{kr_1} F_{(k-1)r_1} \cdots F_{r_1}} \cdot \frac{F_{nr_1-1} F_{nr_1-2} \cdots F_{(n-k)r_1+1}}{F_{kr_1-1} F_{kr_1-2} \cdots F_1}.$$

Using Lemmas 3 and 4 to simplify, we obtain

$$\left[\begin{matrix} nr_1 \\ kr_1 \end{matrix}\right]_{\mathfrak{F}} \equiv \frac{F_{nr_1} F_{(n-1)r_1} \cdots F_{(n-k+1)r_1}}{F_{kr_1} F_{(k-1)r_1} \cdots F_{r_1}} \cdot \frac{F_{nr_1+1}}{F_{kr_1+1}} \cdot \frac{F_{nr_1+1}}{F_{kr_1+1}} \cdot \cdots \cdot \frac{F_{nr_1+1}}{F_{kr_1+1}}$$

$$\equiv \frac{F_{nr_1} F_{(n-1)r_1} \cdots F_{(n-k+1)r_1}}{F_{kr_1} F_{(k-1)r_1} \cdots F_{r_1}} \left(\frac{F_{nr_1+1}}{F_{kr_1+1}}\right)^{k(r_1-1)} \pmod{p}.$$

Using Lemma 4 to simplify further, we get

$$\begin{bmatrix} nr_1 \\ kr_1 \end{bmatrix}_{\mathfrak{F}} \equiv \frac{F_{nr_1}F_{(n-1)r_1}\cdots F_{(n-k+1)r_1}}{F_{kr_1}F_{(k-1)r_1}\cdots F_{r_1}}(F_{(n-k)r_1+1})^{(r_1-1)k} \pmod{p}. \tag{6}$$

Now there are two cases to consider. If the number of factors of p in the numerator of the fraction

$$\frac{F_{nr_1}\cdots F_{(n-k+1)r_1}}{F_{kr_1}\cdots F_{r_1}}$$

is greater than the number of factors of p in the denominator, then $\left[\begin{smallmatrix} nr_1 \\ kr_1 \end{smallmatrix}\right]_{\mathfrak{F}} \equiv 0 \pmod{p}$. But by Kummer's theorem applied to $\mathcal{A} = \{F_{r_1 j}\}_{j=1}^{\infty}$, $p \mid \left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_{\mathcal{A}}$ if and only if there is a carry when adding k and $n-k$ in base $\wp' = \{\rho_0, \rho_1, \rho_2 \ldots\}$, where ρ_i is defined by $p^i \mid F_{r_1 j}$ if and only if $\rho_i \mid j$. By (4), all the ρ_i are powers of p, so there is a carry when adding k and $n-k$ in base $\wp'$ if and only if there is a carry when adding k and $n-k$ in base p (i.e., $\{1, p, p^2, \ldots\}$). By Kummer's Theorem for Generalized Binomial Coefficients, there is a carry when adding k and $n-k$ in base p if and only if $p \mid \binom{n}{k}$. In short, modulo p, the zeros of $\left[\begin{smallmatrix} nr_1 \\ kr_1 \end{smallmatrix}\right]_{\mathfrak{F}}$ correspond to the zeros of $\binom{n}{k}$, since the base $\wp'$ for $\mathcal{A} = \{F_{r_1 j}\}_{j=1}^{\infty}$ is the same, up to repeated terms, as the base corresponding to $\binom{n}{k}$, namely, $\{1, p, p^2, \ldots\}$.

Now consider the case where the number of factors of p in the numerator of the above fraction is the same as the number of factors of p in the denominator. We know that $F_{nr_1} \equiv F_{r_1}(nF_{r_1+1}^{n-1}) \pmod{p^2}$ by Lemma 2, so

$$\frac{F_{nr_1}F_{(n-1)r_1}\cdots F_{(n-k+1)r_1}}{F_{kr_1}F_{(k-1)r_1}\cdots F_{r_1}} \equiv \binom{n}{k}\frac{F_{r_1+1}^{n-1}F_{r_1+1}^{n-2}\cdots F_{r_1+1}^{n-k}}{F_{r_1+1}^{k-1}F_{r_1+1}^{k-2}\cdots F_{r_1+1}^{0}} \equiv \binom{n}{k}F_{r_1+1}^{k(n-k)} \pmod{p}.$$

This means that (6) can be simplified to

$$\begin{bmatrix} nr_1 \\ kr_1 \end{bmatrix}_{\mathfrak{F}} \equiv \binom{n}{k}F_{r_1+1}^{k(n-k)}F_{(n-k)r_1+1}^{(r_1-1)k} \pmod{p}. \tag{7}$$

By Lemma 1, this simplifies to

$$\begin{bmatrix} nr_1 \\ kr_1 \end{bmatrix}_{\mathfrak{F}} \equiv \binom{n}{k}F_{r_1+1}^{k(n-k)}F_{r_1+1}^{(n-k)(r_1-1)k} \equiv \binom{n}{k}F_{r_1+1}^{k(n-k)r_1} \pmod{p}. \tag{8}$$

This proves the first assertion of the theorem.

Now suppose that r_1 is even. By Lemma 5, $F_{r_1+1} \equiv \pm 1 \pmod{p}$. Then (8) reduces to

$$\begin{bmatrix} nr_1 \\ kr_1 \end{bmatrix}_{\mathfrak{F}} \equiv \binom{n}{k} \pmod{p}.$$

Finally, we need to show that when r_1 is odd, Δ_{F_p} is not the same as Pascal's triangle modulo p ($p = 2$ being the lone exception). For this, it is enough to show a single entry that does not match. By (8),

$$\begin{bmatrix} 2r_1 \\ r_1 \end{bmatrix}_{\mathfrak{F}} \equiv \binom{2}{1}F_{r_1+1}^{(1)(2-1)r_1} \pmod{p}.$$

By Lemma 5, when r_1 is odd, F_{r_1+1} has order 4 modulo p. In particular, an odd power of F_{r_1+1} cannot be congruent to 1 modulo p, so

$$\begin{bmatrix} 2r_1 \\ r_1 \end{bmatrix}_{\mathfrak{F}} \not\equiv \binom{2}{1} \pmod{p}. \quad \square$$

In the case $p = 5$, we find Δ_{F_5} is the same as the Fibonacci triangle modulo 5. The case $p = 2$ was dealt with previously in [11].

We note that there are infinitely many primes p for which Δ_{F_p} is the same as Pascal's triangle modulo p and there are infinitely many for which Δ_{F_p} is not the same as Pascal's triangle modulo p. By Theorem 2, this is equivalent to saying there are infinitely many primes p for which r_1 is even, since there are infinitely many F_{2^i} and for $i \geq 2$ there is always a prime factor of F_{2^i} which is not a prime factor of F_{2^j} for any $j < i$ [this follows from $r_1(2) = 3$, $F_{2^i} > F_{2^j}$ for $i > j$ and (4)]. Similarly, F_{3^i}, $i \geq 2$ may be used to show that infinitely many primes p have odd r_1.

As a result of Theorem 2 and Lemma 6, we have the following connection between an arbitrary nonzero Fibonacci coefficient modulo p and a well-defined Fibonacci coefficient in the first r_1 rows of the Fibonacci triangle.

Theorem 3: For $p \neq 2, 5$ a prime, we have

$$\begin{bmatrix} nr_1 + j \\ mr_1 + i \end{bmatrix}_{\mathfrak{F}} \equiv \binom{n}{m} \begin{bmatrix} j \\ i \end{bmatrix}_{\mathfrak{F}} F_{r_1+1}^{r_1 m(n-m)+i(n-m)+m(j-i)} \pmod{p}. \tag{9}$$

Proof: By Lemma 6,

$$\begin{bmatrix} nr_1 + j \\ mr_1 + i \end{bmatrix}_{\mathfrak{F}} \equiv \begin{bmatrix} nr_1 \\ mr_1 \end{bmatrix}_{\mathfrak{F}} \begin{bmatrix} j \\ i \end{bmatrix}_{\mathfrak{F}} F_{(n-m)r_1-1}^{i} F_{mr_1-1}^{j-i} \pmod{p}.$$

By (8), this becomes

$$\begin{bmatrix} nr_1 + j \\ mr_1 + i \end{bmatrix}_{\mathfrak{F}} \equiv \binom{n}{m} \begin{bmatrix} j \\ i \end{bmatrix}_{\mathfrak{F}} F_{r_1+1}^{r_1 m(n-m)} F_{(n-m)r_1-1}^{i} F_{mr_1-1}^{j-i} \pmod{p}.$$

Applying Lemma 1, we get

$$\begin{aligned} \begin{bmatrix} nr_1 + j \\ mr_1 + i \end{bmatrix}_{\mathfrak{F}} &\equiv \binom{n}{m} \begin{bmatrix} j \\ i \end{bmatrix}_{\mathfrak{F}} F_{r_1+1}^{r_1 m(n-m)} F_{r_1+1}^{i(n-m)} F_{r_1+1}^{m(j-i)} \\ &\equiv \binom{n}{m} \begin{bmatrix} j \\ i \end{bmatrix}_{\mathfrak{F}} F_{r_1+1}^{r_1 m(n-m)+i(n-m)+m(j-i)} \pmod{p}. \quad \square \end{aligned}$$

Theorem 3 allows rapid computation of $\begin{bmatrix} n \\ k \end{bmatrix}_{\mathfrak{F}} \pmod{p}$ for large n, k as shown in Examples 1 and 2 in the next section. Theorem 3 may be interpreted geometrically as a relation between columns in rows nr_1 to $nr_1 + (r_1 - 1)$ and the first r_1 rows of the Fibonacci triangle modulo p; each entry in the first r_1 rows is multiplied by the constant $\binom{n}{m} F_{r_1+1}^{r_1 m(n-m)+i(n-m)+m(j-i)}$ modulo p to get the corresponding entry between rows nr_1 and $nr_1 + (r_1 - 1)$. This is demonstrated in Example 3 of Section 5.

5. EXAMPLES

Example 1: In order to calculate $\left[\begin{smallmatrix}83\\46\end{smallmatrix}\right]_{\mathfrak{F}}$ (mod 13), we first note that for $p=13$, $r_1=7$, and $F_{r_1-1}=F_6\equiv 8 \pmod{13}$. Then by (9) we have

$$\begin{bmatrix}83\\46\end{bmatrix}_{\mathfrak{F}}=\begin{bmatrix}11(7)+6\\6(7)+4\end{bmatrix}_{\mathfrak{F}}\equiv\binom{11}{6}\begin{bmatrix}6\\4\end{bmatrix}_{\mathfrak{F}}F_6^{7(6)(11-6)} \pmod{13}.$$

Remembering that F_6 has order 4 modulo 13 (since r_1 is odd), we have

$$\begin{bmatrix}83\\46\end{bmatrix}_{\mathfrak{F}}\equiv\binom{11}{6}\begin{bmatrix}6\\4\end{bmatrix}_{\mathfrak{F}}8^{(3)(2)(1)}\equiv\binom{11}{6}\begin{bmatrix}6\\4\end{bmatrix}_{\mathfrak{F}}8^2 \pmod{13}.$$

Since $\binom{11}{6}\equiv 7 \pmod{13}$ and $\left[\begin{smallmatrix}6\\4\end{smallmatrix}\right]_{\mathfrak{F}}\equiv 1 \pmod{13}$, we conclude that

$$\begin{bmatrix}83\\46\end{bmatrix}_{\mathfrak{F}}\equiv 7(1)(-1)\equiv 6 \pmod{13}.$$

Example 2: In order to calculate $\left[\begin{smallmatrix}1000\\768\end{smallmatrix}\right]_{\mathfrak{F}}$ (mod 89), we note for $p=89$, $r_1=11$, and $F_{r_1-1}=F_{10}\equiv 55 \pmod{89}$. Then by (9) we have

$$\begin{bmatrix}1000\\768\end{bmatrix}_{\mathfrak{F}}=\begin{bmatrix}90(11)+10\\69(11)+9\end{bmatrix}_{\mathfrak{F}}\equiv\binom{90}{69}\begin{bmatrix}10\\9\end{bmatrix}_{\mathfrak{F}}F_{10}^{(11)(69)(90-69)} \pmod{89}.$$

Since $\binom{90}{69}\equiv 0 \pmod{89}$ (i.e., a carry occurs when adding 21 and 69 base 89), we conclude that

$$\begin{bmatrix}1000\\768\end{bmatrix}_{\mathfrak{F}}\equiv 0 \pmod{89}.$$

Example 3: Theorem 3 can be interpreted geometrically. For $p=3$ we have $r_1=4$ and $F_{r_1-1}=2\equiv -1 \pmod{3}$. The first four rows of the Fibonacci triangle taken modulo 3 are:

```
      1
    1   1
  1   1   1
1   2   2   1
```

FIGURE 2. Basic Triangle Modulo 3

By Theorem 3, this 4-row triangle with variations based on the parity of m and n will build the entire Fibonacci triangle modulo 3. Specifically for the 4 cases of m, n even or odd, we have

1	1	1	1
1 1	1 2	2 1	2 2
1 1 1	1 2 1	1 2 1	1 1 1
1 2 2 1	1 1 2 2	2 2 1 1	2 1 1 2
m, n even	m even	neither	n even

FIGURE 3. The Four Variants of the Basic Triangle Modulo 3

For example, the triangle in rows 4 to 7 ($n=1$) and columns 0 to 3 ($m=0$) is the second triangle in Figure 3 with entry multiplied by $\binom{1}{0}=1$. The triangle in rows 8 to 11 ($n=2$) and columns 4 to 7 ($m=1$) is the fourth triangle in Figure 3 with each entry multiplied by $\binom{2}{1}=2$. These are shown in Figure 4.

1
1 1
1 1 1
1 2 2 1
1 0 0 0 1
1 2 0 0 2 1
1 2 1 0 1 2 1
1 1 2 2 2 2 1 1
1 0 0 0 2 0 0 0 1
1 1 0 0 1 1 0 0 1 1
1 1 1 0 2 2 2 0 1 1 1
1 2 2 1 1 2 2 1 1 2 2 1

FIGURE 4. Rows 0 to 11 of the Fibonacci Triangle Modulo 3

More generally, to determine the triangle in rows $4n$ to $4n+3$ and columns $4m$ to $4m+3$, we pick the appropriate triangle in Figure 3, based on the parity of m, n and multiply each entry by $\binom{n}{m} \pmod 3$.

ACKNOWLEDGMENTS

The author would like to thank two of his MA students, Rob and Nicole Fraser, for preliminary discussions in general and for conjecturing Theorem 1 in particular.

REFERENCES

1. N. Fine. "Binomial Coefficients Modulo a Prime." *Amer. Math. Monthly* **54** (1947):589-92.
2. A. Granville. "Zaphod Beeblebrox's Brain and the Fifty-Ninth Row of Pascal's Triangle." *Amer. Math. Monthly* **99.4** (1992):318-31.
3. H. Harborth. "Number of Odd Binomial Coefficients." *Proc. Amer. Math. Soc.* **62** (1977): 19-22.
4. V. E. Hoggatt, Jr. "Fibonacci Numbers and Generalized Binomial Coefficients." *The Fibonacci Quarterly* **5.5** (1967):383-400.
5. 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.
6. C. T. Long & N. Woo. "On Bases for the Set of Integers." *Duke Math. J.* **38** (1971):583-90.
7. E. Lucas. "Sur la théorie des nombres premiers." *Atti R. Acad. Sci. Torino* (Math.) **11** (1875-1876):928-37.
8. D. Singmaster. "Divisibility of Binomial and Multinomial Coefficients by Primes and Prime Powers." In *A Collection of Manuscripts Related to Fibonacci Sequences* 398-113. Santa Clara, Calif.: The Fibonacci Association, 1980.
9. N. N. Vorobyov. *The Fibonacci Numbers*. Tr. Normal Whaland & Olga Titelbaum. Boston: D. Heath and Co., 1963.
10. W. A. Webb & D. Wells. "Kummer's Theorem for Generalized Binomial Coefficients." Personal correspondence, September 6, 1995.
11. D. Wells. "The Fibonacci and Lucas Triangles Modulo 2." *The Fibonacci Quarterly* **32.2** (1994):111-23.
12. D. Wells. "Residue Counts Modulo Three for the Fibonacci Triangle." In *Applications of Fibonacci Numbers* **6:**521-26. Dordrecht: Kluwer, 1996.
13. S. Wolfram. "Geometry of Binomial Coefficients." *Amer. Math. Monthly* **91** (1984):566-71.

AMS Classification Numbers: 11B39, 11B65

❖❖❖

A NOTE ON STIRLING NUMBERS OF THE SECOND KIND

Nenad P. Cakić
Faculty of Technology, Dept. of Math., 16000 Leskovac, Yugoslavia
(Submitted July 1996-Final Revision March 1997)

1. INTRODUCTION

In [3], Todorov proved a theorem related to the explicit expression for Stirling numbers of the second kind, $S(n, m)$, in a very complicated way. In this paper, we shall prove that this result is a consequence of the well-known representation of the Stirling numbers of the second kind.

Starting from the rational generating function for Stirling numbers of the second kind,

$$\frac{t^m}{(1-t)(1-2t)\cdots(1-mt)} = \sum_{n=m}^{\infty} S(n,m)t^n, \tag{1}$$

we find that the left side of (1) is identical to

$$\begin{aligned} &t^m(1+t+t^2+\cdots)(1+2t+2^2t^2+\cdots)\cdots(1+mt+m^2t^2+\cdots) \\ &= \sum_{n=m}^{\infty}\left(\sum_{k_1+k_2+\cdots+k_m=n-m} 1^{k_1}2^{k_2}\cdots m^{k_m}\right)t^m. \end{aligned} \tag{2}$$

If we identify coefficients of t^n from equations (1) and (2), we get (see Aigner [1] or Comtet [2]):

$$S(n,m) = \sum_{k_1+k_2+\cdots+k_m=n-m} 1^{k_1}2^{k_2}\cdots m^{k_m}.$$

This formula is identical to

$$S(n,m) = \sum_{1\le i_1\le i_2\le\cdots\le i_{n-m}\le m} i_1 i_2\cdots i_{n-m}. \tag{3}$$

In this paper, we prove that Todorov's expression for Stirling numbers of the second kind (see [3]) is a simple consequence of the representation (3).

1. THE MAIN RESULT

Let us take, in (3), the change of indices in the following way:

$$i_s = j_s - s \quad (s = 1, 2, \ldots, k). \tag{4}$$

Then, from $1 \le i_1 \le i_2$, we have $2 \le i_1 + 1 \le i_2 + 1$, i.e., $2 \le j_1 \le j_2 - 1$. Similarly, from

$$(\forall s \in \{1, 2, \ldots, k\}), \quad s \le i_{s-1} + s - 1 \le i_s + s - 1,$$

using (4), we get

$$s \le j_{s-1} \le j_s - 1 \quad (s = 2, \ldots, k).$$

For $k = n - m$, we obtain $k + 1 \le j_k - (n - m) \le m$, i.e., $k + 1 \le j_k \le n$. So, the sum on the right side of the equality (3) is identical to

$$S(n,m)=\sum_{j_k=k+1}^{n}\sum_{j_{k-1}=k}^{j_k-1}\cdots\sum_{j_2=3}^{j_3-1}\sum_{j_1=2}^{j_2-1}(j_k-k)(j_{k-1}-k+1)\cdots(j_1-1), \tag{5}$$

which is the result from [3].

Example: We use $n=6$, $m=3$, and $k=n-m=3$. Following the change of indices from the equality (4), we get $i_1=j_1-1$, $i_2=j_2-2$, and $i_3=j_3-3$. Then, from $1\le i_1\le i_2\le i_3\le 3$, we have $2\le j_1\le j_2-1$, $3\le j_2\le j_3-1$, and $4\le j_3-3\le 3$, i.e., $4\le j_3\le 6$.

After these transformations, from formula (3) it follows that

$$\begin{aligned}S(6,3)=90&=\sum_{1\le i_1\le i_2\le i_3\le 3} i_1i_2i_3\\&=1\cdot1\cdot1+1\cdot1\cdot2+1\cdot1\cdot3+1\cdot2\cdot2+1\cdot2\cdot3+1\cdot3\cdot3+2\cdot2\cdot2+2\cdot2\cdot3+2\cdot3\cdot3+3\cdot3\cdot3\\&=1\cdot1\cdot1+2\cdot(1\cdot1+2\cdot1+2\cdot2)+3\cdot(1\cdot1+2\cdot1+2\cdot2+3\cdot1+3\cdot2+3\cdot3)\\&=\sum_{j_3=4}^{6}\sum_{j_2=3}^{j_3-1}\sum_{j_1=2}^{j_2-1}(j_3-3)(j_2-2)(j_1-1),\end{aligned}$$

which is formula (5), where we use $n=6$, $m=3$, and $k=n-m=3$.

REFERENCES

1. M. Aigner. *Combinatorial Theory*, p. 107. Berlin, Heidelberg, New York: Springer-Verlag, 1979. (In Russian.)
2. L. Comtet. *Advanced Combinatorics*, p. 207. Dordrecht: Reidel, 1974.
3. K. Todorov. "Über die Anzahl der Äquivalenzrelationen der endlichen Menge." *Studia Sci. Math. Hung.* **14** (1979):311-14.

AMS Classification Numbers: 05A15, 05A19

❖❖❖

BOUNDS ON THE FIBONACCI NUMBER OF A MAXIMAL OUTERPLANAR GRAPH

Ahmad Fawzi Alameddine
Dept. of Math. Sci., King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
(*Submitted August 1996*)

1. INTRODUCTION

All graphs in this article are finite, undirected, without loops or multiple edges. Let G be a graph with vertices $v_1, v_2, \ldots, v_n$. The *complement* in G of a subgraph H is the subgraph of G obtained by deleting all edges in H. The *join* $G_1 \vee G_2$ of two graphs G_1 and G_2 is obtained by adding an edge from each vertex in G_1 to each vertex in G_2. Let K_n be the complete graph and P_n the path on n vertices.

The concept *Fibonacci number f* of a simple graph G refers to the number of subsets S of $V(G)$ such that no two vertices in S are adjacent [5]. Accordingly, the total number of subsets of $\{1, 2, \ldots, n\}$ such that no two elements are adjacent is F_{n+1}, the $(n+1)^{\text{th}}$ Fibonacci number.

2. THE FIBONACCI NUMBER OF A GRAPH

The following propositions can be found in [1], [2], and [3].

(a) $f(P_n) = F_{n+1}$.

(b) Let $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ be two graphs with $E_1 \subseteq E_2$, then $f(G_2) \le f(G_1)$.

(c) Let $G = (V, E)$ be a graph with $u_1, u_2, \ldots, u_s$ vertices not contained in V. If $G_1 = (V_1, E_1)$ denotes the graph with $V_1 = V \cup \{u_1, \ldots, u_s\}$ and $E_1 = E \cup \{\{u_1, v_j\}, 1 \le i \le s, v_j \in V\}$, then $f(G_1) = f(G) + 2^s - 1$.

(d) A fan on k vertices, denoted by N_k, is the graph obtained from path P_{k-1} by making vertex 1 adjacent to every vertex of P_{k-1}, we have $f(N_k) = F_k + 1$.

(e) If T is a tree on n vertices, then $F_{n+1} \le f(T) \le 2^{n-1} + 1$. The upper and lower bounds are assumed by the stars S_n and paths P_n, where $f(S_n) = 2^{n-1} + 1$ and $f(P_n) = F_{n+1}$.

(f) If G_1 and G_2 are disjoint graphs, then $f(G_1 \cup G_2) = f(G_1) \cdot f(G_2)$.

3. THE SPECTRUM OF A GRAPH

The spectral radius $r(G)$ is the largest eigenvalue of its adjacency matrix $A(G)$. For $n \ge 4$ let $\mathcal{H}_n$ be the class of all *maximal outerplanar graphs* (Mops for short) on n vertices. If $G \in \mathcal{H}_n$, then G has at least two vertices of degree 2, has a plane representation as an n-gon triangulated by $n-3$ chords, and the boundary of this n-gon is the unique Hamiltonian cycle Z of G. As in [4], we let P_n^2 denote the graph obtained from P_n by adding new edges joining all pairs of vertices at a distance 2 apart. An *internal triangle* is a triangle in a Mop with no edge on the outer face. Let $\mathcal{G}_n$ be the subclass of all Mops in $\mathcal{H}_n$ with no internal triangle. Rowlinson [6] proved that $K_1 \vee P_{n-1}$ is the unique graph in $\mathcal{G}_n$ with maximal spectral radius. He also proved the uniqueness

of P_n^2 with minimal $r(G)$ for all graphs in $\mathcal{G}_n$. In [6], Cvetković and Rowlinson conjectured that $K_1 \vee P_{n-1}$ with spectral radius very close to $1+\sqrt{n}$ is the unique graph with the largest radius among all Mops in $\mathcal{H}_n$. In [2], Cao and Vince showed that the largest eigenvalue of $K_1 \vee P_{n-1}$ is between $1+\sqrt{n}-\frac{1}{2+n-2\sqrt{n}}$ and $1+\sqrt{n}$. This result comes close to confirming the conjecture of Rowlinson and Cvetković but does not settle it.

We will show that these two graphs $K_1 \vee P_{n-1}$ and P_n^2 are extremal and unique in $\mathcal{H}_n$ with respect to their Fibonacci numbers.

All Mops of order 8 are shown in Figure 1. Each Mop is labelled by its spectral radius r and Fibonacci number f.

4. THE UPPER BOUND

We established in [1] an upper bound on f of all Mops in $\mathcal{H}_n$ as in the following theorem.

Theorem 1: The Fibonacci number $f(G)$ of a maximal outerplanar graph G of order $n \geq 3$ is bounded above by $F_n + 1$. Moreover, this upper bound is best possible.

The upper bound in Theorem 1 is realized by the Mop $K_1 \vee P_{n-1}$. Here, we prove that this Mop is unique.

Theorem 2: $K_1 \vee P_{n-1}$ is unique in $\mathcal{H}_n$.

Proof: We suppose that $n \geq 6$ because, if $n\{4, 5\}$, then $K_1 \vee P_{n-1} = P_n^2$ and $\mathcal{H}_n$ contains only one graph. We continue the proof by induction on n. Assume uniqueness for all Mops of order less than n, and let G be a Mop of order n, $G \neq K_1 \vee P_{n-1}$. There exists a vertex v of degree 2 in G. We consider two families of subsets of $V(G)$. Each subset in the first family contains v, whereas v is not in any subset of the second family. Let u and w be neighbors of v in G. Deleting u and w, we obtain the outerplanar graph $G_{u,w}$ of order $n-3$ and the isolated vertex v. Since G is a triangulation of a polygon, $G_{u,w}$ contains a path P_{n-3} of length $n-4$.

Note that v can be chosen so that $d(u)+d(w)$ in G is minimum. Also, since $G \neq K_1 \vee P_{n-1}$, then $G_{u,w} \neq P_{n-3}$. Moreover, P_{n-3} is a proper subgraph of $G_{u,w}$. By Proposition (a),

$$f(P_{n-3}) = F_{n-2}$$

and, since v is a member of every subset of $V(G)$,

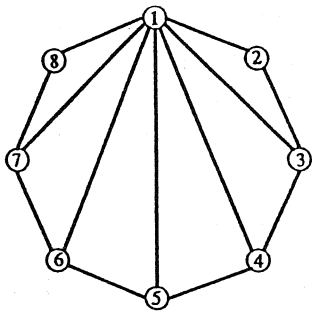
$$f(P_{n-3} \cup \{v\}) = f(P_{n-3}).$$

Now, by Proposition (b),

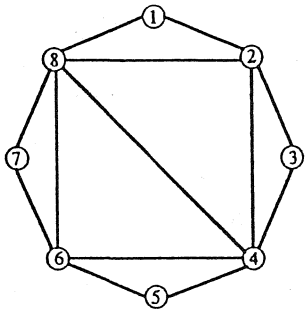
$$f(G_{u,w}) < F_{n-2}.$$

Next, we consider those admissible subsets of $V(G)$ not containing v. Let G_v be the remaining graph of order $n-1$ after deleting v. G_v is maximal outerplanar of order $n-1$. By the induction hypothesis, $K_1 \vee P_{n-2}$ is unique in $\mathcal{H}_{n-1}$, and this implies that $f(G_v)$ is strictly less than $F_{n-1}+1$. Combining the above results, we have

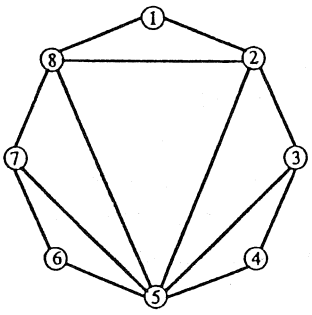
$$f(G) = f(G_{u,w}) + F(G_v) < F_{n-2} + F_{n-1} + 1 < F_n + 1.$$



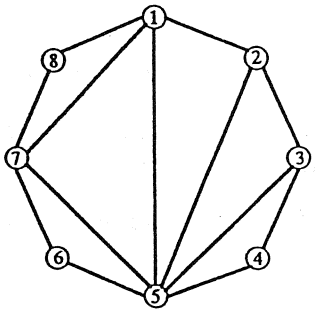
(1) $r \cong 3.676$, $f = 35$



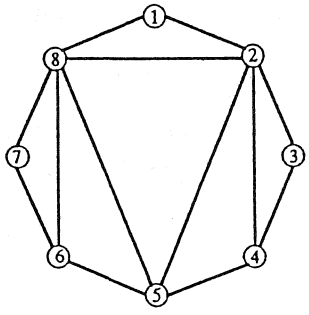
(2) $r \cong 3.646$, $f = 32$



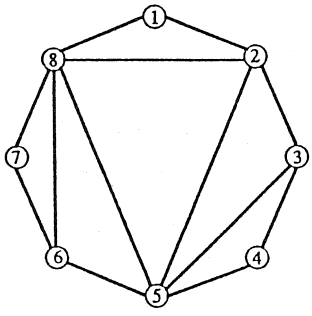
(3) $r \cong 3.639$, $f = 32$



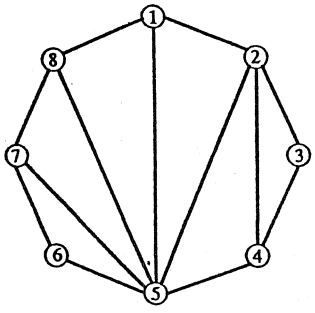
(4) $r \cong 3.63$, $f = 32$



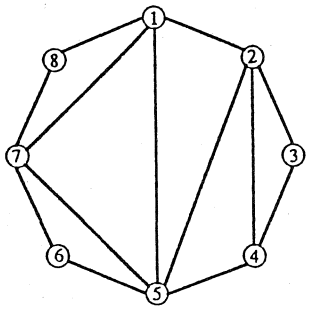
(5) $r \cong 3.602$, $f = 32$



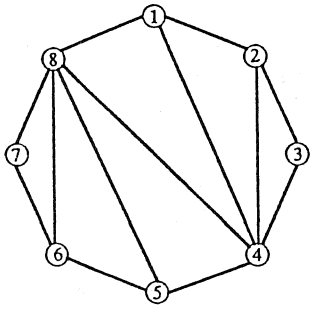
(6) $r \cong 3.608$, $f = 31$



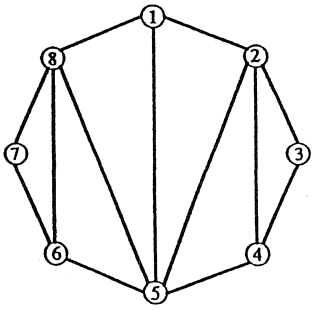
(7) $r \cong 3.590$, $f = 32$



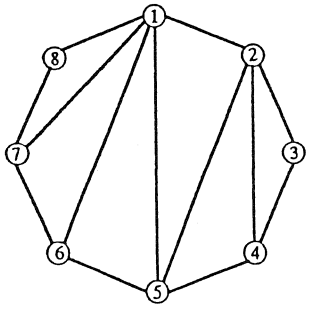
(8) $r \cong 3.570$, $f = 30$



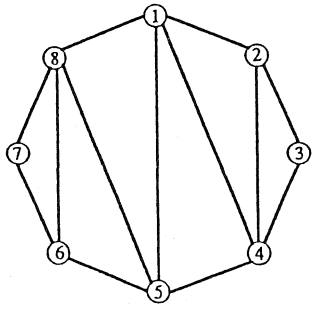
(9) $r \cong 3.550$, $f = 31$



(10) $r \cong 3.520$, $f = 29$



(11) $r \cong 3.516$, $f = 29$



(12) $r \cong 3.477$, $f = 28$

FIGURE 1. Twelve Mops with Their Spectral Radii and Fibonacci Numbers Indicated

5. THE LOWER BOUND

For the lower bound in $\mathcal{H}_n$, we let $H_n = P_n^2$, $n \geq 6$. These Mops H_n satisfy a recurrence relation $f(H_n) = f(H_{n-1}) + f(H_{n-3})$, whose solution h_n is

$$h_n = \left[\frac{u+v+10}{3u+3v}\right]\left[\frac{u+v+1}{3}\right]^n + \left[\frac{u+v-5}{3u+3v}\right]\left[-\frac{u+v-2}{6} + \frac{u-v}{6}\sqrt{3}i\right]^n + \left[\frac{u+v-5}{3u+3v}\right]\left[-\frac{u+v-2}{6} - \frac{u-v}{6}\sqrt{3}i\right]^n,$$

where

$$u = \sqrt[3]{\frac{29+3\sqrt{93}}{2}} \quad \text{and} \quad v = \sqrt[3]{\frac{29-3\sqrt{93}}{2}}.$$

After simplification, we have

$$h_n \cong (1.3134\ldots)(1.4655\ldots)^n.$$

Figure 2 shows a configuration of H_n for the even and odd cases.

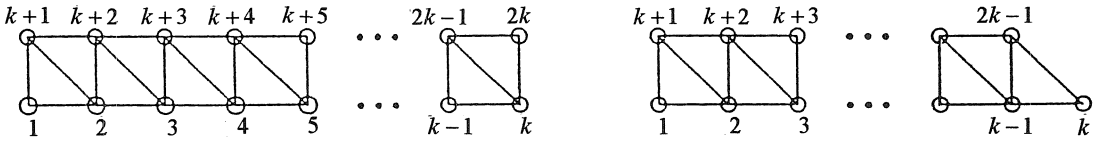


FIGURE 2. H_n Satisfies the Lower Bound

Theorem 3: The Fibonacci number $f(G)$ of a maximal outerplanar graph G of order $n \geq 3$ is bounded below by $f(P_n^2)$. Moreover, P_n^2 is unique.

Proof: As in the proof of Theorem 2, we suppose $n \geq 6$. We will prove the theorem by induction on n. The result is obvious for graphs of small order. Assume the validity of the theorem for all Mops of order less than n and let G be a Mop of order n where $G \neq P_n^2$. Each Mop has at least two vertices of degree 2. Suppose v is a vertex of degree 2 and u and w are adjacent to v. Since there are at least two choices of v, we will choose vertex v such that $d(u)+d(w)$ is maximum. We consider two families of subsets of $V(G)$. Each subset in the first family contains v, whereas v is not in any subset of the second family. Deleting u and w, we obtain the outerplanar subgraph $G_{u,w}$ of order $n-3$ and the isolated vertex v. Now $G_{u,w}$ is not maximal. We construct the Mop $G_{u,w}^*$ containing $G_{u,w}$ by adding edges in such a way that $\Delta(G_{u,w}^*) \geq 5$. This construction is always possible due to our choice of the vertex v. Thus, $G_{u,w}^* \neq P_{n-3}^2$ and, by the induction hypothesis,

$$f(G_{u,w}) > f(G_{u,w}^*) \geq f(P_{n-3}^2) = f(H_{n-3}). \qquad (*)$$

Next, we consider those sets of $V(G)$ not containing v. Let G_v be the remaining graph of order $n-1$ after deleting the vertex v. G_v is a Mop. By the induction hypothesis

$$f(G_v) \geq f(P_{n-1}^2) = f(H_{n-1}). \qquad (**)$$

Combining (*) and (**), we have

$$f(G) = f(G_v) + f(G_{u,w}) > f(H_{n-1}) + f(H_{n-3}) = f(H_n) = f(P_n^2).$$

We summarize our results for $n \leq 20$ in Table 1.

TABLE 1. The Fibonacci Numbers F_n, $f(K_1 \vee P_{n-1})$ and $f(P_n^2)$ for $n \leq 20$

n	F_n	$f(K_1 \vee P_{n-1})$	$f(P_n^2)$
0	1	1	1
1	1	2	2
2	2	3	3
3	3	4	4
4	5	6	6
5	8	9	9
6	13	14	13
7	21	22	19
8	34	35	28
9	55	56	41
10	89	90	60
11	144	145	88
12	233	234	129
13	377	378	189
14	610	611	277
15	987	988	406
16	1597	1598	595
17	2584	2585	872
18	4181	4182	1278
19	6765	6766	1873
20	10946	10947	2745

ACKNOWLEDGMENT

The author gratefully acknowledges the support provided by King Fahd University of Petroleum and Minerals.

REFERENCES

1. A. F. Alameddine. "An Upper Bound for the Fibonacci Number of a Maximal Outerplanar Graph." *Arabian Journal for Science and Engineering* **8** (1983):129-31.
2. D. Cao & A. Vince. "The Spectral Radius of a Planar Graph." *Linear Algebra Appl.* **187** (1993):251-57.
3. L. Comtet. *Advanced Combinatorics.* Dordrecht: Reidel, 1974.
4. D. Cvetković, M. Doob, & H. Sachs. *Spectra of Graphs.* New York: Academic Press, 1980.
5. H. Prodinger & R. F. Tichy. "Fibonacci Number of Graphs." *The Fibonacci Quarterly* **20.1** (1982):16-21.
6. P. Rowlinson. "On the Index of Certain Outerplanar Graphs." *Ars. Comb.* **29C** (1990):221-25.

AMS Classification Numbers: 11B39, 11B65

❖❖❖

ON A FIBONACCI RELATED SERIES

A. Sofo and P. Cerone
Dept. of Computer and Mathematical Sciences, Victoria University of Technology, Melbourne, Australia
(Submitted August 1996-Final Revision April 1997)

1. INTRODUCTION

A Fibonacci-related sequence is used as motivation for the representation of a resulting infinite series in closed form. Use is made of Z transform theory in the solution of a homogeneous difference-delay equation, together with an appeal to some asymptotic properties.

2. METHOD

Consider the homogeneous difference-delay equation

$$\left.\begin{aligned} f_{n+1} - bf_n - cf_{n-a} &= 0, \quad n \geq a, \\ f_{n+1} - bf_n &= 0, \quad n < a, \end{aligned}\right\} \tag{1}$$

with $f_0 = 1$; a and n are positive integers including zero, and b and c are real constants.

The Z transform of a sequence $\{f_n\}$ is a function $F(z)$ of a complex variable defined by $F(z) = Z[f_n] = \sum_{n=0}^{\infty} f_n z^{-n}$ (see [6]) for those values of z for which the infinite series converges.

Taking the Z transform of equation (1) and using the initial condition $f_0 = 1$ yields, upon rearrangement,

$$F(z) = Z[f_n] = \frac{z}{z - b - cz^{-a}} = \frac{z^{a+1}}{z^{a+1} - bz^a - c}. \tag{2}$$

In particular, putting $c = b$, equation (2) may be put in the form

$$F(z) = \frac{z}{(z-b)\left[1 - \frac{bz^{-a}}{z-b}\right]},$$

and expanding in series form results in

$$F(z) = \sum_{r=0}^{\infty} \frac{b^r z^{1-ar}}{(z-b)^{1+r}}. \tag{3}$$

Convergence of the infinite series (3) is assured for $\left|\frac{bz^{-a}}{(z-b)}\right| < 1$.

The inverse Z transform of (3), from tables given in [6], is

$$f_n = \sum_{r=0}^{\infty} \binom{n-ar}{r} b^{(n-ar)} U(n-ar), \tag{4}$$

where $U(n-ar)$ is the discrete step function. Equation (4) may thus be rewritten as

$$f_n = \sum_{r=0}^{[n/(a+1)]} \binom{n-ar}{r} b^{(n-ar)}, \tag{5}$$

where $[x]$ represents the integer part of x.

The inverse Z transform of (3) may also be expressed as

$$f_n = \frac{1}{2\pi i}\int_C z^{n-1}F(z)\,dz = \sum_{j=0}^{a} z^n \mathrm{Res}_j\left(\frac{F(z)}{z}\right), \tag{6}$$

where C is a smooth Jordan curve enclosing the singularities of (2) and the integral is traversed once in an anticlockwise direction around C. [Here in (6) it may be shown that there is no contribution from the integration around the contour.]

For the restriction (which will subsequently be required for a resulting infinite series)

$$\left|\frac{(a+1)^{a+1}}{(ab)^a}\right| < 1, \tag{7}$$

the characteristic function

$$g(z) = z^{a+1} - bz^a - b \tag{8}$$

has $(a+1)$ distinct zeros ξ_j, $j = 0, 1, 2, \ldots, a$. All the singularities in (2) are therefore simple poles such that the residue, Res_j, of the poles in (2) may be evaluated as follows:

$$\mathrm{Res}_j = \lim_{z\to\xi_j}\left[(z-\xi_j)\frac{z^a}{z^{a+1}-bz^a-c}\right] = \frac{\xi_j}{(a+1)\xi_j - ab}. \tag{9}$$

From (5), and using (6) and (9), it can be concluded that

$$f_n = \sum_{r=0}^{[n/(a+1)]}\binom{n-ar}{r}b^{(n-ar)} = \sum_{j=0}^{a}\frac{\xi_j^{n+1}}{(a+1)\xi_j - ab}. \tag{10}$$

3. CONJECTURE

A Tauberian theorem [1] suggests, from (10), that

$$f_n = \sum_{r=0}^{[n/(a+1)]}\binom{n-ar}{r}b^{(n-ar)} \sim \frac{\xi_0^{n+1}}{(a+1)\xi_0 - ab}, \tag{11}$$

where ξ_0 ;is the dominant zero of (8), defined as the one with the greatest modulus.

For n large, more and more terms in the left-hand side of the series (11) are incorporated, and therefore it is *conjectured* that

$$\sum_{r=0}^{\infty}\binom{n-ar}{r}b^{(n-ar)} = \frac{\xi_0^{n+1}}{(a+1)\xi_0 - ab} \tag{12}$$

for all values of n.

Using the ratio test, the infinite series in (12) may be shown to converge in the region given by (7). A diagram of the region of convergence is shown as the shaded region of Figure 1 on the following page.

It is now worthwhile to examine briefly the location of all the zeros of (8) and highlight the fact that ξ_0, the dominant zero of (8) is always real. Details of the following statements may be seen in the work of Sofo and Cerone [4].

It may be shown, by using Rouche's theorem [5], that the characteristic function (8) with restriction (7) has exactly a zeros in the contour $\Gamma: |z| \le \left|\frac{ab}{a+1}\right|$. Since the coefficients of (8) are

real, its complex zeros occur in conjugate pairs. Hence, the one remaining zero of (8), occurring outside the contour Γ, must be real. Furthermore, it can be shown that $\xi_0 > b$ for $b > 0$ and $|\xi_0| > \left|\frac{ab}{a+1}\right|$ for $b < 0$.

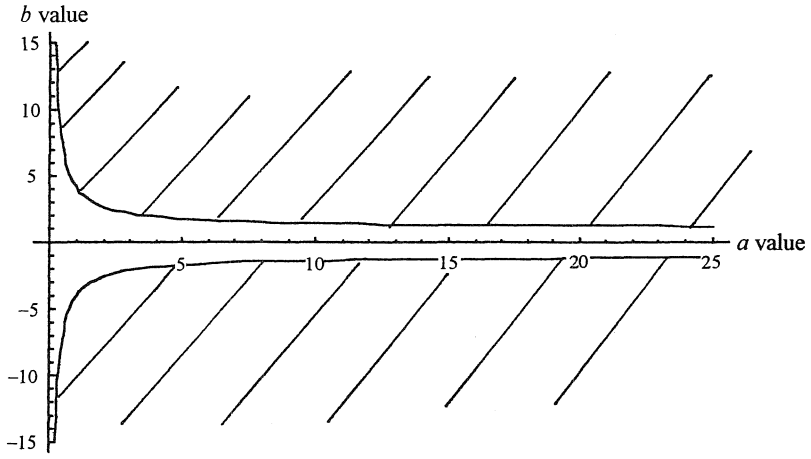


FIGURE 1. The Convergence Region (7)

Utilizing (10) and the conjectured result (12), it may be seen that these would imply

$$\sum_{r=0}^{[n/(a+1)]}\binom{n-ar}{r}b^{(n-ar)} + \sum_{r=\left[\frac{n+1}{a}\right]}^{\infty}\binom{n-ar}{r}b^{(n-ar)} = \frac{\xi_0^{n+1}}{(a+1)\xi_0 - ab},$$

so

$$\sum_{r=\left[\frac{n+1}{a}\right]}^{\infty}\binom{-(n-ar)}{r}b^{-(n-ar)} = -\sum_{j=1}^{a}\frac{\xi_j^{n+1}}{(a+1)\xi_j - ab}$$

such that

$$\sum_{r=\left[\frac{n+1}{a}\right]}^{\infty}(-1)^{r+1}\binom{ar+r-1-n}{r}b^{-(n-ar)} = -\sum_{j=1}^{a}\frac{\xi_j^{n+1}}{(a+1)\xi_j - ab},$$

where use is made of the relation (see [3])

$$\binom{-m}{n} = (-1)^n\binom{m+n-1}{n} \quad \text{and} \quad \binom{0}{n} = 0. \tag{13}$$

4. PROOF OF CONJECTURE

Consider equation (12) and let $n = -aN$ such that

$$\sum_{r=0}^{\infty}\binom{-a(N+r)}{r}b^{-a(N+r)} = \frac{\xi_0^{-aN+1}}{(a+1)\xi_0 - ab}. \tag{14}$$

Utilizing the result

$$b^{-a(N+r)} = \left(\frac{1+\xi_0^a}{\xi_0^{1+a}}\right)^{a(N+r)}$$

from (8) and equation (13) allows the left-hand side of (14) to be expressed as

$$\sum_{r=0}^{\infty}\binom{-a(N+r)}{r}b^{-a(N+r)} = \sum_{r=0}^{\infty}(-1)^r\binom{aN+ar+r-1}{r}\left(\frac{1+\xi_0^a}{\xi_0^{1+a}}\right)^{a(N+r)}$$
$$= \sum_{r=0}^{\infty}(-1)^r\binom{aN+ar+r-1}{r}\sum_{k=0}^{a(N+r)}\binom{aN+ar}{k}\xi_0^{ak-a(1+a)(N+r)}. \tag{15}$$

The convergent double sum (15) may be written term by term as

$$\binom{aN-1}{0}\left[\binom{aN}{0}\xi_0^{-a(1+a)N}+\cdots+\binom{aN}{aN-1}\xi_0^{-a(N+1)}+\binom{aN}{aN}\xi_0^{-a(N+0)}\right]$$
$$-\binom{aN+a}{1}\left[\binom{aN+a}{0}\xi_0^{-a(1+a)(N+1)}+\cdots+\binom{aN+1}{aN+a-1}\xi_0^{-a(N+2)}+\binom{aN+a}{aN+a}\xi_0^{-a(N+1)}\right]$$
$$+\binom{aN+2a+1}{2}\left[\binom{aN+2a}{0}\xi_0^{-a(1+a)(N+2)}+\cdots+\binom{aN+2a}{aN+2a-1}\xi_0^{-a(N+3)}+\binom{aN+2a}{aN+2a}\xi_0^{-a(N+2)}\right] \tag{16}$$
$$-\binom{aN+3a+2}{0}\left[\binom{aN+3a}{0}\xi_0^{-a(1+a)(N+3)}+\cdots+\binom{aN+3a}{aN+3a-1}\xi_0^{-a(N+4)}+\binom{aN+3a}{aN+3a}\xi_0^{-a(N+3)}\right]$$
$$+\cdots$$

Summing (16) diagonally from the top right-hand corner and gathering the coefficient of inverse powers of ξ_0 gives

$$\sum_{r=0}^{\infty}\xi_0^{-a(N+r)}\sum_{k=0}^{r}(-1)^{r-k}\binom{a(N+r-k)}{a(N+r-k)-k}\binom{a(N+r-k)+r-k-1}{r-k}. \tag{17}$$

After some lengthy algebra, (16) may be written as

$$\xi_0^{-aN}\left[1+a\sum_{r=1}^{\infty}(-1)^r(1+a)^{r-1}\xi_0^{-ar}\right] = \xi_0^{-aN}\left[\frac{1+\xi_0^a}{(1+a)+\xi_0^a}\right]$$
$$= \xi_0^{-aN+1}\left[\frac{1}{(1+a)\xi_0-a\left(\frac{\xi_0^{1+a}}{1+\xi_0^a}\right)}\right] = \frac{\xi_0^{-aN+1}}{(1+a)\xi_0-ab},$$

which is identical to the right-hand side of (14); hence, the conjecture is proved.

Some numerical results of the conjecture, to five significant digits, are shown in the following table.

n	a	b	ξ_0	Sum and Right-hand Side of (12)
3	3	e	2.83729	20.28791
3	3	$-e$	−2.55538	−20.63241
3	4	1.9	2.01521	6.66073
3	4	−1.9	−2.01521	−6.66073

5. OBSERVATIONS

1. In the special case in which $a = 1$, $b = 1$, the two zeros of (8) are the Golden ratio $\alpha = \xi_0 = (1+\sqrt{5})/2$ and $\beta = \xi_1 = (1-\sqrt{5})/2$ and equation (1) is the Fibonacci sequence. From (10), the familiar relationship
$$f_n = \sum_{r=0}^{[n/2]} \binom{n-ar}{r} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}$$
is obtained.
2. Other parameter values (a, b, c) may be taken so that the solution of (1) may involve known polynomial solutions, such as the Tchebycheff polynomials.
3. In equation (12) the restriction of (n, a) being natural numbers can be relaxed to (n, a) being real numbers, in which case the combinatorial relation would involve Gamma functions.
4. For $n \geq a$, the closed-form expression at (12), namely, $\xi_0^{n+1}/[(1+a)\xi_0 - ab]$ is, in fact, a solution to the difference-delay equation (1); this may be verified by direct substitution.
5. Equation (1) may be extended easily to consider a forcing term of the type $w_n = \binom{n}{m} b^n$, for example, for m and n positive integers.

6. CONCLUSIONS

A technique has been demonstrated whereby closed-form representation of infinite series may be determined. The method described in this paper may be modified and utilized to consider difference-delay equations of higher order, nonhomogeneous difference-delay equations, equations with poles of multiple order, and equations with multiple delay. These variations will be considered by the authors in a forthcoming paper. The authors [2] also considered differential difference equations in which case resulting series were able to be represented in closed form.

ACKNOWLEDGMENTS

The authors would like to acknowledge the useful suggestions of an anonymous referee. Thanks are also due to A. Maligeorges for an excellent job of typing the manuscript.

REFERENCES

1. R. Bellman & K. L. Cooke. *Differential-Difference Equations*. New York: Academic Press, 1963.
2. P. Cerone & A. Sofo. "Summing Series Arising from Integro-Differential-Difference Equations." V.U.T. Technical Report 53 Math 9 (1995).
3. R. L. Graham, D. E. Knuth, & O. Patashnik. *Concrete Mathematics*. New York: Addison-Wesley, 1990.
4. A. Sofo & P. Cerone. "Summation of Series of Binomial Variation." V.U.T. Technical Report 86 Math 13 (1997).
5. H. Takagi. *Queueing Analysis*. Vol. 1. New York: North Holland, 1991.
6. R. Vich. *Z Transforms Theory and Applications*. Boston: D. Reidel, 1987.

AMS Classification Numbers: 05A15, 05A19, 39A10

❖❖❖

GENERAL FIBONACCI SEQUENCES IN FINITE GROUPS

Hüseyin Aydin
Atatürk Üniversitesi, Fen-Edb. Fakültesi, Matematik Bölümü, 25240-Erzurum/Turkey

Ramazan Dikici
Atatürk Üniversitesi, Kazim Karabekir Eğt. Fakültesi, Matematik Bölümü, 25240-Erzurum/Turkey
(Submitted August 1996–Final Revision June 1997)

1. INTRODUCTION

The study of Fibonacci sequences in groups began with the earlier work of Wall [7], where the ordinary Fibonacci sequences in cyclic groups were investigated. Another early contributor to this field was Vinson , who was particularly interested in ranks of apparition in ordinary Fibonacci sequences [6]. In the mid eighties, Wilcox extended the problem to abelian groups [8]. Campbell, Doostie, and Robertson expanded the theory to some finite simple groups [2]. One of the latest works in this area is [1], where it is shown that the lengths of ordinary 2-step Fibonacci sequences are equal to the length of the 2-step Fibonacci recurrences in finite nilpotent groups of nilpotency class 4 and exponent a prime number p. The theory has been generalized in [3] to the ordinary 3-step Fibonacci sequences in finite nilpotent groups of nilpotency class 2 and exponent p.

Definition 1.1: Let $H \lhd G$, $K \lhd G$, and $K \leq H$. If H/K is contained in the center of G/K, then H/K is called a *central factor* of G. A group G is called *nilpotent* if it has finite series of normal subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_r = 1$ such that G_{i-1}/G_i is a central factor of G for each i = 1, 2, ..., r. The smallest possible r is call the *nilpotency class* of G.

Further details about nilpotent groups and related topics can be found in [4].

Let G be a free nilpotent group of nilpotency class 2 and exponent p. G has a presentation $G = \langle x, y, z : x^p = 1, y^p = 1, z^p = 1, z = (y, x) = y^{-1}x^{-1}yx \rangle$. Suppose that we have integers n and m and a recurrence relation in this group given by

$$x_{i-2}^n * x_{i-1}^m = x_i \quad \forall i \in Z.$$

We assume that p does not divide n. Then we get a definition of a 2-step general standard Fibonacci sequence which will be $(0, 1, m, n+m^2, \ldots)$ in $\mathbf{Z}/\mathbf{pZ}$. If p were permitted to divide n, then the sequence ultimately would be periodic, but would never return to the consecutive pair 0, 1. The length of the standard sequence is k, which we call the *Wall number* of the sequence, sometimes called the *fundamental period* of that sequence.

Each element in the group G can be represented uniquely as $x^a y^b z^c$, where $a, b, c \in \mathbf{Z}/\mathbf{pZ}$. The group relations give us a law of composition of standard forms

$$x^a y^b z^c \cdot x^{a'} y^{b'} z^{c'} = x^{a''} y^{b''} z^{c''},$$

where a'', b'', and c'' are given by the following explicit formulas.

We have $a'' = a + a'$, $b'' = b + b'$, and $c'' = c + c' + a'b$. These product laws are discussed in more detail in [1]. In order to study this recurrence, we need a closed formula to describe how to take the next term of the sequence. Let $(x^a y^b z^c)^n$ and $(x^{a'} y^{b'} z^{c'})^m$ be two elements in G. The relevant formulas are

$$(x^a y^b z^c)^n (x^{a'} y^{b'} z^{c'})^m = x^{a''} y^{b''} z^{c''},$$

where

$$a'' = na + ma',$$

$$b'' = nb + mb',$$

and

$$c'' = nc + mc' + mna'b + \frac{(n-1)n}{2}ab + \frac{(m-1)m}{2}a'b'.$$

2. THE MAIN RESULT AND PROOF

Let us use vector notation to calculate the sequence. We put $(1, 0, 0) = (s_{-1}, r_0, t_0)$ which corresponds to x, and $(0, 1, 0) = (s_0, r_1, t_1)$ which corresponds to y. We demonstrate more vectors using the above product formula for c'' as

$$(n, m, 0) = (s_1, r_2, t_2) \text{ and } \left(mn, m^2 + n, mn^2 + \binom{m}{2}mn\right) = (s_2, r_3, t_3).$$

We obtain two sequences (r_i) and (t_i) via our recurrence. Notice that we have $s_i = nr_i$ for each integer i. By induction on j, the j^{th} term of the third component of our sequence of vectors is

$$t_j = mn^2 \sum_{i=0}^{j-1} r_{j-i-1} r_i^2 + \binom{n}{2} n \sum_{i=0}^{j-1} r_{j-i-1} r_i r_{i-1} + \binom{m}{2} n \sum_{i=0}^{j-1} r_{j-i-1} r_i r_{i+1}.$$

Let us denote the period of the general Fibonacci sequence in the group G by $k(G)$.

Theorem 2.1: Let $p > 3$ be a prime number. Then, if G is a nontrivial finite p-group of exponent p and nilpotency class 2, $k(G) = k$. There are four assumptions that we will insert:

a) $n \not\equiv 0 \pmod{p}$,

b) $m + n - 1 \not\equiv 0 \pmod{p}$,

c) $n^2 - m^3 - n - 3mn \not\equiv 0 \pmod{p}$,

d) $3m(m^2 + n) \not\equiv 0 \pmod{p}$.

Proof: Let

$$t_k = mn^2 \sum_{i=0}^{k-1} r_{k-i-1} r_i^2 + \binom{n}{2} n \sum_{i=0}^{k-1} r_{k-i-1} r_i r_{i-1} + \binom{m}{2} n \sum_{i=0}^{k-1} r_{k-i-1} r_i r_{i+1},$$

where $m, n \in \mathbf{Z}/\mathbf{pZ}$, $p > 2$. In order to show $k(G) = k$, we must check that $t_k = t_{k+1} = 0$. The range of all the following sums is the same as above. Since $r_{i+1} = mr_i + nr_{i-1}$, we can recast the last sum to obtain

$$t_k = \left(mn^2 + \binom{m}{2}mn\right)\sum r_{k-i-1} r_i^2 + \left(\binom{n}{2}n + \binom{m}{2}n^2\right)\sum r_{k-i-1} r_i r_{i-1}.$$

We separate this sum to the two parts,

$$\theta_1 = \left(mn^2 + \binom{m}{2}mn\right)\sum r_{k-i-1} r_i^2 \quad \text{and} \quad \theta_2 = \left(\binom{n}{2}n + \binom{m}{2}n^2\right)\sum r_{k-i-1} r_i r_{i-1}.$$

We can pull out factors without difficulty. We put

$$l_1 = mn^2 + \binom{m}{2}mn \quad \text{and} \quad l_2 = \binom{n}{2}n + \binom{m}{2}n^2$$

and then set

$$\phi_1 = \sum r_{k-i-1}r_i^2 \quad \text{and} \quad \phi_2 = \sum r_{k-i-1}r_i r_{i-1}.$$

Now we have $\theta_1 = l_1\phi_1$ and $\theta_2 = l_2\phi_2$, and we are in a position to show that $\phi_1 = 0$ and $\phi_2 = 0$. First, we prove that

$$\phi_2 = \sum r_{k-i-1}r_i r_{i-1} = \sum r_{-(i+1)}r_i r_{i-1} = 0.$$

Now let us show that

$$r_{-i} = (-1)^{i+1}\left(\frac{1}{n}\right)^i r_i.$$

If α and β are the roots of $x^2 - mx - n = 0$, then $\alpha\beta = -n$ and $\alpha + \beta = m$. We have, from the Binet formula,

$$r_i = \frac{\alpha^i - \beta^i}{\alpha - \beta} \quad \text{and} \quad r_{-i} = \frac{\alpha^{-i} - \beta^{-i}}{\alpha - \beta}.$$

We multiply r_{-i} by $(\alpha\beta)^i$ to see that

$$r_{-i} = (-1)^{i+1}\left(\frac{1}{n}\right)^i r_i, \tag{1}$$

and also we have

$$r_{i+1}r_{i-1} = r_i^2 - (-n)^{i-1}. \tag{2}$$

This formula was known to Somer [5]. By using $r_{-(i+1)} = (-1)^i\left(\frac{1}{n}\right)^{i+1} r_{i+1}$ and (2), we obtain

$$\sum r_{-(i+1)}r_i r_{i-1} = \sum (-1)^i\left(\frac{1}{n}\right)^{i+1} r_i^3 + \frac{1}{n^2}\sum r_i.$$

We will prove that $\sum r_i = 0$. Since our recurrence relation is $r_i = mr_{i-1} + nr_{i-2}$, we deduce that $\sum r_i = m\sum r_{i-1} + n\sum r_{i-2}$. Replace $i-1$ by i in the first sum and $i-2$ by i in the second sum on the right side to yield·

$$(m+n-1)\sum r_i = 0. \tag{3}$$

Thus, $\sum r_i = 0$ unless $m+n-1$ is congruent to 0 modulo p. The next step is to show that

$$\sum (-1)^i\left(\frac{1}{n}\right)^{i+1} r_i^3 = 0,$$

so we will be half way through the proof. From the recurrence relation,

$$\sum (-1)^i\left(\frac{1}{n}\right)^{i+1} r_i^3 = \sum (-1)^i\left(\frac{1}{n}\right)^{i+1} (mr_{i-1} + nr_{i-2})^3.$$

We expand this equation to obtain

$$\sum (-1)^i\left(\frac{1}{n}\right)^{i+1} r_i^3 = m^3\sum (-1)^i\left(\frac{1}{n}\right)^{i+1} r_{i-1}^3 + 3m^2n\sum (-1)^i\left(\frac{1}{n}\right)^{i+1} r_{i-1}^2 r_{i-2}$$
$$+ 3mn^2\sum (-1)^i\left(\frac{1}{n}\right)^{i+1} r_{i-1}r_{i-2}^2 + n^3\sum (-1)^i\left(\frac{1}{n}\right)^{i+1} r_{i-2}^3.$$

Replacing $i-1$ by i in the first, second, and third sums, and $i-2$ by i in the last sum on the right side, we obtain

$$\begin{aligned}\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_i^3 = m^3\sum(-1)^{i+1}\left(\frac{1}{n}\right)^{i+2}r_i^3 + 3m^2n\sum(-1)^{i+1}\left(\frac{1}{n}\right)^{i+2}r_i^2r_{i-1} \\ + 3mn^2\sum(-1)^{i+1}\left(\frac{1}{n}\right)^{i+2}r_ir_{i-1}^2 + n^3\sum(-1)^{i+2}\left(\frac{1}{n}\right)^{i+3}r_i^3.\end{aligned} \tag{4}$$

Now we have

$$\left(n-\frac{m^3}{n}-1\right)\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_i^3 + 3mn\sum(-1)^{i+1}\left(\frac{1}{n}\right)^{i+2}r_ir_{i-1}(mr_i+nr_{i-1}) = 0.$$

Using $mr_i + nr_{i-1} = r_{i+1}$ and $r_{i+1}r_{i-1} = r_i^2 - (-n)^{i-1} = r_i^2 + (-1)^i(n)^{i-1}$, we obtain

$$\left(n-\frac{m^3}{n}-1\right)\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_i^3 - 3m\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_i^3 - 3m\sum\frac{1}{n^2}r_i = 0.$$

The last sum is zero by (3). Then we have

$$\left(n-\frac{m^3}{n}-1-3m\right)\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_i^3 = 0. \tag{5}$$

We multiply (5) by n to see that

$$(n^2-m^3-n-3mn)\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_i^3 = 0.$$

Finally, we have

$$\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_i^3 = 0, \tag{6}$$

unless $n^2-m^3-n-3mn$ is congruent to 0 modulo p. We deduce that $\phi_2 = 0$. Hence, we have completed the first part of the proof. Now we prove that the other part of t_k is 0. By (1), write

$$\phi_1 = \sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_{i+1}r_i^2.$$

By (4), we have

$$\begin{aligned}(n^2-m^3-n)\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_i^3 + 3m^2n^2\sum(-1)^{i+1}\left(\frac{1}{n}\right)^{i+2}r_i^2r_{i-1} \\ + 3mn^3\sum(-1)^{i+1}\left(\frac{1}{n}\right)^{i+2}r_ir_{i-1}^2 = 0.\end{aligned}$$

From (6), we have our first linear equation:

$$3m^2n\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_i^2r_{i-1} + 3mn^2\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_ir_{i-1}^2 = 0. \tag{7}$$

Therefore, from the recurrence relation $nr_i = r_{i+2} - mr_{i+1}$ and (6), we get

$$\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_i^3 = \frac{1}{n^3}\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}(r_{i+2}-mr_{i+1})^3 = 0.$$

We exploit this equation to obtain

$$\frac{1}{n^3}\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_{i+2}^3-3\frac{m}{n^3}\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_{i+2}^2r_{i+1}+3\frac{m^2}{n^3}\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_{i+2}r_{i+1}^2$$
$$-\frac{m^3}{n^3}\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_{i+1}^3=0.$$

Replace $i+2$ by i in the first, second, and third sums and $i+1$ by i in the last sum on the left side to see that

$$\frac{1}{n^3}\sum(-1)^{i-2}\left(\frac{1}{n}\right)^{i-1}r_i^3-3\frac{m}{n^3}\sum(-1)^{i-2}\left(\frac{1}{n}\right)^{i-1}r_i^2r_{i-1}+3\frac{m^2}{n^3}\sum(-1)^{i-2}\left(\frac{1}{n}\right)^{i-1}r_ir_{i-1}^2$$
$$-\frac{m^3}{n^3}\sum(-1)^{i-1}\left(\frac{1}{n}\right)^{i}r_i^3=0.$$

The first and last sums vanish by (6). We multiply the equation by n to obtain a second linear equation

$$-3m\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_i^2r_{i-1}+3m^2\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_ir_{i-1}^2=0. \tag{8}$$

Hence, from the linear equations (7) and (8),

$$\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_i^2r_{i-1}=0 \tag{9}$$

and

$$\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_ir_{i-1}^2=0, \tag{10}$$

unless $3mn(m^2+n)$ is congruent to 0 modulo p. Replacing $i-1$ by i in (10),

$$3m(m^2+n)\sum(-1)^i\left(\frac{1}{n}\right)^{i+1}r_{i+1}r_i^2=0.$$

So we have finished the second part of the proof. Therefore, we have $t_k=0$.

Similarly,

$$t_{k+1}=mn^2\sum_{i=0}^{k}r_{k-i}r_i^2+\binom{n}{2}n\sum_{i=0}^{k}r_{k-i}r_ir_{i-1}+\binom{m}{2}n\sum_{i=0}^{k}r_{k-i}r_ir_{i+1}.$$

From (1), we have

$$t_{k+1}=mn^2\sum_{i=0}^{k}(-1)^{i+1}\left(\frac{1}{n}\right)^{i}r_i^3+\binom{n}{2}n\sum_{i=0}^{k}(-1)^{i+1}\left(\frac{1}{n}\right)^{i}r_i^2r_{i-1}+\binom{m}{2}n\sum_{i=0}^{k}(-1)^{i+1}\left(\frac{1}{n}\right)^{i}r_i^2r_{i+1}$$

This is the same as

$$t_{k+1}=mn^2\sum_{i=0}^{k-1}(-1)^{i+1}\left(\frac{1}{n}\right)^{i}r_i^3+\binom{n}{2}n\sum_{i=0}^{k-1}(-1)^{i+1}\left(\frac{1}{n}\right)^{i}r_i^2r_{i-1}+\binom{m}{2}n\sum_{i=0}^{k-1}(-1)^{i+1}\left(\frac{1}{n}\right)^{i}r_i^2r_{i+1}$$
$$+mn^2(-1)^{k+1}\left(\frac{1}{n}\right)^{k}r_k^3+\binom{n}{2}n(-1)^{k+1}\left(\frac{1}{n}\right)^{k}r_k^2r_{k-1}+\binom{m}{2}n(-1)^{k+1}\left(\frac{1}{n}\right)^{k}r_k^2r_{k+1}.$$

The last three terms are zero by the fact that $r_k = 0$ because the period of the sequence r_i is k. The first three sums are zero by exactly the same argument as in the proof of $t_k = 0$. Hence, $t_{k+1} = 0$. To be more explicit, the same restrictions are still valid for $t_{k+1} = 0$. Thus, the proof of Theorem 2.1 is completed.

This result has an obvious interpretation in terms of quotients of groups with presentations similar to those of Fibonacci groups, which is

$$F(2, r, m, n) = \langle x_1, x_2, \ldots, x_r : x_1^n x_2^m x_3^{-1} = 1, x_2^n x_3^m x_4^{-1} = 1, \ldots, x_{r-1}^n x_r^m x_1^{-1} = 1, x_r^n x_1^m x_2^{-1} = 1 \rangle.$$

ACKNOWLEDGMENT

The authors would like to express their appreciation to the anonymous referee for improving the statement and proof of Theorem 2.1 and for making useful suggestions regarding the presentation of this paper.

REFERENCES

1. H. Aydin & G. C. Smith. "Finite p-Quotient of Some Cyclically Presented Groups." *J. London Math. Soc.* **49.2** ;(1994):83-92.
2. C. M. Campbell, H. Doostie, & E. F. Robertson. "Fibonacci Length of Generating Pairs in Groups." *Applications of Fibonacci Numbers* **3**:27-35. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1990.
3. R. Dikici & G. C. Smith. "Recurrences in Finite Groups." *Turkish J. Math.* **19** (1995):321-29.
4. P. Hall. "The Edmonton Notes on Nilpotent Groups." *Queen Mary College Mathematics Notes* (1979).
5. L. Somer. "The Divisibility Properties of Primary Lucas Recurrences with Respect to Primes." *The Fibonacci Quarterly* **18.4** (1980):316-34.
6. J. Vinson. "The Relations of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence." *The Fibonacci Quarterly* **1.1** (1963):37-45.
7. D. D. Wall. "Fibonacci Series Modulo m." *Amer. Math. Monthly* **67** (1960):525-32.
8. H. J. Wilcox. "Fibonacci Sequences of Period n in Groups." *The Fibonacci Quarterly* **24.4** (1986):356-61.

AMS Classification Number: 11B39

❖❖❖

NOTE ON FIBONACCI PRIMALITY TESTING

John Brillhart
University of Arizona, Tucson, AZ 85721
(Submitted August 1996–Final Revision January 1997)

1. INTRODUCTION

One of the most effective ways of proving an integer N is prime is to show first that N is a probable prime, i.e., that $a^{N-1} \equiv 1 \pmod{N}$ for some base a and $1 < a < N-1$, and then to find enough prime factors of $N \pm 1$ so that certain other conditions are satisfied (see [1] for details of such primality tests). The problem of finding these prime factors is, of course, the difficult and time-consuming part of this process, and anything that assists in the factoring of $N \pm 1$ is of great value, particularly when N is large.

In the case of the Fibonacci and Lucas numbers F_n and L_n, we are quite fortunate that identities exist whose form is exactly suited to this purpose. (These were discovered by Jarden [4, pp. 94-95]. Their use in primality testing was first made by the author in the early 1960's—see [4, p. 36].) The identities are all quite simple, asserting that $F_n \pm 1$ and $L_n \pm 1$ are equal to a product of certain Fibonacci and Lucas numbers with subscripts smaller than n, which numbers in turn may well have many known prime factors. Examples of these identities are:

$$F_{4k+1} - 1 = F_k L_k L_{2k+1} \quad \text{and} \quad F_{4k+1} + 1 = F_{2k+1} L_{2k}.$$

With the assistance of this set of identities, many large F_n's and L_n's have been identified as primes [2, p. 255].

In this note we give a collection of similar, but more complicated identities that can be used to establish the primality of the *primitive part* F_k^* of F_k, i.e., the cofactor remaining after the algebraic factors of F_k have been divided out. This cofactor is given by the formula (see [2, p. 252])

$$F_k^* = \prod_{d|k} F_d^{\mu(k/d)}, \quad \mu \text{ the Möbius function.} \tag{1}$$

The subscript of F_k^* in the identities in the present collection has at most two distinct prime divisors, since an identity with three or more prime factors does not in general have a simple multiplicative structure on its right side, i.e., the right side is not just a ratio of products of F_k's and L_k's. The case of two prime divisors is transitional in that some identities have simple multiplicative structure and others do not [see (17) and (18)].

2. THE IDENTITIES

In the proofs that follow, we use elementary Fibonacci and Lucas identities. Also, throughout this note we use the familiar identity $F_{2r} = F_r L_r$ without further mention. In the first two theorems, the subscript of F_k^* is a power of a single prime.

Theorem 1: For $n \geq 3$,

$$F_{2^n}^* - 1 = \frac{L_{3 \cdot 2^{n-2}}}{L_{2^{n-2}}} \tag{2}$$

and

$$F_{2^n}^* + 1 = \frac{F_{3\cdot 2^{n-2}}}{F_{2^{n-2}}}. \tag{3}$$

Proof of (2): Substituting $r = 2^{n-1}$ and $s = 2^{n-2}$ into the identity

$$L_r L_s = L_{r+s} + (-1)^s L_{r-s}, \tag{4}$$

we obtain

$$F_{2^n}^* = \frac{F_{2^n}}{F_{2^{n-1}}} = L_{2^{n-1}} = \frac{L_{3\cdot 2^{n-2}}}{L_{2^{n-2}}} + 1.$$

Proof of (3): Making the same substitution into the identity

$$F_s L_r = F_{r+s} - (-1)^s F_{r-s}, \tag{5}$$

we obtain

$$F_{2^n}^* = L_{2^{n-1}} = \frac{F_{3\cdot 2^{n-2}}}{F_{2^{n-2}}} - 1. \ \square$$

Theorem 2: Let $p \equiv \varepsilon \pmod 4$ be a prime, where $\varepsilon = \pm 1$. Then, for $n \geq 1$,

$$F_{p^n}^* - 1 = \frac{F_{p^{n-1}(p-\varepsilon)/2} L_{p^{n-1}(p+\varepsilon)/2}}{F_{p^{n-1}}} \tag{6}$$

and

$$F_{p^n}^* + 1 = \frac{F_{p^{n-1}(p+\varepsilon)/2} L_{p^{n-1}(p-\varepsilon)/2}}{F_{p^{n-1}}}. \tag{7}$$

Proof of (6): If we substitute $r = p^{n-1}\left(\frac{p-\varepsilon}{2}\right)$ and $s = p^{n-1}\left(\frac{p+\varepsilon}{2}\right)$ into the identity

$$F_{r+s} = F_r L_s - (-1)^s F_{r-s}, \tag{8}$$

and use the fact that $F_{\varepsilon n} = F_n$ for n odd, then we obtain

$$F_{p^n}^* = \frac{F_{p^n}}{F_{p^{n-1}}} = \frac{F_{p^{n-1}(p-\varepsilon)/2} L_{p^{n-1}(p+\varepsilon)/2}}{F_{p^{n-1}}} + 1.$$

Proof of (7): This follows in the same way by setting $r = p^{n-1}\left(\frac{p+\varepsilon}{2}\right)$ and $s = p^{n-1}\left(\frac{p-\varepsilon}{2}\right)$. $\square$

Remarks:

1. For $p = 3$, formulas (6) and (7) have a particularly nice form:

$$F_{3^n}^* - 1 = L_{3^{n-1}}^2 \quad \text{and} \quad F_{3^n}^* + 1 = L_{2\cdot 3^{n-1}}. \tag{9}$$

2. For $p = 5$, formulas (6) and (7) are of not interest here, since $F_{5^n}^*$, $n \geq 2$, has 5 as an intrinsic factor [2, p. 252] and cannot be a prime. The numbers $F_{5^n}^* / 5$ are dealt with in (26).

3. For $p = 7$, formula (6) becomes the interesting formula

$$F_{7^n}^* - 1 = L_{7^{n-1}} L_{2\cdot 7^{n-1}} L_{3\cdot 7^{n-1}}. \tag{10}$$

4. In general, if $N = \frac{1}{2}(F_n^* \pm 1)$ is a probable prime, then $N \mp 1 = \frac{1}{2}(F_n^* \mp 1)$.

In the next theorems, the subscript of F_k^* has two different prime factors.

Theorem 3: Let q be an odd prime, then for $n \geq 1$,

$$F^*_{2q^n} - (-1)^{(q-1)/2} = \frac{5F_{q^{n-1}(q+1)/2}F_{q^{n-1}(q-1)/2}}{L_{q^{n-1}}} \tag{11}$$

and

$$F^*_{2q^n} + (-1)^{(q-1)/2} = \frac{L_{q^{n-1}(q+1)/2}L_{q^{n-1}(q-1)/2}}{L_{q^{n-1}}}. \tag{12}$$

Also, for $m \geq 2$, we have

$$F^*_{2^m q^n} - 1 = \frac{5F_{2^{m-1}q^{n-1}(q+1)/2}F_{2^{m-1}q^{n-1}(q-1)/2}}{L_{2^{m-1}q^{n-1}}} \tag{13}$$

and

$$F^*_{2^m q^n} + 1 = \frac{L_{2^{m-1}q^{n-1}(q+1)/2}L_{2^{m-1}q^{n-1}(q-1)/2}}{L_{2^{m-1}q^{n-1}}}. \tag{14}$$

Proof of (11): Substituting $r = q^{n-1}\left(\frac{q+1}{2}\right)$ and $s = q^{n-1}\left(\frac{q-1}{2}\right)$ into $L_{r+s} = 5F_rF_s + (-1)^s L_{r-s}$, we obtain

$$F^*_{2q^n} = \frac{F_{2q^n}F_{q^{n-1}}}{F_{q^n}F_{2q^{n-1}}} = \frac{L_{q^n}}{L_{q^{n-1}}} = \frac{5F_{q^{n-1}(q+1)/2}F_{q^{n-1}(q-1)/2}}{L_{q^{n-1}}} + (-1)^{(q-1)/2}.$$

Proof of (12): Making the same substitutions as in (11) into (4) leads to

$$F^*_{2q^n} = \frac{L_{q^n}}{L_{q^{n-1}}} = \frac{L_{q^{n-1}(q+1)/2}L_{q^{n-1}(q-1)/2}}{L_{q^{n-1}}} - (-1)^{(q-1)/2}.$$

Proof of (13) and (14): These results are obtained similarly by using $r = 2^{m-1}q^{n-1}\left(\frac{q+1}{2}\right)$ and $s = 2^{m-1}q^{n-1}\left(\frac{q-1}{2}\right)$ as in (11) and (12). □

Theorem 4: If $p < q$, p and q odd primes, then for $m, n \geq 1$,

$$\begin{aligned} F^*_{p^m q^n} - 1 = {} & \frac{5F_{p^{m-1}q^{n-1}}F_{p^{m-1}q^{n-1}(q-1)}F_{p^{m-1}q^{n-1}(q+1)}}{F_{p^m q^{n-1}}} \\ & \cdot \sum_{r=0}^{\frac{p-3}{2}} \frac{(-1)^r p 5^{\frac{p-3}{2}-r}}{p-r}\binom{p-r}{r}\left\{\frac{F^{p-1-2r}_{p^{m-1}q^n} - F^{p-1-2r}_{p^{m-1}q^{n-1}}}{F^2_{p^{m-1}q^n} - F^2_{p^{m-1}q^{n-1}}}\right\}. \end{aligned} \tag{15}$$

Proof: For brevity's sake, put $w = p^{n-1}q^{n-1}$. Then, using the formula (see [5, p. 209, (79)],

$$F_{pn} = \sum_{r=0}^{\frac{p-1}{2}} (-1)^r \frac{p}{p-r}\binom{p-r}{r} 5^{\frac{p-1}{2}-r} F_n^{p-2r}, \; n \text{ odd}, \tag{16}$$

we have that

$$
\begin{aligned}
&F_w F_{pqw} - F_{qw} F_{pw} \\
&= F_w \sum_{r=0}^{\frac{p-1}{2}} (-1)^r \frac{p}{p-r}\binom{p-r}{r} 5^{\frac{p-1}{2}-r} F_{qw}^{p-2r} - F_{qw} \sum_{r=0}^{\frac{p-1}{2}} (-1)^r \frac{p}{p-r}\binom{p-r}{r} 5^{\frac{p-1}{2}-r} F_w^{p-2r} \\
&= 5F_{qw}F_w \sum_{r=0}^{\frac{p-3}{2}} (-1)^r \frac{p}{p-r}\binom{p-r}{r} 5^{\frac{p-3}{2}-r} (F_{qw}^{p-1-2r} - F_w^{p-1-2r}) \\
&= 5F_{qw}F_w (F_{qw}^2 - F_w^2) \sum_{r=0}^{\frac{p-3}{2}} (-1)^r \frac{p}{p-r}\binom{p-r}{r} 5^{\frac{p-3}{2}-r} \left\{ \frac{F_{qw}^{p-1-2r} - F_w^{p-1-2r}}{F_{qw}^2 - F_w^2} \right\}.
\end{aligned}
$$

But, using the identity $F_{km}^2 - (-1)^{k(m-1)} F_k^2 = F_{k(m+1)} F_{k(m-1)}$ with $k = w$ and $m = q$, we have

$$
\begin{aligned}
&F_w F_{pqw} - F_{qw} F_{pw} \\
&\quad = 5F_{qw}F_w F_{w(q-1)} F_{w(q+1)} \sum_{r=0}^{\frac{p-3}{2}} (-1)^r \frac{p}{p-r}\binom{p-r}{r} 5^{\frac{p-3}{2}-r} \left\{ \frac{F_{qw}^{p-1-2r} - F_w^{p-1-2r}}{F_{qw}^2 - F_w^2} \right\}.
\end{aligned}
$$

Thus,

$$
\begin{aligned}
F_{pqw}^* - 1 &= \frac{F_{pqw}F_w - F_{qw}F_{pw}}{F_{qw}F_{pw}} \\
&= \frac{5F_w F_{w(q-1)} F_{w(q+1)}}{F_{pw}} \sum_{r=0}^{\frac{p-3}{2}} (-1)^r \frac{p}{p-r}\binom{p-r}{r} 5^{\frac{p-3}{2}-r} \left\{ \frac{F_{qw}^{p-1-2r} - F_w^{p-1-2r}}{F_{qw}^2 - F_w^2} \right\}. \quad \square
\end{aligned}
$$

It is worth while to give some special cases.

Corollary 5: If q is a prime, then for $m, n \geq 1$,

$$
F_{3^m q^n}^* - 1 = \frac{5F_{3^{m-1}q^{n-1}} F_{3^{m-1}q^{n-1}(q-1)} F_{3^{m-1}q^{n-1}(q+1)}}{F_{3^m q^{n-1}}}, \quad q \geq 5, \tag{17}
$$

and for $q \geq 7$,

$$
F_{5^m q^n}^* - 1 = \frac{25F_{5^{m-1}q^{n-1}} F_{5^{m-1}q^{n-1}(q-1)} F_{5^{m-1}q^{n-1}(q+1)}}{F_{5^m q^{n-1}}} (F_{5^{m-1}q^n}^2 + F_{5^{m-1}q^{n-1}}^2 - 1). \tag{18}
$$

The following are some further simple cases. Here q is a prime.

$$
F_{3q}^* - 1 = \frac{5}{2} F_{q-1} F_{q+1}, \quad q \geq 5, \tag{19}
$$

$$
F_{5q}^* - 1 = 5F_{q-1} F_q^2 F_{q+1}, \quad q \geq 7, \tag{20}
$$

and

$$
F_{7q}^* - 1 = \frac{5}{13} F_{q-1} F_{q+1} (25F_q^4 - 10F_q^2 + 4), \quad q \geq 11. \tag{21}
$$

The next is a formula containing a "+1". From numerical evidence, there seem to be few identities with a "+" that have a right side with a multiplicative structure.

Theorem 6: If $q \geq 5$ is a prime, then

$$F_{3q}^* + 1 = \frac{L_{3q}}{2L_q}. \tag{22}$$

Proof: Using $F_{3r} = F_r(5F_r^2 + (-1)^r 3)$ and $L_{3r} = L_r(5F_r^2 + (-1)^r)$, we find that $L_q(F_{3q} + 2F_q) = L_qF_q(5F_q^2 - 3) + 2F_qL_q = F_qL_q(5F_q^2 - 1) = F_qL_{3q}$. Thus,

$$F_{3q}^* + 1 = \frac{F_{3q}}{F_3F_q} + 1 = \frac{F_{3q} + 2F_q}{2F_q} = \frac{L_{3q}}{2L_q}. \quad \square$$

Some Examples: We consider the factorizations leading to proofs of the primality of the probable primes F_{145}^*, F_{2285}^*, and F_{14203}^*. In the first, we have

$$F_{145}^* = F_{5\cdot 29}^* = \frac{F_{145}}{F_5F_{29}} = 349619996930737079890201.$$

Then, by (20) and Tables 2 and 3 in [2], we find the complete factorization:

$$\begin{aligned} F_{5\cdot 29}^* - 1 &= 5F_{28}F_{29}^2F_{30} = 5(L_{14}L_7F_7)F_{29}^2(L_{15}F_{15}) \\ &= 5(3\cdot 281\cdot 29\cdot 13)(514229^2)(2^2\cdot 11\cdot 31\cdot 2\cdot 5\cdot 61). \end{aligned}$$

In the second, identity (20) gives

$$\begin{aligned} F_{2285}^* - 1 = F_{5\cdot 457}^* - 1 &= 5F_{456}F_{457}^2F_{458} \\ &= 5(L_{228}L_{114}L_{57}F_{57})F_{457}^2(L_{229}F_{229}), \end{aligned}$$

each factor of which is again completely factored using the tables in [2]. The primality of F_{145}^* and F_{2285}^* is established, respectively, from these complete factorizations using Theorem 1 in [1].

In the third, identity (21) is used to obtain

$$\begin{aligned} F_{14203}^* - 1 = F_{7\cdot 2029}^* - 1 &= \frac{5}{13}F_{2028}F_{2030}G \\ &= \frac{5}{13}(L_{1014}L_{507}F_{507})(L_{1015}F_{1015})G, \end{aligned}$$

where $G = 25F_{2029}^4 - 10F_{2029}^2 + 4$. As it happens, all the F_k's and L_k's can be factored completely and G is partially factored as $G = 7\cdot 2629093\cdot 47472487\cdot c$, where c is a 1682-digit composite cofactor. Since the logarithm of the product of the 64 known prime factors in these factorizations (counting multiplicity) is about 33.9% of the 2544-digit number F_{14203}^*, the "cube root" Theorem 5 in [1] can be used to establish the primality of this number. Fourteen of these factors have more than 20 digits.

For another example, see [3, §4], where (18) is used in the primality proof of the 1137-digit probable prime F_{7225}^*. A final example is the probable prime F_{4849}^*, for which not enough prime factors have been discovered to complete a primality proof. I would like to thank W. Keller for suggesting the above examples and for sending me information about them.

The next theorem deals with those F_n^*'s that have an intrinsic factor, which is divided out of the primitive part. Only the first power of an intrinsic factor can divide the primitive part.

Theorem 7: We have

$$\frac{F^*_{3\cdot 2^n}}{2} - 1 = \frac{1}{2} L_{2^{n-1}-1} L_{2^{n-1}+1}, \quad n \geq 2, \tag{23}$$

$$\frac{F^*_{3\cdot 2^n}}{2} + 1 = \prod_{k=1}^{n-1} F^*_{3\cdot 2^k} \quad n \geq 2, \tag{24}$$

$$\frac{F^*_{4\cdot 3^n}}{3} + 1 = \frac{1}{3} L^2_{2\cdot 3^{n-1}}, \quad n \geq 1, \tag{25}$$

$$\frac{F^*_{5^n}}{5} - 1 = 5F_{5^{n-1}-1} F^2_{5^{n-1}} F_{5^{n-1}+1}, \quad n \geq 2, \tag{26}$$

$$\frac{F^*_{8\cdot 7^n}}{7} + 1 = \frac{1}{7} L^2_{4\cdot 7^{n-1}} (L^4_{4\cdot 7^{n-1}} - 7L^2_{4\cdot 7^{n-1}} + 14), \quad n \geq 1. \tag{27}$$

Proof of (23) and (24): Using $L_{3r} = L_r(L_{2r} - (-1)^r)$ and $L_{2r} = L_r^2 - (-1)^r 2$, we have

$$F^*_{3\cdot 2^n} = \frac{F_{3\cdot 2^n} F_{2^{n-1}}}{F_{3\cdot 2^{n-1}} F_{2^n}} = \frac{L_{3\cdot 2^{n-1}}}{L_{2^{n-1}}} = L_{2^n} - 1 = L^2_{2^{n-1}} - 3. \tag{28}$$

Now, from $L_r^2 - (-1)^r 5 = L_{r-1} L_{r+1}$, we have $F^*_{3\cdot 2^n} - 2 = L^2_{2^{n-1}} - 5 = L_{2^{n-1}-1} L_{2^{n-1}+1}$, from which the identity follows.

Also, from the equalities in (28), we have

$$\begin{aligned}\frac{1}{2}(F^*_{3\cdot 2^n} + 2) &= \frac{1}{2}(L_{2^n} + 1) = \frac{1}{2}(L^2_{2^{n-1}} - 1) = \frac{1}{2}(L_{2^{n-1}} - 1)(L_{2^{n-1}} + 1) \\ &= \frac{1}{2}(L_{2^{n-1}} - 1)(L^2_{2^{n-2}} - 1) = \cdots = \frac{1}{2}(L_2^2 - 1)\sum_{k=2}^{n-1}(L_{2^k} - 1) = 4\sum_{k=2}^{n-1} F^*_{3\cdot 2^k} = \sum_{k=1}^{n-1} F^*_{3\cdot 2^k}.\end{aligned}$$

Proof of (25): Using $L_{3r} = L_r(L_r^2 - (-1)^r 3)$, we find that

$$F^*_{4\cdot 3^n} = \frac{F_{4\cdot 3^n} F_{2\cdot 3^{n-1}}}{F_{2\cdot 3^n} F_{4\cdot 3^{n-1}}} = \frac{L_{2\cdot 3^n}}{L_{2\cdot 3^{n-1}}} = L^2_{2\cdot 3^{n-1}} - 3,$$

which implies the result.

Proof of (26): From (16), we obtain the formula $F_{5r} = 5F_r(5F_r^4 - 5F_r^2 + 1)$, so

$$\frac{F^*_{5^n}}{5} - 1 = \frac{F_{5^n}}{5F_{5^{n-1}}} - 1 = 5F^2_{5^{n-1}}(F^2_{5^{n-1}} - 1) = 5F^2_{5^{n-1}} F_{5^{n-1}-1} F_{5^{n-1}+1},$$

using $F_r^2 + (-1)^r = F_{r-1} F_{r+1}$.

Proof of (27): From [4, p. 212, (86)],

$$L_{pn} = \sum_{r=0}^{\frac{p-1}{2}} (-1)^r \frac{p}{p-r} \binom{p-r}{r} L_n^{p-2r}, \quad n \text{ odd},$$

so $L_{7n} = L_n(L_n^6 - 7L_n^4 + 14L_n^2 - 7)$. Thus,

$$F^*_{8\cdot 7^n} = \frac{F_{8\cdot 7^n} F_{4\cdot 7^{n-1}}}{F_{4\cdot 7^n} F_{8\cdot 7^{n-1}}} = \frac{L_{4\cdot 7^n}}{L_{4\cdot 7^{n-1}}} = L^6_{4\cdot 7^{n-1}} - 7L^4_{4\cdot 7^{n-1}} + 14L^2_{4\cdot 7^{n-1}} - 7,$$

from which the identity follows. □

Remark: Numerical evidence suggests that, for $n \geq 2$, there are no multiplicative formulas for the even integers $N_1 = (F^*_{4\cdot 3^n}/3) - 1$ and $N_2 = (F^*_{5^n}/5) + 1$. On the other hand, if $\frac{1}{2}N_1$ or $\frac{1}{2}N_2$ should be probable primes, then the following formulas, which relate back to (24) and (25), might be useful in establishing their primality:

$$\frac{1}{2}N_1 + 1 = \frac{1}{2}\left(\frac{F^*_{4\cdot 3^n}}{2} + 1\right) \quad \text{and} \quad \frac{1}{2}N_2 - 1 = \frac{1}{2}\left(\frac{F^*_{5^n}}{5} - 1\right).$$

There are some other formulas involving F^*_n and L^*_n of various kinds, but these will not be considered here.

We conclude this note by observing that the identities used in the proofs, such as those in (4), (5), and (8), each contain the factor $(-1)^s$, which becomes the ± 1 in the identity for $F^*_n \pm 1$. In general Lucas sequences, of which the pair $\{F_n\}_{n=0}^{\infty}$ and $\{L_n\}_{n=0}^{\infty}$ is a special case, this factor is Q^s. Thus, the other Lucas sequences that have formulas like those in this note are those for which $|Q| = 1$ (see [1, p. 627]).

REFERENCES

1. J. Brillhart, D. H. Lehmer, & J. L. Selfridge. "New Primality Criteria and Factorizations of $2^m \pm 1$." *Math. of Comp.* **29.130** (1975):620-47.
2. J. Brillhart, P. L. Montgomery, & R. D. Silverman. "Tables of Fibonacci and Lucas Factorizations." *Math. of Comp.* **50.181** (1988):251-60; S1-S15.
3. H. Dubner & W. Keller. "New Fibonacci and Lucas Primes." *Math. of Comp.*, to appear.
4. D. Jarden. *Recurring Sequences*. 3rd ed. Jerusalem: Riveon Lematematika, 1973.
5. E. Lucas. "Ṭhéorie des fonctions numériques simplement périodiques." *Amer. J. Math.* **1.1** (1878):184-240; 289-321.

AMS Classification Numbers: 11A51, 11B39

❖❖❖

POWER DIGRAPHS MODULO n

Brad Wilson
2030 State Street #5, Santa Barbara, CA 93105
(Submitted August 1996-Final Revision October 1996)

1. INTRODUCTION

A directed graph, or digraph, is a finite set of vertices together with directed edges. A closed trail of a digraph in which no vertices are repeated is a cycle. A tree is an acyclic connected digraph and a forest is an acyclic graph (thus a forest is made up of trees) [1].

Starting with the elements of $\mathbb{Z}_n$ as our set of vertices, we can create a digraph associated to any function f modulo n by having an edge from vertex b_1 to vertex b_2 if $f(b_1) \equiv b_2 \pmod{n}$. This digraph reflects properties of $\mathbb{Z}_n$ and f.

Digraphs arising when $f(x) = x^2$ have been studied in [2] and [5]. More recently, digraphs arising from $f(x) = x^k$ and n a prime have been studied in [4]. In this article we study digraphs arising from $f(x) = x^k$ and arbitrary $n \in \mathbb{N}$.

If $n = 2^a \prod_{i=1}^{m} p_i^{a_i}$ with $a_i \geq 1$, $a \geq 0$, define

$$\delta_1 = \begin{cases} 0 & \text{if } a = 0, 1, \\ 1 & \text{if } a \geq 2, \end{cases} \qquad \delta_2 = \begin{cases} 0 & \text{if } a < 3, \\ 1 & \text{if } a \geq 3, \end{cases}$$

and

$$L = \operatorname{lcm}(2^{\delta_1}, 2^{\delta_2(a-2)}, p_1^{a_1-1}(p_1 - 1), \ldots, p_m^{a_m-1}(p_m - 1)).$$

We use L to determine when two digraphs are equal (Theorem 1). Define G_n^k (resp. $G_n^{k^*}$) as the graph whose vertices are elements of $\mathbb{Z}_n$ (resp. $\mathbb{Z}_n^*$) with an edge from b_1 to b_2 if $b_1^k \equiv b_2 \pmod{n}$.

Our principal results on $G_n^{k^*}$ are:

(1) Determine when $G_n^{k_1^*} = G_n^{k_2^*}$ (Theorem 1).

(2) Show that elements in a cycle have the same order, d, and determine the cycle length, $\ell(d)$, based on that order (Theorem 2).

(3) Derive a formula for the number of cycles of order d (Theorem 3).

(4) Show that the trees of all cycle vertices are isomorphic (Theorem 4) and derive a formula for the height of these trees (Theorem 5).

We handle $G_n^k - G_n^{k^*}$ by showing that well-defined parts of this graph are isomorphic to corresponding $G_{n'}^{k}$'s (Theorem 6). Finally, we use these well-defined parts and a result about the number of solutions to congruences (Theorem 7) to fill in the whole of G_n^k.

2. BACKGROUND RESULTS

The following facts will be used in Sections 3 and 4. Facts 1, 2, and 3 are from [3].

Fact 1 (Chinese Remainder Theorem). If $(m_i, m_j) = 1$ $(1 \leq i < j \leq n)$, then the simultaneous congruences $x \equiv a_i \pmod{m_i}$, $1 \leq i \leq n$, have a unique solution mod $m_1 m_2 \ldots m_n$.

Fact 2. A necessary and sufficient condition for m to have a primitive root is that $m = 2$, 4, p^ℓ, or $2p^\ell$, where p is an odd prime.

Fact 3. Let $\ell > 2$. Then the order of 5 with respect to the modulus 2^ℓ is $2^{\ell-2}$.

Fact 4. For p an odd prime either the congruence $x^k \equiv b \pmod{p^m}$, $p \nmid b$ has 0 or $(k, p^{m-1}(p-1))$ solutions. The number of solutions of $x^k \equiv b \pmod{2^a}$ is 0 or $(2, k)^{\delta_1}(2^{a-2}, k)^{\delta_2}$.

Proof: If p is an odd prime, Fact 2 says $\mathbb{Z}^*_{p^m} \cong \mathbb{Z}_{p^{m-1}(p-1)}$. Multiplication in $\mathbb{Z}^*_{p^m}$ corresponds to addition in $\mathbb{Z}_{p^{m-1}(p-1)}$, so x^k corresponds to kx. The map

$$\lambda_k : \mathbb{Z}_{p^{m-1}(p-1)} \to \mathbb{Z}_{p^{m-1}(p-1)} \text{ such that } \lambda_k(x) = kx$$

is a $(k, p^{m-1}(p-1))$-to-one map, so an element in $\mathbb{Z}_{p^{m-1}(p-1)}$ is either the image of $(k, p^{m-1}(p-1))$ elements or none.

For modulus 2^a, Fact 3 says $\mathbb{Z}^*_{2^a} \cong \mathbb{Z}_2^{\delta_1} \times \mathbb{Z}_{2^{a-2}}^{\delta_2}$. In $\mathbb{Z}_2^{\delta_1} \times \mathbb{Z}_{2^{a-2}}^{\delta_2}$, the multiplication by k map is $(2, k)^{\delta_1}(2^{a-2}, k)^{\delta_2}$-to-one, giving our result. □

Fact 5. In $\mathbb{Z}_m$, the cyclic group of order m, there exists an element of order ℓ if and only if $\ell | m$. Further, if there exists an element of order ℓ, then there exist exactly $\phi(\ell)$ of them.

Proof: If $\ell \nmid m$, then Lagrange's Theorem says there is no element of order ℓ.

If $\ell | m$, then $m = \ell u$. For b an element of order m, we have $\ell(ub) = (\ell u)b = mb = \overline{0}$. Further, if $\ell' < \ell$ such that $\ell'(ub) = \overline{0}$, then $m | (\ell' u)$, but $\ell' u < m$, a contradiction, so ub is of order ℓ.

Finally, we need to count the number of elements of order ℓ if there is at least one. For b of order m, we know $\text{ord}(vb) = m/(v, m)$, so we get an element of order ℓ if and only if $u = (v, m)$. Since $u | m$, we know v must be a multiple of u, but $u = (v'u, m)$ if and only if $1 = (v', \ell)$. There are $\phi(\ell)$ such values of v'. □

Fact 6. For $(m_1, m_2) = 1$, we have

$$\mathbb{Z}^*_{m_1 m_2} \cong \mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2}.$$

Proof: The map $\rho : \mathbb{Z}^*_{m_1 m_2} \to \mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2}$ defined by $\rho(x) = (x \pmod{m_1},\ x \pmod{m_2})$ is easily shown to be a homomorphism. It is an isomorphism since Fact 1 allows us to define a map which is the inverse:

$$\rho^{-1} : \mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2} \to \mathbb{Z}^*_{m_1 m_2} \text{ such that } \rho^{-1}(x, y) = z,$$

where $z \equiv x \pmod{m_1}$, $z \equiv y \pmod{m_2}$. □

Facts 2 and 3 tell us the structure of $\mathbb{Z}^*_{p^\ell}$:

$$\mathbb{Z}^*_{p^\ell} \cong \begin{cases} \{\overline{1}\}, & \text{for } p = 2,\ \ell = 1, \\ \mathbb{Z}_2, & \text{for } p = 2,\ \ell = 2, \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{\ell-2}}, & \text{for } p = 2,\ \ell \geq 3, \\ \mathbb{Z}_{p^{\ell-1}(p-1)}, & \text{for } p \text{ an odd prime.} \end{cases} \tag{1}$$

From the structure of $\mathbb{Z}^*_{p^\ell}$ and Fact 6 follows the structure for $\mathbb{Z}^*_n$. If $n = 2^a \prod_{i=0}^{m} p_i^{a_i}$, then

$$\mathbb{Z}^*_n \cong \mathbb{Z}^*_{2^a} \times \mathbb{Z}^*_{p_1^{a_1}} \times \cdots\cdots \mathbb{Z}_{p_m^{a_m}} \cong \mathbb{Z}_2^{\delta_1} \times \mathbb{Z}_{2^{a-2}}^{\delta_2} \times \mathbb{Z}_{p_1^{a_1-1}(p_1-1)} \times \cdots \times \mathbb{Z}_{p_m^{a_m-1}(p_m-1)}. \tag{2}$$

Fact 7. In the group $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$, there are $(m_1, d)(m_2, d) \ldots (m_r, d)$ elements of order dividing d.

Proof: Since the order of $(x_1, x_2, \ldots, x_r)$ is the least common multiple of the orders of the x_i's, it is sufficient to show there are (m_i, d) elements of order dividing d in $\mathbb{Z}_{m_i}$. $\mathbb{Z}_{m_i}$ is cyclic of order m_i, so if $b \mid m_i$, there are $\phi(b)$ elements of order exactly b. If $b \nmid m_i$, there are no elements of order b. The number of elements of order dividing d is thus

$$\sum_{b \mid d,\, b \mid m_i} \phi(b) = \sum_{b \mid (d, m_i)} \phi(b) = (d, m_i)$$

by a famous property of the Euler-ϕ function (e.g., [3], Exercise 1, Section 2.5). □

3. STRUCTURE OF $G_n^{k^*}$

G_n^k is, by definition, the digraph whose vertices are the elements of $\mathbb{Z}_n$ and with an edge from b_1 to b_2 if $b_1^k \equiv b_2 \pmod{n}$. Since $b_1^k \pmod{n}$ is well defined for any given b_1, k and n, the outdegree of any vertex in our digraph is one. Since the outdegree from any vertex is one, we know that each component of G_n^k contains at most one cycle. Since there are only finitely many vertices, it is clear that from any starting point iteration of the k^{th} power map eventually leads to a cycle, so each component contains exactly one cycle. The vertices in a component outside the unique cycle are thus acyclic and form a forest.

If $p \mid n$ is a prime and $p \mid b$, then $p \mid b^k$, so $p \mid (b^k \pmod{n})$. If $p \nmid b$, then $p \nmid b^k$, so $p \nmid (b^k \pmod{n})$. This says, if $n = 2^a p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$, there are at least 2^m components, at least 2^{m+1} if $a \neq 0$. In particular, we will examine the components with vertices relatively prime to n separately from those with vertices not relatively prime to n.

Recall that $G_n^{k^*}$ was defined to be the digraph with the elements of $\mathbb{Z}_n^*$ as vertices and an edge from b_1 to b_2 if $b_1^k \equiv b_2 \pmod{n}$. By the last paragraph, we can study this graph independently of the vertices not relatively prime to n. We start our study with a lemma on $\psi(d)$, the number of elements in $\mathbb{Z}_n^*$ of order d.

Lemma 1: If $n = 2^a \prod_{i=1}^m p_i^{a_i}$ and $\psi(d)$ denotes the number of elements of order d in $\mathbb{Z}_n^*$, then

$$\psi(d) = (2, d)^{\delta_1} (2^{a-2}, d)^{\delta_2} \prod_{i=1}^{m} (d, p_i^{a_i - 1}(p_i - 1)) - \sum_{\delta \mid d,\, \delta \neq d} \psi(\delta).$$

Proof: From Fact 7 and (2), we know the number of elements of order dividing d is $(2, d)^{\delta_1} (2^{a-2}, d)^{\delta_2} \prod_{i=1}^m (d, p_i^{a_i - 1}(p_i - 1))$, i.e.,

$$\sum_{\delta \mid d} \psi(\delta) = (2, d)^{\delta_1} (2^{a-2}, d)^{\delta_2} \prod_{i=1}^{m} (d, p_i^{a_i - 1}(p_i - 1)).$$

Solving this for $\psi(d)$ gives the result. □

The following results are analogs of results 11 through 14 of [4].

Lemma 2: The indegree of any vertex in $G_n^{k^*}$ is 0 or $(2, k)^{\delta_1} (2^{a-2}, k)^{\delta_2} \prod_{i=1}^m (k, p_i^{a_i - 1}(p_i - 1))$.

Proof: $\mathbb{Z}_n^* \cong \mathbb{Z}_2^{\delta_1} \times \mathbb{Z}_{2^{a-2}}^{\delta_2} \times \mathbb{Z}_{p_1^{a_1-1}(p_1-1)} \times \cdots \times \mathbb{Z}_{p_m^{a_m-1}(p_m-1)}$. For $b \in \mathbb{Z}_n^*$, $x^k \equiv b \pmod{n}$ is equivalent to

$$\begin{aligned} x^k &\equiv b \pmod{2^a}, \\ x^k &\equiv b \pmod{p_1^{a_1}}, \\ &\vdots \\ x^k &\equiv b \pmod{p_m^{a_m}}. \end{aligned} \tag{3}$$

By Fact 4 we know that, for p odd, $x^k \equiv b \pmod{p_i^{a_i}}$ has 0 or $(k, p_i^{a_i-1}(p_i-1))$ solutions and, for modulus 2^a, there are 0 or $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}$ solutions. Taken together, the system (3) thus has 0 or $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}\prod_{i=1}^{m}(k, p_i^{a_i-1}(p_i-1))$ solutions. □

Corollary 1: Every component of $G_n^{k^*}$ is cyclic if and only if $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}=1$ and $(k, p_i^{a_i-1}(p_i-1))=1$ for all i.

Proof: If a component of $G_n^{k^*}$ is cyclic, then every indegree must be 1. By Lemma 2, this says $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}\prod_{i=1}^{m}(k, p_i^{a_i-1}(p_i-1))=1$, so each factor must be 1.

Conversely, if $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}=1$ and $(k, p_i^{a_i-1}(p_i-1))=1$ for each i, then Lemma 2 says the indegree of any vertex must be 0 or 1. Since each outdegree is 1 and the sum of the indegrees and outdegrees must be equal, this forces each indegree to be 1, so every component is cyclic. □

Corollary 2: Any cycle vertex has $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}\left(\prod_{i=1}^{m}(k, p_i^{a_i-1}(p_i-1))\right)-1$ noncycle parents.

Proof: If b is a cycle vertex, the indegree is at least one because it has a cycle vertex parent. By Lemma 2, the indegree of b is $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}\prod_{i=1}^{m}(k, p_i^{a_i-1}(p_i-1))$. Since exactly one of b's parents is a cycle vertex, there are

$$(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}\left(\prod_{i=1}^{m}(k, p_i^{a_i-1}(p_i-1))\right)-1$$

noncycle parents. □

Theorem 1: $k_1 \equiv k_2 \pmod{L}$ if and only if $G_n^{k_1^*} = G_n^{k_2^*}$.

Proof: Since $\mathbb{Z}_n^* \cong \mathbb{Z}_2^{\delta_1} \times \mathbb{Z}_{2^{a-2}}^{\delta_2} \times \mathbb{Z}_{p_1^{a_1-1}(p_1-1)} \times \cdots \times \mathbb{Z}_{p_m^{a_m-1}(p_m-1)}$, all elements have orders dividing L and we know that there exists an element of this order, namely, $(\overline{1}, \overline{1}, \ldots, \overline{1})$.

If $k_1 \equiv k_2 \pmod{L}$, then for any $b \in \mathbb{Z}_n^*$, $b^{k_1} \equiv b^{k_2+d\cdot L} \equiv b^{k_2} \pmod{n}$.

Conversely, if $G_n^{k_1^*} = G_n^{k_2^*}$, then $b^{k_1} \equiv b^{k_2} \pmod{n}$ for all $b \in \mathbb{Z}_n^*$. This means $\mathrm{ord}_n b \mid (k_1 - k_2)$. Since there is an element of order L, we get $k_1 \equiv k_2 \pmod{L}$. □

We now classify whether an element of a given order will be in a tree or cycle. First, we fix notation: factor $L = tw$ for t the largest factor relatively prime to k.

Lemma 3: The vertex b is a cycle vertex if and only if $(\mathrm{ord}_n b) \mid t$.

Proof: If b is a cycle vertex, then there is some ℓ such that $b^{k^\ell} \equiv b \pmod{n}$. We assume ℓ is the minimal natural number with this property. Since $b^{k^\ell - 1} \equiv 1 \pmod{n}$, we know that

$(\text{ord}_n b)|(k^\ell - 1)$, so $(\text{ord}_n b, k) = 1$ and $(\text{ord}_n b, w) = 1$. Since $(\text{ord}_n b)|L$, we have $(\text{ord}_n b)|tw$, so $(\text{ord}_n b)|t$.

Conversely, if $(\text{ord}_n b)|t$, then $b^t \equiv 1 \pmod n$, so $(t, k) = 1$ implies there exists $\ell > 0$ so that $k^\ell \equiv 1 \pmod t$. This means $b^{k^\ell - 1} \equiv 1 \pmod n$, so $b^{k^\ell} \equiv b \pmod n$, so b is a cycle vertex. □

An immediate corollary of this classification is a count of the number of cycle vertices in $G_n^{k^*}$.

Corollary 3: There are $(2, t)^{\delta_1}(2^{a-2}, t)^{\delta_2} \prod_{i=1}^{m}(t, p_i^{a_i-1}(p_i - 1))$ cycle vertices.

Proof: By Lemma 3, we are counting the number of elements of $\mathbb{Z}_n^*$ of order dividing t. By (2) and Fact 7, there are $(2, t)^{\delta_1}(2^{a-2}, t)^{\delta_2} \prod_{i=1}^{m}(t, p_i^{a_i-1}(p_i - 1))$ elements of order dividing t. □

The following result gives a connection between cycle vertices in the same cycle.

Lemma 4: Vertices in the same cycle have the same order modulo n.

Proof: It is enough to show that consecutive vertices in a cycle have the same order. Suppose $b_2 \equiv b_1^k \pmod n$. If $\text{ord}_n b_1 = \ell_1$ and $\text{ord}_n b_2 = \ell_2$, then $b_2^{\ell_1} \equiv (b_1^k)^{\ell_1} \equiv (b_1^{\ell_1})^k \equiv 1^k \equiv 1 \pmod n$. This means $\ell_2 | \ell_1$, so

$$\text{ord}_n b_1 \geq \text{ord}_n b_2 = \text{ord}_n(b_1^k) \geq \text{ord}_n(b_1^{(k^2)}) \geq \cdots \geq \text{ord}_n(b_1^{(k^\ell)}) = \text{ord}_n b_1.$$

This forces all the inequalities to be equalities, so the orders of all elements in the same cycle are equal. □

By Lemma 4, it makes sense to speak of the order of a cycle. The next result relates the order and length of a cycle.

Theorem 2: The length $\ell(d)$ of a cycle of order d is the smallest natural number ℓ such that $d|(k^\ell - 1)$, i.e., $\ell(d) = \text{ord}_d k$.

Proof: If $\ell(d)$ denotes the cycle length and b is a cycle vertex, then $b \not\equiv b^{(k^i)} \pmod n$ for any $i < \ell(d)$, but $b \equiv b^{(k^{\ell(d)})} \pmod n$. Stated differently, $b^{(k^i - 1)} \not\equiv 1 \pmod n$ for any $i < \ell(d)$, but $b^{(k^{\ell(d)} - 1)} \equiv 1 \pmod n$. Since $\text{ord}_n b = d$, this says $d \nmid (k^i - 1)$ for any $i < \ell(d)$ but $d|(k^{\ell(d)-1})$. □

We can use Theorem 2 to get the length of the longest cycle in $G_n^{k^*}$.

Corollary 4: The longest cycle in $G_n^{k^*}$ has length $\ell(t) = \text{ord}_t k$.

Proof: By Lemma 3, the order modulo n of every cycle vertex divides t. Further, there exists a cycle vertex of order t. Since, for any $d|t$, we have $k^{\ell(t)} \equiv 1 \pmod t$ implies $k^{\ell(t)} \equiv 1 \pmod d$, Theorem 2 says $\ell(t) = \text{ord}_t k \geq \text{ord}_d k = \ell(d)$. Therefore, the greatest cycle length is $\ell(t) = \text{ord}_t k$. □

The following theorem gives the number of cycles in $G_n^{k^*}$ of a given order.

Theorem 3: The number of cycles of order d in $G_n^{k^*}$ is $\psi(d) / \ell(d)$.

Proof: There are, by definition, $\psi(d)$ elements in $\mathbb{Z}_n^*$ of order d. Each is in a cycle of length $\ell(d)$ containing only elements of order d, so

$$\frac{\psi(d)}{\ell(d)} = \frac{\text{number of vertices of order } d}{\text{number of vertices of order } d \text{ per cycle of order } d}$$

$$= \text{number of cycles of order } d. \ \square$$

Finally, we give a few results about the tree structure. These results parallel those for prime modulus [4]. If b is a noncycle vertex in $G_n^{k^*}$, the height of b is defined to be the minimal natural number h such that b^{k^h} is a cycle vertex. For c a cycle vertex, define F_c^h as all noncycle vertices b of height h such that $b^{k^h} = c$. We define the tree above c as $F_c = \bigcup_h F_c^h$.

Lemma 5: If $b, c \in G_n^{k^*}$, $b \in F_1^h$, and c is a cycle vertex, then $bc \in F_{c^{k^h}}^h$.

Proof: By Lemma 3, $(\text{ord}_n b) \nmid t$ while $(\text{ord}_n c) | t$. Since $\mathbb{Z}_n^*$ is abelian, $(bc)^t \equiv b^t c^t \equiv b^t \not\equiv 1 \pmod{n}$, so the order of bc does not divide t. By Lemma 3, this says bc is not a cycle vertex, so the product of a cycle and noncycle vertex is a noncycle vertex.

Since $(bc)^{k^h} \equiv b^{k^h} c^{k^h} \equiv c^{k^h} \pmod{n}$, we see bc is in the forest above the cycle containing the vertex c. If $i < h$, then $(bc)^{k^i} \equiv b^{k^i} c^{k^i} \pmod{n}$, which is a cycle times a noncycle, thus a noncycle vertex. This means that bc first meets a cycle after h iterations of the k^{th} power map, i.e.,

$$bc \in F_{c^{k^h}}^h. \ \square$$

We can use Lemma 5 to show that any two trees in $G_n^{k^*}$ are isomorphic.

Theorem 4: If c is a cycle vertex, then $F_1 \cong F_c$.

Proof: For each h, we wish to construct a map from F_1^h to F_c^h that is one-to-one, onto, and preserves edges. As in [4], we define c_h as the cycle vertex such that $c_h^{k^h} \equiv c \pmod{n}$. This means c_h is the cycle vertex h cycle vertices before the cycle vertex c and therefore exists and is well defined. Following [4], define $f_h : F_1^h \to F_c^h$ such that $f_h(b) \equiv bc_h \pmod{n}$.

If $b_1, b_2 \in F_1^h$ and $f_h(b_1) \equiv f_h(b_2) \pmod{n}$, then $b_1 c_h \equiv b_2 c_h \pmod{n}$. Since $c_h \in \mathbb{Z}_n^*$, this implies $(b_1 - b_2)c_h \equiv 0 \pmod{n}$, so $b_1 \equiv b_2 \pmod{n}$.

If $b \in F_c^h$, then $(bc_h^{-1})^{k^h} \equiv b^{k^h} (c_h^{k^h})^{-1} \equiv cc^{-1} \equiv 1 \pmod{n}$. Since $(bc_h^{-1})^{k^{h-1}} \equiv b^{k^{h-1}} (c_h^{k^{h-1}})^{-1} \pmod{n}$ is a noncycle times a cycle vertex, we get a noncycle vertex. Therefore, $bc_h^{-1} \in F_1^h$ and $f_h(bc_h^{-1}) \equiv bc_h^{-1} c_h \equiv b \pmod{n}$.

Having shown f_h is one-to-one and onto for vertices, we must show it preserves edges. Specifically, if $b_1 \in F_1^{h+1}$ and $b_2 \in F_1^h$ such that $b_1^k \equiv b_2 \pmod{n}$, then $f_{h+1}(b_1)^k \equiv b_1^k c_{h+1}^k \equiv b_2 c_h \equiv f_h(b_2) \pmod{n}$, where we have used $c_{h+1}^k \equiv c_h \pmod{n}$, since c_{h+1} is $h+1$ vertices before c in the cycle and c_h is h vertices before c in the cycle. Similarly, if $b_1 \in F_c^{h+1}$ and $b_2 \in F_c^h$ such that $b_1^k \equiv b_2 \pmod{n}$, then $(b_1 c_{h+1})^k \equiv b_1^k c_{h+1}^k \equiv b_2 c^k \pmod{n}$. $\square$

Finally, we give two results to help determine the height of the tree, i.e., the maximum height of a noncycle element of $G_n^{k^*}$. Both of these are direct analogs of the prime modulus case [4].

Lemma 6: If $b \in F_c$ and $d = \text{ord}_n c$, then $(\text{ord}_n b) | k^h d$ if and only if $b \in F_c^x$ for some $x \le h$.

Proof: If $(\text{ord}_n b)|k^h d$, then $\text{ord}_n(b^{k^h})|d$ so $\text{ord}_n(b^{k^h})|t$ since $d|t$ as c is a cycle vertex. This means b^{k^h} is a cycle vertex in the same cycle as c, so $b \in F_c^x$ for some $x \le h$.

Conversely, if $b \in F_c^x$ for some $x \le h$, then $b^{k^x} \equiv c \pmod n$ so $\text{ord}_n(b^{k^x}) = d$. Therefore, $\text{ord}_n(b^{k^h}) = \text{ord}_n((b^{k^x})^{k^{h-x}}) = \text{ord}_n c^{k^{h-x}} = d$ by Lemma 4. □

Theorem 5: The height of the trees in $G_n^{k^*}$ is the minimal h such that $L|k^h t$.

Proof: If $(k, L) = 1$, then $t = L$ so Lemma 3 says that all vertices are cycles; thus, the height is 0 and $L|k^0 t$ since $t = L$.

If $(k, L) \ne 1$, then $h > 0$. Take b a vertex of maximal order, $\text{ord}_n b = L$. By Lemma 6, b is of height h since $(\text{ord}_n b)|k^h t$ but $(\text{ord}_n b) \nmid k^{h-1} t$. □

4. STRUCTURE OF $G_n^k - G_n^{k^*}$

Let $\wp$ be the set of all prime divisors of n and consider a partition of this set: $\wp = \wp_1 \cup \wp_2$. Let $G_{n,\wp_1}^k$ be the graph whose vertices are the multiples of $\prod_{p\in\wp_1} p$ relatively prime to all $p \in \wp_2$ and with an edge from b_1 to b_2 if $b_1^k \equiv b_2 \pmod n$. If a_p is such that $p^{a_p}|n$ but $p^{a_p+1} \nmid n$, define $n_1 = \prod_{p\in\wp_1} p^{a_p}$ and $n_2 = \prod_{p\in\wp_2} p^{a_p}$. Define $G_{n,\wp_1,\max}^k$ to be the graph whose vertices are the multiples of n_1 relatively prime to all $p \in \wp_2$ and where there is an edge from b_1 to b_2 if $b_1^k \equiv b_2 \pmod n$. We give a few results to help determine the structure of $G_{n,\wp_1}^k$.

Theorem 6: $G_{n,\wp_1,\max}^k \cong G_{n_2}^{k^*}$.

Proof: Let b_0 be the solution to $n_1 b_0 \equiv 1 \pmod{n_2}$. Define

$$\mu: G_{n_2}^{k^*} \to G_{n,\wp_1,\max}^k \text{ such that } \mu(b) \equiv b b_0 n_1 \pmod n.$$

For $q \in \wp_2$, $q \nmid b_0$, $q \nmid n_1$ so $b \in G_{n_2}^{k^*}$ implies $b b_0 n_1 \pmod n$ is in $G_{n,\wp_1,\max}^k$. Having shown our map is well defined on the set of vertices, we must show it is one-to-one onto, and preserves edges.

If $\mu(b_1) \equiv \mu(b_2) \pmod n$, then $(b_1 - b_2) b_0 n_1 \equiv 0 \pmod n$. This means $(b_1 - b_2) b_0 \equiv 0 \pmod{n_2}$. Since b_0 is invertible modulo n_2, $b_1 - b_2 \equiv 0 \pmod{n_2}$ so $b_1 = b_2$ in $G_{n_2}^{k^*}$.

If $c \in G_{n,\wp_1,\max}^k$, then $c = n_1 c_0$, so we want to show that there exists $b \in G_{n_2}^{k^*}$ such that $\mu(b) \equiv c \pmod n$. This is equivalent to

$$b b_0 n_1 \equiv c_0 n_1 \pmod n,$$

which is equivalent to

$$b b_0 \equiv c_0 \pmod{n_2}.$$

Since b_0 is invertible modulo n_2 and c_0 is relatively prime to all primes in $\wp_2$, $b \equiv b_0^{-1} c_0 \pmod{n_2}$ is an element of $G_{n_2}^{k^*}$ sent to c via μ.

If $b_1, b_2 \in G_{n_2}^{k^*}$ such that $b_1^k \equiv b_2 \pmod{n_2}$, then

$$\mu(b_1)^k \equiv b_1^k b_0^k n_1^k \equiv b_1^k b_0 n_1 \equiv b_2 b_0 n_1 \equiv \mu(b_2) \pmod n.$$

Finally, we deal with those vertices divisible by $\prod_{p\in\wp_1} p$ but not by n_1.

Theorem 7: $\left(\prod_{p\in\wp_1} p^{b_p}\right)b$ with $(b, p) = 1$ for all $p \in \wp$ has zero or

$$\left(\prod_{p\in\wp_2,\, p\neq 2} (k, p^{a_p-1}(p-1))\right)\cdot\left(\prod_{p\in\wp_1,\, p\neq 2,\, b_p\geq a_p,\, kc_p\geq a_p} p^{a_p-c_p-1}(p-1)\right)\cdot$$

$$\left(\prod_{p\in\wp_1,\, p\neq 2,\, a_p>c_pk,\, b_p=c_pk} p^{(k-1)c_p}(k, p^{a_p-b_p-1}(p-1))\right).$$

$$\begin{Bmatrix} (2,k)^{\delta_1}(2^{a-2},k)^{\delta_2} & \text{if } 2\in\wp_2 \\ 2^{a-c_2-1} & \text{if } 2\in\wp_1,\, b_2\geq a,\, c_2k\geq a \\ 2^{(k-1)c_2}(2,k)^{\delta_3}(2^{a-b_2-2},k)^{\delta_4} & \text{if } 2\in\wp_1, a>c_2k,\, b_2=c_2k \end{Bmatrix}$$

parent vertices of the form $\left(\prod_{p\in\wp_1} p^{c_p}\right)c$ with $(c, p) = 1$ for all $p \in \wp$, where

$$\delta_3 = \begin{cases} 0 & \text{if } a-b_2<2, \\ 1 & \text{if } a-b_2\geq 2, \end{cases} \quad \text{and} \quad \delta_4 = \begin{cases} 0 & \text{if } a-b_2<3, \\ 1 & \text{if } a-b_2\geq 3. \end{cases}$$

Proof: We want to find the number of distinct solutions, $\left(\prod_{p\in\wp_1} p^{c_p}\right)c$, to

$$\left(\left(\prod_{p\in\wp_1} p^{c_p}\right)c\right)^k \equiv \left(\prod_{p\in\wp_1} p^{b_p}\right)b \pmod{n},$$

where $(cb, p) = 1$ for all $p \in \wp$.

This is equivalent to counting the number of solutions to the system

$$\left(\left(\prod_{p\in\wp_1} p^{c_p}\right)c\right)^k \equiv \left(\prod_{p\in\wp_1} p^{b_p}\right)b \pmod{2^a},$$

$$\left(\left(\prod_{p\in\wp_1} p^{c_p}\right)c\right)^k \equiv \left(\prod_{p\in\wp_1} p^{b_p}\right)b \pmod{p_1^{a_1}}$$

$$\vdots$$

$$\left(\left(\prod_{p\in\wp_1} p^{c_p}\right)c\right)^k \equiv \left(\prod_{p\in\wp_1} p^{b_p}\right)b \pmod{p_m^{a_m}}.$$

Fact 1 allows us to work with each of these congruences separately and then multiply the number of solutions to each congruence to get the number of solutions to the system.

If $q \in \wp_2$, then all $p \in \wp_1$ are invertible, so the number of solutions to

$$\left(\left(\prod_{p\in\wp_1} p^{c_p}\right)c\right)^k \equiv \left(\prod_{p\in\wp_1} p^{b_p}\right)b \pmod{q^{a_q}}$$

equals the number of solutions to $c^k \equiv b' \pmod{q^{a_q}}$ for some b'. By Fact 4 the number of solutions is zero or $(k, q^{a_q-1}(q-1))$ if q is an odd prime, and zero or $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}$ if $q=2$.

If $q \in \wp_1$, then all $p \in \wp_1 - \{q\}$ are invertible, so the number of solutions to

$$\left(\left(\prod_{p\in\wp_1} p^{c_p}\right)c\right)^k \equiv \left(\prod_{p\in\wp_1} p^{b_p}\right)b \pmod{q^{a_q}}$$

is equal to the number of solutions to $(q^{c_q}c)^k \equiv q^{b_q}b' \pmod{q^{a_q}}$ for some b'. If $c_qk \neq b_q$ and either $b_q < a_q$ or $c_qk < a_q$, then there are no solutions for $(cb', q) = 1$ since the powers of q dividing the left- and right-hand sides of the congruence will be unequal for all k.

If $b_q, c_qk \geq a_q$, then we are trying to solve $0 \cdot c^k \equiv 0 \pmod{q^{a_q}}$. This has $q^{a_q-c_q-1}(q-1)$ solutions c for which $(c,q)=1$ and $q^{c_q}c$ are distinct modulo q^{a_q}. For $q=2$, this reduces to 2^{a-c_2-1}.

Finally, if $a_q > c_qk = b_q$, then; the number of solutions $q^{c_q}c$ to $(q^{c_q}c)^k \equiv q^{b_q}b' \pmod{q^{a_q}}$ is $q^{(k-1)c_q}$ times the number of solutions to $c^k \equiv b' \pmod{q^{a_q-b_q}}$. By Fact 4 this is zero or

$$q^{(k-1)c_q}(k, q^{a_q-b_q-1}(q-1))$$

if q is an odd prime, and zero or

$$2^{(k-1)c_2}(2,k)^{\delta_3}(2^{a-b_2-2},k)^{\delta_4}$$

if $q=2$.

The product of the numbers of solutions to each of these congruences gives the number of solutions to the system, proving the result. □

Remark: Similar results may be developed where the hypothesis $(c,p)=1$ is dropped. For example, if $p \in \wp_1$ is an odd prime and $(b,p)=1$, then the number of solutions to $(p^{c_p}c)^k \equiv p^{b_p}b \pmod{p^{a_p}}$ is zero or $p^{a_p-c_p}$ if $c_pk, b_p \geq a_p$. Other cases for a_p, b_p, c_pk may be worked out as in the proof of the last theorem.

5. AN EXAMPLE

Example 1: We will determine the structure of G_{56}^2. Note that $n=56$, $k=2$, $L=6$, $t=3$, and $w=2$. We start with the components with vertices that are not multiples of 2 or 7. $\mathbb{Z}_{56}^* \cong \mathbb{Z}_7^* \times \mathbb{Z}_8^* \cong \mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. This means the orders of all elements divide $\text{lcm}(6,2,2)=6$. We get the number of elements of each order using Lemma 1.

$$\begin{aligned}
\psi(1) &= (1,6)(1,2)(1,2) = 1,\\
\psi(2) &= (2,6)(2,2)(2,2) - \psi(1) = 7,\\
\psi(3) &= (3,6)(3,2)(3,2) - \psi(1) = 2,\\
\psi(6) &= (6,6)(6,2)(6,2) - \psi(3) - \psi(2) - \psi(1) = 14.
\end{aligned}$$

The one element of order 1 goes to itself since $2^1 \equiv 1 \pmod 1$; the seven elements of order 2 each go to the element of order 1 when squares; the two elements of order 3 are, by Theorem 2, in a cycle of length 2 since $2^1 \not\equiv 1 \pmod 3$, but $2^2 \equiv 1 \pmod 3$; and the fourteen elements of order 6 go to elements of order 3. If b is an element of order 3, we know that $x^2 \equiv b \pmod{56}$ has at

least one solution (the other element of order 3). Solving $x^2 \equiv b \pmod{56}$ is equivalent to solving the system

$$\begin{aligned} x^2 &\equiv b \pmod 7 \\ x^2 &\equiv b \pmod 8. \end{aligned} \tag{4}$$

Since $\mathbb{Z}_7^* \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, the first congruence in our system has 0 or 2 solutions. Since $\mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, the second congruence in our system has 0 or 4 solutions. This means the system (4) has 0 or 8 solutions. Since there is at least one solution, this forces each element of order 3 to have indegree 8, i.e., seven elements of order 6 and one of order 2. This completely classifies the structure of $G_{56}^{2^*}$ (see Fig. 1).

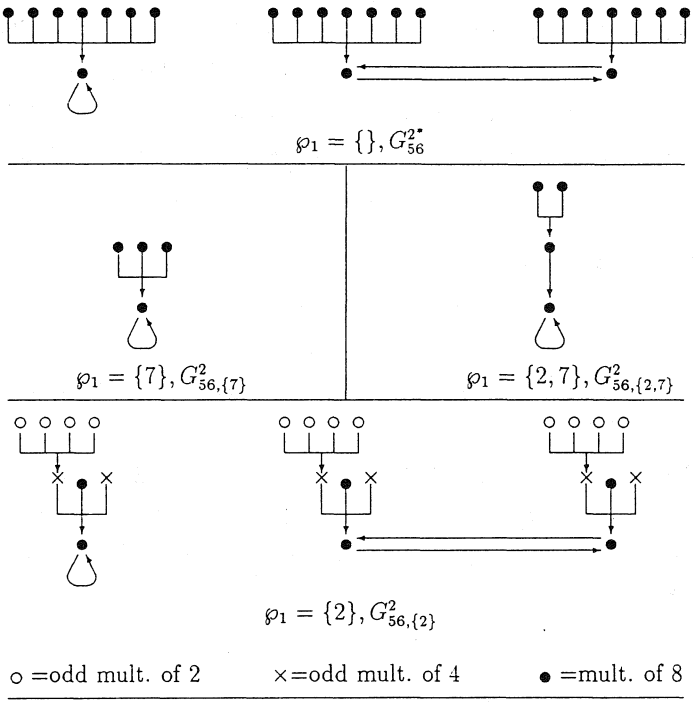


FIGURE 1. G_{56}^{2}

Next, consider the components which are multiples of 7 but relatively prime to 2. By Theorem 6 this will have a digraph structure isomorphic to $G_8^{2^*}$. $\mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, so there is one element of order 1 and three elements of order 2. Each element of order 2, when squared goes to the element or order 1.

The trickiest part is classifying the components that have vertices which are multiples of 2 but relatively prime to 7. By Theorem 6, $G_{56,\{2\},\max}^{2} \cong G_7^{2^*}$. $\mathbb{Z}_7^* \cong \mathbb{Z}_6$, so there is one element of order 1, one of order 2, two of order 3, and two of order 6. Upon squaring, the element of order 1 goes to itself, the element of order 2 goes to the element of order 1, the elements of order 3 go to each other, by Theorem 2, since $2^1 \not\equiv 1 \pmod 3$, $2^2 \equiv 1 \pmod 3$, and the elements of order 6 go to the elements of order 3. By Fact 4, $x^2 \equiv b \pmod 7$ has 0 or 2 solutions (since $\mathbb{Z}_7^* \cong \mathbb{Z}_2 \times \mathbb{Z}_3$) and

each element of order 3 has the other element of order 3 coming to it, we know the indegree must be 2, so each element of order 6 goes to a different element of order 3 (see Fig. 1).

We now add vertices for the multiples of 4 and of 2 that are prime to 7. Theorem 7, with $n = 56, k = 2, \wp_1 = \{2\}, \wp_2 = \{7\}, c_2 = 2$, and $b_2 \geq 3$, says the indegree for vertices that are multiples of 8 from those that are multiples of 4, relatively prime to 7, is zero or $(2, 7^{1-1}(7-1))2^{3-2-1} = 2$. Using the remark after Theorem 7, considering the graph of multiples of 4 relatively prime to 7, each vertex has indegree 0 or 4. There are $56 \cdot \frac{1}{8} \cdot \frac{6}{7} = 6$ odd multiples of 4, so each of the three cycle vertices of $G^2_{56,\{2\},\max}$ has two odd multiples of 4 parents (see Fig. 1).

To add the odd multiples of 2 prime to 7, we note that these will be parents of odd multiples of 4. Using Theorem 7, with $n = 56, k = 2, \wp_1 = \{2\}, \wp_2 = \{7\}, c_2 = 1$, and $b_2 = 2$, says the indegree for vertices that are odd multiples of 4 from those that are odd multiples of 2, relatively prime to 7, is zero or $(2, 7^{1-1}(7-1))2^{(2-1)1}(2,2)^0(2^0,2)^0 = 4$. Using Theorem 7, with $n = 56$, $k = 4 = 2^2$, $\wp_1 = \{2\}$, $\wp_2 = \{7\}$, $c_2 = 1$, and $b_2 \geq 3$, says the number of odd multiples of 2 in each tree in $G^2_{56,\{2\}}$ is zero or $(4, 7^{1-1}(7-1))2^{3-1-1} = 4$. Since there are $56 \cdot \frac{1}{4} \cdot \frac{6}{7} = 12$ odd multiples of 2 relatively prime to 7, we have three sets of four odd multiples of 2 going to one of each pair of odd multiples of 4 over each cycle vertex in $G^2_{56,\{2\},\max}$ (Fig. 1). This completes the structure of $G^2_{56,\{2\}}$.

Finally, $G^2_{56,\{2\},\max} \cong G_1^{2^*}$, which is a single element with edge from and to itself. To map directly onto a multiple of $2^3 \cdot 7$, the power on 2 must be at least 2, so the only parent of our single cycle vertex is the odd multiple of $2^2 \cdot 7$ (mod 56). Odd multiples of $2 \cdot 7$ map to the odd multiple of $2^2 \cdot 7$ when squared. This completes the description of G^2_{56} (see Fig. 1).

REFERENCES

1. M. Behzad & G. Chartrand. *Introduction to the Theory of Graphs.* Boston: Allyn and Bacon, 1971.
2. E. Blanton, Jr., S. Hurd, & J. McCranie. "On a Digraph Defined by Squaring Modulo n." *The Fibonacci Quarterly* **30.4** (1992):322-34.
3. L. K. Hua. *Introduction to Number Theory.* New York: Springer-Verlag, 1982.
4. C. Lucheta, E. Miller, & C. Reiter. "Digraphs from Powers Modulo p." *The Fibonacci Quarterly* **34.3** (1996):226-39.
5. T. D. Rogers. "The Graph of the Square Mapping on the Prime Fields." *Discrete Math.* **148** (1996):317-24.

AMS Classification Numbers: 05C20, 11B50

❖❖❖

THE ZECKENDORF DECOMPOSITION OF CERTAIN FIBONACCI-LUCAS PRODUCTS

Piero Filipponi
Fondazione Ugo Bordoni, Via B. Castiglione 59, I-00142 Rome, Italy
e-mail: filippo@fub.it

Evelyn L. Hart
Dept. of Mathematics, Colgate University, Hamilton, NY 13346-1398
e-mail: ehart@center.colgate.edu
(Submitted September 1996-Final Revision November 1996)

1. INTRODUCTION

The decomposition of any positive integer N as a sum of *positive-subscripted, distinct, non-consecutive* Fibonacci numbers F_k is commonly referred to as the *Zeckendorf decomposition* of N (ZD of N, in brief) [10]. This decomposition is always possible and, apart from the equivalent use of F_1 instead of F_2 (or vice-versa), is *unique* [8].

In the past years sequences of integers $\{a/b\}$, where a and b are certain Fibonacci and/or Lucas numbers (L_k), have been investigated from the point of view of the ZD of their terms (e.g., see [3], [4], [5]). The aim of this paper is to extend these studies to sequences $\{ab\}$. More precisely, in Section 2 we establish the ZD of mF_hF_k and mL_hL_k, with h and k arbitrary positive integers (possibly subject to some trivial restrictions), for the first few positive values of the integer m; the ZD of F_hL_k, $F_h^2L_k$, and $F_hL_k^2$ are also found. In Section 3, after some brief considerations on the ZD of nF_n, we analyze certain Fibonacci-Lucas products that emerge from particular choices of n.

All the identities presented in this paper have been established by proving conjectures based on behavior that became apparent through the study of early cases of h, k, and n. These conjectures were made with the aid of a multi-precision program including the generation of large-subscripted Fibonacci numbers. On the other hand, once the identities were conjectured, their proofs appeared to be rather easy and similar to one another so that, to save space, we confine ourselves to proving but a few among them; this is done in Section 4. Section 5 provides a glimpse of possible further investigations. It is worth mentioning that formula (1.4) of [4], namely,

$$\sum_{j=1}^{h} M_{rj+t} = \frac{M_{r(h+1)+t} - (-1)^r M_{rh+t} - M_{r+t} + (-1)^r M_t}{L_r - (-1)^r - 1} \tag{1.1}$$

(here, M_r stands for either F_r or L_r), plays a crucial role throughout the proofs.

2. THE ZD OF SOME FIBONACCI-LUCAS PRODUCTS

General Remarks

(a) The identities established in this section involve two integral parameters (namely, k and n) and, in most cases, are *valid* for all *positive* values of them. Sometimes they hold also for $n = 0$.

In general, some restrictions have to be imposed on k and n to obtain the ZD (as defined in Section 1) of the quantities on their left-hand sides.

(b) The number of addends in the ZD of the quantities under study depends only on the integer k. In some cases, it is even independent of k, thus assuming a constant value. In light of [2] and [1] (see also [6], p. 147), this fact is not very surprising.

(c) The usual convention that a sum vanishes whenever the upper range indicator is less than the lower one is adopted here. For brevity, we use the notation $F_{a\pm b} = F_{a+b} + F_{a-b}$.

2.1 Fibonacci Products

Proposition 1:

$$F_k F_{k+n} = \begin{cases} \sum_{j=1}^{k/2} F_{4j+n-2} & (k \text{ even}), \\ F_{n+1} + \sum_{j=1}^{(k-1)/2} F_{4j+n} & (k \text{ odd}). \end{cases} \tag{2.1}$$

Remark 1: Expression (2.1) works for $n = 0$ as well. In this case it yields the same result as that obtained by letting $s = 1$ in formulas (2.2) and (2.3) of [5].

Proposition 2:

$$2F_k F_{k+n} = \begin{cases} F_n + F_{2k+n-1} + \sum_{j=1}^{(k-2)/2} F_{4j+n+1} & (k \text{ even}), \\ F_{n+1} + F_{2k+n-1} + \sum_{j=1}^{(k-1)/2} F_{4j+n-1} & (k \geq 3, \text{ odd}). \end{cases} \tag{2.2}$$

Proposition 3: If $n \geq 2$, then

$$3F_k F_{k+n} = \begin{cases} F_n + F_{n+2} + F_{2k+n-3} + F_{2k+n} + \sum_{j=1}^{(k-4)/2} F_{4j+n+3} & (k \geq 4, \text{ even}), \\ F_{n-1} + F_{n+2} + F_{2k+n-3} + F_{2k+n} + \sum_{j=1}^{(k-3)/2} F_{4j+n+1} & (k \geq 5, \text{ odd}). \end{cases} \tag{2.3}$$

Proposition 4: If $n \geq 3$, then

$$4F_k F_{k+n} = \begin{cases} F_{n-2} + F_{n+1} + F_{n+3} + F_{2k+n+1} + \sum_{j=1}^{(k-4)/2} F_{4j+n+4} & (k \geq 4, \text{ even}), \\ F_{n-1} + F_{n+3} + F_{2k+n+1} + \sum_{j=1}^{(k-3)/2} F_{4j+n+2} & (k \geq 3, \text{ odd}). \end{cases} \tag{2.4}$$

Proposition 5: For $k, n \geq 3$, the ZD of $5F_k F_{k+n}$ is given by the right-hand side of (2.5) once the parity of k has been reversed. This fact becomes apparent upon inspection of (1.6) of [4].

2.2 Lucas Products

Proposition 6: If $n \geq 3$, then

$$L_k L_{k+n} = \begin{cases} F_{n-1} + F_{n+1} + F_{2k+n\pm1} & (k \text{ even}), \\ F_{n-2} + F_{n+1} + F_{2k+n+1} + \sum_{j=1}^{k-2} F_{2j+n+2} & (k \geq 3, \text{ odd}). \end{cases} \tag{2.5}$$

Remark 2: The ZD of L_k^2 is given by (4.2) and (4.3) of [5]. The decomposition (2.5) (k even) follows immediately from (17a) of [9].

Proposition 7: If $n \geq 5$, then

$$2L_k L_{k+n} = \begin{cases} F_{n\pm3} + F_{2k+n\pm3} & (k \geq 4, \text{ even}), \\ F_{n-4} + F_{2k+n+3} + \sum_{j=1}^{3} F_{2j+n-3} + \sum_{j=1}^{k-4} F_{2j+n+4} & (k \geq 5, \text{ odd}). \end{cases} \tag{2.6}$$

Proposition 8: If $n \geq 5$, then

$$3L_k L_{k+n} = \begin{cases} \sum_{j=1}^{4} (F_{2j+n-5} + F_{2j+2k+n-5}) & (k \geq 4, \text{ even}), \\ F_{n-4} + F_{n+3} + \sum_{j=1}^{3} F_{2j+2k+n-3} + \sum_{j=1}^{k-4} F_{2j+n+4} & (k \geq 5, \text{ odd}). \end{cases} \tag{2.7}$$

Proposition 9: If $n \geq 6$, then

$$4L_k L_{k+n} = \begin{cases} \sum_{j=1}^{4} (F_{3j+n-8} + F_{3j+2k+n-8}) & (k \geq 6, \text{ even}), \\ F_{n-4} + F_{n-2} + F_{n+1} + \sum_{j=1}^{3} F_{3j+2k+n-5} + \sum_{j=1}^{k-5} F_{2j+n+4} & (k \geq 5, \text{ odd}). \end{cases} \tag{2.8}$$

2.3 Mixed Products

That $F_k L_k = F_{2k}$ is a well-known fact (e.g., see I_7 of [7]).

Proposition 10:

$$F_k L_{k+n} = \begin{cases} \sum_{j=1}^{k} F_{2j+n-1} & (k \text{ even}), \\ F_n + F_{2k+n} & (k \text{ odd}, nk \neq 1), \end{cases} \tag{2.9}$$

$$L_k F_{k+n} = \begin{cases} F_n + F_{2k+n} & (k \text{ even}), \\ \sum_{j=1}^{k} F_{2j+n-1} & (k \text{ odd}). \end{cases} \tag{2.10}$$

Proposition 11: If $n \geq k$, then

$$F_k^2 L_{k+n} = \begin{cases} F_{n\pm k+1} + F_{n+k-2} + \sum_{j=1}^{(k-2)/2} (F_{4j+n-k} + F_{4j+n+k+2}) & (k \geq 4, \text{ even}), \\ F_{n\pm k+1} + \sum_{j=1}^{(k-1)/2} (F_{4j+n-k} + F_{4j+n+k}) & (k \geq 3, \text{ odd}). \end{cases} \tag{2.11}$$

Proposition 12: If $n \geq k+1$, then

$$L_k^2 F_{k+n} = \begin{cases} F_{n-k} + F_{n+k-2} + F_{n+k+1} + F_{n+3k} & (k \geq 4, \text{ even}), \\ F_{n-k} + F_{n+k-1} + \sum_{j=1}^{k-1} F_{2j+n+k+1} & (k \geq 3, \text{ odd}). \end{cases} \tag{2.12}$$

Remark 3: The ZD of $L_2^2 F_{2+n}$ is given by (2.12) above for $n \geq 4$. The decompositions (2.9) (k odd) and (2.10) (k even) follow immediately from (15b) and (15a) of [9], respectively. Further, it is worth mentioning that (30) and (31) of [9] follow by letting $n = 1$ in (2.10).

3. ON THE ZD OF nF_n

A brief study of the ZD of nF_n, beyond being worth undertaking *per se*, allows us to extend the results presented in Section 2 by considering some interesting Fibonacci-Lucas products that result from particular choices of n.

Definitions:

(1) Let $f(N)$ denote the number of addends in the ZD of N.

(2) Let $Q(n)$ denote nF_n.

(3) If F_n is in the ZD of $Q(n)$, then n is said to possess the property $\mathcal{P}$ (n has $\mathcal{P}$, in brief).

We are struck by two particular aspects of the ZD of $Q(n)$ that emerge from a computer experiment carried out for $1 \leq n \leq 10000$. Namely, we observe that

(i) $f[Q(n)]$ is relatively small,

(ii) If n has $\mathcal{P}$, then $n+1$ and $n+2$ have not, whereas either $n+3$ or $n+4$ has.

The numerical evidence leads us to offer the following conjectures.

Conjecture 1: The ratio of the number of naturals not having $\mathcal{P}$ to that of those having $\mathcal{P}$ is $\alpha^2 = 1 + \alpha = 1 + (1+\sqrt{5})/2$.

Conjecture 2: If $m \leq L_{2k} - 1$, with $k \geq 0$, then mL_{2k+1} has $\mathcal{P}$.

Conjecture 3: If $m \leq L_{2k-1}$, with $k \geq 1$, then $mL_{2k} + 1$ has $\mathcal{P}$.

Note. As the final draft of the paper was being prepared, the second author and Laura Sanchis discovered what seems to be a proof of Conjecture 1. Once the details have been verified, the proof will appear in a separate paper.

As for observation (i), we state the following theorem which will be proved in Section 4.

Theorem 1: If $n \le L_{2k+1}$, then $f[Q(n)] \le 2k+1$ [cf. (3.1)].

The following further results have been establised by us.

Proposition 13 (see Conj. 2): Both L_{2k+1} and $2L_{2k+1}$ have $\mathcal{P}$. More precisely, we have

$$Q(L_{2k+1}) = \sum_{j=1}^{2k+1} F_{2j+L_{2k+1}-2(k+1)}, \tag{3.1}$$

$$Q(2L_{2k+1}) = F_{2L_{2k+1}\pm 2(k+1)} + \sum_{j=1}^{2k-1} F_{2j+2L_{2k+1}-2k}. \tag{3.2}$$

Remark 4: The property $\mathcal{P}$ becomes apparent in (3.1) and (3.2) for $j = k+1$ and k, respectively.

Proposition 14 (see Conj. 3): For $k \ge 2$, both $L_{2k}+1$ and $2L_{2k}+1$ have $\mathcal{P}$. More precisely, we have

$$Q(L_{2k}+1) = F_{L_{2k}+1} + 1 + F_{L_{2k}\pm 2k+1}, \tag{3.3}$$

$$Q(2L_{2k}+1) = F_{2L_{2k}+1} + F_{2L_{2k}\pm 2k-1} + F_{2L_{2k}\pm 2k+2}. \tag{3.4}$$

Proposition 15: For $k \ge 3$, $L_k - 3$ has $\mathcal{P}$. More precisely, we have

$$Q(L_k-3) = \begin{cases} F_{L_k-k-3} + F_{L_k-6} + F_{L_k-3} + F_{L_k-1} + \sum_{j=1}^{(k-4)/2} F_{2j+L_k} & (k \text{ even}), \\ F_{L_k-3} + \sum_{j=1}^{(k-3)/2} (F_{2j+L_k-k-4} + F_{2j+L_k-1}) & (k \text{ odd}). \end{cases} \tag{3.5}$$

Proposition 16 [cf. (3.1)]:

$$Q(L_{2k}) = F_{L_{2k}\pm 2k} \quad \text{(from (1.5) of [4])}. \tag{3.6}$$

Proposition 17:

$$Q(F_k) = \begin{cases} \sum_{j=1}^{k/2} F_{4j+F_k-k-2} & (k \text{ even}), \\ F_{F_k-k+1} + \sum_{j=1}^{(k-1)/2} F_{4j+F_k-k} & (k \text{ odd}). \end{cases} \tag{3.7}$$

We observe that the number of addends in some of the decompositions above is independent of k. In fact, from (3.6), (3.3), and (3.4), it is seen that, if $k \ge 1$, then $f[Q(L_{2k})] = 2$ whereas, if $k \ge 2$, then $f[Q(L_{2k}+1)] = 3$ and $f[Q(2L_{2k}+1)] = 5$.

Question. Let $T \ge 1$ be an arbitrary positive integer. Does there exist at least one function $g(k)$ of k for which $f\{Q[g(k)]\} = T$ for all k greater than or equal to a certain minimum value k_0?

Let us conclude this section by showing that, if $T = 4$, then there is such a function. Namely, $g(k) = L_{2k}+3$ will work for $k \ge k_0 = 2$.

Proposition 18: If $k \geq 2$, then

$$Q(L_{2k}+3) = F_{L_{2k}+1} + F_{L_{2k}+5} + F_{L_{2k}\pm 2k+3}. \tag{3.8}$$

4. SOME PROOFS

Proof of (2.3) (k odd): Use (1.1) to rewrite the right-hand side of (2.3) as

$$F_{n-1} + F_{n+2} + F_{2k+n-3} + F_{2k+n} + \frac{F_{2k+n-1} - F_{2k+n-5} - F_{n+5} + F_{n+1}}{5}$$

$$= 2F_{n+1} + 2F_{2k+n-1} + \frac{L_{2k+n-3} - L_{n+3}}{5} \text{ (from (1.5) of [4])}$$

$$= idem + \frac{L_{n+k+(k-3)} - L_{n+k-(k-3)}}{5} = idem + \frac{5F_{n+k}F_{k-3}}{5} \text{ (from (1.6) of [4])}$$

$$= 2(F_{n+k+(k-1)} + F_{n+k-(k-1)}) + F_{n+k}F_{k-3}$$

$$= 2F_{n+k}L_{k-1} + F_{n+k}F_{k-3} \text{ (from (1.5) of [4])}$$

$$= F_{n+k}(2L_{k-1} + F_{k-3}) = 3F_kF_{n+k}.$$

Proof of (2.8) (k even): By using (1.5) of [4], the right-hand side of (2.8) becomes

$$L_k \sum_{j=1}^{4} F_{3j+n+k-8} = L_k \frac{F_{n+k+7} + F_{n+k+4} - F_{n+k-5} - F_{n+k-8}}{4} \text{ [from (1.1)]}$$

$$= L_k \frac{F_{n+k+1+6} - F_{n+k+1-6} + F_{n+k-2+6} - F_{n+k-2-6}}{4}$$

$$= L_k \frac{L_{n+k+1}F_6 + L_{n+k-2}F_6}{4} \text{ (from (1.5) of [4])}$$

$$= 2L_k(L_{n+k+1} + L_{n+k-2}) = 2L_k(2L_{n+k}) = 4L_kL_{n+k}.$$

Proof of (2.12):

Case 1: $k \geq 4$ is even. Rewrite the right-hand side of (2.12) as

$$F_{n+k-2} + F_{n+k+1} + F_{n+k-2k} + F_{n+k+2k} = F_{n+k-2} + F_{n+k+1} + F_{n+k}L_{2k} \text{ (from (1.5) of [4])}$$

$$= 2F_{n+k} + F_{n+k}L_{2k} = F_{n+k}(L_{2k}+2)$$

$$= F_{n+k}L_k^2 \text{ (from identity } I_{15} \text{ of [7]).}$$

Case 2: $k \geq 3$ is odd. First, rewrite the right-hand side of (2.12) as

$$F_{n-k} + F_{n+k-1} + F_{3k+n+1} - F_{3k+n-1} - F_{n+k+3} + F_{n+k+1} \text{ [from (1.1)]}$$

$$= F_{n-k} + F_{n+k-1} + F_{3k+n} - F_{n+k+2},$$

then use (1.5) of [4] thrice to rewrite the expression above as

$$F_{n-k} + F_{3k+n} - 2F_{n+k} = F_{3k+n} - F_nL_k - F_{n+k}$$

$$= F_{n+2k+k} - F_{n+2k-k} - F_nL_k = F_{n+2k}L_k - F_nL_k$$

$$= (F_{n+2k} - F_n)L_k = (F_{n+k+k} - F_{n+k-k})L_k$$

$$= F_{n+k}L_kL_k = F_{n+k}L_k^2.$$

Proof of (3.2): Put $2L_{2k+1} = h$ for notational convenience, and use (1.1) to rewrite the right-hand side of (3.2) as

$$\begin{aligned}
&F_{h-2k-2} + F_{h+2k+2} + (F_{h+2k} - F_{h+2k-2} - F_{h-2k+2} + F_{h-2k}) \\
&= F_{h+2k+2} + F_{h+2k-1} + F_{h-2k-2} - F_{h-2k+1} = 2F_{h+2k+1} - 2F_{h-2k-1} \\
&= 2F_h L_{2k+1} \text{ (from (1.5) of [4])} \\
&= hF_n \overset{\text{def}}{=} Q(h).
\end{aligned}$$

Proof of (3.5) (k even): Put $L_k = h$ for notational convenience, and use (1.1) to rewrite the right-hand side of (3.5) as

$$\begin{aligned}
&F_{h-k-3} + F_{h-6} + F_{h-3} + F_{h-1} + (F_{h+k-2} - F_{h+k-4} - F_{h+2} + F_h) \\
&= F_{h-k-3} + F_{h+k-3} - F_{h+1} + F_{h-6} + F_{h-3} + F_{h-1} \\
&= hF_{h-3} - F_{h+1} + F_{h-6} + F_{h-3} + F_{h-1} \text{ (from (1.5) of [4])} \\
&= hF_{h-3} - 3F_{h-3} = (h-3)F_{h-3} \overset{\text{def}}{=} Q(h-3).
\end{aligned}$$

Proof of Theorem 1: From (2.3) and (2.4) of [6], we see that

$$f[Q(n)] \le \frac{1}{2}[V(n) + U(n)] + 1,$$

where $V(n) = \lfloor \log_\alpha n \rfloor$ ($\alpha = (1+\sqrt{5})/2$) and $U(n)$ is an *even* number defined by $L_{U(n)-1} < n \le L_{U(n)+1}$. It must be observed that $U(n)$ is defined in [6] in a slightly different way, for the authors use the initial values $L_0 = 3$ and $L_1 = 4$ for the Lucas sequence. Now, it can be proved readily that, if $n \le L_{2k+1}$, then both $V(n)$ and $U(n)$ do not exceed $2k$. This fact, along with (4.1), prove the theorem.

5. CONCLUDING COMMENTS

As can be seen from the examples presented in this section, the identities established in this paper represent only a small sample of the possibilities available to us. A thorough investigation on the ZD of $Q(n)$ seems to be worthwhile; this study will be the object of a future paper. An attempt to prove Conjectures 2 and 3 produced the following decompositions [see also (3.1)-(3.4)] the proofs of which, based on the technique shown in Section 4, are left as an exercise to the interested reader. Namely, we see that

$$Q(3L_{2k+1}) = F_{3L_{2k+1}-2k-4} + F_{3L_{2k+1}-2k\pm1} + F_{3L_{2k+1}+2k+3} + \sum_{j=1}^{2k-2} F_{2j+3L_{2k+1}-2(k-1)} \quad (k \ge 2), \tag{5.1}$$

$$Q(4L_{2k+1}) = F_{4L_{2k+1}-2k-4} + F_{4L_{2k+1}\pm2k+1} + F_{4L_{2k+1}+2k+3} + \sum_{j=1}^{2k-2} F_{2j+4L_{2k+1}-2(k-1)} \quad (k \ge 2), \tag{5.2}$$

$$Q(5L_{2k+1}) = F_{5L_{2k+1}\pm2k} + F_{5L_{2k+1}\pm2(k+2)} + \sum_{j=1}^{2k-3} F_{2j+5L_{2k+1}-2(k-1)} \quad (k \ge 2), \tag{5.3}$$

$$Q(3L_{2k}+1) = F_{3L_{2k}+1} + F_{3L_{2k}\pm2k-1} + F_{3L_{2k}\pm2k+3} \quad (k \ge 2), \tag{5.4}$$

$$Q(4L_{2k}+1) = F_{4L_{2k}+1} + F_{4L_{2k}\pm2k-1} + F_{4L_{2k}\pm2k+1} + F_{4L_{2k}\pm2k+3} \quad (k \ge 2), \tag{5.5}$$

$$Q(5L_{2k}+1) = F_{5L_{2k}+1} + F_{5L_{2k}\pm2k-3} + F_{5L_{2k}\pm2k} + F_{5L_{2k}\pm2k+4} \quad (k \ge 3). \tag{5.6}$$

Remark 5: The property $\mathcal{P}$ becomes apparent in (5.1)-(5.3) for $j = k - 1$.

Moreover, we believe that also the ZD of nL_n deserves some study. A medium-range ($1 \le n \le 2000$) computer experiment led us to conjecture that F_n is not in the ZD of nL_n for $n > 2$. This experiment allowed us to observe that, if $n = F_{2k+1}$ ($k = 1, 2, 3, \ldots$), then $f(nL_n) = 2$ with only one exception in the case $k = 2$ for which $f(5L_5) = 1$. In fact, from (1.5) of [4], it can be seen immediately that

$$F_{2k+1}L_{F_{2k+1}} = F_{F_{2k+1} \pm (2k+1)}. \tag{5.7}$$

Remark 6: Letting $k = 1$ and 2 in (5.7) yields $2L_2 = F_{-1} + F_5 = F_2 + F_5$ and $5L_5 = F_0 + F_{10} = F_{10}$ (the exception), respectively.

Further, we observed that, if $n = L_{2k}$ ($k = 2, 3, 4, \ldots$), then $f(nL_n) = 4$. In fact, from identity I_8 of [7] and (1.6) of [4], it can be proved readily that

$$L_{2k}L_{L_{2k}} = F_{L_{2k} \pm 2k-1} + F_{L_{2k} \pm 2k+1}. \tag{5.8}$$

ACKNOWLEDGMENT

The contribution of the first author (P.F.) has been given in the framework of an agreement between the Italian PT Administration (Istituto Superiore PT) and the Fondazione Ugo Bordoni.

REFERENCES

1. P. Bruckman. Solution of Problem H-457. *The Fibonacci Quarterly* **31.1** (1993):93-96.
2. P. Filipponi. Problem H-457. *The Fibonacci Quarterly* **29.3** (1991):284.
3. P. Filipponi & H. T. Freitag. "The Zeckendorf Representation of $\{F_{kn} / F_n\}$." In *Applications of Fibonacci Numbers* **5**:217-19. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1993.
4. P. Filipponi & H. T. Freitag. "The Zeckendorf Decomposition of Certain Classes of Integers." In *Applications of Fibonacci Numbers* **6**:123-35. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1996.
5. H. T. Freitag & P. Filipponi. "On the F-Representation of Integral Sequences $\{F_n^2 / d\}$ and $\{L_n^2 / d\}$ where d is Either a Fibonacci or a Lucas Number." *The Fibonacci Quarterly* **27.3** (1989):276-82, 286.
6. P. J. Grabner, I. Nemes, A. Pethö, & R. F. Tichy. "On the Least Significant Digit of Zeckendorf Expansions." *The Fibonacci Quarterly* **34.2** (1996):147-51.
7. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin, 1969; rpt. The Fibonacci Association, 1979.
8. C. G. Lekkerkerker. "Voorstelling van Natuurlijke Getallen door een Som van Getallen van Fibonacci." *Simon Stevin* **29** (1952):190-95.
9. S. Vajda. *Fibonacci & Lucas Numbers, and the Golden Section*. Chichester: Ellis Horwood Ltd., 1989.
10. E. Zeckendorf. "Répresentation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas." *Bull. Soc. Roy. Sci. Liège* **41** (1972):179-82.

AMS Classification Numbers: 11D85, 05A17, 11B39

❖❖❖

SOLVING LINEAR EQUATIONS USING AN OPTIMIZATION-BASED ITERATIVE SCHEME

I. Tang
ETS-Rosedale, Mail Stop 58-N, Princeton, NJ 08441-0001
(Submitted September 1996)

A system of linear equations such as

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n + c_1 &= 0 \\ a_{21}x_1 + \cdots + a_{2n}x_n + c_2 &= 0 \\ \cdots & \\ a_{n1}x_1 + \cdots + a_{nn}x_n + c_n &= 0 \end{aligned} \tag{1}$$

can be solved using either direct methods such as the Gauss-Jordan procedure or iterative methods such as the Gauss-Seidel procedure. When the equation system is large, and especially when the coefficients are sparsely distributed, iterative methods are often preferred (see [1], [2]) since iterative methods for these systems are quite rapid and may be more economical in memory requirements of a computer. Iterative methods usually require a set of starting values as assumed solution. This article describes a procedure that does not require starting values. The procedure achieves convergence rapidly and can be applied to dependent systems in which there are fewer equations than variables.

Consider the case of n simultaneous equations in matrix form:

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} & c_1 \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} & c_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix}. \tag{2}$$

We propose to solve the system

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = 0 \tag{3}$$

by minimizing a scalar objective function

$$H = f_1^2 + \cdots + f_n^2 = (f_1 \ \cdots \ f_n) \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}. \tag{4}$$

The solution of (3) is obtained when the x values are found such that $H = 0$.

Differentiation of (4) yields

$$\frac{dH}{dt} = 2(f_1 \ \cdots \ f_n) \begin{pmatrix} df_1/dt \\ \vdots \\ df_n/dt \end{pmatrix}. \tag{5}$$

But (2) gives

$$\begin{pmatrix} df_1/dt \\ \vdots \\ df_n/dt \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} dx_1/dt \\ \vdots \\ dx_n/dt \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} & 0 \\ \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} & 0 \end{pmatrix} \begin{pmatrix} dx_1/dt \\ \vdots \\ dx_n/dt \\ dz/dt \end{pmatrix} \tag{6}$$

and, together with (2), (5) becomes

$$\frac{dH}{dt} = 2(f_1 \ \cdots \ f_n)\begin{pmatrix} a_{11} & \cdots & a_{1n} & 0 \\ \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} & 0 \end{pmatrix}\begin{pmatrix} dx_1/dt \\ \vdots \\ dx_n/dt \\ dz/dt \end{pmatrix}$$

$$= 2(x_1 \ \cdots \ x_n \ 1)\begin{pmatrix} a_{11} & \cdots & a_{n1} \\ \vdots & & \vdots \\ a_{1n} & \cdots & a_{nn} \\ c_1 & \cdots & c_n \end{pmatrix}\begin{pmatrix} a_{11} & \cdots & a_{1n} & 0 \\ \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} & 0 \end{pmatrix}\begin{pmatrix} dx_1/dt \\ \vdots \\ dx_n/dt \\ dz/dt \end{pmatrix}. \tag{7}$$

We now set

$$\begin{pmatrix} dx_1/dt \\ \vdots \\ dx_n/dt \\ dz/dt \end{pmatrix} = -\begin{pmatrix} a_{11} & \cdots & a_{n1} \\ \vdots & & \vdots \\ a_{1n} & \cdots & a_{nn} \\ 0 & \cdots & 0 \end{pmatrix}\begin{pmatrix} a_{11} & \cdots & a_{1n} & c_1 \\ \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} & c_n \end{pmatrix}\begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix}, \tag{8}$$

so that $dH/dt \le 0$.

By choosing a small value for Δt (for example, set it equal to the reciprocal of the Euclidean norm [1] of the matrix), one could approximate the derivatives on the left-hand side of (8) by finite differences between the $(i+1)^{\text{th}}$ and the i^{th} iterant of each of the x's (with z remaining a constant = 1), and we write

$$\begin{aligned} \frac{dx_1}{dt} &\cong \frac{\Delta x_1}{\Delta t} = \frac{x_{1,i+1} - x_{1,i}}{\Delta t}, \\ \frac{dx_n}{dt} &\cong \frac{\Delta x_n}{\Delta t} = \frac{x_{n,i+1} - x_{n,i}}{\Delta t}, \\ &\cdots \\ \frac{dz}{dt} &\cong \frac{\Delta z}{\Delta t} = \frac{z_{i+1} - z_i}{\Delta t}. \end{aligned} \tag{9}$$

Then (8) becomes

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \\ z \end{pmatrix}_{i+1} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ z \end{pmatrix}_i - \Delta t\begin{pmatrix} a_{11} & \cdots & a_{n1} \\ \vdots & & \vdots \\ a_{1n} & \cdots & a_{nn} \\ 0 & \cdots & 0 \end{pmatrix}\begin{pmatrix} a_{11} & \cdots & a_{1n} & c_1 \\ \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} & c_2 \end{pmatrix}\begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix}_i, \tag{10}$$

with $z_{i+1} = z_i = 1$.

Let

$$[B] = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} - \Delta t\begin{pmatrix} a_{11} & \cdots & a_{n1} \\ \vdots & & \vdots \\ a_{1n} & \cdots & a_{nn} \\ 0 & \cdots & 0 \end{pmatrix}\begin{pmatrix} a_{11} & \cdots & a_{1n} & c_1 \\ \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} & c_n \end{pmatrix} \tag{11}$$

and

$$[X] = \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix}, \tag{12}$$

then (10) becomes the recursion equation

$$[X]_{i+1} = [B]\ [X]_i. \tag{13}$$

Starting with an arbitrary set of values $[X]=[X]_0$ with $z=1$ as the initial solution, we carry out the iteration

$$\begin{aligned}[X]_1 &= [B]\ [X]_0 \\ [X]_2 &= [B]\ [X]_1 \\ &= [B]^2\ [X]_0 \\ &\text{and so on until} \\ [X]_k &= [B]^k\ [X]_0.\end{aligned} \tag{14}$$

Unless the set of equations is an inconsistent system, for sufficiently small Δt, which serves as an accelerating factor, $[B]^k$ will converge so that

$$[B]^k \to \begin{pmatrix} b_{11} & \cdots & b_{1n} & x_{1,s} \\ \vdots & & \vdots & \vdots \\ b_{n1} & \cdots & b_{nn} & x_{n,s} \\ 0 & \cdots & 0 & 1 \end{pmatrix} \tag{15}$$

as $k \to \infty$. It follows from (13) that

$$[X]_k = \begin{pmatrix} b_{11} & \cdots & b_{1n} & x_{1,s} \\ \vdots & & \vdots & \vdots \\ b_{n1} & \cdots & b_{nn} & x_{n,s} \\ 0 & \cdots & 0 & 1 \end{pmatrix} [X]_0. \tag{16}$$

If the equation system is furthermore not a dependent system, the individual elements b_{ij} will tend to zero upon convergence, and

$$[X]_k = \begin{pmatrix} x_{1,s} \\ \vdots \\ x_{n,s} \\ 1 \end{pmatrix} \tag{17}$$

regardless of the initial starting value, and $[X]=[x_s]$ are obtained for the solution of (2).

Since the last column of the matrix (15) to which $[B]$ converges contains the solution of (2), it is clear that to solve a set of linear equations that does not constitute a dependent system, an assumed starting solution is not required. We only need to multiply $[B]$ of (11) upon itself repeatedly, and if the multiplication is performed by squaring the previous result, convergence is accelerated through the sequence $[B],[B]^2,[B]^4,\ldots$. Although the process diverges for an overdetermined system, for a dependent system, one can obtain a solution from (15) according to the initial starting solution vector.

To illustrate the scheme, consider the following examples.

1. Consider the system: $x+y=-2$

$$2x+y=-3$$

$$[B]=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}-\Delta t\begin{pmatrix}1&2\\1&1\\0&0\end{pmatrix}\begin{pmatrix}1&1&2\\2&1&3\end{pmatrix}=\begin{pmatrix}0.95&-0.03&-0.08\\-0.03&0.98&-0.05\\0&0&1\end{pmatrix},$$

for which the acceleration factor $\Delta t = 0.01$ is used. Convergence leads to

$$[B]^n \to \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 0 & 0 & 1 \end{bmatrix}.$$

From the last column, the solution $(x, y) = (-1, -1)$ is obtained.

2. Given the dependent system: $x + y + z + 2 = 0$

$$2x + y - z + 3 = 0$$

$$[B] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} - \Delta t \begin{pmatrix} 1 & 2 \\ 1 & 1 \\ 1 & -1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 2 \\ 2 & 1 & -1 & 3 \end{pmatrix} = \begin{pmatrix} 0.95 & -.03 & 0.1 & -0.08 \\ -0.03 & 0.98 & 0 & -0.05 \\ 0.01 & 0 & 0.98 & 0.01 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

for which the acceleration factor Δt is again 0.01. Iteration leads to

$$[B]^n \to \begin{pmatrix} 0.2857 & -0.428 & 0.1428 & -1.142 \\ -0.428 & 0.6428 & -0.214 & -0.785 \\ 0.1428 & -0.214 & 0.0714 & -0.071 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The solution is found from (15) for any arbitrarily chosen starting value. For instance, if $x_0 = y_0 = z_0 = 0$, then, from the last column, we obtain $(x, y, z) = (-1.142, -0.785, -0.071)$. If $x_0 = 2, y_0 = 0$, and $z_0 = 1$, then $(x, y, z) = (-0.714, -1.427, 0.143)$ is obtained.

ACKNOWLEDGMENT

The encouragement of Dr. J. R. Davidson of the Department of Mathematics at Oklahoma State University (Oklahoma City) is greatly appreciated.

REFERENCES

1. Curtis F. Gerald & P. O. Wheatley. *Applied Numerical Analysis.* 4th ed. New York: Addison Wesley, 1992.
2. M. L. James, G. M. Smith, & J. C. Wolford. *Applied Numerical Methods for Digital Computation.* New York: Harper Collins, 1993.

AMS Classification Numbers: 15A06, 65F10

❖❖❖

A GENERALIZATION OF STIRLING NUMBERS

Hongquan Yu
Institute of Mathematical Sciences, Dalian University of Technology, Dalian 116024, China
(Submitted September 1996-Final Revision December 1996)

1. INTRODUCTION

Let $W(x)$, $f(x)$, $g(x)$ be formal power series with complex coefficients, and $W(x) \neq 0$, $W(0) = 1$, $f(0) = g(0) = 0$, Then the coefficients $\{B_1(n, k), B_2(n, k)\}$ in the following expansions,

$$W(x)(f(x))^k / k! = \sum_{n \geq k} B_1(n, k)x^n / n!, \quad (g(x))^k / [W(g(x))k!] = \sum_{n \geq k} B_2(n, k)x^n / n!, \tag{1}$$

are called a weighted Stirling pair if $f(g(x)) = g(f(x)) = x$, i.e., f and g are reciprocal.

When $W(x) \equiv 1$, $B_1(n, k)$ and $B_2(n, k)$ reduce to a Stirling type pair whose properties are exhibited in [7].

In this paper, we shall present a weighted Stirling pair that includes some previous generalizations of Stirling numbers as particular cases. Some related combinatorial and arithmetic properties are also discussed.

2. A WEIGHTED STIRLING PAIR

Let t, α, β be given complex numbers with $\alpha \cdot \beta \neq 0$. Let $f(x) = [(1+\alpha x)^{\beta/\alpha} - 1]/\beta$, $g(x) = [(1+\beta x)^{\alpha/\beta} - 1]/\alpha$, and $W(x) = (1+\alpha x)^{t/\alpha}$. Then, in accordance with (1), by noting that $f(x)$ and $g(x)$ are reciprocal, we have a weighted Stirling pair, denoted by

$$\{S(n, k, \alpha, \beta; t), S(n, k, \beta, \alpha; -t)\} = \{B_1(n, k), B_2(n, k)\}.$$

We call it an $(\alpha, \beta; t)$ [resp. a $(\beta, \alpha; -t)$] pair for short. Moreover, one of the parameters α or β may be zero by considering the limit process. For instance, a (1, 0; 0) [resp. a (0, 1; 0)] pair is just Stirling numbers of the first and second kinds.

Note that from the definition of an $(\alpha, \beta; t)$ pair and the first equation in (1), we may obtain the double generating function of $S(n, k, \alpha, \beta; t)$ as

$$(1+\alpha x)^{t/\alpha} \exp\left\{u\frac{(1+\alpha x)^{\beta/\alpha} - 1}{\beta}\right\} = \sum_{n,k} S(n, k, \alpha, \beta; t)\frac{x^n}{n!}u^k. \tag{2}$$

If we differentiate both sides of (2) on x, then multiply by $(1+\alpha x)$ and compare the coefficients of $x^n u^k$, we have

$$S(n, k-1, \alpha, \beta; t+\beta) = S(n+1, k, \alpha, \beta; t) + (n\alpha - t)S(n, k, \alpha, \beta; t), \tag{3}$$

and if we differentiate both sides of (2) on u and then compare the coefficients of $x^n u^k$, we have

$$S(n, k, \alpha, \beta; t+\beta) = \beta(k+1)S(n, k+1, \alpha, \beta; t) + S(n, k, \alpha, \beta; t). \tag{4}$$

Thus, the recurrence relation satisfied by $S(n, k, \alpha, \beta; t)$ may be obtained by combining (3) and (4):

$$S(n+1, k, \alpha, \beta; t) = (t + \beta k - \alpha n)S(n, k, \alpha, \beta; t) + S(n, k-1, \alpha, \beta; t). \tag{5}$$

The initial values of $S(n, k, \alpha, \beta; t)$ may be verified easily from (1) because $S(n, 0, \alpha, \beta; t) = t(t-\alpha)(t-2\alpha)\cdots(t-(n-1)\alpha)$ for $n \geq 1$, $S(n, n, \alpha, \beta; t) = 1$ for $n \geq 0$, and $S(n, k, \alpha, \beta; t) = 0$ for $k > n$. Thus, a table of values of $S(n, k, \alpha, \beta; t)$ can be given by concrete computations.

TABLE 1. $S(n, k, \alpha, \beta; t)$

n \ k	0	1	2	3
0	1			
1	t	1		
2	$t(t-\alpha)$	$2t+\beta-\alpha$	1	
3	$t(t-\alpha)$	$(t+\beta-2\alpha)+t(t-\alpha)$	$3t+3\beta-3\alpha$	1

From (2), we may get the explicit expression for $S(n, k, \alpha, \beta; t)$ via the generalized binomial theorem along the lines of (4.1) in [6].

For a complex number a, define the generalized factorial of x with increment a by $(x|a)_n = x(x-a)(x-2a)\cdots(x-na+a)$ for $n = 1, 2, \ldots$, and $(x|a)_0 = 1$.

Theorem 1: The $(\alpha, \beta; t)$ pair defined by (1) may also be defined by the following symmetric relations:

$$((x+t)|\alpha)_n = \sum_{k=0}^{n} S(n, k, \alpha, \beta; t)(x|\beta)_k; \tag{6}$$

$$(x|\beta)_n = \sum_{k=0}^{n} S(n, k, \beta, \alpha; -t)((x+t)|\alpha)_k. \tag{7}$$

Proof: The proof of the theorem may be carried out by the same argument used by Howard [6], by showing that the sequences defined by (6) and (7) satisfy the same recurrence relations and have the same initial values as that of an $(\alpha, \beta; t)$ pair. □

Examples: Let $\lambda, \theta \neq 0$ be two complex parameters. The so-called weighted degenerate Stirling numbers $(S_1(n, k, \lambda|\theta), S(n, k, \lambda|\theta))$ were first introduced and discussed by Howard [6] with definitions

$$(1-x)^{1-\lambda}\left(\frac{1-(1-x)^{\theta}}{\theta}\right)^k = k!\sum_{n\geq k} S_1(n, k, \lambda|\theta)\frac{x^n}{n!}$$

and

$$(1+\theta x)^{\mu\lambda}((1+\theta x)^{\mu}-1)^k = k!\sum_{n\geq k} S(n, k, \lambda|\theta)\frac{x^n}{n!},$$

where $\theta\mu = 1$. Now it is clear that $(-1)^{n-k}S_1(n, k, 1, \lambda|\theta) = S(n, k, 1, \theta; \theta-\lambda)$ and $S(n, k, \lambda|\theta) = S(n, k, \theta, 1; \lambda)$.

The limiting case $\theta = 0$, $\lambda \neq 0$, gives the weighted Stirling numbers $(R_1(n, k, \lambda), R_2(n, k, \lambda))$ discussed by Carlitz ([2], [3]) with definitions

$$(1-x)^{-\lambda}(-\log(1-x))^k = k!\sum_{n\geq k} R_1(n, k, \lambda)\frac{x^n}{n!}$$

and

$$e^{\lambda x}(e^x-1)^k = k!\sum_{n\geq k} R_2(n,k,\lambda)\frac{x^n}{n!},$$

where the weight function $e^{\lambda x}$ comes from the limit of $(1+\theta t)^{\lambda/\theta}$ as $\theta \to 0$. It is apparent that $((-1)^{n-k}R_1(n,k,\lambda),\ R_2(n,k,\lambda))$ forms a $(1, 0; -\lambda)$ pair.

Further examples are the degenerate Stirling numbers [1] defined by

$$\left(\frac{1-(1-t)^\theta}{\theta}\right)^k = k!\sum_{n\geq k} S_1(n,k|\theta)\frac{t^n}{n!}$$

and

$$((1+\theta t)^\mu - 1)^k = k!\sum_{n\geq k} S(n,k|\theta)\frac{t^n}{n!},$$

where $\theta\mu = 1$. It is clear that $((-1)^{n-k}S_1(n,k|\theta),\ S(n,k|\theta))$ is a $(1, \theta; 0)$ pair.

The noncentral Stirling numbers were first introduced by Koutras in [8] with the definitions:

$$(t)_n = \sum_{k=0}^{n} s_a(n,k)(t-a)^k;$$

$$(t-a)^n = \sum_{k=0}^{n} S_a(n,k)(t)_k.$$

It is now clear by Theorem 1 that $(s_a(n,k),\ S_a(n,k))$ is a $(1, 0; a)$ pair.

3. REPRESENTATIONS OF WEIGHTED STIRLING PAIRS

For $r \geq 0$, $f_r \neq 0$, let $F(x) = \sum_{k=r}^{\infty} f_k x^k / k!$ and $W(x) = \sum_{j=0}^{\infty} W_j x^j / j!$ be two formal power series. Following Howard [6], for complex z, we define the weighted potential polynomial $F_k(z)$ by

$$W(x)\left(\frac{f_r x^r / r!}{F(x)}\right)^z = \sum_{k=0}^{\infty} F_k(z)x^k / k!. \tag{8}$$

Moreover, if $r \geq 1$, define the weighted exponential Bell polynomial $B_{n,k}(0, \ldots, 0, f_r, f_{r+1}, \ldots)$ by

$$W(x)[F(x)]^k = k!\sum_{n=0}^{\infty} B_{n,k}(0, \ldots, 0, f_r, f_{r+1}, \ldots)x^n / n!. \tag{9}$$

The following lemma is due to Howard ([6], Th. 3.1).

Lemma 2: With $F_k(z)$ and $B_{n,k}$ defined above, we have

$$\binom{k-z}{k}F_k(z) = \sum_{j=0}^{k}\left(\frac{r!}{f_r}\right)^j\binom{k+z}{k-j}\binom{k-z}{k+j}\frac{(k+j)!}{(k+rj)!}B_{k+rj,j}(0, \ldots, 0, f_r, f_{r+1}, \ldots).$$

Now, from (9) with $W(x) = (1+\alpha x)^{t/\alpha}$ and $F(x) = [(1+\alpha x)^{\beta/\alpha} - 1]/\beta$, we have

$$S(n,k,\alpha,\beta;t) = B_{n,k}(1, \beta-\alpha, (\beta-\alpha)(\beta-2\alpha), (\beta-\alpha)(\beta-2\alpha)(\beta-3\alpha), \ldots). \tag{10}$$

Define the weighted potential polynomials $A_k(z)$ by

$$(1+\alpha x)^{t/\alpha}\left(\frac{\beta x}{(1+\alpha x)^{\beta/\alpha}-1}\right)^{z}=\sum_{k=0}^{\infty}A_k(z)\frac{x^k}{k!}, \tag{11}$$

If we differentiate both sides of (11) with respect to x, then multiply by $1+\alpha x$ and compare the coefficients of x^k, we obtain

$$zA_k(z+1)=(z-k)A_k(z)+k(t+(\alpha-\beta)z-(k-1)\alpha)A_{k-1}(z).$$

It follows that

$$\begin{aligned}(-1)^k\binom{k-n-1}{k}A_k(n+1)=(-1)^k\binom{k-n}{k}A_k(n)+(t+(\alpha-\beta)n\\ -(k-1)\alpha)(-1)^{k-1}\binom{k-n-1}{k-1}A_{k-1}(n),\end{aligned} \tag{12}$$

with initial conditions

$$\binom{-n-1}{0}A_0(n+1)=1, \text{ for } n\geq 0, \tag{13}$$

and

$$(-1)^n\binom{-1}{n}A_n(n+1)=(t+\alpha-\beta)(t+\alpha-2\beta)\cdots(t+\alpha-n\beta), \text{ for } n\geq 1. \tag{14}$$

Therefore, by equations (12)–(14), and the recurrence relations satisfied by $S(n, n-k, \beta, \alpha; t+\alpha-\beta)$ [may be deduced from (5)] and its initial values, we have that

$$(-1)^k\binom{k-n-1}{k}A_k(n+1)=S(n, n-k, \beta, \alpha; t+\alpha-\beta).$$

It then follows from Lemma 2, by taking $r=1$ and (10) that

$$S(n, n-k, \beta, \alpha; t+\alpha-\beta)=\sum_{j=0}^{k}(-1)^j\binom{k+n+1}{k-j}\binom{k-n-1}{k+j}S(k+j, j, \alpha, \beta; t).$$

By symmetry, we have the following representation formulas for weighted Stirling pairs.

Theorem 3: For $S(n, k, \alpha, \beta; t)$ defined by (1) and $S(n, k, \beta, \alpha; t+\alpha-\beta)$ defined in a like way, we have

$$S(n, k, \alpha, \beta; t)=\sum_{j=0}^{n-k}(-1)^j\binom{2n-k+1}{n-k-j}\binom{n+j}{n-k+j}S(n-k+j, j, \beta, \alpha; t+\alpha-\beta) \tag{15}$$

and

$$S(n, k, \beta, \alpha; t+\alpha-\beta)=\sum_{j=0}^{n-k}(-1)^j\binom{2n-k+1}{n-k-j}\binom{n+j}{n-k+j}S(n-k+j, j, \alpha, \beta; t). \tag{16}$$

Remark: It should be pointed out that similar representation results for the particular case when $\alpha=\theta$, $\beta=1$, and $t=1-\lambda$ has been proved by Howard [6]. Here we borrow his proof techniques.

4. CONGRUENCE PROPERTIES OF WEIGHTED STIRLING PAIRS

A formal power series $\phi(x)=\sum_{n\geq 0}a_n x^n/n!$ is called a Hurwitz series if all of its coefficients are integers. It is well known that, for the Hurwitz series $\phi(x)$ with $a_0=0$, the series $(\phi(x))^k/k!$ is again a Hurwitz series for any positive integer k.

In this section we always assume $\alpha, \beta, t \in \mathbf{Z}$. Then it is clear that both $(f(x))^k/k!$ and $(g(x))^k/k!$ in (1) are Hurwitz series, so that $S(n, k, \alpha, \beta; t)$ and $S(n, k, \beta, \alpha; -t)$ are two integer sequences.

First, let $t = 0$. Then we have

Theorem 4: Let p be a prime number and let k and j be integers such that $j+1 < k < p$. Then the following congruence relation holds:

$$S(p+j, k, \beta, \alpha; 0) \equiv 0 \pmod{p}. \tag{17}$$

Proof: Assume first that $\alpha \not\equiv 0 \pmod{p}$. For a polynomial $\phi(x)$ of degree n in x, we may express it, using Newton's interpolation formula, in the form

$$\phi(x) = \phi(\alpha_0) + \sum_{k=1}^{n} [\alpha_0 \alpha_1 \ldots \alpha_k]\{x|\alpha\}_k, \tag{18}$$

where $[\alpha_0 \alpha_1 \ldots \alpha_k]$ denotes the divided difference at the distinct points $x = \alpha_0, \alpha_1, \ldots, \alpha_k, \ldots$ and $\{x|\alpha\}_k = (x-\alpha_0)(x-\alpha_1)\cdots(x-\alpha_{k-1})$. Moreover, we have

$$[\alpha_0 \alpha_1 \ldots \alpha_k] = \begin{vmatrix} 1 & \alpha_0 & \cdots & \alpha_0^{k-1} & \phi(\alpha_0) \\ 1 & \alpha_1 & \cdots & \alpha_1^{k-1} & \phi(\alpha_1) \\ & & \cdots & & \\ 1 & \alpha_k & \cdots & \alpha_k^{k-1} & \phi(\alpha_k) \end{vmatrix} \Big/ \begin{vmatrix} 1 & \alpha_0 & \cdots & \alpha_0^{k-1} & \alpha_0^k \\ 1 & \alpha_1 & \cdots & \alpha_1^{k-1} & \alpha_1^k \\ & & \cdots & & \\ 1 & \alpha_k & \cdots & \alpha_k^{k-1} & \alpha_k^k \end{vmatrix}. \tag{19}$$

Now take $\phi_p(x) = (x|\beta)_p$, then $\phi_p(0) = 0$. We have, by (7) and (18), that

$$S(p, k, \beta, \alpha; 0) = [\alpha_0 \alpha_1 \ldots \alpha_k], \tag{20}$$

which may be expressed as a quotient of two determinants as in (19), where $\alpha_j = j\alpha$ $(j = 0, 1, 2, \ldots)$.

Notice that the classical argument of Lagrange that applied to the proof of

$$(x-1)\cdots(x-p+1) \equiv x^{p-1} - 1 \pmod{p}$$

may also be applied to prove the relation

$$\phi_p(x) = (x|\beta)_p = x(x-\beta)\cdots(x-(p-1)\beta) \equiv x^p - \beta^{p-1}x \pmod{p}, \tag{21}$$

where the congruence relation between polynomials are defined as usual (cf. [4], pp. 86-87, Th. 112). Also, using Fermat's Little Theorem, we find

$$\phi_p(j\alpha) \equiv (j\alpha)^p - \beta^{p-1}(j\alpha) \equiv \begin{cases} j\alpha \pmod{p}, & \text{if } p|\beta, \\ 0 \pmod{p}, & \text{if } p\nmid\beta, \end{cases}$$

where $j = 0, 1, 2, \ldots$. Consequently, we obtain, with $\alpha_j = j\alpha$ for $k > 1$,

$$\begin{vmatrix} 1 & \alpha_0 & \cdots & \alpha_0^{k-1} & \phi_p(\alpha_0) \\ 1 & \alpha_1 & \cdots & \alpha_1^{k-1} & \phi_p(\alpha_1) \\ & & \cdots & & \\ 1 & \alpha_k & \cdots & \alpha_k^{k-1} & \phi_p(\alpha_k) \end{vmatrix} \equiv 0 \pmod{p}.$$

Moreover, the denominator is given by

$$\begin{vmatrix} \alpha & \cdots & \alpha^{k-1} & \alpha^k \\ 2\alpha & \cdots & (2\alpha)^{k-1} & (2\alpha)^k \\ & \cdots & & \\ k\alpha & \cdots & (k\alpha)^{k-1} & (k\alpha)^k \end{vmatrix} = \alpha^{k(k+1)/2} \prod_{0\le i<j\le k} (j-i) \not\equiv 0 \text{ for } k < p \pmod{p}.$$

Thus, we have that $S(p, k, \beta, \alpha; 0) \equiv 0 \pmod{p}$ for $1 < k < p$.

Furthermore, let $F(x) = (x|\beta)_{p+j}$. We then have $F(x) = \sum_{k\ge 1}^{p+j} S(p+j, k, \beta, \alpha; 0)(x|\alpha)_k$ and

$$\begin{aligned} F(x) &= \phi_p(x)(x - p\beta)\cdots(x-(p+j)\beta+\beta) \\ &\equiv (x^p - \beta^{p-1}x)x(x-\beta)\cdots(x-(j-1)\beta) \pmod{p} \\ &\equiv (x^p - \beta^{p-1}x)(x^j + a_1x^{j-1} + \cdots + a_{j-1}x) \pmod{p}, \end{aligned} \tag{22}$$

where $a_1, \ldots, a_{j-1} \in \mathbf{Z}$. Consequently, we have, for $1 \le i \le p+j$,

$$F(i\alpha) \equiv \begin{cases} 0 \pmod{p}, & \text{if } p \nmid \beta, \\ (i\alpha)^{j+1} + a_1(i\alpha)^j + \cdots + a_{j-1}(i\alpha)^2 \pmod{p}, & \text{if } p \mid \beta. \end{cases}$$

Since $j < k-1$, we have

$$\begin{vmatrix} 1 & \alpha_0 & \cdots & \alpha_0^{k-1} & F(\alpha_0) \\ 1 & \alpha_1 & \cdots & \alpha_1^{k-1} & F(\alpha_1) \\ & & \cdots & & \\ 1 & \alpha_k & \cdots & \alpha_k^{k-1} & F(\alpha_k) \end{vmatrix} \equiv 0 \pmod{p},$$

where the last column is a linear combination of the first k columns modulo p.

Again, the same denominator determinant is not congruent to zero modulo p for $k < p$. Thus, we have that $S(p+j, k, \beta, \alpha; 0) \equiv 0 \pmod{p}$ for $j+1 < k < p$.

The case for $\alpha \equiv 0 \pmod{p}$ may be proved directly using (7), (21), and (22) by comparing the corresponding coefficients of powers of x in both sides of (21) and (22). Hence, the theorem is proved. □

Note that in the particular case in which $\alpha = 1$, $\beta = 0$ or $\beta = 1$, $\alpha = 0$, Theorem 4 reduces to congruences for Stirling numbers of the first and second kinds; see [5] for other congruences for Stirling numbers.

Corollary 5: Let α, β, t be integers. Then the $(\alpha, \beta; t)$ pair satisfies the basic congruence

$$S(p, k, \alpha, \beta; t) \equiv 0 \pmod{p}, \tag{23}$$

where p is a prime and $1 < k < p$.

Proof: Let $W(x) = (1+\alpha x)^{t/\alpha} = \sum_{n\ge 0} a_n x^n/n!$ with $a_n \in \mathbf{Z}$, $a_0 = 1$. Then it is clear from (1) that

$$\sum S(n, k, \alpha, \beta; t)x^n/n! = \left(\sum_{n\ge 0} a_n x^n/n!\right)\left(\sum_{n\ge k} S(n, k, \alpha, \beta; 0)x^n/n!\right),$$

so that we have

$$S(p, k, \alpha, \beta; t) = \sum_{i=k}^{p} a_{p-i} S(i, k, \alpha, \beta; 0)\binom{p}{i}.$$

From Theorem 4 (taking $j = 0$) and the fact that $\binom{p}{i} \equiv 0 \pmod{p}$ for $0 < i < p$, it follows that $S(p, k, \alpha, \beta; t) \equiv 0 \pmod{p}$, and the corollary is proved. □

ACKNOWLEDGMENT

The author is very grateful to the referee for his valuable suggestions which considerably improved the presentation of this article.

REFERENCES

1. L. Carlitz. "Degenerate Stirling, Bernoulli and Eulerian Numbers." *Utilitas Math.* **15** (1979): 51-88.
2. L. Carlitz. "Weighted Stirling Numbers of the First and Second Kind–I." *The Fibonacci Quarterly* **18.2** (1980):147-62.
3. L. Carlitz. "Weighted Stirling Numbers of the First and Second Kind–II." *The Fibonacci Quarterly* **18.3** (1980):242-57.
4. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford: Oxford University Press, 1981.
5. F. T. Howard. "Congruences for the Stirling Numbers and Associated Stirling Numbers." *Acta Arithmetica* **55** (1990):29-41.
6. F. T. Howard. "Degenerate Weighted Stirling Numbers." *Discrete Math.* **57** (1985):45-58.
7. L. C. Hsu. "Some Theorems on Stirling-Type Pairs." *Proceedings of Edinburgh Math. Soc.* **36** (1993):525-35.
8. M. Koutras. "Non-Central Stirling Numbers and Some Applications." *Discrete Math.* **42** (1982):73-89.

AMS Classification Numbers: 05A15, 11B73, 11A07

❖❖❖

PALINDROMIC NUMBERS IN ARITHMETIC PROGRESSIONS

Matúš Harminc and Roman Soták
Dept. of Geometry and Algebra, P. J. Šafárik University, Jesenná 5, 041 54 Košice, Slovakia
(Submitted September 1996-Final Revision November 1996)

Integers have many interesting properties. In this paper it will be shown that, for an arbitrary nonconstant arithmetic progression $\{a_n\}_{n=1}^{\infty}$ of positive integers (denoted by $\mathbb{N}$), either $\{a_n\}_{n=1}^{\infty}$ contains infinitely many palindromic numbers or else $10|a_n$ for every $n \in \mathbb{N}$. (This result is a generalization of the theorem concerning the existence of palindromic multiples, cf. [2].) More generally, for any number system base b, a nonconstant arithmetic progression of positive integers contains infinitely many palindromic numbers if and only if there exists a member of the progression not divisible by b.

WHAT IS A PALINDROMIC NUMBER?

A positive integer is said to be a (decadic) palindromic number or, shortly, a palindrome if its leftmost digit is the same as its rightmost digit, its second digit from the left is equal to its second digit from the right, and so on. For example, 33, 142505241, and 6 are palindromic numbers. More precisely, let $\overline{d_k d_{k-1} \ldots d_1 d_0}$ be a usual decadic expansion of n, where $d_i \in \{0, 1, \ldots, 8, 9\}$ for $i \in \{0, 1, \ldots, k\}$ and $d_k \neq 0$. That is, $n = \sum_{i=0}^{k} d_i \cdot 10^i$.

Definition: A positive integer n is called a palindrome if its decadic expansion $n = \sum_{i=0}^{k} d_i \cdot 10^i$ satisfies $d_i = d_{k-i}$ for all $i \in \{0, 1, \ldots, k\}$.

In Harminc's paper [2], interesting properties of palindromes were observed. For instance, a palindromic number is divisible by 81 if and only if the sum of its digits is divisible by 81. Some open questions were also stated there. For example, it is not known whether there exist infinitely many palindromic primes. Korec has proved in [3] and [4] that there are infinitely many non-palindromic numbers having palindromic squares.

In what follows we will consider arithmetic progressions. Each such progression $\{a_n\}_{n=1}^{\infty}$ is given by its first member a_1 and by its difference d; thus, $a_n = a_1 + (n-1) \cdot d$. Let us recall a well-known result on prime numbers in arithmetic progressions proved by Dirichlet (cf. [1]). As usual, denote by (u, v) the greatest common divisor of integers u and v. If $(u, v) = 1$, then u and v are called pairwise prime integers. Integers a and b are said to be congruent modulo a positive integer m, if $m|(a-b)$; for this, we will write $a \equiv b \pmod{m}$. Then, the theorem of Dirichlet is

Theorem A: Every arithmetic progression in which the first member and the common difference are pairwise prime integers has infinitely many primes.

In other words, if $(a_1, d) = 1$, then the congruence $x \equiv a_1 \pmod{d}$ has infinitely many prime solutions. We will present an analogous result giving easy necessary and sufficient conditions for an arithmetic progression to contain infinitely many palindromic solutions. Clearly, if every member of an arithmetic progression ends in zero, then the progression cannot contain any palindromic number. But as we will see, this is the unique exception.

MULTIPLES OF THE TYPE 999...99

Lemma: Let $e \in \mathbb{N}$ be such that $(e, 10) = 1$. Then, for every $m_0 \in \mathbb{N}$, there exists $m \in \mathbb{N}$ such that $m > m_0$ and $10^m \equiv 1 \pmod{e}$.

Proof: Let us investigate powers of ten. Each number 10^k ($k \in \mathbb{N}$) is congruent (mod e) to one of the numbers $0, 1, 2, \ldots, e-1$. From this fact, it follows that, among the powers 10, 10^2, ..., 10^i, ..., there exist infinitely many numbers pairwise congruent (mod e). Thus, there are $k_1, k_2 \in \mathbb{N}$ such that

$$10^{k_1} \equiv 10^{k_2} \pmod{e} \quad \text{and} \quad k_2 - k_1 > m_0.$$

Then $10^{k_1} \cdot (1 - 10^{k_2 - k_1}) \equiv 0 \pmod{e}$ and, since $(e, 10) = 1$, we obtain $10^{k_2 - k_1} \equiv 1 \pmod{e}$. Hence, $m = k_2 - k_1$ has the desired properties. □

Since $10^m \equiv 1 \pmod{e}$ means that $e \mid \underbrace{999\ldots99}_{m \text{ of } 9\text{'s}}$, the Lemma yields the following corollary.

Corollary: If $e \in \mathbb{N}$ and $(e, 10) = 1$, then there exist infinitely many numbers of the type 999...99 divisible by e.

MAIN RESULT

Before stating Theorem B, let us introduce a notation used in the proof. An integer with the same digits as $n \in \mathbb{N}$, but written in the opposite order, will be denoted by n^*, i.e., if $n = \overline{d_k d_{k-1} \ldots d_1 d_0}$, then $n^* = \overline{d_0 d_1 \ldots d_{k-1} d_k}$. Thus, n is a palindrome if and only if $n = n^*$.

Theorem B: Let $\{a_n\}_{n=1}^{\infty}$ be an arithmetic progression of positive integers with difference $d \in \mathbb{N}$. Then $\{a_n\}_{n=1}^{\infty}$ contains infinitely many palindromes if and only if $10 \nmid a_1$ or $10 \nmid d$.

Proof: Clearly, if there exists $i \in \mathbb{N}$ such that a_i is a palindrome, then a_i and d cannot both be multiples of ten.

Conversely, let $10 \nmid a_1$ or $10 \nmid d$ and let $d = 2^{\beta} \cdot 5^{\gamma} \cdot e$, where $(e, 10) = 1$. Let us denote by c the least member of the sequence $\{a_n\}_{n=1}^{\infty}$ that is not divisible by 10 and let

$$c = \overline{c_t c_{t-1} \ldots c_1 c_0} = \sum_{i=0}^{t} c_i \cdot 10^i$$

where $c_t \neq 0$. (Since $10 \nmid a_1$ or $10 \nmid d$, we have $c = a_1$ or $c = a_2$.)

Consider two cases, $e = 1$ and $e \neq 1$. The idea is (in the first case) to insert a sufficiently large number of 0's between c^* and c (in the second case) to include among the 0's an appropriate number of strategically placed 1's.

First, let $e = 1$. Then, for every integer $l > \max\{t, \beta, \gamma\}$, it is easy to see that the palindrome

$$c^* \cdot 10^l + c = \overline{c_0 c_1 \ldots c_{t-1} c_t \underbrace{0\ldots0}_{l-t-1 \text{ of } 0\text{'s}} c_t c_{t-1} \ldots c_1 c_0}$$

is a member of the sequence $\{a_n\}_{n=1}^{\infty}$.

Now, let $e \neq 1$. By the Lemma above, there exists $m > \max\{t, \beta, \gamma\}$ such that $10^m \equiv 1 \pmod{e}$. Then, for every integer $j \in \mathbb{N}$, we have $10^{jm} \equiv 1 \pmod{e}$. Moreover, there exists $r \in \{0, 1, \ldots, e-1\}$ such that

$$c^* \cdot 10^{m-t} + r \equiv 0 \pmod{e}.$$

Put

$$x = c^* \cdot 10^{rm+m-t} + 10^{rm} + 10^{(r-1)m} + \cdots + 10^m + c$$

$$= \overline{c_0 c_1 \ldots c_{t-1} c_t \underbrace{0\ldots0}_{m-t-1} 1 \underbrace{0\ldots0}_{m-1} 1 \underbrace{0\ldots0}_{m-1} 1 0\ldots0 1 \underbrace{0\ldots0}_{m-1} 1 \underbrace{0\ldots0}_{m-t-1} c_t c_{t-1} \ldots c_1 c_0}.$$

Clearly, x is a palindrome, and we will show that x is a member of the sequence $\{a_n\}_{n=1}^{\infty}$. Therefore, it is sufficient to check that $d \mid (x-c)$. Since $2^{\beta} \mid (x-c)$ and $5^{\gamma} \mid (x-c)$, we will verify only that $e \mid (x-c)$. But

$$x - c = c^* \cdot 10^{rm+m-t} + 10^{rm} + 10^{(r-1)m} + \cdots + 10^m$$

$$\equiv c^* \cdot 10^{rm} \cdot 10^{m-t} + \underbrace{1 + \cdots + 1}_{r} \pmod{e}.$$

Hence

$$x - c \equiv c^* \cdot 10^{m-t} + r \pmod{e},$$

so that $x-c$ is congruent to zero (mod e), and the proof if complete. □

One could define a b-adic palindrome as a positive integer n with b-adic expansion $\overline{d_k d_{k-1} \ldots d_1 d_0}$ (i.e., $n = \sum_{i=0}^{k} d_i \cdot b^i$, where $d_i \in \{0, 1, \ldots, b-1\}$ and $d_k \neq 0$) satisfying $d_i = d_{k-i}$ for all $i \in \{0, 1, \ldots, k\}$. It is not difficult to see that all results proved here for decadic palindromes hold for b-adic ones, too. For any number system base b, the following theorem is true.

Theorem C: Let $\{a_n\}_{n=1}^{\infty}$ be an arithmetic progression of positive integers with difference $d \in \mathbb{N}$. Then $\{a_n\}_{n=1}^{\infty}$ contains infinitely many b-adic palindromes if and only if $b \nmid a_1$ or $b \nmid d$.

To prove Theorem C, the reader can mimic the proof of Theorem B.

Hint: Let $b = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ be the standard form of b and let $d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_s^{\beta_s} \cdot e$, where $(e, b) = 1$. Let c be as before with

$$c = \overline{c_t c_{t-1} \ldots c_1 c_0} = \sum_{i=0}^{t} c_i \cdot b^i.$$

If $e = 1$, take $x = c^* \cdot b^l + c$, where

$$l > \max\left\{t, \frac{\beta_1}{\alpha_1}, \frac{\beta_2}{\alpha_2}, \ldots, \frac{\beta_s}{\alpha_s}\right\}.$$

If $e \neq 1$, take $x = c^* \cdot b^{rm+m-t} + b^{rm} + b^{(r-1)m} + \cdots + b^m + c$, where m is sufficiently large, see the Lemma above for

$$m_0 \geq \max\left\{t, \frac{\beta_1}{\alpha_1}, \frac{\beta_2}{\alpha_2}, \ldots, \frac{\beta_s}{\alpha_s}\right\}. \quad \square$$

Open problem: Characterize geometric progressions without palindromic members.

REFERENCES

1. P. G. L. Dirichlet. *Beweis des Satzes, daß jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Faktor sind, unendlich viele Primzahlen enthält*, pp. 45-71. Abh. AkD. Berlin, 1837.
2. M. Harminc. "The Existence of Palindromic Multiples." *Matematické obzory* **32** (1989):37-42. (Slovak)
3. I. Korec. "Palindromic Squares of Non-Palindromic Numbers in Various Number System Bases." *Matematické obzory* **33** (1989):35-43. (Slovak)
4. I. Korec. "Palindromic Squares for Various Number System Bases." *Math. Slovaca* **41.3** (1991):261-76.

AMS Classification Numbers: 11B25, 11A63

❖❖❖

CONJECTURES ON THE Z-DENSITIES OF THE FIBONACCI SEQUENCE

Paul S. Bruckman
13 Webster Ave., Apt. G., Highwood, IL 60040

Peter G. Anderson
Dept. of Computer Science, Rochester Institute of Technology, Rochester, NY 14623-5608
(Submitted September 1996-Final Revision July 1997)

1. INTRODUCTION

The concept of "Z-densities" is introduced in this paper, leading to several interesting conjectures involving the divisibility properties of the Fibonacci entry-point function.

We let $\mathcal{F} = \{F_n\}_{n=1}^{\infty}$ and $\mathcal{L} = \{L_n\}_{n=1}^{\infty}$ denote the Fibonacci and Lucas sequences, respectively. Given m, the *Fibonacci entry-point of* m, denoted by $Z(m)$, is the smallest $n > 0$ such that $m | F_n$; in this case, we write $Z(m) = n$. If m and n are arbitrary (with $m > 1$), $m | F_n$ iff $Z(m) | n$.

If $m = p$, a prime $\neq 2$ or 5, it is well-known that $Z(p) | (p - \varepsilon_p)$, where $\varepsilon_p = (5/p)$, the Legendre symbol.

Given an arbitrary sequence $\mathcal{U} = \{U_n\}$ of positive integers, we say that p *divides* $\mathcal{U}$, and write $p | \mathcal{U}$ iff $p | U_n$ for some n. Let $\pi_{\mathcal{U}}(x)$ denote the number of primes $p \le x$ such that $p | \mathcal{U}$; also, $\pi(x)$ is the number of primes $p \le x$. The "natural" *density*, or simply the *density*, of $\mathcal{U}$ is given by

$$\theta_{\mathcal{U}} = \lim_{x \to \infty} \pi_{\mathcal{U}}(x) / \pi(x). \tag{1.1}$$

It is well-known that $p | \mathcal{F}$ for all p, and so $\theta_{\mathcal{F}} = 1$. This is certainly not the case for a general $\mathcal{U}$. J. C. Lagarias [6] has determined $\theta_{\mathcal{U}}$ for a few specific sequences, among them $\mathcal{L}$. As far as the topic of this paper is concerned, the most interesting result obtained by Lagarias was the following:

$$\theta_{\mathcal{L}} = 2/3. \tag{1.2}$$

That is to say, $2/3$ of all primes, asymptotically, divide some Lucas number.

Now, it is also known that $p | \mathcal{L}$ iff $Z(p)$ is even. It follows that the density of those primes p for which $Z(p)$ is even is equal to $2/3$; note that this extends our initial definition of "density." The aim of the present paper is to generalize this perspective. Thus, we ask the question: Given m, what is the density of those p for which $m | Z(p)$?

We can also ask the more fundamental question: Given m, what is the density of those p such that $Z(p) = m$? However, it is clear that such densities are zero for all m, since they characterize the *primitive prime divisors* of F_m (for a given m), which are necessarily finite in number; therefore, the density of those p such that $Z(p) = m$ is of no interest to us here.

To obtain answers to the first question above, we introduce various types of densities that involve $Z(p)$ in their definitions; such densities are referred to as "Z-densities." Here is a formal definition: Given m and x, let $M(m, x)$ denote the number of $p \le x$ such that $m | Z(p)$. Then we define $\zeta(m)$, the "Z-density of m as a divisor," as follows (assuming the limit exists):

$$\zeta(m) = \lim_{x \to \infty} M(m, x) / \pi(x). \tag{1.3}$$

Clearly, $\zeta(1) = 1$; also, using Lagarias' result, $\zeta(2) = \theta_{\mathcal{L}} = 2/3$.

Based on an examination of certain Fibonacci entry-point data [4], [5], one of the authors (Bruckman) reached some conclusions regarding the evaluation of $\zeta(m)$ and related Z-densities. More recently, the other author (Anderson) has strengthened the evidence for these conjectures, using extended data produced by computer runs. Much of the numerical evidence for the various conjectures made in this paper has been omitted in the interest of brevity. However, for the sake of demonstration, we have included in the Appendix one of the tables that comprise such evidence (in abridged form). Additional details may be obtained from either author upon request. Known or proven results are annotated in the usual manner. Conjectures and consequences of such conjectures are marked with an asterisk; in the narrative, these are referred to frequently as "conditional results," meaning "results conditional on the conjectures."

The following is one of the consequences of these conjectures, valid for all primes q:

$$\zeta(q) = q/(q^2 - 1). \tag{1.4}^*$$

The characteristic polynomial of the sequences $\mathcal{F}$ and $\mathcal{L}$ has the irrational zeros α and β, the familiar Fibonacci constants. For sequences having a second-degree characteristic polynomial that has *integral* zeros, (1.4)* was proved by C. Ballot [1]. Thus, Ballot's result is, conditionally, more broadly applicable. The methods employed by Ballot to establish his result are beyond the scope of this exploratory paper.

In the present work, the authors have restricted their analysis to the sequences $\mathcal{F}$ and $\mathcal{L}$. Further generalizations are left to other researchers.

Before proceeding to the main points of this paper, we find it convenient to decompose the appropriate Z-densities into certain "component" Z-densities, defined below. Our study of such component Z-densities led to the main conjectures we formulated.

In this paper, lower-case letters represent nonnegative integers, except for x, which may be any positive real number (generally thought of as large). However, the letters m and n represent positive integers, and the letters p and q represent primes.

2. COMPONENT Z-DENSITIES

We begin with a basic definition of "q^i, q^j Z-densities." Given q, x, i, and j, with $i \geq j \geq 0$, let $M(q, x; i, j)$ denote the number of $p \leq x$ such that $q^i \| (p - \varepsilon_p)$ and $q^j \| Z(p)$. The expression $q^0 \| n$ is taken to mean $q \nmid n$. Then the "q^i, q^j Z-density," denoted $\zeta(q; i, j)$, is given as follows (assuming the limit exists):

$$\zeta(q; i, j) \equiv \lim_{x \to \infty} M(q, x; i, j)/\pi(x). \tag{2.1}$$

On the basis of empirical evidence, we formulate the following conjecture.

Conjecture 2.1*:

$$\zeta(q; i, j) = \begin{cases} (q-2)/(q-1) & \text{if } i = j = 0, \\ q^{-2i} & \text{if } i \geq 1,\ j = 0, \\ (q-1)q^{-1-2i+j} & \text{if } i \geq j \geq 1. \end{cases}$$

By the definition of $\zeta(q; i, j)$, it is clear that, for all primes q:

$$\sum_{i\geq j\geq 0}\zeta(q;i,j)=1. \tag{2.2}$$

It is readily verified that Conjecture 2.1* implies (2.2).

Conjecture 2.1* appears to hold even for the "exceptional" primes 2 and 5, which play a special role in the study of $\mathcal{F}$ and $\mathcal{L}$. However, a different type of rule applies when we study the divisibility of $Z(p)$ by both 2 and 5 *in conjunction*. This rule is considerably more complex than that indicated in Conjecture 2.1*, must be offered in the form of a (two-dimensional) table, and requires a special definition:

Given x, i, j, k, and l, with $i \geq j \geq 0$, $k \geq l \geq 0$, we let $M(2, 5, x; i, j; k, l)$ denote the number of $p \leq x$ such that $2^i5^k \| (p-\varepsilon_p)$ and $2^j5^l \| Z(p)$. Then the "$2^i, 2^j, 5^k, 5^l$ Z-density," denoted $\zeta(2, 5; i, j; k, l)$, is defined as follows:

$$\zeta(2,5;i,j;k,l) \equiv \lim_{x\to\infty} M(2,5,x;i,j;k,l)/\pi(x). \tag{2.3}$$

The numerical evidence, combined with general reasoning, suggests the following conjecture.

Conjecture 2.2*: $\zeta(2, 5; i, j; k, l)$.

$(i, j) \setminus (k, l)$:	$(0, 0)$	$k \geq 1$ $l = 0$	$k \geq l \geq 1$	Row Totals
$(0, 0)$	0	0	0	0
$(1, 0)$	$1/4$	0	0	$1/4$
$(1, 1)$	$1/8$	$1/2\cdot 5^{-2k}$	$2\cdot 5^{-1-2k+l}$	$1/4$
$i \geq 2,\ j = 0$	2^{-1-2i}	$2^{1-2i}5^{-2k}$	$2^{3-2i}5^{-1-2k+l}$	2^{-2i}
$(i, i),\ i \geq 2$	2^{-1-i}	0	0	2^{-1-i}
$i > j \geq 2$	$2^{-2-2i+j}$	$2^{-2i+j}5^{-2k}$	$2^{2-2i+j}5^{-1-2k+l}$	$2^{-1-2i+j}$
Column Totals	$3/4$	5^{-2k}	$4\cdot 5^{-1-2k+l}$	1

The row totals in Conjecture 2.2* are the sums over all $k \geq l \geq 0$ and are the $\zeta(2; i, j)$ obtained by setting $q = 2$ in Conjecture 2.1*. Likewise, the column totals are the sums over all $i \geq j \geq 0$ and are the $\zeta(5; k, l)$ obtained from Conjecture 2.1* by setting $q = 5$ and replacing (i, j) by (k, l). Therefore, our conjectures are mutually consistent.

The Z-densities introduced above give information about the divisibility properties of $(p-\varepsilon_p)$ and $Z(p)$. We now derive expressions for Z-densities that only yield information about the divisibility properties of $Z(p)$. Accordingly, we make the following definitions:

$$\zeta(q;j) \equiv \sum_{r\geq 0}\zeta(q;r+j,j); \tag{2.4}$$

$$\zeta(2,5;j,l) \equiv \sum_{r\geq 0}\sum_{s\geq 0}\zeta(2,5;r+j,j;s+l,l). \tag{2.5}$$

Note that $\zeta(q; j)$ is the density of those primes p for which $q^j \| Z(p)$, and $\zeta(2, 5; j, l)$ is the density of those p for which $2^j5^l \| Z(p)$. If we substitute the putative results from Conjectures 2.1*

and 2.2*, respectively, into the formulas indicated in (2.4) and (2.5), we obtain the following expressions:

$$\zeta(q; j) = \begin{cases} (q^2 - q - 1)/(q^2 - 1) & \text{if } j = 0, \\ q^{1-j}/(q+1) & \text{if } j \geq 1. \end{cases} \tag{2.6}^*$$

TABLE 2.1*. $\zeta(2, 5; j, l)$

	$l = 0$	$l \geq 1$	Row Totals
$j = 0$	$43/144$	$5^{1-l}/36$	$1/3$
$j = 1$	$7/36$	$5^{1-l}/9$	$1/3$
$j \geq 2$	$43 \cdot 2^{-j}/72$	$2^{-j}5^{1-l}/18$	$2^{1-j}/3$
Column Totals	$19/24$	$5^{1-l}/6$	1

The row totals in Table 2.1* coincide with the $\zeta(2; j)$ from (2.6)*; the column totals coincide with the $\zeta(5; l)$ from (2.6)* (obtained by setting $q = 5$ and replacing j by l).

We next require an additional set of Z-densities, this time involving mere divisibility of $Z(p)$ by q^j, instead of *exact* divisibility. Note that $q^j | Z(p)$ iff there exists some $r \geq 0$ such that $q^{r+j} \| Z(p)$. Since r satisfying this condition is arbitrary, this suggests the following relations:

$$\zeta(q^j) = \sum_{r \geq 0} \zeta(q; r + j); \tag{2.7}$$

$$\zeta(2^j s^l) = \sum_{r \geq 0} \sum_{s \geq 0} \zeta(2, 5; r + j, s + l). \tag{2.8}$$

The density $\zeta(2^j 5^l)$, according to definition (1.3), is the density of those p such that $2^j 5^l | Z(p)$.

Substituting the conditional results from (2.6)* and Table 2.1* into the expressions in (2.7) and (2.8), we obtain the following:

$$\zeta(q^j) = \begin{cases} 1 & \text{if } j = 0, \\ q^{2-j}/(q^2 - 1) & \text{if } j \geq 1; \end{cases} \tag{2.9}^*$$

$$\zeta(2^j 5^l) = \begin{cases} 1 & \text{if } j = l = 0, \\ 5^{2-l}/24 & \text{if } j = 0, l \geq 1, \\ 5^{3-l}/144 & \text{if } j = 1, l \geq 1, \\ 2^{2-j}/3 & \text{if } j \geq 1, l = 0, \\ 2^{-j}5^{2-l}/36 & \text{if } j \geq 2, l \geq 1. \end{cases} \tag{2.10}^*$$

Note that if we set $l = 0$ in (2.10)*, we obtain $\zeta(2^j)$ as indicated from (2.9)* with $q = 2$; likewise, setting $j = 0$ in (2.10)* yields $\zeta(5^l)$, obtained from (2.9)* by setting $q = 5$ and replacing j by l. Such numerical checks inspire confidence in the validity of our conjectures.

In the next section we use the conditional results obtained in this section to derive a general expression for $\zeta(m)$.

3. DERIVATION OF $\zeta(m)$

We would normally expect that the Z-densities satisfy a multiplicative property of sorts; naively, we might suppose that $\zeta(m) = \prod_{q^j \| m} \zeta(q^j)$. However, there is apparently a certain amount of "distortion" in this putative multiplicativity law, due to the presence of the "special" densities $\zeta(2^j 5^l)$ that might enter into the computation. In order to measure this distortion, we introduce a ratio defined as follows:

$$\rho(j, l) \equiv \zeta(2^j 5^l) / (\zeta(2^j)\zeta(5^l)). \tag{3.1}$$

Computing $\rho(j, l)$ from (2.9)* and (2.10)* is a relatively simple matter, and we obtain the following expressions:

$$\rho(j, l) = \begin{cases} 1/2 & \text{if } j \geq 2, l \geq 1, \\ 5/4 & \text{if } j = 1, l \geq 1, \\ 1 & \text{if } j = 0 \text{ or } l = 0. \end{cases} \tag{3.2}*$$

Based on the foregoing comments, we postulate the following "quasi-multiplicative" property.

Conjecture 3.1*:

$$\zeta(m) = \rho(j, l) \prod_{q^e \| m} \zeta(q^e), \text{ whenever } 2^j 5^l \| m.$$

We may also redefine $\rho(j, l)$ as an explicit function of m, as follows:

$$\rho(m) = \begin{cases} 1 & \text{if } 10 \nmid m, \\ 5/4 & \text{if } m \equiv 10 \pmod{20}, \\ 1/2 & \text{if } 20 \mid m. \end{cases} \tag{3.3}*$$

Therefore, our quasi-multiplicative property now takes the following form:

$$\zeta(m) = \rho(m) \prod_{q^j \| m} \zeta(q^j). \tag{3.4}*$$

We may now substitute the values of $\zeta(q^j)$ from (2.9)* into the formula given by (3.4)*. Note the following:

$$\zeta(m) / \rho(m) = \prod_{q^j \| m} q^{2-j} / (q^2 - 1) = t(m) / m, \text{ where}$$

$$t(m) \equiv \prod_{q \mid m} (1 - q^{-2})^{-1}, \ m > 1; \ t(1) = 1. \tag{3.5}$$

Therefore, we obtain our final formula for $\zeta(m)$:

$$\zeta(m) = \rho(m) t(m) / m, \tag{3.6}*$$

where $\rho(m)$ and $t(m)$ are given by (3.3)* and (3.5), respectively. As we may verify, this formula yields the known results: $\zeta(1) = 1$ and $\zeta(2) = 2/3$. Additional (conditional) results yielded by the

general formula in (3.6)* are as follows: $\zeta(3) = 3/8$, $\zeta(4) = 1/3$, $\zeta(5) = 5/24$, etc. The conditional result of (3.6)*, if true, implies that $\zeta(m)$ is rational (and positive) for all m.

Conditionally, the function $\zeta(m)$ is not multiplicative, while the function $\zeta(m)/\rho(m)$ *is*. Thus, if m and n are coprime, we have the interesting property

$$\zeta(mn) = \rho(mn)/(\rho(m)\rho(n)) \cdot \zeta(m)\zeta(n). \tag{3.7}*$$

Other interesting derived conditional properties of $\zeta(m)$ follow from (3.6)*. In the interest of brevity, we omit the demonstration of these properties, and merely indicate the results. For example, (3.6)* implies the following:

$$\sum_{m\geq 1} \zeta(m)/m = \frac{5 \cdot 7 \cdot 11 \cdot 31{,}277}{2^4 \cdot 601 \cdot 691} = 12{,}041{,}645/6{,}644{,}656. \tag{3.8}*$$

We may also show (conditionally) that the average order of $\zeta(m)$, over all $m \leq x$, if $O(\log x/x)$, but omit the demonstration.

We have omitted discussion of the densities of those p for which $Z(p) = m$, where m is a specified positive integer. Such a density relates to the number of *primitive prime divisors* (p.p.d.'s) of F_m, since these are precisely those primes p such that $Z(p) = m$. Hence, this density must be zero for all values of m, since the number of p.p.d.'s of F_m must be finite. On the other hand, the principles previously employed lead to a formula for such density in terms of the component densities obtained in Section 2. Proceeding thus, we find that each such resultant density has a "constant" multiplier denoted as δ, where

$$\delta \equiv \prod_p \{(p^2 - p - 1)/(p^2 - 1)\}. \tag{3.9}$$

However, the infinite product defining such "constant" δ diverges to zero. To see this, note that

$$0 \leq \delta = \prod_p \{(1 - p/(p^2 - 1)\} < \prod_p \{1 - 1/p\};$$

since it is well known that the latter product is divergent to zero, we see that $\delta = 0$. This, in turn, implies that the density of those primes p such that $Z(p) = m$, as anticipated.

From the definition of density and the Prime Number Theorem, we deduce that, for a given m, the number of p.p.d.'s of F_m is $o(x/\log x)$ for all $m \leq x$. In fact, it seems probable that the number of p.p.d.'s of F_m is $O(\log x)$, which is certainly $o(x/\log x)$. The conditional demonstration of this last statement is deferred, as it will be the subject of a future paper.

4. NUMERICAL VERIFICATION

In the interest of brevity, we have omitted all but one of the appendices that originally formed part of this paper. These contain the results of certain statistical tests conducted by the authors to test the validity of the conjectures. The tests were conducted by analyzing the data on $Z(p)$ and $p - \varepsilon_p$ for the first million primes (the highest such prime being 15,485,863). Although due caution is required in conducting any such tests, *if* we accept their validity, it may be stated with better than 95% statistical confidence that the conjectures are correct.

For the sake of demonstration, we have included one of these tests (in abridged form) in Appendix 1. Anyone interested in seeing the complete results of such analysis may contact either author for copies thereof.

The numerical evidence based on these studies supports our belief that the underlying conjectures made in this paper are correct. However, statistical corroboration does not constitute mathematical proof, and proof is what is required to establish these conjectures rigorously.

APPENDIX 1

$x = 15{,}485{,}863$; $\pi(x) = 1{,}000{,}000$

q	j	(1) $M(q, x; j)$	(2) $\zeta(q; j)$	(3) $\pi(x) \cdot \zeta(q; j)$	(4) = $[(1)-(3)]^2 \div (3)$
2	0	333,286	.3333333	333,333	0.0066
2	1	333,329	.3333333	333,333	0.0000
2	2	166,737	.1666667	166,667	0.0294
2	3	83,216	.0833333	83,333	0.1643
2	4	41,734	.0416667	41,667	0.1077
2	5	20,896	.0208333	20,833	0.1905
2	6	10,460	.0104167	10,417	0.1775
2	7	5,185	.0052083	5,208	0.1016
2	8	2,591	.0026042	2,604	0.0649
2	9	1,307	.0013021	1,302	0.0192
2	10	626	.0006510	651	0.9601
2	11	326	.0003255	326	0.0000
2	12	152	.0001628	163	0.7423
2	13	75	.0000814	81	0.4444
2	14	47	.0000407	41	0.8780
2	15	14	.0000203	20	1.8000
2	16-21	19	.0000200	20	0.0500
Totals for q = 2 :		1,000,000		999,999	5.7365
3	0	625,126	.6250000	625,000	0.0254
3	1	249,889	.2500000	250,000	0.0493
3	2	83,271	.0833333	83,333	0.0461
3	3	27,764	.0277778	27,778	0.0071
3	4	9,331	.0092593	9,259	0.5599
3	5	3,073	.0030864	3,086	0.0548
3	6	1,028	.0010288	1,029	0.0010
3	7	330	.0003429	343	0.4927
3	8	138	.0001143	114	5.0526
3	9	32	.0000381	38	0.9474
3	10-12	18	.0000183	18	0.0000
Totals for q = 3 :		1,000,000		999,998	7.2363

APPENDIX 1 (continued)

q	j	(1) M(q, x ; j)	(2) ζ(q ; j)	(3) π(x) · ζ(q ; j)	(4) = [(1)-(3)]² ÷(3)
5	0	791,679	.7916667	791,667	0.0002
5	1	166,700	.1666667	166,667	0.0065
5	2	33,272	.0333333	33,333	0.1116
5	3	6,612	.0066667	6,667	0.4537
5	4	1,396	.0013333	1,333	2.9775
5	5	278	.0002667	267	0.4532
5	6	51	.0000533	53	0.0755
5	7-8	12	.0000128	13	0.0769
Totals for q = 5 :		1,000,000		1,000,000	4.1551
7	0	854,407	.8541667	854,167	0.0674
7	1	124,742	.1250000	125,000	0.5325
7	2	17,907	.0178571	17,857	0.1400
7	3	2,533	.0025510	2,551	0.1270
7	4	356	.0003644	364	0.1758
7	5-7	55	.0000606	61	0.5902
Totals for q = 7 :		1,000,000		1,000,000	1.6329
11	0	908,281	.9083333	908,333	0.0030
11	1	83,400	.0833333	83,333	0.0539
11	2	7,581	.0075758	7,576	0.0033
11	3	676	.0006887	689	0.2453
11	4-5	62	.0000683	68	0.5294
Totals for q = 11 :		1,000,000		1,000,000	0.8349

SUMMARY

Grouped Values of q	Number of Values	Total Number of Data Points (n)	Chi-Square Statistic	χ^2 Value at 97.5% Confidence
2, 3	2	28	12.9728	14.5733
5,7,11	3	19	6.6229	8.2308
2,3,5,7,11	5	47	19.5957	27.60 (est.)

APPENDIX 1-SUMMARY (continued)

Explanation:

1. $M(q, x; j) = \sum_{i \geq 0} M(q, x; i + j, j)$ enumerates those primes $p \leq x$ such that, for the given prime q, $q^j \| Z(p)$.
2. Column (2) is obtained from the formula given in (2.6)*.
3. In the last data point for each q, values of $M(q, x; j)$ were aggregated with preceding values, in some cases, so as to make the aggregated value 12 or more. This was done to minimize the distortion in the calculated value of the Chi Square statistic. For these entries, Columns (2) and (3) reflect the sum of the values for the indicated values of j.
4. The values of χ^2 at the 97.5% confidence level are taken from *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, ed. M. Abramowitz & I. A. Stegun (National Bureau of Standards, 9th ptg., 1970). These values are read using $n - 1$ as the degrees of freedom.
5. In this Summary, the Chi Square statistic is less than the corresponding χ^2 value at the 97.5% confidence level. This latter amount is the value at which the "tail" of the distribution function, for the indicated degrees of freedom, is .025. Therefore, on the basis of this test alone, we would accept the conjecture in (2.6)* involving $q = 2, 3, 5, 7$, or 11, with 97.5% confidence.

ACKNOWLEDGMENTS

We wish to acknowledge the helpful suggestions and improvements contributed by the anonymous referees. Also, we wish to thank Dr. Daniel C. Fielder, Professor Emeritus of Georgia Institute of Technology, for providing one of the authors (Bruckman) with numerous computer runs and valuable assistance.

REFERENCES

1. C. Ballot. "Density of Prime Divisors of Linear Recurrences." *Memoirs of the Amer. Math. Soc.* **115.551** (1995) (Providence, RI.)
2. J. Brillhart, P. L. Montgomery, & R. D. Silverman. "Tables of Fibonacci and Lucas Factorizations." *Math. of Comp.* **50.181** (1988):251-60.
3. Bro. A. Brousseau, Compiler. *Fibonacci and Related Number Theoretic Tables.* San Jose: The Fibonacci Association, 1972.
4. Bro. A. Brousseau, Ed. *Tables of Fibonacci Entry Points, Part One.* Santa Clara: The Fibonacci Association, 1965.
5. Bro. A. Brousseau, Ed. *Tables of Fibonacci Entry Points, Part Two.* Santa Clara: The Fibonacci Association, 1965.
6. J. C. Lagarias. "The Set of Primes Dividing the Lucas Numbers Has Density 2/3." *Pacific J. Math.* **118.2** (1985):449-61.
7. E. Lucas. "Théorie des fonctions numeriqués simplement périodiques." *Amer. J. Math.* **1** (1898):184-240, 289-321.

AMS Classification Numbers: 11B05, 11B39, 11N25

❖❖❖

DISTRIBUTION OF BINOMIAL COEFFICIENTS MODULO THREE

Zachary M. Franco
Mathematics Department, Butler University, Indianapolis, IN 46208
e-mail: franco@butler.edu
(Submitted September 1996-Final Revision October 1997)

1. INTRODUCTION

In 1947, Fine [1] proved that almost all binomial coefficients are even. That is, if $T_2(n)$ is the number of odd binomial coefficients $\binom{m}{k}$ with $0 \le k \le m < n$, then $T_2(n) = o(n^2)$. In particular, since the total number of such binomial coefficients is $1+2+\cdots+n = \frac{1}{2}n^2 + \frac{1}{2}n$, the proportion of odd coefficients tends to 0 with n. In 1977, Harborth [3] improved this estimate to

$$.812556n^{\log_2 3} \le T_2(n) \le n^{\log_2 3},$$

and although the best constant in the lower bound has been calculated to great accuracy [2], its exact value is still unknown. The behavior of $T_2(n)$ and its generalizations to $T_p(n)$ for prime p have also been studied by Howard [4], Singmaster [6], Stein [7], and Volodin [8]. In the following definitions, let $\binom{0}{0} = 1$. For any prime p, it is convenient to let $P = \binom{p+1}{2}$, $\theta_p = \log_p P$, and to let $S_p(n)$ denote the number of binomial coefficients $\binom{n}{r}$ that are not divisible by p. Then

$$T_p(n) = \sum_{k=0}^{n-1} S_p(k)$$

is the number of binomial coefficients in the first n rows of Pascal's triangle that are not divisible by p. It is known (see [3] and [7]) that the quotient $R_p(n) = T_p(n)/n^{\theta_p}$ is bounded above by $\alpha_p = \sup_{n\ge 1} R_p(n) = 1$ and below by $\beta_p = \inf_{n\ge 1} R_p(n)$. The β_p tend to $\frac{1}{2}$ with p [2], but to this point no exact values for β_p have been found.

2. THE CASE $p = 3$

Henceforth, the terms θ, R, S, T shall denote θ_3, R_3, S_3, T_3, respectively. Also, let

$$n = \sum_{i=1}^{k} a_i 3^{r_i}$$

be n's base-three representation, where each $a_i = 1$ or 2 and $r_1 > r_2 > \cdots > r_k \ge 0$. We list the first few values of $S(n)$, $T(n)$, and $R(n)$ in Table 1.

We shall confirm a conjecture of Volodin [8], namely that $\inf_{n\ge 1} R(n) = 2^{\log_3 2 - 1} = .77428$. The fractal nature of Pascal's triangle modulo 3 implies (see [5], Cor. 2, p. 367) the following recursive formula for T:

$$T(a\cdot 3^s + b) = \frac{1}{2}a(a+1)6^s + (a+1)T(b) \quad \text{for } a = 1 \text{ or } 2,\ b < 3^s.$$

It follows by iteration that

$$T\left(\sum_{i=1}^{k} a_i 3^{r_i}\right) = \frac{1}{2}\sum_{i=1}^{k} a_i(a_1+1)\cdots(a_i+1)6^{r_i}. \tag{1}$$

n	$S(n)$	$T(n)$	$R(n)$	n	$S(n)$	$T(n)$	$R(n)$	n	$S(n)$	$T(n)$	$R(n)$
0	1	0		10	4	38	.88890	20	9	117	.88368
1	2	1	1	11	6	42	.84103	21	6	126	.87887
2	3	3	.96864	12	4	48	.83401	22	8	132	.85345
3	2	6	1	13	8	52	.79294	23	18	144	.86592
4	4	8	.83401	14	12	60	.81077	24	9	162	.87887
5	6	12	.86938	15	6	72	.86938	25	18	171	.89754
6	3	18	.96864	16	18	78	.84773	26	27	189	.93055
7	6	21	.87887	17	12	.96	.94514	27	2	216	1
8	9	27	.90884	18	3	108	.96864	40	16	320	.78037
9	2	36	1	19	6	111	.91152	121	32	1936	.77630

3. MAIN RESULT

Theorem 1: The number of binomial coefficients $\binom{m}{k}$, $k \le m < n$, that are not divisible by 3 is bounded below by $2^{\log_3 2 - 1} n^{\log_3 6}$ and this bound is sharp.

Proof: Let the two sequences $\mathbf{x}$, $\mathbf{y}$ be defined by

$$x_i = 3^{r_i}\left[\frac{1}{2}a_i(a_1+1)\cdots(a_i+1)\right]^{\frac{1}{\theta}} \quad \text{and} \quad y_i = a_i\left[\frac{1}{2}a_i(a_1+1)\cdots(a_i+1)\right]^{\frac{-1}{\theta}},\ 1 \le i \le k.$$

We apply Hölder's inequality to the sequences $\mathbf{x}$, $\mathbf{y}$ with the conjugate exponents $\theta = \log_3 6$ and $\theta' = \log_2 6$:

$$\sum_{i=1}^{k} x_i y_i \le \left(\sum_{i=1}^{k} x_i^{\theta}\right)^{\frac{1}{\theta}} \cdot \left(\sum_{i=1}^{k} y_i^{\theta'}\right)^{\frac{1}{\theta'}},$$

$$n \le \left(\sum_{i=1}^{k}\left\{3^{r_i}\left[\frac{1}{2}a_i(a_1+1)\cdots(a_i+1)\right]^{\frac{1}{\theta}}\right\}^{\theta}\right)^{\frac{1}{\theta}} \cdot \left(\sum_{i=1}^{k}\left\{a_i\left[\frac{1}{2}a_i(a_1+1)\cdots(a_i+1)\right]^{\frac{-1}{\theta}}\right\}^{\theta'}\right)^{\frac{1}{\theta'}},$$

$$n^{\theta} \le \left(\sum_{i=1}^{k} 6^{r_i}\frac{1}{2}a_i(a_1+1)\cdots(a_i+1)\right) \cdot \left(\sum_{i=1}^{k} a_i^{\theta'}\left[\frac{1}{2}a_i(a_1+1)\cdots(a_i+1)\right]^{-\frac{\theta'}{\theta}}\right)^{\frac{\theta}{\theta'}},$$

$$R(n) \ge \frac{1}{2}\left(\sum_{i=1}^{k} a_i\left[(a_1+1)\cdots(a_i+1)\right]^{-\frac{\theta'}{\theta}}\right)^{-\frac{\theta}{\theta'}}. \tag{2}$$

Let $v = \theta'/\theta = \log_2 3 = 1.58496$ and let

$$U_k = \sum_{i=1}^{k} a_i\left[(a_1+1)\cdots(a_i+1)\right]^{-v}.$$

Note that $U_k = f_1 \circ f_2 \circ f_3 \circ \cdots \circ f_k(0)$, where

$$f_i(x) = \frac{x + a_i}{(a_i + 1)^v}.$$

Each f_i is one of the two increasing functions $\frac{x+1}{3}$ or $\frac{x+2}{3^v}$ and U_k will be maximized when each a_i is chosen to maximize f_i. For a given x, we find that $\frac{x+1}{3} > \frac{x+2}{3^v}$ (i.e., $a_i = 1$) if and only if $x > .109253$. So, for $x = 0$, $f_k(0)$ is maximized when $a_k = 2$. For $i < k$, $f_i(x)$ is maximized when $a_i = 1$ since x will now be in the range of f_i and, hence, $\geq \frac{1}{3}$. Thus,

$$\begin{aligned} U_k &\leq \frac{1}{2^v} + \frac{1}{2^{2v}} + \cdots + \frac{1}{2^{(k-1)v}} + \frac{2}{2^{(k-1)v} \cdot 3^v} \\ &= \frac{1}{3} + \frac{1}{3^2} + \cdots + \frac{1}{3^{k-1}} + \frac{2}{3^{k-1} \cdot 3^v} = \frac{1}{2} - \frac{\frac{1}{2} - 2 \cdot 3^{-v}}{3^{k-1}} \\ &\leq \frac{1}{2} \quad \text{since } \frac{1}{2} - 2 \cdot 3^{-v} > 0. \end{aligned}$$

Hence, from (2) we have, for all n,

$$R(n) \geq \frac{1}{2}(U_k)^{-\frac{1}{v}} > \left(\frac{1}{2}\right)^{1-\frac{1}{v}} = 2^{\log_3 2 - 1},$$

whence

$$\beta_3 \geq \left(\frac{3}{2}\right)^{-\frac{1}{v}} = 2^{\log_3 2 - 1}.$$

We now consider numbers of the form $1 + 3 + 3^2 + 3^3 + \cdots + 3^k$. It follows from (1) that

$$\begin{aligned} R(1 + 3 + 3^2 + 3^3 + \cdots + 3^k) &= \frac{\frac{1}{2}(2 \cdot 6^k + 2^2 \cdot 6^{k-1} + \cdots + 2^{k+1})}{(1 + 3 + 3^2 + 3^3 + \cdots + 3^k)^{\log_3 6}} \\ &= \frac{2^k(3^k + 3^{k-1} + \cdots + 1)}{\left(\frac{3^{k+1}-1}{2}\right)^{\log_3 6}} = \frac{2^k}{\left(\frac{3^{k+1}-1}{2}\right)^{\log_3 2}} = \frac{2^{k+1}}{(3^{k+1} - 1)^{\log_3 2}} \cdot 2^{\log_3 2 - 1} \end{aligned}$$

so that $\lim_{k \to \infty} R(1 + 3 + 3^2 + 3^3 + \cdots + 3^k) = 2^{\log_3 2 - 1}$.

Hence, $\beta_3 \leq 2^{\log_3 2 - 1}$. This implies $\beta_3 = 2^{\log_3 2 - 1}$ and $T(n) > 2^{\log_3 2 - 1} n^{\log_3 6}$, the desired result. Note that n and $T(n)$ are integers, so there is strict inequality.

The proof of Theorem 1 works because the sequence $\{1, 1, 1, \ldots\}$ that minimizes $R(n)$ gives rise to sequences x_i, y_i for which equality holds in Hölder's inequality. This does not occur for $p \neq 3$, so the proof does not extend to other primes.

ACKNOWLEDGMENT

I am grateful to Richard Bumby for suggesting this topic to me and to John Gaisser for his many helpful comments.

REFERENCES

1. N. J. Fine. "Binomial Coefficients Modulo a Prime." *Amer. Math. Monthly* **54** (1947):589-92.
2. Z. Franco. "On the Distribution of Binomial Coefficients Modulo p." To appear in *Proceedings of the Diophantine Conference at Eger*. De Gruyter, 1998.

3. H. Harborth. "Number of Odd Binomial Coefficients." *Proc. Amer. Math. Soc.* **62** (1977): 19-22.
4. F. T. Howard. "The Number of Binomial Coefficients Divisible by a Fixed Power of a Prime." *Proc. Amer. Math. Soc.* **37** (1973):358-62.
5. J. R. Roberts. "On Binomial Coefficient Residues." *Canadian J. Math.* **9** (1957):363-70.
6. D. Singmaster. "Notes on Binomial Coefficients III–Any Integer Divides Almost All Binomial Coefficients." *J. London Math. Soc.* **8** (1974):555-60.
7. A. H. Stein. "Binomial Coefficients Not Divisible by a Prime." In *Lecture Notes in Mathematics* **1383:**170-77. Berlin-New York: Springer Verlag, 1989.
8. N. A. Volodin. "Number of Multinomial Coefficients Not Divisible by a Prime." *The Fibonacci Quarterly* **22.5** (1994):402-06.

AMS Classification Numbers: 11B37, 11B65

❖❖❖

A LETTER OF GRATITUDE

The Editor of The Fibonacci Quarterly *and the Board of Directors of The Fibonacci Association wish to express their sincere gratitude to those Fibonacci members who have provided financial support over and above their annual membership renewal dues.*

During its 35 years of operation as a nonprofit corporation, The Fibonacci Association has kept its membership dues at the minimum level needed to produce and distribute four issues of the Quarterly *each year.*

As total membership has increased through the years, so has the number of articles submitted for evaluation and acceptance for publication. To maintain a reasonable backlog of articles approved for publication, it has occasionally been necessary to publish an extra issue of the Quarterly *to attain a minimum lead time from final approval of an article to its actual publication.*

Inasmuch as maintaining a minimum level of membership dues and publishing extra issues of The Fibonacci Quarterly *is a mutually exclusive situation, the additional financial support provided by our members at the time of membership renewal is deeply appreciated.*

Gerald E. Bergum, Editor

CONGRUENCES MOD p^n FOR THE BERNOULLI NUMBERS

A. Simalarides
196 Kifissias Str., Kifissia 14562, Athens, Greece
(Submitted September 1996)

1. INTRODUCTION

Let p be a prime. In 1889 Voronoi proved the congruence

$$(a-a^{p-2k})\frac{B_{2k}}{2k} \equiv \sum_{s=1}^{p-1}\left[\frac{sa}{p}\right]s^{2k-1} \pmod{p}, \tag{1}$$

where k, a are positive integers such that p does not divide a and $p-1$ does not divide $2k$; B_{2k} is the $2k^{\text{th}}$ Bernoulli number. More general versions of this congruence can be found in [6] or [3]. Following Wagstaff, denote congruence (1) also by the symbol $\{a\}$. Adding together congruences $\{2\}$, $\{3\}$, and $-\{4\}$, we obtain the congruence

$$\{2\}+\{3\}-\{4\}$$

which, after some obvious cancellations in the right member, takes the form

$$(2^{p-2k}+3^{p-2k}-4^{p-2k}-1)\frac{B_{2k}}{4k} \equiv \sum_{p/4<s<p/3} s^{2k-1} \pmod{p}, \tag{2}$$

provided that $p>4$. Several such identities are also obtainable in a way analogous to that shown above by using suitable variations of parameter a. Several authors used formulas of this type to test regularity via computer. The best result in this direction is the following one, due to Tanner and Wagstaff [5], which is valid for all primes $p>10$,

$$\begin{aligned}(2^{p-2k}+9^{p-2k}-10^{p-2k}-1)\frac{B_{2k}}{4k} &\equiv (1+2^{2k-1}+3^{2k-1}+4^{2k-1})\sum_{\frac{p}{10}<s<\frac{13p}{120}} s^{2k-1}\\ &+(1+2^{2k-1}+3^{2k-1}+4^{2k-1}+12^{2k-1})\sum_{\frac{13p}{120}<s<\frac{p}{9}} s^{2k-1}\\ &-3^{2k-1}\sum_{\frac{2p}{9}<s<\frac{7p}{30}} s^{2k-1}-(2^{2k-1}+6^{2k-1})\sum_{\frac{5p}{18}<s<\frac{17p}{60}} s^{2k-1}\\ &-2^{2k-1}\sum_{\frac{17p}{60}<s<\frac{3p}{10}} s^{2k-1}-(2^{2k-1}+4^{2k-1}+12^{2k-1})\sum_{\frac{7p}{18}<s<\frac{47p}{120}} s^{2k-1}\\ &-(2^{2k-1}+4^{2k-1})\sum_{\frac{47p}{120}<s<\frac{2p}{5}} s^{2k-1} \pmod{p}.\end{aligned} \tag{3}$$

In formula (3), the sums in the right member contain a total of about $p/18$ terms [formula (2) contains about $p/12$ terms while formula (1) contains $(p-1)/2$ terms for $a=2$]. All the applications of these formulas concerning Fermat's Last Theorem are now mainly of historical interest

after Wiles's proof [8] of FLT. There are congruences of various types for the Bernoulli numbers. Recent results on congruences for Bernoulli numbers of higher order can be found in [2].

We shall prove the following analog of formula (1).

Theorem 1: Let χ be a primitive Dirichlet character with modulus $m \geq 2$. If $a \geq 2$ is an integer such that m does not divide a, then

$$\sum_{s=1}^{m-1} \left[\frac{sa}{m}\right] \chi(s) = \begin{cases} 0 & \text{if } \chi \text{ is even,} \\ -\dfrac{\overline{\chi}(a)-a}{\overline{\chi}(2)-2} \displaystyle\sum_{s=1}^{[m/2]} \chi(s) & \text{if } \chi \text{ is odd,} \end{cases} \tag{4}$$

where the bar means complex conjugation.

The proof of Theorem 1 will be given in Section 2. Formula (4) can be written, equivalently, in the form

$$\sum_{s=1}^{m-1} \left[\frac{sa}{m}\right] \chi(s) = \begin{cases} 0 & \text{if } \chi \text{ is even,} \\ \dfrac{a-\overline{\chi}(a)}{m} \displaystyle\sum_{s=1}^{m-1} s\chi(s) & \text{if } \chi \text{ is odd,} \end{cases} \tag{5}$$

because of the formula

$$\sum_{s=1}^{m-1} s\chi(s) = \frac{m}{\overline{\chi}(2)-2} \sum_{s=1}^{[m/2]} \chi(s), \tag{6}$$

which is valid for an odd primitive character χ.

We use formula (5) to obtain p^n-divisibility criteria for Bernoulli numbers of the form

$$B_{(2k-1)p^n+1}, \quad k = 1, 2, \ldots, \frac{p-3}{2}.$$

Criteria of this type are still of interest because of their connection with the invariants of the irregular class group of a properly irregular cyclotomic field [7] (cf. also [4], p. 189). Assume now that $m = p$, an odd prime. Let ψ be the character defined as the p-adic limit

$$\psi(s) = \lim_{n\to\infty} s^{p^n}$$

for every s prime to p. All the values of ψ belong to $\mathbb{Z}_p$, the ring of p-adic integers. Moreover,

$$\psi(s) \equiv s^{p^{n-1}} \pmod{p^n}, \quad n \geq 1.$$

For an odd character, we have $\chi = \psi^{2k-1}$, for some $k \geq 1$, and

$$\chi(s) \equiv s^{(2k-1)p^{n-1}} \pmod{p^n},$$

$$\overline{\chi}(s) \equiv s^{-p^{n-1}(2k-1)} \equiv s^{p^{n-1}(p-1)-p^{n-1}(2k-1)} \equiv s^{p^{n-1}(p-2k)} \pmod{p^n}.$$

Theorem 2: Let p be a prime >3. If a is an integer such that p does not divide a, then

$$[a - a^{p^{n-1}(p-2k)}] B_{(2k-1)p^n+1} \equiv \sum_{s=1}^{p-1} \left[\frac{sa}{p}\right] s^{(2k-1)p^{n-1}} \pmod{p^n}, \tag{7}$$

for every $k \geq 1$ such that $p-1$ does not divide $2k$.

Proof: We consider the n^{th} Bernoulli polynomial

$$B_n(x) = \sum_{j=0}^{n} \binom{n}{j} B_j x^{n-j}, \quad n \geq 1.$$

Then, for the odd character $\chi = \psi^{2k-1}$, we have

$$\begin{aligned}\sum_{s=1}^{p-1} s\chi(s) &\equiv \sum_{s=1}^{p} s^{(2k-1)p^n+1} \equiv \frac{B_{(2k-1)p^n+2}(p) - B_{(2k-1)p^n+2}}{(2k-1)p^n+2} \\ &\equiv pB_{(2k-1)p^n+1} + \frac{[(2k-1)p^n+1](2k-1)p^n}{3!} p^3 B_{(2k-1)p^n-1} + \cdots \\ &\equiv pB_{(2k-1)p^n+1} \pmod{p^{n+1}}.\end{aligned}$$

Since $p-1$ does not divide $2k$, we obtain the congruence

$$\frac{1}{p}\sum_{s=1}^{p-1} s\chi(s) \equiv B_{(2k-1)p^n+1} \pmod{p^n},$$

which, together with Theorem 1 and relation (5), yields the sought result.

For $n = 1$, congruence (7) reduces to congruence (1) since

$$B_{(2k-1)p+1} = [(2k-1)p+1]\frac{B_{(2k-1)p+1}}{(2k-1)p+1} \equiv \frac{B_{2k}}{2k} \pmod{p}$$

because of Kummer's congruence.

We can prove, using exactly analogous techniques and starting from (7), a p^n-analog of congruence (3). Because of the obvious analogy between the proofs, the sought result follows simply by replacing expressions of the form

$$a^{p-2k}, \quad a^{2k-1}, \quad s^{2k-1}, \quad \frac{B_{2k}}{2k}$$

in congruence (3) with the respective expressions

$$a^{p^{n-1}(p-2k)}, \quad a^{(2k-1)p^{n-1}}, \quad s^{(2k-1)p^{n-1}}, \quad B_{(2k-1)p^n+1}.$$

The following theorem then follows.

Theorem 3: Let p be an odd prime >10, $k \geq 1$, $p-1$ does not divide $2k$ and $n \geq 1$. Then

$$\begin{aligned}&\frac{2^{(p-2k)p^{n-1}} + 9^{(p-2k)p^{n-1}} - 10^{(p-2k)p^{n-1}} - 1}{2} B_{(2k-1)p^n+1} \\ &\equiv [1 + 2^{(2k-1)p^{n-1}} + 3^{(2k-1)p^{n-1}} + 4^{(2k-1)p^{n-1}}] \sum_{\frac{p}{10}<s<\frac{13p}{120}} s^{(2k-1)p^{n-1}} \\ &\quad + [1 + 2^{(2k-1)p^{n-1}} + 3^{(2k-1)p^{n-1}} + 4^{(2k-1)p^{n-1}} + 12^{(2k-1)p^{n-1}}] \sum_{\frac{13p}{120}<s<\frac{p}{9}} s^{(2k-1)p^{n-1}} \\ &\quad - 3^{(2k-1)p^{n-1}} \sum_{\frac{2p}{9}<s<\frac{7p}{30}} s^{(2k-1)p^{n-1}} - [2^{(2k-1)p^{n-1}} + 6^{(2k-1)p^{n-1}}] \sum_{\frac{5p}{18}<s<\frac{17p}{60}} s^{(2k-1)p^{n-1}}\end{aligned}$$

$$-2^{(2k-1)p^{n-1}}\sum_{\frac{17p}{60}<s<\frac{3p}{10}}s^{(2k-1)p^{n-1}}-[2^{(2k-1)p^{n-1}}+4^{(2k-1)p^{n-1}}+12^{(2k-1)p^{n-1}}]\sum_{\frac{7p}{18}<s<\frac{47p}{120}}s^{(2k-1)p^{n-1}}$$

$$-[2^{(2k-1)p^{n-1}}+4^{(2k-1)p^{n-1}}]\sum_{\frac{47p}{120}<s<\frac{2p}{5}}s^{(2k-1)p^{n-1}}\pmod{p^n}.$$

The congruence contains in the right member $p/18$ terms only.

2. PROOF OF THEOREM 1

At first, we note that, obviously,

$$-\sum_{s=1}^{m-1}\left[\frac{sa}{m}\right]\chi(s)=\sum_{j=1}^{a}\sum_{s=0}^{[jm/a]}\chi(s). \tag{8}$$

For integer j, $0<j\le a$, define

$$\Phi(x)=\begin{cases}\frac{1}{2} & \text{if } x=0 \text{ or } 2\pi j/a,\\ 1 & \text{if } 0<x<2\pi j/a,\\ 0 & \text{if } 2\pi j/a<x<2\pi,\end{cases}$$

and continue $\Phi(x)$ periodically with period 2π over the real numbers. The function $\Phi(x)$ has the Fourier expansion

$$\Phi(x)=\sum_{n=-\infty}^{\infty}c_n e^{inx}\quad (i=\sqrt{-1}),$$

where

$$c_n=\frac{1}{2\pi}\int_0^{2\pi}\Phi(x)e^{-inx}dx=\frac{i}{2\pi n}(e^{-\frac{2\pi ijn}{a}}-1).$$

First, we assume that $a<m$. Then

$$\begin{aligned}\sum_{s=0}^{[jm/a]}\chi(s)&=\sum_{s=1}^{m-1}\chi(s)\,\Phi\left(\frac{2\pi s}{m}\right)\\ &=\frac{i}{2\pi}\sum_{s=1}^{m-1}\chi(s)\sum_{n=-\infty}^{\infty}\frac{(e^{-\frac{2\pi ijn}{a}}-1)e^{\frac{2\pi is}{m}n}}{n}\\ &=\frac{i}{2\pi}\sum_{n=-\infty}^{\infty}\frac{e^{-\frac{2\pi ijn}{a}}-1}{n}\sum_{s=1}^{m-1}\chi(s)e^{\frac{2\pi is}{m}n}\\ &=\frac{\tau(\chi)i}{2\pi}\sum_{n=-\infty}^{\infty}\frac{(e^{-\frac{2\pi ijn}{a}}-1)\overline{\chi}(n)}{n},\end{aligned}$$

where

$$\tau(\chi)=\sum_{s=1}^{m-1}\chi(s)e^{\frac{2\pi is}{m}}.$$

As a consequence,

$$\sum_{j=1}^{a}\sum_{s=0}^{[jm/a]}\chi(s)=\frac{\tau(\chi)i}{2\pi}\sum_{n=-\infty}^{\infty}\frac{\overline{\chi}(n)}{n}\left(\sum_{j=1}^{a}e^{-\frac{2\pi ijn}{a}}-a\right)$$

$$=\frac{\tau(\chi)i}{2\pi}\sum_{n=-\infty}^{\infty}\frac{\overline{\chi}(n)}{n}\sum_{j=1}^{a}e^{-\frac{2\pi ijn}{a}}-\frac{\tau(\chi)ia}{2\pi}\sum_{n=-\infty}^{\infty}\frac{\overline{\chi}(n)}{n}.$$

Since

$$\sum_{j=1}^{a}e^{-\frac{2\pi ijn}{a}}=\begin{cases}a & \text{if } n\equiv 0\ (\mathrm{mod}\ a),\\ 0 & \text{if } n\not\equiv 0\ (\mathrm{mod}\ a),\end{cases}$$

it follows that

$$\sum_{j=1}^{a}\sum_{s=0}^{[jm/a]}\chi(s)=\frac{\tau(\chi)i}{2\pi}\sum_{n=-\infty}^{\infty}\frac{\overline{\chi}(na)}{na}a-\frac{\tau(\chi)i}{2\pi}\sum_{n=-\infty}^{\infty}\frac{\overline{\chi}(n)}{n}$$

$$=\frac{\tau(\chi)i}{2\pi}(\overline{\chi}(a)-a)\sum_{n=-\infty}^{\infty}\frac{\overline{\chi}(n)}{n}.$$

For even χ, the last infinite sum is equal to zero while, for odd χ, it is equal to $2L(1,\overline{\chi})$. In view of the formula (cf. [1], p. 336)

$$L(1,\overline{\chi})=\frac{\pi i}{(2-\overline{\chi}(2))\,\tau(x)}\sum_{s=1}^{[m/2]}\chi(s)$$

and relation (8), it follows that

$$\sum_{s=1}^{m-1}\left[\frac{sa}{m}\right]\chi(s)=-\frac{\overline{\chi}(a)-a}{\overline{\chi}(2)-2}\sum_{s=1}^{[m/2]}\chi(s) \tag{9}$$

for $a<m$. It remains to prove the theorem for $a>m$. Then $a=a_1+mt$, where a_1 and t are integers and $0<a_1<m$. Also m does not divide a_1. We have

$$\sum_{s=1}^{m-1}\left[\frac{sa}{m}\right]\chi(s)=\sum_{s=1}^{m-1}\left[\frac{sa_1}{m}+st\right]\chi(s)$$

$$=\sum_{s=1}^{m-1}\left[\frac{sa_1}{m}\right]\chi(s)+t\sum_{s=1}^{m-1}s\chi(s).$$

The last expression is zero for even χ. For odd χ we have, in view of (6) and (9),

$$\sum_{s=1}^{m-1}\left[\frac{sa}{m}\right]\chi(s)=-\frac{\overline{\chi}(a_1)-a_1}{\overline{\chi}(2)-2}\sum_{s=1}^{[m/2]}\chi(s)+\frac{tm}{\overline{\chi}(2)-2}\sum_{s=1}^{[m/2]}\chi(s)$$

$$=-\frac{\overline{\chi}(a)-(a_1+tm)}{\overline{\chi}(2)-2}\sum_{s=1}^{[m/2]}\chi(s)$$

$$=-\frac{\overline{\chi}(a)-a}{\overline{\chi}(2)-2}\sum_{s=1}^{[m/2]}\chi(s),$$

which proves the theorem for $a>m$.

REFERENCES

1. Z. I. Borevich & I. R. Shafarevich. *Number Theory.* New York: Academic Press, 1966.
2. F. T. Howard. "Congruences and Recurrences for Bernoulli Numbers of Higher Order." *The Fibonacci Quarterly* **32.4** (1994):316-28.
3. K. Ireland & M. Rosen. *A Classical Introduction to Modern Number Theory.* New York and Berlin: Springer-Verlag, 1982.
4. P. Ribenboim. *13 Lectures on Fermat's Last Theorem.* New York and Berlin: Springer-Verlag, 1979.
5. J. W. Tanner & S. S. Wagstaff. "New Congruences for the Bernoulli Numbers." *Math. of Comp.* **48** (1987):341-50.
6. J. V. Uspensky & M. A. Heaslet. *Elementary Number Theory.* New York: McGraw-Hill, 1939.
7. H. S. Vandiver. "On the Composition of the Group of Ideal Classes in a Properly Irregular Cyclotomic Field." *Monatsh. f. Math. u. Phys.* **48** (1939):369-80.
8. A. Wiles. "Modular Elliptic Curves and Fermat's Last Theorem." *Annals of Math.* **142** (1995):443-551.

AMS Classification Number: 11B68

❖❖❖

EQUATIONS OF THE BRING-JERRARD FORM, THE GOLDEN SECTION, AND SQUARE FIBONACCI NUMBERS

Michele Elia
Dip. di Elettronica, Politecnico di Torino, I-10129 Torino, Italy; e-mail: elia@polito.it

Piero Filipponi
Fondazione Ugo Bordoni, I-00142 Rome, Italy; e-mail: filippo@fub.it
(Submitted September 1996-Final Revision February 1997)

1. INTRODUCTION

A curious problem is that of finding closed-form expressions for the positive real numbers (say x) that preserve their fractional parts when raised to the k^{th} power ($k \geq 2$, an integer). It is quite obvious that all the positive integers enjoy this property.

Since no positive number less than 1 can enjoy it, the numbers x are characterized by the fact that x^k diminished by x equals a nonnegative integer. In other words, the numbers in question are given by the *positive* roots $x_n(k)$ of the k^{th} ($k \geq 2$) degree equation

$$x^k - x = n. \tag{1.1}$$

where n is an arbitrary *nonnegative* integer. Equations like (1.1) are said to be of the Bring-Jerrard form [1, pp. 179-81]. Observe that the positive integers emerge as solutions of (1.1) when $n = a^k - a$ ($a = 1, 2, 3, \ldots$).

From this point on, the symbol $x_n(k)$ ($n = 0, 1, 2, \ldots$) will denote the n^{th} positive real number that preserves its fractional part when raised to the power k.

The case $k = 2$ has been considered in [4]. In that article k was allowed to assume negative values also, and the author proved that the golden section $\alpha = (1+\sqrt{5})/2 = x_1(-1) = x_1(2)$ is the only nonintegral number that preserves its fractional part both when one squares it and when one takes its reciprocal.

In this article we extend this study by considering the cases $k = 3, 4$, and 5. The solutions for $k = 3$ and 4 are readily found as the closed form expressions for third- and fourth-degree equations are known; we show them only for the sake of completeness. Solving the case $k = 5$ has been a bit more complicated, and is our main result. More precisely, we have established the closed-form expressions for the *only* three nonintegral numbers $x_n(5)$ for which it can be given: these numbers are $x_{15}(5)$, $x_{22440}(5)$, and $x_{2759640}(5)$. This assertion comes from the fact that the quintic of the Bring-Jerrard form $x^5 - x - r$ ($r \in \mathbb{Z}$) can be solved by radicals iff either $r = m^5 - m$, or $r = \pm 15, \pm 22440$, or ± 2759640. The proof of this result involves a well-known property [2] of the Fibonacci numbers F_j.

2. THE NUMBERS $x_n(k)$ FOR $k = 2, 3$ AND 4

By using (1.1) and the well-known formulas for the solution of second-, third-, and fourth-degree equations, the following results have been established:

$$x_n(2) = (1+\sqrt{4n+1})/2 \quad (n = 0, 1, 2, \ldots) \quad \text{(see [4])}, \tag{2.1}$$

$$x_n(3)=\sqrt[3]{\frac{n}{2}-\sqrt{\left(\frac{n}{2}\right)^2-\frac{1}{27}}}+\sqrt[3]{\frac{n}{2}+\sqrt{\left(\frac{n}{2}\right)^2-\frac{1}{27}}}\quad (n=0,1,2,\ldots), \tag{2.2}$$

and

$$x_n(4)=\frac{\sqrt{y_n}+\sqrt{-y_n+2\sqrt{y_n^2+4n}}}{2}\quad (n=0,1,2,\ldots), \tag{2.3}$$

where

$$y_n=\sqrt[3]{\frac{1}{2}-\sqrt{\left(\frac{4n}{3}\right)^3+\frac{1}{4}}}+\sqrt[3]{\frac{1}{2}+\sqrt{\left(\frac{4n}{3}\right)^3+\frac{1}{4}}}. \tag{2.4}$$

A Remark: If $n=0$, then $x_n(2)$ and $x_n(4)$ defined by (2.1) and (2.3), respectively, clearly equal 1, as expected. Let us show that $x_0(3)$ defined by (2.2) equals 1 as well. In fact, letting $n=0$ in (2.2) gives

$$x_0(3)=\sqrt[3]{-\sqrt{-\frac{1}{27}}}+\sqrt[3]{\sqrt{-\frac{1}{27}}}=\sqrt[6]{\frac{1}{27}}\left[\sqrt[3]{-i}+\sqrt[3]{i}\right], \tag{2.5}$$

where i is the imaginary unit. Considering the principal values of the cubic roots in (2.5) yields

$$\begin{aligned}x_0(3)&=\sqrt{\frac{1}{3}}\left(\cos\frac{\pi}{6}-i\sin\frac{\pi}{6}+\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}\right)\\&=2\sqrt{\frac{1}{3}}\cos\frac{\pi}{6}=\sqrt{\frac{1}{3}}\sqrt{3}=1\end{aligned}$$

as expected.

3. SOLVING x^5-x-r

The quintic $q(x)=x^5-x-r$ $(r\in\mathbb{Z})$ may be either irreducible or reducible over the rational field $\mathbb{Q}$. If it is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$ as well [9, Th. 23, p. 24]. Necessary and sufficient conditions for its decomposition are given in [8]. Since the argument leading to the complete characterization of the quintics $q(x)$ that are solvable by radicals is based essentially on properties of irreducible quintics, we settle first the irreducible case, then we complete the discussion by addressing the reducible case.

3.1 The Irreducible Case

We shall prove that, if $q(x)$ is irreducible over $\mathbb{Q}$, then it cannot be solved by radicals. To this aim, we need the following theorem by Dummit [3, p. 389] that we quote in a form specialized to our Bring-Jerrard quintic $q(x)$.

Theorem 1 (Dummit): If $q(x)=x^5-x-r$ $(r\in\mathbb{Z})$ is irreducible, then it can be solved by radicals iff the polynomial

$$x^6-8x^5+40x^4-160x^3+400x^2-(3125r^4+512)x+(9375r^4+256) \tag{3.1}$$

has a rational root. If this is the case, then the polynomial (3.1) factors into the product of a linear polynomial and an irreducible quintic.

Next we state our main theorem.

Theorem 2: If $q(x) = x^5 - x - r$ $(r \in \mathbb{Z})$ is irreducible, then it cannot be solved by radicals.

Proof (reductio ad absurdum): From Theorem 1, it is sufficient to prove that no integer r yields a rational root u of the monic polynomial (3.1). After observing that a rational root of a monic polynomial is necessarily an integer (from the Rational Root Theorem, e.g., see [5, p. 253]), we suppose the existence of an integer root u, thus getting a contradiction.

First, replace x by the integer u in (3.1), equate this polynomial to zero, and solve for r^4, thus obtaining the equality

$$r^4 = \frac{(u-2)^4(u^2+16)}{5^5(u-3)},$$

which can be rewritten in the form

$$u^2 + 16 = 5(u-3)\left(\frac{5r}{u-2}\right)^4. \tag{3.2}$$

Now, observe that $5[5r/(u-2)]^4$ must be an integer because g.c.d.$(u-3, u-2) = 1$. Consequently, if $u-2$ is not divisible by 5, then $r/(u-2)$ must be an integer, while, if $u-2$ is divisible by 5, then $5r/(u-2)$ must be an integer. In both cases it follows that, if u is an integer, then the quantity $v = 5r/(u-2)$ is an integer as well.

Then, from (3.2), write the quadratic equation in u,

$$u^2 - 5v^4u + 15v^4 + 16 = 0, \tag{3.3}$$

whose discriminant $25v^8 - 60v^4 - 64$ must be a perfect square (say, w^2) because u is an integer by hypothesis. Hence, v is a root of the quadratic equation in z,

$$25z^2 - 60z - w^2 - 64 = 0, \tag{3.4}$$

where $z = v^4$. Again, the discriminant $100(w^2+100)$ of (3.4) must be a perfect square (say, $100s^2$) so that w and s satisfy the diophantine equation

$$w^2 + 100 = s^2 \tag{3.5}$$

whose solutions are $(w, s) = (24, 26)$ and $(0, 10)$.

Letting $w = 24$ and 0 in (3.4) yields the roots $(z_1, z_2) = (32/5, -4)$ and $(16/5, -4/5)$, respectively. None of these roots is a fourth power, as is required by the replacement $z = v^4$ above. This contradiction comes from the fact that we supposed that u is an integer. Q.E.D.

3.2 The Reducible Case

Theorem 2 tells us that the quintics of the form $q(x)$ may be solved by radicals only if they are reducible. The solution of this case has been given by Rabinowitz in his nice paper [8]. In fact, after showing that, if $r = m^5 - m$ $(m \in \mathbb{Z})$, then

$$x^5 - x - (m^5 - m) = (x-m)(x^4 + mx^3 + m^2x^2 + m^3x + m^4 - 1), \tag{3.6}$$

this author proves the following.

Theorem 3 (Rabinowitz): If $r \neq m^5 - m$, then $q(x)$ is reducible iff

$$r^2 = \begin{cases} F_{2j-1}^2 F_{2j}^2 F_{2j+2}^2, \\ F_{2j}^2 F_{2j+1}^2 F_{2j-2}^2. \end{cases} \tag{3.7}$$

Since the only square Fibonacci numbers with even subscript are $F_0 = 0$, $F_2 = 1$, and $F_{12} = 144$ (e.g., see [2]), the nonzero values of r (note that $r = 0$ has the form $m^5 - m$ with $m = -1$, 0, or 1) that satisfy (3.7) are given by

$$r = \begin{cases} \pm F_4 F_5 \sqrt{F_2} = \pm 15, \\ \pm F_9 F_{10} \sqrt{F_{12}} = \pm 22440, \\ \pm F_{14} F_{15} \sqrt{F_{12}} = \pm 2759640. \end{cases} \tag{3.8}$$

4. THE NUMBERS $x_n(5)$ THAT HAVE A CLOSED-FORM EXPRESSION

First, from (3.6) and (1.1), it is immediately seen that

$$x_{a^5-a}(5) = a \quad (a = 1, 2, 3, \ldots). \tag{4.1}$$

Then one can readily ascertain that the decompositions of the polynomials $q(x)$ having the *positive* values of r given by (3.8) are

$$x^5 - x - 15 = (x^2 - x + 3)(x^3 + x^2 - 2x - 5),$$
$$x^5 - x - 22440 = (x^2 + 12x + 55)(x^3 - 12x^2 + 89x - 408),$$
$$x^5 - x - 2759640 = (x^2 - 12x + 377)(x^3 + 12x^2 - 233x - 7320).$$

The real positive roots of the above polynomials give the solution of our problem. Namely, we get

$$x_{15}(5) = -\frac{1}{3} + \sqrt[3]{\frac{115}{54} + \frac{\sqrt{1317}}{18}} + \sqrt[3]{\frac{115}{54} - \frac{\sqrt{1317}}{18}}, \tag{4.2}$$

$$x_{22440}(5) = 4 + \sqrt[3]{90 + \frac{\sqrt{862863}}{9}} - \sqrt[3]{-90 + \frac{\sqrt{862863}}{9}}, \tag{4.3}$$

and

$$x_{2759640}(5) = -4 + \sqrt[3]{3130 + \frac{\sqrt{726984777}}{9}} + \sqrt[3]{3130 - \frac{\sqrt{726984777}}{9}}. \tag{4.4}$$

5. CONCLUDING COMMENTS

For solving the problem of finding all numbers $x_n(5)$ that have a closed-form expression, we have characterized all the quintics of the Bring-Jerrard form $x^5 - x - r$ over $\mathbb{Z}$ that are solvable by radicals. This result is not trivial because there are examples of irreducible polynomials of degree five over $\mathbb{Q}$ that can either be solved by radicals or not; e.g., $x^5 + 15x + 12$ can be solved [3], whereas $x^5 - 6x + 3$ cannot [10, p. 147].

Formal solutions applicable to unsolvable quintics were sought by using elliptic functions [6]; in particular, that given by Hermite is based on the Bring-Jerrard form [7].

Let us conclude our paper by posing ourselves the following question.

Question: Do there exist nonintegral numbers $x_n(k)$ with $k \geq 6$, that can be expressed by radicals?

ACKNOWLEDGMENTS

The contribution of the first author has been financially supported by CNR (Italian Council for National Research), whereas the contribution of the second author has been given within the framework of an agreement between the Italian PT Administration (Istituto Superiore PT) and the Fondazione Ugo Bordoni.

REFERENCES

1. W. S. Burnside & A. W. Panton. *The Theory of Equations*. New York: Dover, 1960.
2. J. H. E. Cohn. "On Square Fibonacci Numbers." *Proc. London Math. Soc.* **39** (1964):537-540.
3. D. S. Dummit. "Solving Solvable Quintics." *Math. Comp.* **57.195** (1991):387-401.
4. P. Filipponi. "A Curious Property of the Golden Section." *Int. J. Math. Educ. Sci. Technol.* **23.5** (1992):805-08.
5. J. A. Gallian. *Contemporary Abstract Algebra*. Lexington: D. C. Heath & Co., 1990.
6. R. B. King. *Beyond the Quartic Equation*. Basel: Birkhäuser, 1996.
7. F. Klein. *The Icosahedron and the Solution of Equations of the Fifth Degree*. New York: Dover, 1956.
8. S. Rabinowitz. "The Factorization of $x^5 \pm x + n$." *Math. Magazine* **61.3** (1988):191-93.
9. J. Rotman. *Galois Theory*. New York: Springer-Verlag, 1990.
10. I. Stewart. *Galois Theory*. New York: Chapman & Hall, 1984.

AMS Classification Numbers: 12D05, 11B39, 14H52

❖❖❖

A REMARK ABOUT THE BINOMIAL TRANSFORM

Massimo Galuzzi
Dipartimento di Matematica, Università di Milano, Italy
(Submitted October 1996)

In [1, p. 137], Knuth introduced the idea of the *binomial transform*.*

Given a sequence of numbers $\langle a_n \rangle$, its binomial transform $\langle \hat{a}_n \rangle$ may be defined by the rule

$$\hat{a}_n = \sum_{k=0}^{n} \binom{n}{k} a_k . \tag{1}$$

Denoting the respective generating functions of $\langle a_n \rangle$ and $\langle \hat{a}_n \rangle$ by $A(x)$ and $\hat{A}(x)$, relation (1) corresponds to

$$\hat{A}(x) = \frac{1}{1-x} A\left(\frac{x}{1-x}\right). \tag{2}$$

In [2], Prodinger gives the following generalization. A sequence $\langle a_n \rangle$ may be transformed into $\langle \hat{a}_n \rangle$ by the rule

$$\hat{a}_n = \sum_{k=0}^{n} \binom{n}{k} b^{n-k} c^k \cdot a_k , \tag{3}$$

which corresponds to

$$\hat{A}(x) = \frac{1}{1-bx} A\left(\frac{cx}{1-bx}\right). \tag{4}$$

Now we may look at equation (4) as the action of a group structure over the set of functions.

Let $\mathbb{C}$ denote the field of complex numbers and $\mathbb{C}^*$ denote the set of complex numbers different from 0. We define a group structure in $\mathbb{C} \times \mathbb{C}^*$ by the law

$$(b, c) \circ (b', c') = (b' + bc', cc'). \tag{5}$$

Now

$$\begin{aligned} &\frac{1}{1-b'x} \frac{1}{1-b\dfrac{c'x}{1-b'x}} A\left(c \frac{\dfrac{c'x}{1-b'x}}{1-b\dfrac{c'x}{1-b'x}} \right) \\ &= \frac{1}{1-(b'+bc')x} A\left(\frac{cc'x}{1-(b'+bc')x}\right). \end{aligned} \tag{6}$$

Relation (6) shows that the action of the element (b, c) on $A(x)$ followed by the action of the element (b', c') corresponds to the action of the product $(b' + bc', cc')$ over $A(x)$.

It is easy to verify that the operation in (5) is associative. The unit element is given by (0, 1), and the inverse of the element (b, c) is given by $(-b/c, 1/c)$. We immediately deduce that the inversion formula for the binomial transform is

---

* A slight modification has been introduced in the original definition.

$$a_n = \sum_{k=0}^{n} \binom{n}{k} \left(\frac{-b}{c}\right)^{n-k} \left(\frac{1}{c}\right)^{k} \cdot \hat{a}_k = c^{-n} \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} b^{n-k} \hat{a}_k.$$

It may be observed that the same group structure works equally well with the transformation (for d fixed),

$$A(x) \to \frac{1}{(1-bx)^d} A\left(\frac{cx}{1-bx}\right),$$

introduced by Prodinger in [2], corresponding to

$$\hat{a}_n = \sum_{k=0}^{n} \binom{n+d-1}{n-k} b^{n-k} c^k \cdot a_k.$$

REFERENCES

1. D. E. Knuth. *The Art of Computer Programming* **3**. Reading, MA: Addison Wesley, 1973.
2. H. Prodinger. "Some Information about the Binomial Transform." *The Fibonacci Quarterly* **32.5** (1994):412-15.

AMS Classification Number: 05A10

❖❖❖

SUSTAINING MEMBERS

*H.L. Alder
G.L. Alexanderson
P. G. Anderson
S. Ando
R. Andre-Jeannin
*J. Arkin
D.C. Arney
C. Ashbacher
J.G. Bergart
G. Bergum
G. Berzsenyi
*M. Bicknell-Johnson
R. Bronson
P.S. Bruckman
M.F. Bryn
G.D. Chakerian
C. Chouteau
C.K. Cook
M.J. DeBruin
M.J. DeLeon
J. De Kerf
E. Deutsch
L.A.G. Dresel
U. Dudley
D.R. Farmer
D.C. Fielder
P. Filipponi
C.T. Flynn
E. Frost
Fondazione Ugo Bordoni
*H.W. Gould
P. Hagis, Jr.
H. Harborth
*A.P. Hillman
*A.F. Horadam
Y. Horibe
F.T. Howard
R.J. Howell
J.P. Jones
S. Kasparian
R.E. Kennedy
C.H. Kimberling
Y.H.H. Kwong
J. Lahr
B. Landman
*C.T. Long
G. Lord
*J. Maxwell
W.L. McDaniel
F.U. Mendizabal
J.L. Miller
M.G. Monzingo
J.F. Morrison
H. Niederhausen
S.A. Obaid
S.W. Oka
J. Pla
A. Prince
T. Reuterdahl
B.M. Romanic
S. Sato
J.A. Schumaker
A.G. Shannon
L.W. Shapiro
J.R. Siler
L. Somer
P. Spears
W.R. Spickerman
P.K. Stockmeyer
J. Suck
M.N.S. Swamy
*D. Thoro
J.C. Turner
C. Vanden Eynden
T.P. Vaughan
J.N. Vitale
M. Waddill
M.J. Wallace
J.E. Walton
W.A. Webb
G.E. Weekly
D.L. Wells
R.E. Whitney
B.E. Williams
C. Witzgall

*Charter Members

INSTITUTIONAL MEMBERS

BIBLIOTECA DEL SEMINARIO MATHEMATICO
Padova, Italy

ETH-BIBLIOTHEK
Zurich, Switzerland

CHALMERS UNIVERSITY OF TECHNOLOGY
AND UNIVERSITY OF GOTEBORG
Goteborg, Sweden

GONZAGA UNIVERSITY
Spokane, Washington

HOWELL ENGINEERING COMPANY
Bryn Mawr, Califoria

KLEPCO, INC.
Sparks, Nevada

KOBENHAVNS UNIVERSITY
Matematisk Institut
Copenhagen, Denmark

MATHEMATISCHES
FORSCHUNGSINSTITUT OBERWOLFACH
Lorenzenhof, Germany

MISSOURI SOUTHERN STATE COLLEGE
Joplin, Missouri

NATIONAL LIBRARY OF EDUCATION
Copenhagen, Denmark

SAN JOSE STATE UNIVERSITY
San Jose, California

SANTA CLARA UNIVERSITY
Santa Clara, California

UNIVERSITY OF NEW ENGLAND
Armidale, N.S.W. Australia

UNIVERSITY OF TECHNOLOGY
Sydney, N.S.W. Australia

WASHINGTON STATE UNIVERSITY
Pullman, Washington

YESHIVA UNIVERSITY
New York, New York

JOVE STATISTICAL TYPING SERVICE
2088 Orestes Way
Campbell, California 95008

BOOKS AVAILABLE
THROUGH THE FIBONACCI ASSOCIATION

Introduction to Fibonacci Discovery by Brother Alfred Brousseau, Fibonacci Association (FA), 1965.

Fibonacci and Lucas Numbers by Verner E. Hoggatt, Jr. FA, 1972.

A Primer for the Fibonacci Numbers. Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1972.

Fibonacci's Problem Book, Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1974.

The Theory of Simply Periodic Numerical Functions by Edouard Lucas. Translated from the French by Sidney Kravitz. Edited by Douglas Lind. FA, 1969.

Linear Recursion and Fibonacci Sequences by Brother Alfred Brousseau. FA, 1971.

Fibonacci and Related Number Theoretic Tables. Edited by Brother Alfred Brousseau. FA, 1972

Number Theory Tables. Edited by Brother Alfred Brousseau. FA, 1973.

Tables of Fibonacci Entry Points, Part One. Edited and annotated by Brother Alfred Brousseau. FA, 1965

Tables of Fibonacci Entry Points, Part Two. Edited and annotated by Brother Alfred Brousseau. FA, 1965

A Collection of Manuscripts Related to the Fibonacci Sequence—18th Anniversary Volume. Edited by Verner E. Hoggatt, Jr. and Marjorie Bicknell-Johnson. FA, 1980.

Applications of Fibonacci Numbers, Volumes 1-7. Edited by G.E. Bergum, A.F. Horadam and A.N. Philippou

Generalized Pascal Triangles and Pyramids Their Fractals, Graphs and Applications by Boris A. Bondarenko. Translated from the Russian and edited by Richard C. Bollinger. FA, 1993.

Fibonacci Entry Points and Periods for Primes 100,003 through 415,993 by Daniel C. Fielder and Paul S. Bruckman.

Please write to the Fibonacci Association, P.O. Box 320, Aurora, S.D. 57002-0320, U.S.A., for more information and current prices.