The Fibonacci Quarterly

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

## TABLE OF CONTENTS



VOLUME 41 AUGUST 2003 NUMBER 4

## 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 worldwide web page at:

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

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

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

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

## SUBSCRIPTIONS, ADDRESS CHANGE, AND REPRINT INFORMATION

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

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

Annual domestic Fibonacci Association membership dues, which include a subscription to **THE FIBONACCI QUARTERLY**, are $40 for Regular Membership, $50 for Library, $50 for Sustaining Membership, and $80 for Institutional Membership; foreign rates, which are based on international mailing rates, are somewhat higher than domestic rates; please write for details. **THE FIBONACCI QUARTERLY** is published each February, May, August and November.

All back issues of **THE FIBONACCI QUARTERLY** are available in microfilm or hard copy format from **PROQUEST INFORMATION & LEARNING, 300 NORTH ZEEB ROAD, P.O. BOX 1346, ANN ARBOR, MI 48106-1346.** Reprints can also be purchased from **PROQUEST** 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*





Fibonacci Association Web Page Address: **http://www.MSCS.dal.ca/Fibonacci/**

# DOUBLE INDEXED FIBONACCI SEQUENCES AND THE BIVARIATE PROBABILITY DISTRIBUTION

**Belkheir Essebbar**
Department of Mathematics and Computer Science
Faculté des Sciences of Rabat, Morocco
essebbar@fsr.ac.ma
*(Submitted July 2000-Final Revision May 2003)*

## 1. INTRODUCTION

The classical $r$-Fibonacci sequence $(U_i)_{i\geq 0}$ is defined by some given real numbers $U_0, U_1, \ldots, U_{r-1}$ and the difference equation

$$\sum_{k=0}^{r} a_k U_{i-k} = 0; \quad i \geq r,$$

where $a_k, k = 0, 1, \ldots, r$ are arbitrary real numbers such that $a_r \neq 0, r \geq 2$. The characteristic polynomial of this equation is given by

$$Q(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_r x^r.$$

Many authors have studied the $r$-Fibonacci sequence given above, see for example Mouline and Rachidi (1998). Philippou et. al. (1982) and Philippou (1988) have related the Fibonacci sequences to the one dimensional geometric probability distribution.

Now we introduce the double indexed Fibonacci sequence (DIFS) of order $(n, m)$. Let $(U_{ij})_{i\geq 0, j\geq 0}$ be the double indexed sequence defined by the difference equations of order $(n, m)$ :

$$\sum_{k_1=0}^{n} \sum_{k_2=0}^{m} a_{k_1,k_2} U_{i-k_1, j-k_2} = 0, \quad i \geq n, j \geq m, \tag{1}$$

where $a_{i,j}, i = 0, \ldots, n, j = 0, \ldots, m$ are real numbers such that $a_{00} \neq 0$ and $a_{n,m} \neq 0$. The corresponding characteristic polynomial is defined by

$$Q(x, y) = a_{00} + a_{10} x + a_{01} y + a_{11} xy + \cdots + a_{nm} x^n y^m.$$

Next, we recall that $(X, Y)$ is a discrete random vector in two dimensions with values in $N \times N$ and defined on a certain underlying probability space $(\Omega, A, P)$ with probability generating function given by

$$g(x, y) = E(x^X y^Y) = \sum_{i\geq 0} \sum_{j\geq 0} p_{ij} x^i y^j,$$

where $p_{ij} = P(X = i, Y = j), i \geq 0, j \geq 0$ is the probability mass function of $(X, Y)$. For example, the bivariate negative binomial distribution has the probability generating function defined by

$$g(x,y) = \left(\frac{d}{1 - ax - by - cxy}\right)^r, \tag{2}$$

where $a, b, c$ and $d$ are real numbers such that $0 \leq a \leq 1, 0 \leq b \leq 1, 0 < d < 1$ and $a+b+c+d = 1$. For $r = 1$, we get the bivariate geometric distribution as a special case of (2). For more details about these distributions and their applications see Edwards et. al. (1961), Feller (1968) (page 285), Subrahmanian et. al. (1973) and Davy et. al. (1996).

Philippou et. al. (1989, 1990, 1991) and Antzoulakos et. al. (1991) have related the special case of the above distribution when the crossed term in $x$ and $y$ is null ($c = 0$) with extensions to some particular characteristic polynomials (see section 3).

This work is organized as follows: in the second section we develop the setting of the difference equation given by (1). In section 3, we give examples of DIFS with their combinatorial solutions. In section 4, we study the relationships of DIFS and the bivariate probability distributions given by (2).

## 2. THE DIFS

Let $(U_{ij})_{i\geq 0, j\geq 0}$ be the DIFS of order $(n, m)$ as given by (1), that is,

$$\sum_{k_1=0}^{n} \sum_{k_2=0}^{m} a_{k_1,k_2} U_{i-k_1,j-k_2} = 0, \quad i \geq n, j \geq m, \tag{3}$$

with the initial conditions: $a_{00}U_{00} = 1$ and $a_{n,m} \neq 0$ with $U_{ij} = 0$ if $i < 0$ or $j < 0$. Now let $Q(x, y)$ be the corresponding characteristic polynomial with order $(n, m)$ of the difference equation given by (3), that is,

$$Q(x,y) = \sum_{k_1=0}^{n} \sum_{k_2=0}^{m} a_{k_1,k_2} x^{k_1} y^{k_2}, \tag{4}$$

with $a_{0,0} \neq 0$ and $a_{n,m} \neq 0$. Then we have the development of $1/Q(x, y)$ using power series, that is,

$$\frac{1}{Q(x,y)} = \sum_{i\geq 0, j\geq 0} U_{i,j} x^i y^j.$$

From the equality $Q(x,y)/Q(x,y) = 1$, we get

$$\sum_{k_1=0}^{n}\sum_{k_2=0}^{m} a_{k_1,k_2}x^{k_1}y^{k_2} \cdot \sum_{i\geq 0, j\geq 0} U_{i,j}x^iy^j = 1,$$

which gives the difference equations defined by (3) with specific initial conditions. The combinatorial solution of (3), $(U_{ij})_{i\geq 0, j\geq 0}$, is then given by means of the development of $1/Q(x,y)$ using power series.

There are two cases which the combinatorial solution of (3) could be deduced from elementary combinatorial solutions. Let $Q(x,y)$ be a characteristic polynomial of order $(n,m)$ such that the following decomposition holds

$$Q(x,y) = \prod_{k=1}^{r} Q_k(x,y), \tag{5}$$

where the order of each polynomial $Q_k(x,y)$ is $(n_k, m_k), k = 1, \ldots, r$ with $n = n_1 + \cdots + n_r$ and $m = m_1 + \cdots + m_r$. Let $U_{i,j}^{(k)}$ be the combinatorial solution of $Q_k(x,y)$, that is,

$$\frac{1}{Q_k(x,y)} = \sum_{i,j} U_{i,j}^{(k)} x^iy^j, \quad k = 1, \ldots, r.$$

Let us establish the following result which gives the convolution of independent DIFS's.

**Theorem 1**: *If* $(U_{i,j})$ *is the combinatorial solution of* (3) *with* $Q(x,y)$ *verifying the decomposition* (5) *then*

$$U_{ij} = \sum_{i_1=0}^{i}\sum_{i_2=0}^{i-i_1}\cdots\sum_{i_{r-1}=0}^{i-(i_1+\cdots+i_{r-2})}\sum_{j_1=0}^{j}\sum_{j_2=0}^{j-j_1}\cdots\sum_{j_{r-1}=0}^{j-(j_1+\cdots+j_{r-2})}$$

$$U_{i_1,j_1}^{(1)}U_{i_2,j_2}^{(2)}\cdots U_{i_{r-1},j_{r-1}}^{(r-1)}U_{i-(i_1+\cdots+i_{r-1}),j-(j_1+\cdots+j_{r-1})}^{(r)}.$$

**Proof**: One has,

$$\frac{1}{Q(x,y)} = \prod_{k=1}^{r}\frac{1}{Q_k(x,y)}$$

$$= \sum_{i_1,\ldots,i_r}\sum_{j_1,\ldots,j_r} U_{i_1,j_1}^{(1)}U_{i_2,j_2}^{(2)}\cdots U_{i_r,j_r}^{(r)}x^{i_1+\cdots+i_r}y^{j_1+\cdots+j_r}.$$

Set $i = i_1 + \cdots + i_r$ and $j = j_1 + \cdots + j_r$. Then

$$\frac{1}{Q(x,y)} = \sum_{i,j} x^i y^j \sum_{i_1=0}^{i} \sum_{i_2=0}^{i-i_1} \cdots \sum_{i_{r-1}=0}^{i-(i_1+\cdots+i_{r-2})} \sum_{j_1=0}^{j} \sum_{j_2=0}^{j-j_1} \cdots \sum_{j_{r-1}=0}^{j-(j_1+\cdots+j_{r-2})}$$

$$U^{(1)}_{i_1,j_1} U^{(2)}_{i_2,j_2} \cdots U^{(r-1)}_{i_{r-1},j_{r-1}} U^{(r)}_{i-(i_1+\cdots+i_{r-1}),j-(j_1+\cdots+j_{r-1})}.$$

By the identification with

$$\frac{1}{Q(x,y)} = \sum_{i,j} U_{i,j} x^i y^j$$

one can deduce the result of the theorem. □

Let us now suppose that the characteristic polynomial, $Q(x,y)$, of equation (3) can be decomposed as

$$Q(x,y) = Q_1(x) \cdot Q_2(y) \tag{6}$$

where $Q_1(x)$ and $Q_2(y)$ are polynomials with respective orders $n$ and $m$ such that

$$\frac{1}{Q_1(x)} = \sum_i U_i^{(1)} x^i, \quad \frac{1}{Q_2(y)} = \sum_j U_j^{(2)} y^j.$$

Let us establish this result.

**Theorem 2**: *The characteristic polynomial $Q(x,y)$ of (3) is decomposed as in (6) if and only if the combinatorial solution is given by*

$$U_{ij} = U_i^{(1)} U_j^{(2)}$$

**Proof**: First

$$\frac{1}{Q(x,y)} = \frac{1}{Q_1(x)} \cdot \frac{1}{Q_2(y)}$$

$$= \sum_{i,j} U_i^{(1)} U_j^{(2)} x^i y^j.$$

Then, by identification with

$$\frac{1}{Q(x,y)} = \sum_{i,j} U_{i,j} x^i y^j.$$

the result follows. □

Let us introduce the notion of marginals of the DIFS. Let $U_{ij}$ be a DIFS of order $(n,m)$ as given by (3) and $Q(x,y)$ be the corresponding characteristic polynomial as given by (4). We define the marginal polynomials as polynomials in $x$ or in $y$, that is, $Q(x,1)$ and $Q(1,y)$ given by

$$Q(x,1)=\sum_{l,k}a_{lk}x^l=\sum_{l=0}^{n}x^l\sum_{k=0}^{m}a_{lk},$$

$$Q(1,y)=\sum_{l,k}a_{lk}y^k=\sum_{k=0}^{m}y^k\sum_{l=0}^{n}a_{lk}.$$

The associated equations are respectively

$$\sum_{l=0}^{n}V_{i-l}\sum_{k=0}^{m}a_{lk}=0,$$

$$\sum_{k=0}^{m}W_{j-k}\sum_{l=0}^{n}a_{lk}=0,$$

with $V_i=\sum_j U_{ij}$ and $W_j=\sum_i U_{ij}$ which are the combinatorial marginal solutions.

## 3. EXAMPLES

(a) DIFS of order (1,1): Let $U_{ij}$ be the DIFS given by (3) with $n=m=1$, that is,

$$\sum_{k_1=0}^{1}\sum_{k_2=0}^{1}a_{k_1,k_2}U_{i-k_1,j-k_2}=0.$$

This is equivalent to

$$a_{00}U_{i,j}+a_{10}U_{i-1,j}+a_{01}U_{i,j-1}+a_{11}U_{i-1,j-1}=0, \tag{7}$$

with $a_{00}U_{00}=1$. The associated characteristic polynomial is then

$$Q(x,y)=a_{00}+a_{10}x+a_{01}y+a_{11}xy.$$

For the developement of $1/Q(x,y)$ using power series, we first need to establish the following lemma.

**Lemma 1**: *Let $a, b, c$ be real numbers and $r$ be a positive integer. One has,*
*(i) if $abc \neq 0$ and $(x, y)$ is such that $|ax + by + cxy| < 1$, then*

$$\frac{1}{(1 - ax - by - cxy)^r} = \sum_{i,j} x^i y^j a^i b^j \sum_{k=0}^{\min(i,j)} \left(\frac{c}{ab}\right)^k C_i^k C_{i+j-k}^i C_{i+j+r-k-1}^{r-1},$$

*(ii) if $a = 0, bc \neq 0$ and $(x, y)$ is such that $|by + cxy| < 1$, then*

$$\frac{1}{(1 - by - cxy)^r} = \sum_{i,j} (by)^i (cxy)^j C_{i+j}^i C_{i+j+r-1}^{r-1},$$

*(iii) if $b = 0, ac \neq 0$ and $(x, y)$ is such that $|ax + cxy| < 1$, then*

$$\frac{1}{(1 - ax - cxy)^r} = \sum_{i,j} (ax)^i (cxy)^j C_{i+j}^i C_{i+j+r-1}^{r-1},$$

*(iv) if $ab \neq 0, c = 0$ and $(x, y)$ is such that $|ax + by| < 1$, then*

$$\frac{1}{(1 - ax - by)^r} = \sum_{i,j} (ax)^i (by)^j C_{i+j}^i C_{i+j+r-1}^{r-1},$$

*where $C_n^i = n!i!/(n-i)!$ and the summation $\sum_{i,j}$ is over $i \geq 0, j \geq 0$.*

**Proof**:

(i) It is known that for $|t| < 1$ the expansion of $1/(1-t)^r$ is $\sum_{n\geq 0} t^n C_{n+r-1}^{r-1}$. For $t = ax + by + cxy$, one has,

$$\frac{1}{(1 - ax - by - cxy)^r} = \sum_{n\geq 0} (ax + by + cxy)^n C_{n+r-1}^{r-1}.$$

Now by the multinomial formula, one has,

$$(ax + by + cxy)^n = \sum_{k_1+k_2+k_3=n} (ax)^{k_1} (by)^{k_2} (cxy)^{k_3} \frac{n!}{k_1!k_2!k_3!}$$

$$= \sum_{k_1+k_2+k_3=n} a^{k_1} b^{k_2} c^{k_3} x^{k_1+k_3} y^{k_2+k_3} \frac{n!}{k_1!k_2!k_3!},$$

with the conventions that $0^0 = 0! = 1$. Let us put $i = k_1 + k_3$ and $j = k_2 + k_3$. One can see that $i = 0, \ldots, n, j = 0, \ldots, n$ and $0 \le k_3 \le i, 0 \le k_3 \le j$, that is $0 \le k_3 \le min(i,j)$. Then for $ab \neq 0$

$$\frac{1}{(1-ax-by-cxy)^r} = \sum_{n\ge 0} C_{n+r-1}^{r-1} \sum_{i+j-k_3=n} (ax)^i (by)^j \left(\frac{c}{ab}\right)^{k_3} \frac{n!}{(i-k_3)!(j-k_3)!k_3!}$$

$$= \sum_{i>0}(ax)^i \sum_{j\ge 0}(by)^j \sum_{k_3=0}^{min(i,j)} \left(\frac{c}{ab}\right)^{k_3} \frac{(i+j-k_3)!}{(i-k_3)!(j-k_3)!k_3!} C_{i+j+r-k_3-1}^{r-1},$$

which coincides with the claimed formula.

(ii) If $a = 0$ and $bc \neq 0$, one has

$$(by+cxy)^n = \sum_{k=0}^{n} (by)^k (cxy)^{n-k} C_n^k.$$

Then

$$\frac{1}{(1-by-cxy)^r} = \sum_{n\ge 0} C_{n+r-1}^{r-1} \sum_{k=0}^{n} (by)^k (cxy)^{n-k} C_n^k$$

$$= \sum_{k\ge 0}(by)^k \sum_{j\ge 0}(cxy)^j C_{k+j}^k C_{k+j+r-1}^{r-1}.$$

One can easily derive the other expressions of the lemma. □

Let us derive from Lemma 1. the expression of $1/Q(x,y)$ using power series. It is easy to see that with the parameterizations $a_{00} = 1/d, a_{10} = -a/d, a_{01} = -b/d, a_{1,1} = -c/d$, (7) becomes

$$U_{ij} = aU_{i-1,j} + bU_{i,j-1} + cU_{i-1,j-1}, \quad i \ge 1, j \ge 1, \tag{8}$$

with the initial conditions: $U_{00} = d, U_{10} = ad$, and $U_{01} = bd$. The associated characteristic polynomial is

$$Q(x,y) = \frac{1-ax-by-cxy}{d}.$$

From the above Lemma 1 and for $r = 1$ (with for example $ab \neq 0$) one has

$$\frac{1}{Q(x,y)} = \sum_{i,j} U_{ij} x^i y^j$$

with

$$U_{ij} = da^i b^j \sum_{k=0}^{min(i,j)} \left(\frac{c}{ab}\right)^k \frac{(i+j-k)!}{(i-k)!(j-k)!k!}$$

$$= da^i b^j \sum_{k=0}^{min(i,j)} \left(\frac{c}{ab}\right)^k C_i^k C_{i+j-k}^i,$$

which is the combinatorial solution of equation (8). For $c = 0$, which means that the crossed term is null, the solution is then $U_{ij} = da^i b^j C_{i+j}^i$. This is the solution of the $m$-variate generalized Fibonacci polynomial of order $k$ (here $m = 2,\ k = 1$) given by Philippou et. al. (1991) and Antzoulakos et. al. (1991).

(b) DIFS of order $(r, r)$: Let $Q$ be

$$Q(x, y) = (1 - ax - by - cxy)^r / d^r,$$

which is the characteristic polynomial of the DIFS of order $(r, r)$ given by

$$\sum_{k_1+k_2+k_3+k_4=r} (-a)^{k_2}(-b)^{k_3}(-c)^{k_4} \frac{r!}{k_1!k_2!k_3!k_4!} U_{i-(k_2+k_4),j-(k_3+k_4)}^{(r)} = 0. \tag{9}$$

This is equivalent to

$$\sum_{k_1=0}^{r} C_r^{k_1} \sum_{k_2=0}^{r-k_1} (-a)^{k_2} C_{r-k1}^{k_2} \sum_{k_3=0}^{r-k_1-k_2} (-b)^{k_3}(-c)^{r-k_1-k_2-k_3}$$

$$C_{r-k_1-k_2}^{k_3} U_{i-r+k_1+k_3,j-r+k_1+k_2}^{(r)} = 0.$$

From Lemma 1, one can deduce the combinatorial solution of the above equation. That is,

$$U_{ij}^{(r)} = d^r a^i b^j \sum_{k=0}^{min(i,j)} \left(\frac{c}{ab}\right)^k C_i^k C_{i+j-k}^i C_{i+j+r-k-1}^{r-1},\quad i \geq 0, j \geq 0. \tag{10}$$

This solution can also be derived from Theorem 1 since the characteristic polynomial has the decomposition (5). Since the DIFS of order $(r, r)$ is the $r$-fold convolution of DIFS of order

(1,1), Philippou et. al. (1991) showed that the solution can be evaluated (for small values of $r$) recursively as

$$U_{ij}^{(r)} = \sum_{k_1=0}^{i} \sum_{k_2=0}^{j} U_{k_1,k_2} U_{i-k_1,j-k_2}^{(r-1)}, \quad r \geq 2,$$

with $U_{ij}^{(1)} = U_{ij}$ which is the solution of DIFS of order (1,1).

## 4. THE DIFS AND THE BIVARIATE PROBABILITY DISTRIBUTION

A random couple $(X, Y)$ has a bivariate negative binomial distribution if its probability generating function has the form given by (2), that is

$$g(x,y) = \left( \frac{d}{1 - ax - by - cxy} \right)^r,$$

with $a, b, c$ and $d$ such that $0 \leq a < 1, 0 \leq b < 1, 0 < d < 1$ and $a + b + c + d = 1$. This distribution is the convolution of $r$ independent bivariate geometric distributions. One can recognize the associated stochastic DIFS given in example (b) which the combinatorial solution given by (10) is the probability mass function associated to this bivariate negative binomial distribution, that is for $i \geq 0, j \geq 0$,

$$P(X = i, Y = j) = d^r a^i b^j \sum_{k=0}^{min(i,j)} \left( \frac{c}{ab} \right)^k C_i^k C_{i+j-k}^i C_{i+j+r-k-1}^{r-1}. \tag{11}$$

Equation (9) permits recursive computations of the above probabilities which are more convenient than those given by Edwards et. al. (1961) and Subrahmanian et. al. (1973). The geometric case ($r = 1$) is given by equation (8).

The random variables $X$ and $Y$ have the marginal distributions which are negative binomial distributions with respectively the parameters $(r, d/(1-b))$ and $(r, d/(1-a))$, that is

$$P(X = i) = \left( \frac{d}{1-b} \right)^r U_i; \quad i \geq 0, \tag{12}$$

where $(U_i)$ is the marginal Fibonacci sequence satisfying

$$\sum_{k=0}^{r} C_r^k \left( \frac{a+c}{b-1} \right)^k U_{i-k} = 0, \tag{13}$$

with $U_0 = 1$. The same holds with $P(Y = j)$. The relations (12) and (13) are less practical for the evaluation of $P(X = i)$, since the following recursive scheme is more effective

$$P(X = i) = q\left(1 + \frac{r-1}{i}\right) P(X = i-1); \quad i \geq 1,$$

starting with the initial condition $P(X = 0) = p^r$, where $p = d/(1-b)$ and $p + q = 1$.

The covariance of $X$ and $Y$ is given by (see for example Subrahmanian et. al. (1973))

$$Cov(X, Y) = r\frac{c + ab}{d^2}.$$

It is easy to see that $X$ and $Y$ are independent random variables if and only if $Cov(X, Y) = 0 (c = -ab)$. We can express this result as follows.

**Lemma 2**: *For $i \geq 0, j \geq 0$ and $r \geq 1$, one has*

$$C^{r-1}_{r+i-1} C^{r-1}_{r+j-1} = \sum_{k=0}^{min(i,j)} (-1)^k C^k_i C^i_{i+j-k} C^{r-1}_{i+j+r-k-1}.$$

**Proof**: Let $g(x, y) = d^r/(1 - ax - by - cxy)^r$. The independence of $X$ and $Y$ is given by $c = -ab$, that is

$$\begin{aligned} g(x, y) &= \left(\frac{1-a}{1-ax}\right)^r \left(\frac{1-b}{1-by}\right)^r \\ &= (1-a)^r \sum_{i \geq 0} (ax)^i C^{r-1}_{r+i-1} \cdot (1-b)^r \sum_{j \geq 0} (by)^j C^{r-1}_{r+j-1} \\ &= \sum_{i,j} U_{ij} x^i y^j \end{aligned}$$

with

$$U_{ij} = (1-a)^r (1-b)^r a^i b^j C^{r-1}_{r+i-1} C^{r-1}_{r+j-1}.$$

By identification with (11) when $c = -ab$, we get the result of the lemma. □

## 5. CONCLUSION

As in the case of the one indexed Fibonacci sequences, there is a relationship between the probability distributions of discrete type and these sequences. In this work, some basic definitions, results and examples of DIFS are given. The link between stochastic DIFS and the bivariate negative binomial distribution is established.

There are plenty of problems left to be solved such as: the combinatorial solution of (1) with arbitrary real numbers $(a_{ij})$, the roots of the characteristic polynomial.

Also the generalization to the multiple indexed Fibonacci sequences and their relationship with multivariate probability distribution opens the door to a host of other quesitons.

## ACKNOWLEDGMENT

The author is deeply grateful to an anonymous referee for his advice which improved the quality of this work. Research grants from CNR under project PROTARS P3T1/06 are also gratefully acknowledged.

## REFERENCES

[1] D.L. Antzoulakos and A.N. Philippou. "A Note on the Multivariate Negative Binomial Distributions of Order $k$." *Communications in Statistics - Theory and Methods* **20** (1991): 1389-1399.

[2] P.J. Davy and J.C.W. Ranger. "Multivariate Geometric Distributions." *Comm. in Stat., Theory and Methods* **25** (1996): 2971-2987.

[3] C.B. Edwards and J. Gurland. "A Class of Distributions Applicable to Accidents." *JASA* **56** (1961): 503-517.

[4] W. Feller. *An Introduction to Probability Theory and Its Applications.* Volume 1, Third edition, New-York: Willey, 1968.

[5] M. Mouline and M. Rachidi. "Application of Markov Chains to $r$-Generalized Fibonacci Sequences." *The Fibonacci Quarterly* **37** (1998): 34-38.

[6] G.N. Philippou. "On the $k$-th Order Linear Recurrence and Some Probability Applications." *Applications of Fibonacci Numbers*, Kluwer Academic Publishers, (1988): 89-96.

[7] A.N. Philippou and A.A. Muwafi. "Waiting for the $k$-th Consecutive Success and the Fibonacci Sequence of Order $k$." *The Fibonacci Quarterly* **20** (1982): 28-32.

[8] A.N. Philippou, D.L. Antzoulakos and G.A. Tripsiannis. "Multivariate Distributions of Order $k$." *Statistics and Probability Letters* **7** (1989): 207-216.

[9] A.N. Philippou and D.L. Antzoulakos. "Multivariate Distributions of Order $k$ on a Generalized Sequence." *Statistics and Probability Letters* **9** (1990): 453-463.

[10] A.N. Philippou and D.L. Antzoulakos. "Generalized Multivariate Fibonacci Polynomials of Order $k$ and the Multivariate Negative Binomial Distributions of the Same Order." *The Fibonacci Quarterly* **29** (1991): 322-328.

[11] K. Subrahmanian, and K. Subrahmanian. "On the Estimation of the Parameters in the Bivariate Negative Binomial Distribution." *Journal of the Roy. Stat. Soc. B* **35** (1973): 131-146.

AMS Classification Numbers: 40A05, 40A25, 45M05

✠ ✠ ✠

# HEIGHTS OF HAPPY NUMBERS AND CUBIC HAPPY NUMBERS


**H. G. Grundman[1]**
Department of Mathematics, Bryn Mawr College
101 N. Merion Ave, Bryn Mawr, PA 19010-2899

**E.A. Teeple[2]**
Department of Biostatistics, University of Washington
Campus Mail Stop 357232, Seattle, WA 98195-7232


*(Submitted February 2001-Final Revision May 2001)*


## 1. INTRODUCTION

Let $S_2 : \mathbf{Z}^+ \to \mathbf{Z}^+$ denote the function that takes a positive integer to the sum of the squares of its decimal digits. For $a \in \mathbf{Z}^+$, let $S_2^0(a) = a$ and for $m \geq 1$ let $S_2^m(a) = S_2(S_2^{m-1}(a))$. A *happy number* is a positive integer $a$ such that $S_2^m(a) = 1$ for some $m \geq 0$. It is well known that 4 is not a happy number and that, in fact, for all $a \in \mathbf{Z}^+$, $a$ is not a happy number if and only if $S_2^m(a) = 4$ for some $m \geq 0$. (See [4] for a proof.) The *height* of a happy number is the least $m \geq 0$ such that $S_2^m(a) = 1$. Hence, 1 is a happy number of height 0; 10 is a happy number of height 1; and 7 is a happy number of height 5.

Similarly, we define $S_3 : \mathbf{Z}^+ \to \mathbf{Z}^+$ to be the function that takes a positive integer to the sum of the cubes of its decimal digits. A *cubic happy number* is a positive integer $a$ such that $S_3^m(a) = 1$ for some $m \geq 0$. The height of a cubic happy number is defined in the obvious way. So, 1 is a cubic happy number of height 0; 10 is a cubic happy number of height 1; and 112 is a cubic happy number of height 2.

By computing the heights of each happy number less than 400, it is straightforward to find the least happy numbers of heights up to 6. (These, as well as the least happy number of height 7, can also be found in [2] and [5].) Richard Guy [3] reports that Jud McCranie verified the value of the least happy number of height 7 and determined the value of the least happy number of height 8. Guy further reports that Warut Roonguthai determined the least happy number of height 9. These results and their methods of proof have not, to the best of our knowledge, appeared in the literature.

The goal of this paper is to present a method for confirming these and additional results. Along with determining the least happy number of height 10 and providing proofs for other happy numbers of small heights, we find with proof the least cubic happy numbers of small heights. Our algorithms combine computer and by-hand calculations. It should be noted that none of the computer calculations took special packages beyond the usual C++ language and no program needed longer than a few seconds to run.

In Section 2 we present the least happy numbers of heights 0 through 10 and describe the methods used to determine them. In Section 3 we do the same for the least cubic happy numbers of heights 0 through 8.

## 2. SQUARING HEIGHTS

Table 1 gives the least happy numbers of heights 0 through 10. Those through height 7 are easily found by simply iterating $S_2$ on each positive integer up to about 80,000, until 1 or 4 is reached and recording the number of iterations needed when 1 is attained. The goal of this section is to explain both the derivations and the proofs for the rest of the table.

| height | happy number |
|---|---|
| 0 | 1 |
| 1 | 10 |
| 2 | 13 |
| 3 | 23 |
| 4 | 19 |
| 5 | 7 |
| 6 | 356 |
| 7 | 78999 |
| 8 | $3789 \times 10^{973} - 1$ |
| 9 | $78889 \times 10^{(3789 \times 10^{973} - 306)/81} - 1$ |
| 10 | $259 \times 10^{[78889 \times 10^{(3789 \times 10^{973} - 306)/81} - 13]/81} - 1$ |

Table 1: The least happy numbers of heights 0-10.

As described above, we used a simple computer search to determine the heights of all happy numbers less than 80,000. The only other computer routine we used in this work is a nested search in which we checked when a fixed number was equal to the sum of squares of a certain number of single digit integers. (See below for more details.) Since the number of single digit integers is never large, the search takes very little time.

To prove that $3789 \times 10^{973} - 1$ is the least happy number of height 8, we begin with a lemma that is immediate from the first computer search mentioned above.

**Lemma 1**: *The only happy numbers of height 7 less than* 80,000 *are* 78999, 79899, 79989, *and* 79998.

**Theorem 2**: *The least happy number of height* 8 *is*

$$\sigma_8 = 3789 \times 10^{973} - 1 = 3788\overbrace{99\ldots9}^{973}.$$

**Proof**. It is easy enough to check that $3789 \times 10^{973} - 1$ is indeed a happy number of height 8. To prove that it is least, let $x \leq 3789 \times 10^{973} - 1$ be a happy number of height 8. Then $S_2(x) < 3^2 + 976 \times 9^2 = 79065$. $S_2(x)$ must be a happy number of height 7 so, by Lemma 1, $S_2(x) = 78999$. We see that $x$ must have at least 973 9's in its base 10 expansion since otherwise $S_2(x) < 3^2 + 4 \times 8^2 + 972 \times 9^2 < 78999$. Assuming without loss of generality that the digits of $x$ are in nondecreasing order, we have that

$$x = a_1 a_2 a_3 a_4 \overbrace{99\ldots9}^{973},$$

with $0 \leq a_1 \leq 3$, and $a_1 \leq a_2 \leq a_3 \leq a_4 \leq 9$. Since $S_2(x) = 78999$, we have $a_1^2 + a_2^2 + a_3^2 + a_4^2 = 78999 - 973 \times 9^2 = 186$. A computer search through the possible values of $a_1$, $a_2$, $a_3$, and $a_4$ finds that the only solution is

$$x = 3788\overbrace{99\ldots9}^{973} = \sigma_8,$$

as desired. □

The proofs for the least happy numbers of heights 9 and 10 follow the same general outline. We get as a corollary to the above proof that the only happy numbers of height 8 less than $4 \times 10^{976}$ are numbers whose digits are permutations of the digits of $\sigma_8$. This result will take the place of Lemma 1 in the proof of Theorem 3.

**Theorem 3**: *The least happy number of height* 9 *is*

$$\sigma_9 = 78889 \times 10^{(3789 \times 10^{973} - 306)/81} - 1 = 78888\,\overbrace{999\ldots99}^{(\sigma_8 - 305)/81}.$$

**Proof.** Again, we can easily verify that this is a happy number of the desired height. Let $x \leq \sigma_9$ be a happy number of height 9, with the digits of $x$ in nondecreasing order. Then $S_2(x) < 7^2 + [(\sigma_8 - 305)/81 + 4] \times 9^2 < \sigma_8 + 68$ and so, from the previous proof, $S_2(x) = \sigma_8$. Now, $x$ must have at least $(\sigma_8 - 305)/81$ 9's in its base 10 expansion since otherwise $S_2(x) < 7^2 + 5 \times 8^2 + [(\sigma_8 - 305)/81 - 1] \times 9^2 < \sigma_8$. So we have

$$x = a_1 a_2 a_3 a_4 a_5\,\overbrace{999\ldots99}^{(\sigma_8 - 305)/81},$$

with $0 \leq a_1 \leq 7$, and $a_1 \leq a_2 \leq a_3 \leq a_4 \leq a_5 \leq 9$. Since $S_2(x) = \sigma_8$, we have $\sum_{i=1}^{5} a_i^2 = 305$. A computer search shows that the only solution is $x = \sigma_9$. □

**Theorem 4**: *The least happy number of height* 10 *is*

$$\sigma_{10} = 259 \times 10^{(78889 \times 10^{3789 \times 10^{973} - 306)/81} - 94]/81} - 1 = 258\,\overbrace{999\ldots99}^{(\sigma_9 - 93)/81}.$$

**Proof.** $\sigma_{10}$ is a happy number of height 10, since $S_2(\sigma_{10}) = \sigma_9$. Let $x \leq \sigma_{10}$ be a happy number of height 10, with nondecreasing digits. Then $S_2(x) < 2^2 + [(\sigma_9 - 93)/81 + 2] \times 9^2 \leq \sigma_9 + 73$ and so, from the previous proof, $S_2(x) = \sigma_9$. We see that $x$ must have at least $(\sigma_9 - 93)/81 - 4$ 9's in its base 10 expansion since otherwise $S_2(x) < 2^2 + 7 \times 8^2 + [(\sigma_9 - 93)/81 - 5] \times 9^2 < \sigma_9$. So we have

$$x = a_1 a_2 a_3 a_4 a_5 a_6 a_7\,\overbrace{9999\ldots99}^{(\sigma_9 - 93)/81 - 4},$$

with $0 \leq a_1 \leq 2$, and $a_1 \leq a_2 \leq a_3 \leq a_4 \leq a_5 \leq a_6 \leq a_7 \leq 9$. Since $S_2(x) = \sigma_9$, we have $\sum_{i=1}^{7} a_i^2 = 417$. A computer search shows that $x = \sigma_{10}$. □

This method can certainly be extended to find additional least happy numbers of given heights. There are a few obstacles to be dealt with. The main one is simply finding a good candidate for the least happy number, thus bounding the size of the numbers being considered. It's always possible to find a happy number of a given height: simply take a happy number of the next smaller height and string that many 1's in a row. More efficient is taking as many 9's as possible, then adding digits as needed to obtained the desired sum. This explains the divisions by 81 that appear in the expressions for $\sigma_9$ and $\sigma_{10}$.

The problem is in finding a *good* candidate for the least happy number of a given height. If the candidate is too large, then the size of the search through sums of squares may be prohibitive. Further, it may be impossible to prove that the image under $S_2$ of the least happy number of the desired height must be the least happy number of the next smaller height or even a permutation of its digits. This could lead to the need for separate searches for additional happy numbers of smaller heights.

It may be that these two problems are not solvable by finding a good candidate. Theoretically, it may be that even with the least happy number found, the search through sums of squares may take too long. It would be interesting to know if there is a bound on the size of the search, that is on the number of unknown digits, regardless of the height involved.

## 3. CUBING HEIGHTS

In this section, we apply the methods developed in Section 2 to the problem of finding least cubic happy numbers of given heights. Table 2 gives the least cubic happy numbers of heights 0 through 8.

| height | cubic happy number |
|---|---|
| 0 | 1 |
| 1 | 10 |
| 2 | 112 |
| 3 | 1189 |
| 4 | 778 |
| 5 | 13477 |
| 6 | $238889 \times 10^{16} - 1$ |
| 7 | $1127 \times 10^{3276941015089163237} - 1$ |
| 8 | $35678 \times 10^{(1127 \times 10^{3276941015089163237} - 1055)/729} - 1$ |

Table 2: The least cubic happy numbers of height 0-8.

As in the last section, we start by computing the heights of all cubic happy numbers less than 20,000. This gives us the least cubic happy numbers of heights 0 through 5. To save computing time we use the fact that all cubic happy numbers are congruent to 1 modulo 3, since $S_3$ preserves congruence classes modulo 3. In the case of happy numbers, we used the fact that a positive integer $x$ is not a happy number if and only if, for some $m \geq 0$, $S_2^m(x) = 4$. For the cubic case, we use the fact that a positive integer congruent to 1 modulo 3 is not a cubic happy number if and only if, for some $m \geq 0$, $S_3^m(x) \in \{55, 136, 160, 370, 919\}$. (See [1] or [2].)

Our method of proof is basically as in Section 2. We consider a positive integer $x$ less than or equal to our claimed least cubic happy number and prove that $x$ must, in fact, equal our candidate. Obviously, in place of a search through sums of squares, we do a computer search through sums of cubes. Otherwise, the algorithm is the same.

Again, we begin with a lemma that is immediate from the computation finding the heights of cubic happy numbers less than 20,000.

**Lemma 5**: *The only cubic happy numbers of height 5 less than 16,000 are 13477, 13747, 13774, 14377, 14737, and 14773.*

**Theorem 6**: *The least cubic happy number of height* 6 *is*

$$\gamma_6 = 238889 \times 10^{16} - 1 = 238888\overbrace{9\ldots9}^{16}.$$

**Proof.** Since $S_3(\gamma_6) = 13747$ is a cubic happy number of height 5, $\gamma_6$ is a cubic happy number of height 6. Let $x \leq \gamma_6$ be a cubic happy number of height 6 with digits in nondecreasing order. Then $S_3(x) < 2^3+21\times 9^3 = 15317$. Since $S_3(x)$ must be a cubic happy number of height 6, by Lemma 5, we have that $S_3(x) \in \{13477, 13747, 13774, 14377, 14737, 14773\}$. Further, $x$ must have at least 13 9's in its base 10 expansion since otherwise $S_3(x) < 2^3+9\times 8^3+12\times 9^3 = 13364$ which is too small. This gives us that

$$x = a_1a_2a_3a_4a_5a_6a_7a_8a_9\,\overbrace{99\ldots9}^{13},$$

with $0 \leq a_1 \leq 2$, and $a_1 \leq a_2 \leq a_3 \leq a_4 \leq a_5 \leq a_6 \leq a_7 \leq a_8 \leq a_9 \leq 9$. We search for combinations such that $\sum_{i=1}^{9} a_i^3 + 13 \times 9^3 \in \{13477, 13747, 13774, 14377, 14737, 14773\}$. A computer search shows that the only solution is

$$x = 238888\,\overbrace{9\ldots9}^{16} = \gamma_6. \ \square$$

**Theorem 7**: *The least cubic happy number of height* 7 *is*

$$\gamma_7 = 1127 \times 10^{3276941015089163237} - 1 = 1126\,\overbrace{9999\ldots99}^{(\gamma_6-226)/729}.$$

**Proof.** It's easy to verify that $\gamma_7$ is a cubic happy number of height 7. Let $x \leq \gamma_7$ be a cubic happy number of height 7 with digits in nondecreasing order. Then $S_3(x) < 1^3 + [(\gamma_6 - 226)/729 + 3] \times 9^3 < \gamma_6 + 1962$. From the computer search in the previous proof, it follows that $S_3(x) = \gamma_6$. Now, $x$ must have at least $(\gamma_6 - 226)/729 - 6$ 9's in its base 10 expansion since otherwise $S_3(x) < 1^3 + 10 \times 8^3 + [(\gamma_6 - 226)/729 - 7] \times 9^3 < \gamma_6$. So

$$x = a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}\,\overbrace{99999\ldots999}^{(\gamma_6-226)/729-6},$$

with $0 \leq a_1 \leq 1$, and $a_1 \leq a_2 \leq a_3 \leq a_4 \leq a_5 \leq a_6 \leq a_7 \leq a_8 \leq a_9 \leq a_{10} \leq 9$. Since $S_3(x) = \gamma_6$, we need $\sum_{i=1}^{10} a_i^3 = 4600$. A computer search shows that the only solution is $x = \gamma_7$. $\square$

**Theorem 8**: *The least cubic happy number of height* 8 *is*

$$\gamma_8 = 35678 \times 10^{(1127\times 10^{3276941015089163237}-1055)/729} - 1 = 35677\,\overbrace{9999\ldots999}^{(\gamma_7-1054)/729}.$$

**Proof.** As usual, we start by noting that $\gamma_8$ is indeed a cubic happy number of height 8. Now, let $x \leq \gamma_8$ be a cubic happy number of height 8 with digits in nondecreasing order. Then $S_3(x) < 3^3 + [(\gamma_7 - 1054)/729 + 4] \times 9^3 = \gamma_7 + 1889$. From the computer search in the previous proof, it follows that $S_3(x) = \gamma_7$. Now, $x$ must have at least $(\gamma_7 - 1054)/729 - 4$ 9's in its base 10 expansion since otherwise $S_3(x) < 3^3 + 9 \times 8^3 + [(\gamma_7 - 1054)/729 - 5] \times 9^3 < \gamma_7$. So

$$x = a_1a_2a_3a_4a_5a_6a_7a_8a_9\,\overbrace{99999\ldots999}^{(\gamma_7-1054)/729-4},$$

with $0 \leq a_1 \leq 3$, and $a_1 \leq a_2 \leq a_3 \leq a_4 \leq a_5 \leq a_6 \leq a_7 \leq a_8 \leq a_9 \leq 9$. Since $S_3(x) = \gamma_7$, we need $\sum_{i=1}^{9} a_i^3 = 3970$. A computer search shows that the only solution is $x = \gamma_8$. $\square$

## ACKNOWLEDGMENTS

The first author wishes to acknowledge the support of the Science Scholars Fellowship Program at the Bunting Institute of Radcliffe College. The second author wishes to acknowledge the support of the Dorothy Nepper Marshall Fellows Program of Bryn Mawr College.

## REFERENCES

[1] H.G. Grundman and E.A. Teeple. "Generalized Happy Numbers." *The Fibonacci Quarterly* **39** (2001): 462-466.
[2] R. Guy. *Unsolved Problems in Number Theory*. Springer-Verlag, New York, 1994.
[3] R. Guy. Personal Correspondence. 1997.
[4] R. Honsberger. *Ingenuity in Mathematics*. The Mathematical Association of America, Washington, 1970.
[5] N.J.A. Sloane. *The on-line encyclopedia of integer sequences*. http://www.research.att.com/ñjas/sequences/.

AMS Classification Numbers: 11A63

✠ ✠ ✠

# ON MODULAR FIBONACCI SETS


## Mihai Caragiu

Ohio Northern University and Institute of Mathematics Bucharest
E-mail: m-caragiu1@onu.edu

## William Webb

Department of Pure and Applied Mathematics, Washington State University, Pullman, WA 99164-3113
E-mail: webb@math.wsu.edu



*(Submitted February 2001-Final Revision June 2001)*


## 1. INTRODUCTION

For any prime $p$ let us define the modular Fibonacci set Fib$[p]$ to be the subset of $\mathbf{F}_p = \{0, 1, \ldots, p-1\}$ (the finite field with $p$ elements) consisting of *all the terms appearing in the Fibonacci sequence modulo p*. For example, when $p = 41$ we have the Fibonacci sequence modulo 41

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 14, 7, 21, 28, 8, 36, 3, 39, 1, 40, 0, 40, 40, 39,$$

$$38, 36, 33, 28, 20, 7, 27, 34, 20, 13, 33, 5, 38, 2, 40, 1, 0, \ldots$$

so that the corresponding modular Fibonacci set will be

$$\mathrm{Fib}[41] = \{0, 1, 2, 3, 5, 7, 8, 13, 14, 20, 21, 27, 28, 33, 34, 36, 38, 39, 40\} \subset \mathbf{F}_{41}.$$

Of course there are plenty of ways of picking up a special subset of $\mathbf{F}_p$ for any prime $p$. One possible choice would be to select within any finite prime field $\mathbf{F}_p$ the set of *all perfect squares modulo p*, say Sq$[p]$ so that, for example,

$$\mathrm{Sq}[11] = \{0, 1, 3, 4, 5, 9\}.$$

An interesting thing about the sets Sq$[p]$ is that they admit a uniform description by a first-order logical formula, namely

$$\Phi(X) \equiv (\exists Y)(X = Y^2)$$

The above $\Phi(X)$ is a first-order formula written in the language of rings such that for any prime $p$ the subset Sq$[p]$ of $\mathbf{F}_p$ coincides with the set of all elements $x \in \mathbf{F}_p$ satisfying $\Phi$:

$$\mathrm{Sq}[p] = \{x \in \mathbf{F}_p : \Phi(x) \text{ true}\}.$$

In a more technical language, we can say that *the perfect squares are first-order definable*.

At this moment the following natural question can be asked: is there a formula $\theta(X)$ that defines in each field $\mathbf{F}_p$ the set Fib$[p]$? By providing a *negative answer* to the above question, the present note establishes a worth noting, albeit negative, property of the family of modular Fibonacci sets. Our main result is the following:

**Theorem 1**: *There is no formula $\theta(x)$ written in the first-order language of rings that defines in each field $\mathbf{F}_p$ the set* Fib$[p]$.

For basic concepts of logic and model theory, including that of elementary formula one may consult [1]. An essential role in the proof of Theorem 1 will be played by the following result [2] estimating the number of points of definable subsets of finite fields:

**Theorem 2**: If $\theta(X)$ is a formula in one free variable $X$ written in the first-order language of rings, then there are positive constants $A$, $B$, and positive rational numbers $0 < \mu_1 < \cdots < \mu_k \leq 1$ such that for any finite field $\mathbf{F}_q$, if $N_q(\theta)$ represents the number of elements $a \in \mathbf{F}_q$ such that $\theta(a)$ is true, either

$$N_q(\theta) \leq A$$

or

$$|N_q(\theta) - \mu_i q| \leq B\sqrt{q}$$

for some $i \in \{1, \ldots, k\}$.

**Example**. Consider

$$\theta(x) \equiv (\exists Y_1) \ldots (\exists Y_n)[(X + 1 = Y_1^2) \wedge \cdots \wedge (X + n = Y_n^2)]$$

so that $\theta(X)$ asserts that $X + 1, X + 2, \ldots, X + n$ are perfect squares within the field. In this case one can take $k = 2$ with $\mu_1 = 1/2^n$ and $\mu_2 = 1$. The first value, $\mu_1$, stands for the fields of odd characteristic. Indeed, according to a classical result of Davenport, the number $N = N(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ of elements $x \in GF(q)$ for which the Legendre character takes $n$ preassigned values $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ on $x + d_1,\ x + d_2, \ldots, x + d_n$, can be estimated ([4], p. 263) as $N = q/2^n + O(n\sqrt{q})$ with an absolute implied constant. The second value $\mu_2$ stands for the finite fields of characteristic two, in which every element is a square.

## 2. PROOF OF THE MAIN RESULT

In order to apply Theorem 2 to the proof of our main result, we will need a result on the cardinalities of the modular Fibonacci sets Fib[$p$].

**Proposition 3**: For any $\varepsilon > 0$ there exists a prime $p$ such that

$$|\mathrm{Fib}[p]| < p\varepsilon.$$

**Proof**: From [3] and [5] it follows that if $k(p)$ is the period of the Fibonacci sequence modulo $p$, then $p/k(p)$ is an unbounded function of the prime $p$. Proposition 3 is a straight-forward consequence of this fact.

We now proceed to the proof of Theorem 1. Let us suppose, by contradiction, that there exists some formula $\theta(X)$ in the first-order language of rings, with the property that for any prime $p$ and any $x \in \mathbf{F}_p$

$$x \in \mathrm{Fib}[p] \Leftrightarrow \theta(x) \text{ true in } \mathbf{F}_p.$$

Let $A$, $B$ and $0 < \mu_1 < \cdots < \mu_k \leq 1$ be the constants associated to the formula $\theta$ by Theorem 2. It follows then for any prime $p$, either

$$|\mathrm{Fib}[p]| \leq A \tag{1}$$

or

$$||\mathrm{Fib}[p]| - \mu_i p| \leq B\sqrt{p} \tag{2}$$

for some $i \in \{1, \ldots, k\}$. Note that (1) fails for all sufficiently large $p$, since the sequence of Fibonacci numbers is strictly increasing after the second term. Thus, for $p$ big enough it is

(2) which must be true. However, by proposition 3, there are arbitrarily large $p$ for which (2) fails for $i = 1, \dots, k$. Thus a formula $\theta(X)$ as above cannot exist.

**Remark**: In the same way one can prove that there is no finite set $\{\theta_1(X), \dots, \theta_n(X)\}$ of first-order formulas written in the language of rings such that for each prime $p$ some formula $\theta_i(X)$ defines Fib[$p$] in the field $\mathbf{F}_p$.

## REFERENCES


[1] C.C. Chang and H.J. Keisler. *Model Theory*. Second Edition, North-Holland, Amsterdam, 1977.

[2] Z. Chatzidakis, L.v.d. Dries and A. Macintyre. "Definable Sets Over Finite Fields." *Crelle Journal* **427** (1992): 107-135.

[3] D. Jarden. "Unboundedness of the function [p-(5/p)]/a(p) in Fibonacci's sequence." *A.M. Monthly* **53** (1946): 426-427.

[4] R. Lidl and H. Niederreiter. *Finite Fields*. Second Edition, Cambridge University Press, 1997.

[5] J. Vinson. "The Relation of the Period Modulo $m$ to the Rank of Apparition of $m$ in the Fibonacci Sequence." *The Fibonacci Quarterly* **1** (1963): 37-45.


AMS Classification Numbers: 11TXX, 11B50

✠ ✠ ✠

# A NIM-TYPE GAME AND CONTINUED FRACTIONS

**Tamás Lengyel**
Occidental College, 1600 Campus Road, Los Angeles, CA 90041
*(Submitted April 2001-Final Revision July 2001)*

## 1. INTRODUCTION

In the two-person nim-type game called *Euclid* a position consists of a pair $(a, b)$ of positive integers. Players alternate moves, a move consisting of decreasing the larger number in the current position by any positive multiple of the smaller number, as long as the result remains positive. The first player unable to make a move loses. In the restricted version a set of natural numbers $\Lambda$ is given, and a move decreases the larger number in the current position by some multiple $\lambda \in \Lambda$ of the smaller number, as long as the result remains positive. We present winning strategies and tight bounds on the length of the game assuming optimal play. For $\Lambda = \Lambda_k = \{1, 2, \ldots, k\}, k \geq 2$, the winner is determined by the parity of the position of the first partial quotient that is different from 1 in a reduced form of the continued fraction expansion of $b/a$.

Apparently, the game was introduced by Cole and Davie [1]. An analysis of the game and more references can be found in [1,7] (see also [3]). The goal is to determine those $a$ and $b$ for which the player who goes first from position $(a, b)$ can guarantee a win with optimal play. There is no tie and the game is finite so one of the players must have a winning strategy for each starting position $(a, b)$. The winning positions are intimately related to the ratio of the larger number to the smaller one when compared to the golden ratio, $\Phi = \frac{1+\sqrt{5}}{2} \approx 1.6180$, as it is demonstrated by

**Theorem A**: Player 1 has a winning strategy if and only if the ratio of the larger number to the smaller in the starting position is greater than $\Phi$.

The winning strategy can be described in terms of the set $\mathcal{W}$ of all unordered pairs $(a, b), a, b > 0$, with the property that $b/a > \Phi$, or $a/b > \Phi$ and its complement set $\mathcal{L}$. It is showed [1,8] that for any pair in $\mathcal{W}$, there is at least one move that leaves a pair in $\mathcal{L}$, and for any pair in $\mathcal{L}$, all legal moves leave a pair in $\mathcal{W}$. We describe the solution in geometric terms in Section 2.

Without loss of generality, we can assume that $a < b$ for the starting position $(a, b)$. (Afterwards, whenever it is helpful, we automatically rearrange the terms so that the first number is the smaller one as long as the numbers are different.) Accordingly, Player 1 has a winning strategy if and only if $b/a > \Phi$. We study a simple variation of the game in Section 3. It leads to the use of the Euclidean algorithm to obtain the continued fraction expansion relevant to the game. In Section 4 this approach is applied to the original game, and results on its length $L(a,b)$ are also given. Generalized versions of the game are introduced and analyzed in Section 5.

## 2. THE GEOMETRIC APPROACH

We consider the open cone defined by $\mathcal{L} = \{(x,y)|x,y > 0, 1/\Phi < y/x < \Phi\}$. The goal of the game is to move to the diagonal $y = x$ and thereby prevent the other player from making further moves. We have two cases depending on whether $(a,b)$ is in $\mathcal{L}$ or not. The following two properties describe the differences and are illustrated in Figures 1-3.

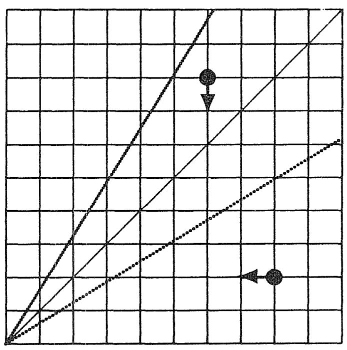

Figure 1

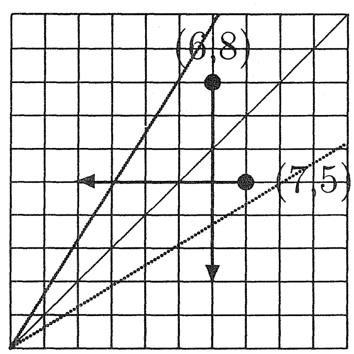


Figure 2

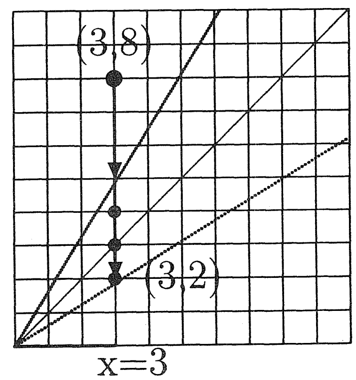


Figure 3

(i) For every pair $(a,b), a \neq b$, there is exactly one direction (horizontal or vertical) in which one can make a legal move. From a position $(a,b) \in \mathcal{L}$ there is only one legal move, and it leads to a position outside $\mathcal{L}$.

(ii) For every $a$ there are exactly $a$ points in $\mathcal{L}$ with $x = a$. Therefore, if $a < b$, then there is a unique integer multiple of $a$, say $d = \lambda a$, such that decreasing $b$ by $d$ places the new pair $(a, b-d)$ in $\mathcal{L}$ provided $(a,b) \notin \mathcal{L}$.

The first graph shows that $(a,b)$ with $a < b$ forces a downward move while we must move to the left if $a > b$. Note that the case $(a,b)$ with $a > b$ can be reduced to the one with $a < b$ by a reflection with respect to the line $y = x$. If $(a,b) \in \mathcal{L}, a < b$, then $a < b < 2a$ and thus $(a, b-a)$ is the only legal move from $(a,b)$ (Figure 2). It is easy to see that $\frac{a}{b-a} > \Phi$, yielding property (i). Property (ii) is illustrated in Figure 3. For every integer $a$ there are exactly $a$ points with integer coordinates on the line $x = a$ within the cone $\mathcal{L}$. This follows by the observation that the line $x = a$ meets $\mathcal{L}$ in a segment of length $\Phi a - \frac{1}{\Phi}a = a$. If $(a,b) \notin \mathcal{L}$ then, by the irrationality of $\Phi$, there is exactly one move leading to a point $(a,b') \in \mathcal{L}$ for some integer $b'$, as opposed to the case $(a,b) \in \mathcal{L}$ when the only legal move will take the player outside $\mathcal{L}$ (Figure 2).

In case of the optimal play the loser has only one legal move available to him at each step, i.e., his moves are forced upon him and he cannot even extend the length of the game.

Figure 4 illustrates two typical games: the starting position (9,2) and (11,8) give the winning strategy to Players 1 and 2, respectively. In Section 5 we introduce variations of the game in which restrictions on the moves guarantee that even the loser has choices to make.

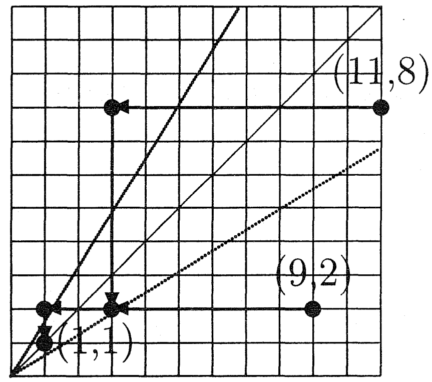


Figure 4

## 3. A VARIATION AND THE EUCLIDEAN ALGORITHM

In this section, we turn to a deterministic version of the game. Players alternate moves, and a move decreases the larger number in the current position by the smaller number, as long as the result remains positive. The first player unable to make a move loses. The reason for introducing this variation is to understand how simple continued fractions help in analyzing these and the original games. In fact, the notion of continued fractions is based on the process of continued alternating subtractions [2]. We can express rational numbers as continued fractions by using the Euclidean algorithm. First we take the finite simple continued fraction expansion of $b/a = [a_0, a_1, a_2, \ldots, a_n]$. The natural number $a_i$ is called the $i^{th}$ partial quotient (or continued fraction digit) of $b/a$. (Note that we start indexing at $i = 0$.) This form provides us with a representation of the steps of this game. Note that if $b = qa+r$ with integers $q$ and $r (0 \leq r < a)$, then $q = a_0$. After $a_0$ consecutive subtractions of $a$ from $b$ the remainder becomes smaller than $a$. We switch their roles and keep continuing the subtractions until $r = 0$, at which point $a = b$. The number of legal moves in this game is $a_0 + a_1 + \cdots + a_n - 1$; thus Player 1 wins if and only if $\sum_{i=0}^{n} a_i$ is even.

Note that if $a_n \neq 1$ then the $n+1$-digit $[a_0, a_1, a_2, \ldots, a_n]$ and the $n+2$-digit $[a_0, a_1, a_2, \ldots a_{n-1}, a_n - 1, 1]$ forms stand for the same rational number and the digit sum is not affected. The former expansion is called the *short* form. In this paper we always use short forms.

Asymptotic results for the average of length $L'(a,b) = \sum_{i=0}^{n} a_i - 1$ of the game are given in [2].

## 4. THE CONTINUED FRACTION BASED APPROACH

We can also completely describe the winning strategy for the original game in terms of the partial quotients $a_i$ of $b/a, a < b$. If $b/a = [a_0, a_1, \ldots, a_{n+1}] = [1, 1, \ldots, 1]$, i.e., $a_i = 1$ for each $i = 0, 1, \ldots, n+1$, then we switch to the short form $[a_0, a_1, \ldots, a_{n-1}, 2]$ with $a_i = 1, i = 0, 1, \ldots, n-1$. (Note that this happens only if we divide two consecutive Fibonacci numbers.) In this way, we can guarantee that at least one of the partial quotients is different from 1.

Clearly, as long as $a_i = 1, i = 0, 1, \ldots, k-1$, players are forced to take the smaller number from the larger. If the next quotient $a_k \neq 1$, then we say that $a_k$ is the first digit different from 1. For any position $(a, b), a < b$, with $b/a = [a_0, a_1, \ldots, a_n]$, the actual move of taking $\lambda a$ from $b$ can be specified by the positive integer multiplier $\lambda$. The resulting position can be described by the fraction $[a_1, \ldots, a_n]$ if $\lambda = a_0$ or $[a_0 - \lambda, a_1, \ldots, a_n]$ if $\lambda < a_0$. Clearly, every move affects the actual first continued fraction digit only. The following theorem was suggested by Richard E. Schwartz [6].

**Theorem 1**: Let $[a_0, a_1, \ldots, a_n]$ with $a_n \geq 2$ be the continued fraction expansion of $b/a$ for the starting position $(a, b), a < b$. Player 1 has a winning strategy if and only if the first partial quotient $a_i$ that is different from 1 appears at a position with an even index. In other words, the first player who can actually make a non-forced move has a winning strategy.

This theorem is the explicit form of the statement made by Spitznagel [7] who noted that "the opponent of someone following the (winning) strategy is likely to notice his moves are being forced every step of the way, and from this observation it might be possible for him to determine what the strategy must be."

Note that the short continued fraction notation guarantees that there is a digit different from 1, namely $a_n \geq 2$. We use the notation $e_{k+1} = [a_{k+1}, a_{k+2}, \ldots, a_n]$.

**Proof**: If $a_k \geq 2$ then the player facing the ratio $b'/a' = [a_k, \ldots, a_n]$ can win. This means that once a player meets the first partial quotient different from 1 then she can win, and the other player will face a 1 in every consecutive step (otherwise a reversal of strategy would be possible). Assume that we have already removed the leading 1s from the expansion and $k < n$. We will see that the optimal play closely follows the continued fraction expansion by processing and removing consecutive digits. It takes one or two moves (one for each player) to eliminate the actual digit. We have two cases.

(*) If $e_{k+1} < \Phi$ then this player can take $a_k a'$ from $b'$ leaving $y = e_{k+1}$ behind, with $1/\Phi < 1 < e_{k+1} < \Phi$. Note that $a_{k+1} = 1$ follows. In this case there is a single move used to remove $a_k$ from the expansion to get position $(a'', b'')$ with ratio $y = [a_{k+1}, a_{k+2}, \ldots, a_n] = [1, a_{k+2}, \ldots, a_n]$.

(**) Otherwise $e_{k+1} > \Phi$ and player takes only $(a_k-1)a'$ from $b'$ leaving $y = [1, a_{k+1}, a_{k+2}, \ldots, a_n]$ behind. Once again $y < \Phi$, for

$$1/\Phi < 1 < y = 1 + 1/e_{k+1} < 1 + 1/\Phi = \Phi.$$

The pair $(a'', b'')$ left for the other player has ratio $y = b''/a'' < \Phi$. Therefore, $y$ has a continued fraction expansion starting with 1 and thus the other player is forced to take $a''$ from $b''$. In this case it takes two moves to remove $a_k$ from the continued fraction expression.

In any case, after the other player's move is finished, we get $\frac{b''-a''}{a''} = \frac{b''}{a''} - 1 < \Phi - 1 = \frac{1}{\Phi}$. We set $b''' = a''$ and $a''' = b'' - a''$, flip the numerator and denominator, and derive that the resulting ratio $b'''/a''' > \Phi$. With $d = \lfloor b'''/a''' \rfloor \geq 1$ we can rewrite $b'''/a''' = d + \frac{1}{z} > \Phi$. In fact, $d = a_{k+2}$ and $z = [a_{k+3}, a_{k+4}, \ldots, a_n]$ if we followed (*), while $d = a_{k+1}$ and $z = [a_{k+2}, a_{k+3}, \ldots, a_n]$ if we used (**). The case $d \geq 2$ can be reduced to that of $a_k \geq 2$. If $d = 1$ then $1/z > \Phi - 1 = 1/\Phi$, i.e., $z < \Phi$, and we proceed with the argument used in (*), with $z$ playing the role of $e_{k+1}$.

We can continue this until $k$ becomes $n$ when the player can take the $(a_n - 1)$-times multiple of the smaller number from the larger one, leaving equal numbers for the other player, who will be unable to make a move. □

We repeatedly applied the simple fact that $1 + \frac{1}{z} > \Phi$ if and only if $z < \Phi$. The player with winning strategy cannot make a mistake if she wants to win. In summary, she can (and must) always leave $y = [1, u_0, u_1, \ldots, u_m]$ with $u = [u_0, u_1, \ldots, u_m] > \Phi$ behind for the other player. This makes $y < \Phi$ and forces the other player to simply take the actual smaller number from the larger one. In turn she will face a position with a "safe fraction" $u > \Phi$, i.e., a position outside $\mathcal{L}$.

**Remark**: Theorems A and 1 both give a necessary and sufficient condition for Player 1 to have a winning strategy. This way we obtain a characterization of the condition that $x = [a_0, a_1, \ldots, a_n]$ is greater than $\Phi$ in terms of the parity of the location of the first continued fraction digit $a_i$ different from 1. This is in agreement with the fact that $\Phi = [1, 1, 1, \ldots]$, and the convergents alternately are above and below the exact value.

Assuming optimal play by the winner, tight bounds for the length $L(a, b)$ of the game are given in

**Theorem 2**: Let $[a_0, a_1, \ldots, a_n]$ with $a_n \geq 2$ be the continued fraction expansion of $b/a$ for the starting position $(a, b), a < b$. For the number $L(a, b)$ of steps of the game we get that

$$n + 1 \leq L(a, b) = n + 1 + \sum_{\substack{a_k \geq 2 \\ [a_{k+1}, \ldots, a_n] > \Phi}} 1 \leq 2n + 1.$$

The lower bound is attained if and only if the partial quotients are equal to 1 at all even or all odd positions. The upper bound is reached if and only if all partial quotients are at least 2.

Note that we use the short notation. For example, the position (5,13) has ratio 13/5=[2,1,1,2]; hence the lower bound is not attained according to the theorem. In fact, $L(5,13) = 5$. The long form $13/5 - [2,1,1,1,1]$ does not satisfy the condition $a_n \geq 2$ of the theorem.

**Proof**: The proof is based on that of Theorem 1. The lower bound assumes that there are only simple moves, i.e., either a 1 is removed or (*) is used. In the latter case, if for some $k$ and $m > k : a_k \neq 1, a_{k+1} = \cdots = a_{m-1} = 1$, and $a_m \neq 1$, then $m - k$ must be even to guarantee that $e_{k+1} < \Phi$ by the Remark made after Theorem 1.

The identity for $L(a, b)$ follows from the observation that an extra move is made when a player applies (**), i.e., when the conditions $a_k \geq 2$ and $e_{k+1} > \Phi$ are satisfied.

To reach the upper bound $a_k \geq 2, k = 0, 1, \ldots, n$, suffices. In this case the game and the Euclidean algorithm are closely related in the following sense. At any position $(a, b)$, if $b = qa + r, q \geq 2, 0 \leq r < a$, then Player 1 takes $q - 1$ (rather than $q$) times $a$ away from $b$. If $r = 0$ then the game is over. Otherwise, the other player is left with no other choice but to take $a$ from $b-(q-1) \cdot a$, for $a < b-(q-1) \cdot a < 2a$. If the original ratio is $b/a = [a_0, a_1, \ldots, a_n]$ then, at each step, Player 1 will take $a_0 - 1, a_1 - 1, \ldots$ times the actual smaller number from the actual bigger one while Player 2 always subtracts the smaller one from the bigger one (and stops when the numbers are equal). Note that Player 1 has a winning strategy when the upper bound is attained. □

**Examples**: The games illustrated in Figure 4 have length $L(9, 2) = 3$ for $9/2 = [4, 2]$ (better yet $9/2 = [4_+, 2]$), and $L(11, 8) = 4$ for $11/8 = [1, 2, 1, 2]$. (The symbol + in the subscript indicates that an extra step is needed due to passing through (**). )

**Example: reverse games**: We can reverse the continued fraction digits of $b/a$ to get the "reverse" game. If $b/a = [a_0, a_1, \ldots, a_n]$ and $\gcd(a, b) = 1$ then we take $c = [a_n, a_{n-1}, \ldots, a_0]$ in its short form. It is easy that the numerator of $c$ (in lowest terms) is $b$, i.e., $c = b/a'$ with some $a'$ such that $\gcd(a', b) = 1$. If $a_0 > 1$ then for the "reverse" game starting at position $(a', b)$ we obtain $L(a', b) = L(a, b)$. For example, $18/7 = [2_+, 1, 1, 3]$ gives $L(7, 18) = 5$ and a reverse $18/5 = [3_+, 1, 1, 2]$ which takes $L(5, 18) = 5$ steps. If Player 2 has the winning strategy then $L(a', b) = L(a, b) - 1$; otherwise $L(a', b) = L(a, b)$ by the Remark made after Theorem 1. In fact, $43/25 = [1, 1, 2_+, 1, 1, 3]$ has $L(25, 43) = 7$ and $43/12 = [3_+, 1, 1, 2_+, 2]$ gives $L(12, 43) = 7$.

The game favors Player 1. In fact, Player 1 has more than 60% chance of winning [7]. Assuming that the average behavior of integers $0 < a < b \leq N$ approximates that of the random reals in $[0, N]$ and using the goemetric approach, Theorem A suggests $1/\Phi \approx .618$ for the winning probability in the following sense: $\lim_{N \to \infty} P((a, b) \in \mathcal{W} | a < b \leq N) = 1/\Phi$.

The length $n+1$ of the *shortest* game is the running time of the Euclidean algorithm, and its average is asymptotically $\frac{12\ln 2}{\pi^2}\ln N \approx 0.843\ln N$ for randomly selected starting positions $(a,b), a < b \leq N$, as $N \to \infty$ (cf. [2]). (The worst case scenario for the length of the shortest game occurs for Fibonacci-type games, i.e., when the starting position is $(a,b) = (q_{n+1}, p_{n+1})$ for some $n \geq 1$ such that $p_{n+2} = p_{n+1} + p_n$ and $q_{n+1} = p_n$ with $p_0 = 1$ and integer $p_1 = c \geq 2$. The resulting ratio is $b/a = [a_0, a_1, \ldots, a_n] = [1, 1, \ldots, 1, c]$, and the length is asymptotically $\frac{\ln N}{\ln \Phi} \approx 2.078\ln N$ in this case.)

For the length $L(a,b)$ computer simulation suggests that it takes about 9-10 steps on the average to finish games with starting positions $(a,b), a < b \leq 10000$.

## 5. THE RESTRICTED GAME: REDUCTION AND GENERALIZATIONS

In this section, emphasizing the competitive nature of the original game, we discuss its restricted versions which, at the same time, generalize the version discussed in Section 3. Given a set of natural numbers $\Lambda$, players alternate moves, and a move decreases the larger number in the current position by some multiple $\lambda \in \Lambda$ of the smaller number, as long as the result remains positive. The first player unable to make a move loses. For the original game we have $\Lambda = \{1, 2, 3, \ldots\}$. We are interested in various subsets of this set. Theorems 4, 5, and 6 give the complete analysis for three different subsets. The simplified deterministic game of Section 3 works with $\Lambda = \{1\}$. By the connection between the game and the corresponding continued fraction expansion we can easily see

**Proposition 3**: Theorems 1 and 2 can be extended to hold under the conditions $\Lambda = \Lambda_k = \{1, 2, \ldots, k\}, b/a = [a_0, a_1, \ldots, a_n]$ with $a < b, a_i \in \{1, 2, \ldots, k\}$ for all $i = 0, 1, \ldots, n$, and $a_n \geq 2$.

The next interesting case is $\Lambda = \Lambda_2$ with no restrictions on the $a_i$'s. We sketch the analysis of this game and characterize winning strategies in Theorem 4. The general case of $\Lambda_k$ is covered by Theorem 5. There is an evident parallelism with the original game though the restricted version seems more fair and interesting, for it is no longer true that the first player who can actually make a non-forced move has a winning strategy.

We introduce a reduction of the partial quotients of $[a_0, a_1, \ldots, a_n]$ resulting in a reduced sequence of digits $[r_0, r_1, \ldots, r_m]$ made of 1s and 2s only. This form helps us in finding the player with a winning strategy. In fact, the characterization of a winning strategy in terms of the digits of the reduced sequence reminds us of that of the original games. Once a player meets the first digit $r_i$ different from 1 then she can win by never letting the other player face a 2 in the reduced sequence.

Every partial quotient $a_i \geq 4$ can be replaced by a 1 if $a_i \equiv 1 \bmod 3$ and by a 2 if $a_i \equiv 2 \bmod 3$. Any multiple of 3 simply can be dropped from the continued fraction expansion as it gives benefit to neither player: it can be used for keeping one's turn but cannot be used to switch turns. (Although this fact can be seen directly, a formal justification of this rule will come out in Cases (e) and (f) in the proof of Theorem 4.) We append a 2 to the end of all reduced sequences not ending in a 2. For example, after replacements, we get $11/9= [1,4,2] \Rightarrow [1,1,2]$ and $36/29 = [1,4,7] \Rightarrow [1,1,1,2]$, and Player 1 and Player 2 can win in the respective games. In both cases the first 2 characterizes the goals of Player 1: in the former one Player 1 will force Player 2 to finish the removal of the partial quotient 4. In the latter one, Player 1 tries to accomplish the removal of 4 but Player 2 can prevent it from happening by moving to 3, and then to 0, thus forcing Player 1 to face the last quotient 7, then 4 and 1. Remarkably, the conditions of Theorem 1 still work.

**Theorem 4**: For the game $\Lambda = \Lambda_2$, Player 1 has a winning strategy if and only if in the reduced form the first digit $r_i$ that is different from 1 appears at a position with an even index.

**Proof**: The proof is done by induction on the length of the reduced sequence $[r_0, r_1, \ldots, r_m]$. We give only the main ideas. Let $x = [a_0, a_1, \ldots, a_n]$ be a ratio with reduced form $[r_0, r_1, \ldots, r_m], r_i \in \{1,2\}, i = 0, 1, \ldots, m$. Player 1 refers to the player facing $x$. The statement holds for $m = 0$, i.e., reduced sequences of length 1. In this case, the $a_i$'s are multiples of 3 potentially followed by a last digit $a_n \equiv 2 \bmod 3$. Winning by Player 1 is assured (cf. Cases (e) and (c) below). Suppose that the statement is true for any reduced sequence $[r_1, r_2, \ldots, r_m]$ of length $m$.

We prove that any reduced sequence $[r_0, r_1, r_2, \ldots, r_m]$ of length $m+1$ means a win for Player 1 if the first digit is $r_0 = 2$ or if the player facing the sequence $[r_1, \ldots, r_m]$ loses. Nothing changes if the first digit $a_0$ is dropped. We have six cases. The first two deal with $r_0 = 1$, while the next two are concerned with $r_0 = 2$. The last two refer to cases when $a_0$ is removed, i.e., when $a_0$ is a multiple of 3. Each step involves a goal to be met by the player with a winning strategy.

Case (a): The player faced with $[r_1, r_2, \ldots, r_m]$ wins and $a_0 \equiv 1 \bmod 3$. Any move with miltiplier $\lambda$ by Player 1 can be complemented by Player 2 using a move with multiplier $3 - \lambda$ to yield $a_0' \equiv 1 \bmod 3$, and finally forcing Player 1 to remove the first digit of $x$, leaving Player 2 in a winning position $[r_1, r_2, \ldots, r_m]$.

Case (b): The player faced with $[r_1, r_2, \ldots, r_m]$ loses and $a_0 \equiv 1 \bmod 3$. Player 1 can always move to some $a_0'$ congruent to 0 mod 3 and finally remove the first digit of $x$. This makes Player 2 start with $[r_1, r_2, \ldots, r_m]$ and hence Player 1 a winner.

Case (c): The player faced with $[r_1, r_2, \ldots, r_m]$ wins and $a_0 \equiv 2 \bmod 3$. Player 1 can always move to some $a_0'$ congruent to 1 mod 3 and finally force Player 2 to remove the first digit of $x$. Now Player 1 is facing $[r_1, r_2, \ldots, r_m]$ and wins.

Case (d): The player faced with $[r_1, r_2, \ldots, r_m]$ loses and $a_0 \equiv 2 \bmod 3$. Player 1 can always move to some $a_0'$ congruent to 0 mod 3 and finally remove the first digit of $x$. This makes Player 2 start with $[r_1, r_2, \ldots, r_m]$ and hence Player 1 is a winner.

Case (e): The player faced with $[r_1, r_2, \ldots, r_m]$ wins and $a_0 \equiv 0 \bmod 3$. Player 1 can always move to some $a_0'$ congruent to 1 mod 3 and finally force Player 2 to remove the first digit of $x$. Now Player 1 is facing $[r_1, r_2, \ldots, r_m]$ and wins.

Case (f): The player faced with $[r_1, r_2, \ldots, r_m]$ loses and $a_0 \equiv 0 \bmod 3$. Any move with multiplier $\lambda$ by Player 1 can be complemented by Player 2 using a move with multiplier $3 - \lambda$ to yield $a_0' \equiv 0 \bmod 3$. Finally Player 2 removes the first digit of $x$. Now Player 1 is facing $[r_1, r_2, \ldots, r_m]$ and loses. This completes the inductive step. □

Note that if the first digit is reduced to 1 then it acts like a negation, i.e., changing the winner-loser relationship based on $[r_1, r_2, \ldots, r_m]$ in agreeement with the theorem. The optimal play can be established by processing the reduced sequence backwards, i.e., from right to left and setting goals for the moves in accordance with the proof. At the end, the winning strategy emerges as a sequence of instructions on how to remove the digits of the original continued fraction one by one, from left to right. The following examples illustrate the process.

**Example**: The starting position (6,19), i.e., $19/6 = [3, 6]$ reduces to [2] which is a win for Player 1. As [6] reduces to [2], which is a win for Player 1, we proceed with Case (e). The goal for Player 1 is to always move to some value $v \equiv 1 \bmod 3$ at this digit. As [3,6] reduces to [2] again, the same goal is set for Player 1. In terms of the actual steps, Player 1 first finds that the first target is $v = 1$ as $v \equiv 1 \bmod 3$. This instructs Player 1 to take twice the smaller number from the larger one, i.e., $2 \cdot 6$ from 19. It leaves the position $(6, 7)$ with $7/6 = [1, 6]$ for Player 2 forcing the removal of the quotient 1. Player 1 is presented with $6/1 = [6]$, i.e., the position (1,6). Player 1 has to move to $4 \equiv 1 \bmod 3$ by Case (e) again. In fact, the game is completed by taking $2 \cdot 1$ from 6 to yield (1,4). Now Player 2 moves to $(1, u), u = 2$ or 3, and Player 1 wraps up the win by moving to 1 mod 3, i.e., (1,1).

**Example**: The ratio $2393/459 = [5, 4, 1, 2, 6, 5]$ results in [2,1,1,2,2], i.e., a win for Player 1. The backward processing provides the following goals: at quotient 5 move to 1 mod 3 by Case (c), at 6 move to 1 mod 3 by Case (e), at 2 move to 1 mod 3 by Case (c), at 4 move to 0 mod 3 by Case (b), and at 5 move to 1 mod 3 by Case (c). Note that $1934/459 = [4, 4, 1, 2, 6, 5]$ is a win for Player 2 according to the reduced sequence [1,1,1,2,2]. The goals for Player 2 are similar to those of the previous example for Player 1 except that at processing the first quotient 4, Player 2 must move to 1 mod 3 by Case (a).

For the length $L_2(a, b)$ of the game we get $L_2(a, b) = 2 \sum_{a_i \neq 1} \lceil \frac{a_i}{3} \rceil + n_1 - n_{a,b,d} - 1$ where $n_1$ and $n_{a,b,d}$ are the number of $a_i$'s that are equal to 1 and the number of times we used Cases (a), (b), and (d).

The general case $\Lambda = \Lambda_k, k \geq 2$, is fairly similar to that of $\Lambda_2$. Reduction can be applied in the following sense: any multiple of $k + 1$ can be dropped from the continued fraction expansion and every partial quotient $a_i > 2$ can be replaced by a 1 if $a_i \equiv 1 \bmod (k + 1)$ and by a 2 if $a_i \equiv 2, 3, \ldots, k \bmod (k + 1)$. Theorem 4 translates into

**Theorem 5**: Player 1 has a winning strategy for the game $\Lambda = \Lambda_k, k \geq 2$, if and only if in the reduced form the first digit $r_i$ that is different from 1 appears at a position with an even index. For the length $L_k(a,b)$ of the game we get $L_k(a,b) = 2\sum_{a_i \neq 1}\lceil\frac{a_i}{k+1}\rceil + n_1 - n_{a,b,d} - 1$ where $n_1$ and $n_{a,b,d}$ are the number of $a_i$'s that are equal to 1 and the number of times we used Cases (a), (b), and (d).

We omit the proof, which closely follows that of Theorem 4 with Cases (c) and (d) referring to $a_0 \equiv 2, 3, \ldots, k \bmod (k+1)$. Note that if $k = 1$ then we never encounter Cases (c) and (d). Cases (a) and (b) correspond to an odd quotient $a_i$ and thus, $L_1(a,b)$ is in agreement with $L'(a,b) = \sum_{i=0}^{n} a_i - 1$.

The winner can be determined by using the reduced sequence in its short form. One might think (but the author has not been able to prove) that the winning probability of Player 1 for game $\Lambda_k$ changes from $1/2$ to $1/\Phi$ as $k \to \infty$.

The reader might consider other generalizations of the original game. Clearly, $\Lambda$ must contain 1 if we want the game to be playable until a ratio of 1 is reached. The referee suggested selecting $\Lambda$ to be the set of all odd natural numbers. It turns out that this version can be analyzed similarly to the deterministic game discussed in Section 3 by means of a slightly more general

**Theorem 6**: For any subset $\Lambda$ of the odd natural number containing 1, Player 1 wins if and only if the parity of the sum of the partial quotients of $b/a$ is even.

The proof is straightforward for every move changes the parity of the sum. The game is deterministic in the sense that the outcome of the game is not influenced by skill. Only the length of the game can be affected by the particular moves.

Note that one can play the general game on the Stern-Brocot tree, starting at point 1 and ending at $b/a$, by playing $n+1$ consecutive subtraction games of sizes $a_0, a_1, \ldots, a_{n-1}$, and $a_n - 1$.

## ACKNOWLEDGMENT

I wish to thank Ramin Naimi for helpful discussions and for involving Richard Schwartz who suggested Theorem 1. I also thank Greg Tollisen for his useful suggestions and comments, and Jerrold Grossman for providing me with some references. The author is grateful to an anonymous referee for careful reading and making helpful recommendations that significantly improved the presentation of the paper.

## REFERENCES

[1] A. J. Cole and A. J. T. Davie. "A Game Based on the Euclidean Algorithm and a Winning Strategy for It." *Math. Gaz.* **53** (1969): 354-357.

[2] Philippe Flajolet, Brigitte Vallée, and Ilan Vardi. "Continued Fractions From Euclid to the Present Day." INRIA preprint, March 2000.

[3] Jerrold W. Grossman. "Problem #1537." *Mathematics Magazine* **70** (1997): 382.
[4] A. Ya. Khinchin. *Continued Fractions.* New York: Dover, 1997.
[5] A. J. van der Poorten. "Notes on Continued Fractions and Recurrence Sequences." *Number Theory and Cryptography* (Sydney, 1989), 86-97, London Math. Soc. Lecture Note Ser. 154, Cambridge Univ. Press, Cambridge, 1990.
[6] Richard E. Schwartz. Personal communication, 2000.
[7] Edward L. Spitznagel, Jr. "Properties of a Game Based on Euclid's Algorithm." *Mathematics Magazine* **46** (1973): 87-92.
[8] Philip D. Straffin. "A Nim-type Game, Solution to Problem #1537." *Mathematics Magazine* **71** (1998): 394-395.

AMS Classification Numbers: 91A46, 91A20, 11A55, 11A05

✠ ✠ ✠

# GENERATING FUNCTIONS, WEIGHTED AND NON-WEIGHTED SUMS FOR POWERS OF SECOND-ORDER RECURRENCE SEQUENCES

**Pantelimon Stănică** *
Auburn University Montgomery, Department of Mathematics, Montgomery, AL 36124-4023
e-mail: pstanica@mail.aum.edu
*(Submitted April 2001-Final Revision July 2002)*

## 1. INTRODUCTION

DeMoivre (1718) used the generating function (found by employing the recurrence) for the Fibonacci sequence $\sum_{i=0}^{\infty} F_i x^i = \frac{x}{1-x-x^2}$, to obtain the identities $F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}, L_n = \alpha^n + \beta^n$ (*Lucas numbers*) with $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$. These identities are called *Binet formulas*, in honor of Binet who in fact rediscovered them more than one hundred years later, in 1843 (see [6]). Reciprocally, using the Binet formulas, we can find the generating function easily $\sum_{i=0}^{\infty} F_i x^i = \frac{1}{\sqrt{5}} \sum_{i=0}^{\infty} (\alpha^i - \beta^i) x^i = \frac{1}{\sqrt{5}} \left( \frac{1}{1-\alpha x} - \frac{1}{1-\beta x} \right) = \frac{x}{1-x-x^2}$, since $\alpha\beta = -1, \alpha + \beta = 1$.

A natural question is whether we can find a closed form for the generating function for powers of Fibonacci numbers, or better yet, for powers of any second-order recurrence sequences. Carlitz [1] and Riordan [4] were unable to find the closed form for the generating functions $F(r,x)$ of $F_n^r$, but found a recurrence relation among them, namely

$$(1 - L_r x + (-1)^r x^2) F(r,x) = 1 + rx \sum_{j=1}^{[\frac{r}{2}]} (-1)^j \frac{A_{rj}}{j} F(r-2j, (-1)^j x),$$

with $A_{rj}$ having a complicated structure (see also [2]). We are able to complete the study started by them by finding a closed form for the generating function for powers of any non-degenerate second-order recurrence sequence. We would like to point out, that this "forgotten" technique we employ can be used to attack successfully other sums or series involving any second-order recurrence sequence. We also find closed forms for non-weighted partial sums for nondegenerate second-order recurrence sequences, generalizing a theorem of Horadam [3] and also weighted (by the binomial coefficients) partial sums for such sequences. Using these results we indicate how to obtain some congruences modulo powers of 5 for expressions involving Fibonacci and/or Lucas numbers.

## 2. GENERATING FUNCTIONS

We consider the general nondegenerate second-order recurrence, $U_{n+1} = aU_n + bU_{n-1}, a, b, U_0, U_1$ integers, $\delta = a^2 + 4b \neq 0$. We intend to find the generating function of

* Also associated with the Institue of Mathematics of Romanian Academy, Bucharest, Romania

powers of its terms, $U(r,x)=\sum_{i=0}^{\infty}U_i^r x^i$. It is known that the Binet formula for the sequence $U_n$ is $U_n=A\alpha^n-B\beta^n$, where $\alpha=\frac{1}{2}(a+\sqrt{a^2+4b}), \beta=\frac{1}{2}(a-\sqrt{a^2+4b})$ and $A=\frac{U_1-U_0\beta}{\alpha-\beta}, B=\frac{U_1-U_0\alpha}{\alpha-\beta}$. We associate the sequence $V_n=\alpha^n+\beta^n$, which satisfies the same recurrence, with the initial conditions $V_0=2, V_1=a$.

**Theorem 1**: *We have*

$$U(r,x)=\sum_{k=0}^{\frac{r-1}{2}}(-AB)^k\binom{r}{k}\frac{A^{r-2k}-B^{r-2k}+(-b)^k(B^{r-2k}\alpha^{r-2k}-A^{r-2k}\beta^{r-2k})x}{1-(-b)^kV_{r-2k}x-b^rx^2},$$

*if $r$ is odd, and*

$$U(r,x)=\sum_{k=0}^{\frac{r}{2}-1}(-AB)^k\binom{r}{k}\frac{B^{r-2k}+A^{r-2k}-(-b)^k(B^{r-2k}\alpha^{r-2k}+A^{r-2k}\beta^{r-2k})x}{1-(-b)^kV_{r-2k}x+b^rx^2}$$

$$+\binom{r}{\frac{r}{2}}\frac{(-AB)^{\frac{r}{2}}}{1-(-b)^{\frac{r}{2}}x},\ \textit{if } r \textit{ is even.}$$

**Proof**: We evalute

$$U(r,x)=\sum_{i=0}^{\infty}\left(\sum_{k=0}^{r}\binom{r}{k}(A\alpha^i)^k(-B\beta^i)^{r-k}\right)x^i$$

$$=\sum_{k=0}^{r}\binom{r}{k}A^k(-B)^{r-k}\sum_{i=0}^{\infty}(\alpha^k\beta^{r-k}x)^i$$

$$=\sum_{k=0}^{r}\binom{r}{k}A^k(-B)^{r-k}\frac{1}{1-\alpha^k\beta^{r-k}x}.$$

If $r$ is odd, then associating $k\leftrightarrow r-k$, we get

$$U(r,x)=\sum_{k=0}^{\frac{r-1}{2}}(-1)^k\binom{r}{k}\left(\frac{A^{r-k}B^k}{1-\alpha^{r-k}\beta^kx}-\frac{A^kB^{r-k}}{1-\alpha^k\beta^{r-k}x}\right)$$

$$=\sum_{k=0}^{\frac{r-1}{2}}(-1)^k\binom{r}{k}\frac{A^{r-k}B^k-A^kB^{r-k}+(A^kB^{r-k}\alpha^{r-k}\beta^k-A^{r-k}B^k\alpha^k\beta^{r-k})x}{1-(\alpha^k\beta^{r-k}+\alpha^{r-k}\beta^k)x+\alpha^r\beta^rx^2}$$

$$=\sum_{k=0}^{\frac{r-1}{2}}(-1)^k\binom{r}{k}\frac{A^{r-k}B^k-A^kB^{r-k}+(-b)^k(A^kB^{r-k}\alpha^{r-2k}-A^{r-k}B^k\beta^{r-2k})x}{1-(-b)^kV_{r-2k}x-b^rx^2}.$$

If $r$ is even, then associating $k \leftrightarrow r-k$, except for the middle term, we get

$$U(r,x)=\sum_{k=0}^{\frac{r}{2}-1}(-1)^k\binom{r}{k}\left(\frac{A^kB^{r-k}}{1-\alpha^k\beta^{r-k}x}+\frac{A^{r-k}B^k}{1-\alpha^{r-k}\beta^kx}\right)+\binom{r}{\frac{r}{2}}\frac{A^{\frac{r}{2}}(-B)^{\frac{r}{2}}}{1-(-b)^{\frac{r}{2}}x}$$

$$=\sum_{k=0}^{\frac{r}{2}-1}(-1)^k\binom{r}{k}\frac{A^kB^{r-k}+A^{r-k}B^k-(A^kB^{r-k}\alpha^{r-k}\beta^k+A^{r-k}B^k\alpha^k\beta^{r-k})x}{1-(\alpha^k\beta^{r-k}+\alpha^{r-k}\beta^k)x+\alpha^r\beta^rx^2}$$

$$+\binom{r}{\frac{r}{2}}\frac{(-AB)^{\frac{r}{2}}}{1-(-b)^{\frac{r}{2}}x}$$

$$=\sum_{k=0}^{\frac{r}{2}-1}(-1)^k\binom{r}{k}\frac{A^kB^{r-k}+A^{r-k}B^k-(-b)^k(A^kB^{r-k}\alpha^{r-2k}+A^{r-k}B^k\beta^{r-2k})x}{1-(-b)^kV_{r-2k}x+b^rx^2}$$

$$+\binom{r}{\frac{r}{2}}\frac{(-AB)^{\frac{r}{2}}}{1-(-b)^{\frac{r}{2}}x}.$$

If $U_0=0$, then $A=B=\frac{U_1}{\alpha-\beta}$, and in this case we can derive the following beautiful identities.

**Theorem 2**: *We have*

$$U(r,x)=A^{r-1}\sum_{k=0}^{\frac{r-1}{2}}\binom{r}{k}\frac{b^kU_{r-2k}x}{1-(-b)^kV_{r-2k}x-b^rx^2},\ \textit{if } r \textit{ is odd}$$

$$U(r,x)=A^r\sum_{k=0}^{\frac{r}{2}-1}(-1)^k\binom{r}{k}\frac{2-(-b)^kV_{r-2k}x}{1-(-b)^kV_{r-2k}x+b^rx^2}+\binom{r}{\frac{r}{2}}\frac{(-1)^{\frac{r}{2}}A^r}{1-(-b)^{\frac{r}{2}}x},\ \textit{if } r \textit{ is even.}$$

**Corollary 3**: *If $\{U_n\}_n$ is a nondegenerate second-order recurrence sequence and $U_0=0$, then*

$$U(1,x)=\frac{U_1x}{1-ax-bx^2} \tag{1}$$

$$U(2,x)=\frac{U_1^2x(1-bx)}{(bx+1)(b^2x^2-V_2x+1)} \tag{2}$$

$$U(3,x)=\frac{\delta A^2U_1x(1-2abx-b^3x^2)}{(1-V_3x-b^3x^2)(1+bV_1x-b^3x^2)}. \tag{3}$$

**Proof**: We use Theorem 2. The first two identities are straightforward. Now,

$$U(3,x) = A^2\left(\frac{U_3x}{1-V_3x-b^3x^2}+\binom{3}{1}\frac{bU_1x}{1+bV_1x-b^3x^2}\right)$$

$$= A^2x\frac{U_3+3bU_1+b(U_3V_1-3U_1V_3)x-b^3(U_3+3bU_1)x^2}{(1-V_3x-b^3x^2)(1+bV_1x-b^3x^2)}$$

$$= \frac{\delta A^2U_1x(1-2abx-b^3x^2)}{(1-V_3x-b^3x^2)(1+bV_1x-b^3x^2)},$$

since $U_3+3bU_1=(a^2+4b)U_1=\delta U_1$ and $U_3V_1-3U_1V_3=-2a\delta U_1$. $\square$

**Remark 4**: *If $U_n=F_n$, the Fibonacci sequence, then $a=b=1$, and if $U_n=P_n$, the Pell sequence, then $a=2, b=1$.*

## 3. HORADAM'S THEOREM

Horadam [3] found some closed forms for partial sums $S_n=\sum_{i=1}^n P_i$, $S_{-n}=\sum_{i=1}^n P_{-i}$, where $P_n$ is the generalized Pell sequence, $P_{n+1}=2P_n+P_{n-1}$, $P_1=p$, $P_2=q$. Let $p_n$ be the ordinary Pell sequence, with $p=1, q=2$, and $q_n$ be the sequence satisfying the same recurrence, with $p=1, q=3$. He proved

**Theorem 5 (Horadam)**: *For any $n$,*

$$\begin{aligned}
S_{4n} &= q_{2n}(pq_{2n-1}+qq_{2n})+p-q; & S_{4n-2} &= q_{2n-1}(pq_{2n-2}+qq_{2n-1})\\
S_{4n+1} &= q_{2n}(pq_{2n}+qq_{2n+1})-q; & S_{4n-1} &= q_{2n}(pq_{2n-2}+qq_{2n-1})-p\\
S_{-4n} &= q_{2n}(-pq_{2n+2}+qq_{2n+1})+3p-q; & S_{-4n+2} &= q_{2n}(-pq_{2n}+qq_{2n-1})+2p\\
S_{-4n+1} &= q_{2n}(pq_{2n+1}-qq_{2n})+p; & S_{-4n-1} &= q_{2n+1}(pq_{2n+2}-qq_{2n+1})+2p-q.
\end{aligned}$$

We observe that Horadam's theorem is a particular case of the partial sum for a non-degenerate second-order recurrence sequence $U_n$. In fact, we generalize it even more by finding $S^U_{n,r}(x)=\sum_{i=0}^n U_i^r x^i$. For simplicity, we let $U_0=0$. Thus, $U_n=A(\alpha^n-\beta^n)$ and $V_n=\alpha^n+\beta^n$. We prove

**Theorem 6**: *We have*

$$S^U_{n,r}(x)=A^{r-1}x\sum_{k=0}^{\frac{r-1}{2}}b^k\binom{r}{k}\frac{U_{r-2k}-(-b)^{kn}U_{(r-2k)(n+1)}x^n+(-b)^{r+k(n-1)}U_{(r-2k)n}x^{n+1}}{1-(-b)^kV_{r-2k}x-b^rx^2}, \quad (4)$$

*if $r$ is odd, and*

$$S^U_{n,r}(x) = A^r(-1)^{\frac{r}{2}}\binom{r}{\frac{r}{2}}\frac{(-b)^{\frac{r}{2}(n+1)}x^{n+1}-1}{(-b)^{\frac{r}{2}}x-1} + A^r\sum_{k=0}^{\frac{r}{2}-1}(-1)^k\binom{r}{k}\cdot$$
$$\frac{2-(-b)^kV_{r-2k}x-(-b)^{k(n+1)}V_{(r-2k)(n+1)}x^{n+1}+(-b)^{r+kn}V_{(r-2k)n}x^{n+2}}{1-(-b)^kV_{r-2k}x+b^rx^2}, \tag{5}$$

*if $r$ is even.*

**Proof**: We evaluate

$$\begin{aligned} S^U_{n,r}(x) &= \sum_{i=0}^{n}\sum_{k=0}^{r}\binom{r}{k}(A\alpha^i)^k(-A\beta^i)^{r-k}x^i \\ &= A^r\sum_{k=0}^{r}(-1)^{r-k}\binom{r}{k}\sum_{i=0}^{n}(\alpha^k\beta^{r-k}x)^i \\ &= A^r\sum_{k=0}^{r}(-1)^{r-k}\binom{r}{k}\frac{(\alpha^k\beta^{r-k}x)^{n+1}-1}{\alpha^k\beta^{r-k}x-1}. \end{aligned}$$

Assume $r$ is odd. Then, associating $k \leftrightarrow r-k$, we get

$$S_{n,r}^{U}(x) = A^r \sum_{k=0}^{\frac{r-1}{2}} (-1)^k \binom{r}{k} \left( \frac{(\alpha^{r-k}\beta^k x)^{n+1} - 1}{\alpha^{r-k}\beta^k x - 1} - \frac{(\alpha^k \beta^{r-k} x)^{n+1} - 1}{\alpha^k \beta^{r-k} x - 1} \right)$$

$$= A^r \sum_{k=0}^{\frac{r-1}{2}} (-1)^k \binom{r}{k} \frac{(\alpha^k\beta^{r-k}x - 1)(\alpha^{(r-k)(n+1)}\beta^{k(n+1)}x^{n+1} - 1) - (\alpha^{r-k}\beta^k x - 1)(\alpha^{k(n+1)}\beta^{(r-k)(n+1)}x^{n+1} - 1)}{(\alpha^k\beta^{r-k}x - 1)(\alpha^{r-k}\beta^k x - 1)}$$

$$= A^r \sum_{k=0}^{\frac{r-1}{2}} (-1)^k \binom{r}{k} \frac{(\alpha^{r(n+1)-kn}\beta^{r+kn}x^{n+2} - \alpha^{(r-k)(n+1)}\beta^{k(n+1)}x^{n+1} - \alpha^k\beta^{r-k}x - \alpha^{r+kn}\beta^{r(n+1)-kn}x^{n+2} + \alpha^{r-k}\beta^k x + \alpha^{k(n+1)}\beta^{(r-k)(n+1)}x^{n+1}}{1 - (-b)^k(\alpha^{r-2k} + \beta^{r-2k})x + \alpha^r\beta^r x^2}$$

$$= A^r \sum_{k=0}^{\frac{r-1}{2}} (-1)^k \binom{r}{k} \frac{(-b)^k(\alpha^{r-2k} - \beta^{r-2k})x - (-b)^{k(n+1)}(\alpha^{(r-2k)(n+1)} - \beta^{(r-2k)(n+1)})x^{n+1} + (-b)^{r+kn}(\alpha^{(r-2k)n} - \beta^{(r-2k)n})x^{n+2}}{1 - (-b)^k V_{r-2k}x - b^r x^2}$$

$$= A^{r-1} x \sum_{k=0}^{\frac{r-1}{2}} b^k \binom{r}{k} \frac{U_{r-2k} - (-b)^{kn}U_{(r-2k)(n+1)}x^n + (-b)^{r+k(n-1)}U_{(r-2k)n}x^{n+1}}{1 - (-b)^k V_{r-2k}x - b^r x^2}.$$

Assume $r$ is even. Then, as before, associating $k \leftrightarrow r-k$, except for the middle term, we get

$$S^U_{n,r}(x) = A^r \sum_{k=0}^{\frac{r}{2}-1} (-1)^k \binom{r}{k} \frac{2-(-b)^k(\alpha^{r-2k}+\beta^{r-2k})x-(-b)^{k(n+1)}(\alpha^{(r-2k)(n+1)}}{}$$

$$\frac{+\beta^{(r-2k)(n+1)})x^{n+1}+(-b)^{r+kn}(\alpha^{(r-2k)n}+\beta^{(r-2k)n})x^{n+2}}{1-(-b)^kV_{r-2k}x+b^rx^2}$$

$$+A^r(-1)^{\frac{r}{2}}\binom{r}{\frac{r}{2}}\frac{(-b)^{\frac{r}{2}(n+1)}x^{n+1}-1}{(-b)^{\frac{r}{2}}x-1}$$

$$=A^r(-1)^{\frac{r}{2}}\binom{r}{\frac{r}{2}}\frac{(-b)^{\frac{r}{2}(n+1)}x^{n+1}-1}{(-b)^{\frac{r}{2}}x-1}+A^r\sum_{k=0}^{\frac{r}{2}-1}(-1)^k\binom{r}{k}\cdot$$

$$\frac{2-(-b)^kV_{r-2k}x-(-b)^{k(n+1)}V_{(r-2k)(n+1)}x^{n+1}+(-b)^{r+kn}V_{(r-2k)n}x^{n+2}}{1-(-b)^kV_{r-2k}x+b^rx^2}. \qquad \square$$

Taking $r=1$, we get the partial sum for any nondegenerate second-order recurrence sequence, with $U_0=0$,

**Corollary 7**: $S^U_{n,1}(x)=\frac{x(U_1-U_{n+1}x^n-bU_nx^{n+1})}{1-V_1x-bx^2}$

**Remark 8**: *Horadam's theorem follows easily, since* $S_n = S^P_{n,1}(1)$. *Also* $S_{-n}$ *can be found without difficulty, by observing that* $P_{-n}=pp_{-n-2}+qp_{-n-1}=-p(-1)^{n+2}p_{n+2}-q(-1)^{n+1}p_{n+1}$, *and using* $S^p_{n,1}(-1)$.

## 4. WEIGHTED COMBINATORIAL SUMS

In [6] there are quite a few identities like $\sum_{i=0}^n \binom{n}{i}F_i = F_{2n}$, or $\sum_{i=0}^n\binom{n}{i}F_i^2$, which is $5^{[\frac{n-1}{2}]}L_n$ if $n$ is even, and $5^{[\frac{n-1}{2}]}F_n$, if $n$ is odd. A natural question is: *for fixed* $r$, *what is the closed form for the weighted sum* $\sum_{i=0}^n\binom{n}{i}F_i^r$ *(if it exists)?* We are able to answer the previous question, not only for the Fibonacci sequence, but also for any second-order recurrence sequence $U_n$, in a more general setting. Let $S_{r,n}(x)=\sum_{i=0}^n\binom{n}{i}U_i^rx^i$.

**Theorem 9**: *We have*

$$S_{r,n}(x)=\sum_{k=0}^r\binom{r}{k}A^k(-B)^{r-k}(1+\alpha^k\beta^{r-k}x)^n.$$

*Moreover, if* $U_0=0$, *then* $S_{r,n}(x)=A^r\sum_{k=0}^r(-1)^{r-k}\binom{r}{k}(1+\alpha^k\beta^{r-k}x)^n$.

**Proof**: Let

$$S_{r,n}(x) = \sum_{i=0}^{n} \binom{n}{i} \sum_{k=0}^{r} \binom{r}{k} (A\alpha^i)^k (-B\beta^i)^{r-k} x^i$$

$$= \sum_{k=0}^{r} \binom{r}{k} A^k (-B)^{r-k} \sum_{i=0}^{n} \binom{n}{i} (\alpha^k \beta^{r-k} x)^i$$

$$= \sum_{k=0}^{r} \binom{r}{k} A^k (-B)^{r-k} (1 + \alpha^k \beta^{r-k} x)^n$$

If $U_0 = 0$, then $A = B$, and $S_{r,n}(x) = A^r \sum_{k=0}^{r} (-1)^{r-k} \binom{r}{k} (1 + \alpha^k \beta^{r-k} x)^n$. □

Although we found an answer, it is not very exciting. However, by studying Theorem 9, we observe that we might be able to get nice sums involving the Fibonacci and Lucas sequences (or any such sequence, for that matter), if we are able to express 1 plus/minus a power of $\alpha, \beta$ as *the same* multiple of a power of $\alpha$, respectively $\beta$. When $U_n = F_n$, the Fibonacci sequence, the following lemma does exactly what we need.

**Lemma 10**: *The following identities are true*

$$\begin{aligned} \alpha^{2s} - (-1)^s &= \sqrt{5}\alpha^s F_s \\ \beta^{2s} - (-1)^s &= -\sqrt{5}\beta^s F_s \\ \alpha^{2s} + (-1)^s &= L_s \alpha^s \\ \beta^{2s} + (-1)^s &= L_s \beta^s. \end{aligned} \tag{6}$$

**Proof**: Straightforward using the Binet formula for $F_s$ and $L_s$. □

**Theorem 11**: *We have*

$$S_{4r+2,n}(1) = 5^{\frac{n+1}{2} - (2r+1)} \sum_{k=0}^{2r} \binom{4r+2}{k} F_{2r+1-k}^n F_{n(2r+1-k)}, \text{ if } n \text{ is odd} \tag{7}$$

$$S_{4r+2,n}(1) = 5^{\frac{n}{2} - (2r+1)} \sum_{k=0}^{2r} (-1)^k \binom{4r+2}{k} F_{2r+1-k}^n L_{n(2r+1-k)}, \text{ if } n \text{ is even} \tag{8}$$

$$S_{4r,n}(1) = 5^{-2r} \left[ \sum_{k=0}^{2r-1} (-1)^{k(n+1)} \binom{4r}{k} L_{2r-k}^n L_{(2r-k)n} + 2^n \binom{4r}{2r} \right]. \tag{9}$$

**Proof**: We use Theorem 9. Associating $k \leftrightarrow 4r+2-k$, except for the middle term in $S_{4r+2,n}(1)$, we obtain

$$S_{4r+2,n}(1) = 5^{-(2r+1)} \sum_{k=0}^{2r} (-1)^k \binom{4r+2}{k} \left[ \left(1+\alpha^k\beta^{4r+2-k}\right)^n + \left(1+\alpha^{4r+2-k}\beta^k\right)^n \right]$$

$$= 5^{-(2r+1)} \sum_{k=0}^{2r} (-1)^k \binom{4r+2}{k} \left[ \left(1+(-1)^k\beta^{4r+2-2k}\right)^n + \left(1+(-1)^k\alpha^{4r+2-2k}\right)^n \right]$$

$$= 5^{-(2r+1)} \sum_{k=0}^{2r} (-1)^{k(n+1)} \binom{4r+2}{k} \left[ \left((-1)^k+\beta^{2(2r+1-k)}\right)^n + \left((-1)^k+\alpha^{2(2r+1-k)}\right)^n \right]. \tag{10}$$

We did not insert the middle term, since it is equal to

$$5^{-(2r+1)}(-1)^{2r+1}\binom{4r+2}{2r+1}(1+\alpha^{2r+1}\beta^{2r+1})^n$$

$$= 5^{-(2r+1)}(-1)^{2r+1}\binom{4r+2}{2r+1}(1+(-1)^{2r+1})^n = 0.$$

In (10), using (6), and observing that $\alpha^{2(2r+1-k)} + (-1)^k = \alpha^{2(2r+1-k)} - (-1)^{2r+1-k}$, we get

$$S_{4r+2,n}(1) = 5^{-(2r+1)} \sum_{k=0}^{2r} (-1)^{(n+1)k} \binom{4r+2}{k} 5^{\frac{n}{2}} F_{2r+1-k}^n \left((-1)^n\beta^{n(2r+1-k)} + \alpha^{n(2r+1-k)}\right).$$

Therefore, if $n$ is odd, then

$$S_{4r+2,n}(1) = 5^{-(2r+1)} \sum_{k=0}^{2r} \binom{4r+2}{k} 5^{\frac{n+1}{2}} F_{2r+1-k}^n F_{n(2r+1-k)}$$

and, if $n$ is even, then

$$S_{4r+2,n}(1) = 5^{-(2r+1)} \sum_{k=0}^{2r} (-1)^k \binom{4r+2}{k} 5^{\frac{n}{2}} F_{2r+1-k}^n L_{n(2r+1-k)}.$$

In the same way, associating $k \leftrightarrow 4r - k$, except for the middle term, and using Lemma 10, we get

$$S_{4r,n}(1) = 5^{-2r} \sum_{k=0}^{2r-1} (-1)^k \binom{4r}{k} \left[\left(1 + \alpha^k \beta^{4r-k}\right)^n + \left(1 + \alpha^{4r-k} \beta^k\right)^n\right] + 5^{-2r} 2^n \binom{4r}{2r}$$

$$= 5^{-2r} \sum_{k=0}^{2r-1} (-1)^{k(n+1)} \binom{4r}{k} \left[\left((-1)^k + \beta^{2(2r-k)}\right)^n + \left((-1)^k + \alpha^{2(2r-k)}\right)^n\right]$$

$$+ 5^{-2r} 2^n \binom{4r}{2r} \tag{11}$$

$$= 5^{-2r} \left[\sum_{k=0}^{2r-1} (-1)^{k(n+1)} \binom{4r}{k} \left(L_{2r-k}^n \beta^{(2r-k)n} + L_{2r-k}^n \alpha^{(2r-k)n}\right) + 2^n \binom{4r}{2r}\right]$$

$$= 5^{-2r} \left[\sum_{k=0}^{2r-1} (-1)^{k(n+1)} \binom{4r}{k} L_{2r-k}^n L_{(2r-k)n} + 2^n \binom{4r}{2r}\right]. \quad \square$$

**Remark 12**: *In the same manner we can find* $\sum_{i=0}^n \binom{n}{i} U_{pi}^r x^i$.

We now list some interesting special cases of Theorems 9 and 11.

**Corollary 13**: *We have*

$$\sum_{i=0}^{n} \binom{n}{i} F_i = F_{2n}$$

$$\sum_{i=0}^{2n} \binom{2n}{i} F_i^2 = 5^{n-1} L_{2n}$$

$$\sum_{i=0}^{2n+1} \binom{2n+1}{i} F_i^2 = 5^n F_{2n+1}$$

$$\sum_{i=0}^{n} \binom{n}{i} F_i^3 = \frac{1}{5}(2^n F_{2n} + 3F_n)$$

$$\sum_{i=0}^{n} \binom{n}{i} F_i^4 = \frac{1}{25}(3^n L_{2n} - 4(-1)^n L_n + 6 \cdot 2^n).$$

**Proof**: The second, third and fifth identities follow from Theorem 11. Now, using Theorem 9, with $A = \frac{1}{\sqrt{5}}$, we get

$$S_{1,n}(1) = \frac{1}{\sqrt{5}} \sum_{k=0}^{1} (-1)^{1-k} \binom{1}{k} (1 + \alpha^k \beta^{1-k})^n$$

$$= \frac{1}{\sqrt{5}} (-(1+\beta)^n + (1+\alpha)^n) = \frac{1}{\sqrt{5}} (\alpha^{2n} - \beta^{2n}) = F_{2n}.$$

Next, the fourth identity follows from

$$S_{3,n}(1) = \frac{1}{5\sqrt{5}} \sum_{k=0}^{3} (-1)^{3-k} \binom{3}{k} (1 + \alpha^k \beta^{3-k})^n$$

$$= \frac{1}{5\sqrt{5}} [-(1+\beta^3)^n + 3(1+\alpha\beta^2)^n - 3(1+\alpha^2\beta)^n + (1+\alpha^3)^n]$$

$$= \frac{1}{5\sqrt{5}} [-(2\beta^2)^n + 3\alpha^n - 3\beta^n + (2\alpha^2)^n] = \frac{1}{5}(2^n F_{2n} + 3F_n),$$

since $1 + \beta^3 = 2\beta^2$, $1 + \alpha^3 = 2\alpha^2$. $\square$

The results in our next theorem are obtained by putting $x = -1$ in Theorem 9, and since the proofs are similar to the proofs in Theorem 11, we omit them.

**Theorem 14**: *We have*

$$S_{4r,n}(-1) = 5^{\frac{n}{2}-2r} \sum_{k=0}^{2r-1} (-1)^k \binom{4r}{k} F_{2r-k}^n L_{(2r-k)n}, \text{ if } n \text{ is even},$$

$$S_{4r,n}(-1) = -5^{\frac{n+1}{2}-2r} \sum_{k=0}^{2r-1} \binom{4r}{k} F_{2r-k}^n F_{(2r-k)n}, \text{ if } n \text{ is odd},$$

$$S_{4r+2,n}(-1) = 5^{-(2r+1)} \left[ \sum_{k=0}^{2r} (-1)^{k(n+1)+n} \binom{4r+2}{k} L_{2r+1-k}^n L_{(2r+1-k)n} - 2^n \binom{4r+2}{2r+1} \right].$$

Next we record some interesting special cases of Theorem 9 and 14.

**Corollary 15**: *We have*

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}F_i = -F_n$$

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}F_i^2 = \frac{1}{5}((-1)^n L_n - 2^{n+1})$$

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}F_i^3 = \frac{1}{5}((-2)^n F_n - 3F_{2n})$$

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}F_i^4 = 5^{\frac{n-4}{2}}(L_{2n} - 4L_n), \text{ if } n \text{ is even}$$

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}F_i^4 = -5^{\frac{n-3}{2}}(F_{2n} + 4F_n), \text{ if } n \text{ is odd.}$$

**Proof**: The first identity is a simple application of Theorem 9. The identities for even powers are immediate consequences of Theorem 14. Now, using Theorem 9, we get

$$S_{3,n}(-1) = \frac{1}{5\sqrt{5}}(-(1-\beta^3)^n + 3(1-\alpha\beta^2)^n - 3(1-\alpha^2\beta)^n + (1-\alpha^3)^n)$$

$$= \frac{1}{5\sqrt{5}}(-(-2)^n\beta^n + 3\beta^{2n} - 3\alpha^{2n} + (-2)^n\alpha^n) = \frac{1}{5}((-2)^n F_n - 3F_{2n}),$$

since $1-\beta^3 = -2\beta$, $1-\alpha^3 = -2\alpha$. □

From (9) we obtain, for $r \geq 1$,

$$\sum_{k=0}^{2r-1}(-1)^{k(n+1)}\binom{4r}{k}L_{2r-k}^n L_{(2r-k)n} + 2^n\binom{4r}{2r} \equiv 0 \pmod{5^{2r}}.$$

Similar congruence results follow from other sums in Section 4, and we leave these for the reader to formulate.

## ACKNOWLEDGMENTS

The author would like to thank the anonymous referee for her/his helpful and very detailed comments, which improved significantly the presentation of the paper.

## REFERENCES

[1] L. Carlitz. "Generating Functions for Powers of Certain Sequences of Numbers." *Duke Math. J.* **29** (1962): 521-537.

[2] A.F. Horadam. "Generating Function for Powers of a Certain Generalized Sequence of Numbers." *Duke Math. J.* **32** (1965): 437-446.

[3] A.F. Horadam. "Partial Sums for Second-Order Recurrence Sequences." *The Fibonacci Quarterly* **32.3** (1994): 429-440.

[4] J. Riordan. "Generating Functions for Powers of Fibonacci Numbers." *Duke Math. J.* **29** (1962): 5-12.

[5] M. Rumney, E.J.F. Primrose. "Relations Between a Sequence of Fibonacci Type and a Sequence of Its Partial Sums." *The Fibonacci Quarterly* **9.3** (1971): 296-298.

[6] S. Vajda. *Fibonacci & Lucas Number and the Golden Section - Theory and Applications*, John Wiley & Sons, 1989.

AMS Classification Numbers: 11B37, 11B39, 05A10, 05A19

✠ ✠ ✠

# SOME COMMENTS ON BAILLIE-PSW PSEUDOPRIMES

**Zhuo Chen**
Department of Mathematics and Statistics,
University of Minnesota, Duluth, Duluth, MN 55812

**John Greene**
Department of Mathematics and Statistics,
University of Minnesota, Duluth, Duluth, MN 55812
*(Submitted April 2001-Final Revision July 2001)*

## 1. INTRODUCTION

In [2], Pomerance, Selfridge and Wagstaff offered \$30 for a number $n$ which is simultaneously a strong base 2-pseudoprime and a Lucas pseudoprime (with a discriminant specified in [2]). Since there is no known composite number that meets this criteria, even if the first condition is weakened to requiring only that $n$ be a base 2-pseudoprime, it was suggested that this might be a reasonable test for "primality" which, though fallible, might be more reliable than current tests. Indeed since their article was published, both Mathematica and Maple have switched to some variation on this method.

In [3], an unpublished manuscript by Carl Pomerance (available on Jon Grantham's web site, www.pseudoprime.com/pseudo.html), Baillie is credited with first proposing such a combination test. In [2], Pomerance, Selfridge and Wagstaff show that there are no counterexamples less then $20 \cdot 10^9$. Subsequently, a composite number which is both a base 2-pseudoprime and a Lucas pseudoprime has been referred to as a Baillie-PSW pseudoprime.

Pomerance [3] gave a heuristic argument to show that there should be infinitely many such numbers. In fact, his argument suggest that for any $\varepsilon > 0$, the number of Baillie-PSW pseudoprimes $< x$ should exceed $x^{1-\varepsilon}$ for $x$ sufficiently large depending on the choice of $\varepsilon$.

With time, the prize for such a number, $n$ has grown to \$620, and the conditions have been relaxed to the following [4]:

1) $2^n \equiv (\text{mod } n)$,
2) $F_{n+1} \equiv (\text{mod } n)$
3) $n \equiv 2$ or $3 (\text{mod } 5)$,
4) $n$ is composite (with explicit factorization provided).

In this paper, we present calculations related to the construction of Baillie-PSW pseudoprimes. We use a variation of the method Pomerance described. It should be pointed out that we have no example of such a number, although we are certain we could construct one if only we could search through a rather large space in which such an example will live.

## 2. PRELIMINARIES

The following are elementary facts related to base 2-pseudoprimes and Fibonacci pseudoprimes. These facts can be found in many books on factoring, cryptography or primality. For example, see [1 Sec. 10.14], [5, Chap. 2 Sec IV], or [6, pp. 107-115].

For each odd number $n > 1$, there is an integer $h > 0$ such that

$$\begin{array}{ll} 1) & 2^h \equiv 1 (\text{mod } n), \\ 2) & \text{if } 2^m \equiv 1 (\text{mod } n) \text{ then } h|m. \end{array}$$

This number $h$ is called the order of 2 modulo $n$ and is denoted $\text{ord}_n(2)$. Since $2^{\phi(n)} \equiv 1$ (mod $n$), it follows that $h|\phi(n)$. Similarly, for each odd number $n > 1$ there is a positive integer $k$ such that

$$\begin{array}{ll} 1) & F_k \equiv 0 (\text{mod } n), \\ 2) & \text{if } F_m \equiv 0 (\text{mod } n) \text{ then } k|m. \end{array}$$

We are unaware of a standard notation for this index $k$. We refer to it as the Fibonacci order of $n$ and denote it by $\text{ord}_f(n)$.

A composite number, $n$, is called a base 2-pseudoprime if $2^{n-1} \equiv 1 (\text{mod } n)$. This happens if and only if $\text{ord}_n(2)$ is a divisor of $n - 1$. For primes $p$, $F_{p-\left(\frac{5}{p}\right)} \equiv 0 (\text{mod } p)$. If for an odd composite number $n$, $F_{n-\left(\frac{5}{n}\right)} \equiv 0 (\text{mod } n)$, we call $n$ a Fibonacci pseudoprime. This happens if and only if $\text{ord}_f(n)$ is a divisor of $n - \left(\frac{5}{n}\right)$.

The following are obvious sufficient conditions for $n$ to be a base 2-pseudoprime or a Fibonacci pseudoprime: Suppose that $n$ is an odd, square free composite number.

$$\begin{array}{l} \text{If for each prime } p|n, \text{ord}_p(2) \text{divides } n - 1 \\ \text{then } n \text{ is a base 2-pseudoprime.} \end{array} \tag{2.1}$$

$$\text{If for each prime } p|n, \text{ord}_f(p) \text{divides } n - \left(\frac{5}{n}\right)$$

$$\text{then } n \text{ is a Fibonacci pseudoprime.} \tag{2.2}$$

As we mentioned in the introduction, Pomerance, Selfridge and Wagstaff offer \$620 for an example of a number $n \equiv 2$ or 3 (mod 5) such that $n$ is both a base 2-pseudoprime and a Fibonacci pseudoprime. In this case, $n - \left(\frac{5}{n}\right) = n + 1$.

Here is a variation on Pomerance's method for searching for such a number: Let $M$ and $N$ be two highly composite numbers with $\text{GCD}(M, N) = 2$. Let $P$ be the set of all primes $p$ with the following properties:

$$\begin{array}{ll} 1) & p \text{ does not divide } MN, \\ 2) & \text{ord}_p(2) \text{ divides } M, \\ 3) & \text{ord}_f(p) \text{ divides } N. \end{array}$$

Define a function $f$ on the subsets of $P$ as follows:

$$f(A) = \prod_{p \in A} p.$$

If a subset, $A$, of $P$ with cardinality at least 2 can be found such that

$$f(A) \equiv 2 \text{ or } 3 (\text{mod } 5),$$

$$f(A) \equiv 1 (\text{mod } M), \text{ and } f(A) \equiv -1 (\text{mod } N),$$

then as an easy consequence of (2.1) and (2.2), $f(A)$ will be a Baillie-PSW pseudoprime. If $P$ is a large set compared with $MN$, then we expect lots of subsets $A$ to exist. That is, assuming that the congruence classes of $f(A)$ are roughly uniformly distributed modulo $M$ and $N$, one might expect

$$\frac{2^{|P|}}{\phi(MN)} \tag{2.3}$$

subsets $A$ to have the desired properties.

In addition to Pomerance's manuscript, Grantham's site also contains a list of 2030 primes, constructed by Grantham and Red Alford. Grantham comments that he and Alford "highly suspect" that some subset product of these primes is a Baillie-PSW pseudoprime. The site does not give reasons. However, an analysis of the primes shows that each has the property that $p-1$ divides $M$ and $p+1$ divides $N$, where $M = 2(13)^2(17)^2(29)^2(37)^2(41)^2(53)^2(61)\ldots(1249)$ and $N = 2^2(3)^7(7)^4(11)^3(19)^2(23)^2(31)^2(43)^2(47)^2(59)^2(67)^2(71)\ldots(1187)$. Here, the only odd primes dividing $M$ are congruent to 1 (mod 4) and the only odd primes dividing $N$ are those congruent to 3(mod 4). In each case, there are exactly 100 such primes. For this choice of $M$ and $N$, $\phi(MN) \cong 1.017659177 \times 10^{545} < 2^{1811}$. The problem, of course, is that a space of size $2^{2030}$ is hard to search even if one expects $2^{219}$ examples.

This current investigation began as a Master's project for the first author. The project was to look for much smaller numbers $M$ and $N$ for which $\frac{2^{|P|}}{\phi(MN)} > 1$. It was thought that using $\text{ord}_p(2)$ and $\text{ord}_f(p)$ instead of $p-1$ and $p+1$ would significantly reduce the size of $M$ and $N$. We performed our calculations using five Pentium III PC's and three Apple PowerMac's. We used C/C++ on the PC's, employing only single precision arithmetic (but with 64 bit integers.) On the PowerMac's, we used Maple $V^{TM}$.

## 3. RESULTS WITHOUT USING ORD$_p(2)$ OR ORD$_f(p)$.

Based on the primes of Grantham's site and their implied numbers $M$ and $N$, we searched for smaller $M$ and $N$ as follows. We attempted to partition the small primes between $M$ and $N$ a bit more evenly. We began with intial values

$$M_{\text{start}} = 2(7)^4(13)^2(19)^2(23)^2(31)^2(43)^2(47)^2(59)^2(67)^2,$$

$$N_{\text{start}} = (2)^6(3)^6(11)^3(17)^2(29)^2(37)^2(41)^2(53)^2.$$

We put the powers of 2 and 3 in $N_{\text{start}}$ because it was thought that this would be advantageouos when we considered $\text{ord}_p(2)$, as discussed in the next section. We chose to favor $\text{ord}_p(2)$ over $\text{ord}_f(p)$ because it was quicker to calculate $\text{ord}_p(2)$ than $\text{ord}_f(p)$. For a given value of $n$, we then construct an

$$M_{\text{tail}} = \text{ product of } n-9 \text{ primes, all congruent to } 3(\text{mod } 4),$$

$$N_{\text{tail}} = \text{ product of } n-7 \text{ primes, all congruent to } 1(\text{mod } 4).$$

We set $M = M_{\text{start}}M_{\text{tail}}$ and $N = 4N_{\text{start}}N_{\text{tail}}$. Thus, $M$ and $N$ are each divisible by exactly $n$ odd primes. Next, we constructed the set

$$N_{\text{init}} = \{a : a \text{ is a divisor of } N_{\text{start}}\}$$

of all divisors of $N_{\text{start}}$. This set contains 47,628 elements. For each $k$, let

$$N_k = \{x : x \text{ is a divisor of } N_{\text{tail}} \text{ and } x \text{ has } k \text{ prime divisors}\}.$$

This set has $\binom{n-7}{k}$ elements. If $g(x,y) = 4xy - 1$, with $x \in N_{\text{init}}$ and $y \in N_k$ (setting $y = 1$ if $k = 0$), then $g(x,y) + 1$ is a divisor of $N$ with exactly $k$ prime divisors in common with $N_{\text{tail}}$. We proceed as follows: As $k$ increases from 0, for each $x$ in $N_{\text{init}}$ and $y$ in $N_k$, determine if $g(x,y) - 1$ is a divisor of $M$. If so, test if $g(x,y)$ is prime. If it is, add $g(x,y)$ to the list of pirmes in $P_k$. At the end, we construct the set $P = \cup_k P_k$. Technically, we should delete any primes $p|MN$ from the list. In the following tables, we have not done this. However, this will not affect our results since the number of such primes is small compared to the size of $P$.

Our first table gives the number of primes found for various values of $n, k$:

| k\n | 10 | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 7 | 9 | 19 | 19 | 24 | 27 | 30 | 32 | 33 | 34 |
| 1 | 1 | 8 | 21 | 40 | 60 | 91 | 123 | 151 | 194 | 224 |
| 2 | 0 | 1 | 10 | 37 | 72 | 119 | 201 | 295 | 416 | 568 |
| 3 | 0 | 0 | 9 | 24 | 58 | 123 | 203 | 342 | 565 | 850 |
| 4 | 0 | 0 | 0 | 5 | 26 | 66 | 122 | 236 | 380 | 528 |
| 5 | 0 | 0 | 0 | 2 | 6 | 13 | 47 | 91 | | |
| 6 | 0 | 0 | 0 | 0 | 0 | 3 | 7 | | | |
| total | 8 | 18 | 59 | 127 | 246 | 442 | 733 | 1147 | 1588 | 2204 |
| needed | 192 | 332 | 490 | 660 | 838 | 1023 | 1214 | 1410 | 1610 | 1813 |

Table 3.1

Some comments on this table: the empty entries indicate computations we did not undertake (there are about 37 million calculations needed for each element of $N_{\text{start}}$ for entry (90,5), for example. Our construction ensures that each $P_k = P_k(n)$ satisfies $P_k(m) \subseteq P_k(n)$ if $m \leq n$. Thus, we know that we will find at least 91 primes for entry $n = 90, k = 5$. Hence, by $n = 90$, the number of primes in $P$ grows past the expected number needed to cover all reduced residue classes. It should also be pointed out that the counts are not complete for the larger numbers $n$: we sped up calculations by using only the smallest entries from $N_{\text{init}}$. Based on numerical evidence, this missed some but not many primes. An interesting feature to the table is that although Alford's and Grantham's $M$ and $N$ seemed very contrived in that each was divisible by exactly 100 odd primes, it appears that they could not have decreased the number of primes by much.

We analyzed our data as follows. A number is called $z$-smooth if all its prime divisors are less than $z$. Riesel [6, page 164] gives a crude estimate of $u^{-u}x^u$ for the number of $x$-smooth numbers less than $x^u$. He indicates that this estimate is often good enough to approximate the run time of computer algorithms which make use of smooth numbers. We are seeking primes such that $p-1$ and $p+1$ are both $z$-smooth with respect to some $z$, and which also have factors from prescribed sets of primes. If one has a set of primes with asymptotic density $1/2$, then Riesel's argument leads to an estimate of $(2u)^{-u}x^u$ numbers less than $x^u$ which are $x$-smooth and have all their prime divisors from that prescribed set.

We use the following model: Given two disjoint sets of $n$ primes; $p_1, p_2, \ldots, p_n$, and $q_1, q_2, \ldots, q_n$ with all the $p$'s and $q$'s of about the same size, we select $j$ of the primes from the $q$-list, multiply them together to get an $m$. We ask that $4m-1$ be prime and $4m-2$ factor over the $p$'s. In fact, what we really need is for $2m-1$ to factor over the $p$'s. In this case, $x^u \cong 2q_n^j$ and $x = p_n \cong q_n$. This gives

$$u \cong \frac{\ln 2 + j \ln q_n}{\ln q_n} = j + \frac{\ln 2}{\ln q_n} = j + \alpha,$$

where $\alpha = \ln(2)/\ln(q_n)$. Thus, the rough probability that $4m-2$ is smooth with factors dividing $M$ is $(2j+2\alpha)^{-j-\alpha}$. We also require that $4m-1$ be prime, which happens with expected probability $\frac{2}{\ln(4m-1)}$. Thus, our estimate of the probability that a number of this form meet our requirements is $\frac{2(2u)^{-u}}{\ln(4q_n^j)}$, where $u = j + \frac{\ln 2}{\ln q_n}$. The expected number of primes of this form is $\frac{2(2u)^{-u}}{\ln(4q_n^j)}\binom{n}{j}$.

Obviously, our primes differ dramatically in size. Moreover, our numbers need more than smoothness – there are limits on the divisibility of our numbers by small primes. However, this model is still useful for making predictions and understanding overall patterns. For example, using $\binom{n}{j} \cong \frac{n^j}{j!} \cong \frac{n^j e^j}{\sqrt{2\pi j}\, j^j}$, we have

$$\frac{2(2u)^{-u}}{\ln(4q_n^j)}\binom{n}{j} \cong \frac{2^{1-u}u^{-u}n^j e^j}{\ln(4q_n^j)\sqrt{2\pi j}\, j^j}.$$

If we ignore the difference between $j$ and $u$, this expression is approximately

$$\frac{2}{\ln(4q_n^j)\sqrt{2\pi j}}\left(\frac{en}{2j^2}\right)^j. \tag{3.1}$$

Thus, we expect no primes to be contributed by the cases where $j > \sqrt{en/2}$. For example looking at Table 3.1, when $n = 50$, we expect no primes for $k \geq 8$. In fact, we got none for $k = 6$ or 7 either. If we trust (3.1) to give good estimates of the numbers of primes for various $k$ in Table 3.1, then for $k = 6$, we should have found $.37 \cong 0$ primes. In fact, we do not trust (3.1) for more than a crude analysis. For example, it predicts 1.59 primes for $n = 50, k = 5$ rather than the 6 we found, and it predicts 4.8 primes for $k = 4$ rather than our 26.

Suppose we accept $\frac{2(2u)^{-u}}{\ln(4q_n^j)}$ as a rough probability that a prime $g(x,y)$ has the desired properties, where $g(x,y) - 1$ has $j$ prime divisors. For each entry $(n,k)$ in Table 3.1, we solved the equation

$$\frac{\#\text{ of primes found}}{\#\text{ of cases looked at}} = \frac{2(2u)^{-u}}{\ln(4q_n^j)} \tag{3.2}$$

for $j$, where $q_n$ is the largest prime divisor of $MN$. We take this "$j$" to be some kind of average number of prime factors. The results are recorded in the table below.

| k\n | 10 | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 3.32 | 3.21 | 2.96 | 2.95 | 2.87 | 2.82 | 2.78 | 2.76 | 2.75 | 2.73 |
| 1 | 4.24 | 4.03 | 3.90 | 3.81 | 3.76 | 3.69 | 3.64 | 3.62 | 3.58 | 3.57 |
| 2 | - | 5.16 | 4.82 | 4.65 | 4.60 | 4.57 | 4.52 | 4.49 | 4.46 | 4.44 |
| 3 | - | - | 5.40 | 5.44 | 5.41 | 5.37 | 5.37 | 5.35 | 5.32 | 5.30 |
| 4 | - | - | - | 6.42 | 6.26 | 6.24 | 6.26 | 6.24 | 6.25 | 6.29 |
| 5 | - | - | - | 7.13 | 7.20 | 7.28 | 7.17 | | | |

Table 3.2

We did not compute values for $k = 6, n = 60$, 70 because we only did partial searches with $k = 6$. We ignored $n = 80, k = 5$ for the same reason. Based on the table, we expect the (5,90) entry to be roughly 7.2. We may use this to estimate the number of primes found for $k = 5, n = 90$. The result is that we expect some 171 primes in this case. Similarly, we expect maybe 46 primes when $k = 6$ (using $j = 8.2$) so that $k$ from 0 to 6, we expect a total of 1805 primes when $n = 90$.

This table may be used to interpolate back to the point where the number of primes exactly matches the minimum number needed to cover all reduced residue classes. This point will be between $n = 80$ and $n = 90$. If we are cautious and use only $k = 0, \ldots, 6$ and $j$-values: 2.76, 3.62, 4.49, 5.34, 6.25, 7.20, 8.20, then the matching point occurs at $n = 88$. Using the most optimistic numbers for $j$ reduces this to $n = 85$.

## 4. THE EFFECT OF USING ORD$_p(2)$ OR ORD$_f(p)$

How much does it help to ask only that $\text{ord}_p(2)$ divide $M$ rather than that $p-1$ divide $M$? Here is one model. Let $M' = 2^4(3^3)(11^2)(17)(29)M$ and search for primes as in Section 3, but for which $p-1$ divides $M'$. Include $p$ in $P$ if $2^M \equiv 1 \pmod{p}$. The only additional primes picked up this way are primes in which $p-1$ does not divide $M$, but $p-1$ divides $M'$ and $\mathrm{ord}_p(2)$ divides $M$. We expect that $p-1$ will have exactly one factor of 11 in $\frac{10}{11^2}$ cases, and that this factor will not divide $\mathrm{ord}_p(2)$ in $\frac{1}{11}$ of those cases. Similarly, exactly two factors of 11 should occur in $\frac{10}{11^3}$ cases, with both factors dropping out $\frac{1}{11^2}$ of the time. Thus, the 11's should increase the count by a factor of $(1+\frac{10}{11^3}+\frac{10}{11^5})$. Arguing likewise for the other divisors $M'/M$ gives a multiplier of

$$\left(1+\frac{1}{8}+\frac{1}{32}+\frac{1}{128}+\frac{1}{512}\right)\left(1+\frac{2}{27}+\frac{2}{243}+\frac{2}{2187}\right)$$

$$\left(1+\frac{10}{1331}+\frac{10}{11^5}\right)\left(1+\frac{16}{17^3}\right)\left(1+\frac{28}{29^3}\right)\cong 1.278.$$

As can be seen, it is the smaller primes that contribute most to this number. This is why we chose to make $N$ divisibile by both powers of 2 and powers of 3. In Table 4.1, we give the actual numbers of primes found for various $n, k$ for which $p-1$ divides $M'$, $\mathrm{ord}_p(2)$ divides $M$, and $p+1$ divides $N$.

| k\n | 10 | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 9 | 11 | 23 | 24 | 30 | 33 | 35 | 39 | 40 | 42 |
| 1 | 2 | 10 | 28 | 55 | 77 | 112 | 151 | 183 | 233 | 268 |
| 2 | 0 | 1 | 19 | 57 | 103 | 173 | 285 | 415 | 580 | 780 |
| 3 | 0 | 0 | 9 | 30 | 71 | 171 | 274 | 472 | 762 | 1144 |
| 4 | 0 | 0 | 0 | 9 | 35 | 91 | 190 | 359 | 564 | 736 |
| 5 | 0 | 0 | 0 | 2 | 8 | 20 | 70 | 134 | | |
| 6 | 0 | 0 | 0 | 0 | 0 | 4 | 10 | | | |
| total | 11 | 22 | 79 | 177 | 324 | 604 | 1015 | 1602 | 2179 | 2970 |
| ratio | 1.38 | 1.22 | 1.34 | 1.39 | 1.32 | 1.37 | 1.38 | 1.39 | 1.37 | 1.35 |
| needed | 192 | 332 | 490 | 660 | 838 | 1023 | 1214 | 1410 | 1610 | 1813 |

Table 4.1

In the table, the actual multiplier (the ratio row) appears to be somewhat higher, closer to 1.37 with the data looked at so far. We do not have an explanation for this discrepancy.

Given the data above, it is natural to ask how low $n$ can be and still have a sufficiently large number of primes to expect to cover the reduced residue classes of $MN$. According to the table, this happens by $n=80$. We estimated the number of primes with $n=75$ as follows: using the formula

$$\frac{\#\text{ of primes found}}{\#\text{ of cases looked at}}=\frac{2(2u)^{-u}}{\ln(4q_n^j)}$$

and solve for $j$ with the data from $n = 70$ and $n = 80$ in table 4.1 (admittedly a questionable thing to do) we interpolated to get estimated values of $j$ for $n = 75$. Here are our results:

| n\k | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 70 | 2.734 | 3.580 | 4.417 | 5.291 | 6.140 | 7.066 | | |
| 75 | 2.715 | 3.572 | 4.404 | 5.277 | 6.134 | 7.066 | 8.016 | 8.966 |
| 80 | 2.695 | 3.563 | 4.391 | 5.262 | 6.128 | | | |

Table 4.2

The row for $n = 75$ was obtained by averaging the results from 70 and 80, but rounding up to three decimal places. However, the prime list for $n = 80, k = 5$ was incomplete, so we used the value from $n = 70, k = 5$ for this entry. We estimated the entries for $k = 6$ and $k = 7$ by adding .95 to the previous entries. Based on this table, when $n = 75$, we should expect to find the following numbers of primes:

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | total | needed |
|---|---|---|---|---|---|---|---|---|---|
| 37 | 165 | 344 | 360 | 263 | 103 | 28 | 6 | 1306 | 1311 |

Table 4.3

Since we were conservative in our estimates for $k = 5, 6, 7$, we decided to actually carry out the computer search for primes. We were lucky to exceed expectations. Here is our actual count of primes found for $n = 75$.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | total | needed |
|---|---|---|---|---|---|---|---|---|---|
| 35 | 165 | 349 | 356 | 279 | 116 | 25 | 1 | 1326 | 1311 |

Table 4.4

Of the total, six primes are divisors of $MN$, leaving a set $P$ with 1320 elements. Thus, we expect a Baillie-PSW pseudoprime to exist at this level. Since we did not complete counts for $k = 6, 7$, it is remotely possible that there are enough primes at $n = 74$ as well.

Introducing the Fibonacci order with our $M$ and $N$ might be expected to have the following effect: Supposing we use an $N' = N(7)^3(13)^2(19)(23)$. We would then expect

$$\left(1 + \frac{1}{1024}\right)\left(1 + \frac{6}{7^3} + \frac{6}{7^7} + \frac{6}{7^7}\right)\left(1 + \frac{12}{13^3} + \frac{12}{13^5}\right)\left(1 + \frac{18}{19^3}\right)\left(1 + \frac{22}{23^3}\right) \cong 1.027$$

times as many primes. In particular, for $n = 70, (1022)(1.027) \cong 1050$, still far short of the 1214 needed in this case. In actual calculations, we again appear to beat this estimate, picking up at least 40 additional primes for $k$ between 0 and 3. However, we estimate fewer than 40 primes remain to be found, leaving us more than 100 short of our goal.

## 5. THE QUEST FOR $n = 70$

Given that we could find enough primes in our set $P$ with $n = 75$, which corresponds to 75 odd primes dividing each of $M$ and $N$, we attempted to push the computational limits of our computers to try to reduce this to $n = 70$. There are several ways to change the way $M$ and $N$ are constructed to try to increase the size of $P$. We have put powers of 2 and 3 in $N$ so as to favor the existence of primes with $\text{ord}_p(2)$ dividing $M$ over $\text{ord}_f(p)$ dividing $N$. Suppose we are a bit more equitable, and start with, say,

$$M_{\text{start}} = 2(3)^6(11)^3(17)^2(23)^2(31)^2(41)^2(47)^2(59)^2,$$

$$N_{\text{start}} = (2)^6(7)^4(13)^2(19)^2(29)^2(37)^2(43)^2(53)^2(61)^2.$$

One might expect this change to produce slightly more primes with $p-1|M, p+1|N$, decrease the number of primes added using $\text{ord}_p(2)$, but increase the number of primes added using $\text{ord}_f(p)$. In fact, for reasons we do not understand, this change slightly decreased the number of primes $p$ with $p-1|M, p+1|N$. The increase in the number of primes added using $\text{ord}_f(p)$ did not offset this decrease.

We only calculated these numbers for $0 \leq k \leq 4$. It is possible that things would improve for higher values of $k$. We considered it very unlikely, however, that searching higher $k$ would yield enough additional primes to make a real difference. This being the case, we went back to our original set up, but increased the multiplicity of the smaller prime divisors of $M$ and $N$. This increased the size of $P$, but also increased $\phi(MN)$, meaning that it increased the number of primes needed. We finally succeeded in obtaining enough primes with

$$M_{\text{start}} = 2(7)^5(13)^3(19)^3(23)^2(31)^2(43)^2(47)^2(59)^2(67)^2,$$

$$N_{\text{start}} = (2)^{12}(3)^8(11)^3(17)^3(29)^2(37)^2(41)^2(53)^2,$$

and $M_{\text{tail}}$ and $N_{\text{tail}}$ as before. That is, $M_{\text{tail}} = (71)(79)\ldots(787)$, a product of 66 primes all congruent to 3(mod 4), and $N_{\text{tail}} = (61)(73)\ldots(829)$, a product of 68 primes all congruent to 1 (mod 4). In this case, we obtained the following table:

| k | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | total |
|---|---|---|---|---|---|---|---|---|---|
| p-1/p+1 | 30 | 137 | 232 | 242 | 137 | 51 | 7 | 1 | 837 |
| $\text{ord}_p(2)$ | 6 | 37 | 108 | 88 | 79 | 27 | 3 | | 348 |
| $\text{ord}_f(\text{p})$ | 0 | 6 | 17 | 21 | 9 | 4 | | | 57 |
| total | 36 | 180 | 357 | 351 | 225 | 82 | 10 | 1 | 1242 |

Table 5.1

The needed number of primes increased from the original 1214 to 1240. Thus, $2^{|P|}$ is only about four times as big as $\phi(MN)$. We only did partial searches with $k = 4, 5$ for primes satisfying $\text{ord}_f(p)|N$, and we suspect that there are more primes to find. Also, we were using only single precision arithmetic in our search on PC's (using 64-bit numbers, however) and at $k = 6, 7$ we were hampered by integer overflow problems, so we expect a few more primes here as well. Thus, we are confident that there is a Baillie-PSW pseudoprime to be found using this $M$ and $N$.

It would be hard to push these calculations down to $n = 69$. The largest primes dividing $M$ and $N$ are 787 and 829 respectively. There are a total of 60 primes in our list requiring one or the other of these. Thus, our list would drop to 1182 primes if these were deleted. Since $\log_2 \phi(MN)$ would only drop to 1221, there would be a large gap to make up. We appeared to be getting diminishing returns from increasing the multiplicity of the smaller primes, so it is doubtful that this gap could be bridged.

## 6. CONCLUSIONS

To date, the \$620 appears to be safe. Unless an efficient scheme to search a space of size $2^{1500}$ is found, or an approach other than that suggested by Pomerance can be found, the problem of constructing a counterexample appears to be intractable. It should be mentioned that Pomerance has indicated a willingness to pay his share even for an existence proof [4]. There might be more hope here. For example, suppose we have an $M, N, P$. Let $A$ be a subset of $P$, and let $U$ be the set of all subset products of elements of $A$ modulo $MN$. Given a prime $p \in P - A$, we might ask how big a set of subset products for $A \cup \{p\}$ is. Giving $pU$ the obvious meaning, this set will clearly be $U \cup pU$ and since $|U| = |PU|$, $|U \cup pU| = 2|U| - |U \cap pU|$. If $x \in U \cap pU$, then for some sets of primes, $x = p_1 p_2 \ldots p_k \equiv p q_1 q_2 \ldots q_j$, with the $p$'s and $q$'s from $A$. This can only happen if $p \equiv p_1 p_2 \ldots p_k q_1^{-1} q_2^{-1} \ldots q_j^{-1}$. Thus, if we can choose $p$ so as to avoid the set

$$\{p_1 p_2 \ldots p_k q_1^{-1} q_2^{-1} \ldots q_j^{-1} (\text{mod } MN) : p\text{'s and } q\text{'s are in } A\},$$

then $|U \cup pU| = 2|U|$. Obviously, we cannot pick $p$ to meet this condition forever. If $|U| > \frac{1}{2}\phi(MN)$, there will be a representation $p \equiv p_1 p_2 \ldots p_k q_1^{-1} q_2^{-1} \ldots q_j^{-1}$. If the number of such representations of $p$ is small, the intersection of $U$ and $pU$ will also be small. Thus, one might have a chance of proving that all reduced residue classes are covered at some stage.

If for some $M$ and $N$, $|P|$ is much larger than $\log_2 \phi(MN)$, perhaps there is a way to exploit this size difference as well. For example, the authors would be interested in a proof or counterexample to the following claim:

**Claim**: Let $m$ and $n$ be relatively prime integers. Let $A$ and $B$ be disjoint sets of primes, with no prime dividing $mn$. Suppose that for each reduced residue class $x$ of $m$ and $y$ of $n$ there are nonempty subsets $S$, $T$ of $A$ and $U$, $V$ of $B$ such that

$$f(S) \equiv x (\text{mod } m) \text{ and } f(U) \equiv x (\text{mod } m),$$

$$f(T) \equiv y (\text{mod } n) \text{ and } f(V) \equiv y (\text{mod } n).$$

Then for each reduced residue class $z$ of $mn$, there is a subset $W$ of $A \cup B$ such that $f(W) \equiv z (\text{mod } mn)$.

The authors have not experimented with the claim enough to actually submit it as a conjecture. However, if such a claim were true, then it might be possible to use the prime factorization of $MN$ to show that $P$ covers all reduced residue classes of $MN$. This approach is wasteful of primes in $P$ so the authors are currently calculating primes for the case $n = 100$, with the same $M_{\text{start}}$ and $N_{\text{start}}$ that were used for $n = 70$. This should give a very large set $P$ compared to $\log_2\phi(MN)$. As of this writing, the set $P$ has 4838 primes, with $\log_2\phi(MN) \cong 1838$. We estimate that $|P|$ may get as large as 5500. Various sets of primes we have found are available on the second author's web site, www.d.umn.edu/~jgreene.

## REFERENCES


[1] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*, Fifth Edition, Oxford University Press, New York, 1979.

[2] C. Pomerance, J.L. Selfridge, and S.S. Wagstaff, Jr. "The Pseudoprimes to $25 \cdot 10^9$." *Math. Comp.* **35** (1980): 1003-1026.

[3] C. Pomerance. "Are There Counter-Examples to the Baillie-PSW Primality Test?" Unpublished manuscript.

[4] C. Pomerance, private communication.

[5] P. Ribenboim. *The Book of Prime Number Records*, Springer-Verlag, New York, 1988.

[6] H. Riesel. *Prime Numbers and Computer Methods for Factorization*, Second Edition, Birkhauser, Boston, 1994.


AMS Classification Numbers: 11N25, 11A07, 11B39

✠ ✠ ✠

# ON THE $k^{th}$-ORDER F-L IDENTITY

**Chizhong Zhou**
Department of Computer and Information Engineering, Yueyang Normal University
Yueyang, Hunan 414000, PR China
email: chizhongz@yeah.net

**Fredric T. Howard**
Department of Mathematics,
Wake Forest University, Box 7388 Reynolda Station, Winston-Salem, NC 27109
*(Submitted April 2001)*

## 1. INTRODUCTION

For convenience, in this paper we adopt the notations and symbols in [3] or [4]:
Let the sequence $\{w_n\}$ be defined by the recurrence relation

$$w_{n+k} = a_1 w_{n+k-1} + \cdots + a_{k-1} w_{n+1} + a_k w_n, \tag{1.1}$$

and the initial conditions

$$w_0 = c_0, w_1 = c_1, \ldots, w_{k-1} = c_{k-1}, \tag{1.2}$$

where $a_1, \ldots, a_k$, and $c_0, \ldots, c_{k-1}$ are complex constants. Then we call $\{w_n\}$ a $k^{th}$- **order Fibonacci-Lucas sequence** or simply an **F-L sequence**, call every $w_n$ an **F-L number**, and call

$$f(x) = x^k - a_1 x^{k-1} - \cdots - a_{k-1} x - a_k \tag{1.3}$$

the **characteristic polynomial** of $\{w_n\}$. A number $\alpha$ satisfying $f(\alpha) = 0$ is called a **characteristic root** of $\{w_n\}$. In this paper we always assume that $a_k \neq 0$, hence we may consider $\{w_n\}$ as $\{w_n\}_{-\infty}^{+\infty}$. The set of F-L sequences satisfying (1.1) is denoted by $\Omega(a_1, \ldots, a_k)$ and also by $\Omega(f(x))$. Let $x_1, \ldots, x_k$ be the roots of $f(x)$ defined by (1.3), and let

$$v_n = x_1^n + x_2^n + \cdots + x_k^n (n \in \mathbb{Z}). \tag{1.4}$$

Then, obviously, $\{v_n\} \in \Omega(a_1, \ldots, a_k)$. Since for $k = 2$ and $a_1 = a_2 = 1, \{v_n\}$ is just the classical Lucas sequence $\{L_n\}$, we call $\{v_n\}$ for any $k$ the $k^{th}$**-order Lucas sequence** in $\Omega(a_1, \ldots, a_k)$. In [1] and [2] Howard proved the following theorem:

**Theorem 1.1**: *Let $\{w_n\} \in \Omega(a_1, \ldots, a_k)$. Then for $m \geq 1$ and all integers $n$,*

$$w_{(k-1)m+n} = \sum_{j=1}^{k} (-1)^{j-1} c_{m,jm} w_{(k-j-1)m+n}.$$

*The numbers $c_{m,jm}$ are defined by*

$$\prod_{i=0}^{m-1} [1 - a_1(\theta^i x) - a_2(\theta^i x)^2 - \cdots - a_k(\theta^i x)^k] = 1 + \sum_{j=1}^{k} (-1)^j c_{m,jm} x^{jm},$$

*where $\theta$ is a primitive $m^{th}$ root of unity.*

Yet in [2] he proved the following result:

**Theorem 1.2**: *Let $\{w_n\} \in \Omega(r, s, t)$. Then for $m, n \in \mathbb{Z}$,*

$$w_{n+2m} = J_m w_{n+m} - t^m J_{-m} w_n + t^m w_{n-m}. \tag{1.5}$$

Here $\{J_n\} \in \Omega(r, s, t)$ satisfies $J_0 = 3, J_1 = r, J_2 = r^2 + 2s$.

It is easy to see that $\{J_n\}$ is just the third-order Lucas sequence in $\Omega(r, s, t)$. Thus we observe that the identity (1.5) involves only the numbers from an arbitrary third-order F-L sequence and from the third-order Lucas sequence in $\Omega(r, s, t)$. This suggests the main purpose of the present paper: we shall prove a general $k^{th}$-order F-L identity which involves only the numbers from an arbitrary $k^{th}$-order F-L sequence and from the $k^{th}$-order Lucas sequence in $\Omega(a_1, \ldots, a_k)$. As an application of the identity we represent $c_{m,jm}$ in Theorem 1.1 by the $k^{th}$-order Lucas numbers. Then to make the identity simpler we give the identity an alternative form in which the negative subscripts for the $k^{th}$-order Lucas sequence are introduced. As a corollary of the identity we generalize the result of Theorem 1.2 from the case $k = 3$ to the case of any $k$. In our proofs we do not need to consider whether the characteristic roots of the F-L sequence are distinct. Also, we can use our results to construct identities for given $k$, and the computations are relatively simple. We first give some preliminaries in Section 2, and then in Section 3 we give the main results and their proofs. Some examples are also given in Section 3.

## 2. PRELIMINARIES

**Lemma 2.1**: *Let $\{v_n\}$ be the $k^{th}$-order Lucas sequence in $\Omega(a_1, \ldots, a_k)$. Denote the generating function of $\{v_n\}$ by*

$$V(x) = \sum_{n=0}^{\infty} v_n x^n. \tag{2.1}$$

*Then*

$$V(x) = \frac{k - (k-1)a_1 x - (k-2)a_2 x^2 - \cdots - 2a_{k-2}x^{k-2} - a_{k-1}x^{k-1}}{1 - a_1 x - a_2 x^2 - \cdots - a_k x^k}. \tag{2.2}$$

**Proof**: Let $x_1, \ldots, x_k$ be the roots of the characteristic polynomial $f(x)$, denoted by (1.3), of sequence $\{v_n\}$. Denote

$$f^*(x) = 1 - a_1 x - a_2 x^2 - \cdots - a_k x^k.$$

Clearly,

$$f^*(x) = x^k f(x^{-1}) = (1 - x_1 x) \ldots (1 - x_k x).$$

Whence

$$\ln f^*(x) = \ln(1 - x_1 x) + \cdots + \ln(1 - x_k x).$$

Differentiating the both sides of the last expression we obtain

$$\frac{f^{*'}(x)}{f^*(x)} = \frac{-x_1}{1-x_1x} + \cdots + \frac{-x_k}{1-x_kx}$$

$$= -\sum_{n=0}^{\infty}(x_1^{n+1} + \cdots + x_k^{n+1})x^n = -\sum_{n=0}^{\infty} v_{n+1}x^n.$$

From (2.1) it follows that

$$V(x) = v_0 - x \cdot \frac{f^{*'}(x)}{f^*(x)} = k + \frac{x(a_1 + 2a_2x + \cdots + ka_kx^{k-1})}{1 - a_1x - a_2x^2 - \cdots - a_kx^k}.$$

Thus the proof is finished. □

From (2.1) and (2.2) it follows that

$$(1 - a_1x - a_2x^2 - \cdots - a_kx^k)\sum_{n=0}^{\infty} v_nx^n$$

$$= k - (k-1)a_1x - (k-2)a_2x^2 - \cdots - 2a_{k-2}x^{k-2} - a_{k-1}x^{k-1}.$$

Comparing the coefficients of $x^i$ in the both sides of the last expression for $i = 1, \ldots, k$ we get the well-known Newton's formula:

**Corollary 2.2**: **(Newton's formula)** *Let $\{v_n\}$ be the $k^{th}$-order Lucas sequence in $\Omega(a_1, \ldots, a_k)$. Then*

$$a_1v_{i-1} + a_2v_{i-2} + \cdots + a_{i-1}v_1 + ia_i = v_i \quad (i = 1, \ldots, k).$$

**Lemma 2.3**: [4] *Let $\{w_n\} \in \Omega(a_1, \ldots, a_k) = \Omega(f(x))$, and $x_1, \ldots, x_k$ be the roots of $f(x)$. For $m \in \mathbb{Z}^+$, let*

$$f_m(x) = (x - x_1^m)\ldots(x - x_k^m) = x^k - b_1x^{k-1} - \cdots - b_{k-1}x - b_k. \tag{2.3}$$

*Then $\{w_{mn+r}\}_n \in \Omega(f_m(x))$. That is,*

$$w_{m(n+k)+r} = b_1w_{m(n+k-1)+r} + \cdots + b_{k-1}w_{m(n+1)+r} + b_kw_{mn+r}.$$

## 3. THE MAIN RESULTS AND PROOFS

**Theorem 3.1**: *Let $\{w_n\}$ be any sequence in $\Omega(a_1,\ldots,a_k)=\Omega(f(x))$, and let $\{v_n\}$ be the $k^{th}$-order Lucas sequence in $\Omega(f(x))$. Let $x_1,\ldots,x_k$ be the roots of $f(x)$ and $f_m(x)$ be defined by (2.3) for $m\in\mathbb{Z}^+$. Then for $n\in\mathbb{Z}$,*

$$w_{m(n+k)+r}=b_1w_{m(n+k-1)+r}+\cdots+b_{k-1}w_{m(n+1)+r}+b_kw_{mn+r}, \tag{3.1}$$

*and $b_1,\ldots,b_k$ can be obtained by solving the trianglular system of linear equations*

$$b_1v_{m(i-1)}+b_2v_{m(i-2)}+\cdots+b_{i-1}v_m+ib_i=v_{mi}\quad (i=1,\ldots,k). \tag{3.2}$$

*In other words, for $i=1,\ldots,k$,*

$$b_i=b_i(m)=\frac{1}{i!}\begin{vmatrix} 1 & & & & & & v_m\\ v_m & 2 & & & & & v_{2m}\\ v_{2m} & v_m & 3 & & & & v_{3m}\\ v_{3m} & v_{2m} & v_m & \ddots & & & v_{4m}\\ \vdots & \vdots & \vdots & \ddots & \ddots & & \vdots\\ v_{(i-2)m} & v_{(i-3)m} & v_{(i-4)m} & \cdots & v_m & i-1 & v_{(i-1)m}\\ v_{(i-1)m} & v_{(i-2)m} & v_{(i-3)m} & \cdots & v_{2m} & v_m & v_{im}\end{vmatrix}. \tag{3.3}$$

**Proof**: In $\Omega(f_m(x))$ the $k^{th}$-order Lucas sequence is

$$V_n=(x_1^m)^n+\cdots+(x_k^m)^n=v_{mn}(n\in\mathbb{Z}).$$

Thus (3.1) and (3.2) follow from Lemma 2.3 and Corollary 2.2. We use Cramer's Rule on (3.2) to obtain (3.3) □

**Remark**: In (3.1) taking $n=-1$ and then taking $r=n$ we get $c_{m,jm}=b_j(m)$. Then $c_{m,jm}$ can be represented by the $k^{th}$-order Lucas numbers and it is more easy to caluclate $c_{m,jm}$'s. For example, by using (3.2) or (3.3) we can obtain:

For $k=3$,

$$w_{n+2m}=v_mw_{n+m}+(v_{2m}-v_m^2)/2\cdot w_n+(2v_{3m}-3v_mv_{2m}+v_m^3)/6\cdot w_{n-m};$$

For $k=4$,

$$\begin{aligned}w_{n+3m}=&v_mw_{n+2m}+(v_{2m}-v_m^2)/2\cdot w_{n+m}+(2v_{3m}-3v_mv_{2m}+v_m^3)/6\cdot w_n+\\&(6v_{4m}-8v_mv_{3m}-3v_{2m}^2+6v_m^2v_{2m}-v_m^4)/24\cdot w_{n-m};\end{aligned}$$

For $k=5$,

$$\begin{aligned}w_{n+4m}=&v_mw_{n+3m}+(v_{2m}-v_m^2)/2\cdot w_{n+2m}+(2v_{3m}-3v_mv_{2m}+v_m^3)/6\cdot w_{n+m}+\\&(6v_{4m}-8v_mv_{3m}-3v_{2m}^2+6v_m^2v_{2m}-v_m^4)/24\cdot w_n+\\&(24v_{5m}-30v_mv_{4m}-20v_{2m}v_{3m}+20v_m^2v_{3m}+15v_mv_{2m}^2-\\&10v_m^3v_{2m}+v_m^5)/120\cdot w_{n-m}.\end{aligned}$$

**Theorem 3.2**: *Under the conditions of Theorem 3.1 we have*

$$b_{k-i}(m) = (-1)^{(k+1)(m+1)+1} a_k^m b_i(-m) \quad (i = 1, \dots, k-1), \tag{3.4}$$

*and*

$$b_k(m) = (-1)^{(k+1)(m+1)} a_k^m. \tag{3.5}$$

*Therefore for odd k we have*

$$\begin{aligned} w_{m(n+k)+r} =& b_1(m) w_{m(n+k-1)+r} + b_2(m) w_{m(n+k-2)+r} + \cdots + \\ & b_{(k-1)/2}(m) w_{m(n+(k+1)/2)+r} - a_k^m (b_{(k-1)/2}(-m) w_{m(n+(k-1)/2)+r} + \\ & \cdots + b_2(-m) w_{m(n+2)+r} + b_1(-m) w_{m(n+1)+r} - w_{mn+r}), \end{aligned} \tag{3.6}$$

*and for even k we have*

$$\begin{aligned} w_{m(n+k)+r} =& b_1(m) w_{m(n+k-1)+r} + b_2(m) w_{m(n+k-2)+r} + \cdots + \\ & b_{k/2-1}(m) w_{m(n+k/2+1)+r} + b_{k/2}(m) w_{m(n+k/2)+r} + \\ & (-a_k)^m (b_{k/2-1}(-m) w_{m(n+k/2-1)+r} + \\ & \cdots + b_2(-m) w_{m(n+2)+r} + b_1(-m) w_{m(n+1)+r} - w_{mn+r}). \end{aligned} \tag{3.7}$$

**Proof**: Clearly,

$$b_k = b_k(m) = -(-1)^k x_1^m \dots x_k^m = (-1)^{k+1}(-(-1)^k a_k)^m.$$

Whence (3.5) holds. Let

$$\begin{aligned} f_m^*(x) &= x^k f_m(x^{-1}) = (1 - x_1^m x) \dots (1 - x_k^m x) \\ &= 1 - b_1 x - b_2 x^2 - \cdots - b_{k-1} x^{k-1} - b_k x^k. \end{aligned}$$

Then the $k^{th}$-order Lucas sequence in $\Omega(f_m^*(x))$ is

$$V_n^* = (x_1^{-m})^n + \cdots + (x_k^{-m})^n = v_{-mn} (n \in \mathbb{Z}).$$

By Newton's formula we have, for $i = 1, \dots, k-1$,

$$b_{k-1} v_{-m(i-1)} + b_{k-2} v_{-m(i-2)} + \cdots + b_{k-(i-1)} v_{-m} + i b_{k-i} = -b_k v_{-mi},$$

where $b_i = b_i(m)$. It follows from Cramer's Rule that

$$b_{k-i} = b_{k-i}(m) = \frac{-b_k(m)}{i!} \begin{vmatrix} 1 & & & & & & v_{-m} \\ v_{-m} & 2 & & & & & v_{-2m} \\ v_{-2m} & v_{-m} & 3 & & & & v_{-3m} \\ v_{-3m} & v_{-2m} & v_{-m} & \ddots & & & v_{-4m} \\ \vdots & \vdots & \vdots & \ddots & \ddots & & \vdots \\ v_{-(i-2)m} & v_{-(i-3)m} & v_{-(i-4)m} & \cdots & v_{-m} & i-1 & v_{-(i-1)m} \\ v_{-(i-1)m} & v_{-(i-2)m} & v_{-(i-3)m} & \cdots & v_{-2m} & v_{-m} & v_{-im} \end{vmatrix}. \tag{3.8}$$

Noticing (3.5) and comparing (3.8) with (3.3) we see that (3.4) holds. This completes the proof. □

**Corollary 3.3**: *Let $\{w_n\}$ be any sequence in $\Omega(a_1, \ldots, a_k\} = \Omega(f(x))$, and let $\{v_n\}$ be the $k^{th}$-order Lucas sequence in $\Omega(f(x))$. Assume that $n, m \in Z$ and $m \neq 0$. Then, for odd $k$ we have*

$$\begin{aligned} w_{n+m(k-1)} =& b_1(m)w_{n+m(k-2)} + b_2(m)w_{n+m(k-3)} + \cdots + \\ & b_{(k-1)/2}(m)w_{n+m(k-1)/2} - a_k^m(b_{(k-1)/2}(-m)w_{n+m(k-3)/2} + \\ & \cdots + b_2(-m)w_{n+m} + b_1(-m)w_n - w_{n-m}), \end{aligned} \tag{3.9}$$

*and for even $k$ we have*

$$\begin{aligned} w_{n+m(k-1)} =& b_1(m)w_{n+m(k-2)} + b_2(m)w_{n+m(k-3)} + \cdots + \\ & b_{k/2-1}(m)w_{n+mk/2} + b_{k/2}(m)w_{n+m(k/2-1)} + \\ & (-a_k)^m(b_{k/2-1}(-m)w_{n+m(k/2-2)} + \\ & \cdots + b_2(-m)w_{n+m} + b_1(-m)w_n - w_{n-m}). \end{aligned} \tag{3.10}$$

**Proof**: For $m > 0$ the conclusion is shown by taking $n = -1$ and then taking $r = n$ in Theorem 3.2. Now, assume that $m < 0$. Then, $-m > 0$, and, by the proved result, for odd $k$ we have

$$\begin{aligned} w_{n-m(k-1)} =& b_1(-m)w_{n-m(k-2)} + b_2(-m)w_{n-m(k-3)} + \cdots + \\ & b_{(k-1)/2}(-m)w_{n-m(k-1)/2} - a_k^{-m}(b_{(k-1)/2}(m)w_{n-m(k-3)/2} + \\ & \cdots + b_2(m)w_{n-m} + b_1(m)w_n - w_{n+m}), \end{aligned} \tag{3.11}$$

and for even $k$ we have

$$\begin{aligned} w_{n-m(k-1)} =& b_1(-m)w_{n-m(k-2)} + b_2(-m)w_{n-m(k-3)} + \cdots + \\ & b_{k/2-1}(-m)w_{n-mk/2} + b_{k/2}(-m)w_{n-m(k/2-1)} + \\ & (-a_k)^{-m}(b_{k/2-1}(m)w_{n-m(k/2-2)} + \\ & \cdots + b_2(m)w_{n-m} + b_1(m)w_n - w_{n+m}). \end{aligned} \tag{3.12}$$

Multiplying both sides of (3.11) by $a_k^m$ and replacing $n$ by $n + m(k - 2)$ we can get (3.9). Multiplying both sides of (3.12) by $(-a_k)^m$ and replacing $n$ by $n+m(k-2)$ we can get (3.10). Thus the proof is finished. □

**Remark**: Corollary 3.3 is a generalization of Theorem 1.2 (for $k = 3$). By using the corollary we can easily give the following examples:

For $k = 4$,

$$w_{n+3m} = v_m w_{n+2m} + (v_{2m} - v_m^2)/2 \cdot w_{n+m} + (-a_4)^m (v_{-m} w_n - w_{n-m});$$

For $k = 5$,

$$\begin{aligned} w_{n+4m} =& v_m w_{n+3m} + (v_{2m} - v_m^2)/2 \cdot w_{n+2m} - \\ & a_5^m ((v_{-2m} - v_{-m}^2)/2 \cdot w_{n+m} + v_{-m} w_n - w_{n-m}); \end{aligned}$$

For $k = 6$,

$$\begin{aligned} w_{n+5m} =& v_m w_{n+4m} + (v_{2m} - v_m^2)/2 \cdot w_{n+3m} + (2v_{3m} - 3v_m v_{2m} + v_m^3)/6 \cdot w_{n+2m} + \\ & (-a_6)^m ((v_{-2m} - v_{-m}^2)/2 \cdot w_{n+m} + v_{-m} w_n - w_{n-m}). \end{aligned}$$

## REFERENCES


[1] F. T. Howard. "Generalizations of a Fibonacci Identity." *Applications of Fibonacci Numbers*, Vol. 8. Edited by Fredric T. Howard. Kluwer Academic Publishers. Dordrecht, The Netherlands, 1999: pp. 201-211.

[2] F. T. Howard. "A Tribonacci Identity." *The Fibonacci Quarterly* **39.4** (2001): 352-357.

[3] C. Z. Zhou. "A Generalization of the 'All or None' Divisibility Property." *The Fibonacci Quarterly* **35.2** (1997): 129-134.

[4] C. Z. Zhou. "Constructing Identities Involving $k$th-order $F$-$L$ Numbers by Using the Characteristic Polynomial." *Applications of Fibonacci Numbers*, Vol. 8. Edited by Fredric T. Howard. Kluwer Academic Publishers. Dordrecht, The Netherlands, 1999: pp. 369-379.


AMS Classification Numbers: 11B39, 11B37

✠ ✠ ✠

# UNEXPECTED PELL AND QUASI MORGAN-VOYCE SUMMATION CONNECTIONS

A. F. Horadam
The University of New England, Armidale, N.S.W., Australia 2351
*(Submitted May 2001-Final Revision May 2002)*

## 1. PRELIMINARIES

### Motivation

In [1], the connection between *Pell convolution numbers* $P_n^{(m)}$ and *Quasi Morgan-Voyce polynomials* $S_n^{(r,u)}(x)$ was established.

Here, the objective is to display a set of nine neat formulas (Theorems 1-9) expressing $S_n^{(r,u)}(x)$ in terms of finite sums involving $P_n^{(m)}(r,u=0,1,2)$ with $P_0^{(m)}=0$, while $P_n^{(m)}(n<0)$ is not defined. Central to this theme is the germinal polynomial $S_n^{(1,1)}(x)$.

Initially, the impetus for this paper originated from a nice result (Theorem 1) discovered by J.M. Mahon [3], [4], to whom indebtedness is gratefully acknowledged.

### Background Material

Firstly, note that [1, (3.3)]

$$S_n^{(r,u)}(x)=\sum_{k=0}^{n} d_{n,k}^{(r,u)}x^k \tag{1.1}$$

with certain restrictions [1, (3.4)] on $d_{n,k}^{(r,u)}$. Secondly [1, Theorem 1],

$$d_{n,0}^{(r,u)}=P_n r+\frac{1}{2}Q_n u \tag{1.2}$$

where $P_n, Q_n$ are the Pell and Pell-Lucas numbers [2], respectively, with $P_n\equiv P_n^{(0)}, Q_n\equiv Q_n^{(0)}$. **Allusion to (1.1) and (1.2) will be constantly made.**

Results (1.3) - (1.6) are required in the demonstration of proofs:

$$P_n^{(m)}=2P_{n-1}^{(m)}+P_{n-2}^{(m)}+P_n^{(m-1)} \quad (\textit{recurrence}) \tag{1.3}$$

$$P_{n+1-m}^{(m)}+P_{n-1-m}^{(m)}=\frac{n}{m}P_{n+1-m}^{(m-1)} \tag{1.4}$$

$$P_n^{(m)}-P_{n-1}^{(m)}=\frac{n+2m-1}{2m}P_n^{(m-1)} \tag{1.5}$$

$$d_{n,k}^{(r,u)}=P_{n+1-k}^{(k-1)}+P_{n-k}^{(k)}r+\frac{n-k}{2k}P_{n+1-k}^{(k-1)}u. \tag{1.6}$$

Results (1.3) - (1.6) occur in [1] as [1, (2.1)], [1, (2.4)], [1, (2.5)], and [1 Theorem 4], respectively. They are necessary tools of trade in this paper.

Please notice the correction in (1.6) to the first factor in the third term in the enunciation of [1, Theorem 4], namely, $\frac{n-k}{2k}$ instead of $\frac{n-2}{2^k}$

### Guiding Comments

(i) Familarity with [1, Table 1] and [1, Table 2] is essential.
(ii) Choice of $n = 3$ in all the Examples of the Theorems provides some basis for comparison.
(iii) Because of the variety of approaches available in the proofs, some detail of all proofs is appropriate.
(iv) Generally (Theorems 3-9), the technique for developing the proofs lies in "spotting" the involvement of two or more $S_n^{(1,1)}(x)$ and hence pursuing the corresponding arithmetic for the $d_{n,k}^{(r,u)}$.

## 2. THE SUMMATION RESULTS

**Theorem 1** (Mahon [3]): $S_n^{(1,1)}(x) = \sum_{k=0}^{n} P_{n+1-k}^{(k)} x^k$.

**Proof**: Now $S_n^{(1,1)}(x) = \sum_{k=0}^{n} d_{n,k}^{(1,1)} x^k$ by (1.1).
But

$$\begin{aligned} d_{n,k}^{(1,1)} &= P_{n+1-k}^{(k-1)} + P_{n-k}^{(k)} + \frac{n-k}{2k} P_{n+1-k}^{(k-1)} \text{ by (1.6)} \\ &= P_{n+1-k}^{(k-1)} + P_{n+1-k}^{(k)} - \frac{(n-k+1+2k-1)}{2k} P_{n+1-k}^{(k-1)} + \frac{n-k}{2k} P_{n+1-k}^{(k-1)} \text{ by (1.5)} \\ &= P_{n+1-k}^{(k)}, \end{aligned}$$

whence the theorem follows by (1.1).

**Alternative Proof** [4]: Use induction on $n$ in conjunction with (1.3).

**Example**: $S_3^{(1,1)}(x) = 12 + 14x + 6x^2 + x^3 = P_4^{(0)} + P_3^{(1)} x + P_2^{(2)} x^2 + P_1^{(3)} x^3$.

**Theorem 2**: $S_n^{(0,0)}(x) = \sum_{k=0}^{n-1} P_{n-k}^{(k)} x^{k+1}$.

**Proof**:

$$\begin{aligned} S_n^{(0,0)}(x) &= x\boldsymbol{B}_n(x) \quad \text{by [1, (4.5)]} \\ &= xS_{n-1}^{(1,1)}(x) \quad \text{by [1, (4.1)]}, \end{aligned}$$

where $\boldsymbol{B}_n(x)$ is the quasi Morgan-Voyce analogue [1] of the corresponding standard Morgan-Voyce polynomial $B_n(x)$. Theorem 2 is thus an immediate consequence of Theorem 1.

**Example**: $S_3^{(0,0)}(x) = 5x + 4x^2 + x^3 = P_3^{(0)} x + P_2^{(1)} x^2 + P_1^{(2)} x^3$.

**Theorem 3**: $S_n^{(0,1)}(x) = \sum_{k=1}^n \frac{n+k}{2k} P_{n+1-k}^{(k-1)} x^k + \frac{Q_n}{2}$.

**Proof**: Consider $S_n^{(1,1)}(x) - S_{n-1}^{(1,1)}(x)$. Then

$$\begin{aligned}
d_{n,k}^{(1,1)} - d_{n-1,k}^{(1,1)} &= P_{n+1-k}^{(k-1)} + P_{n-k}^{(k)} + \frac{n-k}{2k} P_{n+1-k}^{(k-1)} \\
&\quad - P_{n-k}^{(k-1)} - P_{n-1-k}^{(k)} - \frac{n-1-k}{2k} P_{n-k}^{(k-1)} \quad \text{by (1.6)} \\
&= P_{n+1-k}^{(k-1)} + \frac{n-k+2k-1}{2k} P_{n-k}^{(k-1)} + \frac{n-k}{2k} P_{n+1-k}^{(k-1)} \\
&\quad - P_{n-k}^{(k-1)} - \frac{n-1-k}{2k} P_{n-k}^{(k-1)} \quad \text{by (1.5)} \\
&= P_{n+1-k}^{(k-1)} + \frac{n-k}{2k} P_{n+1-k}^{(k-1)} = \frac{n+k}{2k} P_{n+1-k}^{(k-1)} \qquad (\alpha) \\
&= d_{n,k}^{(0,1)} \quad \text{by (1.6).}
\end{aligned}$$

Invoking $(\alpha)$ ensures the theorem. Be aware that the isolated Pell-Lucas term $\frac{1}{2}Q_n$ arises when $k = 0$. Also see (1.2) for $r = 0,\ u = 1$.

**Example**: $S_3^{(0,1)}(x) = 7 + 10x + 5x^2 + x^3 = \frac{1}{2}Q_3 + 2P_3^{(0)}x + \frac{5}{4}P_2^{(1)}x^2 + P_1^{(2)}x^3$.

**Theorem 4**: $S_n^{(1,0)}(x) = \sum_{k=1}^n \left(P_{n-k}^{(k)} + P_{n+1-k}^{(k-1)}\right) x^k + P_n$.

**Proof**: Consider $S_{n-1}^{(1,1)}(x)$ for $k$, added to $S_{n-1}^{(1,1)}(x)$ for $k-1$. So

$$\begin{aligned}
d_{n-1,k}^{(1,1)} + d_{n-1,k-1}^{(1,1)} &= P_{n-k}^{(k-1)} + P_{n-1-k}^{(k)} + \frac{n-1-k}{2k} P_{n-k}^{(k-1)} \\
&\quad + P_{n+1-k}^{(k-2)} + P_{n-k}^{(k-1)} + \frac{n-k}{2(k-1)} P_{n+1-k}^{(k-2)} \quad \text{by (1.6)} \\
&= P_{n-1-k}^{(k)} + P_{n-k}^{(k-1)} + \frac{n-1+k}{2k} P_{n-k}^{(k-1)} + \frac{n-k}{2(k-1)} P_{n+1-k}^{(k-2)} \quad \text{by (1.5)} \\
&= P_{n-k}^{(k)} + P_{n+1-k}^{(k-1)} \qquad (\beta) \\
&= d_{n,k}^{(1,0)} \quad \text{by (1.6),}
\end{aligned}$$

whence the theorem ensues on appeal to $(\beta)$. Observe that the extraneous Pell number $P_n$ occurs when $k=0$, in conformity with (1.2) for $r=1, u=0$.

**Example**: $S_3^{(1,0)}(x) = 5 + 9x + 5x^2 + x^3 = P_3 + \left(P_3^{(0)} + P_2^{(1)}\right)x + \left(P_2^{(1)} + P_1^{(2)}\right)x^2 + \left(P_1^{(2)} + P_0^{(3)}\right)x^3$.

**Theorem 5**: $S_n^{(2,2)}(x) = \sum_{k=1}^n \left(2P_{n+1-k}^{(k)} - P_{n+1-k}^{(k-1)}\right)x^k + 2P_{n+1}$.

**Proof**: Consider $2S_n^{(1,1)}(x)$ for $k$, then subtract $S_{n-1}^{(1,1)}(x)$ for $k-1$. Accordingly,

$$2d_{n,k}^{(1,1)} - d_{n-1,k-1}^{(1,1)} = 2P_{n-k}^{(k)} + \frac{n+k}{k}P_{n+1-k}^{(k-1)} - P_{n-k}^{(k-1)} - \frac{n-2+k}{2(k-1)}P_{n+1-k}^{(k-2)} \quad \text{by (1.6)}$$

$$= 2P_{n+1-k}^{(k)} - P_{n+1-k}^{(k-1)} \quad \text{by (1.4), (1.5), (1.3) and simplifying} \qquad (\gamma)$$

$$= \left(P_{n+1-k}^{(k)} - P_{n-1-k}^{(k)} - P_{n+1-k}^{(k-1)}\right) + P_{n+1-k}^{(k)} + P_{n-1-k}^{(k)}$$

$$= 2P_{n-k}^{(k)} + P_{n+1-k}^{(k)} + P_{n-1-k}^{(k)} \quad \text{by (1.3)}$$

$$= 2P_{n-k}^{(k)} + \frac{n}{k}P_{n+1-k}^{(k-1)} \quad \text{by (1.4)}$$

$$= P_{n+1-k}^{(k-1)} + 2P_{n-k}^{(k)} + 2\cdot\frac{n-k}{2k}P_{n+1-k}^{(k-1)}$$

$$= d_{n,k}^{(2,2)} \quad \text{by (1.6).}$$

Applying $(\gamma)$, we have the theorem where $2P_{n+1}$ originates with $k=0$. Refer again to (1.2), where $r=u=2$ in this case.

**Example**:

$$S_3^{(2,2)}(x) = 24 + 23x + 8x^2 + x^3$$

$$= 2P_4 + (2P_3^{(1)} - P_3^{(0)})x + (2P_2^{(2)} - P_2^{(1)})x^2 + (2P_1^{(3)} - P_1^{(2)})x^3.$$

**Theorem 6**: $S_n^{(1,2)}(x) = \sum_{k=0}^n \left(P_{n+1-k}^{(k)} + P_{n-k}^{(k)} + P_{n-1-k}^{(k)}\right)x^k$.

**Proof**: Consider $S_{n,k}^{(1,1)}(x) + S_{n-1,k}^{(1,1)}(x) + S_{n-2,k}^{(1,1)}(x)$, leading to

$$d_{n,k}^{(1,1)} + d_{n-1,k}^{(1,1)} + d_{n-2,k}^{(1,1)} = P_{n+1-k}^{(k-1)} + \frac{n-k}{2k} P_{n+1-k}^{(k-1)} + P_{n-k}^{(k)}$$

$$+ P_{n-k}^{(k-1)} + \frac{n-1-k}{2k} P_{n-k}^{(k-1)} + P_{n-1-k}^{(k)}$$

$$+ P_{n-1-k}^{(k-1)} + \frac{n-2-k}{2k} P_{n-1-k}^{(k-1)} + P_{n-2-k}^{(k)}$$

$$= P_{n+1-k}^{(k)} + P_{n-k}^{(k)} + P_{n-1-k}^{(k)} \quad \text{using (1.5) three times} \qquad (\delta)$$

$$= P_{n-k}^{(k)} + \frac{n}{k} P_{n+1-k}^{(k-1)} \quad \text{by (1.4)}$$

$$= P_{n+1-k}^{(k-1)} + P_{n-k}^{(k)} + \frac{n-k}{2k} P_{(n+1-k)}^{(k-1)} \cdot 2$$

$$= d_{n,k}^{(1,2)} \quad \text{by (1.6),}$$

whence the theorem is assured by ($\delta$).

**Example**: $S_3^{(1,2)}(x) = 19 + 19x + 7x^2 + x^3 = \left(P_4^{(0)} + P_3^{(0)} + P_2^{(0)}\right) + \left(P_3^{(1)} + P_2^{(1)} + P_1^{(1)}\right) x +$
$\left(P_2^{(2)} + P_1^{(2)} + P_0^{(2)}\right) x^2 + \left(P_1^{(3)} + P_0^{(3)} + P_{-1}^{(3)}\right) x^3.$

**Outlines of Proofs of Theorems 7-9**:

Anticipating that the reader's appetite may have been whetted a little, we hopefully leave the remaining proofs as minor challenges, while giving a indication in each case of the appropriate procedure.

**Theorem 7**: $S_n^{(0,2)}(x) = \sum_{k=1}^{n} \frac{n}{k} P_{n+1-k}^{(k-1)} x^k + Q_n.$

**Proof**: This resembles Theorem 3. Use $S_n^{(1,1)}(x) + S_{n-2}^{(1,1)}(x)$ giving

$$d_{n,k}^{(1,1)} + d_{n-2,k}^{(1,1)} = P_{n+1-k}^{(k)} + P_{n-1-k}^{(k)} \quad \text{by Theorem 1, applied twice}$$

$$= \frac{n}{k} P_{n+1-k}^{(k-1)} \quad \text{by (1.4)}$$

$$= P_{n+1-k}^{(k-1)} + \frac{n-k}{2k} P_{n+1-k}^{(k-1)} \cdot 2$$

$$= d_{n,k}^{(0,2)} \quad \text{by (1.6).}$$

Once again, we recall that the appendage constant term $Q_n$ in the enunciation of the theorem refers to $k = 0$, noting that this is guaranteed by (1.2) for $r = 0, u = 2$.

**Example**: $S_3^{(0,2)}(x) = 14 + 15x + 6x^2 + x^3 = Q_3 + 3P_3^{(0)}x + \frac{3}{2}P_2^{(1)}x^2 + P_1^{(2)}x^3$.

**Theorem 8**: $S_n^{(2,0)}(x) = \sum_{k=1}^n \left(2P_{n-k}^{(k)} + P_{n+1-k}^{(k-1)}\right)x^k + 2P_n$.

**Proof**: This resembles Theorem 4. Use (1.5) and (1.6) to produce

$$\begin{aligned} 2d_{n-1,k}^{(1,1)} + d_{n-1,k-1}^{(1,1)} &= P_{n+1-k}^{(k-1)} + 2P_{n-k}^{(k)} \\ &= d_{n,k}^{(2,0)} \end{aligned}$$

with $k = 0$ yielding the exterior term $2P_n$, confirmed by (1.2) for $r = 2, u = 0$.

**Example**:

$$\begin{aligned} S_3^{(2,0)}(x) &= 10 + 13x + 6x^2 + x^3 \\ &= 2P_3 + (2P_2^{(1)} + P_3^{(0)})x + (2P_1^{(2)} + P_2^{(1)})x^2 + (2P_0^{(3)} + P_1^{(2)})x^3. \end{aligned}$$

**Theorem 9**: $S_n^{(2,1)}(x) = \sum_{k=1}^n \left(2P_{n-k}^{(k)} + \frac{n+k}{2k}P_{n+1-k}^{(k-1)}\right)x^k + 2P_n + \frac{1}{2}Q_n$.

**Proof**: If we consider the simple addition $S_n^{(1,1)}(x) + S_{n-1}^{(1,1)}(x)$, then

$$\begin{aligned} d_{n,k}^{(1,1)} + d_{n-1,k}^{(1,1)} &= 2P_{n-k}^{(k)} + \frac{n+k}{2k}P_{n+1-k}^{(k-1)} \\ &= d_{n,k}^{(2,1)} \end{aligned}$$

eventually, after applying (1.6) and (1.5) and tidying up. Our theorem is then validated, remembering that $d_{n,0}^{(2,1)} = 2P_n + \frac{1}{2}Q_n$ by (1.2).

**Example**:

$$\begin{aligned} S_3^{(2,1)}(x) &= 17 + 18x + 7x^2 + x^3 \\ &= (10 + 7) + (2P_2^{(1)} + 2P_3^{(0)})x + (2P_1^{(2)} + \frac{5}{4}P_2^{(1)})x^2 + (2P_0^{(3)} + P_1^{(2)})x^3. \end{aligned}$$

## 3. AFTERTHOUGHTS

### Relationships among (i) the $d_{n,k}^{(r,u)}$, (ii) the $S_n^{(r,u)}(x)$

Simple links connecting the $d_{n,k}^{(r,u)}$, each with a corresponding nexus involving the $S_n^{(r,u)}(x)$, are relatively easy to discover from the material in Theorems 1-9. For convenience we will drop the functional notation for $S_n^{(r,u)}(x)$ in this segment. Thus:

*Temporary Convention*: $S_n^{(r,u)}(x) \equiv S_n^{(r,u)}$.

| Theorems | Connections | |
|---|---|---|
| 3, 9 | $\left.\begin{array}{l} d_{n,k}^{(0,1)} + d_{n,k}^{(2,1)} = 2d_{n,k}^{(1,1)} \\ S_n^{(0,1)} + S_n^{(2,1)} = 2S_n^{(1,1)} \end{array}\right\}$ | (3.1) |
| 4, 8 | $\left.\begin{array}{l} d_{n,k}^{(2,0)} - d_{n,k}^{(1,0)} = d_{n-1,k}^{(1,1)} \\ S_n^{(2,0)} - S_n^{(1,0)} = S_{n-1}^{(1,1)} \end{array}\right\}$ | (3.2) |
| 6, 7 | $\left.\begin{array}{l} d_{n,k}^{(1,2)} - d_{n,k}^{(0,2)} = d_{n-1,k}^{(1,1)} \\ S_n^{(1,2)} - S_n^{(0,2)} = S_{n-1}^{(1,1)}. \end{array}\right\}$ | (3.3) |

Appropriate right-hand sides of (3.2), (3.3) are the same, whereas those of (3.1) are twice as great.

Furthermore, Theorems 5 and 8 together yield

$$\left.\begin{array}{l} d_{n,k}^{(2,2)} + d_{n,k}^{(2,0)} = 2\left(d_{n,k}^{(1,1)} + d_{n-1,k}^{(1,1)}\right) \\ S_n^{(2,2)} + S_n^{(2,0)} = 2\left(S_n^{(1,1)} + S_{n-1}^{(1,1)}\right). \end{array}\right\} \tag{3.4}$$

Verifications of (3.1) - (3.4) may readily be checked for $n = 3$ by using data already provided in the text, along with $S_2^{(1,1)} = 5 + 4x + x^2$.

Lastly, observe that from (1.2),

$$d_{n,0}^{(r,u)} - d_{n,0}^{(u,r)} = (u-r)P_{n-1} = 0 \text{ if } r = u. \tag{3.5}$$

More generally, a quick investigation of $d_{n,k}^{(r,u)} - d_{n,k}^{(u,r)}$ could be undertaken.

## FINALE

Our self-contained set of propositions (Theorems 1-9) has been a pleasurable challenge to the author who at no time found himself wandering in "the bloomless meadows of algebra", as envisaged by the character in the novel by Robert Louis Stevenson and Lloyd Osbourne, *The Wrecker*. Moreover, it has exploited the opportunity to expand our knowledge of the coefficients $d_{n,k}^{(r,u)}$ from [1].

## ACKNOWLEDGMENT

Appreciation is happily expressed by the author for the referee's careful appraisal of this paper, including the sympathetic understanding of an occasional *lapsus calami* (or careless slip, as camouflaged in Latin by the referee!).

## REFERENCES

[1] A.F. Horadam. "Quasi Morgan-Voyce Polynomials and Pell Convolutions." *Applications of Fibonacci Numbers*, Volume 8. Edited by F.T. Howard. Kluwer Academic Publishers, Dordrecht, The Netherlands, 1999: pp. 179-193.
[2] A.F. Horadam and Br. J.M. Mahon. "Convolutions for Pell Polynomials." *Applications of Fibonacci Numbers*, Volume 1. Edited by G.E. Bergum, A.F. Horadam and A.N. Philippou. Kluwer Academic Publishers, Dordrecht, The Netherlands, 1986: pp. 55.80.
[3] Br. J.M. Mahon. Private Correspondence (18 January, 2001).
[4] Br. J.M. Mahon. Private Correspondence (22 February, 2001).

AMS Classification Numbers: 11B39

✠ ✠ ✠

# A PROBABILISTIC VIEW OF CERTAIN WEIGHTED FIBONACCI SUMS


## Arthur T. Benjamin
Dept. of Mathematics, Harvey Mudd College, Claremont, CA 91711
benjamin@hmc.edu

## Judson D. Neer
Dept. of Science and Mathematics, Cedarville University, 251 N. Main St., Cedarville, OH 45314-0601
jud@poboxes.com

## Daniel E. Otero
Dept. of Mathematics and Computer Science, Xavier University, Cincinnati, OH 45207-4441
otero@xu.edu

## James A. Sellers
Dept. of Mathematics, Penn State University, University Park, PA 16802
sellersj@math.psu.edu


*(Submitted May 2001)*

## 1. INTRODUCTION

In this paper we investigate sums of the form

$$a_n := \sum_{k\geq 1} \frac{k^n F_k}{2^{k+1}}. \tag{1}$$

For any given $n$, such a sum can be determined [3] by applying the $x\frac{d}{dx}$ operator $n$ times to the generating function

$$G(x) := \sum_{k\geq 1} F_k x^k = \frac{x}{1-x-x^2},$$

then evaluating the resulting expression at $x = 1/2$. This leads to $a_0 = 1, a_1 = 5, a_2 = 47$, and so on. These sums may be used to determine the expected value and higher moments of the number of flips needed of a fair coin until two consecutive heads appear [3]. In this article, we pursue the reverse strategy of using probability to derive $a_n$ and develop an exponential generating function for $a_n$ in Section 3. In Section 4, we present a method for finding an exact, non-recursive, formula for $a_n$.

## 2. PROBABILISTIC INTERPRETATION

Consider an infinitely long binary sequence of independent random variables $b_1, b_2, b_3, \ldots$ where $P(b_i = 0) = P(b_i = 1) = 1/2$. Let $Y$ denote the random variable denoting the beginning of the first 00 substring. That is, $b_Y = b_{Y+1} = 0$ and no 00 occurs before then. Thus $P(Y = 1) = 1/4$. For $k \geq 2$, we have $P(Y = k)$ is equal to the probability that our sequence begins $b_1, b_2, \ldots, b_{k-2}, 1, 0, 0$, where no 00 occurs among the first $k-2$ terms. Since the probability of occurence of each such string is $(1/2)^{k+1}$, and it is well known [1] that there are exactly $F_k$ binary strings of length $k-2$ with no consecutive 0's, we have for $k \geq 1$,

$$P(Y = k) = \frac{F_k}{2^{k+1}}.$$

Since $Y$ is finite with probability 1, it follows that

$$\sum_{k \geq 1} \frac{F_k}{2^{k+1}} = \sum_{k \geq 1} P(Y = k) = 1.$$

For $n \geq 0$, the expected value of $Y^n$ is

$$a_n := E(Y^n) = \sum_{k \geq 1} \frac{k^n F_k}{2^{k+1}}. \tag{2}$$

Thus $a_0 = 1$. For $n \geq 1$, we use conditional expectation to find a recursive formula for $a_n$. We illustrate our argument with $n = 1$ and $n = 2$ before proceeding with the general case.

For a random sequence $b_1, b_2, \ldots$, we compute $E(Y)$ by conditioning on $b_1$ and $b_2$. If $b_1 = b_2 = 0$, then $Y = 1$. If $b_1 = 1$, then we have wasted a flip, and we are back to the drawing board; let $Y'$ denote the number of remaining flips needed. If $b_1 = 0$ and $b_2 = 1$, then we have wasted two flips, and we are back to the drawing board; let $Y''$ denote the number of remaining flips needed in this case. Now by conditional expectation we have

$$\begin{aligned} E(Y) &= \frac{1}{4}(1) + \frac{1}{2}E(1 + Y') + \frac{1}{4}E(2 + Y'') \\ &= \frac{1}{4} + \frac{1}{2} + \frac{1}{2}E(Y') + \frac{1}{2} + \frac{1}{4}E(Y'') \\ &= \frac{5}{4} + \frac{3}{4}E(Y) \end{aligned}$$

since $E(Y') = E(Y'') = E(Y)$. Solving for $E(Y)$ gives us $E(Y) = 5$. Hence,

$$a_1 = \sum_{k \geq 1} \frac{kF_k}{2^{k+1}} = 5.$$

Conditioning on the first two outcomes again allows us to compute

$$\begin{aligned} E(Y^2) &= \frac{1}{4}(1^2) + \frac{1}{2}E\left[(1 + Y')^2\right] + \frac{1}{4}E\left[(2 + Y'')^2\right] \\ &= \frac{1}{4} + \frac{1}{2}E(1 + 2Y + Y^2) + \frac{1}{4}E(4 + 4Y + Y^2) \\ &= \frac{7}{4} + 2E(Y) + \frac{3}{4}E(Y^2). \end{aligned}$$

Since $E(Y) = 5$, it follows that $E(Y^2) = 47$. Thus,

$$a_2 = \sum_{k \geq 1} \frac{k^2 F_k}{2^{k+1}} = 47.$$

Following the same logic for higher moments, we derive for $n \geq 1$,

$$E(Y^n) = \frac{1}{4}(1^n) + \frac{1}{2}E\left[(1+Y)^n\right] + \frac{1}{4}E\left[(2+Y)^n\right]$$

$$= \frac{1}{4} + \frac{3}{4}E(Y^n) + \frac{1}{2}\sum_{k=0}^{n-1}\binom{n}{k}E(Y^k) + \frac{1}{4}\sum_{k=0}^{n-1}\binom{n}{k}2^{n-k}E(Y^k).$$

Consequently, we have the following recursive equation:

$$E(Y^n) = 1 + \sum_{k=0}^{n-1}\binom{n}{k}[2 + 2^{n-k}]E(Y^k)$$

Thus for all $n \geq 1$,

$$a_n = 1 + \sum_{k=0}^{n-1}\binom{n}{k}[2 + 2^{n-k}]a_k. \tag{3}$$

Using equation (3), one can easily derive $a_3 = 665, a_4 = 12,551$, and so on.

## 3. GENERATING FUNCTION AND ASYMPTOTICS

For $n \geq 0$, define the exponential generating function

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

It follows from equation (3) that

$$a(x) = 1 + \sum_{n\geq 1}\frac{\left(1 + \sum_{k=0}^{n-1}\binom{n}{k}[2+2^{n-k}]a_k\right)}{n!}x^n$$

$$= e^x + 2a(x)(e^x - 1) + a(x)(e^{2x} - 1).$$

Consequently,

$$a(x) = \frac{e^x}{4 - 2e^x - e^{2x}}. \tag{4}$$

For the asymptotic growth of $a_n$, one need only look at the leading term of the Laurent series expansion [4] of $a(x)$. This leads to

$$a_n \approx \frac{\sqrt{5}-1}{10-2\sqrt{5}}\left(\frac{1}{\ln(\sqrt{5}-1)}\right)^{n+1} n!. \tag{5}$$

## 4. CLOSED FORM

While the recurrence (3), generating function (4), and asymptotic result (5) are satisfying, a closed form for $a_n$ might also be desired. For the sake of completeness, we demonstrate such a closed form here.

To calculate

$$a_n = \sum_{k\geq 1} \frac{k^n F_k}{2^{k+1}},$$

we first recall the Binet formula for $F_k$ [3]:

$$F_k = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right) \tag{6}$$

Then (6) implies that (1) can be rewritten as

$$a_n = \frac{1}{2\sqrt{5}}\sum_{k\geq 1} k^n \left(\frac{1+\sqrt{5}}{4}\right)^k - \frac{1}{2\sqrt{5}}\sum_{k\geq 1} k^n \left(\frac{1-\sqrt{5}}{4}\right)^k. \tag{7}$$

Next, we remember the formula for the geometric series:

$$\sum_{k\geq 0} x^k = \frac{1}{1-x} \tag{8}$$

This holds for all real numbers $x$ such that $|x| < 1$. We now apply the $x\frac{d}{dx}$ operator $n$ times to (8). It is clear that the left-hand side of (8) will then become

$$\sum_{k\geq 1} k^n x^k.$$

The right-hand side of (8) is transformed into the rational function

$$\frac{1}{(1-x)^{n+1}} \times \sum_{j=1}^{n} e(n,j)x^j, \tag{9}$$

where the coefficients $e(n,j)$ are the Eulerian numbers [2, Sequence A008292], defined by

$$e(n,j) = j \cdot e(n-1,j) + (n-j+1) \cdot e(n-1,j-1) \text{ with } e(1,1) = 1.$$

(The fact that these are indeed the coefficients of the polynomial in the numerator of (9) can be proved quickly by induction.) From the information found in [2, Sequence A008292], we know

$$e(n,j) = \sum_{\ell=0}^{j}(-1)^{\ell}(j-\ell)^n\binom{n+1}{\ell}.$$

Therefore,

$$\sum_{k\geq 1} k^n x^k = \frac{1}{(1-x)^{n+1}} \times \sum_{j=1}^{n} \left[ \sum_{\ell=0}^{j} (-1)^\ell (j-\ell)^n \binom{n+1}{\ell} \right] x^j. \tag{10}$$

Thus the two sums

$$\sum_{k\geq 1} k^n \left(\frac{1+\sqrt{5}}{4}\right)^k \text{ and } \sum_{k\geq 1} k^n \left(\frac{1-\sqrt{5}}{4}\right)^k$$

that appear in (7) can be determined explicity using (10) since

$$\left|\frac{1+\sqrt{5}}{4}\right| < 1 \text{ and } \left|\frac{1-\sqrt{5}}{4}\right| < 1.$$

Hence, an exact, non-recursive, formula for $a_n$ can be developed.

## REFERENCES


[1] A.T. Benjamin and J.J. Quinn. "Recounting Fibonacci and Lucas Identities." *College Mathematics Journal* **30.5** (1999): 359-366.

[2] N.J.A. Sloane. *The On-Line Encyclopedia of Integer Sequences*, published electronically at http://www.research.att.com/~njas/sequences/, 2000.

[3] S. Vajda. *Fibonacci and Lucas Numbers, and the Golden Section*, John Wiley and Sons, New York, 1989.

[4] H.S. Wilf. *Generatingfunctionology*, Academic Press, Boston, 1994.


AMS Classification Numbers: 11B39

# ON POSITIVE NUMBERS $n$ FOR WHICH $\Omega(n)$ DIVIDES $F_n$


**Florian Luca**

IMATE de la UNAM, Ap. Postal 61-3 (Xangari), CP 58 089, Morelia, Michoacán, México
e-mail: fluca@matmor.unam.mx



*(Submitted June 4, 2001)*


## 1. INTRODUCTION

Let $n$ be a positive integer $n$ and let $\omega(n)$, $\Omega(n), \tau(n)$, $\phi(n)$ and $\sigma(n)$ be the classical arithmetic functions of $n$. That is, $\omega(n)$, $\Omega(n)$, and $\tau(n)$ count the number of distinct prime divisors of $n$, the total number of prime divisors of $n$, and the number of divisors of $n$, respectively, while $\phi(n)$ and $\sigma(n)$ are the Euler function of $n$ and the sum of divisors function of $n$ respectively.

A lot of interest has been expressed in investigating the asymptotic densities of the sets of $n$ for which one of the "small" arithmetic functions of $n$ divides some other arithmetic function of $n$. For example, in [2], it was shown that the set of $n$ for which $\omega(n)$ divides $n$ is of asymptotic density zero. This result was generalized in [4]. The formalism from [4] implies, in particular, that the set of $n$ for which either $\Omega(n)$ or $\tau(n)$ divide $n$ is also of asymptotic density zero. On the other hand, in [1] it is shown that $\tau(n)$ divides $\sigma(n)$ for almost all $n$ and, in fact, it can be shown that all three numbers $\omega(n)$, $\Omega(n)$ and $\tau(n)$ divide both $\phi(n)$ and $\sigma(n)$ for almost all $n$.

In this note, we look at the set of positive integers $n$ for which one of the small arithmetic functions of $n$ divides $F_n$ or $L_n$. Here, $F_n$ and $L_n$ are the $n^{th}$ Fibonacci numbers and the $n^{th}$ Lucas number, respectively. We have the following result:

**Theorem:**

*The set of $n$ for which either one of the numbers $\omega(n)$, $\Omega(n)$ or $\tau(n)$ divides $F_{2n}$ is of asymptotic density zero.*

Since $F_{2n} = F_n L_n$ for all $n \geq 0$, it follows that for most $n$, none of the numbers $\omega(n)$, $\Omega(n)$ or $\tau(n)$ divides either $F_n$ or $L_n$. Following our method of proof, we can easily generalize the above Theorem to the case when the Fibonacci sequence is replaced by any Lucas or Lehmer sequence. We believe that the above Theorem should hold with the Fibonacci sequence replaced by any non-degenerate linearly recurrent sequence but we have not worked out the details of this statement.

## 2. PRELIMINARY RESULTS

Throughout the proof, we denote by $c_1, c_2, \ldots$ computable constants which are absolute. For a positive integer $k$ and a large positive real number $x$ we let $\log_k(x)$ to be the composition of the natural logarithm with itself $k$ times evaluated in $x$. Finally, assume that $\delta(x)$ is any function defined for large positive values of $x$ which tends to infinity with $x$. We use $p$ to denote a prime number. We begin by pointing out a "large" asymptotic set of positive integers $n$.

**Lemma 1**:

*Let $x$ be a large real number and let $A(x)$ be the set of all positive integers $n$ satisfying the following conditions*:

1. $\sqrt{x} < n < x$;
2. $|\omega(n) - \log_2(x)| < \delta(x)(\log_2(x))^{1/2}$ and $|\Omega(n) - \log_2(x)| < \delta(x)(\log_2(x))^{1/2}$;
3. *Write* $n = \prod_{p|n} p^{\alpha_p}$. *Then,* $\max_{p|n}(\alpha_p) < \log_3(x)$ *and if* $p > \log_3(x)$, *then* $\alpha_p = 1$.

*Then $A(x)$ contains all positive integers $n < x$ except for $o(x)$ of them.*

**The Proof of Lemma 1**:

1. Clearly, there are at most $\sqrt{x} = o(x)$ positive integers which do not satisfy 1.
2. By a result of Túran (see [6])

$$\sum_{n<x}(\omega(n) - \log_2(x))^2 = O(x\log_2(x)). \tag{1}$$

Thus, the inequality

$$|\omega(n) - \log_2(x)| < \frac{1}{2}\delta(x)(\log_2(x))^{1/2} \tag{2}$$

holds for all $n < x$ except for $O(\frac{x}{\delta(x)}) = o(x)$ of them. This takes care of the first inequality asserted at 2. For the second inequality here, we use the fact

$$\sum_{n<x}(\Omega(n) - \omega(n)) = O(x). \tag{3}$$

By (3), it follows that the inequality

$$\Omega(n) - \omega(n) < \frac{1}{2}\delta(x)(\log_2(x))^{1/2} \tag{4}$$

holds for all $n < x$ except for $O(\frac{x}{\delta(x)(\log_2(x))^{1/2}}) = o(x)$ of them. Inequalities (2) and (4) now tell us that

$$|\Omega(n) - \log_2(x)| < \delta(x)(\log_2(x))^{1/2} \tag{5}$$

holds for all $n < x$ except for $o(x)$ of them.

3. Assume first that $n$ is divisible by some prime power $p^\alpha$ with $\alpha \geq \log_3(x)$. Then, the number of such $n < x$ is certainly at most

$$\sum_p \frac{x}{p^{\log_3(x)}} < x(\zeta(\log_3(x)) - 1) = O\left(\frac{x}{2^{\log_3(x)}}\right) = o(x). \tag{6}$$

Here, we used $\zeta$ to denote the classical Riemann zeta function.

Finally, assume that $n$ is divisible by a square of a prime $p > \log_3(x)$. Then, the number of such $n < x$ is at most

$$\sum_{\log_3(x)<p} \frac{x}{p^2} = O\left(\frac{x}{\log_3(x)\log_4(x)}\right) = o(x). \tag{7}$$

Thus, $A(x)$ contains all positive integers $n < x$ but for $o(x)$ of them.

In what follows, for a positive integer $n$ we denote by $z(n)$ the *order of apparition of n* in the Fibonacci sequence; that is, $z(n)$ is the smallest positive integer $n$ for which $n|F_{z(n)}$. In the next Lemma, we recall a few well-known facts about $z(n)$.

**Lemma 2:**

1. *There exist two constants $c_1$ and $c_2$ such that*

$$c_1 \log n < z(n) < c_2 n \log_2(n) \quad \text{for all } n \geq 3. \tag{8}$$

2. $z(2^s) = 3 \cdot 2^{s-2}$*for all* $s \geq 3$.

**The Proof of Lemma 2:**

1. Let $\gamma_1 = \frac{1+\sqrt{5}}{2}$ be the golden section and let $\gamma_2 = \frac{1-\sqrt{5}}{2}$ be its conjugate. Since

$$F_n = \frac{\gamma_1^n - \gamma_2^n}{\gamma_1 - \gamma_2} \quad \text{for all } n \geq 0 \tag{9}$$

it follows easily that

$$F_n < \gamma_1^n \tag{10}$$

holds for all $n \geq 0$. Hence, since $n|F_{z(n)}$, we get, in particular, that

$$n \leq F_{z(n)} < \gamma_1^{z(n)}. \tag{11}$$

Taking logarithms in (11) we get

$$c_1 \log n < z(n) \tag{12}$$

with $c_1 = \frac{1}{\log \gamma_1}$.

For the upper bound for $z(n)$, we recall that if

$$n = \prod_{p|n} p^{\alpha_p} \tag{13}$$

then,

$$z(n) = \mathrm{lcm}_{p|n}(z(p^{\alpha_p})). \tag{14}$$

Moreover, if $p$ is a prime, then

$$z(p)|p - \delta_p, \tag{15}$$

where $\delta_p = \left(\frac{p}{5}\right)$ is the Jacobi symbol of $p$ in respect to 5, and if $\alpha \geq 2$ is a positive integer, then

$$z(p^\alpha)|p^{\alpha-1}z(p). \tag{16}$$

Combining (14), (15) and (16), we get that

$$z(n) \leq \prod_{p|n} p^{\alpha_p - 1}(p+1) \leq \sigma(n) < c_2 n \log_2(n). \tag{17}$$

2. This is well-known (see, for example, [5]).

For a given positive integer $j$ and a positive large real number $x$ let

$$\rho_j(x) = \#\{n < x | \omega(n) = j\} \tag{18}$$

and

$$\pi_j(x) = \#\{n < x | \Omega(n) = j\}. \tag{19}$$

We shall need the following result:

**Lemma 3**:

*There exist two absolute constants $c_3$ and $c_4$ such that if $x > c_3$ and $j$ is any positive integer, then*

$$\max(\rho_j(x), \pi_j(x)) < \frac{c_4 x}{(\log_2(x))^{1/2}}. \tag{20}$$

**The Proof of Lemma 3**: This is well-known (see [3], page 303).

We are now ready to prove the Theorem.

## 3. THE PROOF OF THE THEOREM

We assume that $x$ is large and that $n \in A(x)$, where $A(x)$ is the set defined in Lemma 1 for some function $\delta$.

Throughout the proof, we assume that $\delta(x)$ is any function tending to infinity with $x$ slower than $(\log_2(x))^{1/2}$; that is

$$\lim_{x \to \infty} \frac{\delta(x)}{(\log_2(x))^{1/2}} = 0. \tag{21}$$

We first treat the easiest case, namely $\tau(n) | F_{2n}$. Since $n \in A(x)$, it follows that

$$\omega(n) > \frac{1}{2} \log_2(x) \tag{22}$$

holds for $x$ large enough. Now write

$$n_1 = \prod_{p|n,\ p<\log_3(x)} p^{\alpha_p}$$

and

$$n_2 = \prod_{p|n,\ p \geq \log_3(x)} p.$$

Clearly, $n = n_1 n_2, n_1$ and $n_2$ and coprime and $n_2$ is square-free, therefore

$$\omega(n_2) = \omega(n) - \omega(n_1) > \frac{1}{2} \log_2(x) - \pi(\log_3(x)) > \frac{1}{3} \log_2(x), \tag{23}$$

where the last inequality in (23) holds for $x$ large enough. Now notice that

$$\tau(n) = \tau(n_1)\tau(n_2) = 2^{\omega(n_2)}\tau(n_1). \tag{24}$$

Thus, if $\tau(n)|F_{2n}$, we get, in particular, that $2^{\omega(n_2)}|F_{2n}$, whence $z(2^{\omega(n_2)})|2n$. By inequality (23) and Lemma 2, it follows that if we denote by $\alpha_2$ the exponent at which 2 divides $n$, then

$$\alpha_2 > \omega(n_2) - 3 > \frac{1}{3}\log_2(x) - 3. \tag{25}$$

The expression appearing in the right hand side of inequality (25) is larger than $\log_3(x)$ for large $x$, contradicting the fact that $n \in A(x)$. Thus, if $x$ is large and $n \in A(x)$, then $\tau(n)$ cannot divide $F_{2n}$.

We now treat the cases in which $\omega(n)$ or $\Omega(n)$ divides $F_{2n}$. As the reader will see, the key ingredients for these proofs are the fact that $n$ satisfies both condition 2 of Lemma 1 as well as Lemma 3, and both these results are symmetric in $\omega(n)$ and $\Omega(n)$. Thus, we shall treat in detail only the case in which $\omega(n)$ divides $F_{2n}$.

We fix a positive integer $j$ such that

$$|j - \log_2(x)| < \delta(x)(\log_2(x))^{1/2} \tag{26}$$

and we find an upper bound for the set of $n \in A(x)$ for which $\omega(n) = j$ and $j|F_{2n}$. Since $j|F_{2n}$, it follows that

$$2n = z(j)m, \tag{27}$$

for some positive integer $m$. Assume first that $n$ is odd. In this case,

$$j + 1 = \omega(2n) = \omega(mz(j)) = \omega(m) + \omega(z(j)) - s, \quad \text{where } s = \omega(\gcd(m, z(j))). \tag{28}$$

We now notice that by inequality (26) and Lemma 2,

$$c_5\log_3(x) < z(j) < c_6\log_2(x)\log_4(x) \tag{29}$$

holds for all $x$ large enough and uniformly in $j$. In particular,

$$s \le \omega(z(j)) < c_7\log(z(j)) < c_8\log_3(x) \tag{30}$$

holds for $x$ large enough and uniformly in $j$. Assume that $s$ is a fixed number in the set $\{0, 1, \ldots, \omega(z(j))\}$. Then

$$m = \frac{2n}{z(j)} < \frac{2x}{z(j)} \tag{31}$$

is a number with the property that

$$\omega(m) = j + 1 - \omega(z(j)) + s \tag{32}$$

is fixed. Moreover, it is easy to see that

$$x^{1/2} < \frac{2x}{c_6 \log_2(x) \log_4(x)} < \frac{2x}{z(j)} < \frac{2x}{c_5 \log_3(x)} < x. \tag{33}$$

Now Lemma 3 together with inequality (33) implies that the number of numbers $m < \frac{2x}{z(j)}$ for which $\omega(m)$ is given by formula (32) for fixed $j$ and $s$ is at most

$$\frac{c_9 x}{z(j)(\log_2(x))^{1/2}} \tag{34}$$

and this bound is uniform in $j$ and $s$ when $x$ is large. We now let $s$ vary and we get that the number of odd $n \in A(x)$ for which $\omega(n) = j$ and $j|F_{2n}$ is bounded above by

$$\frac{c_9(x(\omega(z(j)) + 1)}{z(j)(\log_2(x))^{1/2}} < \frac{c_{10} x \log(z(j))}{z(j)(\log_2(x))^{1/2}}. \tag{35}$$

We now use inequality (29) to conclude that (35) is bounded above by

$$\frac{c_{11} x \log_4(x)}{\log_3(x)(\log_2(x))^{1/2}}. \tag{36}$$

A similar analysis can be done to count the number of even $n \in A(x)$ for which $\omega(n) = j$ and $j|F_{2n}$. Thus, the total number of $n \in A(x)$ for which $\omega(n) = j$ and $j|F_{2n}$ is bounded above by

$$\frac{c_{12} x \log_4(x)}{\log_3(x)(\log_2(x))^{1/2}} \tag{37}$$

for large $x$ and uniformly in $j$. Since $j = \omega(n)$ satisfies (26), it follows that $j$ can take at most $2\delta(x)(\log_2(x))^{1/2} + 1$ values. Thus, the totality of $n \in A(x)$ for which $\omega(n)|F_{2n}$ is certainly not more than

$$\frac{c_{13} x \log_4(x) \delta(x)}{\log_3(x)}. \tag{38}$$

It now suffices to observe that one can choose $\delta(x)$ such that the function appearing at (38) is $o(x)$. For example, one can choose $\delta(x) = \frac{\log_3(x)}{\log_4(x)^2}$ and then the last expression appearing in (38) is $O(\frac{x}{\log_4(x)}) = o(x)$.

This shows that the set of $n$ for which $\omega(n)|F_{2n}$ is of asymptotic density zero. As we mentioned before, a similar analysis can be done to treat the case in which $\Omega(n)|F_{2n}$. The Theorem is therefore proved.

## 4. REMARKS

One may ask what about the set of positive integers $n$ for which one of the "large" arithmetic functions of $n$, i.e. $\phi(n)$ or $\sigma(n)$ divides $F_n$ or $L_n$. The answer is that the sets of these $n$ have all asymptotic densities zero, and this follows easily from our Theorem combined with the fact that both $\phi(n)$ and $\sigma(n)$ are divisible by all three numbers $\omega(n)$, $\Omega(n)$ and $\tau(n)$

for almost all $n$. If instead of considering whether or not $F_n$ is a multiple of some other function of $n$, one looks at $F_{\phi(n)}$ or $F_{\sigma(n)}$, then one can show that both $F_{\phi(n)}$ and $F_{\sigma(n)}$ are divisible by all three numbers $\omega(n)$, $\Omega(n)$, $\tau(n)$ for almost all $n$. We do not give more details.

## ACKNOWLEDGMENTS

I would like to thank Carl Pomerance for helpful advice and for suggestions which have improved the quality of this manuscript.

## REFERENCES

[1] P.T. Bateman, P. Erdős, C. Pomerance, E.G. Straus. "The Arithmetic Mean of the Divisors of an Integer." *Analytic Number Theory*, Philadelphia, PA, 1980, Lecture notes in Math. **899** (1981): 197-220.

[2] C.N. Cooper & R.E. Kennedy. "Chebyshev's Inequality and Natural Density." *American Math. Monthly* **96** (1989): 118-124.

[3] P.D.T.A. Elliott. "Probabilistic Numbers Theory II." Springer-Verlag, New York, 1980.

[4] P. Erdös & C. Pomerance. "On a Theorem of Besicovitch: Values of Arithmetical Functions that Divide Their Arguments." *Indian J. of Math.* **32** (1990): 279-287.

[5] T. Lengyel. "The Order of the Fibonacci and Lucas Numbers." *The Fibonacci Quarterly* **33** (1995): 234-239.

[6] P. Túran. "On the Theorem of Hardy and Ramanujan." *J. London Math. Soc.* **9** (1934): 274-276.

AMS Classification Numbers: 11K65, 11N25

✠ ✠ ✠

# SUMS AND DIFFERENCES OF VALUES OF A QUADRATIC POLYNOMIAL

**Alan F. Beardon**
Centre for Mathematical Sciences, Cambridge CB3 0WB, England
*(Submitted May 2001-Final Revision January 2002)*

## 1. INTRODUCTION

Let $P$ be a quadratic polynomial with integer coefficients. Motivated by a series of results on polygonal numbers (which we describe below) we consider the existence of integers $a, b, c, d$ and $n$ such that

$$P(n) = P(a) + P(b) = P(c) - P(d), \qquad P(a)P(b)P(c)P(d) \neq 0. \tag{1}$$

The simplest example of a polynomial $P$ for which (1) has infinitely many solutions is $P(x) = x^2$, for $(3m)^2 + (4m)^2 = (5m)^2 = (13m)^2 - (12m)^2$ for every $m$. Now $x^2 = P_4(x)$ where, for each integer $N$ with $N \geq 3$, $P_N(n)$ is the *polygonal number* $(N-2)n^2/2 - (N-4)n/2$. In 1968 Sierpinski [5] showed that there are infinitely many solutions to (1) when $P = P_3$, and this was subsequently extended to include the cases $P_5$, $P_6$ and $P_7$ (see [2], [4] and [3], respectively). In 1981 S. Ando [1] showed that there are infinitely many solutions to (1) when $P(x) = Ax^2 + Bx$, where $A$ and $B$ are integers with $A - B$ even, and this implies that, for each $N$, (1) has infinitely many solutions when $P = P_N$.

It is easy to find polynomials $P$ for which (1) has no solutions (for example, if $P(n)$ is odd for every $n$), and this leads to the problem of characterizing those $P$ for which (1) has infinitely many solutions. This problem has nothing to do with polygonal numbers, and here we prove the following result.

**Theorem 1:** *Suppose that $P(x) = Ax^2 + Bx + C$, where $A$, $B$ and $C$ are integers, and $A \neq 0$.*

(i) *If $8A^2$ divides $P(k)$ for some integer $k$, then there are infinitely many $n$ such that (1) holds for some integers $a$, $b$, $c$ and $d$.*

(ii) *If $\gcd(A, B)$ does not divide $C$ then there are no integer solutions to (1).*

Theorem 1(i) is applicable when $P(0) = 0$, and this special case implies Ando's result. As illustrations of Theorem 1 we note that (1) has infinitely many solutions when $P(x) = x^2+2x+5$ (because $P(1) = 8$), but no solutions when $P(x) = 6x^2+3x+5$. Not every quadratic polynomial is covered by Theorem 1; for example, $x^2 + 2x + 4$ is not (to check that 8 does not divide $P(k)$ for any $k$ it suffices to consider $k = 0, 1, \ldots, 7$). In fact, if $P(x) = x^2 + 2x + 4$, then $P(u+1) - P(u) = 2u + 3$, and it follows from this that for all $k$,

$$\begin{aligned} P(2k^2) + P(2k-1) &= P(2k^2+1) \\ &= P(2k^4 + 4k^2 + 3) - P(2k^4 + 4k^2 + 2). \end{aligned}$$

The existence of solutions of (1) may have something to do with Diophantine equations; for example, if $P(x) = x^2 - 4x + 3$, then $P(x+2) = P(y+1) + P(y+3)$ is equivalent to Pell's equation $x^2 - 2y^2 = 1$. This link with Diophantine equations suggests perhaps that there may be no simple criterion for (1) to have infinitely many solutions.

## 2. THE PROOF

The proof of (i) is based on the following observation.

**Lemma 2:** *Let p be any polynomial with integer coefficients. Suppose that there are non-constant polynomials $t$, $u$, $v$ and $w$ with integer coefficients such that $u(w(x)) = v(t(x)) + 1$ and $P(v(x)+1) - P(v(x)) = P(u(x))$. Then there exist infinitely many $n$ such that* (1) *holds for some integers $a$, $b$, $c$ and $d$.*

**Proof:** It is easy to see that if, for any integer $x$, we put $n = u(w(x))$, $a = v(t(x))$, $b = u(t(x))$, $c = v(w(x)) + 1$ and $d = v(w(x))$ then (1) holds.

*The Proof of (i):* First, we show that the conclusion of (i) holds if $8A^2$ divides $P(0)(= C)$. Let $u(x) = 1 + 4Ax$ and $v(x) = 8A^2x^2 + (4A + 2B)x + C/2A$. Then $u$ and $v$ have integer coefficients and as is easily checked, $P(v(x)+1) - P(v(x)) = P(u(x))$. Next define $t(x) = 4Ax$ and $w(x) = v(4Ax)/4A$. The assumption that $8A^2$ divides $C$ implies that $w$ has integer coefficients, and by construction, $u(w(x)) = 1 + 4Aw(x) = v(t(x)) + 1$. The conclusion of (i) now follows from Lemma 2.

Now suppose that $8A^2$ divides $P(k)$, and let $Q(x) = P(x + k)$. Then $Q$ has leading coefficient $A$, and $8A^2$ divides $Q(0)$; thus there are infinitely many $n$ such that (1), with $P$ replaced by $Q$, holds for some $a$, $b$, $c$ and $d$. The conclusion of (i) follows immediately from this.

*The Proof of (ii):* If there are integers $n$, $a$ and $b$ such that $P(n) = P(b) - P(a)$, then there are integers $u$ and $v$ such that $Au + Bv = C$, and this implies that $\gcd(A, B)$ divides $C$, contrary to our assumption.

## REFERENCES


[1] S. Ando. "A Note on Polygonal Numbers." *The Fibonacci Quarterly* **19.2** (1981): 180-183.

[2] R.T. Hansen. "Arithmetic of Pentagonal Numbers." *The Fibonacci Quarterly* **8.1** (1970): 83-87.

[3] H.J. Hindin. "A Theorem Concerning Heptagonal Numbers." *The Fibonacci Quarterly* **18.3** (1980): 258-259.

[4] W.J. O'Donnell. "Two Theorems Concerning Hexagonal Numbers." *The Fibonacci Quarterly* **17.1** (1979): 77-79.

[5] W. Sierpinski. "Sur les Nombres Triangulaires Qui Sont Sommes De Deux Nombres Triangulaires." *Elem. Math.* **17** (1962): 63-65.


AMS Classification Numbers: 11D09

✠ ✠ ✠

## ELEMENTARY PROBLEMS AND SOLUTIONS

*Edited by*
**Russ Euler and Jawad Sadek**

*Please submit all new problem proposals and corresponding solutions to the Problems Editor, DR. RUSS EULER, Department of Mathematics and Statistics, Northwest Missouri State University, 800 University Drive, Maryville, MO 64468. All solutions to others' proposals must be submitted to the Solutions Editor, DR. JAWAD SADEK, Department of Mathematics and Statistics, Northwest Missouri State University, 800 University Drive, Maryville, MO 64468.*

*If you wish to have receipt of your submission acknowledged, please include a self-addressed, stamped envelope.*

*Each problem and solution should be typed on separate sheets. Solutions to problems in this issue must be received by February 15, 2004. If a problem is not original, the proposer should inform the Problem Editor of the history of the problem. A problem should not be submitted elsewhere while it is under consideration for publication in this Journal. Solvers are asked to include references rather than quoting "well-known results".*

### BASIC FORMULAS

The Fibonacci numbers $F_n$ and the Lucas numbers $L_n$ satisfy

$$F_{n+2} = F_{n+1} + F_n, \; F_0 = 0, \; F_1 = 1;$$

$$L_{n+2} = L_{n+1} + L_n, \; L_0 = 2, \; L_1 = 1.$$

Also, $\alpha = (1+\sqrt{5})/2$, $\beta = (1-\sqrt{5})/2$, $F_n = (\alpha^n - \beta^n)/\sqrt{5}$, and $L_n = \alpha^n + \beta^n$.

### PROBLEMS PROPOSED IN THIS ISSUE

**B-961 Proposed by Steve Edwards, Southern Polytechnic State University, Marietta, GA**

Show that $\frac{L_{n+1}}{\alpha^{n-1}} + \frac{L_n}{\alpha^n}$ is a constant for all nonnegative integers $n$.

**B-962 Proposed by Steve Edwards, Southern Polytechnic State University, Marietta, GA**

Find

$$\prod_{k=1}^{\infty} \frac{F_{2k}F_{2k+2} + F_{2k-1}F_{2k+2}}{F_{2k}F_{2k+2} + F_{2k}F_{2k+1}}.$$

**B-963 Proposed by Ovidiu Furdui, Western Michigan University, Kalamazoo, MI**

Prove that

$$\frac{F_{2n+1}-1}{F_{2n+4}-3F_{n+2}-L_{n+2}+3} \geq \frac{1}{n}$$

for all $n \geq 1$.

**B-964 Proposed by Stanley Rabinowitz, MathPro, Westford, MA**

Find a recurrence relation for $r_n = \frac{F_n}{L_n}$.

**B-965 Proposed by José Luis Díaz-Barrero and Juan José Egozcue, Universitat Politècnica de Catalunya, Barcelona, Spain**

Let $n$ be a positive integer. Prove that

$$\frac{F_n!(4F_{n+1})!}{(2F_n)!(F_{n-1}+F_{n+1})!(2F_{n+1})!}$$

is an integer.

## SOLUTIONS

### When Do they Converge?

**B-946 Proposed by Mario Catalani, University of Torino, Torino, Italy (Vol. 40, no. 5, November 2002)**

Find the smallest positive integer $k$ such that the following series converge and find the value of the sums:

$$1.\quad \sum_{i=1}^{\infty} \frac{i^2 F_i L_i}{k^i} \qquad 2. \sum_{i=1}^{\infty} \frac{iF_i^2}{k^i}$$

**Solution by Toufik Mansour, Chalmers University of Technology, Sweden.**

1. Using Lemma 3.2 in [1], we get

$$G(x) = \sum_{n \geq 0} F_n L_n x^n = \frac{x}{x^2-3x+1}.$$

It follows that

$$\sum_{n \geq 0} n^2 F_n L_n x^n = x\frac{\partial}{\partial x}\left(x\frac{\partial}{\partial x}G(x)\right) = \frac{x(x^4+3x^3-6x^2+3x+1)}{(x^2-3x+1)^3}.$$

Hence, the sum $\sum_{n\geq 0} n^2 F_n L_n x^n$ converge if and only if $|x| < \frac{1}{2}(3-\sqrt{5})$, which means $k > \frac{1}{2}(3+\sqrt{5})$. Therefore, the smallest positive integer k such that (1) converges is $k = 3$. In this case the sum (1) equals 354.

2. Using Corollary 3.5 in [1], we get

$$H(x) = \sum_{n\geq 0} F_n^2 x^n = \frac{x(1-x)}{(1+x)(1-3x+x^2)}.$$

It follows that

$$\sum_{n\geq 0} nF_n^2 x^n = x\frac{\partial}{\partial x}H(x) = \frac{(1-2x-2x^3+x^4+4x^2)x}{(1+x)^2(1-3x+x^2)^2}.$$

Hence, the sum $\sum_{n\geq 0} nF_n^2 x^n$ converges when $|x| < \frac{1}{2}(3-\sqrt{5})$, which means $k > \frac{1}{2}(3+\sqrt{5})$. Thererore, the smallest positive integer $k$ such that (2) converges is $k = 3$. In this case, the sum (2) equals $\frac{87}{8}$. $\square$

P.S. It is easy to prove by induction that the sums $\sum_{i\geq 1} i^m F_i L_i x^i$ and $\sum_{i\geq 1} i^m F_i^2 x^i$ converge for all $x$ such that $|x| < \frac{1}{2}(3-\sqrt{5})$ (maximum domain), for all $m \geq 1$.

REFERENCES

[1] P. Haukkanen. "A Note on Horadam's Sequence." *The Fibonacci Quarterly* **40.4** (20002): 358-361.

**Also solved by Paul Bruckman, Charles Cook, Kenneth Davenport, L.G. Dresel, Ovidiu Furdiu, Walther Janous, Harris Kwang, David Manes, James Sellers, and the proposer.**

## Integral and Nonsquare!

**B-947 Proposed by Stanley Rabinowitz, MathPro Press, Westford, MA (Vol. 40, no. 5, November 2002)**

(a) Find a nonsquare polynomial $f(x,y,z)$ with integer coefficients such that $f(F_n, F_{n+1}, F_{n+2})$ is a perfect square for all $n$.

(b) Find a nonsquare polynomial $g(x,y)$ with integer coefficients such that $g(F_n, F_{n+1})$ is a perfect square for all $n$.

**Solution by Paul Bruckman, Berkeley, CA and Walther Janous, Ursulinengymnasium, Innsbruck, Austria (separately).**

We begin with the well-known "Wronskian" identity:

$$F_{n+1}F_{n-1} - (F_n)^2 = (-1)^n \tag{1}$$

Two alternative forms of this identity are the following:

$$(F_{n+1})^2 - F_{n+1}F_n - (F_n)^2 = (-1)^n \tag{2}$$

$$(F_{n+1})^2 - F_{n+2}F_n = (-1)^n \tag{3}$$

This suggests the following solution for Part (a):

$$f(x,y,z) = (y^2 - xz)(y^2 - xy - x^2) = y^4 - xy^3 - x^2y^2 - xy^2z + x^2yz + x^3z \tag{4}$$

We see from (2) and (3) that with this $f$, we have: $f(F_n, F_{n+1}, F_{n+2}) = 1$, which is certainly a perfect square for all $n$.

Also, using (2), we may take the following solution for Part (b):

$$g(x,y) = (y^2 - xy - x^2 + 1)(y^2 - xy - x^2 - 1) = y^4 - 2xy^3 - x^2y^2 + 2x^3y + x^4 - 1 \tag{5}$$

It is easily checked that $g(F_n, F_{n+1}) = 0$ for all $n$, which is again a perfect square.
**Also solved by Peter Anderson, Michel Ballieu, L.G. Dresel, Ovidiu Furdui (part (a)), David Manes, and the proposer.**

## A Series Inequality

**B-948 Proposed by José Luis Díaz-Barrero and Juan José Egozcue, Universitat Politècnica de Catalunya, Barcelona, Spain**
**(Vol. 40, no. 5, November 2002)**

Let $\ell$ be a positive integer greater than or equal to 2. Show that, for $x > 0$,

$$\log_{F_{\ell+1}F_{\ell+2}\ldots F_{\ell+n}} x^{n^2} \le \sum_{k=1}^{n} \log_{F_{\ell+k}} x.$$

**Remark.** The condition on $x$ should be $x > 1$. For example, the inequality fails when $n = \ell = 2$ (try, for instance, $x = 1/6$). The proof below shows why we need $x > 1$.

**Solution by Harris Kwong, SUNY College at Fredonia, Fredonia, NY.**

It follows from Cauchy-Schwarz inequality that

$$n^2 = \left(\sum_{k=1}^{n} \sqrt{\ln F_{\ell+k}} \cdot \frac{1}{\sqrt{\ln F_{\ell+k}}}\right)^2 \le \left(\sum_{k=1}^{n} \ln F_{\ell+k}\right)\left(\sum_{k=1}^{n} \frac{1}{\ln F_{\ell+k}}\right).$$

For $x > 1$, we have $\ln x > 0$. Hence

$$\frac{n^2 \ln x}{\ln F_{\ell+1}F_{\ell+2}\ldots F_{\ell+n}} \le \sum_{k=1}^{n} \frac{\ln x}{\ln F_{\ell+k}},$$

which completes the proof, because $\ln x / \ln a = \log_a x$ for any $a > 0$.

**Also solved by Paul Bruckman, Mario Catalani, L.G. Dresel, Ovidiu Furdui, Walther Janous, H.-J. Seiffert, and the proposer.**

## Couples Congruence

**B-949 Proposed by N. Gauthier, Royal Military College of Canada (Vol. 40, no. 5, November 2002)**

For $l$ and $n$ positive integers, find closed form expressions for the following sums,

$$S_1 \equiv \sum_{k=1}^{n} 3^{n-k} F^3_{3^k \cdot 2l} \text{ and } S_2 \equiv \sum_{k=1}^{n} 3^{n-k} L^3_{3^k \cdot (2l+1)}.$$

**Solution by Mario Catalini, University of Torino, Torino, Italy**

We will use the following identities:

$$5F_n^3 = F_{3n} - 3(-1)^n F_n, \tag{1}$$

$$L_n^3 = L_{3n} + 3(-1)^n L_n. \tag{2}$$

$$\sum_{k=1}^{n} 3^{n-k} F^3_{3^k \cdot 2l} = 3^{n-1} F^3_{3 \cdot 2l} + 3^{n-2} F^3_{3^2 \cdot 2l} + 3^{n-3} F^3_{3^3 \cdot 2l} + \cdots + 3F^3_{3^{n-1} \cdot 2l} + F^3_{3^n \cdot 2l}.$$

Using identity (1) and the fact that the subscript is always an even number we get

$$\begin{aligned} 5S_1 = 3^{n-1}[F_{3^2 \cdot 2l} - 3F_{3 \cdot 2l}] + 3^{n-2}[F_{3^3 \cdot 2l} - 3F_{3^2 \cdot 2l}] + 3^{n-3}[F_{3^4 \cdot 2l} - 3F_{3^3 \cdot 2l}] \\ + \cdots + 3[F_{3^n \cdot 2l} - 3F_{3^{n-1} \cdot 2l}] + [F_{3^{n+1} \cdot 2l} - 3F_{3^n \cdot 2l}]. \end{aligned}$$

Because of a telescopic effect we obtain simply

$$5S_1 = -3^n F_{3 \cdot 2l} + F_{3^{n+1} \cdot 2l}.$$

For the second summation we have

$$\sum_{k=1}^{n} 3^{n-k} L^3_{3^k \cdot (2l+1)} = 3^{n-1} L^3_{3 \cdot (2l+1)} + 3^{n-2} L^3_{3^2 \cdot (2l+1)} + 3^{n-3} L^3_{3^3 \cdot (2l+1)} + \ldots$$

$$+ 3L^3_{3^{n-1} \cdot (2l+1)} + L^3_{3^n \cdot (2l+1)}.$$

Using identity 2 and the fact that the subscript is always an odd number we get

$$S_2 = 3^{n-1}\left[L_{3^2\cdot(2l+1)} - 3L_{3\cdot(2l+1)}\right] + 3^{n-2}\left[L_{3^3\cdot(2l+1)} - 3L_{3^2\cdot(2l+1)}\right]$$
$$+ 3^{n-3}\left[L_{3^4\cdot(2l+1)} - 3L_{3^3\cdot(2l+1)}\right] + \dots$$
$$+ 3\left[L_{3^n\cdot(2l+1)} - 3L_{3^{n-1}\cdot(2l+1)}\right] + \left[L_{3^{n+1}\cdot(2l+1)} - 3L_{3^n\cdot(2l+1)}\right].$$

Because of a telescopic effect we obtain

$$S_2 = -3^n L_{3\cdot(2l+1)} + L_{3^{n+1}\cdot(2l+1)}.$$

**Also solved by Paul Bruckman, H.-J. Seiffert, and the proposer.**

## Primes $\cdots$ Again

**B-950 Proposed by Paul S. Bruckman, Berkeley, CA**
**(Vol. 40, no. 5, November 2002)**

For all primes $p > 2$, prove that

$$\sum_{k=1}^{p-1} \frac{F_k}{k} \equiv 0 \pmod{p},$$

where $\frac{1}{k}$ represents the residue $k^{-1} \pmod{p}$.

H.J. Seiffert refers the reader to part (b) of problem H-545 in *The Fibonacci Quarterly* **38.2** (2000): 187-188 and Kenneth B. Davenport quotes Corollary 4 of "Equivalent Conditions for Fibonacci and Lucas Pseudoprimes which Contain a Square Factor," *Pi Mu Epsilon Journal* **10.8** Spring 1988, 634-642.

**Also solved by L.G. Dresel and the proposer.**

# ADVANCED PROBLEMS AND SOLUTIONS

*Edited by*
**Florian Luca**

*Please send all communications concerning ADVANCED PROBLEMS AND SOLUTIONS to FLORIAN LUCA, IMATE, UNAM, AP. POSTAL 61-3 (XANGARI), CP 58 089, MORELIA, MICHOACAN, MEXICO, or by e-mail at fluca@matmor.unam.mx as files of the type tex, dvi, ps, doc, html, pdf, etc. This department especially welcomes problems believed to be new or extending old results. Proposers should submit solutions or other information that will assist the editor. To facilitate their consideration, all solutions sent by regular mail should be submitted on separate signed sheets within two months after publication of the problems.*

## PROBLEMS PROPOSED IN THIS ISSUE

**H-599 Proposed by the Editor**

For every $n \geq 0$ let $C_n := \frac{1}{n+1}\binom{2n}{n}$ be the $n$th Catalan number. Show that all the solutions of the diophantine equation $F_m = C_n$ have $m \leq 5$.

**H-600 Proposed by Arulappah Eswarathasan, Hofstra University, Hempstead, NY**

The Pseudo-Fibonacci numbers $u_n$ are defined by $u_1 = 1$, $u_2 = 4$ and $u_{n+2} = u_{n+1} + u_n$. A number of the form $3s^2$, where $s$ is an integer, is called a one-third square. Show that $u_0 = 3$ and $u_{-4} = 12$ are the only one-third squares in the sequence.

**H-601 Proposed by Walther Janous, Ursulinengymnasium, Innsbruck, Austria**

Prove or disprove that the sequence

$$\left\{\frac{\sqrt[n]{L_2 \cdot \ldots \cdot L_{n+1}}}{\alpha^{(n+3)/2}}\right\}_{n\geq 1}$$

strictly decreases to its limit 1. Here, $\alpha$ is the golden section.

**H-602 Proposed by Ovidiu Furdui, Western Michigan University, Kalamazoo, MI**

Find the limit

$$\lim_{n\to\infty} \frac{\Gamma\left(-k\frac{F_{n+1}}{\alpha F_n}\right)}{\Gamma\left(-\ell\frac{L_{n+1}}{\alpha L_n}\right)},$$

where $k$ and $\ell$ are fixed positive integers, $\Gamma$ is the Euler function, and $\alpha$ is the golden section.

## SOLUTIONS

### Sums of consecutive Fibonacci numbers

**H-588 Proposed by José Luis Díaz-Barrero & Juan José Egozcue, Barcelona, Spain**

Let $n$ be a positive integer. Prove that

$$\sum_{k=1}^{n} F_{k+2} \geq \frac{n^{n+1}}{(n+1)^n} \prod_{k=1}^{n} \left\{ \frac{L_{k+1}^{\frac{n+1}{n}} - F_{k+1}^{\frac{n+1}{n}}}{L_{k+1} - F_{k+1}} \right\}.$$

**Solution by H.-J. Seiffert, Berlin, Germany**

Direct computation shows that equality holds with $n = 1$. Now, suppose that $n \geq 2$. If $a$ and $b$ are real numbers such that $b > a > 0$, then, by Hölder's Inequality,

$$\int_a^b t^{\frac{1}{n}} dt \leq \left( \int_a^b t dt \right)^{\frac{1}{n}} \left( \int_a^b dt \right)^{\frac{n-1}{n}},$$

or, equivalently,

$$\frac{n}{n+1} \cdot \frac{b^{\frac{n+1}{n}} - a^{\frac{n+1}{n}}}{b-a} \leq \left( \frac{a+b}{2} \right)^{\frac{1}{n}}.$$

Applying this inequality with $a := F_{k+1}$ and $b := L_{k+1}$, noting that $F_{k+1} + L_{k+1} = 2F_{k+2}$, and taking the product over $k = 1, \ldots, n$, gives

$$\frac{n^n}{(n+1)^n} \prod_{k=1}^{n} \left\{ \frac{L_{k+1}^{\frac{n+1}{n}} - F_{k+1}^{\frac{n+1}{n}}}{L_{k+1} - F_{k+1}} \right\} \leq \left( \prod_{k=1}^{n} F_{k+2} \right)^{\frac{1}{n}}.$$

By the Arithmetic-Geometric Mean Inequality, we have

$$n \left( \prod_{k=1}^{n} F_{k+2} \right)^{\frac{1}{n}} \leq \sum_{k=1}^{n} F_{k+2},$$

and the desired inequality follows.

**Also solved by Paul Bruckman, Walther Janous and the proposers.**

## Iterated Fibonacci numbers

**H-589 Proposed by Robert DiSario, Bryant College, Smithfield, RI**

Let $f(n) = F(F(n))$, where $F(n)$ is the $n^{\text{th}}$ Fibonacci number. Show that

$$f(n) = \frac{(f(n-1))^2 - (-1)^{F(n)}(f(n-2))^2}{f(n-3)}$$

for $n > 3$.

**Solution by L.A.G. Dresel, Reading, England**

We shall first prove the identity $F_{s+t}F_{s-t} = (F_s)^2 - (-1)^{s-t}(F_t)^2$, which corresponds to formula I (19) on page 59 of [1]. Using $\alpha\beta = -1$ and the Binet form for $F_n$, we have

$$5F_{s+t}F_{s-t} = (\alpha^{s+t} - \beta^{s+t})(\alpha^{s-t} - \beta^{s-t}) = \alpha^{2s} + \beta^{2s} - (\alpha\beta)^{s-t}(\alpha^{2t} + \beta^{2t})$$

$$= \alpha^{2s} - 2(\alpha\beta)^s + \beta^{2s} - (\alpha\beta)^{s-t}\{\alpha^{2t} - 2(\alpha\beta)^t + \beta^{2t}\} = 5\{(F_s)^2 - (-1)^{s-t}(F_t)^2\}.$$

Putting $s := F_{n-1}$ and $t := F_{n-2}$, we have $s + t = F_n$ and $s - t = F_{n-3}$, so that our identity takes the form $f(n)f(n-3) = (f(n-1))^2 - (-1)^{F(n-3)}(f(n-2))^2$. But since $F_n = 2F_{n-2} + F_{n-3}$ we have $(-1)^{F(n-3)} = (-1)^{F(n-1)}$, and for $n > 3$ we can divide by $f(n-3)$, which proves the given formula.

1. V.E. Hoggatt. "Fibonacci and Lucas numbers." Boston: Houghton Mifflin, 1969; rpt. Santa Clara, CA: The Fibonacci Association, 1979.

**Also solved by P. Bruckman, M. Catalani, O. Furdui, W. Janous, H. Kwong, V. Mathe, H.-J. Seiffert, J. Spilker and the proposer.**

## Arithmetic Functions of Fibonacci Numbers

**H-590 Proposed by Florian Luca, IMATE, UNAM, Morelia, Mexico**

For any positive integer $k$ let $\phi(k)$, $\sigma(k)$, $\tau(k)$, $\Omega(k)$, $\omega(k)$ be the Euler function of $k$, the sum of divisors function of $k$, the number of divisors function of $k$, and the number of prime divisors function of $k$ (where the primes are counted with or without multiplicity), respectively.

**1.** Show that $n|\phi(F_n)$ holds for infinitely many $n$.
**2.** Show that $n|\sigma(F_n)$ holds for infinitely many $n$.
**3.** Show that $n|\tau(F_n)$ holds for infinitely many $n$.
**4.** Show that for no $n > 1$ can $n$ divide either $\omega(F_n)$ or $\Omega(F_n)$.

**Solution by J.-Ch. Schlage-Puchta & J. Spilker, Albert-Ludwigs-Universität Freiburg, Germany**

We first prove a

**Lemma:** Let $f : \boldsymbol{N} \to \boldsymbol{Z}$ be multiplicative such that $f(p^k)$ is even for all primes $p > 2$ and all odd positive integers $k$. Then $2^n|f(F_{2^n})$ holds for every $n \geq 6$.

**Examples:**

**1.** The Euler function $\phi$ is multiplicative and $\phi(p^k) = p^{k-1}(p-1)$ is even if $p > 2$. This is part 1 of the Problem.

**2.** The sum of $j$th powers of divisors function $\sigma_j(n) = \sum_{d|n} d^j$, $j \geq 0$ is multiplicative and $\sigma_j(p^k) = 1 + p^j + \cdots + p^{(k-1)j}$ is even if both $p$ and $k$ are odd. The cases $j = 1$ and $j = 0$ are parts 2 and 3 of the Problem, respectively.

**Proof of the Lemma:** Define the multiplicative function

$$f^*(p^k) := \begin{cases} 1, & \text{if } p = 2, \\ f(p^k), & \text{if } p > 2. \end{cases}$$

Then $f^*(2^k n) = f^*(n)$ and $f^*(n)|f(n)$ hold for all positive integers $k$ and $n$. It suffices to show that

(1) $64|f^*(F_{64})$;

(2) if $n > 6$ and $n|f^*(F_n)$, then $2n|f^*(F_{2n})$.

Claim (1) above follows from the fact that $F_{64}$ is odd, squarefree, and has precisely 6 prime factors. For Claim (2) above, we use the facts that $F_{2n} = F_n L_n$ and $L_n^2 - 5F_n^2 = (-1)^n \cdot 4$. From the last formula, it follows that $\gcd(F_n, L_n)|2$. Thus, writing $2^a||F_n$ and $2^b||L_n$, we get

$$f^*(F_{2n}) = f^*(F_n L_n) = f^*\Big(\frac{F_n}{2^a} \cdot \frac{L_n}{2^b}\Big) = f^*\Big(\frac{F_n}{2^a}\Big) f^*\Big(\frac{L_n}{2^b}\Big) = f^*(F_n) f^*(L_n).$$

By the hypotheses of the Lemma, $f^*(L_n)$ is always even except when $L_n$ is a square or twice times a square. A result from [1] says that the only such values of $n$ are $n = 1,\ 3,\ 6$. Thus, if $n > 6$, then $f^*(L_n)$ is even, which completes the proof (2) and of the Lemma.

For part 4 of the Problem, assume that $n > 2$. Then $F_n > 1$, and so on the one hand writing the prime factorization of $F_n$ we get

$$F_n = \prod_j p_j^{k_j} \geq \prod_j 2^{k_j} = 2^{\sum_j k_j},$$

while on the other hand, by the Binet formula, we have

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \alpha^n \Big(\frac{1 - (\beta/\alpha)^n}{\sqrt{5}}\Big) < \alpha^n \cdot \frac{2}{\sqrt{5}} < \alpha^n < 2^n,$$

where $\alpha$ is the golden section and $\beta$ is its conjugate. Thus, $n > \sum_j k_j = \Omega(F_n) \geq \omega(F_n)$, which shows that $n$ cannot divide neither $\omega(F_n)$ nor $\omega(F_n)$.

1. J.H.E. Cohn. "Lucas and Fibonacci numbers and some Diophantine equations." Proc. Glasgow Math. Assoc. 7 (1965): 24-28.

**Editor's Remark:** All solutions used powers of 2 with exponent greater than or equal to 6 to settle parts 1–3 of the problem, and quoted the result from [1] above to the effect that $L_n$ is a perfect square only for $n = 1,\ 3$. However, one does not need the full strength of the result from [1] in this instance. Indeed, since $L_2 = 3$ and $L_{2^n} = L_{2^{n-1}}^2 - 2$ holds for all $n \geq 2$, it follows easily, by induction, that $L_{2^n} \equiv 3 \pmod 4$ holds for all $n \geq 1$, and as such these numbers cannot be perfect squares.

**Also solved P. Bruckman, V. Mathe and the proposer.**

**Please Send in Proposals!**

## The Eleventh International Conference on Fibonacci Numbers and their Applications

July 5 – July 9, 2004
Technical University Carolo-Wilhelmina,
Braunschweig, Germany

Local Organizer: H. Harborth
Conference Organizer: W. Webb

Call for Papers: The purpose of the conference is to bring together people from all branches of mathematics and science with interests in recurrence sequences, their applications and generalizations, and other special number sequences.

Deadline: Papers and abstracts should be submitted in duplicate to W. Webb by May 1, 2004 at:

Department of Mathematics
Washington State University
Pullman, WA 99164-3113
USA
Phone: 509-335-3150

Electronic submissions, preferably in AMS – TeX, sent to webb@math.wsu.edu

Local Information: Contact H. Harborth at
Diskrete Mathematik
TU Braunschweig
38023 Braunschweig, Germany
Phone: 49-531-3917515; 49-531-322213
h.harborth@tu-bs.de

International Committee: A. Adelberg (U.S.A.), M. Bicknell-Johnson (U.S.A.), C. Cooper (U.S.A.), Y. Horibe (Japan), A. Horadam (co-chair)(Australia), J. Lahr (Luxembourg), A.Philippou (co-chair)(Greece), G. Phillips (co-chair)(Scotland), A. Shannon (Australia), L. Somer (U.S.A.), J. Turner (New Zealand).

Local Committee: J-P. Bode, A. Kemnitz, H. Weiss

Information: www.mscs.dal.ca/fibonacci/eleventh.html
www.mathematik.tu-bs.de/dm/fibonacci

# SUSTAINING MEMBERS

*H.L. Alder
G.L. Alexanderson
P. G. Anderson
S. Ando
A.T. Benjamin
J.G. Bergart
G. Bergum
*M. Bicknell-Johnson
W. Blumberg
H. Bottcher
P.S. Bruckman
D. Callan
G.D. Chakerian
H. Chen
C.K. Cook
C. Cooper
M.J. DeBruin
M.J. DeLeon
J. De Kerf
E. Deutsch
L.A.G. Dresel
U. Dudley
M. Elia
L.G. Ericksen, Jr.
D.R. Farmer
D.C. Fielder
C.T. Flynn
E. Frost
N. Gauthier
*H.W. Gould
P. Hagis, Jr.
V. Hanning
H. Harborth
*A.F. Horadam
Y. Horibe
F.T. Howard
R.J. Howell
R.E. Kennedy
C.H. Kimberling
Y.H.H. Kwong
J.C. Lagarias
J. Lahr
*C.T. Long
G. Lord
F. Luca
W.L. McDaniel
F.U. Mendizabal
M.G. Monzingo
J.F. Morrison
E. Nenzell
H. Niederhausen
S.A. Obaid
T.J. Osler
A. Prince
D. Redmond
C. Reiter
B.F. Robertson
S. Sato
D.L. Schweizer
H.J Seiffert
A.G. Shannon
L.W. Shapiro
L. Somer
P. Spears
W.R. Spickerman
P.K. Stockmeyer
D.R. Stone
J. Suck
M.N.S. Swamy
*D. Thoro
J.C. Turner
N. Vallous
C. Vanden Eynden
T.P. Vaughan
J.N. Vitale
M.J. Wallace
J.E. Walton
W.A. Webb
V. Weber
R.E. Whitney

*Charter Members

# INSTITUTIONAL MEMBERS

BIBLIOTECA DEL SEMINARIO MATHEMATICO
*Padova, Italy*

CALIFORNIA STATE UNIVERSITY SACRAMENTO
*Sacramento, California*

FAHD PETRO MIN UNIVERSITY
*Dhahran, Saudi Arabia*

GONZAGA UNIVERSITY
*Spokane, Washington*

HOWELL ENGINEERING COMPANY
*Yucaipa, California*

ITHACA COLLEGE
*Ithaca, New York*

KLEPCO, INC.
*Reno, Nevada*

KOBENHAVNS UNIVERSITY MATEMATISK INSTITUT
*Copenhagen, Denmark*

SAN JOSE STATE UNIVERSITY
*San Jose, California*

SANTA CLARA UNIVERSITY
*Santa Clara, California*

UNIVERSITE DE MONTREAL
*Montreal, Quebec, Canada*

UNIVERSITY OF NEW ENGLAND
*Armidale, N.S.W. Australia*

UNIVERSITY OF PATRAS
*Patras, Greece*

WAKE FOREST UNIVERSITY
*Winston-Salem, North Carolina*

YESHIVA UNIVERSITY
*New York, New York*

SOLSAA STATISTICAL SERVICES
PO Box 320
Aurora, South Dakota 57002