The Fibonacci Quarterly

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

TABLE OF CONTENTS

VOLUME 39 JUNE–JULY 2001 NUMBER 3

PURPOSE

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

EDITORIAL POLICY

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

SUBMITTING AN ARTICLE

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

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

for additional instructions.

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 **BELL & HOWELL INFORMATION & LEARNING, 300 NORTH ZEEB ROAD, P.O. BOX 1346, ANN ARBOR, MI 48106-1346.** Reprints can also be purchased from **BELL & HOWELL** at the same address.

The Fibonacci Quarterly

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

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

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

SOME BASIC LINE-SEQUENTIAL PROPERTIES OF POLYNOMIAL LINE-SEQUENCES

Jack Y. Lee
280 86th Street, Brooklyn, NY 11209
(*Submitted February 1999-Final Revision April 1999*)

0. INTRODUCTION

There have been many reports on the properties of various polynomial sequences and their generalizations (see, e.g., [1], [3], [4], [5], [6], and [9] and the references therein). In this paper we shall try to treat some polynomial sequences by virtue of the line-sequential formalism developed earlier. To this end, we choose [9] as the guide of our endeavor and obtain some results of a different variety supplementary to those appearing in the literature. In particular, we treat the Morgan-Voyce (MV) polynomial sequences in some detail (for the origination of the MV polynomials, see the references in [1]) and then apply the method to the Jacobsthal (J) and the Vieta (V) polynomial sequences. Finally, we illustrate applications of these results with some examples. The line-sequential treatments of at least some of the other well-known polynomial sequences are somewhat more complicated, so these and other related matters will be discussed in a later report.

1. MV-POLYNOMIAL LINE-SEQUENCES

For convenience of reference, we recap here some of the basic conventions employed in the line-sequential formalism. A homogeneous second-order line-sequence is represented by

$$\bigcup_{u_0,\,u_1}(c,b):\ldots,u_{-2},u_{-1},[u_0,u_1],u_2,u_3,\ldots,u_n,\ldots,\quad n\in z,\,u_n\in R, \tag{1.1}$$

where c and b, neither zero, are the anharmonic coefficients of the recurrence relation, $cu_{n-2}+bu_{n-1}=u_n$, and the symbol $[u_0,u_1]$ denotes the generating pair of the line-sequence (see §4 in [7]).

The set of line-sequences (1.1) spans a vector space with the pair of basis vectors:

$$U_{1,0}(c,b):\ldots,(c+b^2)/c^2,-b/c,[1,0],c,cb,c(c+b^2),\ldots; \tag{1.2a}$$

$$U_{0,1}(c,b):\ldots,(c+b^2)/c^3,-b/c^2,1/c,[0,1],b,c+b^2,\ldots \tag{1.2b}$$

(see (4.2) and (4.3) in [7]). For convenience, we describe the pair as being "mutually complementary." A general line-sequence (1.1) is then decomposable into its basis components (see (2.9) in [7]) in the following manner:

$$\bigcup_{u_0,\,u_1}(c,b)=u_0U_{1,0}(c,b)+u_1U_{0,1}(c,b). \tag{1.2c}$$

A word on the nomenclature: to comply to the line-sequential format established previously, the symbols and the names adopted here are necessarily somewhat different from some of the corresponding ones of the polynomial sequences as they appear in the literature. However, this will not cause any confusion, as we shall see. For convenience, we adopt the letter M to denote the MV polynomials that are characterized by the values $b=x+2$ and $c=-1$. For the generating pair [1, 0], we then have what we call the "complementary MV-Fibonacci line-sequence," or, for short, the $M_{1,0}$ line-sequence:

$$M_{1,0}(-1, x+2): \ldots, (x^2+4x+3), x+2, [1, 0], -1, -(x+2), -(x^2+4x+3), \ldots. \tag{1.3a}$$

Let $m_n[1, 0]$ denote the nth term (or element) in $M_{1,0}$, counting from the first member of the basis pair as the zeroth term, that is, $m_0[1, 0] = 1$, and increasing toward the right as the positive direction. Then the parity relation will be shown later to be

$$m_{-n}[1, 0] = -m_{n+2}[1, 0]. \tag{1.3b}$$

Let $M_{1,0}(+)$ denote the positive branch, $n \geq 0$, of the $M_{1,0}$ line-sequence, which is denoted by $\{w_n(1, 0; x+2, 1)\}$ in Horadam's notation. Its coefficients table, adapted to the format employed in [9], is given in Table 1 below. The corresponding table for the negative branch can be inferred from Table 1 by means of the parity relation (1.3b).

TABLE 1. The Coefficients Associated with the $M_{1,0}(+)$ Sequence

n	x^0	x^1	x^2	x^3	x^4	x^5
0	1					
1	0					
2	−1					
3	−2	−1				
4	−3	−4	−1			
5	−4	−10	−6	−1		
6	−5	−20	−21	−8	−1	
7	−6	−35	−56	−36	−10	−1

The complementary line-sequence of (1.3a) is given by

$$M_{0,1}(-1, x+2): \ldots, -(x^2+4x+3), -(x+2), -1, [0, 1], x+2, x^2+4x+3, \ldots, \tag{1.4a}$$

which is the MV-Fibonacci line-sequence, or the $M_{0,1}$ line-sequence for short, the positive branch of which is called the MV Even Fibonacci polynomial sequence in [9]. Its parity relation, according to (4.9) in [7], is given by

$$m_{-n}[0, 1] = -m_n[0, 1]. \tag{1.4b}$$

Clearly, $M_{0,1}$ is the negative of one order translation from $M_{1,0}$, that is,

$$M_{0,1} = -TM_{1,0}, \tag{1.4c}$$

where T denotes the translation operator. In terms of the elements,

$$m_n[0, 1] = -m_{n+1}[1, 0]. \tag{1.4d}$$

Definition 1: We say that a line-sequence B is "translationally dependent" on the line-sequence A if and only if B can be obtained from A by means of some (harmonic or anharmonic combinations of) translation operations on A.

Substituting (1.4d) into (1.4b), we obtain the parity relation (1.3b) for $M_{1,0}$.

The line-sequences $M_{1,0}$ and $M_{0,1}$ then form a pair of orthonormal bases spanning the 2D MV line-sequential vector space. Any line-sequence in this space can then be decomposed into its basis components in the manner according to (1.2c).

Combining the parity relations (1.3b) and (1.4b) with the translation relation (1.4d), we obtain the following set of basis relations between the elements of the two basis line-sequences:

$$m_{-n}[1, 0] = m_{n+1}[0, 1], \tag{1.5a}$$

$$m_{-n}[1, 0] = -m_{-(n+1)}[0, 1]; \tag{1.5b}$$

or

$$m_{-n}[0, 1] = m_{n+1}[1, 0], \tag{1.5c}$$

$$m_{-n}[0, 1] = -m_{-(n-1)}[1, 0]. \tag{1.5d}$$

The $M_{1,1}$ line-sequence, the positive branch of which is named the MV Odd Fibonacci polynomial sequence in [9], is given by

$$M_{1,1}(-1, x+2): \ldots, x^2+3x+1, x+1, [1, 1], x+1, x^2+3x+1, \ldots. \tag{1.6a}$$

It decomposes into its basis components according to (1.2c):

$$M_{1,1} = M_{1,0} + M_{0,1}. \tag{1.6b}$$

Or, in terms of the elements,

$$m_n[1, 1] = m_n[1, 0] + m_n[0, 1]. \tag{1.6c}$$

It is seen that the sum of the corresponding coefficients in Table 1 for $M_{1,0}(+)$ above and Table 2(a) for $M_{0,1}(+)$ in [9] equals the corresponding coefficient in Table 2(b) for $M_{1,1}(+)$ in [9], as can be deduced from (1.6c).

Applying relation (1.4c) to the component equation (1.6b), we obtain the following *translational expression* of $M_{1,1}$ in terms of $M_{1,0}$:

$$M_{1,1} = (I - T)M_{1,0}, \tag{1.6d}$$

where I is the identity operator of translation. In terms of the elements, we have

$$m_n[1, 1] = m_n[1, 0] - m_{n+1}[1, 0]. \tag{1.6e}$$

A look at the relevant terms in Table 1 and in Table 2(b) in [9] bears out this relationship.

Since a line-sequence in the MV space can always be decomposed into its basis components, and since the pair of bases are translationally dependent, all MV line-sequences are translationally dependent on either of the basis line-sequences. Since the two bases (4.2) and (4.3) in [7] for the general case are translationally dependent, the above said property must hold in general. We state this in the form of a theorem.

Theorem 1: All line-sequences defined in a line-sequential vector space are translationally dependent on either basis line-sequence.

Applying (1.5a) and (1.5c) to (1.6c), we obtain the parity rule for $M_{1,1}$,

$$m_{-n}[1, 1] = m_{n+1}[1, 1], \tag{1.6f}$$

a property clearly displayed in (1.6a).

The MV-Lucas line-sequence, the positive branch of which is the MV Even Lucas polynomial sequence according to [9], is given by

$$M_{2,x+2}(-1, x+2): \ldots, x^2+4x+2, x+2, [2, x+2], x^2+4x+2, x^3+6x^2+9x+2, \ldots. \tag{1.7a}$$

Applying the geometrical sequences (1.10a) and (1.10b) to the Binet formula (1.12d), see below, and noting that $\alpha\beta = 1$, it is easy to show that the parity relation among the terms in $M_{2,\,x+2}$ is given by

$$m_{-n}[2, x+2] = m_n[2, x+2], \tag{1.7b}$$

which is clearly displayed in the line-sequence (1.7a).

Decomposing (1.7a) into its basis components, we have

$$M_{2,\,x+2} = 2M_{1,\,0} + (x+2)M_{0,\,1} \tag{1.7c}$$

or, in terms of their elements,

$$m_n[2, x+2] = 2m_n[1, 0] + (x+2)m_n[0, 1]. \tag{1.7d}$$

Applying basis relation (1.5a) with parity relations (1.4b) and (1.7b) to (1.7d) above, we get

$$m_n[2, x+2] = 2m_{n+1}[0, 1] - (x+2)m_n[0, 1]. \tag{1.7e}$$

This is the MV-version of the well-known relation $l_n = 2f_{n+1} - f_n$ between the elements of the Lucas and the Fibonacci sequences.

Applying relation (1.4c) to (1.7c), we obtain

$$M_{2,\,x+2} = [2I - (x+2)T]M_{1,\,0}. \tag{1.7f}$$

This is the *translational representation* of the MV-Lucas line-sequence in terms of its first basis. We say the line-sequence $M_{2,\,x+2}$ is "anharmonically" translationally dependent on the basis $M_{1,\,0}$.

The line-sequential form of $M_{-1,\,1}$, the positive branch of which is called the MV Odd Lucas polynomial sequence in [9], is given by

$$M_{-1,\,1}(-1, x+2): \ldots, -(x^2+5x+5), -(x+3), [-1, 1], x+3, x^2+5x+5, \ldots. \tag{1.8a}$$

Its decomposition is given by

$$M_{-1,\,1} = -M_{1,\,0} + M_{0,\,1}. \tag{1.8b}$$

In terms of the elements,

$$m_n[-1, 1] = -m_n[1, 0] + m_n[0, 1]. \tag{1.8c}$$

It is seen that the sum of the negative of a term in Table 1 above and the corresponding term in Table 2(a) in [9] equals the corresponding term in Table 3(b) in [9], as can be deduced from (1.8c).

Applying the relations (1.5a) and (1.5c) to (1.8c), we find the parity relation for the elements of $M_{-1,\,1}$:

$$m_{-n}[-1, 1] = -m_{n+1}[-1, 1], \tag{1.8d}$$

which is clearly displayed in the line-sequence (1.8a).

Applying the relation (1.4c) to (1.8b), we obtain the following translational representation of $M_{-1,\,1}$ in terms of the first basis $M_{1,\,0}$,

$$M_{-1,\,1} = -(I+T)M_{1,\,0}. \tag{1.8e}$$

The following set of interrelationships among the MV polynomials can be shown to hold:

$$M_{1,0} + M_{-1,1} = M_{0,1}; \tag{1.9a}$$

$$M_{1,1} + M_{-1,1} = 2M_{0,1}; \tag{1.9b}$$

$$M_{1,1} + M_{1,0} = M_{2,1}, \tag{1.9c}$$

$$(x+2)M_{1,1} - xM_{1,0} = M_{2,x+2}; \tag{1.9d}$$

and so forth.

The pair of geometrical line-sequences relating to $M_{1,0}$ is given by

$$M_{1,\alpha}(-1, x+2): \ldots, \alpha^{-2}, \alpha^{-1}, [1, \alpha], \alpha^2, \alpha^3, \ldots, \tag{1.10a}$$

and

$$M_{1,\beta}(-1, x+2): \ldots, \beta^{-2}, \beta^{-1}, [1, \beta], \beta^2, \beta^3, \ldots, \tag{1.10b}$$

where

$$\alpha = [x+2+(x^2+4x)^{1/2}]/2, \quad \beta = [x+2-(x^2+4x)^{1/2}]/2 \tag{1.11a}$$

are the roots of the generating equation

$$q^2 - (x+2)q + 1 = 0. \tag{1.11b}$$

Since $M_{1,\alpha}$ and $M_{1,\beta}$ also form a pair of orthogonal (but not normal) bases of the MV vector space (see §3 in [8]), any MV line-sequence can be expressed as a linear combination of its $M_{1,\alpha}$ and $M_{1,\beta}$ components, which, in a manner of speaking, is just its Binet formula.

Generalizing relation (4.9) in [8] and applying basis decompositions in terms of $M_{1,\alpha}$ and $M_{1,\beta}$, we obtain the following set of Binet's formulas for the family of MV line-sequences:

$$M_{1,0} = (-\beta M_{1,\alpha} + \alpha M_{1,\beta})/(\alpha - \beta); \tag{1.12a}$$

$$M_{0,1} = (M_{1,\alpha} - M_{1,\beta})/(\alpha - \beta); \tag{1.12b}$$

$$M_{1,1} = [(1-\beta)M_{1,\alpha} - (1-\alpha)M_{1,\beta}]/(\alpha - \beta); \tag{1.12c}$$

$$M_{2,x+2} = M_{1,\alpha} + M_{1,\beta}; \tag{1.12d}$$

$$M_{-1,1} = [(1+\beta)M_{1,\alpha} - (1+\alpha)M_{1,\beta}]/(\alpha - \beta). \tag{1.12e}$$

Notice that the form of the Binet formulas (1.12b) and (1.12d) justifies our identifying them as the MV-Fibonacci and MV-Lucas line-sequences, respectively, consistent with works in this area; and as a cross check, multiplying (1.12b) and (1.12d), we obtain, in terms of the elements,

$$m_n[0, 1]m_n[2, 2+x] = m_{2n}[0, 1], \tag{1.13}$$

which is the MV version of the well-known relation $f_n l_n = f_{2n}$ between the Fibonacci and Lucas numbers.

Since, by Theorem 1, a line-sequence can always be translationally represented in terms of either of its bases, and since its basis can always be expressed in terms of the geometrical line-sequence, namely Binet's formula, a line-sequence can always be expressed in terms of the geometrical line-sequence which, naturally, is referred to as its Binet formula. Formulas (1.12c) and (1.12e) are such examples. We state this in the form of a theorem.

Theorem 2: All line-sequences defined in a line-sequential vector space are expressible by means of their respective Binet formulas.

2. THE JACOBSTHAL POLYNOMIAL LINE-SEQUENCES

The Jacobsthal (J) polynomial sequence is characterized by the parameters $b=1$ and $c=x$. (Here, we adopt the convention used in [9]; for another convention used by Horadam, see [4].) The basis pair is given by

$$J_{0,1}(x,1): \ldots, -(2x^{-2}+x^{-3}), x^{-1}+x^{-2}, -x^{-1}, [0,1], x, x, x^2+x, 2x^2+x, \ldots, \tag{2.1a}$$

$$J_{0,1}(x,1): \ldots, -(2x^{-3}+x^{-4}), x^{-2}+x^{-3}, -x^{-2}, x^{-1}, [0,1], 1, x+1, 2x+1, \ldots, \tag{2.1b}$$

where the first one will be referred to as the "complementary J-Fibonacci line-sequence" or $J_{1,0}$ line-sequence for short; the second one is the "J-Fibonacci line-sequence," or $J_{0,1}$ line-sequence whose positive branch is called the J-Fibonacci sequence in [9]. The pair then span the 2D J line-sequential vector space. Obviously, the two basis line-sequences are related translationally,

$$TJ_{1,0} = xJ_{0,1}, \tag{2.2a}$$

or, in terms of the elements,

$$j_{n+1}[1,0] = xj_n[0,1]. \tag{2.2b}$$

The parity relation of the terms in $J_{1,0}$ can be shown to be

$$j_{-n}[1,0] = (-1)^{n+2}x^{-(n+1)}j_{n+2}[1,0]. \tag{2.3a}$$

According to (4.9) in [7], the parity relation for terms in $J_{0,1}$ is given by

$$j_{-n}[0,1] = (-1)^{n+1}x^{-n}j_n[0,1]. \tag{2.3b}$$

Substituting the translation relation (2.2b) into (2.3b), we get (2.3a).

Using these parity relations with the translation relation, we obtain the following set of relations between the elements of the two basis line-sequences:

$$j_{-n}[1,0] = (-x)^{-n}j_{n+1}[0,1], \tag{2.4a}$$

$$j_{-n}[1,0] = xj_{-(n+1)}[0,1]; \tag{2.4b}$$

or

$$j_{-n}[0,1] = (-x)^{-(n+1)}j_{n+1}[1,0], \tag{2.4c}$$

$$j_{-n}[0,1] = x^{-1}j_{-(n-1)}[1,0]. \tag{2.4d}$$

The coefficient table of $J_{1,0}(+)$ is given in Table 2 below.

TABLE 2. The Coefficients Associated with the $J_{1,0}(+)$ Sequence

n	x^0	x^1	x^2	x^3
0	1			
1	0			
2	0	1		
3	0	1		
4	0	1	1	
5	0	1	2	
6	0	1	3	1
7	0	1	4	3

The J-Lucas line-sequence is given by

$$J_{2,1}(x,1): \ldots, -3x^{-2}-x^{-3}, 2x^{-1}+x^{-2}, -x^{-1}, [2,1], 2x+1, 3x+1, 2x^2+4x+1, \ldots, \tag{2.5a}$$

which is a linear combination of the basis line-sequences (2.1a) and (2.1b),

$$J_{2,1} = 2J_{1,0} + J_{0,1} \tag{2.5b}$$

or, in terms of the corresponding members in these line-sequences,

$$j_n[2,1] = 2j_n[1,0] + j_n[0,1]. \tag{2.5c}$$

It is seen that the sum of twice a term in Table 2 for $J_{1,0}(+)$ above and a term in Table 4(a) for $J_{0,1}(+)$ in [9] equals the corresponding term in Table 4(b) for $J_{2,1}(+)$ in [9], as can be deduced from relation (2.5c) above.

From the Binet formula (2.8c) below, using (2.6a) and (2.6b), noting that $\alpha\beta = -x$, we obtain the following parity relation for the J-Lucas line-sequence:

$$j_{-n}[2,1] = (-1)^n x^{-n} j_n[2,1]. \tag{2.5d}$$

Applying parity relation (2.5d) and relations (2.4a) and (2.4c) to the component equation (2.5c), using the translation equation (2.2b), we obtain

$$j_n[2,1] = 2x^{-1} j_{n+2}[1,0] - j_n[0,1], \tag{2.5e}$$

which is the J-version of the relation $l_n = 2f_{n+1} - f_n$.

Applying the translation relation (2.2a) to the basis component equation (2.5b), we obtain the translational representation of the J-Lucas line-sequence in terms of the $J_{1,0}$ basis,

$$J_{2,1} = (2I + x^{-1}T)J_{1,0}, \tag{2.5f}$$

a result consistent with the statement of Theorem 1 above.

The pair of geometrical line-sequences relating to $J_{1,0}$ is given by

$$J_{1,\alpha}(x,1): \ldots, \alpha^{-2}, \alpha^{-1}, [1,\alpha], \alpha^2, \alpha^3, \ldots, \tag{2.6a}$$

$$J_{1,\beta}(x,1): \ldots, \beta^{-2}, \beta^{-1}, [1,\beta], \beta^2, \beta^3, \ldots, \tag{2.6b}$$

where

$$\alpha = [1+(1+4x)^{1/2}]/2, \quad \beta = [1-(1+4x)^{1/2}]/2 \tag{2.7a}$$

are the roots of the generating equation

$$q^2 - q - x = 0. \tag{2.7b}$$

Here, considering the multitude of recurring polynomial sequences which may be treated in this manner, we retain the use of the same pair of letters α and β to represent the roots of the *respective* generating equation of each case, rather than adopt a new pair of letters each time for each case; while the pair of letters A and B remains reserved for representing the large and the (negative) small golden ratios.

Then an arbitrary J line-sequence can be expressed in terms of $J_{1,\alpha}$ and $J_{1,\beta}$. In particular,

$$J_{1,0} = (-\beta J_{1,\alpha} + \alpha J_{1,\beta})/(\alpha - \beta), \tag{2.8a}$$

which is Binet's formula for the complementary J-Fibonacci line-sequence, and

$$J_{0,1} = (J_{1,\alpha} - J_{1,\beta}) / (\alpha - \beta), \tag{2.8b}$$

which is Binet's formula for the J-Fibonacci line-sequence, and

$$J_{2,1} = J_{1,\alpha} + J_{1,\beta}, \tag{2.8c}$$

which is Binet's formula for the J-Lucas line-sequence.

It is easy to see that

$$j_n[0, 1]\, j_n[2, 1] = j_{2n}[0, 1], \tag{2.9}$$

which is the J-version of the basic relation $f_n l_n = f_{2n}$.

3. THE VIETA POLYNOMIAL LINE-SEQUENCES

The V-polynomial sequence is characterized by the parameters $b = x$ and $c = -1$. Observing that, if we put $x + 2 = x'$ for the MV-polynomials, then the latter will be line-sequentially equivalent to the V-polynomials. Therefore, the line-sequential relations of the V-polynomials can be obtained directly from the corresponding ones of the MV-polynomials. For convenience of reference, however, we compile the following essential relations for the V-polynomials.

The basis pair of the V line-sequences is given by

$$V_{1,0}(-1, x): \ldots, -(2x - x^3), -(1 - x^2), x, [1, 0], -1, -x, 1 - x^2, 2x - x^3, \ldots, \tag{3.1a}$$

$$V_{0,1}(-1, x): \ldots, 2x - x^3, 1 - x^2, -x, -1, [0, 1], x, -(1 - x^2), -(2x - x^3) \ldots, \tag{3.1b}$$

where the first one is the complementary V-Fibonacci line-sequence, or $V_{1,0}$ line-sequence for short; the second is the V-Fibonacci line-sequence, or $V_{0,1}$ line-sequence for short. This pair spans the 2D V line-sequential vector space.

Obviously, we have the following translational relation between the two basis line sequences:

$$V_{0,1} = -TV_{1,0} \tag{3.2a}$$

or, in terms of the elements,

$$v_n[0, 1] = -v_{n+1}[1, 0]. \tag{3.2b}$$

The parity relation of the elements in $V_{1,0}$ is found to be

$$v_{-n}[1, 0] = -v_{n+2}[1, 0]. \tag{3.3a}$$

From (4.9) in [7], the parity relation for the elements in $V_{0,1}$ is found to be

$$v_{-n}[0, 1] = -v_n[0, 1], \tag{3.3b}$$

which is clearly borne out in (3.1b). Applying (3.2b) to (3.3b), we obtain (3.3a).

Using these parity relations together with the translation relation (3.2b), we obtain the following set of relations between the elements of the two basis line-sequences:

$$v_{-n}[1, 0] = v_{n+1}[0, 1], \tag{3.4a}$$

$$v_{-n}[1, 0] = -v_{-(n+1)}[0, 1]; \tag{3.4b}$$

or

$$v_{-n}[0, 1] = v_{n+1}[1, 0], \tag{3.4c}$$

$$v_{-n}[0, 1] = -v_{-(n-1)}[1, 0]. \tag{3.4d}$$

This set of relations parallels exactly the set for the MV line-sequences, namely, from (1.5a) to (1.5d), as it should be.

The coefficient table of $V_{1,0}(+)$ is given in Table 3.

TABLE 3. The Coefficients Associated with the $V_{1,0}(+)$ Sequence

n	x^0	x^1	x^2	x^3	x^4	x^5
0	1					
1	0					
2	−1					
3	0	−1				
4	1	0	−1			
5	0	2	0	−1		
6	−1	0	3	0	−1	
7	0	−3	0	4	0	−1

The coefficient table of $xV_{0,1}(+) = V_{0,x}(+)$ is given in Table 4.

TABLE 4. The Coefficients Associated with the $V_{0,x}(+)$ Sequence

n	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7
0	0							
1	0	1						
2	0	0	1					
3	0	−1	0	1				
4	0	0	−2	0	1			
5	0	1	0	−3	0	1		
6	0	0	3	0	−4	0	1	
7	0	−1	0	6	0	−5	0	1

The V-Lucas line-sequence is given by

$$V_{2,x}(-1, x): \ldots, -x(3-x^2), -(2-x^2), x, [2, x], -(2-x^2), -x(3-x^2), \ldots. \tag{3.5a}$$

The coefficient table of $V_{2,x}(+)$ is given in Table 5.

TABLE 5. The Coefficients Associated with the $V_{2,x}(+)$ Sequence

n	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7
0	2							
1	0	1						
2	−2	0	1					
3	0	−3	0	1				
4	2	0	−4	0	1			
5	0	5	0	−5	0	1		
6	−2	0	9	0	−6	0	1	
7	0	−7	0	14	0	−7	0	1

The decomposition of $V_{2,x}$ into its basis components is given by

$$V_{2,x} = 2V_{1,0} + xV_{0,1} \tag{3.5b}$$

or, in terms of the elements,

$$v_n[2, x] = 2v_n[1, 0] + xv_n[0, 1]. \tag{3.5c}$$

It can be seen that the sum of twice a coefficient in Table 3 and the corresponding coefficient in Table 4 equals the corresponding coefficient in Table 5, as can be deduced from (3.5c).

The parity relation among the terms of $V_{2,x}$ is obtained from (1.7b):

$$v_{-n}[2, x] = v_n[2, x], \tag{3.6a}$$

which is apparent in (3.5a).

The V-version of the relation $l_n = 2f_{n+1} - f_n$ is obtained from (1.7e):

$$v_n[2, x] = 2v_{n+1}[0, 1] - xv_n[0, 1]. \tag{3.6b}$$

The translational expression of $V_{2,x}$ in terms of $V_{1,0}$ is obtained from (1.7f):

$$V_{2,x} = (2I - xT)V_{1,0}. \tag{3.6c}$$

The pair of geometrical line-sequences relating to $V_{1,0}$ is given by

$$V_{1,\alpha}(-1, x): \ldots, \alpha^{-2}, \alpha^{-1}, [1, \alpha], \alpha^2, \alpha^3, \ldots, \tag{3.7a}$$

$$V_{1,\beta}(-1, x): \ldots, \beta^{-2}, \beta^{-1}, [1, \beta], \beta^2, \beta^3, \ldots, \tag{3.7b}$$

where

$$\alpha = [x + (x^2 - 4)^{1/2}]/2, \quad \beta = [x - (x^2 - 4)^{1/2}]/2 \tag{3.8a}$$

are the roots of the generating equation

$$q^2 - xq + 1 = 0. \tag{3.8b}$$

Hence, the Binet formula for the $V_{1,0}$ line-sequence is given by

$$V_{1,0} = (-\beta V_{1,\alpha} + \alpha V_{1,\beta}) / (\alpha - \beta), \tag{3.9a}$$

the Binet formula for the $V_{0,1}$ line-sequence is given by

$$V_{0,1} = (V_{1,\alpha} - V_{1,\beta}) / (\alpha - \beta), \tag{3.9b}$$

and the Binet formula for the V-Lucas line-sequence is given by

$$V_{2,x} = V_{1,\alpha} + V_{1,\beta}. \tag{3.9c}$$

Obviously,

$$v_n[0, 1]v_n[2, x] = v_{2n}[0, 1], \tag{3.9d}$$

which is the V-version of the relation $f_n l_n = f_{2n}$.

4. SOME APPLICATIONS

We illustrate the application of the foregoing results with a few examples.

Example 1: For the MV-Lucas line-sequence, by the rule of line-sequential addition, we have

$$M_{1,x+2} + M_{1,0} = M_{2,x+2}.$$

Using translation relation (1.4c), we obtain $(T - T^{-1})M_{0,1} = M_{2,x+2}$. So, in general, we have

$$(T^{n+1} - T^{n-1})M_{0,1} = T^n M_{2,x+2}. \tag{4.1a}$$

This is the translational representation of the MV-Lucas line-sequence in terms of its second basis. In elements form, this becomes

$$m_{n+1}[0,1] - m_{n-1}[0,1] = m_n[2, x+2], \tag{4.1b}$$

which is the MV-version of the well-known relation between the Fibonacci and the Lucas numbers $f_{n+1} + f_{n-1} = l_n$.

Applying parity relation (1.4b) to (4.1b), we obtain

$$m_{-(n-1)}[0,1] - m_{-(n+1)}[0,1] = m_n[2, x+2] \tag{4.1c}$$

or

$$(T^{-(n-1)} - T^{-(n+1)})M_{0,1} = T^n M_{2,x+2}, \tag{4.1d}$$

which is the *negative* translational representation of the MV-Lucas line-sequence. From (4.1d), it can easily be inferred that

$$(T^{-(n-1)} + T^{-(n+1)})F_{0,1} = (-1)^n T^n F_{2,1}, \tag{4.1e}$$

which is the negative translational representation of the Lucas line-sequence. Therefore, in terms of the elements, we obtain the expression of the Lucas numbers in terms of the Fibonacci numbers with *negative* indices, i.e.,

$$f_{-(n-1)} + f_{-(n+1)} = (-1)^n l_n, \tag{4.1f}$$

which is a particular case of equation (2.16) of Horadam [2].

Example 2: For the J-Lucas line-sequence, we have $J_{1,1} + J_{1,0} = J_{2,1}$. Using translation relation (2.2a), we have $[T + xT^{-1}]J_{0,1} = J_{2,1}$. Hence, we obtain

$$[T^{n+1} + xT^{n-1}]J_{0,1} = T^n J_{2,1}. \tag{4.2a}$$

This is the translational expression of the J-Lucas line-sequence in terms of its second basis. In the elements form, we have

$$j_{n+1}[0,1] + x\, j_{n-1}[0,1] = j_n[2,1], \tag{4.2b}$$

which is the J-version of the relation $f_{n+1} + f_{n-1} = l_n$.

Applying parity relation (2.3b) to (4.2b) and using the translation operation, we obtain

$$(-1)^n x^n\, (xT^{-(n+1)} + T^{-(n-1)})\, J_{0,1} = T^n J_{2,1}, \tag{4.2c}$$

which is the negative translational expression of the J-Lucas line-sequence in terms of its second basis.

Example 3: For the V-Lucas line-sequence, we start with $V_{1,x} + V_{1,0} = V_{2,x}$. Using translation relation (3.2a), this becomes $(T - T^{-1})V_{0,1} = V_{2,x}$. Hence, we have

$$(T^{n+1} - T^{n-1})V_{0,1} = T^n V_{2,x}. \tag{4.3a}$$

This is the translational representation of the V-Lucas line-sequence in terms of its second basis. In the elements form, we find that

$$v_{n+1}[0,1]-v_{n-1}[0,1]=v_n[2,x], \tag{4.3b}$$

which is the V-version of the relation $f_{n+1}+f_{n-1}=l_n$.

Applying parity relation (3.3b) to (4.3b) and using the translation operation, we have

$$(-T^{-(n+1)}+T^{-(n-1)})V_{0,1}=T^nV_{2,x}, \tag{4.3c}$$

which is the negative translational expression of the V-Lucas line-sequence in terms of its second basis.

ACKNOWLEDGMENT

The author wishes to express his gratitude to the anonymous referee for valuable suggestions that resulted in the improvement of this report.

REFERENCES

1. Richard André-Jeannin. "A Generalization of Morgan-Voyce Polynomials." *The Fibonacci Quarterly* **32.3** (1994):228-31.
2. A. F. Horadam. "Basic Properties of a Certain Generalized Sequence of Numbers." *The Fibonacci Quarterly* **3.3** (1965):161-76.
3. A. F. Horadam. "A Synthesis of Certain Polynomial Sequences." In *Applications of Fibonacci Numbers* **6**:215-29. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1994.
4. A. F. Horadam. "Jacobsthal Representation Polynomials." *The Fibonacci Quarterly* **35.2** (1997):137-48.
5. A. F. Horadam & P. Filipponi. "Derivative Sequences of Jacobsthal and Jacobsthal-Lucas Polynomials." *The Fibonacci Quarterly* **35.4** (1997):352-57.
6. A. F. Horadam. "Morgan-Voyce Type Generalized Polynomials with Negative Subscripts." *The Fibonacci Quarterly* **36.5** (1998):391-95.
7. Jack Y. Lee. "Some Basic Properties of the Fibonacci Line-Sequence." In *Applications of Fibonacci Numbers* **4**:203-14. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1990.
8. Jack Y. Lee. "The Golden-Fibonacci Equivalence." *The Fibonacci Quarterly* **30.3** (1992): 216-20.
9. A. G. Shannon & A. F. Horadam. "Some Relationships among Vieta, Morgan-Voyce and Jacobsthal Polynomials." In *Applications of Fibonacci Numbers* **8**. Ed. F. T. Howard et al. Dordrecht: Kluwer, 1998.

AMS Classification Numbers: 11B39, 15A03

❖❖❖

ON THE FACTORIZATION OF LUCAS NUMBERS

Wayne L. McDaniel
University of Missouri-St. Louis, MO 63121
(*Submitted March 1999*)

1. INTRODUCTION

If an integer is not a prime, then it can, of course, be written as the product of two integers, say r and $r+k$. In the case of the Lucas numbers, L_n, it has been shown that the two factors may differ by 0 (that is, L_n is a square) only if $n=1$ or 3 [1], [3], may differ by 1 only if $n=0$ [4], [5], and may differ by 2 only if $n=\pm 2$ [6].

It is well known that $L_n^2-5F_n^2=4(-1)^n$, where F_n is the nth Fibonacci number, so if $L_n = r(r+k)$, we have an equation of the form $x^4+2kx^3+x^2k^2\pm 4=5y^2$. Since the left side has 3 distinct zeros, the number of solutions of this equation is finite, by a theorem of Siegel [7]; further, by a theorem of Baker (see [2]), $|x|$ and $|y|$ are effectively bounded. Hence, for a given k, the number of integers n such that $L_n=r(r+k)$ is finite, but the known bounds are extremely large.

We shall show that, if $L_n=r(r+k)$ for $k\equiv 1, 6, 7, 8, 17, 18, 19$, or 24 (mod 25), the number of solutions is bounded by one-half the number of positive divisors of $|k^2-8|$ or $|k^2+8|$, and we provide an algorithm for finding all solutions. In each case,

$$n<\frac{2\log((k^2+9)/4)}{\log((1+\sqrt{5})/2)}.$$

For certain infinite sets, e.g., $k\equiv 8 \pmod{100}$, we show that no solutions exist. When k is even, $L_n=r(r+k)$ is equivalent to $L_n=x^2-(k/2)^2$, so our results extend Robbins' result [6] on the solutions of $L_n=x^2-1$ to the difference of two squares in infinitely many cases.

We write $\square$ for "a square," τ is the usual "number of divisors" function, $(a\,|\,b)$ is the Jacobi symbol, and we will need the following familiar relations. Let g, m, n, and t be integers, t odd.

$$L_{2g}=L_g^2-2(-1)^g \quad\text{and}\quad F_{2g}=F_gL_g, \tag{1}$$

$$L_{-n}=(-1)^nL_n \quad\text{and}\quad F_{-n}=(-1)^{n+1}F_n, \tag{2}$$

$$2L_{m+n}=L_mL_n+5F_mF_n, \tag{3}$$

$$L_{2^um}\equiv\begin{cases}2 \pmod 8 & \text{if } 3\,|\,m \text{ and } u\ge 1,\\ -1 \pmod 8 & \text{if } 3\nmid m \text{ and } u\ge 2,\end{cases} \tag{4}$$

$$L_{2gt+m}\equiv\pm L_{2g+m} \pmod{L_{2g}}. \tag{5}$$

2. L_n AS THE PRODUCT OF TWO FACTORS DIFFERING BY k

We assume, without loss of generality, that k is positive, and note that $L_n=r(r+k)$ for some r implies that $4L_n+k^2=\square$.

Lemma 1: Let $L_n=r(r+k)$. If $k\equiv\pm 11 \pmod{3\cdot 25\cdot 41}$, then $n\equiv 0 \pmod 4$.

Proof: Let $k = \pm 11 \pmod{3 \cdot 25 \cdot 41}$. We find that $4L_n + k^2$ is a quadratic residue modulo 25 only for $n \equiv 0, 1, 4, 8, 9, 12,$ or $16 \pmod{20}$; if n is odd, then $n \equiv 1, 9, 21,$ or $29 \pmod{40}$. Now, the Lucas numbers are periodic modulo 41 with period of length 40, and $4L_n + k^2$ is a quadratic nonresidue modulo 41 for $n \equiv 9, 21,$ and $29 \pmod{40}$, and is a quadratic nonresidue modulo 3 for $n \equiv 1 \pmod 8$. It follows that $4L_n + k^2 = \square$ only if $n \equiv 0, 4, 8, 12,$ or $16 \pmod{20}$; that is, only if $n \equiv 0 \pmod 4$.

Let

$$S_1 = \{k \mid k \equiv 1, 6, 19, \text{ or } 24 \pmod{25}\},$$
$$S_2 = \{k \mid k \equiv 7, 8, 17, \text{ or } 18 \pmod{25}\},$$

and

$$S_3 = \{k \mid k \equiv \pm 11 \pmod{3 \cdot 25 \cdot 41}\}.$$

Theorem 1: Let $k \in S_1 \cup S_2 \cup S_3$. The number of nonnegative integers n for which $L_n = r(r+k)$ is less than or equal to $\tau(k^2 - 8)/2$ if $k \in S_1 \cup S_3$, and less than or equal to $\tau(k^2 + 8)/2$ if $k \in S_2$. If $L_n = r(r+k)$, then

$$n < \frac{2\log((k^2+9)/4)}{\log((1+\sqrt{5})/2)}.$$

Proof: Assume that $L_n = r(r+k)$; then $4L_n + k^2 = \square$. The quadratic residues modulo 25 are the integers in $T = \{0, 1, 4, 6, 9, 11, 14, 16, 19, 21, 24\}$.

We find that, for each integer k in S_1, $4L_n + k^2 \equiv$ an element of $T \pmod{25}$, precisely when $n \equiv 0, 4, 8, 12,$ or $16 \pmod{20}$; combining this with the result of Lemma 1, we have $L_n = r(r+k)$ for each integer k in $S_1 \cup S_2$ only when $n \equiv 0 \pmod 4$. And, for each integer k in S_2, $4L_n + k^2 \equiv$ an element of $T \pmod{25}$, precisely when $n \equiv 2, 6, 10, 14,$ or $18 \pmod{20}$, i.e., only when $n \equiv 2 \pmod 4$.

Let $n = 2t$. Now, $L_n = r(r+k)$ implies that there exists an x such that $x^2 = 4L_{2t} + k^2$, so, by (1), we have $x^2 - (2L_t)^2 = k^2 - 8(-1)^t$. Hence, there exist divisors c and d of $k^2 - 8(-1)^t$ such that $x + 2L_t = c$ and $x - 2L_t = d$, implying that $L_t = \frac{c-d}{4}$. Since, for a given pair (c, d) of divisors of $k^2 - 8(-1)^t$, the system has at most one solution; there exist at most $\tau[k^2 - 8(-1)^t]/2$ integers n for which $L_n = r(r+k)$. Taking t even or odd for the two cases, respectively, proves the first statement of the theorem.

It is well known that $L_n = \alpha^n + \beta^n$, where $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$. Let $s = [k^2 - 8(-1)^t - 1]/4$. Since $\alpha^t - 1/\alpha^t = \alpha^t + \beta^t = L_t = \frac{c-d}{4} \le s$, we readily obtain $\alpha^t < (s + \sqrt{s^2+4})/2$ If $k = 1$, it is easily seen that $n = 0$, and if $k \ne 1$, then $\alpha^t < [s + (s+1)]/2$. One obtains a relatively simple bound upon taking the logarithm of each side of $\alpha^t < s + \frac{1}{2}$, replacing t by $n/2$ and replacing s by the larger of its two values.

Lemma 2: If $k \equiv 0 \pmod 4$, then $L_n = r(r+k)$ only if n is odd.

Proof: Let $k = 4t$, and assume that, for some m, $L_{2m} = r(r+k)$. Then

$$L_{2m} + 4t^2 = r^2 + 4rt + 4t^2 = \square,$$

implying $L_{2m} \equiv 0$ or $1 \pmod 4$, contrary to (4).

We now exhibit several infinite sets of integers k such that L_n does not have the form $r(r+k)$ for any n.

Theorem 2: Let $S = \{k \mid k \equiv 8, 24, 32, 44, 56, 68, 76, 92 \pmod{100}\}$. If $k \in S$, then $L_n \neq r(r+k)$ for any n.

Proof: Let $k \in S$ and assume, for some $n \geq 0$ and some integer r, that $L_n = r(r+k)$. By Lemma 2, n is odd. However, each element of S is in $S_1 \cup S_2$ and, as noted in the proof of Theorem 1, $4L_n + k^2$ is a quadratic nonresidue for n odd.

Corollary: There exist infinitely many primes p such that L_n does not have the form $r(r+4p)$ for any n.

Proof: The sequence $\{2+25b\}$ contains infinitely many primes p and, for $p = 2+25b$, we have $4p \equiv 8 \pmod{100}$.

3. L_n AS THE DIFFERENCE OF TWO SQUARES

The proof of the following theorem is immediate upon writing $x^2 - m^2$ as $r(r+k)$ with $r = x - m$ and $k = 2m$.

Theorem 3: The equation $L_n = x^2 - m^2$

a) is impossible for all $n \geq 0$ if $m \equiv 4, 12, 16, 22, 28, 34, 38,$ or $46 \pmod{50}$,

b) has at most $\tau(4m^2 - 8)/2$ solutions if $2m \in S_1$, and

c) has at most $\tau(4m^2 + 8)/2$ solutions if $2m \in S_2 \cup S_3$,

and, if $L_n = x^2 - m^2$, then

$$n < \frac{2\log(m^2 + 9/4)}{\log((1+\sqrt{5})/2)}.$$

In practice, for a given m, one may find the values of n such that $L_n = x^2 - m^2$ by proceeding as in the proof of Theorem 1: simply write $L_{n/2} = \frac{c-d}{4}$ for all pairs (c, d), $c \equiv d \pmod 4$, of factors of $|4m^2 - 8(-1)^{n/2}|$, and find n. We can now readily obtain the values of n for which $L_n = x^2 - m^2$ for all m such that $2m = k \in S_1 \cup S_2 \cup S_3$. Notice that L_{-n} is the difference of two squares iff L_n is the difference of two squares, since $L_{-n} = \pm L_n$.

By way of example, if $m = 3$, then $2m = 6 \in S_1$, $4m^2 - 8(-1)^{n/2} = 28$, and $L_{n/2} = \frac{c-d}{4}$ for $(c, d) = (14, 2)$; hence, $L_{n/2} = 3$, and we conclude that $L_n = x^2 - 3^2$ only when $n = \pm 4$ ($L_{\pm 4} = 7 = 4^2 - 3^2$).

It may be noted that we now know the values of n for which $L_n = x^2 - m^2$ for $m = 1, 3$, and 4, and can determine the n for many larger values of m. In order to close the gap between 1 and 3, we shall prove that $L_n \neq x^2 - 2^2$ for any n. Unlike the cases considered above, this case presents a difficulty that precludes the possibility of establishing a bound on n for all $k \equiv 2m \equiv 4 \pmod{M}$ for any M.

Lemma 3: If $3 \nmid g$, then $L_{2g\pm 3} \equiv 5F_{2g} \pmod{L_{2g}}$.

Proof: We note first that $F_{\pm 3} = 2$. By (3),

$$2L_{2g\pm 3} = L_{2g}L_{\pm 3} + 5F_{2g}F_{\pm 3} \equiv 10F_{2g} \pmod{L_{2g}}.$$

Since $3 \nmid g$, L_{2g} is odd, and the lemma follows.

Lemma 4: If $3 \nmid g$ and t is odd, then $(L_{2gt\pm 3} + 4 \mid L_{2g}) = (5F_{2g} + 4 \mid L_{2g})$.

Proof: By (5) and Lemma 3,

$$(L_{2gt\pm 3} + 4 \mid L_{2g}) = (\pm L_{2g\pm 3} + 4 \mid L_{2g}) = (5F_{2g} + 4 \mid L_{2g}) \text{ or } (-5F_{2g} + 4 \mid L_{2g}).$$

We prove that these latter two Jacobi symbols are equal by showing that their product is +1:

$$\begin{aligned}(5F_{2g} + 4 \mid L_{2g}) \cdot (-5F_{2g} + 4 \mid L_{2g}) &= (16 - 25F_{2g}^2 \mid L_{2g}) \\ &= (16 - 5(L_{2g}^2 - 4) \mid L_{2g}) = (36 \mid L_{2g}) = +1.\end{aligned}$$

Lemma 5: Let $u \geq 4$. Then $5F_{2^u m} + 2L_{2^u m} \equiv -1 \pmod 8$ $\begin{cases} \text{if } u \text{ is odd and } m = 1, \text{ or} \\ \text{if } u \text{ is even and } m = 5. \end{cases}$

Proof: Let $m > 0$. By (1) and (4),

$$F_{2^u m} = F_{2^{u-2}m}L_{2^{u-2}m}L_{2^{u-1}m} \equiv F_{2^{u-2}m} \equiv F_{2^{u-4}m} \equiv \cdots F_{4m} \text{ or } F_{8m} \pmod 8,$$

depending on whether u is even or odd, respectively. Using (4), $F_8 = 21$, and $F_{20} = 6765$ proves the lemma.

Theorem 4: No term of the sequence $\{L_n\}$ is of the form $x^2 - 4$.

Proof: Assume $L_n = x^2 - 4$. By Lemma 2, we may assume that n is odd. Now $\square = L_n + 4$ modulo 25 only if $n \equiv 13$ or 17 (mod 20), and modulo 11 only if $n \equiv 5, 7, 9$ (mod 10). It follows that $n \equiv 1$ (mod 4) and $n \equiv -3$ (mod 5). For $n \equiv 1$ (mod 4), $\square = L_n + 4$ modulo 7 and modulo 47 only if $n \equiv -3$ or 13 (mod 32). However $L_n + 4$ has period of length 64 modulo 2207, and 13 and 45 are quadratic nonresidues modulo 64; hence, $n \equiv -3$ (mod 32). Combining this with $n \equiv -3$ (mod 5), we have $n \equiv -3$ (mod $5 \cdot 32$).

Let $n = 2gt - 3$, with t odd, $g = 2^u$ if u is odd, and $g = 2^u \cdot 5$ if u is even ($u \geq 4$). We shall use (1), (4), Lemma 5, and the following observation:

$$2L_{2g} = 2(L_g^2 - 2) = 2L_g^2 + 5L_g^2 - L_g^2 = 5F_g^2 + L_g^2. \tag{6}$$

By Lemma 4,

$$\begin{aligned}(L_n + 4 \mid L_{2g}) &= (5F_{2g} + 4 \mid L_{2g}) = (5F_{2g} + 2(L_g^2 - L_{2g}) \mid L_{2g}) = (5F_{2g} + 2L_g^2 \mid L_{2g}) \\ &= (L_g \mid L_{2g})(5F_g + 2L_g \mid L_{2g}) = -(L_{2g} \mid L_g)(-1)(L_{2g} \mid 5F_g + 2L_g) \\ &= (L_g^2 - 2 \mid L_g)(2 \mid 5F_g + 2L_g)(2L_{2g} \mid 5F_g + 2L_g) \\ &= (-1 \mid L_g)(5F_g^2 + L_g^2 \mid 5F_g + 2L_g) \qquad \text{[by (6)]} \\ &= -(45F_g^2 - (25F_g^2 - 4L_g^2) \mid 5F_g + 2L_g) = -(5 \mid 5F_g + 2L_g) \\ &= -(5F_g + 2L_g \mid 5) = -(2 \mid 5)(L_g \mid 5) = (L_g \mid 5).\end{aligned}$$

Since $L_8 = 47 \equiv 2 \pmod 5$, by (1), $L_{16} \equiv 2 \pmod 5$, and, by induction, $L_{2^u} \equiv 2 \pmod 5$. Similarly, $L_{20} = 15127 \equiv 2 \pmod 5$, implying $L_{2^u \cdot 5} \equiv 2 \pmod 5$. Hence, $(L_g \mid 5) = (2 \mid 5) = -1$, a contradiction.

ACKNOWLEDGMENT

The idea for this article occurred to the author following receipt by e-mail from Richard André-Jeannin of a much shorter proof of a theorem in my article "Pronic Lucas Numbers" [5]. André-Jeannin's proof did not involve congruences moduli L_{2g}, where g is a function of n, and the absence of such congruences is essential to obtaining the above results. It is the necessity of over-coming this obstacle that suggests that obtaining an analogous result for the Fibonacci numbers may be difficult.

REFERENCES

1. Brother U. Alfred. "On Square Lucas Numbers." *The Fibonacci Quarterly* **2.1** (1964):11-12.
2. A. Baker. *Transcendental Number Theory*. Cambridge: Cambridge University Press, 1975.
3. J. H. E. Cohn. "Square Fibonacci Numbers, Etc." *The Fibonacci Quarterly* **2.2** (1964):109-113.
4. Ming Luo. "Nearly Square Numbers in the Fibonacci and Lucas Sequences." *Journal of Chongqing Teacher's College* **12.4** (1995):1-5. (In Chinese.)
5. Wayne L. McDaniel. "Pronic Lucas Numbers." *The Fibonacci Quarterly* **36.1** (1998):60-62.
6. N. Robbins. "Fibonacci and Lucas Numbers of the Forms $w^2 - 1$, $w^3 \pm 1$." *The Fibonacci Quarterly* **19.4** (1981):369-73.
7. C. L. Siegel. "Über einige Anwendungen diophantischer Approximationen" (1929), pp. 209-266. In *Collected Works*. New York: Springer-Verlag, 1966.

AMS Classification Numbers: 11B39

❖❖❖

ON THE NUMBER OF MAXIMAL INDEPENDENT SETS OF VERTICES IN STAR-LIKE LADDERS

Dragan Stevanović
Dept. of Math., Faculty of Philosophy, Ćirila i Metodija 2, Niš 18000, Yugoslavia
e-mail: dragance@bankerinter.net
(*Submitted March 1999-Final Revision June 2000*)

1. INTRODUCTION

Let MIS stand for the *maximal independent set* of vertices. Denote the number of MIS of G by M_G. Sanders [1] exhibits a tree $p(P_n)$, called an *extended path*, formed by appending a single degree-one vertex to each vertex of a path on n vertices, and proves $M_{p(P_n)} = F_{n+2}$. In this paper we introduce a new class of graphs, called *star-like ladders*, and show that the number of MIS in star-like ladders has a connection to the Fibonacci numbers. In particular, we show that $M_{L_p} = 2F_{p+1}$, where L_p is the ladder with p squares.

Remember that the *ladder* L_p, $p \geq 1$, is the graph with $2p+2$ vertices $\{u_i, v_i \mid i = 0, 1, \ldots, p\}$ and edges $\{u_i u_{i+1}, v_i v_{i+1} \mid i = 0, 1, \ldots, p-1\} \cup \{u_i v_i \mid i = 0, 1, \ldots, p\}$. Two *end edges* of the ladder L_p are the edges joining vertices of degree 2.

The graph obtained by identifying an end edge of ladder L_p with an edge e of a graph G is denoted by $G[e, p]$. For the sake of completeness, we will put $G[e, 0] = G$. If $p_1, \ldots, p_k \in \mathbf{N}$ and $e_1, \ldots, e_k$ are the edges of G, then we will write $G[(e_1, \ldots, e_k), (p_1, \ldots, p_k)]$ for $G[e_1, p_1] \ldots [e_k, p_k]$. The *star-like ladder* $SL(p_1, \ldots, p_k)$ is the graph $K_2[(e, \ldots, e), (p_1, \ldots, p_k)]$, where e is the edge of K_2. We have that $L_p = SL(p) = K_2[e, p]$, $p \in \mathbf{N}$.

2. MIS IN GRAPHS WITH PENDANT LADDERS

Graph G has *pendant ladders* if there is a graph G^*, the edges e_i of G^* and $p_i \in \mathbf{N}$, $i = 1, \ldots, k$, $k \geq 1$, such that $G = G^*[(e_1, \ldots, e_k), (p_1, \ldots, p_k)]$. In the next lemma, we give the recurrence formula for M_G when G has pendant ladders.

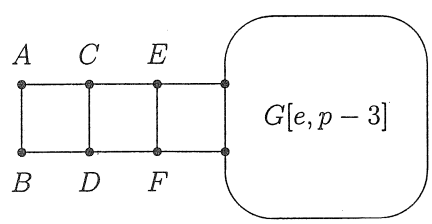

FIGURE 1. The Graph $G[e, p]$

Lemma 1: If e is an edge of a graph G and $p \in \mathbf{N}$, $p \geq 3$, then

$$M_{G[e,\,p]} = M_{G[e,\,p-1]} + M_{G[e,\,p-2]}. \tag{1}$$

Proof: Let M be MIS in $G[e, p]$. Then, for every vertex v of $G[e, p]$, either $v \in M$ or v has a neighbor in M; otherwise, $M \cup \{v\}$ is the independent set of vertices properly containing M. Further, exactly one of vertices A and B (see Fig. 1) belongs to M. Obviously, M cannot contain

both A and B, but if M contains neither A nor B, then from above it must contain both C and D, which is a contradiction.

Suppose that $A \in M$. Then $M - \{A\}$ is MIS in $G[e, p-1]$ or $G[e, p-2]$, but not both. For every MIS M' in $G[e, p-1]$ containing D, we have that $M' \cup \{A\}$ is MIS in $G[e, p]$. If $D \notin M$, then $F \in M$ and $M - \{A\}$ is MIS in $G[e, p-2]$. Also, for every MIS M' in $G[e, p-2]$ containing F, we have that $M' \cup \{A\}$ is MIS in $G[e, p]$. Similar holds if $B \in M$. Since every MIS in $G[e, p-1]$ contains exactly one of C and D, and every MIS in $G[e, p-2]$ contains exactly one of E and F, we conclude that (1) holds. □

Let j_i denote the ith coordinate of the vector j.

Theorem 1: If $e_1, \ldots, e_k$ are the edges of a graph G and $p_1, \ldots, p_k \in \mathbf{N} \setminus \{1, 2\}$, then

$$M_{G[(e_1, \ldots, e_k), (p_1, \ldots, p_k)]} = \sum_{j \in \{1, 2\}^k} \left(\prod_{i=1}^{k} F_{p_i - 3 + j_i} \right) M_{G[(e_1, \ldots, e_k), j]}. \tag{2}$$

Proof: First we prove (2) for $k = 1$ by induction on p_1. If $p_1 = 3$, then

$$M_{G[e_1, 3]} = F_2 M_{G[e_1, 2]} + F_1 M_{G[e_1, 1]}.$$

Supposing that (2) is true for $k = 1$ and all $p_1 < p$ for some p, we have that

$$\begin{aligned} M_{G[e_1, p]} &= M_{G[e_1, p-1]} + M_{G[e_1, p-2]} \\ &= (F_{p-2} M_{G[e_1, 2]} + F_{p-3} M_{G[e_1, 1]}) + (F_{p-3} M_{G[e_1, 2]} + F_{p-4} M_{G[e_1, 1]}) \\ &= F_{p-1} M_{G[e_1, 2]} + F_{p-2} M_{G[e_1, 1]}. \end{aligned}$$

Now we prove (2) by induction on k. Suppose that (2) is true for some $k = n$ and for all $p_1, \ldots, p_n \in \mathbf{N} \setminus \{1, 2\}$. Let $p = (p_1, \ldots, p_n, p_{n+1})$, $p' = (p_1, \ldots, p_n)$, and $e = (e_1, \ldots, e_n, e_{n+1})$, $e' = (e_1, \ldots, e_n)$. We have that

$$\begin{aligned} M_{G[e, p]} = M_{G[(e', p')[e_{n+1}, p_{n+1}]} &= \sum_{j \in \{1, 2\}^n} \left(\prod_{i=1}^{n} F_{p_i - 3 + j_i} \right) M_{G[e', j][e_{n+1}, p_{n+1}]} \\ &= \sum_{j \in \{1, 2\}^n} \left(\prod_{i=1}^{n} F_{p_i - 3 + j_i} \right) (F_{p_{n+1} - 1} M_{G[e', j][e_{n+1}, 2]} + F_{p_{n+1} - 2} M_{G[e', j][e_{n+1}, 1]}) \\ &= \sum_{j \in \{1, 2\}^{n+1}} \left(\prod_{i=1}^{n+1} F_{p_i - 3 + j_i} \right) M_{G[e, j]}. \quad \square \end{aligned}$$

If we define $F_0 = F_2 - F_1 = 0$ and $F_{-1} = F_1 - F_0 = 1$, then we can drop the assumption that $p_i \neq 1, 2$, $i = 1, \ldots, k$ in the previous theorem.

3. MIS IN STAR-LIKE LADDERS

Theorem 2: If $p_1, \ldots, p_k \in \mathbf{N}$, then

$$M_{SL(p_1, \ldots, p_k)} = (2^k - 2) \prod_{i=1}^{k} F_{p_i} + 2 \prod_{i=1}^{k} F_{p_i + 1}.$$

Proof: Let $j \in \{1, 2\}^k$ with $j_{(1)}$ coordinates equal to 1, and $j_{(2)}$ coordinates equal to 2. We prove that

$$M_{K_2[(e,\ldots,e),\,j]} = 2^k + 2\cdot 2^{j_{(2)}} - 2, \tag{3}$$

where e is the edge of K_2. Let M be MIS of $K_2[(e, \ldots, e), j]$ (see Fig. 2). If $X \in M$, then $A_i \in M$ for $i = 1, \ldots, j_{(1)}$, and either $C_i \in M$ or $D_i, E_i \in M$ for $i = 1, \ldots, j_{(2)}$. Similar holds if $Y \in M$, and this gives $2\cdot 2^{j_{(2)}}$ MIS of $K_2[(e, \ldots, e), j]$. If $X, Y \notin M$, then either $A_i \in M$ or $B_i \in M$ for $i = 1, \ldots, j_{(1)}$ and either $C_i, F_i \in M$ or $D_i, E_i \in M$ for $i = 1, \ldots, j_{(2)}$, giving 2^k possibilities. Here we must exclude sets $\{A_1, \ldots, A_{j_{(1)}}, D_1, E_1, \ldots, D_{j_{(2)}}, E_{j_{(2)}}\}$ and $\{B_1, \ldots, B_{j_{(1)}}, C_1, F_1, \ldots, C_{j_{(2)}}, F_{j_{(2)}}\}$ which are not MIS, and so it follows that (3) holds. Now

$$\begin{aligned}
M_{SL(p_1,\ldots,p_k)} &= \sum_{j\in\{1,2\}^k}\left(\prod_{i=1}^{k} F_{p_i-3+j_i}\right) M_{K_2[(e,\ldots,e),\,j]} \\
&= \sum_{j\in\{1,2\}^k}\left(\prod_{i=1}^{k} F_{p_i-3+j_i}\right)(2^k + 2\cdot 2^{j_{(2)}} - 2) \\
&= (2^k-2)\prod_{i=1}^{k}(F_{p_i-2}+F_{p_i-1}) + 2\prod_{i=1}^{k}(F_{p_i-2}+2F_{p_i-1}) \\
&= (2^k-2)\prod_{i=1}^{k} F_{p_i} + 2\prod_{i=1}^{k} F_{p_i+1}. \quad \square
\end{aligned}$$

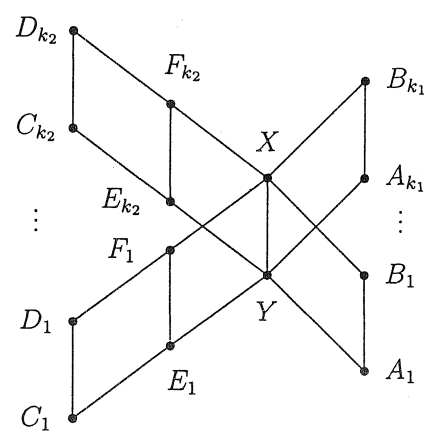

FIGURE 2. The Graph $K_2[(e, \ldots, e), (1, \ldots, 1, 2, \ldots, 2)]$

As an immediate consequence, we get

Corollary 1: If $p \in \mathbf{N}$, then $M_{L_p} = 2F_{p+1}$.

REFERENCE

1. L. K. Sanders. "A Proof from Graph Theory for a Fibonacci Identity." *The Fibonacci Quarterly* **28.1** (1990):48-55.

AMS Classification Numbers: 05C69, 05A15, 11B39

RECIPROCAL SUMS OF SECOND-ORDER RECURRENT SEQUENCES

Hong Hu
Dept. of Math., Huaiyin Normal College, Huaiyin 223001, Jiangsu Province, P.R. China

Zhi-Wei Sun*
Dept. of Math., Nanjing University, Nanjing 210093, P.R. China
E-mail: zwsun@nju.edu.cn

Jian-Xin Liu
The Fundamental Division, Nanjing Engineering College, Nanjing 210013, P.R. China
(Submitted March 1999-Final Revision June 1999)

1. INTRODUCTION

Let $\mathbb{Z}$ and $\mathbb{R}$ ($\mathbb{C}$) denote the ring of the integers and the field of real (complex) numbers, respectively. For a field F, we put $F^* = F \setminus \{0\}$. Fix $A \in \mathbb{C}$ and $B \in \mathbb{C}^*$, and let $\mathcal{L}(A, B)$ consist of all those second-order recurrent sequences $\{w_n\}_{n\in\mathbb{Z}}$ of complex numbers satisfying the recursion:

$$w_{n+1} = Aw_n - Bw_{n-1} \text{ (i.e., } Bw_{n-1} = Aw_n - w_{n+1}) \text{ for } n = 0, \pm 1, \pm 2, \ldots. \tag{1}$$

For sequences in $\mathcal{L}(A, B)$, the corresponding characteristic equation is $x^2 - Ax + B = 0$, whose roots $(A \pm \sqrt{A^2 - 4B})/2$ are denoted by α and β. If $A \in \mathbb{R}^*$ and $\Delta = A^2 - 4B \geq 0$, then we let

$$\alpha = \frac{A - \mathrm{sg}(A)\sqrt{\Delta}}{2} \quad \text{and} \quad \beta = \frac{A + \mathrm{sg}(A)\sqrt{\Delta}}{2} \tag{2}$$

where $\mathrm{sg}(A) = 1$ if $A > 0$, and $\mathrm{sg}(A) = -1$ if $A < 0$. In the case $w_1 = \alpha w_0$, it is easy to see that $w_n = \alpha^n w_0$ for any integer n. If $A = 0$, then $w_{2n} = (-B)^n w_0$ and $w_{2n+1} = (-B)^n w_1$ for all $n \in \mathbb{Z}$. The Lucas sequences $\{u_n\}_{n\in\mathbb{Z}}$ and $\{v_n\}_{n\in\mathbb{Z}}$ in $\mathcal{L}(A, B)$ take special values at $n = 0, 1$, namely,

$$u_0 = 0,\ u_1 = 1,\ v_0 = 2, v_1 = A. \tag{3}$$

It is well known that

$$(\alpha - \beta)u_n = \alpha^n - \beta^n \quad \text{and} \quad v_n = \alpha^n + \beta^n \ \text{ for } n \in \mathbb{Z}. \tag{4}$$

If $A = 1$ and $B = -1$, then those $F_n = u_n$ and $L_n = v_n$ are called Fibonacci numbers and Lucas numbers, respectively.

Let m be a positive integer. In 1974, I. J. Good [2] showed that

$$\sum_{n=0}^{m} \frac{1}{F_{2^n}} = 3 - \frac{F_{2^m-1}}{F_{2^m}}, \quad \text{i.e.,} \quad \sum_{n=0}^{m-1} \frac{(-1)^{2^n}}{F_{2^{n+1}}} = -\frac{F_{2^m-1}}{F_{2^m}};$$

V. E. Hoggatt, Jr., and M. Bicknell [4] extended this by evaluating $\sum_{n=0}^{m} F_{k2^n}^{-1}$, where k is a positive integer. In 1977, W. E. Greig [3] was able to determine the sum $\sum_{n=0}^{m} u_{k2^n}^{-1}$ with $B = -1$; in 1995, R. S. Melham and A. G. Shannon [5] gave analogous results in the case $B = 1$. In 1990, R. André-Jeannin [1] calculated $\sum_{n=1}^{\infty} 1/(u_{kn}u_{k(n+1)})$ and $\sum_{n=1}^{\infty} 1/(v_{kn}v_{k(n+1)})$ in the case $B = -1$ and

* This author is responsible for all the communications, and was supported by the Teaching and Research Award Fund for Outstanding Young Teachers in Higher Education Institutions of MOE, and the National Natural Science Foundation of the People's Republic of China.

$2 \nmid k$, using the Lambert series $L(x) = \sum_{n=1}^{\infty} x^n/(1-x^n)$ $(|x|<1)$; in 1995, Melham and Shannon [5] computed the sums in the case $B=1$, in terms of α and β.

In the present paper we obtain the following theorems that imply all of the above.

Theorem 1: Let m be a positive integer, and f a function such that $f(n) \in \mathbb{Z}$ and $w_{f(n)} \neq 0$ for all $n = 0, 1, \ldots, m$. Then

$$\sum_{n=0}^{m-1} \frac{B^{f(n)} u_{\Delta f(n)}}{w_{f(n)} w_{f(n+1)}} = \frac{B^{f(0)} u_{f(m)-f(0)}}{w_{f(0)} w_{f(m)}}, \tag{5}$$

where $\Delta f(n) = f(n+1) - f(n)$. If $w_1 \neq \alpha w_0$, then

$$\sum_{n=0}^{m-1} \frac{(-1)^n}{w_{f(n)}} \left(\frac{2\alpha^{f(n)}}{w_1 - \alpha w_0} - \frac{B^{f(n)} u_{\Delta f(n)}}{w_{f(n+1)}} \right) = \frac{1}{w_1 - \alpha w_0} \left(\frac{\alpha^{f(0)}}{w_{f(0)}} - (-1)^m \frac{\alpha^{f(m)}}{w_{f(m)}} \right). \tag{6}$$

Theorem 2: Suppose that $A, B \in \mathbb{R}^*$ and $\Delta = A^2 - 4B \geq 0$. Let $f : \{0, 1, 2, \ldots\} \to \{k \in \mathbb{Z} : w_k \neq 0\}$ be a function such that $\lim_{n \to +\infty} f(n) = +\infty$. If $w_1 \neq \alpha w_0$, then we have

$$\begin{aligned} \sum_{n=0}^{\infty} \frac{B^{f(n)} u_{\Delta f(n)}}{w_{f(n)} w_{f(n+1)}} &= \frac{\alpha^{f(0)}}{(w_1 - \alpha w_0) w_{f(0)}} \\ &= \sum_{n=0}^{\infty} \frac{(-1)^n}{w_{f(n)}} \left(\frac{2\alpha^{f(n)}}{w_1 - \alpha w_0} - \frac{B^{f(n)} u_{\Delta f(n)}}{w_{f(n+1)}} \right). \end{aligned} \tag{7}$$

In the next section we will derive several results from these theorems. Theorems 1 and 2 are proved in Section 3.

2. CONSEQUENCES OF THEOREMS 1 AND 2

Theorem 3: Let k and l be integers such that $w_{kn+l} \neq 0$ for all $n = 0, 1, 2, \ldots$. Then

$$u_k \sum_{n=0}^{m-1} \frac{B^{kn}}{w_{kn+l} w_{k(n+1)+l}} = \frac{u_{km}}{w_l w_{km+l}} \quad \text{for all } m = 1, 2, 3, \ldots. \tag{8}$$

If $A, B \in \mathbb{R}^*$, $A^2 \geq 4B$, $k > 0$, and $w_1 \neq \alpha w_0$, then

$$\sum_{n=0}^{\infty} \frac{u_k B^{kn+l}}{w_{kn+l} w_{k(n+1)+l}} = \frac{\alpha^l}{(w_1 - \alpha w_0) w_l} \tag{9}$$

and

$$\sum_{n=0}^{\infty} \left(2\frac{(-\alpha^k)^n}{w_{kn+l}} - (w_1 - \alpha w_0) u_k \beta^l \frac{(-B^k)^n}{w_{kn+l} w_{k(n+1)+l}} \right) = \frac{1}{w_l}. \tag{10}$$

Proof: Simply apply Theorems 1 and 2 with $f(n) = kn + l$.

Remark 1: When $B = 1$, $l = k$, and $\{w_n\} = \{u_n\}$ or $\{v_n\}$, Melham and Shannon [5] obtained (8) with the right-hand side replaced by a complicated expression in terms of α and β.

Theorem 4: Let $A, B \in \mathbb{R}^*$ and $\Delta = A^2 - 4B > 0$. Then, for any positive integer k, we have

$$\sum_{n=1}^{\infty}\frac{(-B^k)^n}{u_{kn}u_{k(n+1)}}=\frac{\alpha^k}{u_k^2}+\mathrm{sg}(A)\frac{\sqrt{\Delta}}{u_k}\left(4L\left(\frac{\alpha^{4k}}{B^{2k}}\right)-2L\left(\frac{\alpha^{2k}}{B^k}\right)\right) \tag{11}$$

and

$$\sum_{n=1}^{\infty}\frac{(-B^k)^n}{v_{kn}v_{k(n+1)}}=\frac{\mathrm{sg}(A)}{\sqrt{\Delta}}\left(\frac{\alpha^k}{u_{2k}}-\frac{2}{u_k}\left(4L\left(\frac{\alpha^{8k}}{B^{4k}}\right)-4L\left(\frac{\alpha^{4k}}{B^{2k}}\right)+L\left(\frac{\alpha^{2k}}{B^k}\right)\right)\right). \tag{12}$$

Proof: Clearly, $|\alpha|<|\beta|$ and $\beta-\alpha=\mathrm{sg}(A)\sqrt{\Delta}$. Thus, $u_n=(\beta^n-\alpha^n)/(\beta-\alpha)$ and $v_n=\alpha^n+\beta^n$ are nonzero for all $n\in\mathbb{Z}\setminus\{0\}$. Obviously $u_1-\alpha u_0=1$ and $v_1-\alpha v_0=A-2\alpha=\beta-\alpha=\mathrm{sg}(A)\sqrt{\Delta}$. Applying Theorem 3 with $l=k$ and $\{w_n\}_{n\in\mathbb{Z}}=\{u_n\}_{n\in\mathbb{Z}}$ or $\{v_n\}_{n\in\mathbb{Z}}$, we then obtain

$$\sum_{n=1}^{\infty}\left(u_k\frac{(-B^k)^n}{u_{kn}u_{k(n+1)}}-2\frac{(-\alpha^k)^n}{u_{kn}}\right)=\frac{\alpha^k}{u_k}$$

and

$$\sum_{n=1}^{\infty}\left(u_k\frac{(-B^k)^n}{v_{kn}v_{k(n+1)}}-\frac{2}{\mathrm{sg}(A)\sqrt{\Delta}}\cdot\frac{(-\alpha^k)^n}{v_{kn}}\right)=\frac{\alpha^k/v_k}{\mathrm{sg}(A)\sqrt{\Delta}}.$$

Clearly,

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{(-\alpha^k)^n}{u_{kn}}&=\sum_{n=1}^{\infty}(\beta-\alpha)\frac{(-\alpha^k)^n}{\beta^{kn}-\alpha^{kn}}=(\beta-\alpha)\sum_{n=1}^{\infty}\frac{(-1)^n(\alpha/\beta)^{kn}}{1-(\alpha/\beta)^{kn}}\\&=(\beta-\alpha)\left(2\sum_{\substack{n=1\\2|n}}^{\infty}\frac{(\alpha/\beta)^{kn}}{1-(\alpha/\beta)^{kn}}-\sum_{n=1}^{\infty}\frac{(\alpha/\beta)^{kn}}{1-(\alpha/\beta)^{kn}}\right)\\&=(\beta-\alpha)\left(2L\left(\frac{\alpha^{2k}}{\beta^{2k}}\right)-L\left(\frac{\alpha^k}{\beta^k}\right)\right)=\mathrm{sg}(A)\sqrt{\Delta}\left(2L\left(\frac{\alpha^{4k}}{B^{2k}}\right)-L\left(\frac{\alpha^{2k}}{B^k}\right)\right).\end{aligned}$$

If $|x|<1$, then

$$\begin{aligned}\sum_{n=1}^{\infty}(-1)^n\frac{x^n}{1+x^n}&=2\sum_{n=1}^{\infty}\frac{x^{2n}}{1+x^{2n}}-\sum_{n=1}^{\infty}\frac{x^n}{1+x^n}\\&=2\sum_{n=1}^{\infty}\left(\frac{x^{2n}}{1-x^{2n}}-\frac{2x^{4n}}{1-x^{4n}}\right)-\sum_{n=1}^{\infty}\left(\frac{x^n}{1-x^n}-\frac{2x^{2n}}{1-x^{2n}}\right)\\&=2L(x^2)-4L(x^4)-L(x)+2L(x^2)=-4L(x^4)+4L(x^2)-L(x).\end{aligned}$$

Thus,

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{(-\alpha^k)^n}{v_{kn}}&=\sum_{n=1}^{\infty}\frac{(-\alpha^k)^n}{\alpha^{kn}+\beta^{kn}}=\sum_{n=1}^{\infty}(-1)^n\frac{(\alpha/\beta)^{kn}}{1+(\alpha/\beta)^{kn}}\\&=-4L\left(\frac{\alpha^{4k}}{\beta^{4k}}\right)+4L\left(\frac{\alpha^{2k}}{\beta^{2k}}\right)-L\left(\frac{\alpha^k}{\beta^k}\right)\\&=-4L\left(\frac{\alpha^{8k}}{B^{4k}}\right)+4L\left(\frac{\alpha^{4k}}{B^{2k}}\right)-L\left(\frac{\alpha^{2k}}{B^k}\right).\end{aligned}$$

Combining the above and noting that $u_kv_k=u_{2k}$, we then obtain the desired (11) and (12).

Remark 2: If $|x| < 1$ then

$$L(-x) = \sum_{n=1}^{\infty} \frac{x^{2n}}{1-x^{2n}} - \sum_{n=1}^{\infty} \frac{x^n}{1+x^n} + \sum_{n=1}^{\infty} \frac{x^{2n}}{1+x^{2n}}$$
$$= L(x^2) - (L(x) - 2L(x^2)) + (L(x^2) - 2L(x^4)) = -2L(x^4) + 4L(x^2) - L(x).$$

Thus, Theorem 2 of André-Jeannin [1] is essentially our (11) and (12) in the special case $B = -1$ and $2 \nmid k$.

Theorem 5: Let k, l, $m \in \mathbb{Z}$ and l, $m > 0$. If $w_{\binom{k+n}{l}} \neq 0$ for all $n = 0, 1, \ldots, m$, then

$$\sum_{n=0}^{m-1} \frac{B^{\binom{k+n}{l}} u_{\binom{k+n}{l-1}}}{w_{\binom{k+n}{l}} w_{\binom{k+n+1}{l}}} = \frac{B^{\binom{k}{l}} u_{\binom{k+m}{l}-\binom{k}{l}}}{w_{\binom{k}{l}} w_{\binom{k+m}{l}}}. \tag{13}$$

Proof: Let $f(n) = \binom{k+n}{l}$ for $n \in \mathbb{Z}$. It is well known that $\Delta f(n) = \binom{k+n+1}{l} - \binom{k+n}{l} = \binom{k+n}{l-1}$. So Theorem 5 follows from Theorem 1.

Remark 3: In the case $k = 0$ and $l = 2$, (13) says that

$$\sum_{n=0}^{m-1} \frac{u_n B^{n(n-1)/2}}{w_{n(n-1)/2} w_{n(n+1)/2}} = \frac{u_{m(m-1)/2}}{w_0 w_{m(m-1)/2}}. \tag{14}$$

Theorem 6: Let a, k be integers, and m a positive integer. Suppose that $w_{ka^n} \neq 0$ for each $n = 0, 1, \ldots, m$. Then

$$\sum_{n=0}^{m-1} \frac{B^{ka^n} u_{k(a-1)a^n}}{w_{ka^n} w_{ka^{n+1}}} = \frac{B^k u_{k(a^m-1)}}{w_k w_{ka^m}}. \tag{15}$$

Proof: Just put $f(n) = ka^n$ in Theorem 1.

Remark 4: In the case $a = 2$ and $\{w_n\} = \{u_n\}$, (15) becomes

$$\sum_{n=0}^{m-1} \frac{B^{k2^n}}{u_{k2^{n+1}}} = \frac{B^k u_{k(2^m-1)}}{u_k u_{k2^m}}. \tag{16}$$

This was obtained by Melham and Shannon [5] in the case $B = 1$ and $k > 0$. In the case $a = 3$ and $\{w_n\} = \{v_n\}$, (15) turns out to be

$$\sum_{n=0}^{m-1} \frac{B^{k3^n} u_{k3^n}}{v_{k3^{n+1}}} = \frac{B^k u_{k(3^m-1)}}{v_k v_{k3^m}} \tag{17}$$

since $u_{2h} = u_h v_h$ for $h \in \mathbb{Z}$.

Theorem 7: Let k be an integer and m a positive integer. If $w_{k(2^n-1)} \neq 0$ for each $n = 0, 1, \ldots, m$, then

$$\sum_{n=0}^{m-1} \frac{B^{k(2^n-1)} u_{k2^n}}{w_{k(2^n-1)} w_{k(2^{n+1}-1)}} = \frac{u_{k(2^m-1)}}{w_0 w_{k(2^m-1)}}. \tag{18}$$

Proof: Just apply Theorem 1 with $f(n) = k(2^n - 1)$.

3. PROOFS OF THEOREMS 1 AND 2

Lemma 1: For $k, l, m \in \mathbb{Z}$, we have

$$w_k u_{l+m} - w_{k+m} u_l = B^l w_{k-l} u_m \tag{19}$$

and

$$w_k \alpha^l - w_l \alpha^k = (w_1 - \alpha w_0) B^l u_{k-l}. \tag{20}$$

Proof: (i) Fix $k, l \in \mathbb{Z}$. Observe that

$$\begin{pmatrix} w_{k+1} & w_k \\ u_{l+1} & u_l \end{pmatrix} = \begin{pmatrix} w_k & w_{k-1} \\ u_l & u_{l-1} \end{pmatrix} \begin{pmatrix} A & 1 \\ -B & 0 \end{pmatrix}$$

$$= \begin{pmatrix} w_{k-1} & w_{k-2} \\ u_{l-1} & u_{l-2} \end{pmatrix} \begin{pmatrix} A & 1 \\ -B & 0 \end{pmatrix}^2 = \cdots = \begin{pmatrix} w_{k-l+1} & w_{k-l} \\ u_1 & u_0 \end{pmatrix} \begin{pmatrix} A & 1 \\ -B & 0 \end{pmatrix}^l.$$

Taking the determinants, we then get that

$$\begin{vmatrix} w_{k+1} & w_k \\ u_{l+1} & u_l \end{vmatrix} = \begin{vmatrix} w_{k-l+1} & w_{k-l} \\ 1 & 0 \end{vmatrix} \times \begin{vmatrix} A & 1 \\ -B & 0 \end{vmatrix}^l,$$

i.e., $w_k u_{l+1} - w_{k+1} u_l = B^l w_{k-l}$. Thus, (19) holds for $m = 0, 1$.

Each side of (19) can be viewed as a sequence in $\mathcal{L}(A, B)$ with respect to the index m. By induction, (19) is valid for every $m = 0, 1, 2, \ldots$; also (19) holds for each $m = -1, -2, -3, \ldots$. Thus, (19) holds for any $m \in \mathbb{Z}$.

(ii) By induction on l, we find that $w_{l+1} - \alpha w_l = (w_1 - \alpha w_0)\beta^l$. Clearly, both sides of (20) lie in $\mathcal{L}(A, B)$ with respect to the index k. Note that, if $k = l$, then both sides of (20) are zero. As

$$(w_1 - \alpha w_0) B^l = (w_1 - \alpha w_0)\beta^l \alpha^l = (w_{l+1} - \alpha w_l)\alpha^l = \alpha^l w_{l+1} - \alpha^{l+1} w_l,$$

(20) also holds for $k = l + 1$. Therefore, (20) is always valid and we are done.

Proof of Theorem 1: Let $d \in \mathbb{Z}$. In view of Lemma 1, for $n = 0, 1, \ldots, m-1$, we have

$$\frac{u_{d+f(n+1)}}{w_{f(n+1)}} - \frac{u_{d+f(n)}}{w_{f(n)}} = \frac{u_{d+f(n+1)} w_{f(n)} - u_{d+f(n)} w_{f(n+1)}}{w_{f(n)} w_{f(n+1)}}$$

$$= \frac{w_{f(n)} u_{d+f(n)+\Delta f(n)} - w_{f(n)+\Delta f(n)} u_{d+f(n)}}{w_{f(n)} w_{f(n+1)}} = \frac{B^{d+f(n)} w_{-d} u_{\Delta f(n)}}{w_{f(n)} w_{f(n+1)}}.$$

It follows that

$$\sum_{n=0}^{m-1} \frac{B^{d+f(n)} w_{-d} u_{\Delta f(n)}}{w_{f(n)} w_{f(n+1)}} = \sum_{n=0}^{m-1} \left(\frac{u_{d+f(n+1)}}{w_{f(n+1)}} - \frac{u_{d+f(n)}}{w_{f(n)}} \right) = \frac{u_{d+f(m)}}{w_{f(m)}} - \frac{u_{d+f(0)}}{w_{f(0)}}$$

and that

$$\sum_{n=0}^{m-1} (-1)^{n+1} \frac{B^{d+f(n)} w_{-d} u_{\Delta f(n)}}{w_{f(n)} w_{f(n+1)}} = \sum_{n=0}^{m-1} \left((-1)^{n+1} \frac{u_{d+f(n+1)}}{w_{f(n+1)}} + (-1)^n \frac{u_{d+f(n)}}{w_{f(n)}} \right)$$

$$= 2\sum_{n=0}^{m-1} (-1)^n \frac{u_{d+f(n)}}{w_{f(n)}} + (-1)^m \frac{u_{d+f(m)}}{w_{f(m)}} - (-1)^0 \frac{u_{d+f(0)}}{w_{f(0)}}.$$

Putting $d = -f(0)$, we then obtain (5) and

$$\sum_{n=0}^{m-1}(-1)^{n+1}w_{f(0)}\frac{B^{f(n)}u_{\Delta f(n)}}{w_{f(n)}w_{f(n+1)}}=2\sum_{n=0}^{m-1}(-1)^n\frac{B^{f(0)}u_{f(n)-f(0)}}{w_{f(n)}}+(-1)^m\frac{B^{f(0)}u_{f(m)-f(0)}}{w_{f(m)}}.$$

Now suppose that $w_1 \neq \alpha w_0$. By Lemma 1, for each $n = 0, 1, \ldots, m$,

$$\alpha^{f(0)}w_{f(n)}-\alpha^{f(n)}w_{f(0)}=(w_1-\alpha w_0)B^{f(0)}u_{f(n)-f(0)},$$

i.e.,

$$-\frac{B^{f(0)}u_{f(n)-f(0)}}{w_{f(n)}}=\frac{\alpha^{f(n)}w_{f(0)}}{(w_1-\alpha w_0)w_{f(n)}}-\frac{\alpha^{f(0)}}{w_1-\alpha w_0}.$$

Thus,

$$\begin{aligned}&w_{f(0)}\sum_{n=0}^{m-1}(-1)^n\frac{B^{f(n)}u_{\Delta f(n)}}{w_{f(n)}w_{f(n+1)}}\\&=2\sum_{n=0}^{m-1}(-1)^n\left(\frac{w_{f(0)}\alpha^{f(n)}}{(w_1-\alpha w_0)w_{f(n)}}-\frac{\alpha^{f(0)}}{w_1-\alpha w_0}\right)+(-1)^m\left(\frac{w_{f(0)}\alpha^{f(m)}}{(w_1-\alpha w_0)w_{f(m)}}-\frac{\alpha^{f(0)}}{w_1-\alpha w_0}\right)\end{aligned}$$

and hence

$$\begin{aligned}&\sum_{n=0}^{m-1}\frac{(-1)^n}{w_{f(n)}}\left(\frac{2\alpha^{f(n)}}{w_1-\alpha w_0}-\frac{B^{f(n)}u_{\Delta f(n)}}{w_{f(n+1)}}\right)\\&=\frac{2}{w_1-\alpha w_0}\sum_{n=0}^{m-1}(-1)^n\frac{\alpha^{f(0)}}{w_{f(0)}}+\frac{(-1)^m}{w_1-\alpha w_0}\left(\frac{\alpha^{f(0)}}{w_{f(0)}}-\frac{\alpha^{f(m)}}{w_{f(m)}}\right)\\&=\frac{1}{w_1-\alpha w_0}\left(\frac{\alpha^{f(0)}}{w_{f(0)}}-(-1)^m\frac{\alpha^{f(m)}}{w_{f(m)}}\right).\end{aligned}$$

This proves (6).

Lemma 2: Let $A, B \in \mathbb{R}^*$ and $\Delta = A^2 - 4B \geq 0$. Then

$$\lim_{n\to+\infty}\frac{\alpha^n}{u_n}=0 \tag{21}$$

and

$$\lim_{n\to+\infty}\frac{w_n}{u_{m+n}}=\frac{w_1-\alpha w_0}{\beta^m}\quad\text{for any } m\in\mathbb{Z}. \tag{22}$$

Proof: When $\Delta = 0$ (i.e., $\alpha = \beta$), by induction $u_n = n(A/2)^{n-1}$ for all $n \in \mathbb{Z}$; thus, $u_n \neq 0$ for $n = \pm 1, \pm 2, \pm 3, \ldots$,

$$\lim_{n\to+\infty}\frac{\alpha^n}{u_n}=\lim_{n\to+\infty}\frac{(A/2)^n}{n(A/2)^{n-1}}=0$$

and

$$\lim_{n\to+\infty}\frac{u_{m+n}}{u_n}=\lim_{n\to+\infty}\frac{(m+n)(A/2)^{m+n-1}}{n(A/2)^{n-1}}=\left(\frac{A}{2}\right)^m=\beta^m.$$

In the case $\Delta > 0$, $|\alpha| < |\beta|$; hence, $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ is zero if and only if $n = 0$. Thus,

$$\lim_{n\to+\infty}\frac{\alpha^n}{u_n}=(\alpha-\beta)\lim_{n\to+\infty}\frac{1}{1-(\beta/\alpha)^n}=0.$$

Also

$$\lim_{n\to+\infty}\left(\frac{u_{n+1}}{u_n}-\beta\right)=\lim_{n\to+\infty}\frac{\alpha^{n+1}-\beta^{n+1}-\beta(\alpha^n-\beta^n)}{\alpha^n-\beta^n}=\lim_{n\to+\infty}\frac{\alpha-\beta}{1-(\beta/\alpha)^n}=0.$$

If $m\in\{0,1,2,\ldots\}$, then

$$\lim_{n\to+\infty}\frac{u_{m+n}}{u_n}=\lim_{n\to+\infty}\prod_{0\le k<m}\frac{u_{k+n+1}}{u_{k+n}}=\beta^m$$

and

$$\lim_{n\to+\infty}\frac{u_{n-m}}{u_n}=\lim_{n\to+\infty}\frac{u_n}{u_{m+n}}=\beta^{-m}.$$

In view of the above, (21) always holds and $\lim_{n\to+\infty}u_{m+n}/u_n=\beta^m$ for all $m\in\mathbb{Z}$. By Lemma 1, $w_1u_n-w_nu_1=Bw_0u_{n-1}$ for $n\in\mathbb{Z}$. Therefore,

$$\lim_{n\to+\infty}\frac{w_n}{u_n}=w_1-\frac{Bw_0}{\lim_{n\to+\infty}u_n/u_{n-1}}=w_1-\frac{Bw_0}{\beta}=w_1-\alpha w_0,$$

and hence (22) is valid.

Proof of Theorem 2: Assume that $w_1\neq\alpha w_0$. In view of Lemma 2,

$$\lim_{m\to+\infty}\frac{B^{f(0)}u_{f(m)-f(0)}}{w_{f(m)}}=B^{f(0)}\frac{\beta^{-f(0)}}{w_1-\alpha w_0}=\frac{\alpha^{f(0)}}{w_1-\alpha w_0}$$

and

$$\lim_{m\to+\infty}\frac{\alpha^m}{w_m}=\lim_{m\to+\infty}\frac{\alpha^m}{u_m}\times\lim_{m\to+\infty}\frac{u_m}{w_m}=0.$$

Applying Theorem 1, we immediately get (7).

Remark 5: On the condition of Theorem 2, if $w_1=\alpha w_0$, then by checking the proof of Theorem 2 we find that

$$\sum_{n=0}^{\infty}\frac{B^{f(n)}u_{\Delta f(n)}}{w_{f(n)}w_{f(n+1)}}=\infty. \tag{23}$$

REFERENCES

1. R. André-Jeannin. "Lambert Series and the Summation of Reciprocals in Certain Fibonacci-Lucas-Type Sequences." *The Fibonacci Quarterly* **28.3** (1990):223-26.
2. I. J. Good. "A Reciprocal Series of Fibonacci Numbers." *The Fibonacci Quarterly* **12.4** (1974):346.
3. W. E. Greig. "On Sums of Fibonacci-Type Reciprocals." *The Fibonacci Quarterly* **15.4** (1977):356-58.
4. V. E. Hoggatt, Jr., & M. Bicknell. "A Reciprocal Series of Fibonacci Numbers with Subscripts 2^nk." *The Fibonacci Quarterly* **14.5** (1976):453-55.
5. R. S. Melham & A. G. Shannon. "On Reciprocal Sums of Chebyshev Related Sequences." *The Fibonacci Quarterly* **33.2** (1995):194-202.

AMS Classification Numbers: 11B39, 11B37

❖❖❖

REMARKS ON THE "GREEDY ODD" EGYPTIAN FRACTION ALGORITHM

Jukka Pihko
Department of Mathematics, P.O. Box 4 (Yliopistonkatu 5),
FIN-00014 University of Helsinki, Finland
e-mail: Jukka.Pihko@csc.fi
(*Submitted March 1999-Final Revision August 1999*)

1. INTRODUCTION

We denote the set of positive integers by $\mathbf{N}$. Consider $a, b \in \mathbf{N}$ with

$$a < b, \quad (a, b) = 1. \tag{1.1}$$

Fibonacci, in 1202 ([8], see also [1], [7]) introduced the *greedy algorithm*: we take the greatest Egyptian fraction $1/x_1$ with $1/x_1 \le a/b$, form the difference $a/b - 1/x_1 =: a_1/b_1$ [where $(a_1, b_1) = 1$] and, if a_1/b_1 is not zero, continue similarly. It is easily seen that the sequence of numerators $a_0 := a, a_1, a_2, \ldots$ is strictly decreasing, from which it follows that after finitely many, say s, steps $(s \le a)$, the process will stop. This gives us a representation

$$\frac{a}{b} = \frac{1}{x_1} + \cdots + \frac{1}{x_s}, \quad 1 < x_1 < \cdots < x_s. \tag{1.2}$$

If b is *odd*, the *greedy odd algorithm* is defined as follows: we take the greatest Egyptian fraction $1/x_1$ with x_1 odd, $1/x_1 \le a/b$, and continue similarly. We have (see [4], [3], [5]) the interesting

Open Problem 1.1: Does the greedy odd algorithm (for b odd) always stop after finitely many steps?

In this paper, using elementary methods, we study some properties of the greedy odd algorithm. In Section 2 we fix the notation and record some obvious facts. In Section 3, the main part of this paper, we prove some results on the possibility of occurrence of certain initial sequences of the sequence $a_0 := a, a_1, a_2, \ldots$ of numerators connected with the greedy odd algorithm. We hope that at least some of our results are new.

2. THE GREEDY ODD ALGORITHM

We suppose that in (1.1) b is *odd* and sometimes we write $b = 2k+1$, where $k \in \mathbf{N}$. Now, since only odd denominators are used in the Egyptian fractions, we agree to write $x = 2n+1$, where $n \in \mathbf{N}$. To start the greedy odd algorithm, we take the unique $n_1 \in \mathbf{N}$ satisfying the condition

$$\frac{1}{2n_1+1} \le \frac{a}{2k+1} < \frac{1}{2n_1-1}, \tag{2.1}$$

and then we write

$$\frac{a}{2k+1} - \frac{1}{2n_1+1} =: \frac{a_1'}{(2k+1)(2n_1+1)} =: \frac{a_1}{2k_1+1} \quad \text{with} \quad (a_1, 2k_1+1) = 1. \tag{2.2}$$

Case A) If

$$\frac{a}{2k+1} \in \left[\frac{1}{2n_1+1}, \frac{1}{2n_1}\right),$$

then $0 \le a_1' < a$ and so $0 \le a_1 < a$ (this case corresponds to the normal greedy algorithm).

Case B) If

$$\frac{a}{2k+1} \in \left[\frac{1}{2n_1}, \frac{1}{2n_1-1}\right),$$

then it is easily seen that $a < a_1' < 2a$.

Case B1) If $d := (a_1', (2k+1)(2n_1+1)) > 1$, we cancel and find that $0 < a_1 < a$. (In fact, as d is odd, $d \ge 3$, and therefore $a_1' = da_1 < 2a$ implies that $a_1 < 2a/d \le 2a/3 < a$.)

Case B2) If $d = 1$, then $a_1 = a_1'$ and so $a < a_1 < 2a$.

We find that A) and B1) are "good" cases (numerator decreases), while B2) is a "bad" case (numerator increases).

We form the sequence of numerators $a_0 := a, a_1, a_2, \ldots$. If $a_s = 0$ for some $s \in \mathbf{N}$, then the greedy odd algorithm stops and we get

$$\frac{a}{b} = \frac{a}{2k+1} = \frac{1}{x_1} + \cdots + \frac{1}{x_s} \tag{2.3}$$

with $x_1 = 2n_1 + 1, \ldots, x_s = 2n_s + 1$. It is clear that $a_s = 0$ if and only if $a_{s-1} = 1$.

From (2.2), it follows immediately that

$$a_i \not\equiv a_{i+1} \pmod 2 \text{ for } i = 0, 1, 2, \ldots. \tag{2.4}$$

Example 2.1: The sequence of numerators $a_0, \ldots, a_{s-1}$ with $s = 19$, corresponding to the greedy odd algorithm for the fraction 5/139, is

$$5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 26, 51, 2, 3, 4, 1.$$

Here, all cases are either B1) (occurs two times) or B2). The reader can find more examples in [4] (see also Examples 3.9 below).

Remark 2.2: Take any $a \in \mathbf{N}$, $a > 1$. Then take any $b \in \mathbf{N}$, b odd, such that (1.1) holds and form the sequence of numerators $a_0 := a, a_1, a_2, \ldots$ connected with the greedy odd algorithm for the fraction a/b. The question "Does 1 occur in this sequence?" is equivalent to Open Problem 1.1 and shows some similarity to the well-known (or "infamous" [4]) "$3x+1$"-problem (see, e.g., [6]).

If the greedy odd algorithm for the fraction a/b stops with $a_s = 0$, we write

$$h\left(\frac{a}{b}\right) = h\left(\frac{a}{2k+1}\right) := s$$

for the *number of steps*. Otherwise, we write

$$h\left(\frac{a}{2k+1}\right) := \infty.$$

If $h(a/b) < \infty$, then a trivial consequence of (2.3) is that

$$h(a/b) \equiv a \pmod 2. \tag{2.5}$$

Theorem 2.3: Suppose that $s \in \mathbf{N}$ is given. There are infinitely many fractions a/b, b odd, satisfying (1.1) such that

$$h(a/b) = s. \tag{2.6}$$

Proof: Take any sequence $x_1, \ldots, x_s$ satisfying

$$x_1 > 1,\ x_{i+1} \geq x_i^2 - x_i + 1,\ i = 1, \ldots, s-1, \tag{2.7}$$

such that x_i is odd for $i = 1, \ldots, s$. (For example, we can take $x_1 := 2n+1$ for $n \in \mathbf{N}$ and then define $x_{i+1} := x_i^2 - x_i + 1$ for $i = 1, \ldots, s-1$.) According to a result of J. J. Sylvester [9], the right-hand side of the definition $a/b := 1/x_1 + \cdots + 1/x_s$ is the result of applying the normal greedy algorithm to the fraction a/b. Note that b is odd since $x_1, \ldots, x_s$ are all odd. (We take, of course, $(a, b) = 1$.) Moreover, $a < b$. (We have, in fact, $a/b < 1/2$, see (2.9) below.) But it is obvious that, if the normal greedy algorithm produces only odd denominators $x_1, \ldots, x_s$, then the greedy odd algorithm, applied to a/b, is identical to the normal greedy algorithm (all cases are A)), and so $h(a/b) = s$. Since different sequences $x_1, \ldots, x_s$ satisfying (2.7) produce different fractions a/b, and since we have indicated how to choose infinitely many such sequences (with all x_i odd), the theorem follows. □

We close this section with two remarks.

Remark 2.4: We saw in (1.2) that $x_2 > x_1$ for the normal greedy algorithm (supposing, of course, that $a > 1$). It is easily seen that, in the case of the greedy odd algorithm for the fraction a/b, b odd, satisfying (1.1), the only possibility for $x_2 = x_1$ is $x_1 = x_2 = 3$, and it occurs if and only if

$$\frac{2}{3} \leq \frac{a}{b}. \tag{2.8}$$

For example, the greedy odd algorithm gives

$$\frac{2}{3} = \frac{1}{3} + \frac{1}{3},\ \frac{4}{5} = \frac{1}{3} + \frac{1}{3} + \frac{1}{9} + \frac{1}{45},\ \frac{5}{7} = \frac{1}{3} + \frac{1}{3} + \frac{1}{21},\ \text{and}\ \frac{6}{7} = \frac{1}{3} + \frac{1}{3} + \frac{1}{7} + \frac{1}{21}.$$

Remark 2.5: If (1.1) holds and b is *even*, then it is clear that the greedy odd algorithm never stops. It is easily seen, for example, that

$$\frac{1}{2} = \frac{1}{3} + \frac{1}{7} + \frac{1}{43} + \cdots = \sum_{i=1}^{\infty} \frac{1}{x_i}, \tag{2.9}$$

where $x_1 := 3$, $x_{i+1} := x_i^2 - x_i + 1$ for $i = 1, 2, \ldots$, is the result of applying the greedy odd algorithm to the fraction $1/2$. The equation (2.9) is, of course, well known (indeed, "famous" [2]).

3. ON SOME INITIAL SEQUENCES OF NUMERATORS

We are interested in the case B) of the greedy odd algorithm (see the beginning of Section 2). We suppose that $a > 1$ and $a < c < 2a$ with $c \in \mathbf{N}$. We search for odd $b = 2k+1$, such that in the first step of the greedy odd algorithm for the fraction a/b, we have $c = a_1'$ (see (2.2)). Here we must suppose that $a \not\equiv c \pmod 2$ (see (2.4)).

Theorem 3.1: Let $a > 1$ and $a < c < 2a$, where $1 + c - a := 2t$ ($t \in \mathbf{N}$). Let $k \in \mathbf{N}$ satisfy $k + t \equiv 0 \pmod a$ and $(a, 2k+1) = 1$. Take $n_1 := (k+t)/a \in \mathbf{N}$. Then $a < 2k+1$, and in the first step of the

greedy odd algorithm for the fraction $a/(2k+1)$, we have the case B). Moreover, $x_1 = 2n_1 + 1$, and

$$\frac{a}{2k+1} - \frac{1}{2n_1+1} = \frac{c}{(2k+1)(2n_1+1)}. \tag{3.1}$$

Proof: We have, by assumption,

$$2t = 1 + c - a < 1 + 2a - a = 1 + a. \tag{3.2}$$

Since $k + t \equiv 0 \pmod{a}$, we have $k + t \geq a$, implying by (3.2) that $k \geq a - t > a - (a+1)/2 = (a-1)/2$. Therefore, $a < 2k+1$.

We prove next that

$$\left\lceil \frac{2k+1}{a} \right\rceil = 2n_1, \tag{3.3}$$

from which it immediately follows that $x_1 = 2n_1 + 1$.

We have $2n_1 = (2k+2t)/a = (2k+1)/a + (2t-1)/a$, where, by (3.2), $0 < (2t-1)/a < 1$. This proves (3.3).

A simple calculation shows that (3.1) holds. Since $a_1' = c > a$, we must have the case B). □

Remark 3.2: In some cases, it is impossible to satisfy the condition $(a, 2k+1) = 1$ in Theorem 3.1. Take, for example, $a := 6$ and $c := 9$. Now $1 + c - a = 1 + 9 - 6 = 4 =: 2t$, so that $t = 2$. If $k + 2 \equiv 0 \pmod 6$, then $2k + 1 \equiv 3 \pmod 6$, and so $(a, 2k+1) = 3$.

Corollary 3.3: Let $a > 1$ and $c := a + 1$. If $k + 1 \equiv 0 \pmod{a}$, then $(a, 2k+1) = 1$ and, for $n_1 := (k+1)/a$, the conclusions of Theorem 3.1 hold.

Proof: In this case, $1 + c - a = 2 =: 2t$, so that $t = 1$. We need only prove that $(a, 2k+1) = 1$. This follows immediately from $2k + 1 = 2(n_1 a - 1) + 1 = 2n_1 a - 1$. □

For the rest of this paper, we consider the following problem. Let $a > 1$ be given. We search for such numbers $k \in \mathbf{N}$ that the greedy odd algorithm, applied to the fraction $a/(2k+1)$, starts with some cases B2) in such a way that the sequence of numerators $a_0 := a, a_1, a_2, \ldots$ starts with $a, a+1, a+2, \ldots$. Our main tool is Corollary 3.3 and our main achievement (see Theorem 3.7) is the following. For any $a > 1$, we give explicitly infinitely many numbers k such that the greedy odd algorithm for the fraction $a/(2k+1)$ starts with two cases B2), the numerator increasing by one in both steps.

Suppose now that we have used Corollary 3.3 once and that the first step corresponded to the case B2). We consider the fraction

$$\frac{a_1}{(2k+1)(2n_1+1)} =: \frac{a_1}{2k_1+1}, \text{ where } a_1 := a + 1,$$

and use Corollary 3.3 again. Now,

$$k_1 = \frac{(2k+1)(2n_1+1) - 1}{2} = \frac{4kn_1 + 2k + 2n_1}{2} = 2kn_1 + k + n_1,$$

so that we should have

$$2kn_1 + k + n_1 + 1 \equiv 0 \pmod{a+1}. \tag{3.4}$$

But $2kn_1+k+n_1+1=2(n_1a-1)n_1+(n_1a-1)+n_1+1=2n_1^2a+n_1a-n_1=n_1(2n_1a+a-1)$ and $2n_1a+a-1=(a+1)+2k$, so that (3.4) will be satisfied if $k\equiv 0 \pmod{a+1}$. We use the Chinese Remainder Theorem to solve the pair of simultaneous congruences

$$\begin{cases} k\equiv -1 \pmod{a} \\ k\equiv 0 \pmod{a+1} \end{cases}$$

and get the (unique) solution $k\equiv -(a+1) \pmod{a(a+1)}$. Now let $n_2:=(k_1+1)/(a+1)$. Then both steps correspond to the case B2) if and only if the conditions

(I) $$(a+1,(2k+1)(2n_1+1))=1 \text{ and}$$

(II) $$(a+2,(2k_1+1)(2n_2+1))=1$$

hold.

Lemma 3.4: Let $k:=-(a+1)+ja(a+1)$ with $j\in\mathbf{N}$. Condition (I) holds for every $j\in\mathbf{N}$.

Proof: We have $2k+1=(a+1)(2ja-2)+1$ (of course, $2k+1\equiv 1 \pmod{a+1}$ since $k\equiv 0 \pmod{a+1}$) and therefore $(a+1,2k+1)=1$. We have $n_1=(k+1)/a=j(a+1)-1$, so $2n_1+1=2j(a+1)-1$ and therefore $(a+1,2n_1+1)=1$. It follows that (I) holds for every $j\in\mathbf{N}$. □

We have $2k+1=(a+2)(2ja-2-2j)+4j+3$, $2n_1+1=(a+2)2j-(2j+1)$, and

$$2n_2+1=(a+2)(4j^2a-4j^2-6j)+(2j+1)(4j+3), \tag{3.5}$$

from which it follows, since $2k_1+1=(2k+1)(2n_1+1)$, that

$$\text{(II) holds if and only if } (a+2,(2j+1)(4j+3))=1. \tag{3.6}$$

Theorem 3.5: Let $a>1$ and define k by $k:=-(a+1)+ja(a+1)$, $j\in\mathbf{N}$. A necessary and sufficient condition for the greedy odd algorithm for all the fractions $a/(2k+1)$, $j=1,2,\ldots$, to start with two cases B2), the numerators increasing by one, is that $a=2^r-2$, $r\geq 2$.

Proof: 1° Suppose that $a=2^r-2$ for some $r\in\mathbf{N}$, $r\geq 2$. By Lemma 3.4, (I) holds for every $j\in\mathbf{N}$. Condition (II) is now trivially satisfied, since $a+2=2^r$ and $(2k_1+1)(2n_2+1)$ is odd.

2° Suppose that $a\notin\{2^r-2: r\in\mathbf{N}, r\geq 2\}$. Then there exists an odd prime p such that $p\mid(a+2)$. Let j be such that $p=2j+1$. Then $p\mid(a+2,(2j+1)(4j+3))$, so that, by (3.6), (II) is not valid. □

By a similar argument, we can show the existence of certain short sequences of numerators of the form $a, a+1, 1$, where one case B2) and one case B1) are involved. More precisely, we have

Theorem 3.6: Let $a>1$ be odd. Let

$$k:=-\left(\frac{a^3+4a^2+5a+2}{2}\right)+ha(a+1)(a+2), \text{ where } h=1,2,\ldots. \tag{3.7}$$

Then the sequence of numerators, corresponding to the greedy odd algorithm for all the fractions $a/(2k+1)$, is $a, a+1, 1$.

Proof: We write $k:=-(a+1)+ja(a+1)$ with $j\in\mathbf{N}$ as before. By Lemma 3.4, (I) holds for every $j\in\mathbf{N}$. By assumption, $a+2$ is odd, so we can find $j_0\in\mathbf{N}$ such that $2j_0+1:=a+2$. If $j\equiv j_0 \pmod{a+2}$, then $2j+1\equiv 0 \pmod{a+2}$, and so, by (3.5), $2n_2+1\equiv 0 \pmod{a+2}$. It

follows that $(a+2,(2k_1+1)(2n_2+1))=a+2$, implying $a_2=1$, for all such j. Writing $j:=j_0+(h-1)(a+2)$, we get (3.7). □

Theorem 3.5 gives, for some special numbers a, infinitely many numbers k such that the greedy odd algorithm, applied to the fraction $a/(2k+1)$, behaves in a certain manner. The first part of the next theorem is completely general, but the form of the numbers k is slightly more complicated.

Theorem 3.7: Let $a>1$ and define k by $k:=-(a+1)^2+ha(a+1)(a+2)$, $h=1,2,\ldots$. Then the greedy odd algorithm for all the fractions $a/(2k+1)$ starts with two cases B2), the numerators increasing by one. Moreover, if $a=2^r-3$ $(r\geq 3)$, then the same holds for the third step.

Proof: We consider $k:=-(a+1)+ja(a+1)$, $j\in\mathbf{N}$. By Lemma 3.4, (I) holds for every $j\in\mathbf{N}$. If $j\equiv -1 \pmod{a+2}$, then $2j+1\equiv 4j+3\equiv -1 \pmod{a+2}$, and therefore, by (3.6), condition (II) holds. Writing $j:=-1+h(a+2)$ with $h\in\mathbf{N}$, we get the first part of the theorem.

Consider now the third step. Defining $(2k_1+1)(2n_2+1)=:2k_2+1$, we should have

$$k_2+1\equiv 0 \pmod{a+2} \tag{3.8}$$

and then we will take $n_3:=(k_2+1)/(a+2)$. By a straightforward calculation,

$$\begin{aligned}\frac{k_2+1}{a+2}=&(-1+h+ah)\cdot(-1-2a+4ah+2a^2h)\cdot(4+15a+14a^2+4a^3-4h-34ah\\&-60a^2h-38a^3h-8a^4h+16ah^2+48a^2h^2+52a^3h^2+24a^4h^2+4a^5h^2),\end{aligned}$$

proving (3.8). The last part of the theorem follows now exactly as in the proof of Theorem 3.5. □

Taking $a:=2$, starting from Theorem 3.5, and using Corollary 3.3 two times, we obtained the following result.

Theorem 3.8: Let $k:=180g-51$, $g=1,2,\ldots$. The greedy odd algorithm for all the fractions $2/(2k+1)$ starts with four cases B2), the numerators increasing by one.

Since we have suppressed the "dirty" details, we would like to give some examples of Theorem 3.8.

Examples 3.9: Using ten smallest values of g in Theorem 3.8, we get the following fractions with corresponding sequences of numerators (which should all start with 2, 3, 4, 5, 6).

$\frac{2}{259}$; 2, 3, 4, 5, 6, 1. $\frac{2}{619}$; 2, 3, 4, 5, 6, 7, 8, 9, 2, 3, 4, 1.

$\frac{2}{979}$; 2, 3, 4, 5, 6, 7, 8, 9, 2, 3, 4, 1. $\frac{2}{1339}$; 2, 3, 4, 5, 6, 7, 2, 1.

$\frac{2}{1699}$; 2, 3, 4, 5, 6, 7, 8, 9, 10, 1. $\frac{2}{2059}$; 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 2, 1.

$\frac{2}{2419}$; 2, 3, 4, 5, 6, 1. $\frac{2}{2779}$; 2, 3, 4, 5, 6, 1.

$\frac{2}{3139}$; 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 1. $\frac{2}{3499}$; 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 1.

Using $g := 19$, we get

$$\frac{2}{6739}; 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 1.$$

We notice here that different fractions may have the same sequence of numerators connected with the greedy odd algorithm. The corresponding representations (2.3) are, of course, all different. Here, in the case of Theorem 3.8, we may note that, according to Corollary 3.3, $x_1 = k+2$. The first fraction $2/259$, for example, has the representation (2.3) with $s = 6$, where

$$\begin{aligned}
x_1 &= 131,\\
x_2 &= 11311,\\
x_3 &= 95942731,\\
x_4 &= 7364006009447959,\\
x_5 &= 45190487089321370649970598273443,\\
x_6 &= 175044010574581841686085399837646254461368671327857105734379019 9.
\end{aligned}$$

We remark, finally, that the sequence of numerators $2, 3, 4, 5, 6, 1$ occurs whenever $g \equiv 0, 1 \pmod 7$ in Theorem 3.8.

REFERENCES

1. M. Dunton & R. E. Grimm. "Fibonacci on Egyptian Fractions." *The Fibonacci Quarterly* **4.4** (1966):339-54.
2. P. Erdös & E. G. Straus. "On the Irrationality of Certain Ahmes Series." *J. Indian Math. Soc.* **27** (1968):129-33.
3. R. K. Guy. *Unsolved Problems in Number Theory*. 2nd ed. New York: Springer-Verlag, 1994.
4. R. K. Guy. "Nothing's New in Number Theory?" *Amer. Math. Monthly* **105** (1998):951-54.
5. V. Klee & S. Wagon. *Old and New Unsolved Problems in Plane Geometry and Number Theory*. Washington, D.C.: Mathematical Association of America, 1991.
6. J. C. Lagarias. "The $3x+1$ Problem and Its Generalizations." *Amer. Math. Monthly* **92** (1985):3-23.
7. H. Lüneburg. *Leonardi Pisani* Liber abbaci *oder Lesevergnügen eines Mathematikers.* 2nd ed. Mannheim: Bibliographisches Institut, 1993.
8. L. Pisano. *Scritti*. Vol. 1. Rome: B. Boncompagni, 1857.
9. J. J. Sylvester. "On a Point in the Theory of Vulgar Fractions." *Amer. J. Math.* **3** (1880): 332-35, 388-89.

AMS Classification Number: 11D68

USING LUCAS SEQUENCES TO FACTOR LARGE INTEGERS NEAR GROUP ORDERS

Zhenxiang Zhang*
Dept. of Math., Anhui Normal University, 241000 Wuhu, Anhui, P.R. China
e-mail: zhangzhx@mail.ahwhptt.net.cn
(*Submitted March 1999-Final Revision August 1999*)

Dedicated to the memory of P. Erdös (1913-1996)

1. INTRODUCTION

Factoring large integers into primes is one of the most important and most difficult problems of computational number theory (the twin problem is primality testing [13]). Trial division, Fermat's algorithm [1], [3], [8], Pollard's $p-1$ method [6], Williams' $p+1$ method [11], Lenstra's elliptic curve method (ECM) [5], Pomerance's quadratic sieve (QS) [7], [10], and Pollard's number field sieve (NFS) [4] are commonly used methods for factorization.

Trial division and Fermat's method are two of the oldest systematic methods of factoring integers. Although, in general, both methods are not very efficient, it is worthwhile attempting them before other methods. Trial division consists of making trial divisions of the integer N by the small primes; it succeeds when

$$N = pq, \text{ prime } p \text{ is small.} \tag{1.1}$$

The practical limit for trial division to locate a prime factor of large N is about 8-10 digits. Fermat's algorithm works in the opposite direction from trial division. It works quickly when N is the product of two almost equal factors, i.e.,

$$N = pq, \ |q-p| \text{ is small.} \tag{1.2}$$

Integers whose largest prime factor is small are called *smooth*. The $p-1$ method succeeds when

$$p-1 \text{ is smooth for some prime divisor } p \text{ of } N. \tag{1.3}$$

The method is based on the consequence of Fermat's Little Theorem: if M is a multiple of $p-1$ and if p does not divide a, then p divides $\gcd(N, a^M-1)$. If $p-1$ is smooth, then we can find a suitable M by taking the product of small primes and powers of very small primes.

In 1982, Hugh Williams [11] showed how to use the structure of Lucas sequences to factor N when

$$p+1 \text{ is smooth for some prime divisor } p \text{ of } N. \tag{1.4}$$

His method is based on the following fact about Lucas sequences (Theorem 12.8, [1]). If we choose an integer u and define a pair of Lucas sequences $U_n = U_n(u)$ and $V_n = V_n(u)$ by

$$\begin{cases} U_0 = 0,\ U_1 = 1,\ V_0 = 2,\ V_1 = u, \\ U_n = uU_{n-1} - U_{n-2},\ V_n = uV_{n-1} - V_{n-2} \ \text{ for } n \ge 2, \end{cases} \tag{1.5}$$

and, if $D = u^2 - 4$, then, for any odd prime p, p divides both $\gcd(N, U_M)$ and $\gcd(N, V_M - 2)$ whenever M is a multiple of $p-(D/p)$, where (D/p) is the Legendre symbol. If $(D/p) = -1$

* Supported by the China State Educational Commission Science Foundation and by NSF of China Grant 10071001.

and $p+1$ is smooth, then we can find a suitable M by taking the product of small primes and powers of very small primes.

So far, either textbooks [1], [3], [8] or survey papers [2], [12] on factorization treated the above four methods separately. In this paper we present algorithms not only to unify but also to enhance these four methods. We state our main results as the following two theorems.

Theorem 1: There exists an algorithm (Algorithm 1) for finding prime divisors $p<q$ of N in $O(\log^3 N+|r|\log^2 N)$ bit operations, provided

$$N=pq \text{ with } q=k(p-1)+r \text{ and } |r|<(p-3)/2. \tag{1.6}$$

Theorem 2: There exists an algorithm (Algorithm 2) for finding prime divisors $p<q$ of N in $O(\log^3 N+|r|\log^2 N)$ bit operations, provided

$$N=pq \text{ with } q=k(p+1)+r \text{ and } |r|<(p+1)/2. \tag{1.7}$$

Remark 1.1: Clearly, Algorithm 1 finds prime factors p and q of N quickly when

$$N=pq \text{ with } q=k(p-1)+r \text{ and } |r| \text{ small}, \tag{1.8}$$

and Algorithm 2 finds prime factors p and q of N quickly when

$$N=pq \text{ with } q=k(p+1)+r \text{ and } |r| \text{ small}. \tag{1.9}$$

We remark that condition (1.8) can be relaxed to

$$N=pq \text{ with } q=k'd+r',\ |r'| \text{ small, and } (p-1)/d \text{ smooth}, \tag{1.10}$$

where d is a divisor of $p-1$; whereas condition (1.9) can be relaxed to

$$N=pq \text{ with } q=k'd+r',\ |r'| \text{ small, and } (p+1)/d \text{ smooth}, \tag{1.11}$$

where d is a divisor of $p+1$. We see that conditions (1.1), (1.2), and (1.3) are contained in condition (1.10); whereas conditions (1.1), (1.2), and (1.4) are contained in condition (1.11). Thus, we have a unified approach for trial division, Fermat's method, and Pollard's $p-1$ method; and a unified approach for trial division, Fermat's method, and Williams' $p+1$ method.

2. PROOF OF THEOREM 1

To prove Theorem 1 we need two lemmas.

Lemma 2.1: Let $N=pq$ be the product of two primes $p<q$ with $q=k(p-1)+r$, where $|r|<(p-3)/2$. Let M be the number of positive integers a modulo N with

$$\gcd(a,N)=1 \quad \text{and} \quad a^N \equiv a^r \mod N. \tag{2.1}$$

Then we have $M<N/2$.

Proof: Since $p<q=k(p-1)+r$ and $|r|<(p-3)/2$, we have $k\ge 2$, or $k=1$ and $r\ge 2$. In both cases, we have $p-r<q-1$. Thus,

$$\gcd(N-r,q-1)=\gcd(p(q-1)+p-r,q-1)=\gcd(p-r,q-1)\le (q-1)/2.$$

The number of such bases a satisfying (2.1) is the number of solutions (mod N) of the congruence $f(x)=x^{N-r}-1\equiv 0 \mod N$. It is well known that congruence $f(x)\equiv 0 \mod p$ has $\gcd(N-r, p-1)=\gcd((p-1)(q+k),p-1)=p-1$ distinct solutions (mod p), and congruence $f(x)\equiv 0$ mod

q has $\gcd(N-r, q-1) \le (q-1)/2$ distinct solutions (mod q). According to the Chinese Remainder Theorem, we have

$$M = \gcd(N-r, p-1)\gcd(N-r, q-1) \le (p-1)(q-1)/2 < N/2. \quad \square$$

Lemma 2.2: Let $N = pq$ with p prime and $q = k(p-1)+r$ not necessarily prime. Let $a > 1$ with $\gcd(a, N) = 1$ and $u = a^N - a^r \bmod N$. Then we have:

(a) $p \mid \gcd(u, N)$;

(b) If q is prime and $u \ne 0$, then $\gcd(u, N) = p$.

Proof:

(a) This follows from the fact that $a^N = a^{pq} \equiv a^q = a^{k(p-1)+r} \equiv a^r \bmod p$.

(b) Since $u \ne 0 \bmod N$ and $u \equiv 0 \bmod p$, $u \ne 0 \bmod q$. Thus, we have $\gcd(u, N) = p$. $\square$

Example 2.1: Let $N = 26544669$. Then

$$2^N \equiv 19445336 \bmod N, \text{ and } \gcd(19445336 - 2^9, N) = 2823 = 941 \cdot 3.$$

In fact, $N = 941 \cdot 28209$, where 941 is prime, whereas $28209 = 30(941-1)+9 = 3 \cdot 9403$ is not prime.

Example 2.2: Let $N = 8848223$. Then

$$2^N \equiv 864787 \bmod N, \text{ and } \gcd(864787 - 2^3, N) = 941.$$

Thus, $N = 941 \cdot 9403$, where both 941 and $9403 = 10(941-1)+3$ are primes.

Example 2.3: Let $N = 8836931$. Then

$$2^N \equiv 4892191 \bmod N, \quad 2^{-1} \equiv 4418466 \bmod N,$$

$$2^{-9} \equiv 2571685 \bmod N, \text{ and } \gcd(4892191 - 2571685, N) = 941.$$

Thus, $N = 941 \cdot 9391$, where both 941 and $9391 = 10(941-1)-9$ are primes.

Now we are ready to prove Theorem 1.

Proof of Theorem 1: Suppose condition (1.6) holds. We present *Algorithm* 1 as follows:

We first select a random integer a with $1 < a < N$ and $\gcd(a, N) = 1$; and do the modular exponentiation $b = a^N \bmod N$ and calculate $a^{-1} \bmod N$ via the Euclidean algorithm. Then, for $i = 1, 2, \ldots,$ calculate $a^i = a^{i-1}a \bmod N$ and $a^{-i} = a^{-(i-1)}a^{-1} \bmod N$ by recurrence, and calculate $\gcd(b - a^i, N)$ and $\gcd(b - a^{-i}, N)$ via the Euclidean algorithm.

By Lemma 2.1, the probability that a random integer a modulo N satisfies

$$a^N \ne a^r \bmod N \tag{2.2}$$

is at least $1/2$. Suppose (2.2) holds for the chosen a. By Lemma 2.2, we have

$$\gcd(a^N - a^r, N) = p \quad \text{and} \quad q = N/p.$$

It is well known that it takes $O(\log^3 N)$ bit operations for modular exponentiation [9] and $O(\log^2 N)$ bit operations to do a gcd with naive arithmetic (Euclidean algorithm) [3]. Thus, in total, it takes $O(\log^3 N + |r| \log^2 N)$ bit operations to find prime divisors $p < q$ of N. This completes the proof. $\square$

Example 2.4: Let $N = 89603 \cdot 10^{198} + 51701096 \cdot 10^{99} + 7457884581$ (203 digits). Using Algorithm 1, we obtain $N = pq$, where both

$$p = \gcd(2^N - 2^{165}, N) = 10^{99} + 289 \quad \text{(100 digits)}$$

and

$$q = N/p = 89603(p-1) + 165 = 89603 \cdot 10^{99} + 25805829 \quad \text{(104 digits)}$$

are primes. Our Pascal program (with multi-precision package partially written in Assembly language) ran about eighteen seconds on my PC 486/66 to get the desired results.

3. COMBINED WITH POLLARD'S $p-1$ METHOD

The following *Extended Algorithm* 1 combines *Algorithm* 1 presented in the proof of Theorem 1 with Pollard's $p-1$ algorithm, thus it unifies trial division, Fermat's method, and the $p-1$ method.

Extended Algorithm 1: We first select a random integer g with $1 < g < N$ and $\gcd(g, N) = 1$. Then calculate $a = g^M \bmod N$, where M is the product of all small primes and some powers of very small primes. If $1 < \gcd(a-1, N) < N$, then a nontrivial factor is found (the $p-1$ algorithm ends up here); otherwise, calculate $b = a^N \bmod N$. If condition (1.10) holds, then the prime divisor p could be found quickly, since in this case we would most likely have $\gcd(b - a^{r'}, N) = p$.

Example 3.1: Let $N =$

21599677 4125459698 7880191329 6573463347 1444517931 6954707436
3533196547 4958078521 1295059800 6895461157 4586337662 0125667872
2212935015 1101826633 4121506661 8644391868 2033158453 4956423476
3200995905 4369044649 0215558908 4213065793 (218 digits).

Let $a = 2^M \bmod N$, where M is the product of the first 120 primes. We obtain $N = pq$, where $p = \gcd(a^N - a^{23}, N) =$

2912 4205259383 1345758783 9106248908 4606333874 4736995720
6878160308 4991206875 7497656678 0499080822 1052741991 (104 digits)

and $q = N/p =$

7416 4006262753 0801524787 1419019374 7405994078 1097519023
9058213161 4441575950 4705008092 8187116939 4073700000 0000000023
(114 digits).

The whole calculation took about twenty seconds on my PC 486. We find that

$$q = k(p-1) + r = 10^{15}d + 23,$$

where $(p-1)/d = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17$ is smooth, and $r' = 23$ is small, although $r = 245\ldots39493$ (103 digits) is large.

4. PROOF OF THEOREM 2

In this section and the following section, we need the pair of Lucas sequences $U_n = U_n(u)$ and $V_n = V_n(u)$ to the parameter u as defined by (1.5). When there is no doubt as to the values of the parameter u, we often omit it. Moreover, the U's and V's are calculated modulo N, and the

words "mod N" are often omitted, where N is the integer to be factored. We shall use both $|\,|$ and # to denote cardinality of a set, reserving the latter symbol for a set written with braces. Legendre's symbol is denoted by $\left(\frac{*}{p}\right)$ of $(*/p)$ with p an odd prime.

To prove Theorem 2 and describe *Algorithm* 2, we need four lemmas.

Lemma 4.1: Let $N = pq$, with p an odd prime and q not necessarily prime. Then we have

$$\#\left\{u : 0 \le u < N, \left(\frac{u^2-4}{p}\right) = -1\right\} = \frac{p-1}{p}\cdot\frac{N}{2}.$$

Proof: It is well known that

$$\sum_{u=0}^{p-1}\left(\frac{u^2-4}{p}\right) = -1.$$

Since

$$\#\left\{u : 0 \le u < p, \left(\frac{u^2-4}{p}\right) = 0\right\} = 2,$$

we have

$$\#\left\{u : 0 \le u < p, \left(\frac{u^2-4}{p}\right) = -1\right\} = (p-1)/2,$$

and

$$\#\left\{u : 0 \le u < p, \left(\frac{u^2-4}{p}\right) = 1\right\} = (p-3)/2.$$

Thus,

$$\#\left\{u : 0 \le u < p, \left(\frac{u^2-4}{p}\right) = -1\right\} = \frac{p-1}{2}\cdot\frac{N}{p} = \frac{p-1}{p}\cdot\frac{N}{2}. \quad \square$$

Lemma 4.2: (Lemma 12.15 of [1], see also Section 2 of [11].) If p is an odd prime, $m \in \mathbb{Z}^+$, and $\varepsilon = \left(\frac{u^2-4}{p}\right)$, then we have $U_{m(p-\varepsilon)} \equiv 0 \bmod p$, and $V_{m(p-\varepsilon)} \equiv 2 \bmod p$.

Lemma 4.3: Let $N = pq$ with p an odd prime and $q = k(p+1)+r$ not necessarily prime. Let integer u be such that $\left(\frac{u^2-4}{p}\right) = -1$. Then we have $U_{N+r} \equiv 0 \bmod p$, and $V_{N+r} \equiv 2 \bmod p$.

Proof: Since $N + r = pq + r = (p+1)(pk+r)$, the lemma follows by Lemma 4.2. $\square$

In Lemma 4.4 below we investigate the number of integers u satisfying

$$\left(\frac{u^2-4}{q}\right) = 1,\ U_{N+r}(u) \equiv 0 \bmod q, \text{ and } V_{N+r}(u) \equiv 2 \bmod q; \tag{4.1}$$

or satisfying

$$\left(\frac{u^2-4}{q}\right) = -1,\ U_{N+r}(u) \equiv 0 \bmod q, \text{ and } V_{N+r}(u) \equiv 2 \bmod q. \tag{4.2}$$

Lemma 4.4: Let N, p, q, k, and r be as given in Theorem 2, with $k \ge 7$,

$$S_1 = \{u : 0 \le u < N, u \text{ satisfies (4.1)}\}, \quad \text{and} \quad S_2 = \{u : 0 \le u < N, u \text{ satisfies (4.2)}\}.$$

Then we have $|S_1 \cup S_2| < N/4$.

Proof: It is easy to see that condition (4.1) is equivalent to

$$\left(\frac{u^2-4}{q}\right)=1, \text{ there exists a } w \in GF^*(q) \text{ with } w^2-uw+1=0 \text{ and } w^{N+r}=1, \tag{4.1'}$$

and condition (4.2) is equivalent to

$$\left(\frac{u^2-4}{q}\right)=-1, \text{ there exists a } \xi \in GF^*(q^2) \text{ with } \xi^2-u\xi+1=0 \text{ and } \xi^{N+r}=1. \tag{4.2'}$$

Since $q=k(p+1)+r>(k-1/2)(p+1)$, we have $p+1<\frac{q}{k-1/2}$.

In the group $GF^*(q)$, the number of solutions of the equation $x^{N+r}=1$ is

$$\gcd(N+r, q-1)=\gcd(p+r, q-1)\le p+r<3(p+1)/2<3q/(2k-1)<q/4.$$

Since every u (mod q) of the set S_1 corresponds to two different w's, and different u (mod q)'s correspond to different pairs of w's, we have

$$|S_1|<(1/2)\cdot(q/4)\cdot(N/q)=N/8.$$

In the group $GF^*(q^2)$, if ξ is such that

$$\xi^2-u\xi+1=0 \text{ with } \left(\frac{u^2-4}{q}\right)=-1,$$

then $\xi^{q+1}=1$. The number of solutions of the system of equations

$$\begin{cases} x^{q+1}=1, \\ x^{N+r}=1, \end{cases}$$

is

$$\gcd(N+r, q+1)=\gcd(p-r, q+1)\le p-r<3(p+1)/2<q/4.$$

Since every u (mod q) of the set S_2 corresponds to two different ξ's, and different u (mod q)'s correspond to different pairs of ξ's, we have

$$|S_2|<(1/2)\cdot(q/4)\cdot(N/q)=N/8.$$

Therefore, we have $|S_1\cup S_2|<(N/8)+(N/8)=N/4$. □

Now we are ready to prove Theorem 2.

Proof of Theorem 2: Suppose condition (1.7) holds. We present *Algorithm* 2 as follows: Select a random integer u with $0\le u<N$, $u\ne 2$, $u\ne N-2$ and

$$\gcd(u, N)=1 \text{ and } \gcd(D, N)=1, \text{ where } D=u^2-4. \tag{4.3}$$

If (4.3) does not hold, then a nontrivial factor of N is found. Suppose (4.3) holds.

By Lemma 4.1, for a random integer u, the probability that $(D/p)=-1$ is about $1/2$. Suppose $(D/p)=-1$ with the chosen u.

We first calculate the pair U_N and V_N via the formulas (cf. Lemma 12.5 of [1]):

$$U_{2i}=U_iV_i, \qquad V_{2i}=V_i^2-2,$$
$$U_{2i+1}=U_{i+1}V_i-1, \quad V_{2i+1}=V_{i+1}V_i-u.$$

(This is something like doing modular exponentiation in Algorithm 1.) Then calculate

$$U_{N+1} = (uU_N + V_N)/2, \quad V_{N+1} = (uV_N + DU_N)/2,$$
$$U_{N-1} = uU_N - U_{N+1}, \quad V_{N-1} = uV_N - V_{N+1}.$$

For $i = 2, 3, \ldots,$ calculate by recurrence,

$$U_{N+i} = uU_{N+i-1} - U_{N+i-2}, \quad V_{N+i} = uV_{N+i-1} - V_{N+i-2},$$
$$U_{N-i} = uU_{N-i+1} - U_{N-i+2}, \quad V_{N-i} = uV_{N-i+1} - V_{N-i+2}.$$

By Lemma 4.3, we have $p \mid U_{N+r}$ and $p \mid (V_{N+r} - 2)$.

Suppose $k \geq 7$. (If $k < 7$, then $N = pq$ with $q = k(p+1) + r = k(p-1) + 2k + r$ can be easily factored by Algorithm 1.) By Lemma 4.4, for a random u, the probability that

$$q \mid U_{N+r}(u) \quad \text{and} \quad q \mid (V_{N+r}(u) - 2) \tag{4.4}$$

is less than $1/4$. Suppose (4.4) does not hold for the chosen u. Then we have $\gcd(U_{N+r}, N) = p$ and/or $\gcd(V_{N+r} - 2, N) = p$, and $N/p = q$.

The time taken by computer for the calculation of $U_N \pmod N$ and $V_N \pmod N$ as explained above and for the calculation of $a^N \pmod N$ are the same order of magnitude for large values of N. So, as analyzed in Theorem 1, bit operations used here is also $O(\log^3 N + |r| \log^2 N)$, but with a larger constant related to the big O-notation than that in Theorem 1. □

Example 4.1: Let $N = 525837811$, $u = 6$, and $D = u^2 - 4 = 32$. Then

$$U_N = 128529829, \; V_N = 365916885, \; U_{N-9} = 154978947, \text{ and } V_{N-9} = 215276907.$$

We have $N = pq$, where

$$p = \gcd(U_{N-9}, N) = \gcd(V_{N-9} - 2, N) = 1621 \text{ and } q = N/p = 324391.$$

We find that $q = 200(p+1) - 9$, $(D/p) = -1$, and $(D/q) = 1$.

Example 4.2: Let $N = 262940789$, $u = 6$, and $D = u^2 - 4 = 32$. Then

$$U_N = 90848206, \; V_N = 211151910, \; U_{N+9} = 256455168, \text{ and } V_{N+9} = 78409393.$$

We have $N = pq$, where

$$p = \gcd(U_{N+9}, N) = \gcd(V_{N+9} - 2, N) = 1621, \text{ and } q = N/p = 162209.$$

We find that $q = 100(p+1) + 9$, $(D/p) = -1$, and $(D/q) = 1$.

Remark 4.1: In Algorithm 2, if the integer u happens to be selected with $(D/p) = 1$ (with probability about $1/2$), then $p \mid U_{p-1}$ and $p \mid (V_{p-1} - 2)$, instead of $p \mid U_{p+1}$ and $p \mid (V_{p+1} - 2)$. If k in (1.7) is small or condition (1.6) holds, we would have $\gcd(U_{N-r}, N) = \gcd(V_{N-r} - 2, N) = p$, where r satisfies (1.6). In this case, Algorithm 2 acts essentially as Algorithm 1 does.

Example 4.3: Let $N = 13157657$, $u = 6$, and $D = u^2 - 4 = 32$. Then

$$U_N = 2945491, \quad V_N = 1183255,$$
$$U_{N+7} = 3350607, \quad V_{N+7} = 6668796.$$

We have $N = pq$, where

$$p = \gcd(U_{N+7}, N) = \gcd(V_{N+7} - 2, N) = 1621, \text{ and } q = N/p = 8117.$$

We find that $q = 5(p+1)+7$, $(D/p) = (D/q) = -1$.

If $u = 3$ is selected, then $D = u^2 - 4 = 5$ and

$$\begin{aligned} U_N &= 6604163, & V_N &= 281690, \\ U_{N-17} &= 12418481, & V_{N-17} &= 3076660. \end{aligned} \quad D = u^2 - 4 = 5$$

We have $N = pq$, where

$$p = \gcd(U_{N-17}, N) = \gcd(V_{N-17} - 2, N) = 1621, \text{ and } q = N/p = 8117.$$

We find that $q = 5(p-1)+17$, $(D/p) = 1$, and $(D/q) = -1$. This example explains Remark 4.1.

Example 4.4: Let

$$N = 10^{224} + 67 \cdot 10^{198} + 579 \cdot 10^{125} + 39052 \cdot 10^{99} + 8381 \cdot 10^{27} + 5690121 \text{ (225 digits)},$$

$u = 4$, and $D = u^2 - 4 = 12$. Then we have $N = pq$, where

$$p = \gcd(U_{N+259}, N) = \gcd(V_{N+259} - 2, N) = 10^{99} + 289$$

and

$$q = N/p = 10^{125} + 67 \cdot 10^{99} + 29 \cdot 10^{27} + 19689.$$

The entire calculation took about forty seconds on my PC 486. We find that

$$q = (10^{26} + 67)(p+1) + 259, \ (D/p) = -1, \text{ and } (D/q) = 1.$$

Remark 4.2: One may calculate only the V's using Algorithm 8.3 of [1]. It takes a little less time than calculating both U's and V's. However, it might happen that $\gcd(N, V_{N+r} - 2) = N$, but $\gcd(N, U_{N+r}) = p$ (cf. Lemma 4.4). So we prefer to calculate both U's and V's.

5. COMBINED WITH WILLIAMS' $p + 1$ METHOD

The following *Extended Algorithm* 2 combines *Algorithm* 2 presented in the proof of Theorem 2 with Williams' $p+1$ method, thus it unifies trial division, Fermat's method, and the $p+1$ method.

Extended Algorithm 2: Let u, D be as given in the proof of Theorem 2. Calculate $a = U_M(u)$ and $b = V_M(u)$, where M is the product of all small primes and some powers of very small primes. If $1 < \gcd(a, N) < N$ or $1 < \gcd(b-2, N) < N$, then a nontrivial factor of N is found (the $p+1$ algorithm ends up here). Otherwise, calculate (cf. Lemma 12.14 of [1]) $U_{MN}(u) = a \cdot U_N(b)$ and $V_{MN}(u) = V_N(b)$. Then, for $i = 1, 2, \ldots$, calculate

$$\begin{aligned} U_{M(N+i)}(u) &= \tfrac{1}{2}(b \cdot U_{M(N+i-1)}(u) + a \cdot V_{M(N+i-1)}(u)), \\ V_{M(N+i)}(u) &= \tfrac{1}{2}(b \cdot V_{M(N+i-1)}(u) + D \cdot a \cdot U_{M(N+i-1)}(u)), \\ U_{M(N-i)}(u) &= \tfrac{1}{2}(b \cdot U_{M(N-i+1)}(u) - a \cdot V_{M(N-i+1)}(u)), \\ V_{M(N-i)}(u) &= \tfrac{1}{2}(b \cdot V_{M(N-i+1)}(u) - D \cdot a \cdot U_{M(N-i+1)}(u)). \end{aligned}$$

If condition (1.11) holds, even though $|r|$ in (1.9) is large, the prime divisor p could be found quickly, since in this case we would most likely have

$$\gcd(U_{M(N+r)}(u), N) = p \text{ and/or } \gcd(V_{M(N+r)}(u) - 2, N) = p.$$

Example 5.1: Let

$$N = 3041465128 \cdot 10^{219} + 355851419976 \cdot 10^{198} + 1757966843983 \cdot 10^{120}$$
$$+ 206120091724443 \cdot 10^{99} + 25402620895539900002984764006054838 7 \text{ (229 digits)},$$

$u = 9$, and $D = u^2 - 4 = 77$. Let

$$M = \prod_{p \text{ prime},\ p^{m_p} < 32768} p^{m_p}.$$

Then we have $N = pq$, where

$$p = \gcd(U_{M(N+144)}(u), N) = \gcd(V_{M(N+144)}(u) - 2, N)$$
$$= 3041465128 \cdot 10^{99} + 878983421991 \text{ (109 digits)}$$

and

$$q = N / p = 10^{120} + 117 \cdot 10^{99} + 289 \cdot 10^{21} + 33957 \text{ (121 digits)}.$$

The entire calculation took about twenty minutes on my PC 486. We found that

$$q = k(p+1) + r = (10^{21} + 117)d + 144 \text{ and } (D/p) = (D/q) = -1,$$

where $d = 10^{99} + 289$, $(p+1)/d = 2^3 \cdot 13 \cdot 19 \cdot 47 \cdot 32749$, which is smooth and divides M, and $r' = 144$ is small, whereas $|r| = -r = 1369\ldots51187$ (109 digits) is large.

Remark 5.1: As mentioned in Remark 4.1, if the integer u happens to be selected with $(D/p) = 1$, then Extended Algorithm 2 acts essentially as Extended Algorithm 1 does. Thus, Extended Algorithm 2 not only unifies trial division, Fermat's method, Pollard's $p-1$ method, and Williams' $p+1$ method, but also enhances these four methods.

6. CONCLUSIONS

The algorithms we have presented each operate in an Abelian group. Algorithm 1 uses the multiplicative group $GF^*(p)$ of nonzero elements of $GF(p)$. The work on Lucas sequences in Algorithm 2 is really arithmetic done in a subgroup, with order $p+1$, of the multiplicative group $GF^*(p^2)$ of nonzero elements of $GF(p^2)$. The prime factor p of N can be found quickly when $N = pq$ satisfies one of the four conditions (1.8), (1.9), (1.10), and (1.11) or, in other words, when $N = pq$ is near the related group orders $p \pm 1$. Moreover, it is easy to see that the "factoring large integers near group orders" idea can be used to Lenstra's Elliptic Curve Method [5] to enhance the ability of ECM for factoring more large integers near the order d_p of the group E_p, elliptic curve E modulo p.

Our algorithms not only unify trial division, Fermat's method, Pollard's $p-1$ method, and Williams' $p+1$ method, but also can quickly factor a class of large integers, which could not be factored by other available methods (such as QS or NFS) within a reasonable amount of time. Thus, such integers should be excluded from RSA moduli candidates.

ACKNOWLEDGMENTS

I thank Professors D. M. Bressoud, R. K. Guy, A. K. Lenstra, H. W. Lenstra, Jr., C. Pomerance, G. Robin, S. S. Wagstaff, Jr., and H. C. Williams for their sending me reprints concerning

this subject or other topics in computational number theory. Special thanks go to the editors and the referees for kind and helpful comments that improved the presentation of this paper.

REFERENCES

1. D. M. Bressoud. *Factorization and Primality Testing*. New York: Springer-Verlag, 1989.
2. John D. Dixon. "Factorization and Primality Tests." *Amer. Math. Monthly* **91** (1984):333-352.
3. D. E. Knuth. *The Art of Computer Programming: Semi-Numerical Algorithms*. Vol. 2. 2nd ed. Reading, MA: Addison-Wesley, 1981.
4. A. K. Lenstra & H. W. Lenstra, Jr. *The Development of the Number Field Sieve*. Lecture Notes in Math., 1554. Berlin: Springer-Verlag, 1993.
5. H. W. Lenstra, Jr. "Factoring Integers with Elliptic Curves." *Ann. of Math.* **126** (1987):649-673.
6. J. M. Pollard. "Theorems on Factorization and Primality Testing." *Proc. Cambridge Philos. Soc.* **76** (1974):521-28.
7. C. Pomerance. "Factoring." *Proc. SIAM* **42** (1990):27-47.
8. H. Riesel. *Prime Numbers and Computer Methods for Factorization*. Boston: Birkhaüser, 1985.
9. K. H. Rosen. *Elementary Number Theory and Its Applications*. Reading, MA: Addison-Wesley, 1984.
10. R. D. Silverman. "The Multiple Pollynomial Quadratic Sieve." *Math. Comp.* **48** (1987):329-39.
11. H. C. Williams. "A $p+1$ Method of Factoring." *Math. Comp.* **39** (1982):225-34.
12. H. C. Williams & J. O. Shallit. "Factoring Integers before Computers." *Proc. of Symposia in Applied Mathematics* **48** (1994):481-531.
13. Zhenxiang Zhang. "Finding Strong Pseudoprimes to Several Bases." *Math. Comp.* **70** (2001): 863-72.

AMS Classification Numbers: 11Y05, 11A51, 11B39

❖❖❖

RATIONAL POINTS IN CANTOR SETS

Judit Nagy
Dept. of Analysis of Eötvös Lorand University, Kecskemeti u. 10-12, 1053 Budapest, Hungary
e-mail: nmm@cs.elte.hu
(*Submitted April 1999-Final Revision December 1999*)

1. INTRODUCTION

The idea for this article was given by a problem in real analysis. We wanted to determine the one-dimensional Lebesgue-measure of the set $f^{-1}(C)$, where C stands for the classical triadic Cantor set and f is the Cantor-function, which is also known as "devil's staircase." We could see immediately that to determine the above measure we needed to know which dyadic rationals were contained in C. We soon found that the solution is well known; namely, there are only two such fractions: $\frac{1}{4}$ and $\frac{3}{4}$. This inspired a question: Are there any other primes such that only finitely many fractions are contained in the classical triadic Cantor set, where the denominator is a power of p? The aim of this paper is to verify the surprising result: every $p \neq 3$ prime fulfills the condition. Charles R. Wall showed in [2] that the Cantor set contains only 14 terminating decimals. His article gave very important information regarding the proof. We may ask if the quality of containing "very few" rational numbers and that of having zero Lebesgue measure are in close connection for a Cantor set. The answer seems to be "yes" at first sight, but in [1] Duane Boes, Richard Darst, and Paul Erdös showed a symmetric Cantor set family which, for each $\lambda \in [0, 1]$, has a member of Lebesgue measure $1-\lambda$, but the sets of the family typically do not contain "any" rational numbers.

2. DEFINITIONS, NOTATIONS, AND LEMMAS

Definition 1: Let n be a positive integer and m a positive integer relatively prime to n. The order of n modulo m is the smallest positive exponent g such that $n^g \equiv 1 \pmod{m}$.

Notation 1: Since our proofs require only the case $n = 3$, for the reason of simplicity we omit n and denote the order of 3 modulo m by $\text{ord}(m)$.

Lemma 1: If l and m are relatively prime to 3 and l divides m, then $\text{ord}(l)$ divides $\text{ord}(m)$.

Proof: This follows immediately from the definition of the order. □

Lemma 2: Let $p > 3$ be prime and $\text{ord}(p) = d$. If $\text{ord}(p^b) = d$ for an integer b, then $\text{ord}(p^{b+1})$ either equals d, or p divides $\text{ord}(p^{b+1})$.

Proof: (We denote a divides b in the usual way by $a|b$ and denote a does not divide b by $a \nmid b$.) We observe that $d|p-1$. It is enough to verify that if $p \nmid \text{ord}(p^{b+1})$ then $\text{ord}(p^{b+1}) = d$.

It is well known that if m is relatively prime to 3 then $\text{ord}(m)$ divides $\phi(m)$, where ϕ is Euler's function; hence, $\text{ord}(p^{b+1}) | \phi(p^{b+1}) = (p-1) \cdot p^b$ and, furthermore, $\text{ord}(p^{b+1}) | p-1$, since $p \nmid \text{ord}(p^{b+1})$.

From Lemma 1, it follows that $d | \text{ord}(p^{b+1})$; hence, there exists a positive integer t such that $\text{ord}(p^{b+1}) = d \cdot t$.

Now, $3^d \equiv 1 \pmod{p^b}$ gives $3^{d\cdot p} \equiv 1 \pmod{p^{b+1}}$, which implies that $d\cdot t \mid d\cdot p$. But, since $d\cdot t$ divides both $p-1$ and $d\cdot p$, it also divides their greatest common divisor d. Therefore $t=1$, which completes the proof. □

Lemma 3: Let $p>3$ be a prime. If $\operatorname{ord}(p)=d$, then there exists a unique positive integer n, for which $\operatorname{ord}(p^k)=d$ whenever $1\le k\le n$ and $\operatorname{ord}(p^{n+t})=d\cdot p^t$ whenever t is a positive integer.

Proof: By Lemma 1 and Lemma 2, there exists a maximal exponent n such that $\operatorname{ord}(p^n)=d$. We use mathematical induction on t.

Let $t=1$. We show that $\operatorname{ord}(p^{n+1})=d\cdot p$.

From $3^d\equiv 1 \pmod{p^n}$, it follows that $3^{d\cdot p}\equiv 1 \pmod{p^{n+1}}$; hence, $\operatorname{ord}(p^{n+1})\mid d\cdot p$. On the other hand, using the first two lemmas, $d\mid \operatorname{ord}(p^{n+1})$ and $p\mid \operatorname{ord}(p^{n+1})$; therefore, $d\cdot p\mid \operatorname{ord}(p^{n+1})$. Next, supposing $\operatorname{ord}(p^{n+t})=d\cdot p^t$, we prove that $\operatorname{ord}(p^{n+t+1})\mid d\cdot p^{t+1}$ for any positive integer t.

1. Let y denote $3^{d\cdot p^t}$. Then

$$3^{d\cdot p^{t+1}}-1=(3^{d\cdot p^t})^p-1=y^p-1=A\cdot B, \tag{1}$$

where $A=y-1$ and $B=y^{p-1}+y^{p-2}+\cdots+y+1$. From $y\equiv 1 \pmod{p^{n+t}}$, it follows that $p^{n+t}\mid A$ and $p\mid B$, since $y\equiv 1 \pmod{p}$. Thus, $3^{d\cdot p^{t+1}}\equiv 1 \pmod{p^{n+t+1}}$, which implies $\operatorname{ord}(p^{n+t+1})\mid d\cdot p^{t+1}$

2. Next, we prove $d\cdot p^{t+1}\mid \operatorname{ord}(p^{n+t+1})$. First, $d\cdot p^t\mid \operatorname{ord}(p^{n+t+1})$ and $\operatorname{ord}(p^{n+t+1})\mid d\cdot p^{t+1}$ by Lemma 1 and the previous result. So $\operatorname{ord}(p^{n+t+1})$ can only be $d\cdot p^t$ or $d\cdot p^{t+1}$.

We now show that $d\cdot p^t$ is impossible, that is, $p^{n+t+1}\nmid 3^{d\cdot p^t}-1$. Let z denote $3^{d\cdot p^{t-1}}$. Then

$$3^{d\cdot p^t}-1=(3^{d\cdot p^{t-1}})^p-1=z^p-1=A_*\cdot B_*, \tag{2}$$

where $A_*=z-1$ and $B_*=z^{p-1}+z^{p-2}+\cdots+z+1$. From the condition $\operatorname{ord}(p^{n+t})=d\cdot p^t$ follows $p^{n+t}\nmid A_*$, so it is enough to show that $p^2\nmid B_*$. To obtain this, we write B_*-p as a product:

$$\begin{aligned} B_*-p &= (z^{p-1}-1)+(z^{p-2}-1)+(z^{p-3}-1)+\cdots+(z-1)\\ &= (z-1)\cdot(z^{p-2}+2\cdot z^{p-3}+\cdots+(p-2)\cdot z+(p-1)). \end{aligned}$$

We have $z\equiv 1 \pmod{p}$ and thus $z^{p-2}+2\cdot z^{p-2}+\cdots+(p-2)\cdot z+(p-1)\equiv(1+2+\cdots+p-1) \pmod{p}$. Since $1+2+\cdots+p-1=p\cdot\frac{p-1}{2}$ and $\frac{p-1}{2}$ is an integer, we obtain

$$p\mid z^{p-2}+2\cdot z^{p-2}+\cdots+(p-2)\cdot z+(p-1). \tag{3}$$

On the other hand, we have $p\mid z-1$; hence, $p^2\mid B_*-p$. Then p^2 cannot divide B_*. □

Notation 2: Given a positive integer L relatively prime to 3, let

$$N(L)=\{K: 1\le K\le L-1 \text{ and } (K,L)=1\}. \tag{4}$$

Remark 1: Observe that $N(L)$ consists of all the possible numerators of simplified fractions in $[0,1]$ with denominator L. It is also clear that $N(L)$ has exactly $\phi(L)$ many elements. Recall from Charles Wall's article [2] that $N(L)$ decomposes into $\frac{\phi(L)}{\operatorname{ord}(L)}$ equivalence classes, each of which has $\operatorname{ord}(L)$ many elements. These can be written in the form

$$[k(L)]=\{k, k\cdot 3,\ldots,k\cdot 3^{\operatorname{ord}(L)-1} : \bmod L\}, \tag{5}$$

where k is an element of $N(L)$.

Definition 2: We call the $[k(L)]$ equivalence classes briefly the classes of $N(L)$.

Remark 2: In addition, we recall that, for each $k \in N(L)$, either all the elements of a $[k(L)]$ class, or none of them, are numerators of fractions in the Cantor set, so it is enough to find a $k' \in [k(L)]$ such that $\frac{k'}{L} \notin C$, that is, $\frac{k'}{L}$ was eliminated during the construction of the Cantor set. This guarantees that all the elements of $[k(L)]$ are numerators of eliminated fractions.

Definition 3: We call the class $[k(L)]$ "eliminated" if there exists a $k' \in [k(L)]$ such that $\frac{k'}{L} \notin C$.

Remark 3: Now, let n be the positive integer determined in Lemma 3. Then $N(p^n)$ has

$$\frac{\phi(p^n)}{\operatorname{ord}(p^n)} = \frac{(p-1)\cdot p^{n-1}}{d}$$

classes and, for each positive integer t, the set $N(p^{n+t})$ has

$$\frac{\phi(p^{n+t})}{\operatorname{ord}(p^{n+t})} = \frac{(p-1)\cdot p^{n+t-1}}{d\cdot p^t} = \frac{(p-1)\cdot p^{n-1}}{d}$$

classes.

3. THE MAIN RESULTS

Theorem 1: Let $p > 3$ be a prime such that 3 is a primitive root modulo p^2. Then there are no fractions $\frac{a}{b} \in C$ (where a and b are relatively prime numbers) such that b is a power of p.

Proof: First, $\operatorname{ord}(p^2) = p\cdot(p-1)$ immediately implies $\operatorname{ord}(p) = p-1$. Thus, Lemma 3 with $d = p-1$ gives $n = 1$, so $\operatorname{ord}(p^{t+1}) = (p-1)\cdot p^t$ for each positive integer t. Then $\phi(p^t) = \operatorname{ord}(p^t)$, so $N(p^t)$ consists of one class, for example, $N(p^t) = [1(p^t)]$. Therefore, $N(p^t)$ has $(p-1)\cdot p^{t-1}$ elements and, for each prime $p > 3$ and positive integer t,

$$(p-1)\cdot p^{t-1} > 2\cdot\left[\frac{p^t}{3}\right], \tag{6}$$

$\left(\text{where } \left[\frac{p^t}{3}\right] \text{ denotes the integer part of the real number } \frac{p^t}{3}\right)$. Thus, there exists an $i \in [1(p^t)]$ such that $\frac{1}{3} < \frac{i}{p^t} < \frac{2}{3}$, hence, $N(p^t)$ is eliminated. □

Next, we show that if n is the largest integer for which $\operatorname{ord}(p) = \operatorname{ord}(p^n)$ then n is also the largest exponent such that the nth power of p can be the denominator of a fraction in C.

Theorem 2: For each prime $p > 3$, there are finitely many fractions $\frac{a}{b} \in C$ such that b is a power of p.

Proof: Let $k \in N(p^{n+t})$ for any positive integer t. We show that $[k(p^{n+t})]$ is eliminated. Suppose

$$[k(p^{n+t-1})] = \{x_1, \ldots, x_{\operatorname{ord}(p^{n+t-1})}\}. \tag{7}$$

Then

$$[k(p^{n+t})] = \{x_i + j\cdot p^{n+t-1} : i = 1, \ldots, \operatorname{ord}(p^{n+t-1}),\ j = 0, 1, \ldots, p-1\}. \tag{8}$$

This can be seen easily concerning the following. For each number of the form $k \cdot 3^y$, there exists a $1 \le i \le \operatorname{ord}(p^{n+t-1})$ such that $k \cdot 3^y \equiv x_i \pmod{p^{n+t-1}}$. Hence, there is a $j \in \{0, 1, \ldots, p-1\}$ such that $k \cdot 3^y \equiv x_i + j \cdot p^{n+t-1} \pmod{p^{n+t}}$. This implies

$$[k(p^{n+t})] \subseteq \{x_i + j \cdot p^{n+t-1} : i = 1, \ldots, \operatorname{ord}(p^{n+t-1}),\ j = 0, 1, \ldots, p-1\}. \tag{9}$$

On the other hand, the two sets have the same number of elements, so they are equal.

What does this mean?

Take any element x_i of $[k(p^{n+t-1})]$ and observe the situation of the fractions

$$\frac{x_i}{p^{n+t}} < \frac{x_i + p^{n+t-1}}{p^{n+t}} < \frac{x_i + 2 \cdot p^{n+t-1}}{p^{n+t}} < \cdots < \frac{x_i + (p-1) \cdot p^{n+t-1}}{p^{n+t}} \tag{10}$$

in the interval $[0, 1]$. Writing them, respectively, in the form

$$\frac{x_i}{p^{n+t}} < \frac{x_i}{p^{n+t}} + \frac{1}{p} < \frac{x_i}{p^{n+t}} + \frac{2}{p} < \cdots < \frac{x_i}{p^{n+t}} + \frac{p-1}{p}, \tag{11}$$

we can see that the difference of each neighboring fraction is $\frac{1}{p}$ and, as $p > 3$, there must be at least one of them in the middle open third of $[0, 1]$. Therefore, $[k(p^{n+t})]$ is eliminated. □

REFERENCES

1. D. Boes, R. Darst, & P. Erdös. "Fat, Symmetric, Irrational Cantor Sets." *Amer. Math. Monthly* **88.5** (1981):340-41.
2. C. R. Wall. "Terminating Decimals in the Cantor Ternary Set." *The Fibonacci Quarterly* **28.2** (1990):98-101.
3. Solution to Problem H-339. *The Fibonacci Quarterly* **21.3** (1983):239.

AMS Classification Numbers: 11A41, 28A80

❖❖❖

DIOPHANTINE TRIPLETS AND THE PELL SEQUENCE

M. N. Deshpande
Institute of Science, Nagpur 440 001, India

Ezra Brown
Department of Mathematics, Virginia Tech, Blacksburg, VA 24061-0123
(Submitted April 1999-Final Revision August 2000)

1. INTRODUCTION

A Diophantine triplet is a set of three positive integers (a, b, c) such that $a < b < c$ and $ab = 1$, $bc + 1$, and $ac + 1$ are integer squares. Examples of such triplets are $(1, 3, 8)$, $(2, 4, 12)$, and $(2990, 22428, 41796)$.

The following four families of Diophantine triplets are well known:

$$\mathbf{F}_1 = \{(F_{2n}, F_{2n+2}, F_{2n+4}) : n \geq 1\},$$
$$\mathbf{F}_2 = \{(F_{2n}, F_{2n+4}, 5F_{2n+2}) : n \geq 1\},$$
$$\mathbf{P}_1 = \{(P_{2n}, 2P_{2n}, P_{2n+2}) : n \geq 1\},$$
$$\mathbf{P}_2 = \{(P_{2n}, P_{2n+2}, 2P_{2n+2}) : n \geq 1\}.$$

We refer readers to [2], [3], and [4] for these families. Here, F_k and P_k denote the kth element of the Fibonacci sequence and the Pell sequence, respectively. In [1], the first author posed the problem of finding infinitely many such Diophantine triplets.

The aim of this paper is to construct several different infinite families of Diophantine triplets using elements of the Pell sequence. We then formulate and prove a general result which gives formulas for a doubly infinite family of Diophantine triples. We conclude with a result on Diophantine quadruplets.

2. THE PELL SEQUENCE

Although the Pell sequence is quite well known, we describe it here for the sake of completeness. The Pell sequence is the sequence $\{P_n\}$, where $P_1 = 1$, $P_2 = 2$, and $P_{n+2} = 2P_{n+1} + P_n$ for $n \geq 1$. That is, the Pell sequence is the sequence $\{1, 2, 5, 12, 29, 70, 169, 408, \ldots\}$. (We note that this is the sequence of denominators for the successive convergents to the continued fraction expansion of $\sqrt{2}$.) The following two properties of the Pell sequence are used in this paper:

Property 1: P_n is even if n is even.

Property 2: For all $n \geq 1$, $2P_{2n}^2 + 1 = \left(\frac{3P_{2n} - P_{2n-2}}{2}\right)^2$.

3. SOME FAMILIES OF DIOPHANTINE TRIPLETS

For convenience, we shall use the following notation. $FP(k)$ denotes the kth family obtained by using the Pell sequence. The nth element of $FP(k)$ is a triple denoted by $T_n(k)$, whose elements in turn are denoted by $A_{n,k}$, $B_{n,k}$, and $C_{n,k}$. That is,

$$FP(k) = \{T_n(k) : n = 1, 2, \ldots\}, \text{ and } T_n(k) = (A_{n,k}, B_{n,k}, C_{n,k}).$$

Theorem 1: Let $A_{n,1} = \frac{P_{2n}}{2}$, $B_{n,1} = 4P_{2n}$, and $C_{n,1} = \frac{15}{2}P_{2n} - P_{2n-2}$. Then

$$FP(1) = \{T_n(1) : n = 1, 2, \ldots\} = \{(A_{n,1}, B_{n,1}, C_{n,1}) : n = 1, 2, \ldots\}$$

is a family of Diophantine triplets.

Proof: For each $n \geq 1$, using the definition of the Pell sequence and Property 2 leads to the equations

$$A_{n,1}B_{n,1} + 1 = 2P_{2n}^2 + 1 = \left(\frac{3P_{2n} - P_{2n-2}}{2}\right)^2,$$

$$\begin{aligned} A_{n,1}C_{n,1} + 1 &= \frac{P_{2n}}{2}\left(\frac{15}{2}P_{2n} - P_{2n-2}\right) + 1 \\ &= \frac{P_{2n}}{2}\left(\frac{15}{2}P_{2n} - P_{2n-2}\right) + \left(\frac{3P_{2n} - P_{2n-2}}{2}\right)^2 - 2P_{2n}^2 \\ &= 4P_{2n}^2 - 2P_{2n}P_{2n-2} + \frac{P_{2n-2}^2}{4} = \left(2P_{2n} - \frac{P_{2n-2}}{2}\right)^2, \end{aligned}$$

and

$$\begin{aligned} B_{n,1}C_{n,1} + 1 &= 4P_{2n}\left(\frac{15}{2}P_{2n} - P_{2n-2}\right) + 1 \\ &= 4P_{2n}\left(\frac{15}{2}P_{2n} - P_{2n-2}\right) + \left(\frac{3P_{2n} - P_{2n-2}}{2}\right)^2 - 2P_{2n}^2 \\ &= \frac{121}{4}P_{2n}^2 - \frac{11}{2}P_{2n}P_{2n-2} + P_{2n-2}^2 \\ &= \left(\frac{11}{2}P_{2n} - \frac{P_{2n-2}}{2}\right)^2. \end{aligned}$$

By Property 1, since P_{2n} and P_{2n-2} are even, each of the above squared expressions is an integer square, and the result follows.

We list a few elements of $FP(1)$:

n	Triple
1	$T_1(1) = (1, 8, 15)$
2	$T_2(1) = (6, 48, 88)$
3	$T_3(1) = (35, 280, 513)$
4	$T_4(1) = (204, 1632, 2990)$

Theorem 2: Let $A_{n,2} = 2P_{2n}$, $B_{n,2} = 15P_{2n} - 2P_{2n-2}$, and $C_{n,2} = 28P_{2n} - 3P_{2n-2}$. Then $FP(2) = \{T_n(2) : n = 1, 2, \ldots\} = \{(A_{n,2}, B_{n,2}, C_{n,2}) : n = 1, 2, \ldots\}$ is a family of Diophantine triplets.

Proof: Noting that $A_{n,2}B_{n,2} = B_{n,1}C_{n,1}$, we see from Theorem 1 that

$$A_{n,2}B_{n,2} + 1 = \left(\frac{11}{2}P_{2n} - \frac{P_{2n-2}}{2}\right)^2.$$

Using algebraic techniques similar to those used in the proof of Theorem 1, we also obtain

$$A_{n,2}C_{n,2}+1=\left(\frac{15}{2}P_{2n}-P_{2n-2}\right)^2 \quad \text{and} \quad B_{n,2}C_{n,2}+1=\left(\frac{41}{2}P_{2n}-\frac{5}{2}P_{2n-2}\right)^2.$$

Again, since the subscripts are even, these squares are integer squares, and the result follows.

A few triples in the family $FP(2)$ are listed here:

n	Triple
1	$T_1(2) = (4, 30, 56)$
2	$T_2(2) = (24, 176, 330)$
3	$T_3(2) = (140, 1026, 1924)$
4	$T_4(2) = (816, 5980, 11214)$

Theorem 3: Let $A_{n,3}=\frac{15}{2}P_{2n}-P_{2n-2}$, $B_{n,3}=56P_{2n}-6P_{2n-2}$, and $C_{n,3}=\frac{209}{2}P_{2n}-12P_{2n-2}$. Then $FP(3)=\{T_n(3):n=1,2,\ldots\}=\{(A_{n,3},B_{n,3},C_{n,3}):n=1,2,\ldots\}$ is a family of Diophantine triplets.

Proof: Noting that $A_{n,3}B_{n,3}=B_{n,2}C_{n,2}$, we see from Theorem 2 that

$$A_{n,3}B_{n,3}+1=\left(\frac{41}{2}P_{2n}-\frac{5}{2}P_{2n-2}\right)^2.$$

Using algebraic techniques similar to those used in the proof of Theorem 1, we also obtain

$$A_{n,3}C_{n,3}+1=\left(28P_{2n}-\frac{7}{2}P_{2n-2}\right)^2 \quad \text{and} \quad B_{n,3}C_{n,3}+1=\left(\frac{153}{2}P_{2n}-\frac{17}{2}P_{2n-2}\right)^2.$$

As before, since the subscripts are even, these squares are integer squares, and the result follows.

Here are a few triples in the family $FP(3)$:

n	Triple
1	$T_1(3) = (15, 112, 209)$
2	$T_2(3) = (88, 660, 1230)$
3	$T_3(3) = (513, 3848, 7171)$
4	$T_4(3) = (2990, 22428, 41796)$

4. A DOUBLY INFINITE FAMILY OF DIOPHANTINE TRIPLETS

It is apparent from the previous section that the families $FP(1)$, $FP(2)$, and $FP(3)$ fit into an infinite family of such families. In this section we will derive formulas for such a double infinite family.

First, we define the auxiliary sequences $\{G_n : n \geq 1\}$, $\{H_n : n \geq 1\}$, and $\{S_n : n \geq 1\}$ by

$$G_1=1, G_2=4, \text{ and } G_{n+2}=4G_{n+1}-G_n \qquad \text{for } n \geq 1;$$
$$H_1=H_2=0, \text{ and } H_{n+2}=4H_{n+1}-H_n-2(-1)^n \qquad \text{for } n \geq 1;$$
$$S_1=4, S_2=14, \text{ and } S_{n+2}=4S_{n+1}-S_n \qquad \text{for } n \geq 1.$$

Thus, $(G_n) = (1, 4, 15, 56, 209, 780, 2911, \ldots)$, $(H_n) = (0, 0, 2, 6, 24, 88, 330, 1230, \ldots)$, and $(S_n) = (4, 14, 52, 194, 724, \ldots)$.

Our main result is the following.

Theorem 4: Let n and k be positive integers, and let

$$E(n, k) = \frac{G_k P_{2n} - H_k P_{2n-2}}{2}.$$

Then $(E(n, k), 2E(n, k+1), E(n, k+2))$ is a Diophantine triplet.

If we now define $FP(k) = \{(E(n, k), 2E(n, k+1), E(n, k+2)) : n = 1, 2, \ldots\}$, then the cases $k = 1, 2$, and 3 agree with our previous definitions. Hence, this is the doubly infinite family we seek.

Proof of Theorem 4 uses the properties of the G_n, H_n, and S_n contained in Propositions G, H, and S; their proofs use only induction and some tedious but straightforward algebra.

Define the algebraic integers γ and δ by $\gamma = 2 + \sqrt{3}$ and $\delta = 2 - \sqrt{3}$.

Proposition G: For n a positive integer:

(1) $G_n = \dfrac{\gamma^n - \delta^n}{\gamma - \delta}$,

(2) $G_{n+2}G_n + 1 = G_{n+1}^2$,

(3) $2G_nG_{n+1} + 1 = (G_{n+1} - G_n)^2$,

(4) $G_{n+3} + G_n = 3(G_{n+1} + G_{n+2})$.

Proposition H: For n a positive integer:

(1) $H_n = \dfrac{(1+\sqrt{3})\gamma^{n-2} - (\sqrt{3}-1)\delta^{n-2}}{6} - \dfrac{(-1)^{n-2}}{3}$,

(2) $H_{n+2}H_n + 1 = (H_{n+1} + (-1)^{n+1})^2$,

(3) $H_n + H_{n+1} = 2G_{n-1}$,

(4) $H_{n+3} + H_n = 3(H_{n+1} + H_{n+2})$.

Proposition S: For n a positive integer:

(1) $S_n = \gamma^n + \delta^n$,

(2) $S_n + (-1)^n$ is divisible by 3,

(3) $S_{n+3} + S_n = 3(S_{n+1} + S_{n+2})$,

(4) $G_{n+2} - G_n = S_{n+1}$.

Remark: The reader will note that (G_n) and (S_n) are related in the same way as the Fibonacci and Lucas sequences are related.

The following lemmas are quite useful in deriving the main result. We give the proof of Lemma 1 here; proofs of Lemmas 2 and 3 are similar but longer, and we have relegated them to the appendix.

Lemma 1: For every positive integer n, $2H_nH_{n+1} + 1 = \left(\frac{S_{n-1} + (-1)^{n-1}}{3}\right)^2$.

Lemma 2: For every positive integer n, $G_nH_{n+2}+G_{n+2}H_n+6=2G_{n+1}(H_{n+1}+(-1)^{n+1})$.

Lemma 3: For every positive integer n, $G_nH_{n+1}+G_{n+1}H_n+3=\frac{1}{3}(G_{n+1}-G_n)(S_{n-1}+(-1)^{n+1})$.

Proof of Lemma 1: Using Proposition H(1), we see that

$$\begin{aligned}2H_nH_{n+1}+1&=2\left(\frac{(1+\sqrt{3})\gamma^{n-2}-(\sqrt{3}-1)\delta^{n-2}}{6}-\frac{(-1)^{n-2}}{2}\right)\\&\quad\times\left(\frac{(1+\sqrt{3})\gamma^{n-1}-(\sqrt{3}-1)\delta^{n-1}}{6}-\frac{(-1)^{n-2}}{2}\right)+1\\&=\frac{2}{36}((1+\sqrt{3})^2\gamma^{2n-3}+(\sqrt{3}-1)^2\delta^{2n-3}-2(\gamma+\delta))-\frac{2}{9}+1\\&\quad-\frac{2}{18}((\sqrt{3}+1)\gamma^{n-2}(\gamma-1)-(\sqrt{3}-1)\delta^{n-2}(\delta-1))(-1)^{n-2},\end{aligned}$$

since $\gamma\delta=1$. Now we know that $\gamma-1=\sqrt{3}+1$, $\delta-1=1-\sqrt{3}$, $\gamma+\delta=4$, $(1+\sqrt{3})^2=2\gamma$, and $(\sqrt{3}-1)^2=2\delta$. Hence,

$$\begin{aligned}2H_nH_{n+1}+1&=\frac{\gamma^{2n-2}}{9}+\frac{\delta^{2n-2}}{9}-\frac{4}{9}-\frac{2}{9}+1-\frac{(-1)^{n-2}2(\gamma^{n-1}+\delta^{n-1})}{9}\\&=\frac{(\gamma^{n+1}+\delta^{n+1})^2-2}{9}-\frac{6}{9}+1+\frac{2(-1)^{n-1}(\gamma^{n-1}+\delta^{n-1})}{9}\\&=\left(\frac{\gamma^{n-1}+\delta^{n-1}}{3}+\frac{(-1)^{n-1}}{3}\right)^2=\left(\frac{S_{n-1}+(-1)^{n-1}}{3}\right)^2,\end{aligned}$$

as claimed.

We note that defining $P_0=0$ is consistent with the Pell sequence recurrence and allows the proofs to go through in the case $n=1$.

Proof of the Main Result: For n, k positive integers, it suffices to show that

$$E(n,k)E(n,k+2)+1 \quad\text{and}\quad 2E(n,k)E(n,k+1)+1$$

are integer squares. The proof breaks into two parts: First, we expand $E(n,k)E(n,k+2)+1$ and find that

$$\begin{aligned}E(n,k)E(n,k+2)+1&=\frac{1}{4}(G_kP_{2n}-H_kP_{2n-2})(G_{k+2}P_{2n}-H_{k+2}P_{2n-2})+1\\&=\frac{1}{4}(G_kG_{k+2}P_{2n}^2+H_kH_{k+2}P_{2n-2}^2-P_{2n}P_{2n-2}(G_kH_{k+2}+G_{k+2}H_k))+1.\end{aligned}$$

Now, by Property 2,

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

i.e.,

$$1=\frac{P_{2n}^2}{4}+\frac{P_{2n-2}^2}{4}-\frac{6}{4}P_{2n}P_{2n-2}.$$

Using Propositions G(2) and H(2), we find that in the expansion of $E(n,k)E(n,k+2)+1$ the coefficients of P_{2n}^2 and P_{2n-2}^2 are

$$\frac{G_{k+1}^2}{4} \quad \text{and} \quad \frac{(H_{k+1}-(-1)^{k+1})}{4},$$

respectively. By Lemma 2, we find that the coefficient of $P_{2n}P_{2n-2}$ is

$$-2G_{k+1}\frac{H_{k+1}+(-1)^{k+1}}{4}.$$

Hence,

$$E(n,k)E(n,k+2)+1=\frac{1}{4}(G_{k+1}P_{2n}-(H_{k+1}+(-1)^{k+1})P_{2n-2})^2,$$

which—since the Pell sequence subscripts are even—is an integer square, as desired. Next, we expand $E(n,k)E(n,k+1)+1$ and find that

$$\begin{aligned}E(n,k)E(n,k+1)+1&=\frac{1}{4}(2G_kP_{2n}-H_kP_{2n-2})(G_{k+1}P_{2n}-H_{k+1}P_{2n-2})+1\\&=\frac{1}{4}(2G_kG_{k+1}P_{2n}^2+2H_kH_{k+1}P_{2n-2}^2-2P_{2n}P_{2n-2}(G_kH_{k+1}+G_{k+1}H_k))+1.\end{aligned}$$

As before, recall that

$$1=\frac{P_{2n}^2}{4}+\frac{P_{2n-2}^2}{4}-\frac{6}{4}P_{2n}P_{2n-2}.$$

Using Proposition G(3) and Lemma 1, we find that in the expansion of $2E(n,k)E(n,k+1)+1$ the coefficients of P_{2n}^2 and P_{2n-2}^2 are

$$\frac{(G_{k+1}-G_k)^2}{4} \quad \text{and} \quad \frac{1}{4}\left(\frac{(S_{k-1}+(-1)^{k-1}}{3}\right)^2,$$

respectively. By Lemma 3, we find that the coefficient of $P_{2n}P_{2n-2}$ is

$$\frac{2}{4}\frac{(G_{k+1}-G_k)(S_{k-1}+(-1)^{k-1})}{3}.$$

Hence,

$$2E(n,k)E(n,k+1)+1=\frac{1}{4}\left((G_{k+1}-G_k)P_{2n}-\frac{S_{k-1}+(-1)^{k-1}}{3}P_{2n-2}\right)^2$$

which—by Proposition S(2) and the fact that the Pell sequence subscripts are even—is an integer square, as desired.

Diophantine Quadruples: Let us recall that a Diophantine quadruple is an ordered quadruple (a,b,c,d) of positive integers such that $ab+1$, $ac+1$, $ad+1$, $bc+1$, $bd+1$, and $cd+1$ are all integer squares. A recent result on Diophantine quadruples is the following (see [2]).

Theorem 5: If (a,b,c) is a Diophantine triplet for which $ab=1=x^2$, $ac+1=y^2$, $bc+1=z^2$, and $d=a+b+c+2abc+2xyz$, then (a,b,c,d) is a Diophantine quadruple.

This result and our Theorem 4 produce an infinite family of Diophantine quadruples, namely,

$$\begin{aligned}a&=E(n,k), & b&=2E(n,k+1),\\c&=E(n,k+2), & d&=a+b+c+2abc+2xyz,\end{aligned}$$

where

$$x=\frac{1}{4}\left((G_{k+1}-G_k)P_{2n}-\frac{S_{k-1}+(-1)^{k+1}}{3}P_{2n-2}\right)^2,$$

$$y=\frac{1}{4}(G_{k+1}P_{2n}-(H_{k+1}+(-1)^{k+1})P_{2n-2})^2,$$

$$z=\frac{1}{4}\left((G_{k+2}-G_{k+1})P_{2n}-\frac{S_k+(-1)^k}{3}P_{2n-2}\right)^2.$$

For example, if we let $n=4$ and $k=3$, we obtain the Diophantine quadruple

$$(2990, 22428, 41796, 11211312362908);$$

the six relevant squares are p^2, q^2, r^2, s^2, t^2, and u^2, where (p, q, r, s, t, u) is the sextuple

$$(8189, 11179, 30617, 183089661, 501445225, 684534886).$$

APPENDIX

In this appendix, we give proofs of Lemmas 2 and 3.

Lemma 2: For every positive integer n, $G_nH_{n+2}+G_{n+2}H_n+6=2G_{n+1}(H_{n+1}+(-1)^{n+1})$.

Proof: Let us abbreviate $G_nH_{n+2}+G_{n+2}H_n+6$ by LHS. From Propositions G and H, we see that

$$\begin{aligned}\text{LHS}&=\frac{\gamma^n-\delta^n}{\gamma-\delta}\,\frac{(1+\sqrt{3})\gamma^n-(\sqrt{3}-1)\delta^n}{6}-\frac{(-1)^{n-2}}{3}\\&\quad+\frac{\gamma^{n+2}-\delta^{n+2}}{\gamma-\delta}\,\frac{(1+\sqrt{3})\gamma^{n-2}-(\sqrt{3}-1)\delta^{n-2}}{6}-\frac{(-1)^{n-2}}{3}+6.\end{aligned}$$

Using the facts that $\gamma\delta=1$, $(1+\sqrt{3})\delta^4+(\sqrt{3}-1)\gamma^4=82\sqrt{3}$, $\gamma-\delta=2\sqrt{3}$, and a little algebra, we find that

$$\begin{aligned}\text{LHS}&=\frac{1}{6(\gamma-\delta)}\left(2(1+\sqrt{3})\gamma^{2n}+2(\sqrt{3}-1)\delta^{2n}-2\sqrt{3}-8(-1)^n\gamma^{n+1}+8(-1)^n\delta^{n+1}-82\sqrt{3}\right)+6\\&=\frac{2(1+\sqrt{3})\gamma^{2n}+2(\sqrt{3}-1)\delta^{2n}}{6(\gamma-\delta)}-\frac{8}{6}G_{n+1}(-1)^n-1.\end{aligned}$$

On the other hand, abbreviating $2G_{n+1}(H_{n+1}+(-1)^{n+1})$ by RHS, we similarly see that

$$\begin{aligned}\text{RHS}&=\frac{2}{6}\,\frac{\gamma^{n+1}-\delta^{n+1}}{\gamma-\delta}\left((1+\sqrt{3})\gamma^{n-1}-(\sqrt{3}-1)\delta^{n-1}-2(-1)^{n-1}\right)+2(-1)^{n+1}G_{n+1}\\&=\frac{2\left((1+\sqrt{3})\gamma^{2n}+(\sqrt{3}-1)\delta^{2n}-(1+\sqrt{3})\delta^2-(\sqrt{3}-1)\gamma^2\right)}{6(\gamma-\delta)}-\left(\frac{4}{6}-2\right)(-1)^{n+1}G_{n+1}.\end{aligned}$$

But $2((1+\sqrt{3})\delta^2+(\sqrt{3}-1)\gamma^2)=6(\gamma-\delta)=12\sqrt{3}$ and $(-1)^n=-(-1)^{n+1}$, so

$$\text{RHS}=\frac{2(1+\sqrt{3})\gamma^{2n}+2(\sqrt{3}-1)\delta^{2n}}{6(\gamma-\delta)}-1-\frac{8}{6}(-1)^nG_{n+1}.$$

Hence, LHS = RHS and the lemma is proved.

Lemma 3: For every positive integer n, $G_nH_{n+1}+G_{n+1}H_n+3=\frac{1}{3}(G_{n+1}-G_n)(S_{n-1}+(-1)^{n+1})$.

Proof: Let us abbreviate $G_nH_{n+1}+G_{n+1}H_n+3$ by LHS. Using Propositions G and H and the equalities cited in the proof of Lemma 2, we see that

$$\begin{aligned}\text{LHS} &= \frac{\gamma^n-\delta^n}{\gamma-\delta}\,\frac{(1+\sqrt{3})\gamma^{n-1}-(\sqrt{3}-1)\delta^{n-1}-2(-1)^{n-1}}{6}\\ &\quad+\frac{\gamma^{n+1}-\delta^{n+1}}{\gamma-\delta}\,\frac{(1+\sqrt{3})\gamma^{n-2}-(\sqrt{3}-1)\delta^{n-2}-2(-1)^{n-2}}{6}+3.\end{aligned}$$

A little more algebra leads to the equation:

$$\begin{aligned}\text{LHS} &= \frac{1}{6(\gamma-\delta)}\big(2(1+\sqrt{3})\gamma^{2n-1}+2(\sqrt{3}-1)\delta^{2n-1}-(\sqrt{3}-1)4\gamma^2\\ &\quad-(\sqrt{3}+1)4\delta^2+2(-1)^{n-1}(\gamma^n(\gamma-1)-\delta^n(\delta-1))\big)+3.\end{aligned}$$

We use the facts that $(\sqrt{3}-1)4\gamma^2+(\sqrt{3}+1)4\delta^2=24\sqrt{3}$ and $6(\gamma-\delta)=12\sqrt{3}$ and arrive at

$$\text{LHS}=\frac{1}{6(\gamma-\delta)}\big(2(1+\sqrt{3})\gamma^{2n-1}+2(\sqrt{3}-1)\delta^{2n-1}+2(-1)^n((1+\sqrt{3})\gamma^n+(\sqrt{3}-1)\delta^n)\big)+1.$$

On the other hand, abbreviating $\frac{1}{3}(G_{n+1}-G_n)(S_{n-1}+(-1)^{n-1})$ by RHS, we similarly see by Proposition S that

$$\begin{aligned}\text{RHS} &= \frac{1}{3(\gamma-\delta)}(\gamma^{n+1}-\delta^{n+1}-\gamma^n+\delta^n)(\gamma^{n-1}+\delta^{n-1}+(-1)^{n-1})\\ &= \frac{1}{3(\gamma-\delta)}\big(\gamma^{2n-1}(1+\sqrt{3})+\delta^{2n-1}(\sqrt{3}-1)+(1+\sqrt{3})\gamma\\ &\quad+(\sqrt{3}-1)\delta+(-1)^{n-1}(\gamma^n(1+\sqrt{3})+\delta^n(\sqrt{3}-1))\big).\end{aligned}$$

Since $\gamma-1=1+\sqrt{3}$, $\delta-1=-(\sqrt{3}-1)$, and $(1+\sqrt{3})\gamma+(\sqrt{3}-1)\delta=6\sqrt{3}$, we find that

$$\text{RHS}=\frac{1}{3(\gamma-\delta)}\big((1+\sqrt{3})\gamma^{2n-1}+(\sqrt{3}-1)\delta^{2n-1}+(-1)^{n-1}((1+\sqrt{3})\gamma^n+(\sqrt{3}-1)\delta^n)\big)+1.$$

Hence, LHS = RHS and this proves Lemma 3.

REFERENCES

1. M. N. Deshpande. Problem No. 10622. *Amer. Math. Monthly* **104** (1997):870.
2. A. Dujella. "Generalized Fibonacci Numbers and the Problem of Diophantus." *The Fibonacci Quarterly* **34.1** (1996):25-30.
3. A. Dujella. "A Problem of Diophantus and Pell Numbers." *Applications of Fibonacci Numbers* **7**:69-76. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1998.
4. V. E. Hoggatt, Jr., & G. E. Bergum. "A Problem of Fermat and Fibonacci Sequences." *The Fibonacci Quarterly* **15.4** (1977):323-30.

AMS Classification Numbers: 11B39, 11B61

❖❖❖

AN ALGORITHM FOR DETERMINING $R(N)$ FROM THE SUBSCRIPTS OF THE ZECKENDORF REPRESENTATION OF N

David A. Englund
9808 Wilcox Drive, Belvidere, IL 61008
(*Submitted April 1999-Final Revision July 1999*)

1. INTRODUCTION

Let $R(N)$ be the number of representations of the positive integer N as the sum of distinct Fibonacci numbers. N has a unique Zeckendorf representation [4], [3], in which no two consecutive Fibonacci numbers appear in the sum. Several methods have been developed for determining $R(N)$, many of which involve recursive formulas based on the number of representations of smaller integers [1]. In this paper we present an algorithm for determining $R(N)$ solely from the subscripts of the Zeckendorf representation of N. Carlitz [2, p. 210] has given a similar algorithm that can be used in the special case in which the subscripts in the Zeckendorf representation have the same parity.

2. STATEMENT OF THE ALGORITHM

Algorithm for $R(N)$: Write the Zeckendorf representation of N with the subscripts in descending order as follows:

$$N = \sum_{i=1}^{t} F(S_{t+1-i}) = F(S_t) + F(S_{t-1}) + F(S_{t-2}) + \cdots + F(S_j) + F(S_{j-1}) + \cdots + F(S_1),$$

where $S_j \geq S_{j-1} + 2$ and $S_1 \geq 2$, and $F(k) = F_k$. Define:

$T_0 = 1$;

$T_1 = [S_1/2]$ (where [ ] is the greatest integer function). Let

$T_j = [(S_j - S_{j-1} + 2)/2]T_{j-1}$ if S_j and S_{j-1} are of opposite parity;

$T_j = [(S_j - S_{j-1} + 2)/2]T_{j-1} - T_{j-2}$ if S_j and S_{j-1} are of the same parity.

Then $R(N) = T_t$.

Example 1: Find $R(63)$. The Zeckendorf representation of $63 = F_{10} + F_6$. Thus:

$T_0 = 1$ (by definition);

$T_1 = [6/2] = 3$;

$T_2 = [(10-6+2)/2]T_1 - T_0 = (3)(3) - 1 = 8 = R(63)$.

Example 2: Find $R(824)$. The Zeckendorf representation of $824 = F_{15} + F_{12} + F_{10} + F_7 + F_3$. Thus:

$T_0 = 1$ (by definition);

$T_1 = [3/2] = 1$;

$T_2 = [(7-3+2)/2]T_1 - T_0 = (3)(1) - 1 = 2$;

$T_3 = [(10-7+2)/2]T_2 = (2)(2) = 4$;

$T_4 = [(12-10+2)/2]T_3 - T_2 = (2)(4) - 2 = 6$;

$T_5 = [(15-12+2)/2]T_4 = (2)(6) = 12 = R(824)$.

Remark: In the special case in which all S_i are even, the validity of the present algorithm follows easily from the algorithm of Carlitz [2, p. 210]. (Alternatively, the validity of the algorithm of Carlitz follows from the validity of the present algorithm.) Suppose that all S_i are even. We write $S_t = 2k_1$, $S_{t-1} = 2k_2, \ldots, S_1 = 2k_t$, and $j_s = k_s - k_{s+1}$, $s = 1, \ldots, t-1$, $j_t = k_t$. Still following Carlitz, we define $C_0 = 1$, $C_1 = j_1 + 1$, and $C_s = (j_s + 1)C_{s-1} - C_{s-2}$, $s = 2, \ldots, t$. Slightly modifying the last step, we define $C_t' = j_t C_{t-1} - C_{t-2}$. Writing

$$C(x_1, \ldots, x_t) = \begin{vmatrix} x_1 & -1 & 0 & \cdots & 0 \\ -1 & x_2 & -1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & x_t \end{vmatrix}$$

for the continuant, we have [2, p. 212]

$$\begin{aligned} R(N) &= C_t - C_{t-1} = C_t' \\ &= C(j_1 + 1, j_2 + 1, \ldots, j_{t-1} + 1, j_t) \\ &= C(j_t, j_{t-1} + 1, j_{t-2} + 1, \ldots, j_1 + 1) = T_t. \end{aligned}$$

For example, if $N = F_{16} + F_8 + F_4 = 1011$, then $(j_1 + 1, j_2 + 1, j_3) = (5, 3, 2)$ and the (modified) Carlitz algorithm gives:

$C_0 = 1;$

$C_1 = 5;$

$C_2 = (3)(5) - 1 = 14;$

$C_3' = (2)(14) - 5 = 23 = R(N).$

Using the present algorithm, we obtain:

$T_0 = 1;$

$T_1 = 2;$

$T_2 = (3)(2) - 1 = 5;$

$T_3 = (5)(5) - 2 = 23 = R(N).$

3. PROOF OF THE ALGORITHM

Lemma: Following the steps of the algorithm set forth in Section 2, if $N = F_m - 1$ $(m \geq 3)$, then $T_0 = T_1 = \cdots = T_t = 1$.

Proof: This follows immediately from the formulas [3]

$$F_3 + F_5 + \cdots + F_{2n-1} = F_{2n} - 1 \ (n \geq 2) \text{ and } F_2 + F_4 + \cdots + F_{2n} = F_{2n+1} - 1 \ (n \geq 1).$$

Theorem: Following the steps of the algorithm set forth in Section 2, $R(N) = T_t$.

Proof: We use induction on t, the number of terms in the Zeckendorf representation of N. (Note that, if $t > 1$, then the Zeckendorf representation of $N - F(S_t)$ is clearly $F(S_{t-1}) + F(S_{t-2}) + \cdots + F(S_j) + F(S_{j-1}) + \cdots + F(S_1)$.)

1. The cases $t = 1$ and $t = 2$ follow immediately from the formula [1, p. 53] $R(F_n) = [n/2]$ and from [1, Theorem 7, p. 58], respectively.

2. We suppose now that $t \geq 3$ and that the theorem is valid for $t-1$ and $t-2$. Let $S_t = m$ and $S_{t-1} = n$, so that $m-n \geq 2$ and $n \geq 4$. We write

$$N' = N - F(S_t) = F(S_{t-1}) + F(S_{t-2}) + \cdots + F(S_j) + F(S_{j-1}) + \cdots + F(S_1).$$

Then we have $F_n \leq N' \leq F_{n+1} - 1$.

a) If $F_n \leq N' \leq F_{n+1} - 2$, we use [1, Corollary 3.1, p. 53].

a-1) Suppose that $m-n$ is odd. Then

$$R(n) = [(m-n+1)/2]R(N') = [(m-n+2)/2]T_{t-1} = T_t,$$

using the induction hypothesis.

a-2) Suppose that $m-n$ is even. Using [1, Theorem 2, p. 48] and the induction hypothesis, we get

$$\begin{aligned} R(N) &= [(m-n+1)/2]R(N') + R(F_{n+1} - 2 - N') \\ &= [(m-n+2)/2]R(N') - (R(N') - R(F_{n+1} - 2 - N')) \\ &= [(m-n+2)/2]R(N') - R(N' - F_n) = [(m-n+2)/2]T_{t-1} - T_{t-2} = T_t. \end{aligned}$$

b) Suppose now that $N' = F_{n+1} - 1 = F_n + F_{n-2} + \cdots$. By [1, Theorem 7, p. 58], we have $R(N) = [(m-n+1)/2]$. On the other hand, using the Lemma, we have

$$T_t = ([(m-n+2)/2])(1) = [(m-n+1)/2]$$

if $m-n$ is odd, while

$$T_t = ([(m-n+2)/2])(1) - 1 = [(m-n+1)/2]$$

if $m-n$ is even. So we have $R(N) = T_t$ in this case also. This completes the proof.

ACKNOWLEDGMENT

The author wishes to thank the anonymous referee for useful suggestions and for a proof of the algorithm by induction, which is considerably shorter than the proof in graph form contained in the author's original submission.

REFERENCES

1. M. Bicknell-Johnson & D. C. Fielder. "The Number of Representations of N Using Distinct Fibonacci Numbers, Counted by Recursive Formulas." *The Fibonacci Quarterly* **37.1** (1999): 47-60.
2. L. Carlitz. "Fibonacci Representations." *The Fibonacci Quarterly* **6.4** (1968):193-220.
3. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin, 1969; rpt. Santa Clara, CA: The Fibonacci Association, 1979.
4. E. Zeckendorf. "Representation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas." *Bull. Soc. Royale Sci. Liège* **41** (1972):179-82,

AMS Classification Numbers: 11B39, 11B37, 11Y55

❖❖❖

AN ANALYSIS OF n-RIVEN NUMBERS

H. G. Grundman*

Department of Mathematics, Bryn Mawr College, Bryn Mawr, PA 19010

(*Submitted April 1999-Final Revision July 2000*)

1. INTRODUCTION

For a positive integer a and $n \geq 2$, define $s_n(a)$ to be the sum of the digits in the base n expansion of a. If s_n is applied recursively, it clearly stabilizes at some value. Let $S_n(a) = s_n^k(a)$ for all sufficiently large k.

A Niven number [3] is a positive integer a that is divisible by $s_{10}(a)$. We define a riven number (short for recursive Niven number) to be a positive integer a that is divisible by $S_{10}(a)$. As in [2], these concepts are generalized to n-Niven numbers and n-riven numbers, using the functions s_n and S_n, respectively.

In [1], Cooper and Kennedy proved that there does not exist a sequence of more than 20 consecutive Niven numbers and that this bound is optimal. Wilson [4] determined the digit sum of the smallest number initiating a maximal Niven number sequence. The author [2] proved that, for each $n \geq 2$, there does not exist a sequence of more than $2n$ consecutive n-Niven numbers and Wilson [5] proved that this bound is optimal.

This paper presents general properties of n-riven numbers and examines the maximal possible lengths of sequences of consecutive n-riven numbers. We begin with a basic lemma characterizing the value of $S_n(a)$, which leads to many general facts about n-riven numbers. In Section 3 we determine the maximal lengths of sequences of consecutive n-riven numbers. We construct examples of sequences of maximal length for each n including ones that are provably as small as possible in terms of the values of the numbers in them.

2. BASIC PROPERTIES

Lemma 1: Fix $n \geq 2$ and $a > 0$. Then $S_n(a)$ is the unique integer such that $0 < S_n(a) < n$ and $S_n(a) \equiv a \pmod{n-1}$.

Proof: Let $a = \sum_{i=0}^{r} a_i n^i$. Then $s_n(a) = \sum_{i=0}^{r} a_i$. Since $n \equiv 1 \pmod{n-1}$, $s_n(a) \equiv a \pmod{n-1}$. Hence, for all k, $s_n^k(a) \equiv a \pmod{n-1}$, and so $S_n(a) \equiv a \pmod{n-1}$. From this, the lemma easily follows.

Corollary 2: Every positive integer is 2-riven.

Proof: It follows from Lemma 1 that, for every a, $S_2(a) = 1$.

Corollary 3: Every positive integer is 3-riven.

Proof: It follows from Lemma 1 that, for every a, $S_3(a) \equiv a \pmod 2$. So $S_3(a) = 1$ if a is odd and $S_3(a) = 2$ if a is even. Clearly, in either case, a is divisible by $S_3(a)$.

Corollary 4: For each $n \geq 2$, if a is divisible by $n-1$, then a is an n-riven number.

---

* The author wishes to acknowledge the support of the Science Scholars Fellowship Program at the Bunting Institute of Radcliffe College.

Proof: If a is divisible by $n-1$, then by Lemma 1, $S_n(a) = n-1$. So a is an n-riven number.

Corollary 5: For each $n \geq 2$, there are infinitely many n-riven numbers.

3. CONSECUTIVE n-RIVEN NUMBERS

We now examine sequences of consecutive n-riven numbers. In light of Corollaries 2 and 3, we *fix a positive integer* $n \geq 4$.

Lemma 6: Let $a < b$ be numbers in a sequence of consecutive n-riven numbers. If $a \equiv b \pmod{n-1}$, then $S_n(a) | (n-1)$.

Proof: Since $a < b$ and $a \equiv b \pmod{n-1}$, $n-1 \leq b-a$. Therefore, $a+n-1 \leq b$ and so $a+n-1$ is also in the sequence of n-riven numbers. Hence, $S_n(a) | a$ and $S_n(a+n-1) | (a+n-1)$. By Lemma 1, $S_n(a+n-1) = S_n(a)$. Therefore, $S_n(a) | (a+n-1)$ and so $S_n(a) | (n-1)$.

Corollary 7: At most one number in a sequence of consecutive n-riven numbers is congruent to -1 modulo $n-1$.

Proof: Let $a < b$ be numbers in a sequence of consecutive n-riven numbers with $a \equiv b \equiv -1 \pmod{n-1}$. By Lemma 6, $S_n(a) | (n-1)$. But this means that $(n-2) | (n-1)$, which is impossible for $n \geq 4$. Thus, by contradiction, no such distinct a and b can exist.

Corollary 8: There does not exist an infinitely long sequence of n-riven numbers. Equivalently, there are infinitely many numbers which are not n-riven.

Fix $m_n = \min\{k \in \mathbf{Z}^+ | k \nmid (n-1)\}$. In Theorem 9, we prove that there do not exist more than $n+m_n-1$ consecutive n-riven numbers. In Theorem 10, we prove that this bound is the best possible. Further, we find the smallest number initiating an n-riven number sequence of maximal length.

In Table 1 we present the maximal lengths of sequences of consecutive n-riven numbers for various values of n, along with the maximal sequences of minimal values.

TABLE 1. Maximal Sequences for $4 \leq n \leq 10$

n	Length	Minimal Sequence of Maximal Length
4	5	6, 7, 8, 9, 10
5	7	12, 13, 14, 15, 16, 17, 18
6	7	60, 61, 62, 63, 64, 65, 66
7	10	60, 61, 62, 63, 64, 65, 66, 67, 68, 69
8	9	420, 421, 422, 423, 424, 425, 426, 427, 428
9	11	840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850
10	11	2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530

Theorem 9: A sequence of consecutive n-riven numbers consists of at most $n+m_n-1$ numbers. Further, any such sequence of maximal length must start with a number congruent to zero modulo $n-1$.

Proof: Let a, $a+1$, $a+2$, ..., $a+n+m_n-2$ be a sequence of consecutive n-riven numbers and suppose $S_n(a) = k \neq n-1$.

Case 1. $1 \le k \le n - m_n$. Modulo $n-1$, we have $a \equiv a+n-1 \equiv k$, $a+1 \equiv a+n \equiv k+1$, ..., $a+m_n-1 \equiv a+n+m_n-2 \equiv k+m_n-1$. Since each of these is an n-riven number and $k+m_n-1 \le n-1$, we can apply Lemma 6 to get that each of k, $k+1, \ldots, k+m_n-1$ divides $n-1$. There are m_n consecutive numbers in this list. Therefore, m_n divides one of them, and thus m_n divides $n-1$. But this contradicts the definition of m_n.

Case 2. $n-m_n < k < n-1$. Since $k+1 \le n-1$, $a+(n-1)-(k+1)$ is in the sequence, and since $2n-k-3 < n+m_n-2$, $a+2(n-1)-(k+1)$ is in the sequence. But each of these in congruent to -1 modulo $n-1$, so we have a contradiction to Corollary 7.

Therefore, $S_n(a) = n-1$.

Now, suppose that $a+n+m_n-1$ is also n-riven. Then $a+m_n$ and $a+m_n+(n-1)$ are both in the sequence. So, $S_n(a+m_n) = m_n$ divides $n-1$, by Lemma 6, contradicting the definition of m_n.

We now construct an infinite family of sequences of n-riven numbers that are of length $n+m_n-1$, thus proving that the bound in Theorem 9 is optimal. One of these sequences, we will prove, is minimal in that there exist no smaller numbers forming an n-riven number sequence of maximal length.

Theorem 10: Fix $\ell = \text{lcm}(1, 2, 3, \ldots, n-1)$ and let a be any integral multiple of ℓ. Then a, $a+1$, $a+2, \ldots, a+n+m_n-2$ is a sequence of consecutive n-riven numbers of maximal length. Further, ℓ is minimal such that ℓ, $\ell+1$, $\ell+2, \ldots$, $\ell+n+m_n-2$ is a sequence of consecutive n-riven numbers of maximal length.

Proof: We first show that each of these numbers is n-riven. Since $(n-1)|a$, it is n-riven, by Corollary 4. For $1 \le t \le n-1$, $S_n(a+t) = t$, which divides a and therefore $a+t$ Thus, $a+t$ is n-riven. Finally, for $1 \le t \le m_n - 1$, $S_n(a+n-1+t) = t$ which, as above, divides $a+t$. Further, by definition of m_n, t divides $n-1$. Hence, $t|(a+n-1+t)$ and so $a+n-1+t$ is an n-riven number.

It remains to show that ℓ is the smallest number initiating a maximal sequence of consecutive n-riven numbers. Let $a, a+1, a+2, \ldots, a+n+m_n-2$ be such a sequence. Then, by Theorem 9, $a \equiv 0 \pmod{n-1}$ and so $S_n(a) = n-1$. For all $1 \le t \le n-1$, $a+t$ is an n-riven number, implying that $t|(a+t)$ and so $t|a$. Thus, $\text{lcm}(1, 2, 3, \ldots, n-1)|a$. The result now follows trivially.

REFERENCES

1. C. Cooper & R. E. Kennedy. "On Consecutive Niven Numbers." *The Fibonacci Quarterly* **31.2** (1993):146-51.
2. H. G. Grundman. "Sequences of Consecutive n-Niven Numbers." *The Fibonacci Quarterly* **32.2** (1994):174-75.
3. R. Kennedy, T. Goodman, & C. Best. "Mathematical Discovery and Niven Numbers." *The MATYC Journal* **14** (1980):21-25.
4. B. Wilson. "Construction of Small Consecutive Niven Numbers." *The Fibonacci Quarterly* **34.3** (1996):240-43.
5. B. Wilson. "Construction of $2*n$ Consecutive Niven Numbers." *The Fibonacci Quarterly* **35.2** (1997):122-28.

AMS Classification Number: 11A63

❖❖❖

ON THE REPRESENTATION OF THE INTEGERS AS A DIFFERENCE OF NONCONSECUTIVE TRIANGULAR NUMBERS

M. A. Nyblom
Dept. of Math., Royal Melbourne Institute of Technology
GPO Box 2476V, Melbourne, Victoria 3001, Australia
(*Submitted April 1999-Final Revision September 1999*)

1. INTRODUCTION

The problem of determining the set of integer solutions of a polynomial equation, over $\mathbf{Z}$, occurs frequently throughout much of the theory of numbers. Typically, the most common form of these problems involves quadratic functions in several variables, such as those dealing with the polygonal representation of the integers. The nth polygonal number of order k is defined as the nth partial sum of a sequence of integers in arithmetic progression, having a first term of one and a common difference of $k-2$, and so is given by $\frac{1}{2}[(k-2)n^2-(k-4)n]$. One of the earliest results in connection with representing the positive integers as sums of polygonal numbers was due to Gauss, who proved that every positive integer could be expressed as a sum of three triangular numbers. Despite these classical origins, many difficult and interesting problems dealing with polygonal representations of the integers are still unresolved at present (see [1]). In this paper we shall continue with the theme of polygonal representation but in a slightly different direction by examining the following problem involving the differences of triangular numbers denoted here by $T(x)=\frac{1}{2}x(x+1)$.

Problem: Given any $M \in \mathbf{Z}\setminus\{0\}$, for what values $x, y \in \mathbf{N}$ is it possible that $M = T(x)-T(y)$ such that $|x-y|>1$, and how many such representations can be found?

The fact that a number can be represented as a difference of triangular number is not at all surprising since, by definition, $M = T(M)-T(M-1)$; hence, the restriction $|x-y|>1$ in the problem statement. To establish the existence or otherwise of a representation for M, we will see that the problem can be reduced to solving the diophantine equation $X^2-Y^2=8M$ in odd integers. Although this equation is solvable for all $M \in \mathbf{Z}\setminus\{0\}$, there is a subset of $\mathbf{Z}\setminus\{0\}$, namely, $\{\pm 2^m : m \in \mathbf{N}\}$, for which the consecutive triangular number difference is the only possible representation. Apart from the set mentioned, all other $M \in \mathbf{Z}\setminus\{0\}$ will have a nonconsecutive triangular representation and, moreover, the exact number will be shown to equal $D-1$, where D is the number of odd divisors of M, which will require a combinatorial type argument to establish. We note that a somewhat similar problem to the one above was studied in [3] where, for a given $s \in \mathbf{N}$, it was asked for what $r \in \mathbf{N}\setminus\{0\}$ could $T(r+s)-T(s)$ be a triangular number. However, unlike our result, for every $r \in \mathbf{N}\setminus\{0\}$, there corresponded an infinite number $m \in \mathbf{N}\setminus\{0\}$ such that $T(m)$ was expressible as a difference of triangular numbers indicated. In addition to the above, we shall provide an alternate proof of a result of E. Lucas dated around 1873, namely, that all triangular numbers greater than one can never be a perfect cube. This result, as we shall see, will follow as a corollary of the main representation theorem.

2. MAIN RESULT

We begin in this section by introducing a preliminary definition and lemma which will be required later in developing a formula for the total number of nonconsecutive triangular number representations of the integers.

Definition 2.1: For a given $M \in \mathbb{N} \setminus \{0\}$, a factorization $M = ab$ with $a, b \in \mathbb{N} \setminus \{0\}$ is said to be nontrivial if $a \neq 1, M$. Two such factorizations, $a_1 b_1 = a_2 b_2 = M$, are distinct if $a_1 \neq a_2, b_2$.

The following result, which concerns counting the total number of distinct nontrivial factorizations $ab = M$, may be known, but it is included here for completeness. Note that in the subsequent definition for $d(M)$ we include both 1 and M when counting the total number of divisors of M.

Lemma 2.1: Let M be an integer greater than unity and $d(M)$ be the number of divisors of M. Then the total number $N(M)$ of nontrivial distinct factorizations of M is given by

$$N(M) = \begin{cases} \frac{d(M)-2}{2} & \text{for nonsquare } M, \\ \frac{d(M)-1}{2} & \text{for square } M. \end{cases}$$

Proof: Suppose $M = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$, then the total number of divisors of M is

$$d(M) = (1+m_1)(1+m_2)\cdots(1+m_n).$$

Clearly, if $d|M$, then $(M/d)|M$; thus, the required factorization $ab = M$ will be given by $(a,b) = (d, M/d)$ provided $d \neq 1, M$. Excluding $d = 1$ and $d = M$, we have $d(M) - 2$ divisors d_i of M such that $1 < d_i < M$ for $i = 1, 2, \ldots, (d(M) - 2)$. Arrange these divisors in ascending order and consider the set of ordered pairs

$$I = \{(d_i, M/d_i) : i = 1, 2, \ldots, (d(M) - 2)\}.$$

If M is not a perfect square, then $2|d(M)$ and so there will be an even number of elements in I. Consider for each $i = 1, 2, \ldots, (d(M) - 2)/2$ the subset $I_i = \{(d_i, M/d_i), (M/d_i, d_i)\}$ and note that $I_i \cap I_j = \emptyset$ for $i \neq j$ together with

$$I = \bigcup_{i=1}^{(d(M)-2)/2} I_i.$$

As both ordered pairs in each particular I_i correspond to the same nontrivial factorization of M, which must be distinct from that in I_j for $i \neq j$, one can conclude that $N(M) = (d(M) - 2)/2$. Suppose now that M is a square, then $d(M)$ will be odd, and so I contains an odd number of elements. Furthermore, there must exist a unique $j \in \{1, 2, \ldots, (d(M) - 2)\}$ such that $d_j = M/d_j$, from which it is clear that $I_j = \{(d_j, d_j)\}$. Considering now the set $I' = I \setminus I_j$ which contains only $d(M) - 3$ elements, one again has

$$I' = \bigcup_{i=1, i \neq j}^{(d(M)-3)/2} I_i,$$

from which we can count $(d(M) - 3)/2$ nontrivial distinct factorizations of M together with the one from I_j to obtain $N(M) = 1 + (d(M) - 3)/2 = (d(M) - 1)/2$. □

Using Lemma 2.1, we can now establish the required representation theorem.

Theorem 2.1: Let $M \in \mathbf{Z} \setminus \{0\}$, then the number of distinct representations of M as a difference of nonconsecutive triangular numbers is given by $N_{\Delta}(M) = D - 1$, where D is the number of odd divisors of M.

Proof: Without loss of generality, we may assume that M is a positive integer. Our aim here will be to determine whether there exists $x, y \in \mathbf{N} \setminus \{0\}$ such that $M = T(x) - T(y)$. By completing the square, observe that the previous equation can be recast in the form $8M = X^2 - Y^2$, where $X = 2x + 1$ and $Y = 2y + 1$. To analyze the solvability of this equation, suppose $ab = 8M$, where $a, b \in \mathbf{N} \setminus \{0\}$ and consider the following system of simultaneous linear equations:

$$\begin{aligned} X - Y &= a \\ X + Y &= b \end{aligned} \tag{1}$$

whose general solution is given by

$$(X, Y) = \left(\frac{a+b}{2}, \frac{b-a}{2}\right).$$

Now, for there to exist a representation of M as a difference of nonconsecutive triangular numbers, one must be able to find factorizations $ab = 8M$ for which the system (1) will yield a solution (X, Y) in odd integers.

Remark 2.1: We note that it is sufficient to consider only (1), since if for a chosen factorization $ab = 8M$ an odd solution pair (X, Y) is found, then the corresponding representation $M = T(x) - T(y)$ is also obtained if the right-hand side of (1) is interchanged. Indeed, one finds upon solving

$$\begin{aligned} X' - Y' &= b \\ X' + Y' &= a \end{aligned}$$

where $X' = 2x' + 1$, $Y' = 2y' + 1$ that

$$X' = \frac{a+b}{2} \quad \text{and} \quad Y' = \frac{a-b}{2} = -Y.$$

Thus, $x' = x$ while $y' = (-Y - 1)/2 = -y - 1$, so

$$T(y') = \frac{(-y-1)(-y)}{2} = T(y) \quad \text{and} \quad T(x') - T(y') = T(x) - T(y) = M.$$

We deal with the existence or otherwise of those factorizations $ab = 8M$ which give rise to an odd solution pair (X, Y) of (1). It is clear from the general solution of (1) that, for X to be an odd positive integer a, b must be at least chosen so that $a + b = 2(2s + 1)$ for some $s \in \mathbf{N} \setminus \{0\}$. As ab is even, this can only be achieved if a and b are also both even. Furthermore, such a choice of a and b will also ensure that $Y = X - a$ is odd. With this reasoning in mind, it will be convenient to consider the following cases separately.

Case 1. $M = 2^n$, $n \in \mathbf{N} \setminus \{0\}$.

In this instance, consider $8M = 2^{n+3} = ab$, where $(a, b) = (2^i, 2^{n+3-i})$ for $i = 0, 1, \ldots, n+3$ with $a + b = 2(2^{i-1} + 2^{n+2-i}) = 2(2s + 1)$ only when $i = 1, n+2$. However, since both factorizations are equivalent, we need only investigate the solution of (1) when $(a, b) = (2, 2^{n+2})$. Thus, one finds

that $(X, Y) = (1+2^{n+1}, 2^{n+1}-1)$ and so $(x, y) = (2^n, 2^n - 1)$. Hence, there exists only the trivial representation $M = T(M) - T(M-1)$.

Case 2. $M \neq 2^n$.

Clearly, $M = 2^m(2n+1)$ for an $n \in \mathbf{N} \setminus \{0\}$ and $m \in \mathbf{N}$. However, as there are more available factorizations of $8M$, due to the presence of the term $2n+1$, it will be necessary to consider the following subcases based on the possible factorizations $cd = 2n+1$.

Subcase 1. $(c, d) = (1, 2n+1)$.

Here consider $8M = 2^{m+3}(2n+1) = ab$, where $(a, b) = (2^i, 2^{m+3-i}(2n+1))$ for $i = 0, 1, \ldots, m+3$ with $a+b = 2(2^{i-1} + 2^{m+2-i}(2n+1)) = 2(2s+1)$ only when $i = 1, m+2$. Solving (1) with $(a, b) = (2, 2^{m+2}(2n+1))$, one finds that $(x, y) = (2^m(2n+1), 2^m(2n+1)-1)$, which corresponds to a consecutive triangular number difference of M, while for $(a, b) = (2^{m+2}, 2(2n+1))$ we have $(x, y) = (2^m + n, n - 2^m)$ and so

$$M = T(2^m + n) - T(y'), \tag{2}$$

where $y' = 2^m - n - 1$ if $y < 0$ and $y' = y$ otherwise. In either situation, one has $|x - y'| > 1$, giving a nonconsecutive triangular number representation of M.

Subcase 2. $(c, d), c \neq 1, 2n+1$.

Here consider $8M = 2^{m+3}cd = ab$, where $(a, b) = (2^i c, 2^{m+3-i}d)$ for $i = 0, 1, \ldots, m+2$ with $a+b = 2(2^{i-1}c + 2^{m+2-i}d) = 2(2s+1)$ when $i = 1, m+2$. Solving (1) with $(a, b) = (2c, 2^{m+2}d)$, one has $(X, Y) = (c + 2^{m+1}d, 2^{m+1}d - c)$, from which it is immediate that

$$(x, y) = \left(\frac{c-1}{2} + 2^m d, 2^m d - \frac{c+1}{2}\right)$$

and so

$$M = T\left(\frac{c-1}{2} + 2^m d\right) - T(y'), \tag{3}$$

where $y' = \frac{c+1}{2} - 2^m d - 1$ if $y < 0$ and $y' = y$ otherwise. Alternatively, when $(a, b) = (2^{m+2}c, 2d)$, one has $(X, Y) = (2^{m+1}c + d, d - 2^{m+1}c)$, from which we obtain

$$(x, y) = \left(2^m c + \frac{d-1}{2}, \frac{d-1}{2} - 2^m c\right)$$

and again

$$M = T\left(2^m c + \frac{d-1}{2}\right) - T(y'), \tag{4}$$

where $y' = 2^m c - \frac{d-1}{2} - 1$ if $y < 0$ and $y' = y$ otherwise. In either of the representations in (3) and (4), it is again easily seen that $|x - y'| > 1$. Consequently, for every distinct factorization $cd = 2n+1$ with $c \neq 1, (2n+1)$, we can expect at most two representations of $M = 2^m(2n+1)$ as a difference of two nonconsecutive triangular numbers.

We now address the problem of finding the exact number $N_\Delta(M)$ of representations for an M in Case 2. Primarily, this will entail determining whether any duplication occurs between the various representations given in (2), (3), and (4). Recall that two factorizations $a_i b_i = a_j b_j = 8M$

are said to be distinct if $a_i \neq a_j, b_j$ for $i \neq j$. First, it will be necessary to show that any two distinct factorizations of $8M$ considered in Case 2 will always produce two different triangular representations for M. To this end, we need to demonstrate that if in $\mathbf{Z} \setminus \{0\}$ $a_i b_i = a_j b_j$, with $a_i \neq a_j$, b_j for $i \neq j$, then one has $a_i + b_i \neq a_j + b_j$. Suppose to the contrary that $a_i + b_i = a_j + b_j$, then there must exist an $r \in \mathbf{Z} \setminus \{0\}$ such that $a_j = a_i + r$ and $b_i = b_j + r$. Substituting these equations into the equality $a_i b_i = a_j b_j$, one finds $a_i(b_j + r) = (a_i + r)b_j$. Hence, r must be a nonzero integer solution of

$$r(a_i - b_j) = 0. \tag{5}$$

However, this is impossible because $r = 0$ is the only possible solution of (5) since $a_i - b_j \neq 0$; a contradiction. Consequently, if for two distinct factorizations $a_i b_i = a_j b_j = 8M$, one solves (1) to produce corresponding odd solution pairs (X_i, Y_i) and (X_j, Y_j), then we must have

$$X_i = (a_i + b_i)/2 \neq (a_j + b_j)/2 = X_j$$

and so $x_i \neq x_j$. Moreover, as $x_i, x_j \geq 0$, we immediately see that $T(x_i) \neq T(x_j)$, hence

$$T(y_i) = T(x_i) - M \neq T(x_j) - M = T(y_j).$$

Thus, in order to calculate $N_\Delta(M)$ for $M = 2^m(2n+1)$, one must determine the total number of distinct factorizations $ab = 8M$ examined in Case 2. Recall that in Subcase 2 the only triangular representation of M was found by the factorization $(a, b) = (2^{m+2}, 2(2n+1))$. Clearly, this cannot be repeated by the factorizations $(a, b) = (2c, 2^{m+2}d)$ or $(a, b) = (2^{m+2}c, 2d)$ in Subcase 2 since $c \neq 1, 2n+1$. Now, if $2n+1$ is not a perfect square, that is, $c \neq d$, then $2c \neq 2^{m+2}c, 2d$ and so, by the above, each factorization $cd = 2n+1$ with $c \neq 1, 2n+1$ will produce two unique representations of M as a difference of two nonconsecutive triangular numbers. Consequently, in this instance, by combining both subcases we see that $N_\Delta(M)$ must be one more than twice the total number of nontrivial distinct factorizations $cd = 2n+1$. Thus, if one denotes by D the total number of divisors of $2n+1$, then by Lemma 2.1,

$$N_\Delta(M) = 1 + 2\left(\frac{D-2}{2}\right) = D - 1.$$

However, if $2n+1$ is a perfect square, then $(2c, 2^{m+2}d)$ and $(2^{m+2}c, 2d)$ will be equivalent factorizations when $c = d$. So by Lemma 2.1 only $\frac{D-1}{2} - 1$ of the factorizations in Subcase 2 will produce two distinct triangular representations of M. Hence, counting the remaining factorization $(2c, 2^{m+2}c)$ together with the one in Subcase 1, we find that

$$N_\Delta(M) = 2\left(\frac{D-1}{2} - 1\right) + 2 = D - 1.$$

To conclude, we note that the formula $N_\Delta(M) = D - 1$ also holds for all integers 2^m, where $m = 0, 1, \ldots$, since by Case 1, $N_\Delta(2^m) = 0$ while, clearly, $D - 1 = 0$ because 1 is the only odd divisor of 2^m. □

Example 2.1: For a given integer M whose prime factorization is known, one can use equations (2), (3), and (4) to determine all of the $D-1$ representations of M as a difference of triangular numbers. To illustrate this, we shall calculate the representations in the case of a square and non-

square number. Beginning with, say $M = 2^2 \cdot 5 \cdot 7^2$, we have $N_\Delta(980) = 5$. So, if $cd = 5 \cdot 7^2$ and $m = 2$, then apart from $(c, d) = (1, 5 \cdot 7^2)$ each of the factorizations $(c, d) \in \{(5, 7^2), (5 \cdot 7, 7)\}$ will produce two distinct representations via (3) and (4). The remaining representation can be calculated using (2), with $n = (5 \cdot 7^2 - 1)/2$. Consequently, one obtains that

$$\begin{aligned} 980 &= T(126) - T(118) = T(198) - T(193) \\ &= T(45) - T(10) = T(143) - T(136) = T(44) - T(4). \end{aligned}$$

If, on the other hand, $M = (2 \cdot 5 \cdot 7)^2$, then; $N_\Delta(4900) = 8$. So again, for $(c, d) = (1, (2 \cdot 5 \cdot 7)^2)$ and $m = 2$, there corresponds one representation calculated via (2) with $n = ((2 \cdot 5 \cdot 7)^2 - 1)/2$. Apart from $(c, d) = (5 \cdot 7, 5 \cdot 7)$, all of the factorizations $(c, d) \in \{(5, 5 \cdot 7^2), (5^2, 7^2), (5^2 \cdot 7, 7)\}$ will each produce two distinct representations via (3) and (4). However, for $(c, d) = (5 \cdot 7, 5 \cdot 7)$, the representations given in (3) and (4) are identical as $c = d$. Thus, we obtain

$$\begin{aligned} 4900 &= T(616) - T(608) = T(982) - T(977) = T(142) - T(102) = T(208) - T(183) \\ &= T(124) - T(75) = T(115) - T(59) = T(703) - T(696) = T(157) - T(122). \end{aligned}$$

We now use Theorem 2.1 to deduce that all triangular numbers greater than unity cannot be a perfect cube. To achieve this end, the following two technical lemmas will be required, the first of which gives a necessary and sufficient condition for a positive integer to be a triangular number.

Lemma 2.2: An integer M greater than unity is triangular if and only if out of the $D-1$ distinct representations of $M = T(x) - T(y')$, with $|x - y'| > 1$, there exists one in which $y' = 0$.

Proof: Clearly, if $M = T(x) - T(0)$ for some $x \in \mathbb{N}$, then M is triangular. Conversely, assume M is a triangular number. To show there exists a representation of the above form, with $y' = 0$, it will be sufficient to find a factorization $ab = 8M$ such that the system of equations in (1) has a solution (X, Y) with $Y = 1$. From the general solution

$$(X, Y) = \left(\frac{a+b}{2}, \frac{b-a}{2}\right),$$

this is equivalent to finding positive integers a, b which simultaneously satisfy $b - a = 2$ and $ab = 8M$. Solving for b in terms of a from the first equation and substituting the result into the second, one finds upon simplifying that $0 = a^2 + 2a - 8M$. Hence, $a = -1 + \sqrt{1 + 8M}$; however, this must be a positive integer since $1 + 8M$ is a perfect square greater than unity. Consequently, $b = 2 + a$ is also a positive integer. □

Lemma 2.3: If c is an odd cube greater than unity, then neither $(c+1)/2$ nor $(c-1)/2$ can be perfect cubes.

Proof: To demonstrate the result, it is equivalent to show that the diophantine equations $X^3 - 2Y^3 = 1$ and $X^3 - 2Y^3 = -1$ have no solutions (X, Y) with $X > 1$. By Theorem 5 of [2], we have that $x^3 + dy^3 = 1$ $(d > 1)$ has at most one integer solution (x, y) with $xy \neq 0$. Now, since $(x, y) = (-1, 1)$ is such a solution of $x^3 + 2y^3 = 1$, it can be the only one with $xy \neq 0$. Making the substitution $X = x$, $Y = -y$, we deduce that $(X, Y) = (-1, -1)$ is the only integer solution $X^3 - 2Y^3 = 1$ while, if we take $X = -x$, $Y = y$, then $(X, Y) = (1, 1)$ can be the only integer solution of $X^3 - 2Y^3 = -1$. Hence, in either case, no other integer solutions (X, Y) exists where $X > 1$. □

Combining the previous two lemmas, we can now prove the desired result, which is stated here in terms of the solvability of a diophantine equation.

Corollary 2.1: The only solutions of the diophantine equation $x(x+1) = 2y^3$ are given by $(x, y) = (1, 1), (-2, 1), (-1, 0), (0, 0)$.

Proof: Note that, as $x(x+1) \geq 0$ for all $x \in \mathbf{Z}$, one may assume, without loss of generality, that x and y are positive integers. We shall first establish that no integer solution (x, y) exists for $x > 1$. To this end, let M be a triangular number greater than unity and *assume* it is a perfect cube. In order to derive the necessary contradiction, we will show that all of the $D-1$ representations of $M = T(x) - T(y')$ have $y' \neq 0$, which is in violation of Lemma 2.2. Now, since $M = 2^m(2n+1)$ for some $n \in \mathbf{N} \setminus \{0\}$ and $m \in \mathbf{N}$, 2^m and $2n+1$ must be perfect cubes because $(2^m, 2n+1) = 1$. Considering the representation given in (2), suppose $y' = 0$, then either $n = 2^m$ or $n = 2^m - 1$. Taking $n = 2^m = Y^3 > 1$, we then have $2n+1 = 2Y^3 + 1 = X^3$ for some $X \in \mathbf{N} \setminus \{0\}$, which is impossible by the argument used to establish Lemma 2.3. Similarly, if $n = 2^m - 1$, then $2n+1 = 2Y^3 - 1 = X^3$ for some $X \in \mathbf{N} \setminus \{0\}$, which again is impossible. Hence, for the representation in (2), $y' \neq 0$. Writing now $M = 2^m cd$, where $c \neq 1$, $2n+1$ and setting $y' = 0$ in the representation given in (3), we must have either $2^m d = \frac{c+1}{2}$ or $2^m d = \frac{c-1}{2}$. Multiplying both sides of these equations by c, one deduces $M = T(c)$ or $M = T(c-1)$. Now, since $(c, \frac{c+1}{2}) = 1$ and $(c, \frac{c-1}{2}) = 1$, we conclude that either c and $\frac{c+1}{2}$ or c and $\frac{c-1}{2}$ are a pair of perfect cubes; a contradiction by Lemma 2.3. Thus, for the representation in (3), $y' \neq 0$. By setting $y' = 0$ in the remaining representation given in (4), one can similarly arrive at the contradictory conclusion that either d and $\frac{d+1}{2}$ or d and $\frac{d-1}{2}$ are a pair of perfect cubes. Thus, for the representation in (4), $y' \neq 0$. Consequently, via Lemma 2.2, M is not a triangular number; a contradiction. Therefore, M cannot be a perfect cube and so $x(x+1) = 2y^3$ has no integer solutions (x, y) with $x > 1$. The solutions indicated can now be found upon inspecting the solvability for the remaining integers $x \in [-2, 1]$. □

Remark 2.2: The above argument could be applied in exactly the same manner to investigate the solvability of the diophantine equation $x(x+1) = 2y^n$ for $n \geq 4$, provided one could ascertain for each such n the solvability of $X^n - 2Y^n = \pm 1$ in integers (X, Y).

In conclusion, we consider some further consequences of Theorem 2.1. The first of these gives a necessary and sufficient condition for a positive integer to be an odd prime and follows directly from the fact that a number $p \in \mathbf{N}$ is an odd prime if and only if $D = 2$.

Corollary 2.2: An integer $p \in \mathbf{N} \setminus \{0\}$ is prime if and only if $N_\Delta(p) = 1$.

In connection with the representation of primes as a difference of the polygonal numbers of order $k = 6$, namely, the hexagonal numbers, we have the following.

Corollary 2.3: Let $p \in \mathbf{N} \setminus \{0\}$ be a prime number. If $p \equiv 1 \pmod 4$, then there exists exactly one representation of p as a difference of hexagonal numbers, while no such representation exists if $p \equiv 3 \pmod 4$.

Proof: By definition, the nth hexagonal number is equal to $T(2n-1)$. Thus, the problem of representing an integer as a hexagonal number difference is equivalent to finding a triangular number difference $T(m_1) - T(m_2)$, where both m_1 and m_2 are odd integers. For a prime p, the only

possible triangular representations are those of the form given in Case 2 Subcase 1; that is, if $p = 2^0(2n+1)$ for some $n \in \mathbf{N} \setminus \{0\}$, then $p = T(1+n) - T(n-1)$. Now, if $p \equiv 1 \pmod 4$, then clearly $2|n$, and so both $1+n$ and $n-1$ are odd integers. However, for $p \equiv 3 \pmod 4$, one must have $n = 2s+1$ for some $s \in \mathbf{N} \setminus \{0\}$, and so $1+n$ and $n-1$ are even integers. □

Clearly, in comparison with the triangular case, a larger subset of $\mathbf{Z} \setminus \{0\}$ fails to have a representation as a difference of hexagonal numbers. Consequently, in view of this, one might consider the following conjecture.

Conjecture 2.1: Denote the nth polygonal number of order k by $P_k(n)$ and consider the set $A_k = \{M \in \mathbf{Z} \setminus \{0\} : M = P_k(n_1) - P_k(n_2) \text{ for some } n_1, n_2 \in \mathbf{N}\}$. Does the set inclusion $A_{k+1} \subseteq A_k$ hold for all $k = 3, 4, \ldots$, and, if so, is $\bigcap_{k=3}^{\infty} A_k \neq \emptyset$?

REFERENCES

1. R. K. Guy. "Every Number Is Expressible as a Sum of How Many Polygonal Numbers?" *Amer. Math. Monthly* **101** (1994):169-72.
2. L. J. Mordell. *Diophantine Equations*. London, New York: Academic press, 1969.
3. M. Zafrullah & H. Lee. "A Note on Triangular Numbers." *Punjab University Journal of Mathematics* **26** (1993):75-83.

AMS Classification Numbers: 11B83, 11D85

❖❖❖

SUMMATION OF RECIPROCALS WHICH INVOLVE PRODUCTS OF TERMS FROM GENERALIZED FIBONACCI SEQUENCES–PART II

R. S. Melham
Department of Mathematical Sciences, University of Technology
Sydney, PO Box 123, Broadway, NSW 2007 Australia
(*Submitted May 1999*)

1. INTRODUCTION

We consider the sequence $\{W_n\}$ defined, for all integers n, by

$$W_n = pW_{n-1} + W_{n-2},\ W_0 = a, W_1 = b. \tag{1.1}$$

Here a, b, and p are real numbers with $p \neq 0$. Write $\Delta = p^2 + 4$. Then it is known [3] that

$$W_n = \frac{A\alpha^n - B\beta^n}{\alpha - \beta}, \tag{1.2}$$

where $\alpha = (p + \sqrt{\Delta})/2$, $\beta = (p - \sqrt{\Delta})/2$, $A = b - a\beta$, and $B = b - a\alpha$. As in [3], we will put $e_W = AB = b^2 - pab - a^2$.

We define a companion sequence $\{\overline{W}_n\}$ of $\{W_n\}$ by

$$\overline{W}_n = A\alpha^n + B\beta^n. \tag{1.3}$$

Aspects of this sequence have been treated, for example, in [2] and [4].

For $(W_0, W_1) = (0, 1)$, we write $\{W_n\} = \{U_n\}$ and, for $(W_0, W_1) = (2, p)$, we write $\{W_n\} = \{V_n\}$. The sequences $\{U_n\}$ and $\{V_n\}$ are generalizations of the Fibonacci and Lucas sequences, respectively. From (1.2) and (1.3) we see that $\overline{U}_n = V_n$ and $\overline{V}_n = \Delta U_n$. Thus, it is clear that $e_U = 1$ and $e_V = -\Delta = -(\alpha - \beta)^2$.

The purpose of this paper is to investigate the infinite sums

$$S_{k,m} = \sum_{n=1}^{\infty} \frac{\overline{W}_{k(n+m)}}{W_{kn}W_{k(n+m)}W_{k(n+2m)}}, \tag{1.4}$$

and

$$T_{k,m} = \sum_{n=1}^{\infty} \frac{1}{W_{kn}W_{k(n+m)}W_{k(n+2m)}W_{k(n+3m)}}, \tag{1.5}$$

where k and m are positive integers with k even. Indeed, $S_{k,m}$ and the alternating sum derived from $T_{k,m}$ have been studied in [5], where k and m were assumed to be odd positive integers. Both sums were expressed in terms of an infinite sum, and certain finite sums. Here, however, with the altered constraints on k and m, we express $S_{k,m}$ and $T_{k,m}$ in terms of finite sums only.

Now, if $p > 0$, then $\alpha > 1$ and $\alpha > |\beta|$, so that

$$W_n \cong \frac{A}{\alpha - \beta}\alpha^n \quad \text{and} \quad \overline{W}_n \cong A\alpha^n. \tag{1.6}$$

On the other hand, if $p < 0$, then $\beta < -1$ and $|\beta| > |\alpha|$, and so

$$W_n \cong \frac{-B}{\alpha-\beta}\beta^n \quad \text{and} \quad \overline{W}_n \cong B\beta^n. \tag{1.7}$$

Hence, assuming that a and b are chosen so that no denominator vanishes, we see from the ratio test that $S_{k,m}$ and $T_{k,m}$ are absolutely convergent.

2. PRELIMINARY RESULTS

We require the following, in which k and m are taken to be integers with k *even*.

$$\frac{\beta^{kn}}{W_{kn}} - \frac{\beta^{k(n+m)}}{W_{k(n+m)}} = \frac{AU_{km}}{W_{kn}W_{k(n+m)}}, \tag{2.1}$$

$$W_{k(n+m)}W_{k(n+2m)} - W_{kn}W_{k(n+3m)} = e_W U_{km} U_{2km}, \tag{2.2}$$

$$W_{n+k} - W_{n-k} = \overline{W}_n U_k, \tag{2.3}$$

$$B\beta^n = W_{n+1} - \alpha W_n. \tag{2.4}$$

Identities (2.1) and (2.2) are readily proved with the use of (1.2) and (1.3). Identity (2.3) is a special case of (75) in [2], while (2.4) can be obtained from (3.2) in [1].

We will also make use of the following lemma.

Lemma 1: Let k and m be positive integers with k even. Then

$$\sum_{n=1}^{\infty} \frac{1}{W_{kn}W_{k(n+m)}} = \frac{1}{e_W U_{km}}\left[\sum_{n=1}^{m} \frac{W_{kn+1}}{W_{kn}} - m\alpha\right]. \tag{2.5}$$

Proof: If we sum both sides of (2.1), we obtain

$$\sum_{n=1}^{\infty} \frac{1}{W_{kn}W_{k(n+m)}} = \frac{1}{AU_{km}} \sum_{n=1}^{m} \frac{\beta^{kn}}{W_{kn}},$$

and (2.5) follows from (2.4) and the fact that $e_W = AB$. □

In fact, under the hypotheses of Lemma 1, Theorem 2′ of [1] yields

$$\sum_{n=1}^{\infty} \frac{1}{W_{kn}W_{k(n+m)}} = \frac{1}{e_W U_k U_{km}}\left[\sum_{n=1}^{m} \frac{W_{k(n+1)}}{W_{kn}} - m\alpha^k\right]. \tag{2.6}$$

To see that (2.6) reduces to (2.5), we use the identities $\alpha^k = U_k\alpha + U_{k-1}$ and $W_{k(n+1)} = U_k W_{kn+1} + U_{k-1}W_{kn}$. From the first of these, which is easily proved by induction, we obtain the second if we first note that $\alpha^{kn+k} = U_k\alpha^{kn+1} + U_{k-1}\alpha^{kn}$, and write down the corresponding result involving β.

3. THE MAIN RESULTS

Our main results can now be given in two theorems.

Theorem 1: Let k and m be positive integers with k even. Then

$$S_{k,m} = \frac{1}{U_{km}} \sum_{n=1}^{m} \frac{1}{W_{kn}W_{k(n+m)}}. \tag{3.1}$$

Proof: Consider the expression

$$\frac{\beta^{kn}}{W_{kn}}-\frac{\beta^{k(n+m)}}{W_{k(n+m)}}+\frac{\beta^{k(n+2m)}}{W_{k(n+2m)}}. \tag{3.2}$$

Using (2.1), we can write this as

$$\frac{AU_{km}}{W_{kn}W_{k(n+m)}}+\frac{\beta^{k(n+2m)}}{W_{k(n+2m)}} \tag{3.3}$$

or as

$$\frac{\beta^{kn}}{W_{kn}}-\left[\frac{\beta^{k(n+m)}}{W_{k(n+m)}}-\frac{\beta^{k(n+2m)}}{W_{k(n+2m)}}\right]=\frac{\beta^{kn}}{W_{kn}}-\frac{AU_{km}}{W_{k(n+m)}W_{k(n+2m)}}. \tag{3.4}$$

Now

$$\begin{aligned}\frac{AU_{km}}{W_{kn}W_{k(n+m)}}-\frac{AU_{km}}{W_{k(n+m)}W_{k(n+2m)}}&=\frac{AU_{km}}{W_{k(n+m)}}\left[\frac{1}{W_{kn}}-\frac{1}{W_{k(n+2m)}}\right]\\&=\frac{AU_{km}}{W_{k(n+m)}}\left[\frac{W_{k(n+2m)}-W_{kn}}{W_{kn}W_{k(n+2m)}}\right]\\&=\frac{AU_{km}^2\overline{W}_{k(n+m)}}{W_{kn}W_{k(n+m)}W_{k(n+2m)}},\quad\text{by (2.3).}\end{aligned} \tag{3.5}$$

But from (3.2)-(3.4), we then have

$$2\left[\frac{\beta^{kn}}{W_{kn}}-\frac{\beta^{k(n+m)}}{W_{k(n+m)}}+\frac{\beta^{k(n+2m)}}{W_{k(n+2m)}}\right]=\frac{\beta^{kn}}{W_{kn}}+\frac{\beta^{k(n+2m)}}{W_{k(n+2m)}}+\frac{AU_{km}^2\overline{W}_{k(n+m)}}{W_{kn}W_{k(n+m)}W_{k(n+2m)}},$$

so that

$$\frac{AU_{km}^2\overline{W}_{k(n+m)}}{W_{kn}W_{k(n+m)}W_{k(n+2m)}}=\left[\frac{\beta^{kn}}{W_{kn}}-\frac{\beta^{k(n+m)}}{W_{k(n+m)}}\right]-\left[\frac{\beta^{k(n+m)}}{W_{k(n+m)}}-\frac{\beta^{k(n+2m)}}{W_{k(n+2m)}}\right]. \tag{3.6}$$

Finally, summing both sides of (3.6), we obtain

$$AU_{km}^2S_{k,m}=\sum_{n=1}^{m}\frac{\beta^{kn}}{W_{kn}}-\sum_{n=1}^{m}\frac{\beta^{k(n+m)}}{W_{k(n+m)}},$$

and (3.1) follows from (2.1). □

If we put $W_n=F_n$ and $W_n=L_n$, and take $k=2$ and $m=1$, (3.1) becomes, respectively,

$$\sum_{n=1}^{\infty}\frac{L_{2n+2}}{F_{2n}F_{2n+2}F_{2n+4}}=\frac{1}{3}, \tag{3.7}$$

and

$$\sum_{n=1}^{\infty}\frac{F_{2n+2}}{L_{2n}L_{2n+2}L_{2n+4}}=\frac{1}{105}. \tag{3.8}$$

Theorem 2: Let k and m be positive integers with k even. Then

$$e_WU_{km}U_{2km}T_{k,m}=\frac{1}{e_W}\left[\frac{1}{U_{3km}}\sum_{n=1}^{3m}\frac{W_{kn+1}}{W_{kn}}-\frac{1}{U_{km}}\sum_{n=1}^{m}\frac{W_{kn+1}}{W_{kn}}\right]+\sum_{n=1}^{m}\frac{1}{W_{kn}W_{k(n+m)}}+\frac{m\alpha}{e_W}\left[\frac{1}{U_{km}}-\frac{3}{U_{3km}}\right]. \tag{3.9}$$

Proof: From (2.2), we see that

$$\frac{e_W U_{km} U_{2km}}{W_{kn} W_{k(n+m)} W_{k(n+2m)} W_{k(n+3m)}} = \frac{1}{W_{kn} W_{k(n+3m)}} - \frac{1}{W_{k(n+m)} W_{k(n+2m)}}.$$

Summing both sides we obtain, with the aid of (2.5),

$$e_W U_{km} U_{2km} T_{k,m} = \frac{1}{e_W U_{3km}} \left[\sum_{n=1}^{3m} \frac{W_{kn+1}}{W_{kn}} - 3m\alpha \right] - \left[\frac{1}{e_W U_{km}} \left[\sum_{n=1}^{m} \frac{W_{kn+1}}{W_{kn}} - m\alpha \right] - \sum_{n=1}^{m} \frac{1}{W_{kn} W_{k(n+m)}} \right],$$

which is (3.9). □

If we put $W_n = F_n$ and $W_n = L_n$, and take $k = 2$ and $m = 1$, (3.9) becomes, respectively,

$$\sum_{n=1}^{\infty} \frac{1}{F_{2n} F_{2n+2} F_{2n+4} F_{2n+6}} = \frac{60\sqrt{5} - 133}{576}, \tag{3.10}$$

and

$$\sum_{n=1}^{\infty} \frac{1}{L_{2n} L_{2n+2} L_{2n+4} L_{2n+6}} = \frac{9\sqrt{5} - 20}{2160}. \tag{3.11}$$

REFERENCES

1. R. André-Jeannin. "Summation of Reciprocals in Certain Second-Order Recurring Sequences." *The Fibonacci Quarterly* **35.1** (1997):68-74.
2. G. E. Bergum & V. E. Hoggatt, Jr. "Sums and Products for Recurring Sequences." *The Fibonacci Quarterly* **13.2** (1975):115-20.
3. A. F. Horadam. "Basic Properties of a Certain Generalized Sequence of Numbers." *The Fibonacci Quarterly* **3.3** (1965):161-76.
4. C. T. Long. "Some Binomial Fibonacci Identities." In *Applications of Fibonacci Numbers* **3:** 241-54. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1990.
5. R. S. Melham. "Summation of Reciprocals Which Involve Products of Terms from Generalized Fibonacci Sequences." *The Fibonacci Quarterly* **38.4** (2000):294-98.

AMS Classification Numbers: 11B39, 11B37, 40A99

❖❖❖

THE FILBERT MATRIX

Thomas M. Richardson
Department of Mathematics and Statistics, Western Michigan University, Kalamazoo, MI 49008
e-mail: ribby@alumni.umich.edu
(*Submitted May 1999*)

1. INTRODUCTION

The $n \times n$ Hilbert matrix is the $n \times n$ matrix whose (i, j)-entry is $\frac{1}{i+j-1}$. In [1], Man-Duen Choi explores many fascinating properties of the Hilbert matrix, including the fact that the (i, j)-entry of its inverse is

$$\alpha_{ij} = (-1)^{i+j}(i+j-1)\binom{n+i-1}{n-j}\binom{n+j-1}{n-i}\binom{i+j-2}{i-1}^2. \tag{1}$$

Choi asks what sort of coincidence it is if the inverse of a matrix of reciprocals of integers has integer entries. In this paper we show that the inverses of the Hankel matrices based on the reciprocals of the Fibonacci numbers, the reciprocals of the binomial coefficients $\binom{i+j}{2}$, and the reciprocals of the binomial coefficients $\binom{i+j+2}{3}$ all have integer entries. We also find formulas for the entries of the inverses of these matrices and related matrices.

Definition 1.1: Let $\{a_k\}$ be an integer sequence with $a_k \neq 0$ for $k \geq 1$. A *reciprocal Hankel matrix* based on $\{a_k\}$ is a matrix whose (i, j)-entry is $1/a_{i+j-1}$. We denote the $n \times n$ reciprocal Hankel matrix based on $\{a_k\}$ by $R_n(a_k)$.

The formula for the entries of the inverse of $R_n(F_k)$ bears a striking resemblance to the formula for the entries of the inverse of the Hilbert matrix. Therefore, we call a reciprocal Hankel matrix based on the Fibonacci numbers a *Filbert matrix*.

2. FILBERT MATRICES

We need the Fibonomial coefficients to describe the inverse of the Filbert matrix. See [2] for more information on the Fibonomial coefficients.

Definition 2.1: The *Fibonomial coefficients* are

$$\left(\!\binom{n}{k}\!\right) = \prod_{i=1}^{k} \frac{F_{n-i+1}}{F_i},$$

where n and k are nonnegative integers.

Theorem 2.1: Let $e(n, i, j) = n(i+j+1) + \binom{i}{2} + \binom{j}{2} + 1$, and let $W(n)$ be the $n \times n$ matrix whose (i, j)-entry is

$$W_{ij}(n) = (-1)^{e(n,i,j)} F_{i+j-1} \left(\!\binom{n+i-1}{n-j}\!\right)\left(\!\binom{n+j-1}{n-i}\!\right)\left(\!\binom{i+j-2}{i-1}\!\right)^2.$$

Then the $n \times n$ matrix $W(n)$ is the inverse of the Filbert matrix $R_n(F_k)$, and $W(n)$ is an integer matrix.

This theorem is a special case of Theorem 2.2, which we prove below. The formula for the entries of the inverse closely corresponds to the formula for the entries of the inverse of the $n \times n$ Hilbert matrix. It results from (1) by changing all binomial coefficients to Fibonomial coefficients and changing the exponent of -1. The pattern of the signs of entries the inverse of $R_n(F_k)$ is that they are constant on 2×2 blocks, and alternate between blocks.

The Fibonacci polynomials $f_n(x)$ are defined by $f_0(x) = 0$, $f_1(x) = 1$, $f_n(x) = xf_{n-1}(x) + f_{n-2}(x)$ for $n \geq 2$. We also use f_n to denote the Fibonacci polynomial $f_n(x)$, especially when we want to reduce the clutter in some equations. The x-Fibonomial coefficients are the obvious generalization of the Fibonomial coefficients.

Definition 2.2: The *x-Fibonomial coefficients* are

$$\left(\!\binom{n}{k}\!\right)_x = \prod_{i=1}^{k} \frac{f_{n-i+1}(x)}{f_i(x)},$$

where n and k are nonnegative integers.

To form the (i, j)-entry of the inverse of $R_n(f_k(x))$, replace each Fibonacci number and Fibonomial coefficient in $W_{ij}(n)$ with the corresponding Fibonacci polynomial and x-Fibonomial coefficient.

Theorem 2.2: Let $V(n)$ be the $n \times n$ matrix whose (i, j)-entry is

$$V_{ij}(n) = (-1)^{e(n,i,j)} f_{i+j-1} \left(\!\binom{n+i-1}{n-j}\!\right)_x \left(\!\binom{n+j-1}{n-i}\!\right)_x \left(\!\binom{i+j-2}{i-1}\!\right)_x^2.$$

Then the $n \times n$ matrix $V(n)$ is the inverse of the Filbert matrix $R_n(f_k(x))$, and the entries of $V(n)$ are integer polynomials.

The recurrence

$$\left(\!\binom{n}{k}\!\right)_x = f_{k-1}(x)\left(\!\binom{n-1}{k}\!\right)_x + f_{n-k+1}(x)\left(\!\binom{n-1}{k-1}\!\right)_x$$

shows that the Fibonomial coefficients are integer polynomials, which implies that the entries of $V(n)$ are integer polynomials.

3. TECHNOLOGY

The proof of Theorem 2.2 and proofs of succeeding theorems amount to proving various identities involving sums of products of Fibonomial coefficients and binomial coefficients. We supply computer proofs of these identities. In some cases, the computer cannot do the entire proof directly, and human intervention is required to separate the proof into smaller pieces that can be done by computer.

The program and packages used to produce the proofs for this paper include Maple V Release 5, the Maple package EKHAD written by Doron Zeilberger, and the Mathematica package `MultiSum` written by Kurt Wegschaider. EKHAD is described in [3] and is available through the web site www.math.temple.edu/~zeilberg. `MultiSum` is described in [4] and is available through the web site www.risc.uni-linz.ac.at/software/. The particular functions that we use from these packages are `zeil` from EKHAD and `FindRecurrence` from `MultiSum`.

Both of these functions find a telescoped recurrence for a summand $F(n,k)$, where k is the summation variable. The function `zeil` uses Zeilberger's algorithm to find a rational function $R(n,k)$ and a recurrence operator $P(n,N)$, where N is the shift operator in n such that

$$P(n,N)(F(n,k)) = R(n,k+1)F(n,k+1) - R(n,k)F(n,k). \tag{2}$$

Let $f(n)$ be the unrestricted sum $\sum_k F(n,k)$. In many situations, equation (2) implies that $P(n,N)f(n) = 0$, making it easy to verify that $f(n)$ is constant.

The function `FindRecurrence` gives similar results with summands of the form $F(\mathbf{n},\mathbf{k})$, where $\mathbf{n}$ and $\mathbf{k}$ are vectors.

Maple V Release 5 also includes an implementation of Zeilberger's algorithm as the function `sumrecursion` of the package `sumtools`. However, `sumrecursion` only gives the recurrence operator $P(n,N)$, and not the rational function $R(n,k)$, which will be essential when we prove identities involving a restricted sum.

The sums involved in the proof of Theorem 2.2 are of products of Fibonomials not binomials, so these procedures do not apply. However, we obtained recurrences for sums of products of Fibonomials by modifying recurrences found by these procedures for the corresponding sums of products of binomials.

4. PROOF OF THEOREM 2.2

The (i,m)-entry of the product $V(n)R_n(f_k(x))$ is $p(n,i,m) = \sum_{j=1}^{n} P(n,i,m,j)$, where

$$P(n,i,m,j) = (-1)^{e(n,i,j)} \frac{f_{i+j-1}}{f_{j+m-1}} \left(\binom{n+i-1}{n-j}\right)_x \left(\binom{n+j-1}{n-i}\right)_x \left(\binom{i+j-2}{i-1}\right)_x^2.$$

The summand satisfies the following recurrence relation that is related to a recurrence produced by `FindRecurrence` for an entry of the product of the Hilbert matrix and its inverse.

Lemma 4.1: The summand $P(n,i,m,j)$ satisfies the recurrence relation

$$\begin{aligned} &-f_{n-i+1}f_{n+i-2}(P(n,i-1,m,j) - P(n-1,i-1,m,j)) \\ &\quad + (-1)^{n+i} f_{i-1}^2 (P(n,i,m,j) - P(n-1,i,m,j)) = 0, \end{aligned} \tag{3}$$

and the sum $p(n,i,m)$ satisfies the recurrence relation

$$\begin{aligned} &-f_{n-i+1}f_{n+i-2}(p(n,i-1,m) - p(n-1,i-1,m)) \\ &\quad + (-1)^{n+i} f_{i-1}^2 (p(n,i,m) - p(n-1,i,m)) = 0. \end{aligned} \tag{4}$$

Proof: Write each of the terms in (3) as a multiple of $P(n-1,i-1,m,j)$ to get the equation

$$\begin{aligned} &-f_{n-i+1}f_{n+i-2}(P(n,i-1,m,j) - P(n-1,i-1,m,j)) \\ &\quad + (-1)^{n+i} f_{i-1}^2 (P(n,i,m,j) - P(n-1,i,m,j)) \\ &\quad = \frac{f_{n+i-2}}{f_{n-i+1}f_{n-j}f_{i+j-1}} M(n,i,j) P(n-1,i-1,m,j), \end{aligned} \tag{5}$$

where

$$\begin{aligned} M(n,i,j) &= (-1)^{i+j} f_{n+i-1}f_{n+j-1}f_{i+j-2} + f_{n-i}f_{n-j}f_{i+j-2} \\ &\quad + (-1)^{i+j-1} f_{n+i-2}f_{n+j-1}f_{i+j-1} + f_{n-i+1}f_{n-j}f_{i+j-1}. \end{aligned} \tag{6}$$

It suffices to show that $M(n,i,j)=0$. But this follows from the standard Fibonacci identities $f_{n-i}f_{i+j-2}+f_{n-i+1}f_{i+j-1}=f_{n+j-1}$ and $f_{n+i-2}f_{i+j-1}-f_{n+i-1}f_{i+j-2}=(-1)^{i+j-2}f_{n-j}$. □

If we can establish $p(n,1,1)=1$, $p(n,1,m)=0$ if $m\neq 1$, and $p(n,n,n)=1$, then (4) shows that $p(n,i,m)=1$ if $i=m$ and $p(n,i,m)=0$ if $i\neq m$, for $1\le i,m\le n$.

Case $p(n,1,m)$. The summand $P(n,1,m,j)$ satisfies the recurrence

$$\begin{aligned}(-1)^{m+1}f_{n-1}f_{n+m-2}P(n,1,m-1,j)-f_nf_{n-m+1}P(n-1,1,m-1,j)\\ +(-1)^m f_{n-1}f_{n+m-1}P(n,1,m,j)+f_nf_{n-m}P(n-1,i,m,j)=0,\end{aligned}\tag{7}$$

and this implies a similar recurrence for $p(n,1,m)$. The proof of (7) is similar to the proof of Lemma 4.1. The initial values of this recurrence are $p(m,1,m)$ and $p(n,1,1)$. The summand $P(m,1,m,j)$ satisfies the recurrence

$$(-1)^m f_m f_{m-1}P(m,1,m,j)=G_1(m,j+1)-G_1(m,j)$$

where $G_1(m,j)=(-1)^{j-1}f_jf_{j-1}P(m,1,m,j)$. Since the support of G_1 is $2\le j\le m$, this equation implies that $(-1)^m f_m f_{m-1}p(m,1,m)=0$. Therefore, when $m>1$ we get $p(m,1,m)=0$. Finally, the summand $P(n,1,1,j)$ satisfies

$$(-1)^n f_n^2 P(n,1,1,j)=G_2(n,j+1)-G_2(n,j),$$

where $G_2(n,j)=(-1)^{j-1}f_j^2P(n,1,1,j)$. In this case, the support of G_2 is $1\le j\le n$, so summing over j from 1 to n gives $(-1)^n f_n^2 p(n,1,1)=-G_2(n,1)=(-1)^n f_n^2$, implying $p(n,1,1)=1$.

Case $p(n,n,n)$. The summand $P(n,n,n,j)$ satisfies the recurrence

$$P(n+1,n+1,n+1,j)-P(n,n,n,j)=G_3(n,j+1)-G_3(n,j),$$

where

$$G_3(n,j)=(-1)^{e(n,n,j)}\left(\frac{f_{3n+j-1}}{f_{n+j-1}}+2(-1)^n\right)\left(\binom{2n-1}{n-j+1}\right)_x\left(\binom{n+j-2}{j-2}\right)_x^2.$$

When we sum over j, the right-hand side telescopes to 0 and the left-hand side is $p(n+1,n+1,n+1)-p(n,n,n)$. This completes the proof of Theorem 2.2.

5. RECIPROCAL HANKEL MATRICES BASED ON BINOMIAL COEFFICIENTS

In this section we will prove that certain reciprocal matrices based on binomial coefficients have integer entries. We will give formulas for the entries of the inverses of these matrices.

Let $a_k=\binom{k+1}{2}$.

Theorem 5.1: Let $A(n)$ be the $n\times n$ matrix whose (i,j)-entry is

$$A_{ij}(n)=\sum_{k=0}^{j-1}(-1)^{i+k+1}\binom{n+i}{n-k}\binom{n+k}{n-i}\binom{i+k-1}{k}\binom{i+k}{k}\frac{i}{2}.$$

Then $A_{ij}(n)$ is an integer, and $A(n)$ is the inverse of the matrix $R_n(a_k)$.

Proof: First, we show that $A_{ij}(n)$ is an integer. We use the well-known fact that, if a is even and b is odd, then $\binom{a}{b}$ is even. If i is even, then obviously $A_{ij}(n)$ is an integer, so assume that i is odd. Now, if k is also odd, then $\binom{i+k}{k}$ is even, so we may assume that k is even. Now, one of $\binom{n+i}{i+k}$ and $\binom{n+k}{i+k}$ is even.

Theorem 5.2 below shows that $A(n)$ is the inverse of the matrix $R_n(a_k)$. □

Let $b_k = b_k(r)$ be the binomial coefficient $\binom{k+r-1}{r}$. Suppose that r is a positive integer and $r \geq 3$. Then the inverse of $R_n(b_k(r))$ does not always have integer entries, but the values of n for which the inverse does have integer entries seem to occur periodically. Further, when the entries are not integers, the denominators are divisors of r. The following conjecture is true for $n \leq 20$, $r \leq 10$, and r an integer.

Conjecture 5.1: Suppose that r is a positive integer. The inverse of the matrix $R_n(b_k(r))$ has integer entries if and only if $n \equiv 0 \pmod{q}$ or $n \equiv 1 \pmod{q}$ for all prime powers q that divide r.

We do have an explicit formula for the entries of the inverse.

Theorem 5.2: Let $B(n,r)$ be the $n \times n$ matrix whose (i,j)-entry is

$$B_{ij}(n,r) = \sum_{k=0}^{j-1} (-1)^{i+k+1} \binom{n+i+r-2}{i} \binom{n}{i} \binom{n+k+r-2}{k} \binom{n}{k} \frac{i^2 \prod_{l=0}^{r-3} i+j+l}{r \prod_{l=0}^{r-2} i+k+l}.$$

Then $B(n,r)$ is the inverse of the matrix $R_n(b_k)$.

The theorem is valid if r is an indeterminate, not just if it is a positive integer. Also note that $B_{ij}(n,1)$ simplifies to α_{ij}, the (i,j)-entry of the inverse of the Hilbert matrix, and $B_{ij}(n,2)$ is equal to $A_{ij}(n)$.

Proof: Let

$$\begin{aligned} H(n,i,m,j,k) &= (-1)^{i+k+1} \binom{n+i+r-2}{i} \binom{n}{i} \\ &\quad \times \binom{n+k+r-2}{k} \binom{n}{k} \frac{i^2 \prod_{l=0}^{r-3} i+j+l}{r \prod_{l=0}^{r-2} i+k+l} \frac{1}{\binom{j+m+r-2}{r}}, \end{aligned}$$

so that $h(n,i,m) = \sum_{j=1}^{n} \sum_{k=0}^{j-1} H(n,i,m,j,k)$ is the (i,m)-entry of $B(n,r)R_n(b_k)$. Then H satisfies the recurrence

$$\begin{aligned} & n^2(i-m+r-1)(n-i+r-1)(n+i+r-3)H(n-1,i-1,m-1,j,k) \\ & -n^2(i-m-1)(n-i+r-1)(n+i+r-3)H(n-1,i-1,m,j,k) \\ & +n^2(i-1)^2(i-m+1)H(n-1,i,m-1,j,k) \\ & -n^2(i-1)^2(i-m-r+1)H(n-1,i,m,j,k) \\ & -(n+r-2)^2(i-m+r-1)(n-i+1)(n+i-1)H(n,i-1,m-1,j,k) \\ & +(n+r-2)^2(i-m-1)(n-i+1)(n+i-1)H(n,i-1,m,j,k) \\ & -(n+r-2)^2(i-1)^2(i-m+1)H(n,i,m-1,j,k) \\ & +(n+r-2)^2(i-1)^2(i-m-r+1)H(n,i,m,j,k) = 0. \end{aligned} \tag{8}$$

The preceding recurrence was found by `FindRecurrence`. The theorem will follow if we can establish the correct values of $h(n,1,m)$, $h(n,n,n)$, and $h(n,i,1)$.

Case $h(n,1,m)$. Maple computes $h(n,1,1)=1$, and it computes

$$H_1(n,1,m,j)=\sum_{k=0}^{j-1}H(n,1,m,j,k)=\frac{(-1)^{j+1}j\binom{n+j+r-2}{j}\binom{n}{j}}{r\binom{j+m+r-2}{r}}.$$

Now $h(n,1,m)=\sum_j H_1(n,1,m,j)$, and with $H_1(n,1,m,j)$ as input, the function `sumrecursion` gives the recurrence $(n-1)(n-2+m+r)h(n,1,m)-(n+r-1)(n-m)h(n-1,1,m)=0$, and Maple gives the initial value $h(m,1,m)=0$ for $m>1$.

Case $h(n,n,n)$. Maple computes

$$H_1(n,n,n,j)=\sum_{k=0}^{j-1}H(n,n,n,j,k)=\frac{(-1)^{n+j}j\binom{2n+r+2}{n}\binom{n+j+r-3}{j-1}\binom{n}{j}}{r\binom{n+j+r-2}{r}}.$$

Similarly to the previous case, `sumrecursion` gives the recurrence $h(n,n,n)-(n-1,n-1,n-1)=0$ and, obviously, $h(1,1,1)=1$.

Case $h(n,i,1)$. We need to do something different in this case. First, we show that our conjectured inverse is symmetric. Let

$$S(n,i,j,k)=(-1)^{i+k+1}\binom{n+i+r-2}{i}\binom{n}{i}\binom{n+k+r-2}{k}\binom{n}{k}\frac{i^2\prod_{l=0}^{r-3}i+j+l}{r\prod_{l=0}^{r-2}i+k+l},$$

so that $B_{ij}(n,r)=\sum_{k=0}^{j-1}S(n,i,j,k)$. Now `zeil` produces the recurrence

$$S(n+1,i,j,k)-S(n,i,j,k)=T(n,i,j,k+1)-T(n,i,j,k)$$

where

$$T(n,i,j,k)=\frac{-(2n+r)k^2(i+k+r-2)}{(n+r-1)^2(n-i+1)(n-k+1)}S(n,i,j,k).$$

This implies that $B_{ij}(n+1,r)-B_{ij}(n,r)=T(n,i,j,j)-T(n,i,j,0)$. Now Maple tells us that

$$T(n,i,j,j)-T(n,i,j,0)-T(n,j,i,i)+T(n,j,i,0)=0,$$

which means that $B_{ij}(n+1,r)-B_{ji}(n+1,r)=B_{ij}(n,r)-B_{ji}(n,r)$. Maple also tells us that

$$B_{in}(n,r)-B_{ni}(n,r)=\frac{\binom{n+i+r-2}{i}i(n+i+r-3)!\Gamma(2-r)\Gamma(2-n-i-r)(-1)^i}{r(n+i-1)!(i+r-2)!\Gamma(2-n-r)\Gamma(2-i-r)\Gamma(1-i)},$$

which implies $B_{in}(n,r)-B_{ni}(n,r)=0$.

Since $R_n(b_k)$ and $B(n,r)$ are symmetric, the $(1,i)$-entry of $R_n(b_k)B(n,r)$ equals the $(i,1)$-entry of $B(n,r)R_n(b_k)$. The former is $\sum_{j=1}^{n}\sum_{k=1}^{i-1}U(n,i,j,k)$, where

$$U(n,i,j,k)=\binom{j+r-1}{r}^{-1}S(n,j,i,k).$$

The function `zeil` produces

$$Y(n,i,j,k)=\frac{-(2n+r)k^2(j+k+r-2)}{(n+r-1)^2(n-j+1)(n-k+1)}U(n,i,j,k)$$

which satisfies

$$U(n+1,i,j,k)-U(n,i,j,k)=Y(n,i,j,k+1)-Y(n,i,j,k).$$

Then we have

$$\sum_{k=1}^{i-1}U(n+1,i,j,k)-\sum_{k=1}^{i-1}U(n,i,j,k)=Y(n,i,j,i)-Y(n,i,j,0),$$

and Maple tells us that $\sum_{j=1}^{n}Y(n,i,j,i)-Y(n,i,j,0)=0$. All that remains is to check the initial value $\sum_{j=1}^{i}\sum_{k=1}^{i-1}U(i,i,j,k)=0$. Maple also tells us that

$$\sum_{j=1}^{i}\sum_{k=1}^{i-1}U(i,i,j,k)=\frac{\Gamma(1-r)\Gamma(2i-r)\Gamma(2i+r+1)\Gamma(2i+r-1)}{\Gamma(-r-1)^2\Gamma(i+r+1)^2\Gamma(i+r)}\frac{(-1)^i}{(i-1)\Gamma(-i)},$$

which implies that $\sum_{j=1}^{i}\sum_{k=1}^{i-1}U(i,i,j,k)=0$ when $i>1$. □

We consider reciprocal Hankel matrices based on one more sequence of binomial coefficients. Let $c_k=\binom{k+3}{3}$.

Theorem 5.3: Let $C(n)$ be the $n\times n$ matrix whose (i,j)-entry is

$$C_{ij}(n)=\sum_{k=0}^{j-1}(-1)^{i+k+1}\binom{n+i+2}{i+k+1}\binom{n+k+1}{i+k+1}\binom{i+k+1}{i}\binom{i+k}{i}\frac{i(j-k)}{3}.$$

Then $C_{ij}(n)$ is an integer, and $C(n)$ is the inverse of the matrix $R_n(c_k)$.

Proof: First, we show that each summand of the sum that defines each entry is an integer. It is well known that, if $a\equiv 0 \pmod 3$, $b\equiv 1 \pmod 3$, and $c\equiv 2 \pmod 3$, then $\binom{a}{b}$, $\binom{a}{c}$, and $\binom{b}{c}$ are all divisible by 3. Using this fact, we find that one of the terms $\binom{i+k+1}{i}$, $\binom{i+k}{i}$, or i is divisible by 3 unless $i\equiv 1 \pmod 3$ and $k\equiv 0 \pmod 3$. But now $n+i+2\equiv n \pmod 3$, $n+k+1\equiv n+1 \pmod 3$, and $i+k+1\equiv 2 \pmod 3$. Thus, 3 divides one of the terms $\binom{n+i+2}{i+k+1}$ or $\binom{n+k+1}{i+k+1}$.

The proof that $C(n)$ is the inverse of $R_n(c_k)$ is similar to the proof of Theorem 5.2. Let

$$Z(n,i,m,j,k)=(-1)^{i+k+1}\binom{n+i+2}{i+k+1}\binom{n+k+1}{i+k+1}\binom{i+k+1}{i}\binom{i+k}{i}\frac{i(j-k)}{3\binom{j+m+2}{3}},$$

so that $z(n,i,m)=\sum_{j=1}^{n}\sum_{k=0}^{j-1}Z(n,i,m,j,k)$ is the (i,m)-entry of $C(n)R_n(c_k)$. Then Z satisfies the recurrence

$$\begin{aligned}(n-i+1)(n+i+1)(Z(n-1,i-1,m,j,k)-Z(n,i-1,m,j,k))\\ +i(i-1)(Z(n-1,i,m,j,k)-Z(n,i,m,j,k))=0.\end{aligned}$$

Now the proof proceeds similarly to the proof of Theorem 5.2, except that we do not have to do the difficult initial value $m=1$. □

One might wonder whether there is not a simpler formula than the one we give for $B_{ij}(n,r)$. If we fix i and j and consider B_{ij} as a polynomial of n, then it usually has an irreducible factor of

degree $\min\{2i-2, 2j-2\}$. Thus, it seems unlikely that one could avoid the sum in the given formula. The next section suggests that the given sum is the "right" way to describe $B_{ij}(n,r)$.

6. RECIPROCAL HANKEL MATRICES BASED ON FIBONOMIAL COEFFICIENTS

Remarkably, by changing the exponent of -1 and changing the binomial coefficients to Fibonomial coefficients in the formula for B_{ij}, we get a formula for the entries of the inverses of reciprocal Hankel matrices based on Fibonomial coefficients.

Let $d_k = d_k(r)$ be the Fibonomial coefficient $\left(\!\binom{k+r-1}{r}\!\right)$.

Conjecture 6.1: Let $D(n,r)$ be the $n \times n$ matrix whose (i,j)-entry is

$$D_{ij} = D_{ij}(n,r) = \sum_{k=0}^{j-1} (-1)^{e(n,i,k)} \left(\!\binom{n+i+r-2}{i}\!\right)\left(\!\binom{n}{i}\!\right) \times \left(\!\binom{n+k+r-2}{k}\!\right)\left(\!\binom{n}{k}\!\right) \frac{F_i^2 \prod_{l=0}^{r-3} F_{i+j+l}}{F_r \prod_{l=0}^{r-2} F_{i+k+l}}.$$

Then the $D(n,r)$ is the inverse of the matrix $R_n(d_k)$.

We have verified this conjecture for $n \le 16$ and $r \le 10$. (We assume that r is a positive integer.) We also observe that the inverse of a reciprocal Hankel matrix based on Fibonomial coefficients has integer entries exactly when the corresponding reciprocal Hankel matrix based on binomial coefficients has integer entries. This may just be a consequence of known divisibility properties of the Fibonomials. It seems likely that this conjecture may be proved by combining the methods of the proofs of Theorem 2.2 and Theorem 5.2, and that it may be extended to the corresponding sequence of x-Fibonomial coefficients.

REFERENCES

1. Man-Duen Choi. "Tricks or Treats with the Hilbert Matrix." *American Math. Monthly* **90** (1983):301-12.
2. Donald Knuth. *The Art of Computer Programming*. 2nd ed., Vol. 1. New York: Addison-Wesley, 1973.
3. Marko Petkovšek, Herbert S. Wilf, & Doron Zeilberger. $A = B$. London: A. K. Peters, 1996.
4. Kurt Wegschaider. "Computer Generated Proofs of Binomial Multisum Identities." Diploma Thesis, Johannes Kepler Universität, Linz, 1997.

AMS Classification Numbers: 11B39, 11B65, 15A09

ALGORITHMIC DETERMINATION OF THE ENUMERATOR FOR SUMS OF THREE TRIANGULAR NUMBERS

John A. Ewell
Department of Mathematical Sciences, Northern Illinois University, DeKalb, IL 60115
(*Submitted May 1999-Final Revision October 1999*)

1. INTRODUCTION

In order to lend greater precision to statements of results and methods of proof, we begin our discussion with a definition.

Definition 1.1: As usual, $\mathbb{P} := \{1, 2, 3, \ldots\}$, $\mathbb{N} := \mathbb{P} \cup \{0\}$, and $\mathbb{Z} := \{0, \pm 1, \pm 2, \ldots\}$. Then, for each $n \in \mathbb{N}$,

$$t_3(n) := \left| \left\{ (h, j, k) \in \mathbb{N}^3 \,|\, n = \frac{h(h+1)}{2} + \frac{j(j+1)}{2} + \frac{k(k+1)}{2} \right\} \right|;$$

and $q(n) :=$ the number of partitions of n into distinct parts. We define $q(0) := 1$ and $q(n) := 0$ for $n < 0$. The function $q(n)$, $n \in \mathbb{N}$, is generated by the infinite product expansion

$$\prod_1^\infty (1 + x^n) = \sum_0^\infty q(n) x^n,$$

which is valid for each complex number x such that $|x| < 1$.

As so many arithmetical discussions do, our discussion begins with Gauss, who first proved the following theorem. (The result was conjectured by Fermat about 150 years earlier.)

Theorem 1.2: Every natural number can be represented by a sum of three triangular numbers, i.e., for each $n \in \mathbb{N}$, $t_3(n) > 0$.

In this paper our major objective is to give an algorithmic procedure for computing $t_3(n)$, $n \in \mathbb{N}$. This is accomplished by the following two results.

Theorem 1.3: For each $n \in \mathbb{N}$,

$$q(n) + 2 \sum_{k \in \mathbb{P}} (-1)^k q(n - k^2) = \begin{cases} (-1)^m, & \text{if } n = m(3m \pm 1)/2, \\ 0, & \text{otherwise.} \end{cases} \tag{1.1}$$

Theorem 1.4: For each $n \in \mathbb{N}$,

$$t_3(n) = q(n) - \sum_{k \in \mathbb{P}} (-1)^k q(n - 3k^2 + 2k)(3k - 1) + \sum_{k \in \mathbb{P}} (-1)^k q(n - 3k^2 - 2k)(3k + 1). \tag{1.2}$$

For a proof of Theorem 1.3, see [1, pp. 1-2]. Section 2 is dedicated to the proof of Theorem 1.4.

2. PROOFS

In our development we require the following three identities:

$$\prod_1^\infty (1 + x^n)(1 - x^{2n-1}) = 1; \tag{2.1}$$

$$\prod_{1}^{\infty}\frac{1-x^{2n}}{1-x^{2n-1}}=\sum_{0}^{\infty}x^{n(n+1)/2}\,; \tag{2.2}$$

$$\prod_{1}^{\infty}\frac{(1-x^{2n})(1-a^{2}x^{2n-2})(1-a^{-2}x^{2n})}{(1+ax^{2n-1})(1+a^{-1}x^{2n-1})}=\sum_{-\infty}^{\infty}x^{n(3n+2)}(a^{-3n}-a^{3n+2}). \tag{2.3}$$

Identities (2.1) and (2.2) are valid for all complex numbers x such that $|x|<1$, while (2.3) is valid for each pair of complex numbers a, x such that $a\neq 0$ and $|x|<1$. For proofs of (2.1) and (2.2), see [2, pp. 277-84]; for a proof of (2.3), see [3, pp. 23-27]. In passing, we observe that the cube of the right-hand side of (2.2) generates the sequence $t_3(n)$, $n\in\mathbb{N}$. Proof of Theorem 1.4 is facilitated by the following lemma.

Lemma 2.1: For each complex number x such that $|x|<1$,

$$\prod_{1}^{\infty}\frac{(1-x^{2n})^{3}}{(1+x^{2n-1})^{2}}=\sum_{-\infty}^{\infty}(3n+1)x^{n(3n+2)}. \tag{2.4}$$

Proof: Multiply (2.3) by $-a^{-1}$ to get

$$(a-a^{-1})\prod_{1}^{\infty}\frac{(1-x^{2n})(1-a^{2}x^{2n})(1-a^{-2}x^{2n})}{(1+ax^{2n-1})(1+a^{-1}x^{2n-1})}=\sum_{-\infty}^{\infty}x^{n(3n+2)}(a^{3n+1}-a^{-3n-1}).$$

Now we operate on both sides of the foregoing identity with aD_a, D_a denoting differentiation with respect to a, subsequently, let $a\to 1$ and cancel a factor of 2 to draw the desired conclusion.

Returning to the proof of Theorem 1.4, we multiply both sides of (2.4) by

$$\prod_{n=1}^{\infty}(1+x^{2n-1})^{-1},$$

and appeal to (2.1), where we let $x\to -x$, to get

$$\begin{aligned}\sum_{n=0}^{\infty}(-1)^{n}t_3(n)x^{n}&=\prod_{1}^{\infty}\frac{(1-x^{2n})^{3}}{(1+x^{2n-1})^{3}}\\&=\prod_{n=1}^{\infty}(1+(-x)^{n})\sum_{-\infty}^{\infty}(3n+1)x^{n(3n+2)}\\&=\sum_{n=0}^{\infty}(-1)^{n}q(n)x^{n}\sum_{-\infty}^{\infty}(3n+1)x^{n(3n+2)}.\end{aligned}$$

Now we expand the product of the two series and, subsequently, equate coefficients of like powers of x to prove Theorem 1.4.

Our algorithm proceeds in two steps:

(i) Use the recursive determination of q in Theorem 1.3 to compile a table of values of q, as in Table 1.

(ii) Utilizing Theorem 1.4 and the values of q computed in Table 1, we then compile a list of values of t_3, as shown in Table 2.

TABLE 1

n	$q(n)$	n	$q(n)$
0	1	13	18
2	1	14	22
3	2	16	32
4	2	17	38
5	3	18	46
6	4	19	54
7	5	20	64
8	6	21	76
9	8	22	89
10	10	23	104
11	12	24	122
12	15	25	142

TABLE 2

n	$t_3(n)$	n	$t_3(n)$
0	1	10	9
1	3	11	6
2	3	12	9
3	4	13	9
4	6	14	6
5	3	15	6
6	6	16	15
7	9	17	9
8	3	18	7
9	7	19	12

3. CONCLUDING REMARKS

The brief tables above are compiled to show the effectiveness of the algorithm. For a fixed but arbitrary choice of $n \in \mathbb{P}$, we observe that: (1) to compute $q(n)$ we need about $\sqrt{n}$ of the values $q(k)$, $0 \le k < n$; and then (2) to compute $t_3(n)$ we need $q(n)$ and about $\sqrt{4n/3}$ of the values $q(k)$, $0 \le k < n$. Doubtless, the formulas (1.1) and (1.2) can be adapted to machine computation, and the corresponding tables can then be extended indefinitely.

For given $n \in \mathbb{P}$, there are formulas that express $t_3(n)$ in terms of certain divisor functions. But, for each divisor function f, evaluation of $f(k)$, $k \in \mathbb{P}$, requires factorization of k. By comparison we observe that our algorithm is entirely additive in character. In a word, no factorization is required.

ACKNOWLEDGMENT

The author wishes to express his gratitude to the anonymous referee for suggestions that led to an improved exposition.

REFERENCES

1. J. A. Ewell. "Recurrences for Two Restricted Partition Functions." *The Fibonacci Quarterly* **18.1** (1980):1-2.
2. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*. 4th ed. Oxford: Oxford University Press, 1960.
3. M. V. Subbarao & M. Vidyasagar. "On Watson's Quintuple-Product Identity." *Proc. Amer. Math. Soc.* **26** (1970):23-27.

AMS Classification Numbers: 11E25, 05A19

❖❖❖

IDENTITIES AND CONGRUENCES INVOLVING HIGHER-ORDER EULER-BERNOULLI NUMBERS AND POLYNOMIALS

Guodong Liu
Dept. of Mathematics, Huizhou University, Huizhou, Guangdong 516015, People's Republic of China
(*Submitted May 1999-Final Revision April 2000*)

1. INTRODUCTION

Let t be a complex number with $|t| < \frac{\pi}{2}$ and let the Euler numbers E_{2n} $(n = 0, 1, 2, \ldots)$ be defined by the coefficients in the expansion of

$$\sec t = \sum_{n=0}^{\infty} E_{2n} \frac{t^{2n}}{(2n)!}.$$

That is, $E_0 = 1$, $E_2 = 1$, $E_4 = 5$, $E_6 = 61$, $E_8 = 1385$, $E_{10} = 50521$, ...

We denote

$$E(n,k) = \sum_{\alpha_1+\alpha_2+\cdots+\alpha_k=n} \frac{E_{2\alpha_1}E_{2\alpha_2}\ldots E_{2\alpha_k}}{(2\alpha_1)!(2\alpha_2)!\ldots(2\alpha_k)!}, \tag{1}$$

where the summation is over all k-dimensional nonnegative integer coordinates $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ such that $\alpha_1 + \alpha_2 + \cdots + \alpha_k = n$ and k is any positive integer. Recently, several researchers have studied the numbers $E(n,k)$. In [3], Wenpeng Zhang obtained an expression for $E(n, 2m+1)$ $(m \geq 1)$ as a linear combination of Euler numbers and obtained some interesting congruence expressions for Euler numbers. The main purpose of this paper is to express $E(n, 2m)$ as a linear combination of second-order Euler numbers, so that some congruence expressions are obtained correspondingly. The two identities,

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}B_n^{(pj)} = p^n\sum_{j=0}^{n}(-1)^j\binom{n}{j}B_n^{(j)} \tag{2}$$

and

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}E_n^{(pj)}(0) = p^n\sum_{j=0}^{n}(-1)^j\binom{n}{j}E_n^{(j)}(0), \tag{3}$$

which were obtained by David Zeitlin (see [2], p. 238) are deduced, and some more common results than (2) and (3) are achieved.

2. DEFINITIONS AND LEMMAS

Definition 1: If (A_n) is any sequence with $A_0 = 1$ and if $f(t) = \sum_{n=0}^{\infty} A_n t^n / n!$ is its generating function, then the "umbral" sequence $A_n^{(k)}$ of order k and the associated Appel sequence of polynomials $A_n^{(k)}(x)$ of order k are defined, respectively, by

$$f(t)^k = \sum_{n=0}^{\infty} A_n^{(k)} t^n / n! \tag{4}$$

and

$$e^{xt} f(t)^k = \sum_{n=0}^{\infty} A_n^{(k)}(x) t^n / n!, \tag{5}$$

where k is any integer. Clearly, $A_n^{(k)}(0) = A_n^{(k)}$ and $A_n^{(1)} = A_n$. It is also easy to see that

$$A_n^{(k)}(x) = \sum_{j=0}^{n} \binom{n}{j} A_j^{(k)} x^{n-j} \quad \text{and that} \quad \frac{d}{dx} A_n^{(k)}(x) = nA_{n-1}^{(k)}(x).$$

Remark 1: ***(a)*** When $f(t) = \sec t$, $|t| < \pi/2$, (4) becomes

$$(\sec t)^k = \sum_{n=0}^{\infty} E_n^{(k)} t^n / n!, \tag{6}$$

where $E_n^{(k)}$ are called Euler numbers of order k;

(b) When $f(t) = t/(e^t - 1)$, $|t| < 2\pi$, (4) becomes

$$(t/(e^t - 1))^k = \sum_{n=0}^{\infty} B_n^{(k)} t^n / n!, \tag{7}$$

where $B_n^{(k)}$ are called Bernoulli numbers of order k (cf. [1], [2]);

(c) When $f(t) = 2/(e^t + 1)$, $|t| < \pi$, (5) becomes

$$e^{xt}(2/(e^t + 1))^k = \sum_{n=0}^{\infty} E_n^{(k)}(x) t^n / n!, \tag{8}$$

where $E_n^{(k)}(x)$ are called Euler polynomials of order k (cf. [1], [2]);

(d) When $f(t) = t/(e^t - 1)$, $|t| < 2\pi$, (5) becomes

$$e^{xt}(t/(e^t - 1))^k = \sum_{n=0}^{\infty} B_n^{(k)}(x) t^n / n!, \tag{9}$$

where $B_n^{(k)}(x)$ are called Bernoulli polynomials of order k (cf. [1], [2]).

Clearly, the usual Euler numbers $E_n = E_n^{(1)}$, Bernoulli numbers $B_n = B_n^{(1)}$, Euler polynomials $E_n(x) = E_n^{(1)}(x)$, and Bernoulli polynomials $B_n(x) = B_n^{(1)}(x)$. Using (6), (7), (8), and (9), we have $E_{2n-1}^{(k)} = 0$ $(n \geq 1)$, $E_{2n}^{(k)} = (-1)^n 2^{2n} E_{2n}^{(k)}(\frac{k}{2})$, and $B_n^{(k)} = B_n^{(k)}(0)$.

Definition 2: $\sigma_j(x_1, x_2, \ldots, x_n)$ $(j = 0, 1, 2, \ldots, n)$ are defined as the coefficients of the polynomial

$$(x + x_1)(x + x_2) \cdots (x + x_n) = \sum_{j=0}^{n} \sigma_j(x_1, x_2, \ldots, x_n) x^{n-j}.$$

Lemma 1: $$E_{2n}^{(k)} = \frac{1}{(k-1)(k-2)} E_{2n+2}^{(k-2)} + \frac{k-2}{k-1} E_{2n}^{(k-2)} \quad (k > 2). \tag{10}$$

Proof: By (6), we have

$$\begin{aligned}
&\sum_{n=0}^{\infty} \left(\frac{1}{(k-1)(k-2)} E_{2n+2}^{(k-2)} + \frac{k-2}{k-1} E_{2n}^{(k-2)} \right) \frac{t^{2n}}{(2n)!} \\
&= \frac{1}{(k-1)(k-2)} \sum_{n=1}^{\infty} E_{2n}^{(k-2)} \frac{t^{2n-2}}{(2n-2)!} + \frac{k-2}{k-1} \sum_{n=0}^{\infty} E_{2n}^{(k-2)} \frac{t^{2n}}{(2n)!} \\
&= \frac{1}{(k-1)(k-2)} \frac{d^2}{dt^2} (\sec t)^{k-2} + \frac{k-2}{k-1} (\sec t)^{k-2} = (\sec t)^k = \sum_{n=0}^{\infty} E_{2n}^{(k)} \frac{t^{2n}}{(2n)!},
\end{aligned} \tag{11}$$

and comparing the coefficient of t^{2n} on both sides of (11), we immediately obtain (10). □

Lemma 2: $E_{2n}^{(2)} = \dfrac{(-1)^n 2^{2n+1}(2^{2n+2}-1)}{n+1} B_{2n+2}.$ (12)

Proof: By (6) and (7), we have

$$\sum_{n=0}^{\infty} \frac{2}{n+1}(2^{2n+2}-1)B_{2n+2}\frac{t^{2n}}{(2n)!} = \sum_{n=1}^{\infty} \frac{2}{n}(2^{2n}-1)B_{2n}\frac{t^{2n-2}}{(2n-2)!}$$

$$= 4\sum_{n=1}^{\infty}(2n-1)(2^{2n}-1)B_{2n}\frac{t^{2n-2}}{(2n)!} = 4\frac{d}{dt}\sum_{n=1}^{\infty}(2^{2n}-1)B_{2n}\frac{t^{2n-1}}{(2n)!}$$

$$= 4\frac{d}{dt}\left(t^{-1}\sum_{n=1}^{\infty}B_{2n}\frac{(2t)^{2n}}{(2n)!} - t^{-1}\sum_{n=1}^{\infty}B_{2n}\frac{t^{2n}}{(2n)!}\right) = 4\frac{d}{dt}\left(t^{-1}\left(\frac{2t}{e^{2t}-1}-1+t\right) - t^{-1}\left(\frac{t}{e^{t}-1}-1+\frac{1}{2}t\right)\right)$$

$$= \frac{4e^t}{(e^t+1)^2} = \left(\sec\frac{it}{2}\right)^2 = \sum_{n=0}^{\infty}E_{2n}^{(2)}\frac{(\frac{i}{2}t)^{2n}}{(2n)!} = \sum_{n=1}^{\infty}(-1)^n\frac{1}{2^{2n}}E_{2n}^{(2)}\frac{t^{2n}}{(2n)!}, \tag{13}$$

and comparing the coefficient of t^{2n} on both sides of (13), we immediately obtain (12). □

Remark 2: By (12), we have $E_0^{(2)} = 1$, $E_2^{(2)} = 2$, $E_4^{(2)} = 16$, $E_6^{(2)} = 272$, $E_8^{(2)} = 7936$, $E_{10}^{(2)} = 353792$, $E_{12}^{(2)} = 22368256, \ldots$.

3. MAIN RESULTS

Theorem 1: $E_{2n}^{(2m)} = \dfrac{1}{(2m-1)!}\displaystyle\sum_{j=0}^{m-1}\sigma_{mj}E_{2n+2m-2-2j}^{(2)},$ (14)

where $\sigma_{mj} = \sigma_j(2^2, 4^2, 6^2, \ldots, (2m-2)^2)$, and m is a positive integer.

Proof: We prove Theorem 1 using mathematical induction.

(a) When $m = 1$, (14) is clearly true.

(b) Suppose (14) is true for some natural number m. By the supposition and (10), we have

$$E_{2n}^{(2m+2)} = \frac{1}{(2m+1)(2m)}E_{2n+2}^{(2m)} + \frac{2m}{2m+1}E_{2n}^{(2m)}$$

$$= \frac{1}{(2m+1)!}\sum_{j=0}^{m-1}\sigma_{mj}E_{2n+2m-2j}^{(2)} + \frac{(2m)^2}{(2m+1)!}\sum_{j=0}^{m-1}\sigma_{mj}E_{2n+2m-2j-2}^{(2)}$$

$$= \frac{1}{(2m+1)!}\sum_{j=0}^{m-1}\sigma_{mj}E_{2n+2m-2j}^{(2)} + \frac{(2m)^2}{(2m+1)!}\sum_{j=1}^{m-1}\sigma_{m(j-1)}E_{2n+2m-2j}^{(2)}$$

$$= \frac{1}{(2m+1)!}\left(E_{2n+2m}^{(2)} + \sum_{j=1}^{m-1}(\sigma_{mj} + (2m)^2\sigma_{m(j-1)})E_{2n+2m-2j}^{(2)} + (2m)^2\sigma_{m(m-1)}E_{2n}^{(2)}\right)$$

$$= \frac{1}{(2m+1)!}\left(E_{2n+2m}^{(2)} + \sum_{j=1}^{m-1}\sigma_{(m+1)j}E_{2n+2m-2j}^{(2)} + \sigma_{(m+1)m}E_{2n}^{(2)}\right)$$

$$= \frac{1}{(2m+1)!}\sum_{j=0}^{m}\sigma_{(m+1)j}E_{2n+2m-2j}^{(2)}, \tag{15}$$

and (15) shows that (14) is also true for the natural number $m+1$. From (a) and (b), we know that (14) is true. □

Corollary 1: $$E(n,2m)=\frac{1}{(2m-1)!(2n)!}\sum_{j=0}^{m-1}\sigma_{mj}E_{2n+2m-2-2j}^{(2)}. \tag{16}$$

Proof: From formulas (1) and (6), we have

$$\sum_{n=0}^{\infty}E(n,2m)t^{2n}=\left(\sum_{n=0}^{\infty}E_{2n}\frac{t^{2n}}{(2n)!}\right)^{2m}=(\sec t)^{2m}=\sum_{n=0}^{\infty}E_{2n}^{(2m)}\frac{t^{2n}}{(2n)!}. \tag{17}$$

Comparing the coefficients of t^{2n} on both sides of (17), we have

$$E(n,2m)=\frac{1}{(2n)!}E_{2n}^{(2m)}. \tag{18}$$

By (14) and (18), we immediately obtain (16). □

Corollary 2: For any odd prime p, we have the congruence

$$E_{p-1}^{(2)}\equiv\begin{cases}1 \pmod p & \text{if } p\equiv 1 \pmod 4,\\ -1 \pmod p & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

Proof: Taking $n=0$ and $2m-1=p$ in Corollary 1, and noting that $E_0=E_0^{(2)}=1$, $(p-1)!\equiv -1 \pmod p$, we can get

$$\begin{aligned}0\equiv p!&=\sum_{j=0}^{\frac{p-1}{2}}\sigma_{\frac{p+1}{2}j}E_{p-1-2j}^{(2)}\equiv E_{p-1}^{(2)}+\sigma_{\frac{p+1}{2}\frac{p-1}{2}}E_0^{(2)}\\ &=E_{p-1}^{(2)}+2^2\cdot 4^2\cdot 6^2\cdot 8^2\cdots(p-1)^2\equiv E_{p-1}^{(2)}+(-1)^{\frac{p+1}{2}} \pmod p,\end{aligned}$$

where we have used the congruence

$$\sigma_{\frac{p+1}{2}j}\equiv 0 \pmod p,\ j=1,2,\ldots,\frac{p-3}{2}.$$

Therefore,

$$E_{p-1}^{(2)}\equiv\begin{cases}1 \pmod p & \text{if } p\equiv 1 \pmod 4,\\ -1 \pmod p & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

This completes the proof. □

Corollary 3: For any odd prime p, we have the congruence

$$\frac{2^{p+1}(2^{p+1}-1)}{p+1}B_{p+1}\equiv 1 \pmod p.$$

Proof: By Corollary 2 and (12). □

Remark 3: For $p=3$, the preceding congruence says that $60B_4\equiv 1 \pmod 3$ while, for $p>3$, using Fermat's little theorem, i.e., $2^p\equiv 2 \pmod p$, the congruence says that $12B_{p+1}\equiv 1 \pmod p$. These facts can be derived directly from the standard recursion for Bernoulli numbers.

Theorem 2: If p is any integer, then

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}A_n^{(pj)}(jx)=n!(-x-pA_1)^n, \tag{19}$$

where $A_n^{(k)}(x)$ are defined as in Definition 1.

Proof: We use the notation $[t^n]h(t)$ to denote the coefficient of t^n in the power series expansion at 0 of $h(t)$. Then, by the definition of $A_n^{(k)}(x)$ and the binomial expansion,

$$\begin{aligned}\sum_{j=0}^{n}(-1)^j\binom{n}{j}A_n^{(pj)}(jx)&=n![t^n]\sum_{j=0}^{n}(-1)^j\binom{n}{j}e^{tjx}f(t)^{pj}\\&=n![t^n](1-e^{tx}f(t)^p)^n.\end{aligned}$$

If $g(t)=1-e^{tx}f(t)^p$, then $g(0)=0$ and $g'(t)=-e^{tx}(xf(t)^p+pf(t)^{p-1}f'(t))$, so that $g'(0)=-(x+pA_1)$. Thus, $g(t)=-(x+pA_1)t+0(t^2)$ and $g(t)^n=(-x-pA_1)^nt^n+0(t^{n+1})$.

Corollary 4: If p is any integer, then

(a)
$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}E_n^{(pj)}(jx)=n!\left(\frac{p}{2}-x\right)^n; \tag{20}$$

(b)
$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}B_n^{(pj)}(jx)=n!\left(\frac{p}{2}-x\right)^n. \tag{21}$$

Proof: By formula (19), we immediately obtain (20) and (21), since in the Euler case $f(t)=2/(e^t+1)$ and in the Bernoulli case $f(t)=t/(e^t-1)$. In both cases, $A_0=f(0)=1$ and $A_1=f'(0)=-1/2$. □

Corollary 5: If p is any integer, then

(a) $\displaystyle\sum_{j=0}^{n}(-1)^j\binom{n}{j}E_n^{(pj)}(0)=p^n\cdot\frac{n!}{2^n}$,

(b) $\displaystyle\sum_{j=0}^{n}(-1)^j\binom{n}{j}E_n^{(j)}(0)=\frac{n!}{2^n}$,

(c) $\displaystyle\sum_{j=0}^{n}(-1)^j\binom{n}{j}B_n^{(pj)}=p^n\cdot\frac{n!}{2^n}$,

(d) $\displaystyle\sum_{j=0}^{n}(-1)^j\binom{n}{j}B_n^{(j)}=\frac{n!}{2^n}$.

Proof: Taking $x=0$ in Corollary 4, we immediately obtain Corollary 5. □

Remark 4: By Corollary 5, we immediately obtain (2) and (3) (see [2], p. 238).

Corollary 6:
$$\sum_{j=0}^{2n}(-1)^j\binom{2n}{j}E_{2n}^{(pj)}=0. \tag{23}$$

Proof: Taking $x=p/2$ in Corollary 4(a) and noting that $E_{2n}^{(pj)}=(-1)^n2^{2n}E_{2n}^{(pj)}\left(\frac{pj}{2}\right)$, we immediately obtain (23). □

ACKNOWLEDGMENT

The author would like to thank the referee for valuable comments, including the statement and proof of Theorem 2, which improved the presentation of the original paper.

REFERENCES

1. Leetsch C. Hsu. "Finding Some Strange Identities via Faa di Bruno's Formula." *J. Math. Research & Exposition* **13** (1993):159-65.
2. David Zeitlin. "The nth Derivative of a Class of Functions." *Duke Math. J.* **30** (1963):229-38.
3. Wenpeng Zhang. "Some Identities Involving the Euler and the Central Factorial Numbers." *The Fibonacci Quarterly* **36.2** (1998):154-57.

AMS Classification Numbers: 11B37, 11B39, 11B68

❖❖❖

NEW PROBLEM WEB SITE

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

http://problems.math.umr.edu

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

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

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

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

A NEW RECURRENCE FORMULA FOR BERNOULLI NUMBERS

Harunobu Momiyama
Dept. of Math., School of Education, Waseda University,
1-6-1 Nishi-Waseda, Sinjuku-ku, Tokyo, 169-8050, Japan
(*Submitted May 1999-Final Revision September 1999*)

1. INTRODUCTION

Let B_n be the Bernoulli numbers defined by the expansion

$$\frac{t}{e^t-1}=\sum_{n=0}^{\infty}B_n\frac{t^n}{n!}.$$

Kaneko [3] proved a recurrence formula for B_n,

$$\sum_{j=0}^{n}\binom{n+1}{j}(n+j+1)B_{n+j}=0 \quad (n\geq 1), \tag{1}$$

which needs only half the number of terms to calculate B_{2n} in comparison with the usual recurrence (cf. [5], §15, Lemma 1):

$$\sum_{j=0}^{n}\binom{n+1}{j}B_j=0 \quad (n\geq 1). \tag{2}$$

The aim of this paper is to prove the following recurrence formula that yields Kaneko's formula when $m=n$ and also the usual one.

Theorem: For nonnegative integers m and n with $m+n>0$, we have the formula

$$\sum_{j=0}^{m}\binom{m+1}{j}(n+j+1)B_{n+j}+(-1)^{m+n}\sum_{k=0}^{n}\binom{n+1}{k}(m+k+1)B_{m+k}=0.$$

As an application of our theorem, we can derive the Kummer congruence. The proof of our theorem uses the Volkenborn integral (whose properties are found in [4]).

2. PROOF OF THE THEOREM

Let p be a prime number and let $\mathbb{Z}_p$ and $\mathbb{Q}_p$ denote the ring of p-adic integers and the field of p-adic numbers, respectively. For any uniformly differentiable function $f:\mathbb{Z}_p\to\mathbb{Q}_p$, we define the Volkenborn integral of f by

$$\int_{\mathbb{Z}_p}f(x)\,dx:=\lim_{n\to\infty}p^{-n}\sum_{j=0}^{p^n-1}f(j).$$

In particular, the Bernoulli number B_n is given by the formula

$$B_n=\int_{\mathbb{Z}_p}x^n\,dx. \tag{3}$$

Let m and n be nonnegative integers with $m+n>0$. If we define the polynomial function $G(x)$ on $\mathbb{Z}_p$ by

$$G(x) := x^{m+1}(x-1)^{n+1} + (-1)^{n+m}x^{n+1}(x-1)^{m+1},$$

then we have $G'(x+1) = -G'(-x)$. Therefore, we have

$$\int_{\mathbb{Z}_p} G'(x+1)\,dx = 0$$

(see [4], Proposition 55.7). To calculate the left-hand side of this equation, we write $G(x+1)$ in the form

$$G(x+1) = \sum_{j=0}^{m+1}\binom{m+1}{j}x^{n+j+1} + (-1)^{m+n}\sum_{k=0}^{n+1}\binom{n+1}{k}x^{m+k+1}.$$

Applying formula (3) to the derivative $G'(x+1)$, we obtain

$$\sum_{j=0}^{m+1}\binom{m+1}{j}(n+j+1)B_{n+j} + (-1)^{m+n}\sum_{k=0}^{n+1}\binom{n+1}{k}(m+k+1)B_{m+k} = 0.$$

Since $B_j = 0$ for odd $j > 1$ and, hence, the terms involving B_{n+m+1} vanish, this gives the formula of our theorem.

Remark: For a positive integer s, we consider the polynomial function

$$F(x) := x^{m+1}(x-s-1)^{n+1} + (-1)^{n+m}x^{n+1}(x-s-1)^{m+1}$$

on $\mathbb{Z}_p$. Then we have $F(x+s+1) = F(-x)$. It follows from Propositions 55.5 and 55.7 in [4] that

$$\begin{aligned}\int_{\mathbb{Z}_p} F'(x+s+1)\,dx &= \sum_{j=1}^{s}\int_{\mathbb{Z}_p}(F'(x+j+1) - F'(x+j))\,dx + \int_{\mathbb{Z}_p} F'(x+1)\,dx \\ &= \sum_{j=1}^{s} F''(j) + \int_{\mathbb{Z}_p} F'(-x)\,dx \\ &= \sum_{j=1}^{s} F''(j) - \int_{\mathbb{Z}_p} F'(x+s+1)\,dx.\end{aligned}$$

Therefore, we obtain

$$\begin{aligned}&\sum_{j=0}^{n}\binom{n+1}{j}(s+1)^{n+1-j}(m+j+1)B_{m+j} \\ &\quad + (-1)^{m+n}\sum_{k=0}^{m}\binom{m+1}{k}(s+1)^{m+1-k}(n+k+1)B_{n+k} = \frac{1}{2}\sum_{j=1}^{s}F''(j).\end{aligned}$$

If $s = 1$ and $m = n$, then we have the formula

$$\sum_{k=0}^{n}\binom{n+1}{k}2^{n+1-k}(n+k+1)B_{n+k} = (-1)^n(n+1) \quad (n \geq 1),$$

which resembles the well-known formula (see [2], §15, Theorem 1)

$$\sum_{k=0}^{n}\binom{n+1}{k}2^{n+1-k}B_k = n+1.$$

3. SEVERAL CONSEQUENCES

We shall derive the usual formula (2) from our theorem. If $m = 0$, we obtain

$$(-1)^n \sum_{k=0}^{n} \binom{n+1}{k} (k+1) B_k = -(n+1) B_n \quad (n \geq 1). \tag{4}$$

For convenience, we put

$$C_n := (-1)^n (n+2) \sum_{k=0}^{n} \binom{n+1}{k} B_k .$$

It is obvious that the usual formula is equivalent to $C_n = 0$ for $n \geq 1$. Substituting the identity

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

into equation (4) yields

$$C_n + C_{n-1} = -(n+1)(1-(-1)^n) B_n.$$

Since $B_j = 0$ for odd $n > 1$, the right-hand side of this equation vanishes for $n \geq 2$. It is clear that $C_1 = 0$, hence $C_n = 0$ for $n \geq 1$.

We next show Kummer's congruence

$$\frac{B_n}{n} \equiv \frac{B_{n+(p-1)}}{n+(p-1)} \pmod{p\mathbb{Z}_p}$$

when p is a prime number with $p \geq 5$ and n is an integer with $1 \leq n \leq p-2$. Our argument is similar to Agoh's argument [1].

If $m = p-1$, the formula of our theorem is

$$\sum_{j=0}^{p-1} \binom{p}{j} (n+j+1) B_{n+j} + (-1)^n \sum_{k=0}^{n} \binom{n+1}{k} (p+k) B_{p-1+k} = 0. \tag{5}$$

Note that $1 \leq n+j < 2(p-1)$ for $0 \leq j \leq p-1$. From the well-known fact (see von Staudt and Clausen [2], §15, Corollary to Theorem 3) that

$$pB_{n+j} \equiv \begin{cases} -1 \pmod{p\mathbb{Z}_p} & \text{if } n+j = p-1, \\ 0 \pmod{p\mathbb{Z}_p} & \text{otherwise,} \end{cases} \tag{6}$$

we have

$$\binom{p}{j} (n+j+1) B_{n+j} \equiv 0 \pmod{p\mathbb{Z}_p}$$

for $j \neq 0$. Thus, equation (5) yields

$$(n+1) B_n + (-1)^n \sum_{k=0}^{n} \binom{n+1}{k} (p+k) B_{p-1+k} \equiv 0 \pmod{p\mathbb{Z}_p}.$$

Applying congruence (6) to the above, we have

$$(n+1) B_n + (-1)^n \sum_{k=1}^{n} \binom{n+1}{k} k B_{p-1+k} \equiv (-1)^n \pmod{p\mathbb{Z}_p}.$$

We remark that combining equation (2) with (4) gives

$$(n+1)B_n = (-1)^{n+1}\sum_{k=1}^{n}\binom{n+1}{k}(k+p-1)B_k + (-1)^{n+1}(p-1)B_0.$$

Since $B_0 = 1$, we have

$$\sum_{k=1}^{n}\binom{n+1}{k}(kB_{p-1+k} - (k+p-1)B_k) \equiv 0 \pmod{p\mathbb{Z}_p}.$$

From these congruences, we have by induction on n that

$$nB_{p-1+n} \equiv (p+n-1)B_n \pmod{p\mathbb{Z}_p}$$

for $1 \le n \le p-2$. This yields Kummer's congruence as desired.

REFERENCES

1. T. Agoh. "On Bernoulli Numbers I." *C. R. Math. Rep. Acad. Sci. Canada* **10.1** (1988):7-12.
2. K. Ireland & M. Rosen. *A Classical Introduction to Modern Number Theory.* Graduate Texts in Math. New York: Springer-Verlag, 1982.
3. M. Kaneko. "A Recurrence Formula for the Bernoulli Numbers." *Proc. Japan Acad. Ser. A. Math. Sci.* **71** (1995):192-93.
4. W. H. Schikhof. *Ultrametric Calculus.* Cambridge: Cambridge University Press, 1984.

AMS Classification Number: 11B68

❖❖❖

SUSTAINING MEMBERS

*H.L. Alder
G.L. Alexanderson
P. G. Anderson
S. Ando
R. Andre-Jeannin
J.G. Bergart
G. Bergum
*M. Bicknell-Johnson
P.S. Bruckman
G.D. Chakerian
H. Chen
C. Chouteau
C.K. Cook
C. Cooper
M.J. DeBruin
M.J. DeLeon
J. De Kerf
E. Deutsch
L.A.G. Dresel
U. Dudley
M. Elia
L.G. Ericksen, Jr.
D.R. Farmer
D.C. Fielder
C.T. Flynn
E. Frost
N. Gauthier
*H.W. Gould
P. Hagis, Jr.
V. Hanning
H. Harborth
*A.P. Hillman
*A.F. Horadam
Y. Horibe
F.T. Howard
R.J. Howell
J.P. Jones
R.E. Kennedy
C.H. Kimberling
R. Knott
Y.H.H. Kwong
J.C. Lagarias
J. Lahr
*C.T. Long
G. Lord
W.L. McDaniel
F.U. Mendizabal
M.G. Monzingo
J.F. Morrison
H. Niederhausen
S.A. Obaid
T.J. Osler
A. Prince
D. Redmond
B.M. Romanic
S. Sato
J.A. Schumaker
H.J Seiffert
A.G. Shannon
L.W. Shapiro
L. Somer
P. Spears
W.R. Spickerman
P.K. Stockmeyer
D.R. Stone
I. Strazdins
J. Suck
M.N.S. Swamy
*D. Thoro
J.C. Turner
C. Vanden Eynden
T.P. Vaughan
J.N. Vitale
M.J. Wallace
J.E. Walton
W.A. Webb
V. Weber
R.E. Whitney

*Charter Members

INSTITUTIONAL MEMBERS

BIBLIOTECA DEL SEMINARIO MATHEMATICO
Padova, Italy

CALIFORNIA STATE UNIVERSITY SACRAMENTO
Sacramento, California

ETH-BIBLIOTHEK
Zurich, Switzerland

GONZAGA UNIVERSITY
Spokane, Washington

HOWELL ENGINEERING COMPANY
Bryn Mawr, Califoria

KLEPCO, INC.
Sparks, Nevada

KOBENHAVNS UNIVERSITY MATEMATISK INSTITUT
Copenhagen, Denmark

MISSOURI SOUTHERN STATE COLLEGE
Joplin, Missouri

SAN JOSE STATE UNIVERSITY
San Jose, California

SANTA CLARA UNIVERSITY
Santa Clara, California

UNIVERSITY OF NEW ENGLAND
Armidale, N.S.W. Australia

WAKE FOREST UNIVERSITY
Winston-Salem, North Carolina

WASHINGTON STATE UNIVERSITY
Pullman, Washington

YESHIVA UNIVERSITY
New York, New York

JOVE STATISTICAL TYPING SERVICE
2088 Orestes Way
Campbell, California 95008

BOOKS AVAILABLE
THROUGH THE FIBONACCI ASSOCIATION

Introduction to Fibonacci Discovery by Brother Alfred Brousseau, Fibonacci Association (FA), 1965. $18.00

Fibonacci and Lucas Numbers by Verner E. Hoggatt, Jr. FA, 1972. $23.00

A Primer for the Fibonacci Numbers. Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1972. $32.00

Fibonacci's Problem Book, Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1974. $19.00

The Theory of Simply Periodic Numerical Functions by Edouard Lucas. Translated from the French by Sidney Kravitz. Edited by Douglas Lind. FA, 1969. $6.00

Linear Recursion and Fibonacci Sequences by Brother Alfred Brousseau. FA, 1971. $6.00

Fibonacci and Related Number Theoretic Tables. Edited by Brother Alfred Brousseau. FA, 1972. $30.00

Number Theory Tables. Edited by Brother Alfred Brousseau. FA, 1973. $39.00

Tables of Fibonacci Entry Points, Part One. Edited and annotated by Brother Alfred Brousseau. FA, 1965. $14.00

Tables of Fibonacci Entry Points, Part Two. Edited and annotated by Brother Alfred Brousseau. FA, 1965. $14.00

A Collection of Manuscripts Related to the Fibonacci Sequence—18th Anniversary Volume. Edited by Verner E. Hoggatt, Jr. and Marjorie Bicknell-Johnson. FA, 1980. $38.00

Applications of Fibonacci Numbers, Volumes 1-7. Edited by G.E. Bergum, A.F. Horadam and A.N. Philippou. Contact Kluwer Academic Publishers for price.

Applications of Fibonacci Numbers, Volume 8. Edited by F.T. Howard. Contact Kluwer Academic Publishers for price.

Generalized Pascal Triangles and Pyramids Their Fractals, Graphs and Applications by Boris A. Bondarenko. Translated from the Russian and edited by Richard C. Bollinger. FA, 1993. $37.00

Fibonacci Entry Points and Periods for Primes 100,003 through 415,993 by Daniel C. Fielder and Paul S. Bruckman. $20.00

Handling charges will be $4.00 for the first book and $1.00 for each additional book in the United States and Canada. For Foreign orders, the handling charge will be $8.00 for the first book and $3.00 for each additional book.

Please write to the Fibonacci Association, P.O. Box 320, Aurora, S.D. 57002-0320, U.S.A., for more information.