The Fibonacci Quarterly

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

VOLUME 26 NOVEMBER 1988 NUMBER 4

PURPOSE

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

EDITORIAL POLICY

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

SUBMITTING AN ARTICLE

Articles should be submitted in the format of the current issues of the **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.

Two copies of the manuscript should be submitted to: **GERALD E. BERGUM, EDITOR, THE FIBONACCI QUARTERLY, DEPARTMENT OF COMPUTER SCIENCE, SOUTH DAKOTA STATE UNIVERSITY, BOX 2201, BROOKINGS, SD 57007-0194.**

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

SUBSCRIPTIONS, ADDRESS CHANGE, AND REPRINT INFORMATION

Address all subscription correspondence, including notification of address change, to: **RICHARD VINE, SUBSCRIPTION MANAGER, THE FIBONACCI ASSOCIATION, SANTA CLARA UNIVERSITY, SANTA CLARA, CA 95053.**

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

Annual domestic Fibonacci Association membership dues, which include a subscription to **THE FIBONACCI QUARTERLY,** are $27 for Regular Membership, $37 for Sustain Membership, and $67 for Institutional Membership; foreign rates, which are based on international mailing rates, are somewhat higher than domestic rates; please write for details. **THE FIBONACCI QUARTERLY** is published each February, May, August and November.

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

A Report On

The Third International Conference on Fibonacci Numbers And Their Applications

Herta T. Freitag

A newspaper article at Pisa, Italy, with a prominent headline: "CONVEGNO PARLANO I MATEMATICI L'INCONTRO IN OMMAGIO A FIBONACCI" hearalded our Third International Conference on Fibonacci Numbers and Their Applications which was held in Pisa, Italy, July 25th-29th, 1988. A stamp: "I NUMERI DI FIBONACCI CONGRESSO INTERNAZIONALE, 26-7-1988" commemorated it.

Of course, mathematicians all across the globe, and especially those who are so fortunate as to have become interested in "Fibonacci-type mathematics," had known about it for some time. The August 1987 issue of *The Fibonacci Quarterly* had brought the glad tidings: an announcement that our third conference was to take place at the University of Pisa during the last week of July 1988.

By mid June 1988, we held the coveted program in our hands. 66 participants were listed, and they came from 22 different countries, the U.S. heading the list with a representation of 20, followed by Italy and Australia. Of course, it was to be expected that at conference time proper additional names would lengthen the count. Forty-five papers were to be presented, several of them with coauthors; there were 3 women speakers.

Theoretically sounding titles abounded. There was Andreas N. Philippou's paper, coauthored by Demetris L. Antzoulakes: "Multivariate Fibonacci Polynomials of Order K and the Multiparameter Negative Binomial Distribution of the Same Order." But, rather intriguingly, practical interests wedged themselves in also with Piero Filipponi's paper, coauthored by Emilio Montolivo: "Representation of Natural Numbers as a Sum of Fibonacci Numbers: An Application to Modern Cryptography." This again highlighted one of the joys mathematicians experience: the interplay between theoretical and applied mathematics.

What a delight it was to meet in Pisa, Italy, the birthplace of Leonardo of Pisa, son of Bonacci, "our" Fibonacci (= 1170-1250). We already knew that—befittingly, and much to our pleasure—Pisa had honored its mathematical son by a statue. My friends and I were among the many (maybe it was all of them) who made a pilgrimage to Fibonacci's statue. It was a fairly long walk, eventually on Via Fibonacci(!), along the Arno River, until we finally found him in a pretty little park. He seemed thoughtful, and appeared to enjoy the sight of the nearby shrubs and flowers. I felt like thanking him for "having started it all," for having coined the sequence that now bears his name. It would have been nice to invite him to our sessions. I predict he would have been thoroughly startled. What had happened since 1202 when his *Liber Abaci* was published?!

Almost invariably, the papers were of very high caliber. The great variety of topics and the multitude of approaches to deal with a given mathematical idea was remarkable and rather appealing. And it was inspiring to coexperience the deep involvement which authors feel with their topic.

We worked hard. The sessions started at 9 a.m. and with short intermissions (coffee break and lunch) they lasted till about 5:30 p.m. As none of the papers were scheduled simultaneously, we could experience the luxury of hearing ALL presentations.

We did take out time to play. Of course, just to BE in Pisa was a treat. We stepped into the past, enwrapped into the charm of quaint, old buildings, which—could they only talk—would fascinate us with their memories of olden times. As good fortune would have it (or, was it the artistry of Roberto Dvornicich, Professor of Mathematics at the University of Pisa, who arranged housing for the conference participants) my friends and I stayed at the Villa Kinzica—across the street from the Leaning Tower of Pisa. Over a plate of spaghetti, we could see that tower, one of the "seven wonders of the world" whose very construction took 99 years. And—it REALLY leans! We were charmed by the seven bells, all chiming in different tones. But—most of all—we pictured Galileo Galilei excitedly experimenting with falling bodies . . .

I would be amiss if I did not mention the Botanical Garden of Pisa—situated adjacent to our conference room at POLO DIDATTICO DELLA FACOLTA DI SCIENZE. In the summer of 1543 (the University of Pisa itself was founded in the 12th century) this garden was opened as the first botanical garden in Western Europe. Its present location was taken up 50 years later. While we may not have been able to recognize "METASEQUOIA GLYPTOSTROBOIDES" the peace and serenity of this beautiful park struck chords in all of us.

On the third day, the Conference terminated at noon, and we took the bus to Volterra. The bus ride itself ushered in a trip long to be remembered. The incredibly luscious fields of sunflowers and sunflowers—an

(Continued on page 331)

AN ITERATED QUADRATIC EXTENSION OF $GF(2)$

DOUG WIEDEMANN
University of Waterloo, Waterloo, Ontario, Canada

(Submitted November 1986)

1. A CONSTRUCTION

It is well known (see, for example, Ex. 3.96 of [1]) that the polynomials $x^{2 \cdot 3^j} + x^{3^j} + 1$ are irreducible in $GF(2)[x]$ for $j = 0, 1, 2, \ldots$. Since

$$(x^{2 \cdot 3^j} + x^{3^j} + 1)(x^{3^j} + 1) = x^{3^{j+1}} + 1$$

is a square-free polynomial, it follows that the period of each root of $x^{2 \cdot 3^j} + x^{3^j} + 1$ is precisely 3^{j+1}, only one and a half times the degree of the polynomial. The field

$$C_j \approx GF(2)[x]/(x^{2 \cdot 3^j} + x^{3^j} + 1) \approx GF(2^{2 \cdot 3^j})$$

may be obtained by iterated cubic extensions beginning with $C_0 \approx GF(2)(x_0)$, where $x_0 \neq 1$ is a cube root of unity. We have $C_1 \approx C_0(x_1)$, where x_1 is any solution to $x_1^3 = x_0$. Iterating, $C_{j+1} \approx C_j(x_{j+1})$, where $x_{j+1}^3 = x_j$.

This paper deals with an iterated quadratic extension of $GF(2)$, whose generators are described by

$$x_{j+1} + x_{j+1}^{-1} = x_j \text{ for } j \geqslant 0, \text{ where } x_0 + x_0^{-1} = 1. \tag{1}$$

Let

$$E_0 \approx GF(2)(x_0),\ E_1 \approx E_0(x_1),\ \ldots,\ E_{j+1} \approx E_j(x_{j+1}).$$

Note that $x_0^2 + x_0 + 1 = 0$ has no root in $GF(2)$ so the first extension is quadratic. To show that each subsequent extension is quadratic, it need only be shown that the equation for x_{j+1}, which may be rewritten $x_{j+1}^2 + x_{j+1}x_j + 1 = 0$, has no root in E_j, for all $j \geqslant 0$. Although this follows almost immediately from theorems about finite fields, for example, Theorem 6.69 of Berlekamp [2], a more elementary proof will be given here. Let

$$Tr^{(n)}(x) = \sum_{i=1}^{2^n - 1} x^{2^i}.$$

Also, let $|E|$ denote the order or number of elements of a finite field E.

Theorem 1: For $j \geqslant 0$, $x_{j+1} \notin E_j$, $|E_{j+1}| = 2^{2^{j+2}}$ and

$$Tr^{(j+2)}(x_{j+1}) = Tr^{(j+2)}(x_{j+1}^{-1}) = 1.$$

Proof (mathematical induction): Note $x_0 \notin GF(2)$ and $Tr^{(1)}(x_0) = Tr^{(1)}(x_0^{-1}) = 1$. The statement of the theorem is therefore true for $j = -1$ if E_{-1} is defined to be $GF(2)$. In a field of characteristic 2, assume $x^2 = xz + 1$. Then,

$$x^4 = x^2z^2 + 1 = xz^3 + z^2 + 1,\ x^8 = xz^7 + z^6 + z^4 + 1,$$

and, in general,

$$x^{2^k} = xz^{2^k - 1} + \sum_{i=1}^{k} z^{2^k - 2^i}.$$

Hence,

$$x_{j+1}^{2^{2^{j+1}}} = x_{j+1}x_j^{2^{2^{j+1}}-1} + x_j^{2^{2^{j+1}}}(Tr^{(j+1)}(x_j^{-1}))^2. \tag{2}$$

Now assume that the statement of the theorem holds for $j - 1$. Then E_j has order $2^{2^{j+1}}$ so, if x_{j+1} were in E_j, by the Fermat theorem and (2), $x_{j+1} = x_{j+1} + x_j(Tr^{(j+1)}(x_j^{-1}))^2$. But $Tr^{(j+1)}(x_j^{-1}) = 1$ by hypothesis, so, by contradiction, x_{j+1} is not in E_j itself but in a quadratic extension of E_j. The order of E_{j+1} is, therefore, $|E_j|^2 = 2^{2^{j+2}}$, using the second statement of the hypothesis.

Note that the other root to (1) for x_{j+1} is x_{j+1}^{-1}. Also, $Gal(E_{j+1}/E_j)$ has order 2 so, if σ denotes the nontrivial Galois automorphism, $\sigma(x_{j+1}) = x_{j+1}^{-1}$. Finally, $Tr^{(j+2)}$ is the trace map of E_{j+1} to $GF(2)$, so

$$Tr^{(j+2)}(x_{j+1}^{-1}) = Tr^{(j+2)}(x_{j+1}) = Tr^{(j+1)}(x_{j+1} + \sigma(x_{j+1})) = Tr^{(j+1)}(x_j) = 1$$

by the last part of the hypothesis, completing the statement of the theorem for j. ■

Corollary: $x_n^{F_n} = 1$, when $n \geq 0$ and $F_n = 2^{2^n} + 1$ is the Fermat number.

Proof: Define E_{-1} to be $GF(2)$. Since $|E_n| = 2^{2^{n+1}}$, the nontrivial member of $Gal(E_n/E_{n-1})$ is given by $\sigma_n(y) = y^{2^{2^n}}$. Since the conjugate of x_n over the field E_{n-1} is x^{-1}, $x_n^{2^{2^n}} = x_n^{-1}$. Thus, $x_n^{F_n} = 1$. ■

The order of a field element is defined to be the smallest nonnegative power which equals 1. In the case where F_n is prime, the above result implies that x_n has order F_n. In any case, the order of x_n divides F_n. Since the Fermat numbers are known to be mutually relatively prime, for example, see Theorem 16 of [3], the order of $x_n x_{n-1} \cdots x_0$ is the product of the orders of the x_i, $i \leq n$. We say an element of a field is primitive if its order is the same as the number of nonzero field elements. If the order of x_i is, in fact, F_i for $i \leq n$, then $x_n x_{n-1} \cdots x_0$ is a primitive element of E_n, because

$$F_n F_{n-1} \cdots F_0 = 2^{2^{n+1}} - 1 = |E_n| - 1.$$

We have not been able to determine if $x_n x_{n-1} \cdots x_0$ is always primitive.

2. BASIS SETS

There are several natural ways to construct a basis of E_n as a vector space over $GF(2)$. One such is of course the set of powers x_n^i, $0 \leqslant i < 2^{n+1}$, because $E_n = GF(2)(x_n)$ is a degree 2^{n+1} extension of $GF(2)$. Another basis is the collection of elements of the form $x_n^{\delta_n} \cdots x_0^{\delta_0}$, where each $\delta_i \in \{0, 1\}$. This can be shown by induction on n. Clearly, $x_0^0 = 1$ and x_0^1 span E_0. Since E_n is a quadratic extension of E_{n-1}, every member of E_n is uniquely expressible as $ax_n + b$, where $a, b \in E_{n-1}$. Assuming a and b can be expressed as sums of the $x_{n-1}^{\delta_{n-1}} \cdots x_0^{\delta_0}$, it follows easily that E_n is spanned by the $x_n^{\delta_n} \cdots x_0^{\delta_0}$. It immediately follows that these elements form a basis because the number of them is the same as the dimension of the space spanned.

Another basis consists of elements of the form $x_n^{\varepsilon_n} \cdots x_0^{\varepsilon_0}$, where $\varepsilon_i \in \{\pm 1\}$. This is shown by a similar argument which uses the fact that each element of E_n equals $ax_n + b = ax_n + cx_{n-1} = (a + c)x_n + cx_n^{-1}$ for some $a, b, c \in E_{n-1}$.

Theorem 2: The following are bases of E_n:

i) $x_n^{\delta_n} \cdots x_0^{\delta_0}$ $\quad \delta_i \in \{0, 1\}$ $\qquad$ ii) $x_n^{\varepsilon_n} \cdots x_0^{\varepsilon_0}$ $\quad \varepsilon_i \in \{-1, 1\}$

iii) $x_n^{2^i}$ $\quad 0 \leqslant i < 2^{n+1}$

Proof: It has already been shown that i) and ii) each form a basis. The elements iii) are the conjugates of x_n over $GF(2)$, and it will be shown that they are linearly independent. This will be done by induction. Certainly, x_0 and $x_0^2 = x_0 + 1$ are linearly independent over $GF(2)$. Assume that the conjugates of x_{n-1} in E_{n-1} are linearly independent. The transformation $\sigma_n(y) = y^{2^{2^n}}$ takes each conjugate of x_n to its reciprocal. If a combination of the conjugates vanishes, then grouping by reciprocal pairs gives

$$\sum_{i=0}^{2^n-1} (\alpha_i x_n^{2^i} + \beta_i x_n^{-2^i}) = 0, \tag{3}$$

where $\alpha_i, \beta_i \in GF(2)$. Applying σ_n to both sides interchanges α_i and β_i. Adding this to the original equation gives

$$0 = \sum_{i=0}^{2^n-1} (\alpha_i + \beta_i)(x_n^{2^i} + x_n^{-2^i}) = \sum_{i=0}^{2^n-1} (\alpha_i + \beta_i)x_{n-1}^{2^i}.$$

By the inductive hypothesis, $\alpha_i + \beta_i \equiv 0$. Thus, the sum (3) can be rewritten:

$$\sum_{i=0}^{2^n-1} \alpha_i x_{n-1}^{2^i};$$

this time the hypothesis implies $\alpha_i \equiv \beta_i \equiv 0$. Thus, iii) forms a basis. ■

In some sense the most interesting is the basis i) because the set for E_{n-1} is contained in the set for E_n. Therefore, the union of all bases given by i) is a basis for the infinite field which is the union of all the E_n. Another interesting property of the basis i) is that every boolean polynomial in n variables corresponds to an element of E_n. These boolean polynomials can be multiplied as elements of E_n in a straightforward if tedious manner. To multiply two such elements, collect all terms containing x_n to one side. Then using

$$(ax_n + b)(cx_n + d) = (acx_{n-1} + bc + ad)x_n + (ac + bd)$$

the product is computable in terms of a few products in E_{n-1}. Using this formula, it can be seen, though the proof is omitted, that the "degree" of the product of the two elements does not exceed the sum of their degrees. By the degree of a field element, we mean the degree of the associated boolean polynomial.

Each basis element of i) can be identified with the 0-1 vector, or bit vector, $(\delta_n, \ldots, \delta_0)$ which, in turn, can be identified with the integer

$$\delta_n 2^n + \cdots + \delta_0 2^0.$$

Let b_i be the basis element associated with the integer i. We now prove a fact regarding the expansion of a product of two basis elements as the sum of basis elements.

Theorem 3: For any i, j, and k the expansion of $b_i b_j$ contains b_k if and only if the expansion of $b_i b_k$ contains b_j.

Lemma: For all i and j, $b_i b_j$ contains the basis element $b_0 = 1$ if and only if $i = j$.

Proof of the Lemma: Once again, we use induction on n. Obviously, the Lemma holds whenever the two basis elements are in E_{-1}. Assume it holds whenever the two basis elements are in E_{n-1}. Now, in E_n, if both b_i and b_j are in E_{n-1}, the statement of the Lemma is true. If x_n is a factor of one but not the other, the product is in $x_n E_{n-1}$ and b_0 cannot occur in the expansion. If $b_i = x_n c$ and $b_j = x_n d$, where $c, d \in E_{n-1}$, then $b_i b_j = x_n x_{n-1} cd + cd$. The first term is in $x_n E_{n-1}$ and does not contain b_0. By hypothesis, the second term contains b_0 if and only if $c = d$, meaning $i = j$. This establishes the statement of the Lemma for E_n in all cases. ∎

Proof of Theorem 3: Consider the coefficient of b_0 in $(b_i b_j) b_k$. By the Lemma, it is the coefficient of b_k in $b_i b_j$. Since

$$(b_i b_j)b_k = (b_i b_k)b_j$$

it is also the coefficient of b_j in $b_i b_k$. ■

Corollary 1: Let $i \oplus j$ be the mod 2 sum of i and j as bit vectors. The coefficient of $b_{i\oplus j}$ in $b_i b_j$ is one.

Proof: Let $i \cap j$, $i \cup j$ be the bitwise AND, bitwise OR of i and j, respectively. It will be shown that the coefficient of b_0 in $b_{i\oplus j} b_i b_j$ is one which, together with the Lemma proves the Corollary. Now, by rearranging terms,

$$b_{i\oplus j} b_i b_j = (b_{i\oplus j} b_{i\cap j})^2 = (b_{i\cup j})^2,$$

and by the Lemma, this contains a b_0 in its expansion. ■

The following corollary is an immediate consequence of the Lemma.

Corollary 2: For any $a \in E_n$, a^2 contains b_0 in its expansion if and only if a is the sum of an odd number of basis elements.

3. MINIMAL POLYNOMIALS

The minimal polynomials over $GF(2)$ of the x_n are quite easy to compute. Starting with $p_0(y) = y^2 + y + 1$, let $p_1(y) = y^2 p_0(y + y^{-1})$ and, in general, $p_n(y) = y^{2^n} p_n(y + y^{-1})$. It is clear that $p_n(x_n) = 0$ for all n because

$$p_{k+1}(x_{k+1}) = x_{k+1}^{2^{k+1}} p_k(x_k) = 0.$$

Since p has degree 2^{n+1}, it is the minimal polynomial of x_n. The following result gives a method for computing the p_n which is probably better suited to calculation.

Theorem 4: Let sequences of polynomials $a_n(y)$ and $b_n(y)$ be defined as follows:

$$a_0 = 1 + y^2,\ b_0 = y \text{ and } a_{n+1} = a_n^2 + b_n^2,\ b_{n+1} = a_n b_n, \text{ for } n = 1, 2, 3, \ldots .$$

Then $a_n + b_n$ is the minimal polynomial of x_n.

Proof: Let $x_{-1} = 1$ and observe that, for $n \geqslant 0$, $y = x_{n+1}$ is a root of $a_0 + x_n b_0$ and, therefore, a root of

$$(a_0 + x_n b_0)(a_0 + x_n^{-1} b_0) = a_1 + x_{n-1} b_1.$$

If $n \geqslant 1$, $y = x_{n+1}$ is a root of

$$(a_1 + x_{n-1} b_1)(a_1 + x_{n-1}^{-1} b_1) = a_2 + x_{n-2} b_2.$$

After repeating this $n+1$ times, we see that $y = x_{n+1}$ is a root of $a_{n+1} + b_{n+1}$. It follows from the definition that a_n has degree 2^{n+1} and that b_n has degree

$2^{n+1} - 1$. Thus, $a_n + b_n$ has degree 2^{n+1} with x_n as a root, so it must be the minimal polynomial of x_n. ■

4. EXPERIMENT

The numbers F_0, F_1, F_2, F_3, F_4 are prime so, by the Corollary to Theorem 1, x_n has order F_n for $n \leqslant 4$. In addition, using the complete factorizations [4, 5] of F_n for $5 \leqslant n \leqslant 8$, it has been checked on a computer that $x_{n_k} \neq 1$ for any proper divisor k of F_n for $n \leqslant 8$. It would be desirable to know whether x_n always has order F_n. If this is true, then $y_n = x_{n-1} \ldots x_0$ is primitive. It would be useful to have a good way to compute the minimal polynomials of the y_n.

5. A FIELD USED BY CONWAY

J. H. Conway has given an iterated quadratic extension [6, 7] of $GF(2)$ that comes from the theory of Nim-like games. In our terminology, this extension would be defined by

$$c_n^2 + c_n = c_{n-1} \ldots c_0 \text{ for } n \geqslant 1 \quad\text{and}\quad c_0^2 + c_0 = 1.$$

It is well known that any two finite fields of the same order are isomorphic. However, we do not yet know of an explicit isomorphism between $GF(2)(x_n)$ and $GF(2)(c_n)$.

ACKNOWLEDGMENT

The author would like to thank Norman Herzberg and Neal Zierler for their assistance.

REFERENCES

1. R. Lidl & H. Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge: Cambridge University Press, 1986.
2. E. R. Berlekamp. *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.
3. G. H. Hardy & E. M. Wright. *The Theory of Numbers*. Oxford: Oxford University Press, 1971. Fourth Edition.
4. R. P. Brent & J. M. Pollard. "Factorization of the Eighth Fermat Number." *Math. Comp.* *36* (1981):627-630.
5. J. C. Hallyburton, Jr., & J. Brillhart. "Two New Factors of Fermat Numbers." *Math. Comp.* *29* (1975):109-112; see also Corrigenda, *Math. Comp.* *30* (1976):198.
6. J. H. Conway. *On Numbers and Games*. New York: Academic Press, 1976.
7. J. H. Conway & N. J. A. Sloane. "Lexicographic Codes: Error-Correcting Codes from Game Theory." *IEEE Transactions on Information Theory* *32* (May 1986).

◆◇◆◇◆

A NOTE ON THE PRIMALITY OF $6^{2^n} + 1$ AND $10^{2^n} + 1$

H. C. WILLIAMS*

University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2

(Submitted November 1986)

1. INTRODUCTION

In 1877, Lucas [3] presented the first practical test for the primality of the Fermat numbers $F_n = 2^{2^n} + 1$. We give a version of this test below, using the slightly modified form which Lucas used later in [5, p. 313] and with some minor errors corrected.

Test (T1.1) for the Primality of $F_n = 2^{2^n} + 1$ $(r = 2^n)$

Let $S_0 = 6$ and define $S_{i+1} = S_i^2 - 2$. F_n is a prime when $F_n \mid S_{r-1}$; F_n is composite if $F_n \nmid S_i$ for all $i \leqslant r - 1$. Finally, if t is the least subscript for which $F_n \mid S_t$, the prime divisors of F_n must have the form $2^{t+1}q + 1$.

Three weeks after Lucas' announcement of this test, Pepin [8] pointed out that the test was possibly not effective; that is, it might happen that a prime F_n would divide S_t, where t is too small for the primality of F_n to be proved. He provided the following effective primality test.

Test (T1.2) for the Primality of F_n

Let $S_0 = 5^2$ and define $S_{i+1} \equiv S_i^2 \pmod{F_n}$. F_n is a prime if and only if $S_{r-1} \equiv -1 \pmod{F_n}$.

Pepin also noted that his test would be valid with $S_0 = 10^2$.

Somewhat later, Proth [9], [10] gave, without a complete proof, another effective test for the primality of F_n. His test is essentially that of Pepin with $S_0 = 3^2$. The proof of Proth's test was completed by Lucas [7], who also noted [5, p. 313] that Pepin's test would be valid for $S_0 = a^2$ when the Jacobi symbol $(a/F_n) = -1$.

While effective tests for the primality of F_n have been known for almost 100 years, little seems to have been done concerning the development of effec-

Research supported by NSERC of Canada, Grant #A7649.

tive tests for the primality of other integers of the form $(2a)^{2^n}+1$. The two smallest values of a after 1 for which this form could possibly yield primes distinct from the Fermat numbers are $a=3$ and $a=5$. Riesel [11] denoted these numbers by $G_n = 6^{2^n}+1$ and $H_n = 10^{2^n}+1$; he also provided a small table of factors for some of these numbers. Now G_n is of the form $A3^r+1$ and H_n is of the form $2A5^r+1$. These are forms of integers for which Lucas [4], [5], [6] presented primality tests. These tests, which are given in a modified and corrected form (there are several errors in Lucas' statements of these tests) make use of the Fibonacci numbers $\{U_m\}$, where $U_0 = 0$, $U_1 = 1$, and $U_{k+1} = U_k + U_{k-1}$. Note that neither Test T1.3 nor Test T1.4 is an effective test for the primality of N.

Test (T1.3) for the Primality of $A3^r+1$

Let $N = A3^r+1$ with $N \equiv \pm 1 \pmod{10}$. Put $S_0 \equiv U_{3A}/U_A \pmod{N}$ and define

$$S_{k-1} \equiv S_k^3 - 3S_k^2 + 3 \pmod{N}. \tag{1.1}$$

N is a prime when $N|S_{r-1}$; if t is the least subscript such that $N|S_t$, the prime factors of N must be of the form $2q3^{t+1}+1$ or $2q3^{t+1}-1$.

There are a number of puzzling aspects of this test. First, why did Lucas restrict himself to a test for numbers $N \equiv \pm 1 \pmod 5$? Of course, as we shall see below, it is necessary for $N \equiv \pm 1 \pmod 5$ in order to use the Fibonacci numbers in a primality test for N, but other Lucas sequences could also be used. For example, if $N \equiv -1 \pmod 4$, we could use $P = 4$, $Q = 1$; if $N \equiv 5 \pmod 8$, we could use $P = 10$, $Q = 1$; and if $N \equiv 1 \pmod 8$, we could use $P = 6$, $Q = 1$ (see Section 2). It may be that because of Lucas' great interest in Fibonacci numbers, he restricted his values of N to those that could be tested by making use of them. Also, why did Lucas give this test in a form which, unlike T1.1 and T1.4, does not allow for the inclusion of a test for the compositeness of N? Finally, to the author's knowledge, nowhere among the vast number of identities that Lucas developed for the Lucas functions does he mention the simple identity on which (1.1) is based.

Lucas also gave:

Test (T1.4) for the Primality of $N = 2A5^r+1$

Put $S_0 \equiv U_A \pmod{N}$ and define $S_{k+1} \equiv 25S_k^5 + 25S_k^3 + 5S_k \pmod{N}$. N is a prime when the first S_k divisible by N is S_r; if none of the S_i ($i \leqslant r$) is divisible by N, N is composite; if t is the least subscript such that $N | S_t$, then the prime factors of N must be of the form $2q5^t + 1$ or $2q5^t - 1$.

The purpose of this paper is to derive tests for the primality of G_n and H_n, which are very much in the spirit of Lucas' test for the primality of F_n. We will do this by modifying tests T1.3 and T1.4. Further, like Pepin's test, our tests will be effective. In order to achieve this, we shall be guided by the methods developed by Williams [12], [13], and [14]. It should be mentioned here that the techniques we use here could also be applied, as in the manner of [14], to other numbers of the form $Ar^n + 1$.

2. SOME PROPERTIES OF THE LUCAS FUNCTIONS

In order to develop primality tests for G_n and H_n, we will require some properties of the Lucas functions V_n and U_n. Most of these properties are well known and are included here for reference.

Let α, β be the zeros of $x^2 - Px + Q$, where P, Q are coprime integers. We define

$$V_n = \alpha^n + \beta^n,\ U_n = (\alpha^n - \beta^n)/(\alpha - \beta), \tag{2.1}$$

and put $\Delta = (\alpha - \beta)^2 = P^2 - 4Q$. The following identities can be found in [5] or verified by direct substitution from (2.1):

$$V_n^2 - \Delta U_n^2 = 4Q^n, \tag{2.2}$$
$$V_{2n} = V_n^2 - 2Q^n, \tag{2.3}$$
$$U_{2n} = U_n V_n, \tag{2.4}$$
$$V_{3n} = V_n(V_n^2 - 3Q^n), \tag{2.5}$$
$$U_{3n} = U_n(\Delta U_n^2 + 3Q^n), \tag{2.6}$$
$$U_{3n} = U_n(V_n^2 - Q^n), \tag{2.7}$$
$$V_{5n} = V_n(V_n^4 - 5Q^n U_n^2 + 5Q^{2n}), \tag{2.8}$$
$$U_{5n} = U_n(\Delta^2 U_n^4 + 5Q^n \Delta U_n^2 + 5Q^{2n}), \tag{2.9}$$
$$U_{5n} = U_n(V_n^4 - 3Q^n V_n^2 + Q^{2n}). \tag{2.10}$$

If we put $X_n = U_{3n}/U_n$, then

$$X_n = \Delta U_n^2 + 3Q^n, \tag{2.11}$$

by (2.6), and

$$X_{3n} = \Delta U_{3n}^2 + 3Q^{3n} = \Delta U_n^2 X_n^2 + 3Q^{3n} = X_n^2(X_n - 3Q^n) + 3Q^{3n},$$

by (2.11). Hence,

$$X_{3n} = X_n^3 - 3Q^n X_n^2 + 3Q^{3n}; \tag{2.12}$$

also

$$X_{2n} = U_{6n}/U_{2n} = (U_{3n}/U_n)(V_{3n}/V_n) = X_n(X_n - 2Q^n),$$

by (2.4), (2.5), and (2.2). Hence, by (2.12), we get

$$X_{6n} = X_n^3(X_n - 2Q^n)^3 - 3Q^{2n}X_n^2(X_n - 2Q^n)^2 + 3Q^{6n}. \tag{2.13}$$

To obtain a result analogous to (2.12) for $Y_n = U_{5n}/U_n$, we note that

$$Y_n = \Delta^2 U_n^4 + 5Q^n\Delta U_n^2 + 5Q^{2n},$$

by (2.9); thus,

$$\begin{aligned} Y_{5n} &= \Delta^2 U_n^4 Y_n^4 + 5Q^{5n}\Delta U_n^2 Y_n^2 + 5Q^{10n} \\ &= Y_n^4(Y_n - 5Q^n\Delta U_n^2 - 5Q^{2n}) + 5Q^{5n}\Delta U_n^2 Y_n^2 + 5Q^{10n}. \end{aligned}$$

We get

$$Y_{5n} = Y_n^5 + 5Q^n(Q^n - \Delta U_n^2)Y_n^4 + 5Q^{5n}\Delta U_n^2 Y_n^2 + 5Q^{10n}. \tag{2.14}$$

For the development of one of our tests, it will be convenient to define

$$W_n \equiv V_{2n}Q^{-n} \pmod{N}. \tag{2.15}$$

Here the modulus N is assumed to be coprime to Q. From (2.8) and (2.2), we get

$$W_{10n} \equiv W_n^2(W_n^3 - 5W_n^2 + 5)^2 - 2 \pmod{N}. \tag{2.16}$$

Also, by (2.10), we have

$$(U_{10n}/U_{2n})Q^{-4n} \equiv W_n^4 - 3W_n^2 + 1 \pmod{N}. \tag{2.17}$$

We will also require some standard number-theoretic properties of the Lucas functions. We list these as a collection of theorems together with appropriate references. We let p be an odd prime and put

$$\varepsilon = (\Delta/p),\ \eta = (Q/p),$$

where $(\cdot/p)$ is the Legendre symbol.

Theorem 2.1 (Carmichael [1], Lehmer [2]): If $p \nmid \Delta Q$, then $p \mid U_{p-\varepsilon}$. □

Theorem 2.2 (Lehmer [2]): If $p \nmid \Delta Q$, then $p \mid U_{(p-\varepsilon)/2}$ if and only if $\eta = 1$. □

Theorem 2.3 (Carmichael [1], p. 51): The g.c.d. of U_{pn}/U_n and U_n divides p. (This result is true as well for $p = 2$.) □

Theorem 2.4: Let g.c.d.$(N, 2pQ) = 1$. If $p \mid m$, $N \mid U_m$, and g.c.d.$(U_{m/p}, N) = 1$, then the prime factors of N must be of the form $kp^\nu \pm 1$, where ν is the highest power to which p occurs as a factor of m ($p^\nu \| m$). □

By combining Theorem 2.4 with Theorem 2.3, we get the following

Corollary: If g.c.d.$(N, 2pQ) = 1$ and

$$U_{pn}/U_n \equiv 0 \pmod{N},$$

then the prime factors of N must be of the form $kp^{\nu} \pm 1$, where $p^{\nu-1} \| m$.

If we put $p = 2$, we have $U_{pk}/U_k = V_k$; hence, $N = F_n$ is a prime if for some P, Q we have $V_{(N-1)/2} \equiv 0 \pmod{N}$. On the other hand, if $N = F_n$ is a prime, we must have $V_{(N-1)/2} \equiv 0 \pmod{N}$ if $N \nmid \Delta Q$, $(\Delta/N) = 1$, and $(Q/N) = -1$. This will certainly be the case if we put $P = a + 1$, $Q = a$ ($\alpha = a$, $\beta = 1$), where $(a/N) = -1$. Thus, $N = F_n$ is a prime if and only if $V_{(N-1)/2} \equiv 0 \pmod{N}$ when $P = a + 1$, $Q = a$, and $(a/N) = -1$. This, of course, is the Pepin ($a = 5, 10$) or the Proth ($a = 3$) test for the primality of F_n.

To extend these ideas to the G_n and the H_n numbers, we must find a result analogous to Theorem 2.2 for $U_{(p-\varepsilon)/3}$ and $U_{(p-\varepsilon)/5}$ when $\varepsilon = 1$. This can be done by using a simple modification of an idea developed in Williams [12] and [13]. We describe this briefly here and refer the reader to [13] for more details. (In [13] we deal with the case $p \equiv -q \equiv 1 \pmod{r}$ only.)

We let p, q, and r be odd primes such that $p \equiv q \equiv 1 \pmod{r}$ and let $K = GF(p^{q-1})$. Write $t = \text{ind}\, m$, where $m \equiv g^t \pmod{q}$ $(0 \leqslant t \leqslant q - 2)$ and g is a fixed primitive root of q. We consider the Gauss sum

$$(\xi, \omega) = \sum_{1}^{q-1} \xi^{\text{ind}\, k} \omega^k,$$

where ξ and ω are, respectively, primitive r^{th} and q^{th} roots of 1 in K. If, as in [13], we let $j = \text{ind}\, p$,

$$q\alpha = (\xi, \omega)^r, \quad q\beta = (\xi^{-1}, \omega)^r,$$

then $\alpha + \beta$, $\alpha\beta \in GF(p)$, and in K,

$$(q\alpha)^{(p-1)/r} = (\xi, \omega)^{p-1} = (\xi, \omega)^{-1}(\xi, \omega\ ) = \xi^{-j}.$$

Thus, if $P \equiv \alpha + \beta \pmod{p}$ and $Q \equiv \alpha\beta \pmod{p}$, then $U_{p-1} \equiv 0 \pmod{p}$. Also

$$U_{(p-1)/r} \not\equiv 0 \pmod{p},$$

if $\quad p^{(q-1)/r} \not\equiv 0, 1 \pmod{q}$.

This result is analogous to Theorem 2.2; however, in order for it to be useful, we must be able to compute values for $\alpha + \beta$ and $\alpha\beta$. The value of $\alpha\beta$ is simply q^{r-2}, but $\alpha + \beta$ is rather more complicated. It can be written as

$$\alpha + \beta \equiv \sum_{i=0}^{(r-3)/2} C(i, r, q) R^i \pmod{p}, \tag{2.18}$$

where the coefficients $C(i, r, q)$ are independent of p, and R can be any solution of a certain polynomial congruence (modulo p). In the case of $r = 3$, R does not occur in (2.18); in the case of $r = 5$, R can be any solution of

$$x^2 + x - 1 \equiv 0 \pmod{p}.$$

For more details on R and tables of $C(i, r, q)$, we refer the reader to [12] and [14]. Here, it is sufficient to note that $C(0, 3, 7) = 1$, $C(0, 5, 11) = -57$, and $C(1, 5, 11) = -25$.

3. THE PRIMALITY TESTS

It is evident from the results in Section 2 that it is a very simple matter to develop a sufficiency test for the primality of numbers like G_n and H_n. One need only select some integer a such that g.c.d.$(a, N) = 1$, put $P = a + 1$, $Q = a$, and determine whether

$$U_{N-1}/U_{(N-1)/r} \equiv 0 \pmod{N}. \tag{3.1}$$

Here, $r = 3$ for $N = G_n$ and $r = 5$ for $N = H_n$. If (3.1) holds, N is a prime; however, if (3.1) does not hold, we have no information about N and must select another value for a. In practical tests for the primality of these numbers we would use, instead of (3.1), the two conditions

$$\text{g.c.d.}(a^{(N-1)/r} - 1, N) = 1 \tag{3.2a}$$

and

$$a^{N-1} \equiv 1 \pmod{N}. \tag{3.2b}$$

In this case, if (3.2a) and (3.2b) hold, then (3.1) holds; if (3.2b) does not hold, N is composite. Also, if N is a prime, the first value of a selected (by trial) usually causes both (3.2a) and (3.2b) to hold. Nevertheless, this test is not effective, in that we cannot give *a priori* a value for a such that, if N is a prime, (3.2a) and (3.2b) must hold.

We will now give effective tests for the primality of G_n and H_n. We first note that, since $(\Delta/G_n) = (5/G_n) = (2/5) = -1$, we cannot use the Fibonacci numbers in a test for the primality of G_n. However, we can still give a very simple test like Test T1.2 for the primality of G_n.

Let $N = G_n$. By the results at the end of the last section we know that if $P = 1$ and $Q = 7$ then, since $N^2 \not\equiv 0, 1 \pmod{7}$, we must have

$$U_{N-1}/U_{(N-1)/3} \equiv 0 \pmod{N}$$

when N is a prime. Also, under the assumption that N is a prime,

$$(Q/N) = (7/N) = (N/7) = (2/7) = 1 \quad \text{and} \quad U_{(N-1)/2} \equiv 0 \pmod{N}$$

by Theorem 2.2. Further, since $U_{(N-1)/3} \not\equiv 0 \pmod{N}$, we cannot have $U_{(N-1)/6} \equiv 0 \pmod{N}$ by (2.4); hence,

$$U_{(N-1)/2}/U_{(N-1)/6} \equiv 0 \pmod{N}. \tag{3.3}$$

If we define $Z_m \equiv (U_{3m}/U_m)Q^{-m} = X_m Q^{-m} \pmod{N}$, then by (2.13) we have

$$Z_{6m} \equiv Z_m^3(Z_m - 2)^3 - 3Z_m^2(Z_m - 2)^2 + 3 \pmod{N}.$$

by putting $S \equiv Z_{6^k} \pmod{N}$, we have

$$S_{k+1} \equiv S_k^3(S_k - 2)^3 - 3S_k^2(S_k - 2)^2 + 3 \pmod{N}. \tag{3.4}$$

If $r = 2^n$, then

$$S_{r-1} \equiv (U_{(N-1)/2}/U_{(N-1)/6})Q^{-(N-1)/6} \pmod{N}. \tag{3.5}$$

It follows that, if $S_r \equiv 0 \pmod{N}$, then any prime factor of N must have the form $k3^{2^n} \pm 1$. Since $(2 \cdot 3^{2^n} - 1)^2 > N$, we see that N must be a prime.

Now,

$$S_0 = Z_1 \equiv (U_3/U_1)Q^{-1} \pmod{N} \quad \text{and} \quad U_3/U_1 = P^2 - Q;$$

hence,

$$S_0 \equiv P^2Q^{-1} - 1 \equiv 7^{-1} - 1 \equiv 3(N - 2)/7 \pmod{N}. \tag{3.6}$$

Thus, by combining the results (3.6), (3.4), (3.5), (3,3), and the theorems of Section 2, we get the following necessary and sufficient primality test for G_n:

<u>Primality Test (T3.1) for $N = 6^{2^n} + 1$ $(r = 2^n)$</u>

1. Put $S_0 = 3(N - 2)/7$ and define

$$S_{k+1} \equiv S_k^3(S_k - 2)^3 - 3S_k^2(S_k - 2)^2 + 3 \pmod{N}.$$

2. N is a prime if and only if

$$S_{r-1} \equiv 0 \pmod{N}.$$

Unfortunately, because of the difficulty in finding R, the primality test which we shall develop for H_n is not as simple or elegant as T3.1. Also, the formula (2.14) for Y_{5n} is not as simple as (2.12); that is, we cannot express Y_{5n} in terms of a simple polynomial in Y_n and Q^n only. However, in this case, we can directly integrate Lucas' Test T1.4 into an effective test for the primality of H_n.

Let $N = H_n$. Since $N^2 \not\equiv 0, 1 \pmod{11}$, by the results at the end of Section 2 we know that, if N is a prime, then

$$U_{N-1}/U_{(N-1)/5} \equiv 0 \pmod{N} \tag{3.7}$$

when $P \equiv -57 - 25R \pmod{N}$, $Q = 11^3 = 1331$, and

$$R^2 + R - 1 \equiv 0 \pmod{N}. \tag{3.8}$$

If we put $T_k \equiv W_{10^k} \pmod{N}$, by (2.16) we get

$$T_{k+1} \equiv T_k^2(T_k^4 - 5T_k^2 + 5)^2 - 2 \pmod{N}. \tag{3.9}$$

Hence, if $r = 2^n$, we also get

$$T_{r-1} \equiv W_{(N-1)/10} \equiv V_{(N-1)/5}Q^{-(N-1)/10} \pmod{N}.$$

It follows from (2.17) that (3.7) holds if and only if

$$T_{r-1}^4 - 3T_{r-1}^2 + 1 \equiv 0 \pmod{N}. \tag{3.10}$$

As mentioned above, the difficulty in using this as a test for the primality of H_n resides in the fact that we do not usually know *a priori* a value for R. We can, however, apply the noneffective Test T1.4 of Lucas. If this succeeds, we need not use the result above; but, even if it fails, it will provide us with a value for R and then we can use a test that we know is effective.

We note that in Lucas' test we have $P = 1$, $Q = -1$. Hence,

$$\varepsilon = (\Delta/N) = (5/N) = 1, \quad \eta = (Q/N) = 1,$$

and

$$U_{(N-1)/2} \equiv 0 \pmod{N} \tag{3.11}$$

when N is a prime.

Define

$$X_i \equiv V_{2^i} \pmod{N}$$
$$Y_i \equiv U_{2^i} \pmod{N} \quad (i \geqslant 1).$$

By (2.3) and (2.4), we have

$$Y_{i+1} \equiv Y_i X_i, \quad X_{i+1} \equiv X_i^2 - 2 \pmod{N}. \tag{3.12}$$

Also, by (2.2),

$$X_i^2 - 5Y_i^2 \equiv 4 \pmod{N}. \tag{3.13}$$

If we put $H_n = 2A5^r + 1$ $(r = 2^n)$, then $A = 2^{r-1}$ and

$$U_A \equiv Y_{r-1} \equiv \prod_{i=0}^{r-2} X_i \pmod{N} \tag{3.14}$$

by (2.4). Thus, if N is a prime and $N | U_A$, we must have

$$X_m \equiv 0 \pmod{N} \tag{3.15}$$

for some $1 < m \leqslant r - 2$ $(X_1 = V_2 = 3)$. Hence, by using (3.15) and (3.13), we see that

$$R \equiv 25(2 + 5 \cdot 10^{r/2}Y_m)10^{r-2} \pmod{N} \tag{3.16}$$

is a solution of (3.8).

Put

$$S_0 \equiv Y_{r-1} \pmod{N} \tag{3.17}$$

and define

$$S_{k+1} \equiv 25S_k^5 + 25S_k^3 + 5S_k \pmod{N}. \tag{3.18}$$

Using (2.9) we see that $S_k \equiv U_{A5^k} \pmod{N}$. If N is a prime, by (3.11) we must have $S_r \equiv 0 \pmod{N}$. If $S_0 \not\equiv 0 \pmod{N}$, then, for some $t < r$, we have

$$S_t \not\equiv 0 \pmod{N} \quad \text{and} \quad S_{t+1} \equiv 0 \pmod{N}.$$

By (3.18) we find that

$$R \equiv 5S_t^2 + 2 \pmod{N} \tag{3.19}$$

is a solution of (3.8). Also, if $(2 \cdot 5^{t+1} - 1)^2 > N$, then, by the Corollary of Theorem 2.4, we know that N is a prime.

We are now able to assemble this information and use (3.12), (3.16)-(3.19), (3.9) and (3.10) to develop the following test.

Primality Test (T3.2) for $H_n = 10^{2^n} + 1$ $(r = 2^n)$

1. Put $X_1 = 3$, $Y_1 = 1$ and define

$$Y_{k+1} \equiv Y_k X_k \pmod{N},$$
$$X_{k+1} \equiv X_k^2 - 2 \pmod{N}.$$

2. If $X_m \equiv 0 \pmod{N}$ for some $m \leqslant r - 2$, put

$$R \equiv 25(2 + 5 \cdot 10^{r/2} Y_m)10^{r-2} \pmod{N}$$

and go directly to step 5; otherwise,

3. Put $S_0 \equiv Y_{r-1} \pmod{N}$ and define

$$S_{k+1} \equiv 25S_k^5 + 25S_k^3 + 5S_k \pmod{N}.$$

4. Find some $t < r$ such that

$$S_{t+1} \equiv 0 \pmod{N} \text{ and } S_t \not\equiv 0 \pmod{N}.$$

If no such t exists, then N is composite and our test ends. If

$$(2 \cdot 5^{t+1} - 1)^2 > N,$$

then N is a prime and our test ends. If

$$(2 \cdot 5^{t+1} - 1)^2 < N,$$

put

$$R \equiv 5S_t^2 + 2 \pmod{N}.$$

5. Put

$$T_0 \equiv (57 + 25R)^2((5N + 1)/11)^3 - 2 \pmod{N}$$

and define

$$T_{k+1} \equiv T_k^{10} - 10T_k^8 + 35T_k^6 - 50T_k^4 + 25T_k^2 - 2 \pmod{N}.$$

6. N is a prime if and only if

$$T_{r-}^4 - 3T_{r-1}^2 + 1 \equiv 0 \pmod{N}.$$

REFERENCES

1. R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$." *Annals of Math.* (2) *15* (1913-1914):30-70.
2. D. H. Lehmer. "An Extended Theory of Lucas' Functions." *Annals of Math.* (2) *31* (1930):419-448.
3. E. Lucas. "Sur la division de la circonference en parties égales." Académie des Sciences de Paris, *Comptes rendues 85* (1877):136-139.
4. E. Lucas. "Considérations nouvelles sur la théorie des nombres premiers et sur la division géométrique de la circonference en parties égales." Assoc. Francaise pour l'Avancement des Sciences, *Comptes Rendues des Sessions*, 1877, pp. 159-167.
5. E. Lucas. "Theorie des functions numériques simplement périodiques." *Amer. J. Math. 1* (1878):184-240, 289-321.
6. E. Lucas. "Sur la série récurrent de Fermat." *Bulletino di Bibliografia e di storia delle Scienze Mathematiche e Fisiche 11* (1878):783-798.
7. E. Lucas. "Question 453." *Nouv. Corresp. Math. 5* (1879):137.
8. P. Pepin. "Sur la formule $2^{2^n}+1$." Académie des Sciences de Paris, *Comptes rendues 85* (1877):329-331.
9. F. Proth. "Mémoires présentés." Académie des Sciences de Paris, *Comptes rendues 87* (1878):374, see also p. 926.
10. F. Proth. "Extrait d'une lettre de M. Proth." *Nouv. Corresp. Math. 4* (1878):210-211.
11. H. Riesel. "Some Factors of the Numbers $G_n = 6^{2^n} + 1$ and $H_n = 10^{2^n} + 1$." *Math. Comp. 23* (1969):413-415; Corrigenda, *Math. Comp. 24* (1970):243.
12. H. C. Williams. "An Algorithm for Determining Certain Large Primes." *Congressus Numerantium III, Proc. of the Second Louisiana Conf. on Combinatorics, Graph Theory and Computing*, Utilitas Mathematica, Winnipeg, 1971, pp. 533-556.
13. H. C. Williams. "A Class of Primality Tests for Trinomials Which Include the Lucas-Lehmer Test." *Pacific J. Math. 98* (1982):477-494.
14. H. C. Williams. "Effective Primality Tests for Some Integers of the Forms $A5^n - 1$ and $A7^n - 1$." *Math. Comp.* (To appear.)

◆◇◆◇◆

SUPPOSE MORE RABBITS ARE BORN

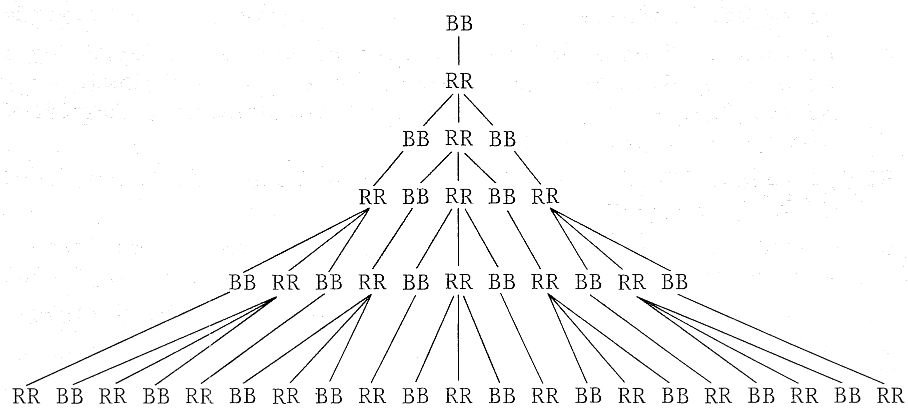
SHARI LYNN LEVINE
Student, Half Hollow Hills H.S. East, Dix Hills, NY 11746

(Submitted November 1986)

How would Fibonacci's age-old sequence be redefined if, instead of bearing one pair of baby rabbits per month, the mature rabbits bear two pairs of baby rabbits per month? The answer is an intriguing sequence that has led to the development of what are herein defined as "multi-nacci sequences of the order q," where q is the number of rabbit pairs per litter. Table 1 illustrates the sequence with $q = 2$.

Table 1

Pair Sequence	Month
1	1
1	2
3	3
5	4
11	5
21	6
43	7



Key: RR = Pair of rabbits ready to reproduce
BB = Pair of bunnies (immature rabbits)

Call this sequence the "Beta-nacci sequence"; note that each term can be generated by adding the preceding term to twice the one before that, i.e.,

$$B_n = B_{n-1} + 2B_{n-2}.$$

Using a similar process, sequences can be developed for situations when 3, 4, 5, and 6 rabbit pairs per litter are born. Call these multi-nacci sequences Gamma-, Delta-, Epsi-, and Zeta-nacci sequences, respectively. Table 2 illustrates the first seven terms in each of these multi-nacci sequences and the general formulas for each sequence.

Table 2

Beta-nacci		Gamma-nacci		Delta-nacci		Epsi-nacci		Zeta-nacci	
n	B_n	n	G_n	n	D_n	n	E_n	n	Z_n
0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1
2	1	2	1	2	1	2	1	2	1
3	3	3	4	3	5	3	6	3	7
4	5	4	7	4	9	4	11	4	13
5	11	5	19	5	29	5	41	5	55
6	21	6	40	6	65	6	96	6	133
7	43	7	97	7	181	7	301	7	463
$B_{n-1} + 2B_{n-2}$		$G_{n-1} + 3G_{n-2}$		$D_{n-1} + 4D_{n-2}$		$E_{n-1} + 5E_{n-2}$		$Z_{n-1} + 6Z_{n-2}$	

SUCCESSIVE TERM RATIOS

When one examines the ratio created from two successive terms of the Fibonacci sequence, as n gets larger, the ratio under investigation approaches the Golden Ratio, $\phi = 1.618033989\ldots$, which is the decimal representation of

$$\phi = (1 + \sqrt{5})/2.$$

For the multi-nacci sequences to be analogous to the Fibonacci sequence, each sequence should also have a unique ratio that is approached when one forms a ratio of one term to its preceding term. Indeed, this is the case. Let S_q = the limit, as $n \to \infty$, of successive term ratios of any multi-nacci sequence of order q. (By this definition, $S_1 = \phi$.) Let ${}_nS_q$ = the successive term ratios of the n^{th} term to its preceding term in any multi-nacci sequence of order q, e.g., ${}_5S_2 = 2.20$. The Beta-nacci sequence ratio is examined in Table 3.

Table 3

n	B_n	${}_nS_2$*	n	B_n	${}_nS_2$*
1	1		7	43	2.048
2	1	1.000	8	85	1.977
3	3	3.000	9	171	2.012
4	5	1.667	10	341	1.994
5	11	2.200	11	683	2.003
6	21	1.909	12	1365	1.999

**To the nearest thousandth.*

Thus, we can see that for the Beta-nacci sequence $S_2 \to 2$.

It can be shown that for the Gamma-nacci, Delta-nacci, Epsi-nacci, and Zeta-nacci sequences, the following ratios are approached:

Gamma-nacci: $S_3 \rightarrow 2.30277$
Delta-nacci: $S_4 \rightarrow 2.56155$
Epsi-nacci: $S_5 \rightarrow 2.79129$
Zeta-nacci: $S_6 \rightarrow 3.00000$

The technique of the proofs of these ratios is illustrated below using the Gamma-nacci sequence.

Let $A = G_{n-2}$ when n is very large. Then, the next term in the sequence, G_{n-1}, will be approximately $S_3(A)$, and the next term, G_n, will be $(S_3)^2A$.

Remember that, by definition, $G_n = G_{n-1} + 3G_{n-2}$.

But this is $(S_3)^2A = S_3A + 3A$, whose solution is $S_3 = (1 \pm \sqrt{13})/2$.

Disregarding the $-\sqrt{13}$, because there are no negative rabbits,

$S_3 = 2.30277\ldots$.

Note that the equation $(S_3)^2 - S_3 - 3 = 0$ bears a striking resemblance to the equation $(S_1)^2 - S_1 - 1 = 0$ that generates ϕ. In fact, an entire family of equations can be created which when solved yield the ratios indicated earlier. Specifically, the general equation is $(S_q)^2 - S_q - q = 0$, and the ratio

$S_q = (1 + \sqrt{1 + 4q})/2$.

SPECIAL RECIPROCAL PROPERTIES

One special property of the Golden Ratio is that it is its own reciprocal after one has been subtracted from it. With the multi-nacci sequences, some more general questions can be investigated, such as: "What number, when one is subtracted from it, is twice its own reciprocal, or three times its own reciprocal, or four times its own reciprocal?" The answers, in this order, are the Beta-nacci, Gamma-nacci, and Delta-nacci successive term ratios: S_2, S_3, and S_4, respectively.

The proof of a generalized version of this question is very straightforward.

$$
\begin{aligned}
(S_q)^2 - S_q - q &= 0 \\
(S_q)^2 &= S_q + q \\
S_q &= 1 + \frac{q}{S_q} \\
(S_q - 1) &= q\left(\frac{1}{S_q}\right)
\end{aligned}
$$

Thus, the special reciprocal property of the Fibonacci sequence is but one of a more general set of reciprocal properties of the ratio limits of the multi-nacci sequences.

BETA-NACCI SEQUENCE PROPERTIES

In particular, the Beta-nacci sequence has been given additional examination because it appears to have many interesting properties.

Table 4

n	B_n	$2B_n$	2^n	$\sum_{n=0}^{n} B_n$	$(B_n)^2$	$(B_{n-1})(B_{n+1})$
0	0	0	1	0	0	
1	1	2	2	1	1	0
2	1	2	4	2	1	3
3	3	6	8	5	9	5
4	5	10	16	10	25	33
5	11	22	32	21	121	105
6	21	42	64	42	441	473
7	43	86	128	85	1849	1785
8	85	170	256	170	7225	7353
9	171	342	512	341	29241	28985
10	341	682	1024	682	116281	116793
11	683	1366	2048	1365	466489	465465

Notice that in Table 4 the sum of any two successive terms in the B_n column is a power of 2, or

$$B_n + B_{n-1} = 2^{n-1}. \tag{1}$$

The $\sum_{n=0}^{n} B_n$ column is remarkably like the B_n. In fact,

$$\sum_{n=0}^{n} B_{n-1} = B_n + \frac{(-1)^n - 1}{2}.$$

Examining the $2B_n$ column, it appears that there is a difference of ±1 between the entries in the B_n and $2B_{n-1}$ locations. That is,

$$B_n - 2B_{n-1} = (-1)^{n-1}. \tag{2}$$

Because in the Fibonacci sequence there is a relationship between $(F_n)^2$ and $(F_{n-1})(F_{n+1})$, the Beta-nacci numbers have been examined for a similar relationship. From Table 4 entries, the results of $(B_n)^2 - (B_{n-1})(B_{n+1})$ are +1, -2, +4, -8, +16, -32, +64, -128, +256, -512, and +1024, so that $(B_n)^2 - (B_{n-1})(B_{n+1}) = (-2)^{n-1}$. Fibonacci numbers have the same relationship using the base of (-1) instead of (-2). It can be shown that $(T_n)^2 - (T_{n-1})(T_{n+1}) = (-q)^{n-1}$, where T is any term of a multi-nacci series of order q.

Equation (1) shows that the summation of two successive terms in the Beta-nacci sequence is 1, 2, 4, 8, 16, ... If this sequence is studied, it, too, is observed to be a Beta-nacci-type sequence. For example, 16 = 8 + 2(4). In other words, the powers of 2 are a Beta-nacci sequence. (Interestingly, also, is the fact that the powers of 3 are a Zeta-nacci sequence.) Furthermore, if two terms of the 2, 4, 8, 16, ... sequence are summed, a sequence with the terms 3, 6, 12, 24, 48, ... develops. This is also a Beta-nacci-type sequence, i.e., 24 = 12 + 2(6). In fact, summing two successive terms in any multi-nacci sequence creates a new sequence of the same multi-nacci type.

Moreover, summing three successive terms of the Beta-nacci sequence creates the sequence 2, 5, 9, 19, 37, 75, 149, ..., which is yet another Beta-nacci-type sequence, i.e., 37 = 19 + 2(9). Summing any number of successive terms in any multi-nacci sequence results in a new multi-nacci sequence of the same type:

If T_n is the n^{th} term of any type of multi-nacci sequence, then

$$\begin{aligned}
T_n &= T_{n-1} &&+ qT_{n-2}\\
T_{n+1} &= T_n &&+ qT_{n-1}\\
T_{n+2} &= T_{n+1} &&+ qT_n\\
T_{n+3} &= T_{n+2} &&+ qT_{n+1}\\
&\vdots && \vdots\\
T_{n+m} &= T_{n+m-1} &&+ qT_{n+m-2}\\
\sum_{N=n}^{m} T_N &= \sum_{N=n}^{m} T_{N-1} &&+ q\sum_{N=n}^{m} T_{N-2}
\end{aligned}$$

Similarly, it can be shown that summing the terms in any two or more non-sequential multi-nacci sequences of the same order results in sums which are also a multi-nacci sequence of the same order.

BETA-NACCI n^{th} TERM

In the past, mathematicians have developed formulas for the n^{th} term of the Fibonacci sequence. This is important because, without such a formula, one must enumerate every single term up to the one in question. Thus, the Beta-nacci sequence has been examined for a formula for the n^{th} term.

Using (1) and (2), as defined,

$$B_n + B_{n-1} = 2^{n-1}$$
$$B_n - 2B_{n-1} = (-1)^{n-1}$$

we have:

$$B_n = 2B_{n-1} + (-1)^{n-1}$$
$$2B_{n-1} + (-1)^{n-1} + B_{n-1} = 2^{n-1}$$
$$3B_{n-1} = 2^{n-1} - (-1)^{n-1}$$

For ease in examination, let $n - 1 = n$, so $3B_n = 2^n - (-1)^n$. Then

$$B_n = \frac{2^n - (-1)^n}{3}.$$

This formula is much less complicated than one for Fibonacci's n^{th} term.

REPEATING UNITS DIGITS

One can observe that the units digits in the Beta-nacci sequence are 1, 1, 3, 5, 1, 1, 3, 5, 1, 1, 3, 5, ... They repeat every four terms. The units digits of the ΣB_n terms also repeat every four terms as 0, 1, 2, 5, 0, 1, 2, 5, etc. In 1963, Dov Jarden showed in [1] that the units digit of the Fibonacci sequence repeats every 60 terms. Thus, in this regard, Beta-nacci is a vast improvement over Fibonacci. All multi-nacci sequences have units digit repeat periods.

RABBIT PAIRS PER LITTER, q	SEQUENCE	UNITS DIGIT REPEAT PERIOD
1	Fibonacci	60
2	Beta-nacci	4
3	Gamma-nacci	24
4	Delta-nacci	6
5	Epsi-nacci	3
6	Zeta-nacci	20
7	Eta-nacci	12
8	Theta-nacci	24
9	Iota-nacci	6
10	Kappa-nacci	1
11	Lambda-nacci	60

Moreover, the sequence of units digit repeat periods 60, 4, 24, 6, 3, 20, 12, 24, 6, 1 now repeats as we get into the higher-order multi-nacci sequences. The determination of the tens digit repeat periods is left to the reader.

CONCLUSIONS

Fibonacci-type sequences develop from multiple rabbit births. This paper demonstrates that these sequences also have interesting properties of their own which are ripe for future study.

REFERENCE

1. Dov Jarden. "On the Periodicity of the Last Digits of the Fibonacci Numbers." *The Fibonacci Quarterly* *1*, no. 4 (1963):21-22.

◆◇◆◇◆

NEW UNITARY PERFECT NUMBERS HAVE AT LEAST NINE ODD COMPONENTS

CHARLES R. WALL
Trident Technical College, Charleston, SC 29411

(Submitted November 1986)

1. INTRODUCTION

We say that a divisor d of an integer n is a *unitary divisor* if

$$\gcd(d, n/d) = 1,$$

in which case we write $d \| n$. By a *component* of an integer we mean a prime power unitary divisor.

Let $\sigma^*(n)$ denote the sum of the unitary divisors of n. Then σ^* is a multiplicative function, and $\sigma^*(p^e) = p^e + 1$ if p is prime and $e \geqslant 1$. Throughout this paper we will let f be the *ad hoc* function defined by $f(n) = \sigma^*(n)/n$.

An integer n is *unitary perfect* if $\sigma^*(n) = 2n$, i.e., if $f(n) = 2$. Subbarao and Warren [2] found the first four unitary perfect numbers, and this author [3] found the fifth. No other such numbers have been found, so at this stage the only known unitary perfect numbers are:

$$6 = 2 \cdot 3,\ 60 = 2^2 3 \cdot 5;\ 90 = 2 \cdot 3^2 5;\ 87360 = 2^6 3 \cdot 5 \cdot 7 \cdot 13;\ \text{and}$$

$$146361946186458562560000 = 2^{18} 3 \cdot 5^4 7 \cdot 11 \cdot 13 \cdot 19 \cdot 37 \cdot 79 \cdot 109 \cdot 157 \cdot 313$$

It is easy to show that any unitary perfect number must be even. Suppose that $N = 2^a m$ is unitary perfect, where m is odd and m has b distinct prime divisors (i.e., suppose that N has b odd components). Subbarao and his co-workers [1] have shown that any new unitary perfect number $N = 2^a m$ must have $a > 10$ and $b > 6$. In this paper we establish the improved bound $b > 8$.

Much of this paper rests on a results in an earlier paper [4]:

> Any new unitary perfect number has an odd component larger than 2^{15} (the smallest candidate is 32771).

Essential to this paper is the ability to find bounds for the smallest unknown odd component of a unitary perfect number. The procedure is laborious but simple, and can be illustrated by an example:

Suppose $N = 2^a 3 \cdot 5 \cdot 7 \cdot 19 \cdot 43 \cdot rqp$ is unitary perfect, where r, q, and p are distinct odd prime powers, $r < q < p$, $a \geqslant 12$, and $p \geqslant 32771$. Then $64 < r < 261$, because

$$f(3 \cdot 5 \cdot 7 \cdot 19 \cdot 43) \cdot (262/261)^4 < 2 < f(3 \cdot 5 \cdot 7 \cdot 19 \cdot 43) \cdot (65/64).$$

Consequently, $r < 2^a$ and $r < 32771$. But $f(2^a) \leqslant 4097/4096$ as $a \geqslant 12$, and

$$f(3 \cdot 5 \cdot 6 \cdot 19 \cdot 43) \cdot (4097/4096) \cdot (32772/32771) \cdot (134/132)^2 < 2,$$

so $64 < r < 133$.

In the interests of brevity, we will simply outline the proofs, omitting repetitive details.

2. SEVEN ODD COMPONENTS

Throughout this section, suppose $N = 2^a vutsrqp$ is unitary perfect, where $p, \ldots, v$ are powers of distinct odd primes, and $v < u < t < s < r < q < p$. Then we know that $a \geqslant 11$ and $p \geqslant 32771$.

Theorem 2.1: $v = 3$, $u = 5$, $t = 7$, and $a \geqslant 12$.

Proof: We have $v = 3$ or else $f(N) < 2$, so there is only one component $\equiv -1 \pmod 3$, and none $\equiv -1 \pmod 9$. But

$$f(2^{11} 3 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 25 \cdot 32771) < 2,$$

so $u = 5$. Then there are no more components $\equiv -1 \pmod 3$, only one $\equiv -1 \pmod 5$, and none $\equiv -1 \pmod{25}$. As a result, a is even, so $a \geqslant 12$. Then $t = 7$, or else $f(N) < 2$. ■

Theorem 2.2: $s = 13$.

Proof: We easily have $s = 13$ or $s = 19$, or else $f(N) < 2$, so suppose $s = 19$. Then $25 < r < 53$. If r is 43 or 37, then (respectively) $64 < q < 66$ or $85 < q < 88$, both of which are impossible. Thus, $r = 31$, so $151 < q < 159$ and then $q = 157$. But then $79 | p$ and $p > 2^{15}$, so $p = 79^c$ with $c \geqslant 3$, whence $79^2 | \sigma^*(2^a)$, which is impossible. ■

Theorem 2.3: $r = 67$.

Proof: We have $N = 2^a 3 \cdot 5 \cdot 7 \cdot 13 \cdot rqp$, $p \geqslant 32771$, and $a \geqslant 12$, so $64 < r < 131$. If $r > 79$, easy contradictions follow.

If $r = 79$, then $341 < q < 377$, so $q = 361$, 367, or 373. But $q = 373$ implies $11 \cdot 17 | p$, a contradiction. If $q = 367$, then $p = 23^c$ with $c \geqslant 4$, so $23^3 | \sigma^*(2^a)$, which is impossible. If $q = 361$, then $p = 181^c$ with $c \geqslant 3$, so $181 | \sigma^*(2^a)$, hence $90 | a$, whence $5^2 | N$, a contradiction.

Finally, if $r = 73$, then $526 < q < 615$ and $37 | qp$, so $p = 37^c$ with $c \geqslant 3$. But $73 \nmid \sigma^*(2^a 37^c)$, so $73 | (q + 1)$, which is impossible.

Theorem 2.4: There is no unitary perfect number with exactly seven odd components.

Proof: If this is so, then $N = 2^a 3 \cdot 5 \cdot 7 \cdot 13 \cdot 67 \cdot qp$. Then $1450 < q < 4353$, so $p \geqslant 32771$, whence $1450 < q < 3037$. Then $a \geqslant 12$ implies $1450 < q < 2413$. Now, $17^3 \| N$ implies $3^3 | N$, so $p = 17^c$ with $c \geqslant 4$. But $17^2 \nmid \sigma^*(2^a)$, or else q is a multiple of 354689, so $17^3 | (q + 1)$, which is impossible. ■

3. EIGHT ODD COMPONENTS

Throughout this section, assume that $N = 2^a wvutsrqp$ is unitary perfect, where $p, \ldots, w$ are powers of distinct odd primes, and $w < v < u < t < s < r < q < p$. Then $a \geqslant 11$ and $p \geqslant 32771$ as before.

Theorem 3.1: $w = 3$, $v = 5$, and $a \geqslant 12$.

Proof: Similar to that for Theorem 2.1. ■

Theorem 3.2: $u = 7$, and $t = 13$ or $t = 19$.

Proof: From $f(2^{12} 3 \cdot 5 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 43 \cdot 32771) < 2$, we have $u = 7$, so there is only one component $\equiv -1 \pmod 7$. Thus, $t \leqslant 31$. If t is neither 13 nor 19, then $t = 31$, so $a \geqslant 14$, and we quickly obtain $s = 37$ and $r = 43$. But then we have $N = 2^a 3 \cdot 5 \cdot 7 \cdot 31 \cdot 37 \cdot 43 \cdot qp$, subject to $121 < q < 125$ and $11 \cdot 19 | qp$, an impossibility. ■

Theorem 3.3: If $t = 19$, then $s = 31$.

Proof: Suppose $N = 2^a 3 \cdot 5 \cdot 7 \cdot 19 \cdot srqp$ with $s < r < q < p$. Then $25 < s < 73$. Easy contradictions follow if $s > 43$.

If $s = 43$, then $64 < r < 133$. If $r = 121$, then $140 < q < 147$, which is impossible. Other choices for r force q and p to be powers of 11 and another odd prime (in some order) with no acceptable choice for q in its implied interval.

If $s = 37$, then $85 < r < 176$, so r is 103, 121, 127, 157, or 163. If r is 157 or 163, there in only one choice for q, and it implies that p is divisible by two different odd primes. If $r = 127$, then $a > 20$ and so $262 < q < 265$, an impossibility. If $r = 121$, then $291 < q < 318$, so q is 307 or 313; but $q = 313$ implies $61 \cdot 157 | p$, and if $q = 307$, then $p = 61^c$ with $c \geqslant 3$, so $61^2 | \sigma^*(2^a)$, whence $5^2 | N$, a contradiction. If $r = 103$, then $502 < q < 583$ and $13 | qp$, so $p = 13$ with $c \geqslant 4$; but $13 \nmid \sigma^*(2^a)$, or else $5^2 | N$, so $13^3 | (q + 1)$, which is impossible. ■

Theorem 3.4: $t = 13$.

Proof: If $t \neq 13$, then $N = 2^a 3 \cdot 5 \cdot 7 \cdot 19 \cdot 31 \cdot rqp$ with $r < q < p$ and $a \geqslant 16$, so $151 < r < 307$. Since $r \not\equiv -1 \pmod 5$, r must be 157, 163, 181, 193, 211, 223, 241, 271, 277, or 283. If r is 271, 241, or 223, there is no prime power in the implied interval for q (note $a \geqslant 20$ if $r = 223$). If r is 283, 277, 211, or 193, the only choices for q require that p be divisible by two distinct primes.

If $r = 163$, then $2202 < q < 2450$, so $p = 41$ with $c \geqslant 4$; thus, $2202 < q < 2281$, and the only primes that can divide $q + 1$ are 2, 7, 19, 31, 41, and 163, but no such q exists. If $r = 181$, then $p = 13^c$ with $c \geqslant 4$, as $942 < q < 985$ and $13 | qp$; but $13 \nmid \sigma^*(2^a)$, or else $5^2 | N$, so $13^3 | (q + 1)$, which is impossible. If $r = 157$, then $79 | qp$ and $4525 < q < 5709$, so $p = 79^c$ with $c \geqslant 3$; however, $79 \nmid \sigma^*(2^a)$, and so $79^2 | (q + 1)$, an impossibility. ■

Corollary: There are no more components $\equiv -1 \pmod 7$, and none $\equiv -1 \pmod{13^2}$.

Theorem 3.5: $s \leqslant 73$.

Proof: We have $N = 2^a 3 \cdot 5 \cdot 7 \cdot 13 \cdot srqp$, and $61 < s < 193$ follows easily, so s is 67, 73, 79, 103, 109, 121, 151, 157, or 163.

If s is 163 or 157, then any acceptable choice of r forces qp to be divisible by two distinct odd primes with no acceptable choice for q in its implied interval. The same occurs with $s = 151$ unless $r = 163$; but if $s = 151$ and $r = 163$, then $358 < q < 398$ and $19 \cdot 41 | qp$, so $q = 19^2$, whence $41 \cdot 181 | p$, an impossibility. If $s = 127$, then $a \geqslant 16$ and, for each r, any acceptable choice for q forces p to be divisible by two distinct primes.

If $s = 121$ and $r \neq 241$, then two known odd primes divide qp and there is no acceptable choice for q in its implied interval. If $s = 121$ and $r = 241$, then $318 < q < 350$ and $61 | qp$, so $p = 61^c$ with $c \geqslant 3$; but $61 \nmid \sigma^*(2^a)$ unless $41 | q$, hence $61^2 | (q + 1)$, which is impossible.

Suppose $s = 109$. Then $156 < r < 328$ and $11 | rqp$, so $11^4 | qp$ as $11^3 \| N$ implies $3^2 | N$. Now, $109 \nmid \sigma^*(2^a)$, or else $5^2 | N$. If $109 | \sigma^*(11^c)$, then $11 \cdot 61 \cdot 1117 | rqp$, an impossibility. Thus, one of q and p is 11^c with $c \geqslant 4$, and the other is a component $\equiv -1 \pmod{109}$, and the least candidate for this component is 2833. Then $156 < r < 175$, so r is 157 or 163. If $r = 163$, then $a \neq 12$, or else $11 \cdot 17 \cdot 41 \cdot 241 | rqp$, so $a \geqslant 14$, whence $11 \cdot 41 | qp$ and $3913 < p < 6100$, an impossibility. If $r = 157$, then $a \geqslant 16$, and $11 \cdot 79 | qp$ and $44000 < q < 300000$, whence $q = 11^5$ and $3^2 | N$, a contradiction.

If $s = 103$ and $r = 271$, then $a \geqslant 16$ and $462 < q < 473$, so $q = 463$ and $17 \cdot 29 | p$, an impossibility. If $s = 103$ and $r \neq 271$, then $r + 1$ includes an odd prime π and the interval for q forces $p = \pi^c$ $(c \geqslant 2)$. But in each case, $\pi | \sigma^*(2^a)$ implies a contradiction, so $\pi^{c-1} | (q + 1)$, an impossibility.

If $s = 79$, then $a \geqslant 16$, as $a = 14$ implies $5^2 | N$, so $341 < r < 695$. Except for $r = 373$, $r + 1$ includes an odd prime π and the interval for q forces $p = \pi^c$

$(c \geqslant 2)$, but in each instance $\pi | \sigma^*(2^a)$ either is impossible or implies conditions on q which cannot be met. If $r = 373$, then $4031 < q < 4944$ and $11 \cdot 17 | qp$, so $q = 17^3$, whence $3^2 | N$, a contradiction. ■

Theorem 3.6: $s = 67$.

Proof: Suppose not: then $N = 2^a 3 \cdot 5 \cdot 7 \cdot 13 \cdot 73 \cdot rqp$, $526 < r < 1232$, and $37 | rqp$. The cases $37^2 \| N$ and $37^3 \| N$ are easily eliminated, so $37^4 | N$. Now, $73 \nmid \sigma^*(2^a 37^c)$, so N has an odd component, not 37^c, which is $\equiv -1 \pmod{73}$, and the two smallest candidates are 1459 and 5839. If $N = 2^a 3 \cdot 5 \cdot 7 \cdot 13 \cdot 73 \cdot 1459 \cdot qp$, then $823 < q < 1032$, but $37 \nmid \sigma^*(2^a)$, or else $5^2 | N$, so $37^3 | (q + 1)$, which is impossible.

Now, call $p = 37^c$ $(c \geqslant 4)$, $q \equiv -1 \pmod{73}$, and $q \geqslant 5839$. Then $526 < r < 674$, so $37 \nmid (r + 1)$. Consequently, $q \equiv -1 \pmod{37^3}$, so $q + 1 \geqslant 2 \cdot 37^3 73$ and, hence, $q \geqslant 7395337$. If $a = 12$ or $a = 14$, then r is in an interval with no prime powers. Therefore, $a \geqslant 16$, so $526 < r < 531$, which forces $r = 529$. Then $a \geqslant 18$, but $a = 18$ implies $5^2 | N$, so $a \geqslant 20$. But then $100000 < q < 240000$ and $53 \cdot 37 | qp$, so $q = 53^3$, which implies $3^2 | N$, a contradiction. ■

Theorem 3.7: There is no unitary perfect number with exactly eight odd components.

Proof: Assume not: then we have $N = 2^a 3 \cdot 5 \cdot 7 \cdot 13 \cdot 67 \cdot rqp$ with $1450 < r < 4825$. Now, $67 \nmid \sigma^*(2^a)$, or else $3^2 | N$. Also, $17 | N$ and $17^2 < r$. But 17 cannot divide N an odd number of times, or else $3^2 | N$, so $17^4 | N$.

We already have $a \geqslant 12$ and a even. The cases $a = 12$ and $a = 14$ are easily eliminated, so $a \geqslant 16$ and then $1450 < r < 3022$.

Note that $67 \nmid \sigma^*(17^c)$, so N has an odd component, not 17^c, which is $\equiv -1$ (mod 67), and the three smallest candidates are 1741, 2143, and 4153. If the component $\equiv -1 \pmod{67}$ exceeds 2143, then $1450 < r < 2375$. Thus, we may require $1450 < r < 2375$ in any event.

We cannot have $17^2 | \sigma^*(2^a)$, or else $17 \cdot 3546898 \cdot 2879347902817 | rqp$, and this is obviously impossible. If $17 | (r + 1)$, then r is 1597, 1801, 2209, or 2311. If $67 | (r + 1)$, then r is 1741 or 2143. If $r + 1$ is divisible by neither 17 nor 67, then we may take $p = 17^c$ $(c \geqslant 4$, so $p \geqslant 83521)$ and $q \equiv -1 \pmod{17^2 67}$, whence $q \geqslant 116177$, so $1450 < r < 1531$. Thus, in any event, r must be one of the following numbers: 1453, 1459, 1471, 1489, 1597, 1741, 1801, 2143, 2209, or 2311. But each of these cases leads to a contradiction, so the theorem is proved. ■

REFERENCES

1. M. V. Subbarao, T. J. Cook, R. S. Newberry, & J. M. Weber. "On Unitary Perfect Numbers." *Delta* 3, no. 1 (Spring 1972):22-26. MR 48#224.

2. M. V. Subbarao & L. J. Warren. "Unitary Perfect Numbers." *Canad. Math. Bull.* 9 (1966):147-153. MR 33#3994.

3. Charles R. Wall. "The Fifth Unitary Perfect Number." *Canad. Math. Bull.* 18 (1975):115-122. MR 51#12690.

4. Charles R. Wall. "On the Largest Odd Component of a Unitary Perfect Number." *The Fibonacci Quarterly* 25 (1987):312-316.

◆◇◆◇◆

A NOTE ON FIBONACCI TREES AND THE ZECKENDORF REPRESENTATION OF INTEGERS

RENATO M. CAPOCELLI*
Oregon State University, Corvalis, OR 97331

(Submitted November 1986)

The *Fibonacci numbers* are defined, as usual, by the recurrence

$$F_0 = 0,\ F_1 = 1,\ F_k = F_{k-1} + F_{k-2},\ k > 1.$$

The *Fibonacci tree of order* k, denoted T_k, can be constructed inductively as follows: If $k = 0$ or $k = 1$, the tree is simply the root 0. If $k > 1$, the root is F_k; the left subtree is T_{k-1}; and the right subtree is T_{k-2} with all node numbers increased by F_k. T_6 is shown in Figure 1. For an elegant role of the node numbers in the Fibonacci search algorithm, the reader is referred to [5].

Fibonacci trees have been studied in detail by Horibe [2], [3]. The aim of this note is to present some additional considerations on Fibonacci tree codes and to explore the relationships existing between the codes and the *Zeckendorf representation* of integers.

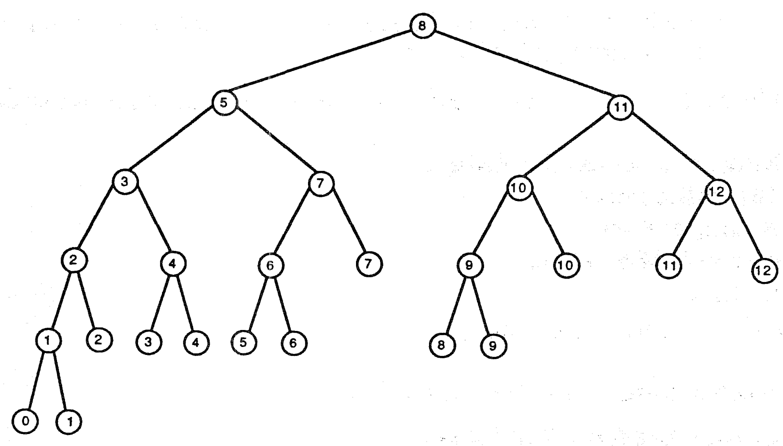


Figure 1. The Fibonacci Tree of Order 6, T_6

---

*On leave from Dipartimento di Informatica ed Applicazioni, Universita' di Salerno, Salerno, Italy 84100.

Work supported by F.O.R.M.E.Z. and by Italian Ministry of Education, M.P.I.

Recall that each integer N, $0 \leqslant N < F_{k+1}$, has the following unique Zeckendorf representation in terms of Fibonacci numbers [6]:

$$N = \alpha_2 F_2 + \alpha_3 F_3 + \alpha_4 F_4 + \cdots + \alpha_k F_k, \text{ where } \alpha_i \in \{0, 1\} \text{ and } \alpha_i \alpha_{i-1} = 0.$$

Let us write this as $\alpha_k \alpha_{k-1} \alpha_{k-2} \ldots \alpha_3 \alpha_2$. The Zeckendorf representation of an integer then provides a binary sequence, called a *Fibonacci sequence*, that does not contain two consecutive ones, and the number of Fibonacci sequences of length $k - 1$ is exactly F_{k+1}.

The Zeckendorf representation of integers perserves the lexicographic ordering based on $0 < 1$ (see [1]).

A *tree code* is the code obtained by labeling each branch of a tree with a code symbol and representing each terminal node with the path of labels from the root to it. We stress that tree codes are *prefix* codes (i.e., no codeword is the beginning of any other codeword) and have a natural encoding and decoding. Moreover, tree codes preserve the order structure of the encoded set in the sense that, if x precedes y, the codeword for x *lexicographically* precedes the codeword for y.

In the sequel, we use 0 for each left branch and 1 for each right branch in a binary tree. The Fibonacci code, denoted C_k, is the binary code obtained in this way from T_k. For example, C_6 is shown in the following table.

0	00000	5	0100	10	101
1	00001	6	0101	11	110
2	0001	7	011	12	111
3	0010	8	1000		
4	0011	9	1001		

The first result of this note is the determination of the asymptotic proportions of zeros and ones in the Fibonacci codes.

Let N_k^0 and N_k^1 denote the total number of 0's and 1's in C_k, respectively, and let $N_k = N_k^0 + N_k^1$ denote the total number of symbols. For example, $N_6^0 = 30$ and $N_6^1 = 20$. Put $p = \lim\limits_{k \to \infty}(N_k^0/N_k)$ and $q = 1 - p = \lim\limits_{k \to \infty}(N_k^1/N_k)$. We will show the following

Theorem 1: $p = \dfrac{1}{\Phi}$ and $q = 1 - \dfrac{1}{\Phi}$, where $\Phi = \lim\limits_{n \to \infty} \dfrac{F_{n+1}}{F_n}$ is the *golden ratio* $\dfrac{1 + \sqrt{5}}{2}$.

Proof: From the inductive construction of the Fibonacci tree and the fact that T_k has F_{k+1} terminal nodes, one has the following equations:

$$N_k = F_{k+1} + N_{k-1} + N_{k-2};$$

$$N_k^0 = F_k + N_{k-1}^0 + N_{k-2}^0;$$
$$N_k^1 = F_{k-1} + N_{k-1}^1 + N_{k-2}^1.$$

These equations, applied recursively, give

$$N_k = \sum_{i=0}^{k-1} F_i F_{k-i+2}, \quad N_k^0 = \sum_{i=0}^{k-1} F_i F_{k-i+1}, \quad N_k^1 = \sum_{i=0}^{k-1} F_i F_{k-i}.$$

Therefrom one gets: $N_k^0/N_k = \sum_{i=0}^{k-1} F_i F_{k-i+1} \Big/ \sum_{i=0}^{k-1} F_i F_{k-i+2}$.

To evaluate the asymptotic behavior of $\sum_{i=0}^{k-1} F_i F_{k-i+j}$, we use Binet's formula

$$F_k = \frac{1}{\sqrt{5}}(\Phi^k - \Gamma^k), \text{ where } \Gamma = \frac{1-\sqrt{5}}{2}.$$

We then have

$$\begin{aligned}\sum_{i=0}^{k-1} F_i F_{k-i+j} &= \frac{1}{5}\left(\sum_{i=0}^{k-1} \Phi^{k+j} + \sum_{i=0}^{k-1} \Gamma^{k+j} - \sum_{i=0}^{k-1} \Phi^i \Gamma^{k-i+j} - \sum_{i=0}^{k-1} \Phi^{k-i+j}\Gamma^i\right)\\
&= \frac{1}{5}\left(k\Phi^{k+j} + k\Gamma^{k+j} - \Gamma^{j+1}\frac{\Gamma^k - \Phi^k}{\Gamma - \Phi} - \Phi^{j+1}\frac{\Phi^k - \Gamma^k}{\Phi - \Gamma}\right)\\
&= \frac{1}{5}\left(k\Phi^{k+j} + k\Gamma^{k+j} - \frac{\Gamma^{j+1}}{\sqrt{5}}(\Phi^k - \Gamma^k) - \frac{\Phi^{j+1}}{\sqrt{5}}(\Phi^k - \Gamma^k)\right)\\
&= \frac{1}{5}k\Phi^{k+j} + O(\Phi^k).\end{aligned}$$

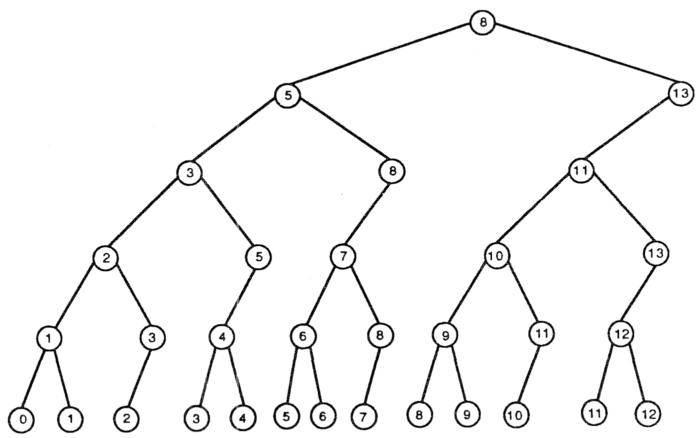


Figure 2. The Uniform Fibonacci Tree of Order 6, U_6

From the above, one finally obtains

$$\lim_{k\to\infty} \frac{N_k^0}{N_k} = \lim_{k\to\infty} \frac{\sum_{i=0}^{k-1} F_i F_{k-i+1}}{\sum_{i=0}^{k-1} F_i F_{k-i+2}} = \frac{1}{\Phi}. \blacksquare$$

The remainder of this note is devoted to exploring relationships between the Fibonacci codes and the Zeckendorf representation of integers. In particular, we show that the Zeckendorf representation of integers can be obtained as a variant of the Fibonacci codes by inserting some redundant digits 0.

To this end, let us define the *uniform Fibonacci tree* of order k (denoted U_k) as follows: For $k \leqslant 2$, the uniform Fibonacci tree coincides with the Fibonacci tree. If $k > 2$, the root is F_k; the left subtree is U_{k-1}; the right subtree has root $F_k + F_{k-1}$ whose right subtree is empty and whose left subtree is U_{k-2} with all numbers increased by F_k.

A uniform Fibonacci tree is the Fibonacci tree with dummy nodes after each right branch that force the leaves to be at the same level. The uniform Fibonacci tree can be obtained from the branch labeling of the Fibonacci tree, as described in [3]. The relationships between this labeling and the Zeckendorf representation of integers have been unnoticed. Figure 2 above shows U_6. Some properties of U_k are given in the following theorems.

Theorem 2: U_k has F_{i+2} nodes at level i, $0 \leqslant i \leqslant k-1$.

Proof: Theorem 2 is trivially true for $k = 1, 2$. Suppose it is true for each U_i, $i < k$ $(k > 2)$. We prove that it is true for U_k.

Let us denote by $L(i, k)$ the number of nodes that U_k has at level i. The construction of U_k implies

$$L(0, k) = F_2, \quad L(1, k) = F_3,$$

and

$$L(i, k) = L(i-1, k-1) + L(i-2, k-2), \; 2 \leqslant i \leqslant k-1.$$

By the induction hypothesis, this gives $L(i, k) = F_{i+1} + F_i = F_{i+2}$. ■

Corollary 1: U_k is obtained by adding $F_k - 1$ internal nodes to T_k.

Proof: From Theorem 2, U_k has $\sum_{i=2}^{k} F_i = F_{k+2} - 2$ internal nodes. Since T_k has $F_{k+1} - 1$ internal nodes, we get that U_k has $F_{k+2} - 2 - F_{k+1} + 1 = F_k - 1$ additional nodes. ■

Similarly, as was done in [3] for Fibonacci trees, it is possible to classify terminal nodes of U_k into:

$\mathcal{R}$-nodes, the terminal nodes that are right sons, and
$\mathcal{L}$-nodes, the terminal nodes that are left sons.

Lemma 1: U_k has F_{k-1} $\mathcal{R}$-nodes and F_k $\mathcal{L}$-nodes.

Proof: By induction. Trivially true for $k = 2, 3$. Suppose the lemma is true for each uniform Fibonacci tree of order less than k, $k > 3$. The definition of $\mathcal{R}$-nodes and $\mathcal{L}$-nodes implies that the type ($\mathcal{R}$ or $\mathcal{L}$) determination within each of the left and right subtrees of any uniform Fibonacci tree gives the correct type determination in the whole tree. Hence, by the construction of U_k and by the induction hypothesis, U_k has $F_{k-2} + F_{k-3}$ $\mathcal{R}$-nodes and $F_{k-1} + F_{k-2}$ $\mathcal{L}$-nodes. This completes the proof. ■

As was done in [2] for Fibonacci trees, and as Theorem 2 suggests, one can construct U_{k+1} by properly splitting terminal nodes of U_k. However, the recursive construction for uniform Fibonacci trees is slightly different from that described in [2] for Fibonacci trees. This time, all terminal nodes generate offsprings.

Theorem 3: If each $\mathcal{R}$-node of U_k, $k \geqslant 2$, generates only the left node and each $\mathcal{L}$-node generates two nodes, then the resulting tree that has F_k $\mathcal{R}$-nodes and $F_{k-1} + F_k$ $\mathcal{L}$-nodes is exactly U_{k+1}.

Proof: By induction. Suppose the theorem is true for each U_i, $i < k$, $k > 3$ (when $k = 2, 3$, the assertion is easily shown). U_k has, as its left subtree, U_{k-1} with F_{k-2} $\mathcal{R}$-nodes and F_{k-1} $\mathcal{L}$-nodes. Making terminal nodes of this U_{k-1} generate offsprings produces U_k by the induction hypothesis. Similarly, the right subtree of U_k has empty right subtree and has U_{k-2} as the left subtree. Making the F_{k-3} $\mathcal{R}$-nodes and the F_{k-2} $\mathcal{L}$-nodes of this U_{k-2} generate offsprings produces U_{k-1} by the induction hypothesis. Therefore, making all $\mathcal{R}$-nodes of U_k generate left sons and all $\mathcal{L}$-nodes generate two sons produces U_{k+1}. ■

We now relate the tree code of U_k, *the uniform Fibonacci tree code* of order k (denoted in the sequel by B_k), to the Zeckendorf representation of integers. For example, B_6 is given by:

0	00000	5	01000	10	10010
1	00001	6	01001	11	10100
2	00010	7	01010	12	10101
3	00100	8	10000		
4	00101	9	10001		

Lemma 2: The uniform Fibonacci code of order k is the set of all Fibonacci sequences of length $k - 1$.

Proof: From the construction of the uniform Fibonacci tree, the uniform Fibonacci code does not allow two consecutive 1's in any codeword and contains F_{k+1} distinct codewords of length $k - 1$. The number of Fibonacci sequences of length $k - 1$ is also given by F_{k+1}. ■

Theorem 4: In a uniform Fibonacci code, the codeword that represents the terminal node i is the Zeckendorf representation of the integer i.

Proof: From Lemma 2, the uniform Fibonacci tree code of order k is the set of Fibonacci sequences of length $k - 1$. By definition, they provide the Zeckendorf representation of nonnegative integers $< F_{k+1}$. Since the Zeckendorf representation preserves the lexicographic ordering, the assertion is a straightforward consequence of the order-preserving property of tree codes. ■

Uniform Fibonacci trees, therefore, provide an efficient pretty mechanism for obtaining the Zeckendorf representation of integers. The procedure is:

> *Given the integer i, $0 \leqslant i < F_{k+1}$, construct the uniform Fibonacci tree of order k. The Zeckendorf representation of i is the path of labels from the root to terminal node i.*

It is also worthwhile to note that the uniform Fibonacci trees in the setting of the Fibonacci numeration system play a role analogous to that of the complete binary trees in the setting of the binary numeration system:

> *The number of nodes at each level is given by a Fibonacci number (power of 2, in the binary case);*
>
> *The path of labels to a terminal node is the Zeckendorf representation (the binary representation, in the binary case).*

The last result is the determination of the number $\overline{N}_k^1$ of 1's and the number $\overline{N}_k^0$ of 0's in B_k. With the same notation of Theorem 1, we have

Theorem 5: $\overline{N}_k^1 = N_k^1$; $\overline{N}_k^0 = N_k^0 + N_k^1 - F_{k-1}$, $k \geqslant 2$.

Proof: The first part is immediate from the construction of trees T_k and U_k. The second part can be proved by induction. Suppose Theorem 5 is true for each uniform Fibonacci tree of order less than k, $k > 3$ (when $k = 2, 3$, the assertion is trivially true). By the construction of U_k, one has the equation:

$$\overline{N}_k^0 = (F_k + \overline{N}_{k-1}^0) + (F_{k-1} + \overline{N}_{k-2}^0).$$

By the induction hypothesis, this gives

$$\overline{N}_k^0 = F_k + F_{k-1} + N_{k-1}^0 + N_{k-1}^1 - F_{k-2} + N_{k-2}^0 + N_{k-2}^1 - F_{k-3}.$$

Since $N_k^0 = F_k + N_{k-1}^0 + N_{k-2}^0$ and $N_k^1 = F_{k-1} + N_{k-1}^1 + N_{k-2}^1$ (see Theorem 1), the assertion is true. ■

Theorem 5 allows immediate computation of the asymptotic proportion of 1's (and 0's) in Fibonacci sequences (see [4]). Indeed, denoting by p, q and $\overline{p}$, $\overline{q}$, respectively, the asymptotic proportions of 0's and 1's in C_k and B_k, and recalling Theorem 1 and its proof, one obtains

$$\overline{q} = 1 - \overline{p} = \lim_{k\to\infty} \frac{\overline{N}_k^1}{\overline{N}_k} = \lim_{k\to\infty} \frac{N_k^1}{N_k + N_k^1 - F_{k-1}} = \frac{q}{1+q} = \frac{\Phi - 1}{2\Phi - 1} = \frac{5-\sqrt{5}}{10}.$$

ACKNOWLEDGMENT

The author wishes to express his sincere gratitude to the anonymous referee whose suggestions led to a substantial improvement in the presentation of this note.

REFERENCES

1. V. E. Hoggatt, Jr., & M. Bicknell-Johnson. "Lexicographic Ordering and Fibonacci Representations." *The Fibonacci Quarterly* **20**, no. 3 (1982):193-218.
2. Y. Horibe. "An Entropy View of Fibonacci Trees." *The Fibonacci Quarterly* **20**, no. 2 (1982):168-178.
3. Y. Horibe. "Notes on Fibonacci Trees and Their Optimality." *The Fibonacci Quarterly* **21**, no. 2 (1983):118-128.
4. P. H. St. John. "On the Asymptotic Proportions of Zeros and Ones in Fibonacci Sequences." *The Fibonacci Quarterly* **22**, no. 2 (1984):144-145.
5. D. E. Knuth. *The Art of Computer Programming.* Vol. 3: *Sorting and Searching.* Reading, Mass.: Addison-Wesley, 1973.
6. E. Zeckendorf. "Representation des Nombres Naturels par une Somme de Nombres de Fibonacci ou de Nombres de Lucas." *Bulletin de la Société Royale des Sciences de Liége*, Nos. 2-3 (1972):179-182. This paper contains Zeckendorf's original proof dated 1939.

◆◇◆◇◆

A NOTE ON SPECIALLY MULTIPLICATIVE ARITHMETIC FUNCTIONS

PENTTI HAUKKANEN
University of Tampere, SF-33101 Tampere, Finland

(Submitted December 1986)

An arithmetic function f is called multiplicative if

$$f(mn) = f(m)f(n), \tag{1}$$

whenever $(m, n) = 1$. A multiplicative function f is called completely multiplicative if (1) holds for all m, n. Further, a multiplicative function f is said to be a quadratic (see [1], [3], [8]) or a specially multiplicative function (see [2], [4], [6], [7]) if

$$f = a \circ b, \tag{2}$$

where a, b are completely multiplicative functions and $\circ$ denotes the Dirichlet product. It is known that (2) is equivalent to

$$f(mn) = \sum_{d|(m,n)} f(m/d)f(n/d)g(d)\mu(d),$$

where g is a completely multiplicative function and μ denotes the Möbius function. The completely multiplicative function g is defined for every prime by

$$g(p) = (ab)(p) \quad \text{or} \quad g(p) = f(p)^2 - f(p^2) \quad \text{or} \quad g(p) = f^{-1}(p^2),$$

where f^{-1} denotes the Dirichlet inverse of f. Since a quadratic f is multiplicative, the values $f(n)$ are known if the values $f(p^m)$ are known for all primes p and all positive integers m. Furthermore, the values $f(p^m)$ are known if the values $f(p)$, $f(p^2)$ [or the values $f(p)$, $f^{-1}(p^2)$ or the values $a(p)$, $b(p)$] are known. The values $f(p^m)$ are given recursively by

$$f(1) = 1,$$
$$f(p),\ f(p^2) \text{ are arbitrary},$$
$$f(p^m) = f(p)f(p^{m-1}) - g(p)f(p^{m-2}),\ m = 3, 4, \ldots . \tag{3}$$

Consequently, if we put $f(p^m) = S_m$, we obtain a generalized Fibonacci sequence determined by

$$S_0 = 1,$$
$$S_1,\ S_2 \text{ are arbitrary},$$
$$S_{m+1} = S_1S_m - ((S_1)^2 - S_2)S_{m-1},\ m = 2, 3, 4, \ldots .$$

If we let $S_1 = 1$, $S_2 = 2$, we obtain the Fibonacci sequence.

If f is specially multiplicative and $f = a \circ b$, where a, b are completely multiplicative, then the generating series of f to the base p is given by

$$f_{(p)}(x) = \frac{1}{(1 - \alpha x)(1 - \beta x)} \quad (p \text{ a prime}),$$

where $\alpha = a(p)$, $\beta = b(p)$. Then

$$f_{(p)}(x) = \frac{1}{1 - f(p)x + g(p)x^2},$$

where $f(p) = \alpha + \beta$ and $g(p) = \alpha\beta$. Noting that the generating function of the Fibonacci sequence $\{F_n\}$ is

$$\sum_{n=0}^{\infty} F_n x^n = \frac{1}{1 - x - x^2},$$

$f_{(p)}(x)$ will generate $\{F_n\}$ if $f(p) = 1$ and $g(p) = -1$.

If a is any nonzero complex number, one could consider f for which $f(p) = a$ and $g(p) = -a^2$. It will follow that

$$f_{(p)}(x) = \frac{1}{1 - ax - a^2x^2} = \sum_{n=0}^{\infty} a^n F_n x^n.$$

Hence, $f(p^n) = a^n F_n$. Write $f(p^n) = G_n$. Using known properties (see [5], [9]) of the Fibonacci sequence $\{F_n\}$, for example, the following properties of the sequence $\{G_n\}$ can be derived:

$$\sum_{k=0}^{n} a^{n-k+2} G_k = G_{n+2} - a^{n+2},$$

$$\sum_{k=0}^{n} (-1)^k a^{n-k} G_k = (-1)^n a G_{n-1} + a^n,$$

$$\sum_{k=0}^{n} a^{2(n-k)+1} G_{2k} = G_{2n+1},$$

$$\sum_{k=1}^{n} a^{2(n-k)+1} G_{2k-1} = G_{2n} - a^{2n},$$

$$2\sum_{k=1}^{n} a^{3(n-k)+2} G_{3k-1} = G_{3n+1} - a^{3n+1},$$

$$\sum_{k=0}^{n} (n - k) a^{n-k+3} G_k = G_{n+3} - (n + 3) a^{n+3},$$

$$\sum_{k=0}^{2n} a^{2(2n-k)+1} G_k G_{k+1} = G_{2n+1}^2,$$

$$\sum_{k=0}^{2n-1} a^{2(2n-k)-1} G_k G_{k+1} = G_{2n}^2 - a^{4n},$$

$$\sum_{k=0}^{n} a^{2(n-k)+1} G_k^2 = G_n G_{n+1},$$

$$10\sum_{k=0}^{n} a^{3(n-k)+4}G_k^3 = G_{3n+4} + (-1)^n 6a^{2n+5}G_{n-1} + 5a^{3n+4},$$

$$G_{n+m} = G_nG_m + a^2G_{n-1}G_{m-1},$$

$$G_n^2 - G_{n-k}G_{n+k} = (-1)^{n-k+1}G_{k-1}^2 a^{2(n-k+1)},$$

$$aG_{3n+2} = G_{n+1}^3 + a^3G_n^3 - a^6G_{n-1}^3,$$

$$aG_{2n+1} = G_{n+1}^2 - a^4G_{n-1}^2.$$

The proofs of the above relations are omitted.

ACKNOWLEDGMENT

The author wishes to thank the referee for his valuable comments.

REFERENCES

1. T. B. Carroll & A. A. Gioia. "On a Subgroup of the Group of Multiplicative Arithmetic Functions." *J. Austral. Math. Soc.*, Ser. A, *20*, no. 3 (1975):348-358.
2. D. H. Lehmer. "Some Functions of Ramanujan." *Math. Student 27* (1959):105-116.
3. P. J. McCarthy. "Busche-Ramanujan Identities." *Amer. Math. Monthly 67* (1960):966-970.
4. A. Mercier. "Remarques sur les Fonctions Specialement Multiplicatives." *Ann. Sc. Math. Quebec 6*, no. 1 (1982):99-107.
5. K. Subba Rao. "Some Properties of Fibonacci Numbers." *Amer. Math. Monthly 60* (1953):680-684.
6. D. Redmond & R. Sivaramakrishnan. "Some Properties of Specially Multiplicative Functions." *J. Number Theory 13*, no. 2 (1981):210-227.
7. R. Sivaramakrishnan. "On a Class of Multiplicative Arithmetic Functions." *J. Reine Angew. Math. 280* (1976):157-162.
8. R. Vaidyanathaswamy. "The Theory of Multiplicative Arithmetic Functions." *Trans. Amer. Math. Soc. 33* (1931):579-662.
9. N. N. Vorob'ev. *Fibonacci Numbers*. New York: Pergamon Press, 1961.

◆◇◆◇◆

IDENTITIES DERIVED ON A FIBONACCI MULTIPLICATION TABLE

ALVIN TIRMAN
East Tennessee State University, Kingsport, TN 37660
T. HENRY JABLONSKI, JR.
East Tennessee State University, Johnson City, TN 37660

(Submitted December 1986)

A multiplication table constructed only with Fibonacci numbers assumes the appearance shown in Table 1. In any of its rows among three successive integers, the sum of the first two equals the third. This may be expressed as

$$F_mF_n + F_mF_{n+1} = F_mF_{n+2}. \tag{1}$$

Table 1

		F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	
		1	1	2	3	5	8	13	21	34	...
F_1	1	1	1	2	3	5	8	13	21	34	...
F_2	1	1	1	2	3	5	8	13	21	34	...
F_3	2	2	2	4	6	10	16	26	42	68	...
F_4	3	3	3	6	9	15	24	39	63	102	...
F_5	5	5	5	10	15	25	40	65	105	170	...
F_6	8	8	8	16	24	40	64	104	168	272	...
F_7	13	13	13	26	39	65	104	169	273	442	...
F_8	21	21	21	42	63	105	168	273	441	714	...
F_9	34	34	34	68	102	170	272	442	714	1156	...
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

While this result is rather trivial, it does suggest that the table should be scrutinized to uncover analogs. Doing this, an investigator perceives that along any descending diagonal the sum of two successive integers is a Fibonacci number. This is expressed as

$$F_mF_n + F_{m+1}F_{n+1} = F_{m+n+1}. \tag{2}$$

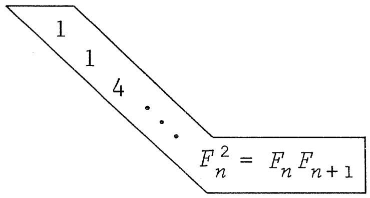
Combining formulas (1) and (2) "geometrically" leads to the following triangular representation in the table:

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

One of the identities known by practically every student of the Fibonacci numbers is

$$F_1^2 + F_2^2 + F_3^2 + \cdots + F_n^2 = F_nF_{n+1}.$$

On the Fibonacci multiplication table, this assumes the following appearance:



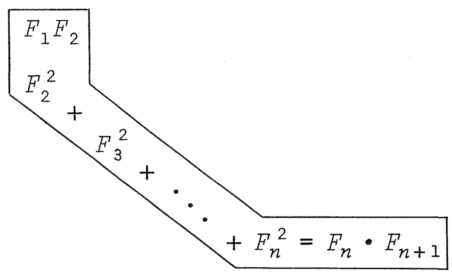
When analogs are sought in the table, none appears. In view of the findings of identities (1), (2), and (3), this is surprising.

If, however, this well-known result is altered to assume the form

$$F_1F_2 + (F_2^2 + F_3^2 + \cdots + F_n^2) = F_n \cdot F_{n+1},$$

it remains numerically identical to $1^2 + 1^2 + 2^2 + \cdots + F_n^2 = F_n \cdot F_{n+1}$.

As the revised form



has analogs throughout the table, it is evident that $1 + 1 + 2 + \cdots + F_n^2 = F_n \cdot F_{n+1}$ is just a special case of the more general identity

$$F_{m-1}F_n + F_mF_n + F_{m+1}F_{n+1} + F_{m+2}F_{n+2} + \cdots + F_{m+k}F_{n+k} = F_{m+k}F_{n+k+1},$$

that is,

$$\sum_{j=0}^{k} F_{m+j}F_{n+j} = F_{m+k}F_{n+k+1} - F_{m-1}F_n \text{ for } m \geqslant 2,\ n \geqslant 1. \tag{4}$$

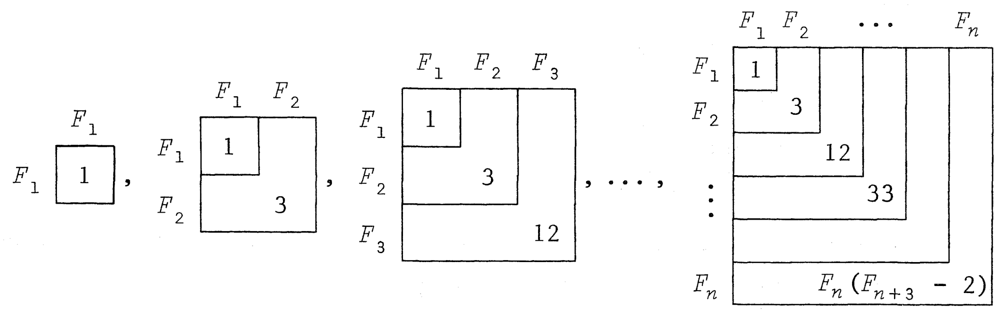
A sequence of squares beginning in the upper left-hand corner of the table may be built as follows:

$$\begin{array}{cc} & F_1 \\ F_1 & \boxed{1} \end{array}, \quad \begin{array}{c|cc|} & F_1 & F_2 \\ \hline F_1 & 1 & 1 \\ F_2 & 1 & 1 \\ \hline \end{array}, \quad \begin{array}{c|ccc|} & F_1 & F_2 & F_3 \\ \hline F_1 & 1 & 1 & 2 \\ F_2 & 1 & 1 & 2 \\ F_3 & 2 & 2 & 4 \\ \hline \end{array}, \quad \ldots, \quad \begin{array}{c|ccc|} & F_1 & F_2 \cdots & F_n \\ \hline F_1 & 1 & 1 \ \ldots & F_n \\ F_2 & 1 & & \\ \vdots & \vdots & & \vdots \\ F_n & F_n & \ldots & F_n^2 \\ \hline \end{array}$$

$$F_1^2 \qquad (F_1 + F_2)^2 \qquad (F_1 + F_2 + F_3)^2 \qquad (F_1 + F_2 + \cdots + F_n)^2$$

$$1^2 \qquad (1 + 1)^2 \qquad (1 + 1 + 2)^2 \qquad (1 + 1 + \cdots + F_n)^2$$

This same sequence could also be developed by summing rows and columns in the manner indicated below:



As these constructions cover identical squares, it becomes evident that the entries of any n by n square in the upper left-hand corner of the table may be summed in any two distinct ways both of which equal $(F_{n+2} - 1)^2$. This results in the following identities:

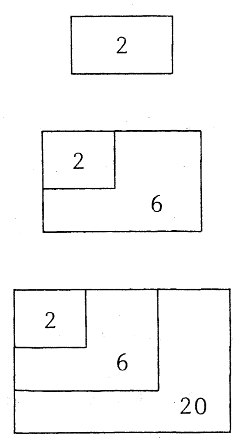
$$\left(\sum_{i=1}^{n} Fi\right)^2 = \sum_{i=1}^{n} Fi(F_{i+3} - 2) = (F_{n+2} - 1)^2. \tag{5}$$

An analog of the sequence of squares is the sequence of oblong rectangles of dimension n by $n + 1$.

1	1

1	1	2
1	1	2

1	1	2	3
1	1	2	3
2	2	4	6



By pursuing an analysis similar to that performed on the squares, the following oblong identities are obtained:

$$\left(\sum_{i=1}^{n} Fi\right)\left(\sum_{i=1}^{n+1} Fi\right) = \sum_{k=1}^{n} (F_{k+2}^2 - F_{k+2}) = (F_{n+2} - 1)(F_{n+3} - 1). \tag{6}$$

Other identities that may be gleaned from the table include

$$F_{2n+1}^2 = F_{2n} \cdot F_{2n+2} + 1 \tag{7}$$

and

$$F_{2n}^2 = F_{2n-1} \cdot F_{2n+1} - 1, \tag{8}$$

which can readily be combined into

$$F_{n-1}F_{n+1} - F_n^2 = (-1)^n, \tag{9}$$

the basis for one of Charles Dodgson's favorite geometrical puzzles:

$$F_{n-1}F_{n+1} - F_{n+2}F_{n-2} = 2(-1)^n. \tag{10}$$

◆◇◆◇◆

Third International Conference *(Continued from page 289)*

actual ocean of yellows—were not only joyous, but also touched our mathematical souls. Do Fibonacci numbers not play an important role in deciphering nature's handiwork in sunflowers?

Volterra, situated about 550 metres above sea-level, immediately transplanted us into enigmatic Etruscan, as well as into problematic Medieval times. While we were fascinated both by the histroic memorabilia, as well as by the artifacts and master pieces, the magnificent panorama of the surrounding landscape enhanced our enjoyment still further.

As has become tradition in our conference, a banquet was held on the last night before the closing of our sessions. Lucca, the site of the meeting, provided a wonderful setting for a memorable evening, Ligurian in origin, it bespeaks of Etruscan culture, and exudes the charm of an ancient city.

The spirit at the banquet highlighted what had already become apparent during the week: that the Conference had not only been mind-streatching, but also heartwarming. Friendships which had been started, became knitted more closely. New friendships were formed. The magnetism of common interest and shared enthusiasm wove strong bonds amoung us. We had come from different cultural and ethnic backgrounds, and our native tongues differed. Yet, we truly understood each other. And we cared for each other.

I believe, I speak for all of us if I express my heartfelt thanks to all members of the International, as well as of the Local Committee whose dedication and industriousness gave us this unforgettable event. Our gratitude also goes to the University of Pisa whose generous hospitality we truly appreciated. I would also like to thank all participants, without whose work we could not have had this treat.

"Auf Wiedersehen" then, at Conference number Four in 1990.

ON SUMS OF THREE TRIANGULAR NUMBERS

JOHN A. EWELL
Northern Illinois University, DeKalb, IL 60115

(Submitted December 1986)

1. INTRODUCTION

According to Dickson [3, pp. 6 and 17], Fermat conjectured and Gauss proved the following theorem.

Theorem 1: Every nonnegative integer can be expressed as a sum of three triangular numbers [including $0 = 0(0 + 1)/2$].

Gauss also gave a method for counting the number of such representations of a given nonnegative integer. In this paper we propose to express the implicit counting function in terms of simple divisor functions. All of these functions are collected in the following definition.

Definition:

(i) For each nonnegative integer n, $t_3(n)$ denotes the cardinality of the set
$$\left\{(x_1, x_2, x_3) \in \mathbb{N}^3 \,\middle|\, n = \sum_{i=1}^{3} x_i(x_i + 1)/2\right\}.$$
(Here, $\mathbb{N} = \{0, 1, 2, \ldots\}$.)

(ii) For each positive integer n and $i \in \{1, 5\}$,
$$d_i(n) := \sum_{\substack{\delta \mid n, \\ \delta \equiv i \ (\mathrm{mod}\ 6)}} 1;$$
and, $\varepsilon(n) := d_1(n) - d_5(n)$.

Theorem 2: Let n denote an arbitrary nonnegative integer.

(i) If $n = 3i(i + 1)/2$, for some $i \in \mathbb{N}$, then
$$t_3(n) = 1 + 3\sum_{i=0} \varepsilon(n - 3i(i + 1)/2).$$

(ii) If n is not of the form $3i(i + 1)/2$, then
$$t_3(n) = 3\sum_{i=0} \varepsilon(n - 3i(i + 1)/2).$$

In both cases, summation extends over all $i \in \mathbb{N}$ for which $n - 3i(i + 1)/2 > 0$.

Section 2 is dedicated to proof of Theorem 2. In view of the two theorems we then deduce a corollary concerning the behavior of the function ε.

2. PROOF OF THEOREM 2

The leading role in our argument is played by the following variant of the quintuple-product identity.

$$\prod_1^\infty \frac{(1 - x^{2n})(1 - a^2x^{2n-2})(1 - a^{-2}x^{2n})}{(1 + ax^{2n-1})(1 + a^{-1}x^{2n-1})} = \sum_{-\infty}^{\infty} x^{n(3n+2)}(a^{-3n} - a^{3n+2}). \tag{1}$$

(Here and throughout our discussion we assume that a and x denote complex numbers with $a \neq 0$ and $|x| < 1$.) For a discussion of (1) and other forms of the quintuple-product identity see [5]. We shall also require the classical triple-product identity:

$$\prod_1^\infty (1 - x^{2n})(1 + ax^{2n-1})(1 + a^{-1}x^{2n-1}) = \sum_{-\infty}^{\infty} x^{n^2}a^n. \tag{2}$$

In [2] Carlitz and Subbarao show how to deduce one form of the quintuple-product identity from (2).

Multiplying (1) by a^{-1}, we have

$$(a - a^{-1}) \prod_1^\infty \frac{(1 - x^{2n})(1 - a^2x^{2n})(1 - a^{-2}x^{2n})}{(1 + ax^{2n-1})(1 + a^{-1}x^{2n-1})} \tag{3}$$

$$= a \sum_{-\infty}^{\infty} x^{3n^2+2n}a^{3n} - a^{-1} \sum_{-\infty}^{\infty} x^{3n^2+2n}a^{-3n}$$

$$= a \prod_1^\infty (1 - x^{6n})(1 + a^3x^{6n-1})(1 + a^{-3}x^{6n-5})$$

$$- a^{-1} \prod_1^\infty (1 - x^{6n})(1 + a^{-3}x^{6n-1})(1 + a^3x^{6n-5}).$$

In the last step we have used (2) to transform the infinite series into infinite products. For the sake of brevity, put

$$F(a) = F(a, x) := \prod_1^\infty \frac{(1 - a^2x^{2n})(1 - a^{-2}x^{2n})}{(1 + ax^{2n-1})(1 + a^{-1}x^{2n-1})}$$

$$G(a) = G(a, x) := \prod_1^\infty (1 + a^3x^{6n-1})(1 + a^{-3}x^{6n-5}),$$

$$H(a) := G(a^{-1}).$$

Hence, (3) becomes

$$\prod_1^\infty (1 - x^{2n})(a - a^{-1})F(a) = \prod_1^\infty (1 - x^{6n})\{aG(a) - a^{-1}H(a)\}.$$

Differentiating the foregoing identity with respect to a, we get

$$\prod_1^\infty (1 - x^{2n})\{(1 + a^{-2})F(a) + (a - a^{-1})F'(a)\} \tag{4}$$

$$= \prod_1^\infty (1 - x^{6n})\{G(a) + a^{-2}H(a) + aG'(a) - a^{-1}H'(a)\}.$$

Now, using the technique of logarithmic differentiation, we evaluate $G'(a)$ and $H'(a)$, then substitute these evaluations into (4), let $a \to 1$, and cancel a factor of 2 in the resulting identity to get

$$\prod_1^\infty \frac{(1 - x^{2n})^3}{(1 + x^{2n-1})^2}$$

$$= \prod_1^\infty (1 - x^{6n})(1 + x^{6n-1})(1 + x^{6n-5})\left\{1 + 3\sum_1^\infty \left(\frac{x^{6n-1}}{1 + x^{6n-1}} - \frac{x^{6n-5}}{1 + x^{6n-5}}\right)\right\}.$$

In the foregoing identity we then let $x \to -x$, utilize the definition of ε, and simplify to get

$$\prod_1^\infty \frac{(1 - x^{2n})^3 \cdot (1 - x^{6n-3})}{(1 - x^{2n-1})^3 \cdot (1 - x^{6n})} = 1 + 3\sum_1^\infty \varepsilon(n)x^n. \tag{5}$$

At this juncture, we appeal to the following well-known identity of Gauss [4, p. 284].

$$\prod_1^\infty \frac{1 - x^{2n}}{1 - x^{2n-1}} = \sum_0^\infty x^{n(n+1)/2}.$$

Hence, (5) becomes

$$\left\{\sum_0^\infty x^{n(n+1)/2}\right\}^3 = \sum_0^\infty x^{3n(n+1)/2}\left\{1 + 3\sum_1^\infty \varepsilon(n)x^n\right\},$$

or, equivalently (owing to the fact that the left side of this identity generates t_3),

$$\sum_0^\infty t_3(n)x^n = \sum_{i=0}^\infty x^{3i(i+1)/2} + 3\sum_{n=1}^\infty x^n \sum_{i=0} \varepsilon(n - 3i(i + 1)/2).$$

Equating coefficients of like powers of x, we thus prove our theorem.

Corollary: If n is any positive integer which is not of the form $3i(i + 1)/2$, then there exists $j \in \{0, 1, \ldots, [(-1 + \sqrt{(8/3)n + 1})/2]\}$ such that

$$\varepsilon(n - 3j(j + 1)/2) > 0.$$

Proof: Let such an n be given. By multiplicative induction it follows easily that $\varepsilon(m) \geqslant 0$ for each positive integer m. Hence, the sum on the right side of the equation of Theorem 2(ii) is nonnegative. Now, by Theorem 1, $t_3(n) > 0$. Hence, the aforementioned sum is positive, whence there exists

$$j \in \{0, 1, \ldots, [(-1 + \sqrt{(8/3)n + 1})/2]\}$$

such that

$$\varepsilon(n - 3j(j + 1)/2) > 0.$$

CONCLUDING REMARKS

In a recent paper, Andrews [1] has presented a proof of Theorem 1 which (unlike Gauss's proof) is independent of the theory of ternary quadratic forms. Of course, such proofs of Theorem 1 and Theorem 2 then combine to yield a proof of the Corollary that is independent of the theory of ternary quadratic forms. However, if one could find another such *direct* proof of the Corollary, then one could use the statement of the Corollary (then independent of Theorems 1 and 2) and Theorem 2 to produce yet another proof of Theorem 1.

REFERENCES

1. G. E. Andrews. "EYPHKA! Num = $\Delta + \Delta + \Delta$." *J. of Number Theory* **23**, no. 3 (2986):285-293.
2. L. Carlitz & M. V. Subbarao. "A Simple Proof of the Quintuple-Product Identity." *Proc. Amer. Math. Soc.* **32** (1972):42-44.
3. L. E. Dickson. *History of the Theory of Numbers*, II. New York: Chelsea, 1952.
4. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*, 4th ed. Oxford: Oxford University Press, 1960.
5. M. V. Subbarao & M. Vidyasagar. "On Watson's Quintuple-Product Identity." *Proc. Amer. Math. Soc.* **26** (1970):23-27.

◆◇◆◇◆

STROEKER'S EQUATION AND FIBONACCI NUMBERS

ANDRZEJ MĄKOWSKI
University of Warsaw, 00-901 Warsaw, Poland

(Submitted December 1986)

R. J. Stroeker [1] considered the Diophantine equation

$$(x^2 + y)(x + y^2) = N(x - y)^3, \tag{1}$$

where N is a positive integer. He found all solutions of (1) for $N \leqslant 51$ and proved that if x, y satisfy this equation with $N \neq 1, 2, 4$ then

$$\max(|x|, |y|) < N^3 \quad \text{(see Theorem 1 of [1]).}$$

For every N equation, (1) has the trivial solution $x = y = -1$. Theorem 2 of [1] asserts that for odd $N > 1$ there exists a nontrivial solution with $xy \neq 0$, and for infinitely many such values of N there are at least five such solutions. The table given at the end of [1] shows that for many even N there is only the trivial solution.

Below, we exhibit a connection between (1) and Fibonacci numbers defined by $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$. The following identities are well known:

$$F_k F_{k+1} + (-1)^k = F_{k-1}F_{k+2}; \tag{2}$$

$$F_{k-n}F_{k+n} - F_k^2 = (-1)^{k+n+1}F_n^2. \tag{3}$$

When we put $n = 1$ or 2 in identity (3), it becomes, respectively,

$$F_{k-1}F_{k+1} - F_k^2 = (-1)^k, \tag{4}$$

$$F_k^2 - (-1)^k = F_{k-2}F_{k+2}. \tag{5}$$

Taking (4) with k replaced by $k + 1$ and multiplying it by F_{k+1}, we get

$$F_k F_{k+1} F_{k+2} - F_{k+1}^3 = (-1)^{k+1} F_{k+1},$$

$$F_{k+1}^3 - (-1)^k (F_{k+2} - F_k) = F_k F_{k+1} F_{k+2},$$

$$F_{k+1}^3 + (-1)^k F_k = [F_k F_{k+1} + (-1)^k] F_{k+2},$$

which, in view of (2), may be written in the form

$$F_{k+1}^3 + (-1)^k F_k = F_{k-1} F_{k+2}^2. \tag{6}$$

Multiplying (5) and (6), we get

$$[F_k^2 - (-1)^k][F_{k+1}^3 + (-1)^k F_k] = F_{k-2}F_{k-1}(F_k + F_{k+1})^3,$$

and

$$[F_k^2F_{k+1}^2 - (-1)^kF_{k+1}^2][F_{k+1}^4 + (-1)^kF_kF_{k+1}] = F_{k-2}F_{k-1}(F_kF_{k+1} + F_{k+1}^2)^3.$$

This shows that, for $N = F_{k-2}F_{k-1}$, equation (1) is satisfied by

$$x = F_kF_{k+1},\ y = -F_{k+1}^2 \quad (k \text{ even})$$

and by

$$x = F_{k+1}^2,\ y = -F_kF_{k+1} \quad (k \text{ odd}).$$

Therefore, for infinitely many values of N, the number $\max(|x|, |y|)$ is larger than $11N$ because

$$\lim_{k\to\infty} \frac{F_{k+1}^2}{F_{k-2}F_{k-1}} = \left(\frac{1}{2} + \frac{1}{2}\sqrt{5}\right)^5 > 11.$$

Furthermore, since there are infinitely many even Fibonacci numbers, there are infinitely many positive even integers N such that (1) has a nontrivial solution. The last result, however, can be proved in a simpler way:

For $N = [(a+1)^3 + 1](a^3 + 1)$, the numbers $x = a(a+1)^2$, $y = a^2(a+1)$ satisfy (1).

The following question remains open: Do there exist infinitely many positive (even) integers N such that equation (1) has only the trivial solution?

REFERENCE

1. R. J. Stroeker. "The Diophantine Equation $(x^2 + y)(x + y^2) = N(x - y)^3$." *Simon Stevin* 54 (1980):151-163.

◆◇◆◇◆

SOME OBSERVATIONS ON THE CLASSICAL CUBOID AND ITS PARAMETRIC SOLUTIONS

W. J. A. COLMAN
North East London Polytechnic, Essex RMB 2AS, England

(Submitted December 1986)

1. The classical cuboid has integral edges and face diagonals. We require integer solutions of the Diophantine equations:

$$x^2 + y^2 = u^2, \quad x^2 + z^2 = v^2, \quad \text{and} \quad y^2 + z^2 = \omega^2. \tag{1.1}$$

The first parametric solution was given by Saunderson (Dickson [1], p. 497) and subsequent two-parameter solutions have been given by a number of writers; a listing of these authors can be found in Kraitchik [2]. The general solution of equations (1.1) is unknown. In this paper a method is given which leads to an infinity of two-parameter solutions which are of ever-increasing degree and complexity.

2. A solution of (1.1) is given by

$$\begin{aligned} x &= (a^2 - d^2)(c^2 - b^2) \\ y &= 2ad(c^2 - b^2) \\ z^2 &= 4c^2b^2\left(a^2 + \frac{2abd}{c} - d^2\right)\left(a^2 + \frac{2acd}{b} - d^2\right), \end{aligned} \tag{2.1}$$

because

$$\begin{aligned} x^2 + y^2 &= ((c^2 - b^2)(a^2 + d^2))^2 \\ x^2 + z^2 &= ((a^2 - d^2)(b^2 + c^2) + 4abcd)^2 \\ y^2 + z^2 &= 4(ad(b^2 + c^2) + bc(a^2 - d^2))^2. \end{aligned}$$

We see from these equations that a cuboid with two integral edges and integral face diagonals has a four-parameter solution. The problem here is to make z rational.

Putting $a/d = w$ and $b/c = D$ (say), where w and D are rationals, we have

$$z^2 = 4c^2b^2d^4(w^2 + 2Dw - 1)\left(w^2 + \frac{2}{D}w - 1\right). \tag{2.2}$$

If we multiply the quadratics and put $A = D + 1/D$, we require rational solutions of

$$w^4 + 2Aw^3 + 2w^2 - 2Aw + 1 = t^2. \tag{2.3}$$

We wish to determine solutions of (2.3) in the form $w = w(A)$. If (2.3) has a rational solution $w = w_0$, then it also has a rational solution

$$w = -\frac{1}{w_0}.$$

But this will just interchange a and d and will not effect the solution.

We can equate (2.3) to the square of a quadratic in w in the usual way, to show that there is a rational solution

$$w = \frac{A}{4}, \quad t = \frac{3A^2}{16} - 1. \tag{2.4}$$

This gives the classical solution of Saunderson:

$$\begin{aligned} x &= (c^2 - b^2)((b^2 + c^2)^2 - 16b^2c^2) \\ y &= 8bc(c^4 - b^4) \\ z &= 2bc(3(b^2 + c^2)^2 - 16b^2c^2). \end{aligned} \tag{2.5}$$

Equation (2.2) has another simple solution. Putting $w = 1/2D$, we see that $w^2 + 2Dw - 1$ is square, and we require

$$\frac{5}{4D^2} - 1 = \square.$$

This has the standard rational solution

$$D = \frac{\alpha^2 + \alpha\beta - \beta^2}{\alpha^2 + \beta^2} \quad \text{and} \quad \square = \left(\frac{\alpha^2 - 4\alpha\beta - \beta^2}{2(\alpha^2 + \alpha\beta - \beta^2)}\right)^2,$$

which gives

$$a = \alpha^2 + \beta^2, \quad b = \alpha^2 + \alpha\beta - \beta^2, \quad c = \alpha^2 + \beta^2, \quad d = 2(\alpha^2 + \alpha\beta - \beta^2),$$

and we have the solution:

$$\begin{aligned} x &= \alpha\beta(\alpha^2 - \beta^2)(3\alpha - \beta)(3\beta + \alpha)(2\alpha + \beta)(2\beta - \alpha) \\ y &= 4\alpha\beta(\alpha^2 + \beta^2)(2\alpha + \beta)(2\beta - \alpha)(\alpha^2 + \alpha\beta - \beta^2) \\ z &= 2(\alpha^2 + \beta^2)^2(\alpha^2 + \alpha\beta - \beta^2)(\alpha^2 - 4\alpha\beta - \beta^2). \end{aligned} \tag{2.6}$$

3. To determine further solutions of (2.3), we can put $w = n + w_0$, where $w_0^4 + 2Aw_0^3 + 2w_0^2 - 2Aw_0 + 1 = t_0^2$, and write

$$\begin{aligned} &n^4 + (4w_0 + 2A)n^3 + (6w_0^2 + 6Aw_0 + 2)n^2 + (4w_0^3 + 6Aw_0^2 + 4w_0 - 2A)n + t_0^2 \\ &= (Cn^2 + Bn + t_0)^2 \quad \text{(say)}. \end{aligned}$$

Therefore,

$$\begin{aligned} 2Bt_0 &= 4w_0^3 + 6Aw_0^2 + 4w_0 - 2A \\ B^2 + 2Ct_0 &= 6w_0^2 + 6Aw_0 + 2 \end{aligned}$$

and

$$w = \frac{2BC - 4w_0 - 2A}{1 - C^2} + w_0.$$

These equations give:

$$w = \frac{Aw_0^9 + 12w_0^8 + 12Aw_0^7 + 32w_0^6 + 30Aw_0^5 + 24w_0^4 - 36Aw_0^3 + 9Aw_0 - 4}{4w_0^9 + 9Aw_0^8 - 36Aw_0^6 - 24w_0^5 + 30Aw_0^4 - 32w_0^3 + 12Aw_0^2 - 12w_0 + A}. \tag{3.1}$$

If we put $w_0 = A/4$, then the next solution generated is

$$w = \frac{A^{10} + 240A^8 + 9728A^6 - 122880A^4 + 589824A^2 - 1048576}{8A(5A^8 - 288A^6 + 3072A^4 + 8192A^2 - 65536)}.$$

Putting $D = 2 = b/c$, we obtain $A = 5/2$ and $w = 602697401/880248720$. Hence, we have a cuboid with $b = 2$, $c = 1$, $a = 602697401$, and $d = 880248720$.

Equation (3.1) will generate an infinity of rational solutions w, and each such solution gives a two-parameter solution of equations (1.1). It is evident that these solutions increase very rapidly in degree and complexity. The solutions do not necessarily give independent parametric formulas. If we put $w_0 = 1$, then $w = \frac{A+4}{A-4}$, which, again, gives Saunderson's solution (2.5).

4. It is seen that the solution

$$w = \frac{A}{4} = \frac{1}{4}\left(D + \frac{1}{D}\right)$$

makes both quadratics, $w^2 + 2Dw - 1$ and $w^2 + \frac{2}{D}w - 1$, simultaneously square. We will now consider this further.

We have

$$w^2 + 2Dw - 1 = \left(\frac{\alpha^2 + 2D\alpha - 1}{2\alpha + 2D}\right)^2 \quad \text{if } w = \frac{\alpha^2 + 1}{2\alpha + 2D} \tag{4.1}$$

and

$$w^2 + \frac{2}{D}w - 1 = \left(\frac{\beta^2 + \frac{2}{D}\beta - 1}{2\beta + \frac{2}{D}}\right)^2 \quad \text{if } w = \frac{\beta^2 + 1}{2\beta + \frac{2}{D}}, \tag{4.2}$$

where α and β are arbitrary rationals such that w is finite. Equating (4.1) and (4.2), we require rationals α and β such that

$$\frac{\alpha^2 + 1}{2\alpha + 2D} = \frac{\beta^2 + 1}{2\beta + \frac{2}{D}}. \tag{4.3}$$

If $\alpha = \beta$, then $D = 1$, which is trivial. If $\alpha = -\beta$, then we again obtain the classical solution (2.5). Thus, we have

$$(\alpha + D)(\beta^2 + 1) = \left(\beta + \frac{1}{D}\right)(\alpha^2 + 1).$$

Put $\alpha + D = K\left(\beta + \frac{1}{D}\right)$ and $\beta^2 + 1 = \frac{1}{K}(\alpha^2 + 1)$ for some rational K:

$$\therefore \quad \beta^2(K^2 - K) + \beta\left(\frac{2K^2}{D} - 2KD\right) + \left(\frac{K^2}{D^2} - 3K + D^2 + 1\right) = 0$$

$$\therefore \quad \beta = \left(KD - \frac{K^2}{D} \pm \left(\frac{(1 + D^2)K^3}{D^2} - 4K^2 + (1 + D^2)K\right)^{1/2}\right)\Big/ K^2 - K.$$

We require

$$\frac{(1 + D^2)}{D^2}K^3 - 4K^2 + (1 + D^2)K = \square. \tag{4.4}$$

Multiply equation (4.4) by $\left(\frac{D^2 + 1}{D^2}\right)^2$ and put $\frac{(D^2 + 1)K}{D^2} = m$ (say).

$$\therefore \quad m^3 - 4m^2 + \left(\frac{D^2 + 1}{D}\right)^2 m = \square.$$

Let us put, as before, $A = D + 1/D$, then we have

$$m^3 - 4m^2 + A^2 m = t^2. \tag{4.5}$$

Equation (4.5) is an elliptic curve and has the obvious rational solution $m = 4$. We can see, by direct substitution, that if $m = m_0$ is a rational solution then $m = A^2/m_0$ is also a rational solution. Employing the same technique as before, we can put $m = n + m_0$ and consider

$$n^3 + n^2(3m_0^2 - 4) + n(3m_0 - 8m_0 + A^2) + t_0^2 = (Bn + t_0)^2, \tag{4.6}$$

which gives

$$m = \frac{(m_0^2 - A^2)^2}{4(m_0^3 - 4m_0^2 + A^2 m_0)}. \tag{4.7}$$

The right-hand side of (4.7) is unchanged if m_0 is replaced by A^2/m_0. We can therefore generate two sequences of solutions starting with $m_0 = 4$. Thus, we have

$$m_0 = 4 \quad \text{and} \quad \frac{A^2}{4}$$

$$m_1 = \frac{(16 - A^2)^2}{16A^2} \quad \text{and} \quad \frac{16A^4}{(16 - A^2)^2}$$

$$m_2 = \frac{((16 - A^2)^4 - 256A^6)^2}{64A^2(A^2 - 16)^2(A^4 + 64A^2 - 256)} \quad \text{and} \quad \frac{64A^4(A^2 - 16)^2(A^4 + 64A^2 - 256)}{((16 - A^2)^4 - 256A^6)^2}$$

etc.

Using these values of m we can determine β, and hence α, as a rational function of D. This will then give w as a rational function of D and will lead to a two-parameter solution. For $m = 4$, we have solution (2.5). For $m = A^2/4$, we have

$$\alpha = \frac{D^4 + 8D^2 - 1}{2D(D^2 - 3)} \quad \text{and} \quad \beta = \frac{5D^2 + 1}{D(D^2 - 3)}$$

with $$w = \frac{(D^2 + 1)(D^4 + 18D^2 + 1)}{4D(3D^4 - 10D^2 + 3)}.$$

With this values for w, we have

$$w^2 + 2Dw - 1 = \left(\frac{5D^6 + 27D^4 - 41D^2 + 1}{4D(3D^4 - 10D^2 + 3)}\right)^2$$

and

$$w^2 + \frac{2}{D}w - 1 = \left(\frac{D^6 - 41D^4 + 27D^2 + 5}{4D(3D^4 - 10D^2 + 3)}\right)^2.$$

Putting $D = b/c$ and removing common factors gives the solution:

$$\begin{aligned} x &= (c^2 - b^2)((b^2 + c^2)^2(b^4 + 18b^2c^2 + c^4)^2 \\ &\qquad - 16b^2c^2(3b^4 - 10b^2c^2 + 3c^4)^2) \end{aligned} \tag{4.8}$$

$$y = 8bc(c^4 - b^4)(b^4 + 18b^2c^2 + c^4)(3b^4 - 10b^2c^2 + 3c^4)$$

$$z = 2bc(b^6 - 41b^4c^2 + 27b^2c^4 + 5c^6)(5b^6 + 27b^4c^2 - 41b^2c^4 + c^6)$$

Putting $b = 2$, $c = 1$ gives

$$x = 570843, \quad y = 234960, \quad z = 1128524;$$

and putting $b = 3$, $c = 1$ gives

$$x = 153076, \quad y = 570960, \quad z = 600357.$$

Neither of these solutions is in Lal and Blundon's [3] computer-generated list.

For $m_1 = \dfrac{(16 - A^2)^2}{16A^2}$ we have, if $D = 2$, that

$$\alpha = \frac{-509}{40}, \quad \beta = \frac{-1139}{78}, \quad w = \frac{-260681}{34320};$$

thus, $a = -260681$, $b = 2$, $c = 1$, and $d = 34320$. This gives

$$x = 3(295001)(226361)$$
$$y = 6(260681)(34320) = 2^5 \cdot 3^2 \cdot 5 \cdot 11 \cdot 13 \cdot 29 \cdot 89 \cdot 101$$
$$z = 4(176041)(240479).$$

We can also determine another set of solutions of 4.5 by writing

$$n^3 + n^2(3m_0 - 4) + n(3m_0^2 - 8m_0 + A^2) + t_0^2 = (Cn^2 + Bn + t_0)^2.$$

This gives

$$m = m_0\left(\frac{m_0^4 - 6A^2m_0^2 + 16A^2m_0 - 3A^4}{3m_0^4 - 16m_0^3 + 6A^2m_0^2 - A^4}\right)^2. \tag{4.9}$$

Equation (4.9) will again generate two infinite sets of two-parameter formulas.

5. It is clear that the sequences of parametric solutions given in this paper by (3.1), (4.7), and (4.9) rapidly lead to solutions of high degree with "large" values for x, y, and z. But we know from Lal and Blundon's list [3] that there are many smaller solutions, and so there must be other parametric solutions of smaller degree, like (2.5) and (2.6). Some other solutions of degree 8 or more are given in Kraitchik [2, Ch. 5]. For each such parametric solution x, y, and z, we have the derived solution given by $X = yz$, $Y = xz$, and $Z = xy$. This effectively doubles the number of formulas. Whether there are solutions of (2.3) which give these smaller solutions remains open. It seems intuitively clear that the number of parametric solutions of given degree is finite, but that this number increases with the degree. Unfortunately, we have no idea what this rate of increase might be.

6. Finally, we see, from (2.1), that

$$x^2 + y^2 + z^2 = c^4d^4D^2\left(\frac{D^2+1}{D}\right)^2\left(w^4 + \frac{8w^3}{\left(\frac{D^2+1}{D}\right)} + 2w^2 - \frac{8w}{\left(\frac{D^2+1}{D}\right)} + 1\right).$$

Therefore, putting $D + 1/D = A$ as before, we see that $x^2 + y^2 + z^2$ is square if

$$w^4 + \frac{8}{A}w^3 + 2w^2 - \frac{8}{A}w + 1 = \square.$$

This equation is similar to (2.3). If we change A into $4/A$, we can deduce rational solutions using (3.1), starting with $w_0 = 1/A$. Therefore, we can generate a sequence of two-parameter formulas for a cuboid with edges x, y, and z^2, such that $x^2 + y^2$, $x^2 + z^2$, $y^2 + z^2$, and $x^2 + y^2 + z^2$ are all square.

A perfect cuboid would exist if we could find rational w and $A = D + \frac{1}{D} \neq 2$, where D is also rational, such that

$$w^4 + 2Aw^3 + 2w^2 - 2Aw + 1 \quad \text{and} \quad w^4 + \frac{8}{A}w^3 + 2w^2 - \frac{8}{A}w + 1$$

are both square, or if we could determine a solution $w = w(A)$ satisfying both quartics. This, of course, seems unlikely, but the problem of perfect cuboids remains stubbornly open.

REFERENCES

1. L. E. Dickson. *History of the Theory of Numbers*. Vol. 2: *Diophantine Analysis*. New York: Chelsea, 1966.
2. M. Kraitchik. *Theorie des nombres*. T. 3: *Analyse Diophantine et applications aux cuboides rationnels*. Paris: Gauthier-Villars, 1947.
3. M. Lal & W. J. Blundon. "Solutions of the Diophantine Equations $x^2 + y^2 = \ell^2$, $y^2 + z^2 = m^2$, $z^2 + x^2 = n^2$." *Math. Comp.* *20* (1966):144-147.

◆◇◆◇◆

PELL POLYNOMIALS AND A CONJECTURE OF MAHON AND HORADAM

PAUL DUVALL and THERESA VAUGHAN
University of North Carolina at Greensboro, NC 27412

(Submitted December 1986)

1. INTRODUCTION

In [1], Horadam and Mahon define a family of $n \times n$ matrices V_n in connection with the Pell polynomials $U_n(x)$. They conjecture that the characteristic polynomial of V_n is given by

$$C_n(\lambda) = \sum_{k=0}^{n} (-1)^{(k^2+k)/2}\{n, k\}\lambda^{n-k}, \tag{1.1}$$

where

$$\{n, k\} = \prod_{i=1}^{n} U_i(x) \Big/ \prod_{i=1}^{k} U_i(x) \prod_{i=1}^{n-k} U_i(x). \tag{1.2}$$

In this paper we prove the conjecture of Horadam and Mahon and also derive various other results concerning the structure of V_n and $C_n(\lambda)$.

2. NOTATION

The Pell polynomials are defined recursively by

$$U_0(x) = 0, \quad U_1(x) = 1,$$
$$U_n(x) = 2xU_{n-1}(x) + U_{n-2}(x) \qquad (n \geqslant 2)$$

and the associated Pell-Lucas polynomials by

$$W_0(x) = 2, \quad W_1(x) = 2x,$$
$$W_n(x) = 2xW_{n-1}(x) + W_{n-2}(x) \qquad (n \geqslant 2).$$

In this paper, to keep the notation as simple as possible, we shall work with the following closely related polynomials in the indeterminate t:

$$P_0(t) = 0, \quad P_1(t) = 1,$$
$$P_n(t) = tP_{n-1}(t) + P_{n-2}(t) \qquad (n \geqslant 2)$$

and

$$Q_0(t) = 2, \quad Q_1(t) = t,$$
$$Q_n(t) = tQ_{n-1}(t) + Q_{n-2}(t) \qquad (n \geqslant 2).$$

Standard manipulations with difference equations give the *Binet formulas*:

$$P_n(t) = (\alpha^n - \beta^n)/(\alpha - \beta) \quad \text{and} \quad Q_n(t) = \alpha^n + \beta^n,$$

where α, β are the roots of the polynomial $y^2 - ty - 1$;

$$= \frac{1}{2}[t + \sqrt{t^2 + 4}] \quad \text{and} \quad = \frac{1}{2}[t - \sqrt{t^2 + 4}].$$

We shall require the easily proven identity

$$P_n(t) = \sum_{k=1}^{[n/2]} \binom{n - k - 1}{k} t^{n-1-2k}. \tag{2.1}$$

V_n is defined to be the $n \times n$ matrix whose (i, j) entry is

$$(V_n)_{ij} = \binom{j - 1}{j + i - n - 1} t^{i+j-n-1},$$

for example,

$$V_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 3t \\ 0 & 1 & 2t & 3t^2 \\ 1 & t & t^2 & t^3 \end{bmatrix}.$$

3. A SIMILARITY TRANSFORMATION ON V_n

The main result of this section (Theorem 3.2) shows that V_n is similar to a particularly nice matrix in block upper triangular form. This form will lead to a recursion for the characteristic polynomial of V_n.

Let T_n be the $n \times n$ matrix whose columns carry the recurrence satisfied by $P_n(-t)$, i.e.,

$$(T_n)_{ij} = \begin{cases} 1, & \text{if } i = j \\ t, & \text{if } i = j + 1 \\ -1, & \text{if } i = j + 2 \\ 0, & \text{otherwise.} \end{cases}$$

Then we have

Lemma 3.1: The inverse of T_n is given by

$$(T_n^{-1})_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i < j \\ P_{k+1}(-t), & \text{if } i = j + k. \end{cases}$$

Proof: Let A denote the matrix defined in the statement of the Lemma, and let $B = T_n A$. Then B is lower triangular, with diagonal elements all equal to one. A typical element below the diagonal has the form

$$P_i(-t) + tP_{i-1}(-t) - P_{i-2}(-t) = P_i(-t) - (-t)P_{i-1}(-t) - P_{i-2}(-t) = 0,$$

since this is the recursion defining $P_i(-t)$. Thus, $B = I$ and $A = T_n^{-1}$. ∎

Theorem 3.2: The matrix $T_n^{-1} V_n T_n$ has the block form $\begin{bmatrix} -V_{n-2} & X \\ 0 & Y \end{bmatrix}$, where X is $(n - 2) \times 2$, Y is 2×2, and

$$Y = \begin{bmatrix} P_n(t) & P_{n-1}(t) \\ P_{n-1}(t) & P_{n-2}(t) \end{bmatrix}.$$

Proof: First we show, by induction, that the first $n - 2$ columns of the matrix

$$A = (a_{ij}) = T_n^{-1}V_nT_n$$

have the desired form.

The i^{th} row of T_n^{-1} is

$$R_i = [P_i(-t), P_{i-1}(-t), \ldots, P_2(-t), 1, 0, \ldots, 0]$$

and the j^{th} column of V_nT_n is $C_j = \operatorname{col}(x_1, \ldots, x_n)$, where

$$x_k = 0 \; (k = 1, 2, \ldots, n - j - 2)$$
$$x_{n-j-1} = -1$$
$$x_{n-j} = -\binom{j+1}{1}t + t$$
$$x_{n-j+k} = -\binom{j+1}{k+1}t^{k+1} + \binom{j}{k}t^{k+1} + \binom{j-1}{k-1}t^{k-1}.$$

Then a_{ij} is the dot product $R_i \cdot C_j$, and to start the induction, we have:

$$a_{ij} = 0 \text{ if } n - j - 2 \geqslant i$$
$$a_{ij} = -1 \text{ if } n - j - 2 = i - 1$$
$$a_{ij} = -\binom{j-1}{1}t \text{ if } n - j - 2 = i - 2$$
$$a_{ij} = -\binom{j-1}{2}t^2 \text{ if } n - j - 2 = i - 3.$$

Now suppose that, if $0 \leqslant s < r$ and $n - j - 2 = i - s$, then

$$a_{ij} = -\binom{j-1}{s-1}t^{s-1}.$$

Then, for $n - j - 2 = i - r$,

$$\begin{aligned} a_{ij} &= \sum_{k=1}^{i} P_{i+1-k}(-t)x_k = \sum_{k=i-r+1}^{i} P_{i+1-k}(-t)x_k \\ &= \sum_{k=i-r+1}^{i-1} P_{i+1-k}(-t)x_k + P_1(-t)x_i \\ &= \sum_{k=i-r+1}^{i-1} [(-t)P_{i-k}(-t) + P_{i-k-1}(-t)]x_k + P_1(-t)x_i \\ &= (-t)\left[-t^{r-2}\binom{j-1}{r-2}\right] + \left[-t^{r-3}\binom{j-1}{r-3}\right] - \binom{j+1}{r-1}t^{r-1} \\ &\qquad + \binom{j}{r-2}t^{r-1} + \binom{j-1}{r-3}t^{r-3} \end{aligned}$$

(continued)

$$= -t^{r-1}\binom{j-1}{r-1}.$$

This completes the induction.

From the definition of V_n, the j^{th} column of V_{n-2} must be

$$\operatorname{col}\left[0,\ 0,\ \ldots,\ 0,\ 1,\ \binom{j-1}{1}t,\ \binom{j-1}{2}t\ ,\ \ldots,\ \binom{j-1}{j-2}t^{j-2},\ t^{j-1}\right];$$

therefore, the upper left diagonal $(n-2)\times(n-2)$ block of $T_n^{1}V_nT_n$ is indeed $-V_{n-2}$.

The entries $a_{n-1,j}$ and $a_{n,j}$ for $1 \leqslant j \leqslant n-2$ are all zero because, if $i = n-1$, then $n-j-2 = i-r$ implies $r = j+1$. Then the term

$$-t^{r-1}\binom{j-1}{r-1} = -t^{r-1}\binom{j-1}{j} = 0.$$

If $i = n$ and $n-j-2 = i-r$, then $r = j+2$ and we have

$$-t^{r-1}\binom{j-1}{r-1} = -t^{r-1}\binom{j-1}{j+1} = 0.$$

It remains to show that the lower right diagonal 2×2 block of $T_n^{-1}V_nT_n$ is given by

$$\begin{bmatrix} P_n(t) & P_{n-1}(t) \\ P_{n-1}(t) & P_{n-2}(t) \end{bmatrix}.$$

We shall compute $a_{n,n}$ in detail. The other three cases are similar. Recalling that

$$R_n = [P_n(-t),\ P_{n-1}(-t),\ \ldots,\ P_2(-t),\ 1]$$

and

$$C_n = \operatorname{col}\left[1,\ \binom{n-1}{1}t,\ \binom{n-1}{2}t^2,\ \ldots,\ t^{n-1}\right],$$

we have

$$\begin{aligned} a_{n,n} &= \sum_{k=0}^{n-1}\binom{n-1}{k}t^kP_{n-k}(-t) \\ &= \sum_{k=0}^{n-1}\binom{n-1}{k}t^k\sum_{j=0}^{[(n-k)/2]}\binom{n-k-1-j}{j}(-t)^{n-k-1-2j}, \end{aligned}$$

by (2.1). Reversing the order of summation gives

$$a_{n,n} = \sum_{j=0}^{[n/2]}t^{n-1-2j}\sum_{k=0}^{n-2j}\binom{n-1}{k}\binom{n-j-k-1}{j}(-1)^{n-k-1-2j}.$$

Consider the inner sum

$$S = \sum_{k=0}^{n-2j}\binom{n-1}{k}\binom{n-j-k-1}{j}(-1)^{n-k-1-2j}.$$

When $k = n-2j$, the binomial coefficient $\binom{n-j-k-1}{j} = \binom{j-1}{j} = 0$, so we may take the upper limit to be $n-2j-1$.

Now, make the substitution $p = n - 2j - 1$ in S to get

$$S = \sum_{k=0}^{p} \binom{p + 2j}{k} \binom{p + j - k}{j} (-1)^{p-k} = \sum_{k=0}^{p} \binom{p + 2j}{k} \binom{p + j - k}{p - k} (-1)^{p-k}.$$

Note that $\binom{p + 2j}{k}$ is the coefficient of x^k in the expansion of $(1 + x)^{p+2j}$ and that $\binom{p + j - k}{p - k}(-1)^{p-k}$ is the coefficient of x^{p-k} in the expansion of $(1 + x)^{-j-1}$. Then S is the coefficient of x^p in the expansion of

$$(1 + x)^{p+2j-j-1} = (1 + x)^{n-j-2},$$

that is,

$$S = \binom{n - j - 2}{n - 2j - 1} = \binom{n - j - 2}{j - 1}.$$

Returning to the calculation of $a_{n,n}$, we have

$$a_{n,n} = \sum_{j=0}^{[n/2]} t^{n-1-2j} \binom{n - j - 2}{j - 1} = \sum_{k=0}^{[(n-2)/2]} \binom{n - 3 - k}{k} t^{n-3-2k}$$

(eliminating zero terms and replacing $j - 1$ by k). Thus, $a_{n,n} = P_{n-2}(t)$, by (2.1). The sums for $a_{n,n-1}$, $a_{n-1,n}$, and $a_{n-1,n-1}$ can be evaluated by the same methods, but we omit the proofs here. ■

4. THE CHARACTERISTIC POLYNOMIAL OF $V_n(t)$

Let A_n denote the matrix $T_n^{-1} V_n T_n$ and let $C_n(\lambda)$ be the characteristic polynomial of V_n. As before, let $Y = Y_n$ be the matrix

$$Y_n = \begin{bmatrix} P_n(t) & P_{n-1}(t) \\ P_{n-1}(t) & P_{n-2}(t) \end{bmatrix}.$$

In this section, we establish some basic properties of $C_n(\lambda)$ and prove the conjecture of Mahon and Horadam.

Lemma 4.1: The characteristic polynomial $C_n(\lambda)$ of V_n satisfies the recurrence:

$$C_2(\lambda) = \lambda^2 - t\lambda - 1$$
$$C_3(\lambda) = (\lambda + 1)(\lambda^2 + Q_2(t)\lambda + 1)$$
$$C_n(\lambda) = (-1)^{n-2} C_{n-2}(-\lambda)(\lambda^2 - Q_{n-1}(t)\lambda + (-1)^{n-1}).$$

Proof: Since A_n and V_n are similar, $C_n(\lambda) = |\lambda I - A_n|$. By the block form of A_n,

$$|\lambda I - A_n| = |\lambda I + V_{n-2}| \cdot |\lambda I - Y_n|.$$

Since $P_n(t)P_{n-2}(t) - P_{n-1}(t)^2 = (-1)^{n-1}$ and $P_n(t) + P_{n-2}(t) = Q_{n-1}(t)$,

$$|\lambda I - Y_n| = \lambda^2 - Q_{n-1}(t)\lambda + (-1)^{n-1}.$$

Since $|\lambda I + V_{n-2}| = (-1)^{n-2}C_{n-2}(-\lambda)$, Lemma 4.1 follows. ■

Corollary 4.2:

a) If n is even, say $n = 2k$, then

$$C_{2k}(\lambda) = \prod_{j=0}^{k-1}(\lambda^2 - Q_{n-1-2j}(t)\cdot(-1)^j\lambda - 1),$$

and the characteristic roots of $C_{2k}(\lambda)$ are

$$\{(-1)^j\alpha^{n-1-2j},\ (-1)^j\beta^{n-1-2j} : j = 0, 1, \ldots, k-1\}.$$

b) If n is odd, say $n = 2k + 1$, then

$$C_{2k+1}(\lambda) = (\lambda - (-1)^k)\prod_{j=0}^{k-1}(\lambda^2 - Q_{n-1-2j}(t)\cdot(-1)^j\lambda + 1),$$

and the characteristic roots of $C_{2k+1}(\lambda)$ are

$$\{(-1)^k,\ (-1)^j\alpha^{n-1-2j},\ (-1)^j\beta^{n-1-2j} : j = 0, 1, \ldots, k-1\}.$$

Proof: We prove b); the proof of a) is similar. From Lemma 4.1, we get

$$C_5(\lambda) = (\lambda^2 - Q_4(t)\lambda + 1)(\lambda^2 - Q_2(t)(-\lambda) + 1)(\lambda - 1),$$

and from the recurrence, for $n \geqslant 5$, we derive

$$C_n(\lambda) = (\lambda^2 - Q_{n-1}(t)\lambda + 1)(\lambda^2 - Q_{n-3}(t)(-\lambda) + 1)C_{n-4}(\lambda).$$

Since $C_3(\lambda)$ has the factor $(\lambda + 1)$, if $n \equiv 3 \pmod 4$, $C_n(\lambda)$ will also have the the factor

$$(\lambda + 1) = \lambda + (-1)^{(n-1)/2}.$$

Since $C_5(\lambda)$ has the factor $(\lambda - 1)$, if $n \equiv 1 \pmod 4$, $C_n(\lambda)$ will also have the factor

$$(\lambda - 1) = \lambda + (-1)^{(n-1)/2}.$$

The rest of b) is clear.

The characteristic roots of $C_n(\lambda)$ are the roots of its factors. We have

$$(\lambda - \alpha^j)(\lambda - \beta^j) = \lambda^2 - (\alpha^j + \beta^j)\lambda + (\alpha\beta)^j = \lambda^2 - Q_j(t) + (-1)^j$$

and

$$(\lambda + \alpha^j)(\lambda + \beta^j) = \lambda^2 - Q_j(t)(-\lambda) + (-1)^j,$$

and this completes the proof. ■

Define the coefficient $\{n, k\}$ by

$$\{n, k\} = \prod_{i=1}^{n}P_i(t)\Big/\prod_{i=1}^{k}P_i(t)\prod_{i=1}^{n-k}P_i(t)$$

and define the polynomial $R_n(\lambda)$ by

$$R_n(\lambda) = \sum_{k=0}^{n} (-1)^{(k^2+k)/2}\{n, k\}\lambda^{n-k}.$$

The next theorem states that $R_n(\lambda) = C_n(\lambda)$. Then the conjecture of Mahon and Horadam follows by making the substitution $t = 2x$.

Theorem 4.3: For all $n \geqslant 2$, $R_n(\lambda) = C_n(\lambda)$.

Proof: It is easy to verify the cases $n = 2, 3$. Thus, we need only show that $R_n(\lambda)$ satisfies the recurrence of Lemma 4.1; that is, we must show that

$$R_n(\lambda) = (-1)^n R_{n-2}(-\lambda)\cdot(\lambda^2 - Q_{n-1}(t)\lambda + (-1)^{n-1}). \tag{$*$}$$

Let $F(\lambda)$ denote the right-hand side of $(*)$, let a_j denote the coefficient of λ^j in $R_n(\lambda)$, and b_j the coefficient of λ^j in $F(\lambda)$. Then, from the definition of $R_n(\lambda)$, $a_n = 1$, $a_{n-1} = -P_n$, $a_1 = (-1)^{(n^2-n)/2}P_n$, and $a_0 = (-1)^{(n^2+n)/2}$.

The n^{th} term in $F(\lambda)$ is

$$(-1)^n(-\lambda)^{n-2}\lambda^2 = \lambda^n,$$

so $b_n = 1 = a_n$.

The $(n-1)^{\text{th}}$ term in $F(\lambda)$ is

$$\begin{aligned}&(-1)^n\lambda^2(-\lambda)^{n-2}(-1)\{n-2, 1\} + (-1)^n(-Q_{n-1}(t)\lambda)(-\lambda)^{n-2}\\ &= \lambda^{n-1}(P_{n-2}(t) - Q_{n-1}(t)) = \lambda^{n-1}(-P_{n-1}(t)),\end{aligned}$$

so $b_{n-1} = a_{n-1}$.

The constant term of $F(\lambda)$ is

$$(-1)^n(-1)^{n-1}(-1)^{(n-1)(n-2)/2} = (-1)^{(n+1)n/2},$$

so $a_0 = b_0$.

For b_1, we have

$$\begin{aligned} b_1 &= (-1)^n(-Q_{n-1}(t))\lambda(-1)^{(n-1)(n-2)/2}\\ &\qquad + (-1)^n(-1)^{n-1}(-\lambda)(-1)^{(n-2)(n-3)/2}\{n-2, n-3\}\\ &= (-1)^{n(n-1)/2}(Q_{n-1}(t) - P_{n-2}(t))\lambda\\ &= (-1)^{n(n-1)/2}P_n(t),\end{aligned}$$

giving $a_1 = b_1$.

For the remaining coefficients we need to show that, for $2 \leqslant k \leqslant n-2$, $a_{n-k} = b_{n-k}$; that is,

$$\begin{aligned}(-1)^{(k+1)k/2}\{n, k\} &= (-1)^n(-1)^{n-k-2}(-1)^{(k+1)k/2}\{n-2, k\}\\ &\quad + (-1)^n(-1)^{n-k-1}(-1)^{k(k-1)/2}\{n-2, k-1\}(-Q_{n-1}(t))\\ &\quad + (-1)^n(-1)^{n-k}(-1)^{(k-1)(k-2)/2}\{n-2, k-2\}(-1)^{n-1}.\end{aligned}$$

Clearing signs, this reduces to

$$\{n, k\} = (-1)^k\{n-2, k\} + Q_{n-1}(t)\{n-2, k-1\} + (-1)^{n+k}\{n-2, k-2\}. \quad (**)$$

Factoring out $\{n - 2, k - 1\}$ reduces (**) to

$$\frac{P_n(t)P_{n-1}(t)}{P_k(t)P_{n-k}(t)} = (-1)^k \frac{P_{n-k-1}(t)}{P_k(t)} + Q_{n-1}(t) + (-1)^{n+k} \frac{P_{k-1}(t)}{P_{n-k}(t)}.$$

Thus, it suffices to show that for $2 \leqslant k \leqslant n - 2$,

$$P_n(t)P_{n-1}(t) - P_k(t)P_{n-k}(t)Q_{n-1}(t) = (-1)^k P_{n-k}(t)P_{n-k-1}(t) + (-1)^{n-k}P_k(t)P_{k-1}(t).$$

This last identity is proven using the Binet formulas and the properties of α and β. For convenience, denote $P_n(t)$ by P_n and so on. First,

$$P_nP_{n-1} = (\alpha^n - \beta^n)(\alpha^{n-1} - \beta^{n-1})/(\alpha - \beta)^2 = Q_{2n-1} + (-1)^n Q_1,$$

and

$$\begin{aligned} Q_{n-1}P_kP_{n-k} &= (\alpha^{n-1} + \beta^{n-1})(\alpha^n + \beta^n - \beta^k\alpha^{n-k} - \alpha^k\beta^{n-k})/(\alpha - \beta)^2 \\ &= (\alpha^{2n-1} + \beta^{2n-1} + (-1)^{n-1}(\beta + \alpha) - (-1)^k(\alpha^{2n-2k-1} \\ &\quad + \beta^{2n-2k-1}) - (-1)^{n-k}(\alpha^{2k-1} + \beta^{2k-1}))/(\alpha - \beta)^2 \\ &= (Q_{2n-1} + (-1)^{n-1}Q_1 + (-1)^{k+1}Q_{2n-2k-1} \\ &\quad + (-1)^{n-k-1}Q_{2k-1})/(\alpha - \beta)^2. \end{aligned}$$

Then

$$P_nP_{n-1} - P_kP_{n-k}Q_{n-1} = ((-1)^kQ_{2n-2k-1} + (-1)^{n-k}Q_{2k-1} + 2(-1)^nQ_1)/(\alpha - \beta)^2.$$

On the other side,

$$\begin{aligned} &(-1)^kP_{n-k}P_{n-k-1} + (-1)^{n-k}P_kP_{k-1} \\ &= (-1)^k(Q_{2n-2k-1} + (-1)^{n-k}Q_1)/(\alpha - \beta)^2 \\ &\quad + (-1)^{n-k}(Q_{2k-1} + (-1)^kQ_1)/(\alpha - \beta)^2 \\ &= ((-1)^kQ_{2n-2k-1} + (-1)^{n-k}Q_{2k-1} + 2(-1)^nQ_1)/(\alpha - \beta)^2. \end{aligned}$$

Thus, the identity is true, and (**) is true; that is, $a_{n-k} = b_{n-k}$ for all k, $2 \leqslant k \leqslant n - 2$. Then $R_n(\lambda)$ satisfies the recurrence and initial conditions of Lemma 4.1, and it follows that $R_n(\lambda) = C_n(\lambda)$. ■

5. THE EIGENVECTORS OF V_n

The eigenvectors of V_n can be computed in a recursive way. The initial cases are given below.

Lemma 5.1: V_2 has eigenvalues α, β. Eigenvectors $\mathbf{v}_1$ and $\mathbf{v}_2$ corresponding to α and β are given by

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ \alpha \end{bmatrix}, \quad \mathbf{v}_2 = \begin{bmatrix} 1 \\ \beta \end{bmatrix}.$$

The matrix V_3 has eigenvalues -1, α^2, β^2 with corresponding eigenvectors $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$ given by

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ t \\ -1 \end{bmatrix}, \quad \mathbf{v}_2 = \begin{bmatrix} 1 \\ 2\alpha \\ \alpha^2 \end{bmatrix}, \quad \mathbf{v}_3 = \begin{bmatrix} 1 \\ 2\beta \\ \beta^2 \end{bmatrix}. \quad \blacksquare$$

Lemma 5.2: Let $\mathbf{u} = \mathrm{col}(u_1, u_2, \ldots, u_n)$ and $\mathbf{w} = \mathrm{col}(w_1, w_2, \ldots, w_n)$ be adjacent columns of V_n, with $\mathbf{u}$ to the left of $\mathbf{w}$. Then

$$tu_n = w_n$$
$$tu_i + u_{i+1} = w_i \quad (i = 1, 2, \ldots, n - 1).$$

Proof: If $\mathbf{u}$ is column j, then for $i = 1, 2, \ldots, n - j - 1$ we have $u \;\; = 0$ and $tu_i + u_{i+1} = w_i$. If $i = n - j + k$ for some k, $0 \leqslant k < j$, then

$$tu_i + u_{i+1} = t\binom{j-1}{i-1}t^{i-1} + \binom{j-1}{i}t^i = \binom{j}{i}t^i = w_i.$$

Since $u_n = t^{j-1}$ and $w_n = t^j$, we have $tu_n = w_n$. $\blacksquare$

Corollary 5.3: Define vectors $\mathbf{x}$ and $\mathbf{y}$ by

$$\mathbf{x} = \mathrm{col}(\underbrace{0, \ldots, 0}_{j}, x_1, \ldots, x_t, \underbrace{0, \ldots, 0}_{k})$$

$$\mathbf{y} = \mathrm{col}(\underbrace{0, \ldots, 0}_{j+1}, x_1, \ldots, x_t, \underbrace{0, \ldots, 0}_{k-1})$$

where $j + t + k = n$ and $k > 0$. Put

$$\mathbf{u} = V_n\mathbf{x} \quad \text{and} \quad \mathbf{v} = V_n\mathbf{y}$$

with $\mathbf{u} = \mathrm{col}(u_1, \ldots, u_n)$ and $\mathbf{v} = \mathrm{col}(v_1, \ldots, v_n)$. Then $tu_i + u_{i+1} = v_i$.

Proof: Let $\mathbf{e}_k$ denote the column vector with 1 in the k^{th} place and 0 everywhere else. By Lemma 5.2, the result is true for

$$\mathbf{x} = \mathbf{e}_{j+1} \quad \text{and} \quad \mathbf{y} = \mathbf{e}_{j+2} \quad (j + 2 \leqslant n),$$

and hence is true in general by linearity. $\blacksquare$

Theorem 5.4: Let $n > 1$ be odd, so that V_n has

$$\varepsilon = (-1)^{(n-1)/2}$$

as an eigenvalue. Let

$$\mathbf{v} = \mathrm{col}(v_1, \ldots, v_n)$$

be an eigenvector corresponding to ε. Put

$$\begin{aligned} \mathbf{w} &= \mathrm{col}(v_1, \ldots, v_n, 0, 0) \\ &\quad + \mathrm{col}(0, tv_1, \ldots, tv_n, 0) \\ &\quad + \mathrm{col}(0, 0, -v_1, \ldots, -v_n). \end{aligned}$$

Then $\mathbf{w}$ is an eigenvector for V_{n+2}, corresponding to the eigenvalue

$$-\varepsilon = (-1)^{(n+1)/2}.$$

Proof: Put $\mathbf{w} = \mathbf{w}_1 + \mathbf{w}_2 + \mathbf{w}_3$, where the $\mathbf{w}_i$ are the summands in the statement of the Theorem. From the form of V_n (it has V_{n-2} in the lower left block, with zeros above it), it is clear that

$$V_{n+2}\mathbf{w}_1 = \varepsilon(0, 0, v_1, \ldots, v_n)$$

since $\mathbf{v}$ is an eigenvector for V_n corresponding to ε. Then by Corollary 5.3,

$$V_{n+2}\mathbf{w}_2 = t\varepsilon[(0, v_1, \ldots, v_n, 0) + t(0, 0, v_1, \ldots, v_n)]$$

$$V_{n+2}\mathbf{w}_3 = -\varepsilon[\mathbf{w}_1 + 2\mathbf{w}_2 - t^2\mathbf{w}_3]$$

so

$$V_{n+2}\mathbf{w} = \varepsilon(-\mathbf{w}_1 - \mathbf{w}_2 - \mathbf{w}_3) = -\varepsilon\mathbf{w}. \blacksquare$$

Theorem 5.5: Suppose that $\mathbf{v} = \operatorname{col}(v_1, \ldots, v_{n-1})$ is an eigenvector for V_{n-1} corresponding to the eigenvalue α^i ($i \geqslant 0$). Put

$$\mathbf{w} = \operatorname{col}(v_1, \ldots, v_{n-1}, 0) + \alpha \operatorname{col}(0, v_1, \ldots, v_n) = \mathbf{x} + \alpha\mathbf{y}.$$

Then $\mathbf{w}$ is an eigenvector for V_n corresponding to the eigenvalue α^{i+1}.

Proof: We have

$$V_n\mathbf{x} = \alpha^i\mathbf{y}$$

$$V_n\mathbf{y} = \alpha^i\mathbf{x} + \alpha^i t\mathbf{y}$$

so that

$$V_n(\mathbf{x} + \alpha\mathbf{y}) = \alpha^i(\mathbf{y} + \alpha\mathbf{x} + \alpha t\mathbf{y}).$$

Since $\alpha^2 = 1 + \alpha t$,

$$V_n(\mathbf{x} + \alpha\mathbf{y}) = \alpha^i(\alpha\mathbf{x} + \alpha^2\mathbf{y}) = \alpha^{i+1}(\mathbf{x} + \alpha\mathbf{y})$$

as required. $\blacksquare$

Remark: The analogous result also holds for the eigenvectors corresponding to the eigenvalues β^i.

Corollary 5.6: All of the eigenvectors of V_n can be computed in terms of the eigenvectors of V_{n-1} and V_{n-2}. $\blacksquare$

REFERENCE

1. J. M. Mahon & A. F. Horadam. "Matrix and Other Summation Techniques for Pell Polynomials." *The Fibonacci Quarterly* 24, no. 4 (1986):290-308.

◆◇◆◇◆

CONVOLUTION TREES AND PASCAL-T TRIANGLES

JOHN C. TURNER
University of Waikato, Hamilton, New Zealand

(Submitted December 1986)

1. INTRODUCTION

Pascal (1623-1662) made extensive use of the famous arithmetical triangle which now bears his name. He wrote upon its properties in 1653, but the paper was not printed until 1665 ([1], "Traité du triangle arithmétique"). The triangle now appears in virtually every text on elementary combinatorics. All textbook authors note the recurrence relation satisfied by binomial coefficients in adjacent rows of the triangle, and a few point out the "curious" fact that certain diagonals of the triangle have Fibonacci numbers as their sums (apparently first noted by E. Lucas in 1876).

In this paper we give a graph theory approach that provides an easy access to associations between Pascal-T triangles and generalized Fibonacci sequences. The approach is to use certain sequences of tree graphs, which are called *convolution trees* for a reason which is explained in Section 3. These trees consist of nodes and branches that are introduced and "grown" according to a given construction rule; integer weights are assigned to the nodes as the construction proceeds.

The weights are obtained from a *color sequence* $\{c_n\}$, and they are assigned to the nodes in a well-defined manner. The choice of generalized Fibonacci sequences of use for $\{c_n\}$ enables many attractive identities to be discovered, almost by inspection.

In Section 6 we define a *level counting function* for the trees that counts certain of the colored nodes in the trees and also provides generalizations of Pascal's triangle. The arithmetic triangles which arise are known as Pascal-T triangles [2].

The main results of the paper are collected together as Theorem 5 in Section 6. This demonstrates the links between various properties of the Pascal-T triangles and the generalized Fibonacci sequences which the study of colored convolution trees reveals.

A *graph* is a set of *nodes* (or *points*) together with a set of *edges* (in tree graphs they are often called *branches*). An *edge* is, informally, a line joining two of the nodes. The total number of edges which attach to a given node is the *valency* (or *degree*) of that node. A *circuit* is a *path* in a graph which proceeds from node-edge-node-edge-node- $\cdots$ -node and is such that the first node and the last node are the same node.

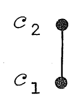
A *tree* is a graph that has no circuits.

In a tree we may distinguish any one node and call it the *root* of the tree. Then we may distinguish all nodes in the tree (other than the root) whose valencies are one (unity) and call them *leaf nodes*.

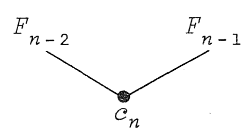
We are now in a position to present the rules by which colored convolution trees are constructed.

2. FIBONACCI CONVOLUTION TREES

The Fibonacci convolution trees are defined by a *recurrence construction* which builds the trees $\{F_n\}$ sequentially, assigning the integer weights or *colors* $\{c_n\}$ as they are built. A similar construction (but not the coloring) was given in [3]. The method parallels the definition of Fibonacci numbers (namely $f_n = f_{n-2} + f_{n-1}$, with $f_1 = 1$, $f_2 = 1$), with a binary operation $\oplus$ that works as follows. We define the initial colored rooted trees in the sequence to be

$F_1 \equiv c_1$ • and $F_2 \equiv$ 

Then, given any two consecutive trees F_{n-2}, F_{n-1}, we obtain the next tree by $F_n = F_{n-2} \oplus F_{n-1}$, the joining operation $\oplus$ being indicated by the diagram:



$\equiv F_n$.

Note that one new root node, labelled c_n, is introduced during this operation. Figure 1 shows the first four trees in the sequence. In Figure 1 and in subsequent tree diagrams, the color alone is used to depict the colored node, for convenience.

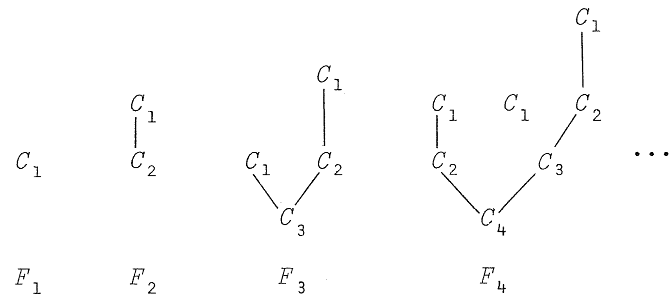


Figure 1. Fibonacci Convolution Tree Sequence

3. PROPERTIES OF A CONVOLUTION TREE

We next tabulate basic graph properties of the convolution trees. It will be seen that the parameters listed have an attractive set of formulas in terms of the Fibonacci numbers $\{f_n\} = \{1, 1, 2, 3, 5, \ldots\}$. Some graph terms used in the table may require definition for the reader, thus:

> In any rooted tree a unique path may be traced from the root to any other given node in the tree. The number of edges (branches) in that path is called the *level* of the given node. The *height* of a convolution tree is the maximum level occurring.

The symbols $(\mathbf{c} * \mathbf{f})_n$ refer to the n^{th} term of the convolution of sequences $\mathbf{c}$ and $\mathbf{f}$; this term is defined to be $c_1f_n + c_2f_{n-1} + \cdots + c_nf_1$.

Table 1. Properties of Fibonacci Convolution Trees

	Parameter		Formula (for F_n)
(i)	Number of nodes		$F^n \equiv \sum_1^n f_i$
(ii)	Number of edges		$F^n - 1$
(iii)	Number of nodes of valency v: ($n > 2$)	$v = 1$	f_n
		$v = 2$	$f_{n-1} + 1$
		$v = 3$	$f_n - 2$
(iv)	Number of leaf nodes		f_n
(v)	Height		$n - 1$
(vi)	Weight (sum of node colors)		$(\mathbf{c} * \mathbf{f})_n$
(vii)	Lowest leaf-node level		$\left[\frac{n}{2}\right]$
(viii)	Number of leaf nodes at level m		$\binom{m}{n-m-1}$

Proofs: All of the formulas given in the table can be proved using a combination of graph definitions, the tree construction rule, simple algebra, and mathematical induction.

The convolution result (vi) is the reason for the name we gave to the tree graphs. To demonstrate a proof method, we shall give the proof for (vi) only. It is proved as follows: using $\Omega(F)$ to mean "weight of F" (i.e., the sum of the node colors in F), we have, from the construction rule,

$$\Omega(F_n) = \Omega(F_{n-2}) + \Omega(F_{n-1}) + c_n, \text{ for } n \geqslant 2. \tag{1}$$

Noting that $\Omega(F_1) = c_1 f_1 = (\mathbf{c} * \mathbf{f})_1$, and $\Omega(F_2) = c_1 f_2 + c_2 f_1 = (\mathbf{c} * \mathbf{f})_2$, it is easy to proceed by induction. That is, we may show that, if

$$\Omega(F_i) = c_1 f_i + c_2 f_{i-1} + \cdots + c_i f_1 = (\mathbf{c} * \mathbf{f})_i$$

for $i = 1, 2, \ldots, n$, then

$$\Omega(F_{n+1}) = (\mathbf{c} * \mathbf{f})_{n+1}.$$

We leave the details to the reader.

4. SOME THEOREMS DERIVED FROM THE TREES

Weighted convolution trees are structured configurations of integers, and in the long tradition of such structures (c.f. figurate numbers, Ferrer's diagrams and the like) they can be used to reveal identities and relations between given sequence elements. The next four theorems illustrate many interesting relations between Fibonacci numbers, Fibonacci convolutions, and binomial coefficients.

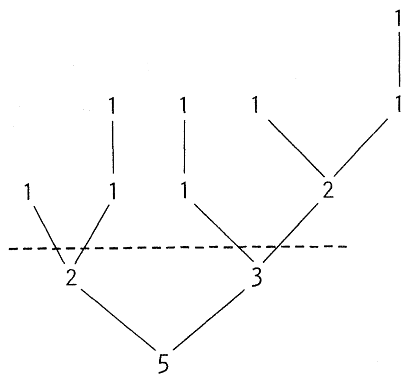
Theorem 1 (Lucas, 1876): $f_n = \sum_m \binom{m}{n-m-1}$ with m varying from $\left[\frac{n}{2}\right]$ to $n-1$, where $[x]$ is the greatest integer function.

This follows from formulas (iv) and (viii) of Table 1.

Theorem 2: Let $r = \left[\frac{n-1}{2}\right]$ with $n \geqslant 3$. Then

$$rf_n = (\mathbf{f} * \mathbf{f})_n - \sum_{i=0}^{r} \binom{r}{i} (\mathbf{f} * \mathbf{f})_{i+1}.$$

Proof strategy: This theorem gives a relationship between Fibonacci integers, terms of the convolution sequence $\mathbf{f} * \mathbf{f}$, and binomial coefficients. It is an example of how interesting identities may be discovered virtually by inspection of the colored convolution trees. We shall describe the proof strategy with reference to tree F_5. The reader may care to fill in the details of the proof, and then to look for other identities of a similar nature.



Tree F_5

First we note that a cut along a dotted line drawn immediately below the lowest leaf-node (which is $[n/2]$; see Table 1(vii)) would, in effect, split the tree into a lower portion that is a full binary-tree and an upper collection of separated smaller convolution trees.

By *full binary tree* we mean a rooted tree of which the root node has valency two, and all other non-leaf nodes have valency three.

Next we observe that the smaller convolution trees are F_1, F_2, and F_3 and that they occur with frequencies given by the binomial coefficients

$$\binom{r}{0}, \binom{r}{1}, \text{ and } \binom{r}{2}, \text{ with } r = \left[\frac{n}{2}\right] = 2.$$

Collecting this information together, and equating the weight of F_5 to the sum of the weights of all the subtrees we have described, we get

$$\Omega(F_5) = (\mathbf{f} * \mathbf{f})_5 = \Omega(\text{full binary tree}) + \sum_{i=0}^{2} \binom{2}{i} (\mathbf{f} * \mathbf{f})_{i+1}.$$

Finally, inspection of the full binary tree reveals that the sum of the colors on the nodes at each level is f_5; and there are $r = 2$ levels, so

$$\Omega(\text{full binary tree}) = 2f_5.$$

Inserting this in the above equation and rearranging to place $2f_5$ alone on the left-hand side, we obtain a demonstration of the formula for the tree F_5.

Each one of the observations made with regard to the properties of the subtrees of F_5 can be shown by induction to hold, generally, for subtrees obtained similarly from tree F_n. Then the proof strategy carries through for F_n, for $n \geqslant 3$.

Note that the Lucas sum for f_n from Theorem 1 can be exchanged for f_n in Theorem 2 and another identity obtained immediately.

Theorem 3 (general $\mathbf{c}$): We have already noted in Section 3 the *fundamental convolution property*, namely,

$$(\mathbf{c} * \mathbf{f})_n = (\mathbf{c} * \mathbf{f})_{n-2} + (\mathbf{c} * \mathbf{f})_{n-1} + c_n,$$

where $\mathbf{f}$ is the Fibonacci sequence and $\mathbf{c} = \{c_1, c_2, \ldots\}$.

We now examine the effect on the total weight, say $\Omega_n(\mathbf{c})$, of the n^{th} convolution tree when $\mathbf{c}$ is changed to $\mathbf{c}^{(r)} = \{c_{r+1}, c_{r+2}, \ldots\}$. In terms of the shift operator E, operating on the subscripts of the sequence terms c_i, we can write $\mathbf{c}^{(1)} = E\mathbf{c}$; and, in general, $\mathbf{c}^{(r)} = E^r\mathbf{c} = \{c_{r+1}, \ldots\}$. Let us also introduce the difference operator Δ, now operating on subscripted terms, so that $\Delta\mathbf{c} = \{c_2 - c_1, c_3 - c_2, \ldots\}$; and then $\Delta^2\mathbf{c} = \Delta(\Delta\mathbf{c})$, and so on to $\Delta^r\mathbf{c}$ in general. Then the following results hold, pertaining to the total weight of the convolution trees. We now give Theorem 4 as further illustration of how attractive identities and formulas (this time involving E and Δ) can be derived with little effort from the colored tree sequence.

Theorem 4:

(i) $\delta_n^{(1)} \equiv \Omega_n(E\mathbf{c}) - \Omega_n(\mathbf{c}) = (\mathbf{f} * \Delta\mathbf{c})_n;$

$\vdots$

$$\delta_n^{(r)} \equiv \Omega_n(E^r\mathbf{c}) - \Omega_n(\mathbf{c}) = (\mathbf{f} * E^{r-1}(\Delta\mathbf{c}))_n + \sum_{j=1}^{r-1} \delta_n^{(j)}, \quad r \geqslant 2.$$

(ii) (setting $\mathbf{c} = \mathbf{f}$)

(a) $\Delta\mathbf{c} = \Delta\mathbf{f} = E^{-1}\mathbf{f}; \quad (\mathbf{f} * \Delta^r\mathbf{f})_n = (\mathbf{f} * E^r\mathbf{f})_{n-r}.$

(b) $(\mathbf{f} * \mathbf{f})_n = f_n + (\mathbf{f} * E\mathbf{f})_{n-1}.$

(c) $\Omega_n(E^r\mathbf{f}) = \Omega_n(E^{r-2}\mathbf{f}) + \Omega_n(E^{r-1}\mathbf{f}),\ r > 2$, with

$\Omega_n(E^r\mathbf{f}) = (\mathbf{f} * \mathbf{f})_n$ when $r = 0$, and

$\qquad = (\mathbf{f} * \mathbf{f})_n + (\mathbf{f} * \mathbf{f})_{n-1}$ when $r = 1$.

(iii) [corollary of (ii)(c), writing $\Omega_{n,r}$ for $\Omega_n(E^r\mathbf{f})$]

$$\Omega_{n,r} = (\mathbf{f} * \mathbf{f})_n f_{r+1} + (\mathbf{f} * \mathbf{f})_{n-1} f_r, \quad r \geqslant 1.$$

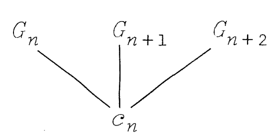
The proofs of (i), (ii), and (iii) require only simple algebra and Fibonacci number identities.

5. HIGHER ORDER CONVOLUTION TREES

The construction rules given in Section 2 may be extended to define sequences of higher-order convolution trees. Thus, for third-order trees:

Recurrence rule: $G_{n+3} = G_n \oplus G_{n+1} \oplus G_{n+2}$, using a triple fork to effect the tree combinations thus:

$G_{n+3} \equiv$



In Figure 2 we show the first five trees in the sequence obtained when the F_1, F_2, F_3 trees are used as the initial ones.

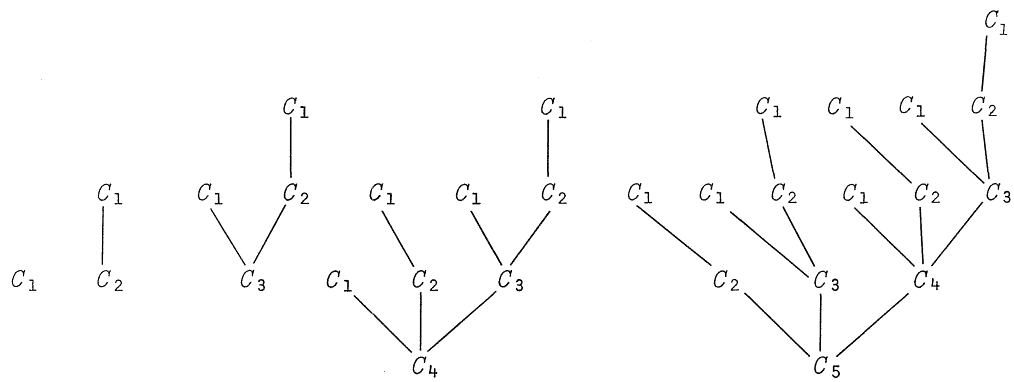


Figure 2. The First Five Third-Order Convolution Trees

We will not tabulate their structural properties as we did for the second-order ones, but we may note that the numbers of leaf nodes follow the sequence $\mathbf{g} = \{1, 1, 2, 4, 7, \ldots\}$, and that the weight $\Omega(G_n)$ can be shown to be $(\mathbf{c} * \mathbf{g})_n$, which are generalizations of the second-degree convolution tree properties.

We are now in a position to derive Pascal-*T* triangles from the sequences of trees.

6. A COMBINATORIC FUNCTION AND THE PASCAL-*T* TRIANGLES

Consider the convolution tree G_n, colored by integers of the sequence $\mathbf{c} = \{c_1, c_2, c_3, \ldots\}$. We define the *level counting function*:

$$L \equiv \binom{n}{m|i} \equiv \text{the number of nodes in } G_n \text{ having level } m \text{ and color } c_i.$$

Then, if G is defined in some tree sequence $\{G_n : n = 1, 2, 3, \ldots\}$, we can tabulate L in a sequence of (m, n) tables for each value of i. We show tables for the second- and third-order trees with regard to color c_1 only.

Table 2. $\binom{n}{m|1}$ for the Second-Order Trees F_n

m \ n	F_1	F_2	F_3	F_4	F_5	F_6	F_7	Row Sum
0	1	0	0	0	0	0	0 ...	1
1	0	1	1	0	0	0	0 ...	2
2	0	0	1	2	1	0	0 ...	4
3	0	0	0	1	3	3	1 ...	8
4	0	0	0	0	1	4	6 ...	(16)
5	0	0	0	0	0	1	5 ...	(32)
6	0	0	0	0	0	0	1 ...	(64)
Column Sum	1	1	2	3	5	8	13 ...	

We observe the following:

(i) the nonzero elements correspond to Pascal's triangle, the rows beginning on the diagonal; let us designate this triangle $\Delta^{(2)}$;

(ii) the m^{th} row sum of the table is 2^m;

(iii) the j^{th} column sum of the table is f_j, the j^{th} Fibonacci number.

Table 3. $\binom{n}{m|1}$ for the Third-Order Trees G_n

m \ n	G_1	G_2	G_3	G_4	G_5	G_6	G_7	Row Sum
0	1	0	0	0	0	0	0 ...	1
1	0	1	1	1	0	0	0 ...	3
2	0	0	1	2	3	2	1 ...	9
3	0	0	0	1	3	6	7 ...	(27)
4	0	0	0	0	1	4	10 ...	(81)
5	0	0	0	0	0	1	5 ...	(243)
6	0	0	0	0	0	0	1 ...	(729)
Column Sum	1	1	2	4	7	13	24 ...	

Notes:

(i) the triangle now resting on the leading diagonal is the third-degree one, $\Delta^{(3)}$;

(ii) the m^{th} row sum of the table is 3^m;

(iii) the j^{th} column sum of the table is g_j, where g is defined by

$$g_{n+3} = g_n + g_{n+1} + g_{n+2},$$

with $(g_1, g_2, g_3) = (f_1, f_2, f_3)$, a generalized Fibonacci sequence.

It should be clear from the construction rules given in Section 5 how we can extend the order of convolution trees indefinitely, obtaining the sequence $\{G_2\}$, $\{G_3\}$, $\{G_4\}$, ... of tree sequences. Then, tabulating $\binom{n}{m|1}$ for each would give a sequence of the triangles $\Delta^{(\delta)}$, $\delta = 2, 3, 4, \ldots$; and the row and column sums of the tables would be, respectively, powers of δ and generalized Fibonacci numbers.

We note also that every $\binom{n}{m|1}$ is a multinomial coefficient; it is easy to show that the m-row elements in each table are generated by the function:

$$x(x + x^2 + x^3 + \cdots + x^\delta)^m,$$

where δ is the order of the trees being considered.

We show below the second-, third-, and fourth-order triangles in the form that Pascal's triangle is usually shown. We do this in order to comment on the generalized row-to-row method of constructing the elements.

$\Delta^{(2)}$

1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

... ...

$\Delta^{(3)}$

1

1 1 1

1 2 3 2 1

1 3 6 7 6 3 1

1 4 10 16 19 16 10 4 1

... ...

$\Delta^{(4)}$

1

1 1 1 1

1 2 3 4 3 2 1

1 3 6 10 12 12 10 6 3 1

1 4 10 20 31 40 44 40 31 20 10 4 1

... ...

Figure 3. Pascal-T Triangles

Note that, in each case, to get the j^{th} element in the m^{th} row, take the sum of the δ ($\delta = 2, 3, 4$) elements immediately above it in the preceding [i.e., the $(m-1)^{\text{th}}$] row. Use zeros if the summation has to extend beyond a boundary of the triangle. For example, to get 10, the third element in row 5 of $\Delta^{(4)}$, we add 0 + 1 + 3 + 6.

Theorem 5 (Pascal-Lucas-Turner): Let S_δ be a sequence of colored convolution trees of order δ, $\delta = 2, 3, 4, \ldots$. Then the level function $\binom{n}{m|i}$, with $i = 1$, has a table of values with the following properties:

(i) $m = 0, 1, 2, \ldots$; $n = 1, 2, 3, \ldots$;

(ii) the leading diagonal elements are all 1's, and elements below this diagonal are all 0's;

(iii) the sum of the m-row elements is δ^m;

(iv) the sum of the n-column elements is g_n, where g is the generalized Fibonacci sequence defined by

$$g_{n+\delta} = \sum_{i=0}^{\delta-1} g_{n+i}, \text{ with initial values } f_1, f_2, \ldots, f_\delta;$$

(v) $\binom{n}{m|1}$ is the coefficient of x^n in the expansion of $x\left(\sum_{i=1}^{\delta} x^i\right)^m$;

(vi) $\binom{n}{m|1} = \binom{n-1}{m-1|1} + \binom{n-2}{m-1|1} + \cdots + \binom{n-\delta}{m-1|1}$ for $n > 1$, $m > 0$; with

$$\binom{1}{0|1} = 1, \binom{n}{0|1} = 0, \text{ for } n > 1, \text{ and } \binom{n-i}{m-1|1} \equiv 0 \text{ when } n < i.$$

Proofs: The proofs follow directly from the recurrence construction rules for the trees.

7. OTHER LEVEL-FUNCTION TRIANGLES

Although we have presented our topic so far by showing how level functions (with $i = 1$) provide Pascal's triangle and generalizations of it, we would now like to shift the point of view firmly.

In the theory of convolution trees, the level function seems to us to be an important object of study. Every sequence of convolution trees gives rise to a sequence of tables for the level functions $\binom{n}{m|i}$, and the types of values they take depend entirely on the construction rules used to define the trees. Changing the tree recurrences, or the initial trees, or using a more complex coloring rule, will produce triangles of numbers which are not, in general, multinomial coefficients. If generating functions can be found, they will be more complex than the ones given above.

Therefore, we wish to view the tabulation of level functions of convolution trees as a broad topic in its own right. Pascal's triangle arises as a special case in connection with second-order Fibonacci trees.

For reasons of space we cannot give many examples of other triangles here; however, we discuss two further cases to help make our point clear. The first gives rise to "shifted" Pascal triangles; the second arises from Lucas trees, and turns out to be a superposition of two Pascal triangles.

Case 1. $\binom{n}{m|2}$, **from the Fibonacci trees**

If we look at the rooted trees in $\{F_i\}$ and $\{G_i\}$, we see that all the leaf nodes are colored c_1. Pruning any tree F_n (i.e., removing all the leaf nodes and their adjacent branches) leaves the tree F_{n-1}, but with colors c_2, c_3, c_4, ... instead of c_1, c_2, c_3, ...

Hence, the table of $\binom{n}{m|2}$ again has a Pascal triangle in it, but "shifted to the right" and starting at the diagonal above the leading diagonal.

Similarly, $\binom{n}{m|3}$ has a Pascal triangle shifted one step further to the right; and so on.

Case 2. $\binom{n}{m|1}$, **Lucas convolution trees**

Using a special initial tree, L_2, we can generate the sequence L_1, L_2, L_3, ..., called Lucas convolution trees and shown below in Figure 4. Note that the numbers of leaves follow the Lucas sequence $\ell = 1, 3, 4, 7, \ldots$, which is generated by the recurrence equation $\ell_{n+2} = \ell_n + \ell_{n+1}$, with $\ell_1 = 1$, $\ell_2 = 3$. The color sequence used is $\mathbf{c} = (c_0, c_1, c_2, c_3, \ldots)$; the recurrence construction begins with tree L_3 and color c_4.

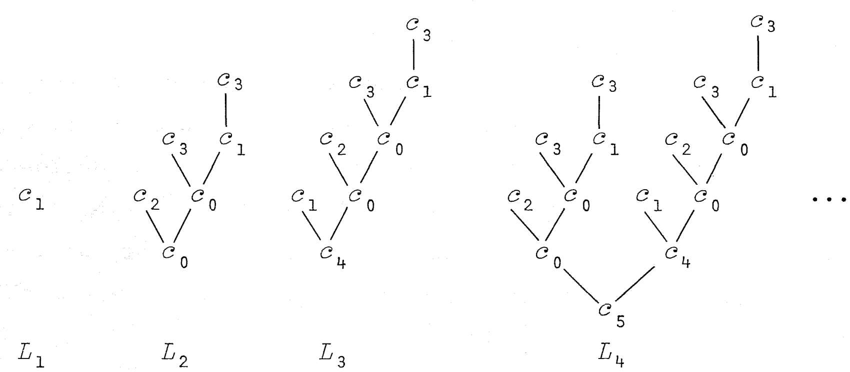


Figure 4. The Lucas Convolution Trees

These trees have many properties which relate the Fibonacci and Lucas numbers. We give the table for $\binom{n}{m|1}$, then follow it by the Lucas-T triangle for this level function.

Table 4. $\binom{n}{m|1}$ for the Second-Order Lucas Trees

m \ n	L_1	L_2	L_3	L_4	L_5	L_6	L_7	Row Sum
0	1	0	0	0	0	0	0 ...	1
1	0	0	1	0	0	0	0 ...	1
2	0	1	0	1	1	0	0 ...	$3 \times 2^0 = 2^0 + 2^1$
3	0	0	1	1	1	2	1 ...	$3 \times 2^1 = 2^1 + 2^2$
4	0	0	0	1	2	2	3 ...	$3 \times 2^2 = 2^2 + 2^3$
5	0	0	0	0	1	3	4 ...	$3 \times 2^3 = 2^3 + 2^4$
6	0	0	0	0	0	1	4 ...	$3 \times 2^4 = 2^4 + 2^5$
Column Sum	1	1	2	3	5	8	...	

Note that the row sums are (after $m = 1$) expressible as $2^{m-2} + 2^{m-1}$, and that the column sums are again Fibonacci numbers. The diagram below shows (by dotted and full lines) how the triangle from these Lucas trees is the superposition of two Pascal triangles (after $m = 0$).

$$
\begin{array}{ccccccccccccccc}
 & & & & & & & 1 & & & & & & & \\
 & & & & & & 0 & & 1 & & & & & & \\
 & & & & & 1 & & 0 & & 1 & & 1 & & & \\
 & & & & 1 & & 1 & & 1 & & 2 & & 1 & & \\
 & & & 1 & & 2 & & 2 & & 3 & & 3 & & 1 & \\
 & & 1 & & 3 & & 4 & & 5 & & 6 & & 4 & & 1 \\
 & 1 & & 4 & & 7 & & 9 & & 11 & & 10 & & 5 & & 1 \\
 & & & \cdots & & & & \cdots & & & & \cdots & & &
\end{array}
$$

Figure 5. The Lucas $\binom{n}{m|1}$ Triangle

We have developed a notation for writing the $\binom{n}{m|i}$ triangles to be derived from various types of recurrently constructed and colored trees, expressing them as superpositions of triangles of multinomial coefficients. The formulas can be given once the construction and coloring rules are given.

REFERENCES

1. D. E. Smith. *A Source Book in Mathematics*. New York: Dover, 1959.
2. S. J. Turner. "Probability via the N^{th} Order Fibonacci-T Sequence." *The Fibonacci Quarterly 17*, no. 1 (1979):23-28.
3. Y. Horibe. "Notes on Fibonacci Trees and Their Optimality." *The Fibonacci Quarterly 20*, no. 2 (1983):118-128.

◆◇◆◇◆

A NOTE ON THE THIRD-ORDER STRONG DIVISIBILITY SEQUENCES

PAVEL HORAK
J. E. Purkyně University, Brno, Czechoslovakia

(Submitted January 1987)

A k^{th}-order linear recurrent sequence $\mathbf{u} = \{u_n : n = 1, 2, \ldots\}$ of integers satisfying the following equation for greatest common divisors,

$$(u_i, u_j) = |u_{(i,j)}| \quad \text{for all } i, j \geqslant 1, \tag{1}$$

is called a k^{th}-order strong divisibility sequence. A complete characterization of all the second-order strong divisibility sequences was given in [1] for integers and then in [3] for an arbitrary algebraic number field. In this note we shall study the third-order strong divisibility sequences.

The system of all the sequences of integers $\mathbf{u} = \{u_n : n = 1, 2, \ldots\}$ defined by

$$u_1 = 1, \quad u_2 = \nu, \quad u_3 = \mu, \tag{2}$$

$$u_{n+3} = a \cdot u_{n+2} + b \cdot u_{n+1} + c \cdot u_n \text{ for } n \geqslant 1 \tag{3}$$

(where ν, μ, a, b, c are integers) will be denoted by U. The system of all the strong divisibility sequences from U [i.e., sequences from U satisfying (1)] will be denoted by D.

The aim of this paper is to find all the strong divisibility sequences in certain subsystems of U and, further, to give some necessary conditions for a sequence from U to be a strong divisibility sequence. Notice that we may take $u_1 = 1$ without loss of generality because all the third-order strong divisibility sequences are obviously all the integral multiples of sequences from D.

1. THE CASES $u_2 = 0$ AND $u_3 = 0$

Let U_1 denote the system of all the sequences from U satisfying $u_2 = 0$ and let U_2 denote all the sequences from U satisfying $u_3 = 0$. Further, let

$$A = \{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4\} \quad \text{and} \quad B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4, \mathbf{b}_5, \mathbf{b}_6\},$$

where

$$\mathbf{a}_1 = \{1, 0, 1, 0, 1, \ldots\} \qquad \mathbf{a}_2 = \{1, 0, 1, 0, -1, 0, 1, 0, -1, \ldots\}$$
$$\mathbf{a}_3 = \{1, 0, -1, 0, -1, \ldots\} \qquad \mathbf{a}_4 = \{1, 0, -1, 0, 1, 0, -1, 0, 1, \ldots\}$$

$$\mathbf{b}_1 = \{1, 1, 0, 1, 1, 0, \ldots\}$$
$$\mathbf{b}_2 = \{1, 1, 0, -1, -1, 0, 1, 1, 0, -1, -1, 0, \ldots\}$$
$$\mathbf{b}_3 = \{1, 1, 0, -1, 1, 0, -1, 1, 0, \ldots\}$$
$$\mathbf{b}_4 = \{1, -1, 0, -1, 1, 0, 1, -1, 0, \ldots\}$$
$$\mathbf{b}_5 = \{1, -1, 0, 1, -1, 0, \ldots\}$$
$$\mathbf{b}_6 = \{1, -1, 0, 1, 1, 0, -1, -1, 0, 1, 1, 0, \ldots\}$$

Directly from the definitions, we get: $A \subseteq D \cap U_1$; $B \subseteq D \cap U_2$. The following propositions show that both the inclusions are, in fact, equalities, i.e., the sequences from A (from B) are precisely all the strong divisibility sequences from U_1 (from U_2).

Proposition 1.1: Let $\mathbf{u} = \{u_n\} \in U_1$. Then $\mathbf{u} \in D$ if and only if $\mathbf{u} \in A$.

Proof: Let $\mathbf{u} \in D$; then, from $(u_2, u_{2k}) = 0$ and $(u_2, u_{2k+1}) = 1$, we get $u_{2k} = 0$ and $u_{2k+1} = \pm 1$ for every $k \geqslant 1$. Now, from $u_3 = \pm 1$, $u_4 = 0$, $u_5 = \pm 1$, we obtain four cases:

(i) $u_3 = u_5 = 1 \Rightarrow \mathbf{u} = \mathbf{a}_1$;

(ii) $u_3 = 1,\ u_5 = -1 \Rightarrow \mathbf{u} = \mathbf{a}_2$;

(iii) $u_3 = -1,\ u_5 = 1 \Rightarrow \mathbf{u} = \mathbf{a}_4$;

(iv) $u_3 = u_5 = -1 \Rightarrow \mathbf{u} = \mathbf{a}_3$;

hence, we get $\mathbf{u} \in A$. The converse is obvious.

Proposition 1.2: Let $\mathbf{u} = \{u_n\} \in U_2$. Then $\mathbf{u} \in D$ if and only if $\mathbf{u} \in B$.

Proof: Let $\mathbf{u} \in D$; then, from

$$|u_n| = (u_3, u_n) = \begin{cases} |u_3| & \text{for } 3|n \\ |u_1| & \text{for } 3\nmid n \end{cases}, \text{ we get } u_n = \begin{cases} 0 & \text{for } 3|n \\ \pm 1 & \text{for } 3\nmid n \end{cases}.$$

Thus, $u_2 = \pm 1$, $u_4 = \pm 1$, $u_5 = \pm 1$, $u_6 = 0$, and we obtain eight cases:

(i) $u_2 = u_4 = u_5 = 1 \Rightarrow \mathbf{u} = \mathbf{b}_1$;

(ii) $u_2 = u_4 = 1,\ u_5 = -1 \Rightarrow u_6 = 2$, a contradiction;

(iii) $u_2 = 1,\ u_4 = -1,\ u_5 = 1 \Rightarrow \mathbf{u} = \mathbf{b}_3$;

(iv) $u_2 = 1,\ u_4 = u_5 = -1 \Rightarrow \mathbf{u} = \mathbf{b}_2$;

(v) $u_2 = -1,\ u_4 = u_5 = 1 \Rightarrow \mathbf{u} = \mathbf{b}_6$;

(vi) $u_2 = -1,\ u_4 = 1,\ u_5 = -1 \Rightarrow \mathbf{u} = \mathbf{b}_5$;

(vii) $u_2 = u_4 = -1,\ u_5 = 1 \Rightarrow \mathbf{u} = \mathbf{b}_4$;

(viii) $u_2 = u_4 = u_5 = -1 \Rightarrow u_6 = -2$, a contradiction;

hence, we get $\mathbf{u} \in B$. Again, the converse is obvious.

2. THE CASE $u_2 \neq 0$, $u_3 \neq 0$

Let U_3 denote the system of all the sequences from U satisfying $u_2 \neq 0$ and $u_3 \neq 0$. Obviously: $U = U_1 \cup U_2 \cup U_3$ and $U_1 \cap U_3 = U_2 \cap U_3 = \emptyset$. Moreover, it is obvious that, for all the sequences from U, it holds that

$$(u_1,\, u_n) = |u_{(1,\,n)}| \quad \text{for all } n \geqslant 1.$$

Proposition 2.1: Let $\mathbf{u} = \{u_n\} \in U_3$. Then $(u_i,\, u_j) = |u_{(i,\,j)}|$ for $1 \leqslant i,\, j \leqslant 4$ if and only if the following conditions hold:

$$(\nu,\, \mu) = 1; \tag{4}$$

$$c = f \cdot \nu - a \cdot \mu, \text{ where } f \text{ is a fixed integer;} \tag{5}$$

$$(\mu,\, b + f) = 1. \tag{6}$$

Proof: Obviously $(u_2,\, u_3) = |u_1| \Leftrightarrow (\nu,\, \mu) = 1$ and $(u_2,\, u_4) = |u_2| \Leftrightarrow$ there exists an integer f such that $f\nu = a\mu + c$. Finally, let (4) and (5) hold; then,

$$(u_3,\, u_4) = |u_1| \Leftrightarrow (\mu,\, b\nu + f\nu) = 1 \Leftrightarrow (\mu,\, b + f) = 1.$$

Proposition 2.2: Let $\mathbf{u} = \{u_n\} \in U_3$. Then $(u_i,\, u_j) = |u_{(i,\,j)}|$ for $1 \leqslant i,\, j \leqslant 5$ if and only if (4), (5), (6), and the following conditions hold:

$$(\nu,\, b) = 1; \tag{7}$$

$$(\mu,\, \nu f + a \cdot (b + f)) = 1; \tag{8}$$

$$(b + f,\, \nu \cdot (\nu f - \mu a) + \mu b) = 1. \tag{9}$$

Proof: Let (4) and (5) hold; then,

$$u_4 = \nu \cdot (b + f),\; u_5 = a\nu(b + f) + b\mu + (f\nu - a\mu)\nu.$$

Thus, $u_5 \equiv b\mu \pmod{|\nu|}$ and we get $(u_2,\, u_5) = |u_1| \Leftrightarrow (\nu,\, b) = 1$. Furthermore, $u_5 \equiv \nu \cdot (ab + af + f\nu) \pmod{|\mu|}$ and, therefore,

$$(u_3,\, u_5) = |u_1| \Leftrightarrow (\mu,\, ab + af + f\nu) = 1.$$

Finally, let (4), (5), and (7) hold; then,

$$\begin{aligned}(u_4,\, u_5) = |u_1| &\Leftrightarrow (\nu(b + f),\, \nu(\nu f - a\mu) + \mu b) = 1\\ &\Leftrightarrow (b + f,\, \nu(\nu f - a\mu) + \mu b) = 1,\end{aligned}$$

which completes the proof.

Proposition 2.3: Let $\mathbf{u} = \{u_n\} \in U_3$. Then $(u_i,\, u_j) = |u_{(i,\,j)}|$ for $1 \leqslant i,\, j \leqslant 6$ if and only if (4)-(9) and the following conditions hold:

$$\nu | a(b - \mu); \tag{10}$$

$$\mu \mid (\nu af + (a^2 + b)(b + f)); \tag{11}$$

$$\left(b + f,\ \nu af + \mu\left(f - a^2 + \frac{a(b - \mu)}{\nu}\right)\right) = 1; \tag{12}$$

$$(\nu(a(b + f - \mu) + f\nu) + \mu b,\ \nu((b + f)(a^2 + b) + + a(f\nu - a\mu) + f\mu) + \mu a(b - \mu)) = 1. \tag{13}$$

Proof: Let (5) hold, then $u_4 = \nu \cdot (b + f)$; $u_5 = \nu \cdot (a(b + f - \mu) + f\nu) + \mu b$; $u_6 = \nu((b + f)(a^2 + b) + a(f\nu - a\mu) + f\mu) + \mu a(b - \mu)$; and obviously $(u_5, u_6) = |u_1| \Longleftrightarrow (13)$. Further, let (4) and (5) hold; then,

$$(u_2, u_6) = |u_2| \Longleftrightarrow (10) \quad \text{and} \quad (u_3, u_6) = |u_3| \Longleftrightarrow (11).$$

Finally, let (5) and (10) hold; then

$$(u_4, u_6) = |u_2| \Longleftrightarrow (12),$$

which completes the proof.

Lemma 2.4: Let $\mathbf{u} = \{u_n\} \in U_3$, $\mathbf{u}$ satisfying (5) and (10). Then

$$u_{2k} \equiv 0 \pmod{|\nu|}; \quad u_{2k+1} \equiv b^{k-1} \cdot \mu \pmod{|\nu|} \quad \text{for all } k \geqslant 1. \tag{14}$$

Proof: From (5) and (10), we get: $c \equiv -ab \pmod{|\nu|}$ and, hence,

$$u_{n+3} \equiv a \cdot u_{n+2} + b \cdot u_{n+1} - ab \cdot u_n \pmod{|\nu|}.$$

Now, using mathematical induction with respect to k, we get (14).

Theorem 2.5: Let $\mathbf{u} = \{u_n\} \in U_3$, $\mathbf{u}$ satisfying (4), (5), (7), and (10). Then

$$(u_2, u_j) = |u_{(2,j)}| \quad \text{for all } j \geqslant 1.$$

Proof: Let $j \geqslant 1$ be even; then, from Lemma 2.4, we get

$$(u_2, u_j) = |\nu| = |u_{(2,j)}|.$$

Now, let $j \geqslant 1$ be odd; then, from (4) and (7), it follows that $(\nu, b^{k-1} \cdot \mu) = 1$ for all $k \geqslant 1$ and, hence, from Lemma 2.4, we get

$$(u_2, u_j) = 1 = |u_{(2,j)}|.$$

3. A SPECIAL CASE OF $u_2 \neq 0$, $u_3 \neq 0$

Let $\overline{U}_3$ denote the system of all the sequence from U_3 satisfying the conditions,

$$(u_i, u_j) = |u_{(i,j)}| \quad \text{for } 1 \leqslant i,\ j \leqslant 6, \tag{15}$$

$$b + f = 0, \tag{16}$$

where f is the integer from (5). Further, let

$$\mathbf{c} = \{1, 2, 1, 0, 1, 2, 1, 0, \ldots\}, \quad \mathbf{d} = \{1, -2, 1, 0, 1, -2, 1, 0, \ldots\}.$$

The following theorem will give a complete characterization of all the strong divisibility sequences in $\overline{U}_3$, showing that **c** and **d** are the only strong divisibility sequences in $\overline{U}_3$, i.e., $\overline{U}_3 \cap D = \{\mathbf{c}, \mathbf{d}\}$.

Theorem 3.1: Let $\mathbf{u} = \{u_n\} \in \overline{U}_3$. Then $\mathbf{u} \in D$ if and only if $\mathbf{u} = \mathbf{c}$ or $\mathbf{u} = \mathbf{d}$.

Proof: Obviously, $\mathbf{c}, \mathbf{d} \in \overline{U}_3 \cap D$. Conversely, let $\mathbf{u} \in \overline{U}_3$ be a strong divisibility sequence. Let us denote $x = \nu \cdot (\nu f - \mu a) + \mu b$, $y = \nu^2 af + \nu\mu(f - a^2) + \mu a(b - \mu)$. Then, from (16), (6), (9), and (12), we get $\mu = \pm 1$, $x = \pm 1$, $y = \pm\nu$, so that we have eight possibilities:

(i) $\mu = 1$, $x = 1$, $y = \nu$

From $\mu = 1$ and $x = 1$, we get $b - 1 = \nu a - \nu^2 f$. Then, from $y = \nu$, we get $\nu f = \nu$ so that $f = 1$ and, consequently, $b = -1$, $a\nu = \nu^2 - 2$, and $c = \nu - a$, using (5). Then $\mathbf{u} = \{1, \nu, 1, 0, 1, \nu, \nu^2 - 3, \ldots\}$. But from $(u_4, u_7) = |u_1|$, we get $\nu = \pm 2$ and, hence, $\mathbf{u} = \mathbf{c}$ or $\mathbf{u} = \mathbf{d}$.

(ii) $\mu = 1$, $x = 1$, $y = -\nu$

Similarly, as in (i), we get $f = -1$, $b = 1$, $a = -\nu$, and $c = 0$. Then we obtain $\mathbf{u} = \{1, \nu, 1, 0, 1, -\nu, \nu^2 + 1, \ldots\}$, a contradiction, since $(u_4, u_7) = \nu^2 + 1 \neq |u_1|$.

(iii) $\mu = 1$, $x = -1$, $y = \nu$

Using $\mu = 1$, $f = -b$ in $x = -1$, we get $\nu a = -\nu^2 b + b + 1$ and then, from $y\nu = \nu^2$, we get $b \cdot (\nu^2 - 2) = \nu^2 + 2$. Let $|\nu| \geqslant 2$, then $\nu^2 \equiv -2 \pmod{(\nu^2 - 2)}$. Trivially, $\nu^2 \equiv 2 \pmod{(\nu^2 - 2)}$, so that $(\nu^2 - 2) | 4$ and, consequently, $\nu = \pm 2$. But $\nu = \pm 2$ implies $b = 3$, $a = \mp 4$, and $c = \mp 2$, a contradiction, since $(u_4, u_7) = 11 \neq |u_1|$. The remaining cases $\nu = \pm 1$ lead to $b = -3$, $a = \pm 1$, and $c = \pm 2$, a contradiction, since $(u_4, u_7) = 4 \neq |u_1|$.

(iv) $\mu = 1$, $x = -1$, $y = -\nu$

Similarly, as in (iii), we get $\nu a = -\nu^2 b + b + 1$ and $b \cdot (\nu^2 - 2) = -\nu^2 + 2$ so that $b = -1$, $a = \nu$, and $c = 0$. Then $\mathbf{u} = \{1, \nu, 1, 0, -1, -\nu, -\nu^2 + 1, \ldots\}$, a contradiction, since $(u_4, u_7) \neq |u_1|$.

(v) $\mu = -1$, $x = 1$, $y = \nu$

Similarly, as in (i), we get $f = -1$, $b = 1$, $c = a - \nu$, and $a\nu = \nu^2 + 2$, which gives $\mathbf{u} = \{1, \nu, -1, 0, 1, \nu, \nu^2 + 3, \ldots\}$, a contradiction, since $(u_4, u_7) = \nu^2 + 3 \neq |u_1|$.

(vi) $\mu = -1$, $x = 1$, $y = -\nu$

In the same way as in (i), we get $f = 1$, $b = -1$, $a = -\nu$, and $c = 0$ so that $\mathbf{u} = \{1, \nu, -1, 0, 1, -\nu, \nu^2 - 1, \ldots\}$, a contradiction, since $(u_4, u_7) = \nu^2 - 1 \neq |u_1|$.

(vii) $\mu = -1$, $x = -1$, $y = \nu$

Similarly, as in (iii), we get $b \cdot (\nu^2 + 2) = -\nu^2 + 2$ and, hence, $\nu^2 \equiv 2 \pmod{\nu^2 + 2}$. Trivially, $\nu^2 \equiv -2 \pmod{\nu^2 + 2}$, so that we get $(\nu^2 + 2)|4$ and, consequently, $\nu^2 = -1, 0, 2$, a contradiction.

(viii) $\mu = -1$, $x = -1$, $y = -\nu$

Similarly, as in (iii), we get $\nu a = \nu^2 b + b - 1$ and $b(\nu^2 + 2) = \nu^2 + 2$, so that $b = 1$, $a = \nu$, $c = 0$. Hence, $\mathbf{u} = \{1, \nu, -1, 0, -1, -\nu, -\nu^2 - 1, \ldots\}$, a contradiction, since $(u_4, u_7) = \nu^2 + 1 \neq |u_1|$.

Remark: We did not use conditions (8), (11), and (13) in the proof of Theorem 3.1, so that we can, in fact, weaken the assumptions (15) by omitting

$$(u_3, u_5) = |u_1|, \quad (u_3, u_6) = |u_3|, \quad \text{and} \quad (u_5, u_6) = |u_1|.$$

REFERENCES

1. P. Horak & L. Skula. "A Characterization of the Second-Order Strong Divisibility Sequences." *The Fibonacci Quarterly* 23, no. 2 (1985):126-132.
2. C. Kimberling. "Strong Divisibility Sequences and Some Conjectures." *The Fibonacci Quarterly* 17 , no. 1 (1979):13-17.
3. A. Schinzel. "Second-Order Strong Divisibility Sequences in an Algebraic Number Field." *Archivum Mathematicum* (Brno) 23 (1987):181-186.

◆◇◆◇◆

ELEMENTARY PROBLEMS AND SOLUTIONS

Edited by
A. P. HILLMAN

Please send all communications regarding ELEMENTARY PROBLEMS AND SOLUTIONS to Dr. A. P. HILLMAN; 709 SOLANO DR., S.E.; ALBUQUERQUE, NM 87108. Each solution or problem should be on a separate sheet (or sheets). Preference will be given to those typed with double spacing in the format used below. Solutions should be received within four months of the publication date.

DEFINITIONS

The Fibonacci numbers F_n and the Lucas numbers L_n satisfy

$$F_{n+2} = F_{n+1} + F_n,\ F_0 = 0,\ F_1 = 1$$

and

$$L_{n+2} = L_{n+1} + L_n,\ L_0 = 2,\ L_1 = 1.$$

PROBLEMS PROPOSED IN THIS ISSUE

B-628 *Proposed by David Singmaster, Polytechnic of the South Bank, London, England*

What is the present average age of Fibonacci's rabbits? (Recall that he introduced a pair of mature rabbits at the beginning of his year and that rabbits mature in their second month. Further, no rabbits died. Let us say that he did this at the beginning of 1202 and that he introduced a pair of one-month-old rabbits. At the end of the first month, this pair would have matured and produced a new pair, giving us a pair of 2-month-old rabbits and a pair of 0-month-old rabbits. At the end of the second month we have a pair of 3-month-old rabbits and pairs of 1-month-old and of 0-month-old rabbits.) Before solving the problem, make a guess at the answer.

B-629 *Proposed by Mohammad K, Azarian, Univ. of Evansville, Evansville, IN*

For which integers a, b, and c is it possible to find integers x and y satisfying

$$(x + y)^2 - cx^2 + 2(b - a + ac)x - 2(a - b)y + (a - b)^2 - ca^2 = 0?$$

B-630 *Proposed by Herta T. Freitag, Roanoke, VA*

Let a and b be constants and define sequences $\{A_n\}_{n=1}^{\infty}$ and $\{B_n\}_{n=1}^{\infty}$ by $A_1 = a$, $A_2 = b$, $B_1 = 2b - a$, $B_2 = 2a + b$, and $A_n = A_{n-1} + A_{n-2}$ and $B_n = B_{n-1} + B_{n-2}$ for $n \geqq 3$.

(i) Determine a and b so that $(A_n + B_n)/2 = [(1 + \sqrt{5})/2]^n$.

(ii) For these a and b, obtain $(B_n + A_n)/(B_n - A_n)$.

<u>B-631</u> *Proposed by L. Kuipers, Sierre, Switzerland*

For N in $\{1, 2, \ldots\}$ and $N \geqq m + 1$, obtain, in closed form,

$$u_N = \sum_{k=m+1}^{m+N} k(k-1) \cdots (k-m)\binom{n+k}{k}.$$

<u>B-632</u> *Proposed by H.-J. Seiffert, Berlin, Germany*

Find the determinant of the n by n matrix (x_{ij}) with $x_{ij} = (1 + \sqrt{5})/2$ for $j > i$, $x_{ij} = (1 - \sqrt{5})/2$ for $j < i$, and $x_{ij} = 1$ for $j = i$.

<u>B-633</u> *Proposed by Piero Filipponi, Fond. U. Bordoni, Rome, Italy*

Let $n \geqq 2$ be an integer and define

$$A_n = \sum_{k=0}^{\infty} \frac{F_k}{n^k}, \quad B_n = \sum_{k=0}^{\infty} \frac{L_k}{n^k}.$$

Prove that $B_n/A_n = 2n - 1$.

SOLUTIONS

Recurrence Relation for Squares

<u>B-604</u> *Proposed by Heinz-Jürgen Seiffert, Berlin, Germany*

Let c be a fixed number and $u_{n+2} = cu_{n+1} + u_n$ for n in $N = \{0, 1, 2, \ldots\}$. Show that there exists a number h such that

$$u_{n+4}^2 = hu_{n+3}^2 - hu_{n+1}^2 + u_n^2 \text{ for } n \text{ in } N.$$

Solution by Demetris Antzoulakos, Univ. of Patras, Patras, Greece

We shall show that $h = c^2 + 2$.

Using successively the above recurrence relation, we get:

$$\begin{aligned} u_{n+4}^2 &= c^2u_{n+3}^2 + u_{n+2}^2 + 2cu_{n+3}u_{n+2} = c^2u_{n+3}^2 + u_{n+2}^2 + 2u_{n+3}^2 - 2u_{n+3}u_{n+1} \\ &= (c^2 + 2)u_{n+3}^2 + u_{n+2}^2 - 2cu_{n+1}u_{n+2} - 2u_{n+1}^2 \\ &= (c^2 + 2)u_{n+3}^2 + c^2u_{n+1}^2 + u_n^2 + 2cu_{n+1}u_n - 2c^2u_{n+1}^2 - 2cu_{n+1}u_n - 2u_{n+1}^2 \\ &= (c^2 + 2)u_{n+3}^2 - (c^2 + 2)u_{n+1}^2 + u_n^2. \end{aligned}$$

<u>Note</u>: The above recurrence includes the exponent 2 dropped by the E.P.S. editor.

Also solved by Paul S. Bruckman, Piero Filipponi, Herta T. Freitag, C. Georghiou, L. Kuipers, Sahib Singh, and the proposer.

Never Prime

B-605 *Proposed by Herta T. Freitag, Roanoke, VA*

Let

$$S(n) = \sum_{i=1}^{n} L_{2n+2i-1}.$$

Determine the positive integers n, if any, for which $S(n)$ is prime.

Solution by Paul S. Bruckman, Fair Oaks, CA

First, we obtain a closed form for $S(n)$. Since

$$S(n) = \sum_{i=1}^{n} (L_{2n+2i} - L_{2n+2i-2}),$$

thus,

$$S(n) = L_{4n} - L_{2n}. \tag{1}$$

Also, $L_{4n} = L_{2n}^2 - 2$. Hence,

$$S(n) = L_{2n}^2 - L_{2n} - 2. \tag{2}$$

In turn, this implies

$$S(n) = (L_{2n} - 2)(L_{2n} + 1).$$

Note that $S(1) = (3 - 2)(3 + 1) = 4$, which is not prime; also, each factor of $S(n)$ is greater than 1 if $n > 1$. Therefore, $S(n)$ is composite for all n.

Also solved by Frank Cunliffe, Piero Filipponi, C. Georghiou, Hans Kappus, L. Kuipers, Bob Prielipp, H.-J. Seiffert, Sahib Singh, and the proposer.

Very Much Simplified

B-606 *Proposed by L. Kuipers, Sierre, Switzerland*

Simplify the expression

$$L_{n+1}^2 + 2L_{n-1}L_{n+1} - 25F_n^2 + L_{n-1}^2.$$

Solution by Gregory Wulczyn, Lewisburg, PA

$$\begin{aligned} L_{n+1}^2 + 2L_{n-1}L_{n+1} + L_{n-1}^2 - 25F_n^2 &= (L_{n+1} + L_{n-1})^2 - 25F_n^2 \\ &= (5F_1F_n)^2 - 25F_n^2 = 0. \end{aligned}$$

Also solved by Demetris Antzoulakos, Paul S. Bruckman, Frank Cunliffe, Piero Filipponi, Herta T. Freitag, C. Georghiou, Hans Kappus, Joseph J. Kostal, Bob Prielipp, H.-J. Seiffert, Sahib Singh, and the proposer.

Product of Exponential Generating Functions

B-607 *Proposed by Charles R. Wall, Trident Technical College, Charleston, SC*

Let

$$C_n = \sum_{k=0}^{n} \binom{n}{k} F_k L_{n-k}.$$

Show that $C_n/2^n$ is an integer for n in $\{0, 1, 2, \ldots\}$.

Solution by Bob Prielipp, Univ. of Wisconsin-Oshkosh, WI

Since $F_k = (\alpha^k - \beta^k)/\sqrt{5}$ and $L_{n-k} = \alpha^{n-k} + \beta^{n-k}$ where $\alpha = (1 + \sqrt{5})/2)$ and $\beta = (1 - \sqrt{5})/2$, $F_k L_{n-k} = (\alpha^n - \beta^n)/\sqrt{5} - (\alpha^{n-k}\beta^k)/\sqrt{5} + (\beta^{n-k}\alpha^k)/\sqrt{5}$. Hence,

$$C_n = \sum_{k=0}^{n} \binom{n}{k} F_n - \frac{1}{\sqrt{5}} \sum_{k=0}^{n} \binom{n}{k} \alpha^{n-k}\beta^k + \frac{1}{\sqrt{5}} \sum_{k=0}^{n} \binom{n}{k} \beta^{n-k}\alpha^k$$

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

[using the fact that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ and the Binomial Theorem]

$$= 2^n F_n.$$

The required result follows.

Also solved by Demetris Antzoulakos, Paul S. Bruckman, Frank Cunliffe, Russell Euler, Piero Filipponi, Herta T. Freitag, C. Georghiou, Hans Kappus, Joseph J. Kostal, L. Kuipers, H.-J. Seiffert, Sahib Singh, Gregory Wulczyn, and the proposer.

Integral Average of Squares

B-608 *Proposed by Piero Filipponi, Fond. U. Bordoni, Rome, Italy*

For $k = \{2, 3, \ldots\}$ and n in $N = \{0, 1, 2, \ldots\}$, let

$$S_{n,k} = \frac{1}{k} \sum_{j=n}^{n+k-1} F_j^2$$

denote the quadratic mean taken over k consecutive Fibonacci numbers of which the first is F_n. Find the smallest such $k \geqq 2$ for which $S_{n,k}$ is an integer for all n in N.

Solution by Philip L. Mana, Albuquerque, NM

Since $S_{1,k} - S_{0,k} = F_k^2/k$, a necessary condition on k is that $k | F_k^2$. The two smallest such k in $\{2, 3, \ldots\}$ are 5 and 12. $S_{0,5}$ and $S_{1,5}$ are integers but $S_{2,5}$ is not since $F_6^2 \not\equiv F_1^2 \pmod 5$. Thus, 5 is not a solution.

It is known that

$$\sum_{j=0}^{m-1} F_j^2 = F_m F_{m-1}.$$

Hence,

$$S_{nk} = (F_{n+k}F_{n+k-1} - F_k F_{k-1})/k.$$

Since $F_{12} = 144 \equiv 0 \pmod{12}$ and $F_{13} = 233 \equiv 5 \pmod{12}$, it follows by induction that $F_{n+12} \equiv 5F_n \pmod{12}$. This implies that $F_{n+12}F_{n+11} \equiv 25F_n F_{n-1} \pmod{12}$ and hence $S_{n,12}$ is an integer for all n in N. Thus, $k = 12$ is a solution.

Note: P. S. Bruckman points out that $S_{n,k}$ is a "mean of squares" rather than a "quadratic mean."

Also solved by Paul S. Bruckman, Frank Cunliffe, Herta T. Freitag, C. Georghiou, L. Kuipers, Chris Long, Bob Prielipp, H.-J. Seiffert, Sahib Singh, Lawrence Somer, David Zeitlin, and the proposer.

Sum of Squares

B-609 *Proposed by Adina DiPorto & Piero Filipponi, Fond. U. Bordoni, Rome, Italy*

Find a closed form expression for

$$S = \sum_{k=1}^{n} (kF_k)^2$$

and show that $S_n \equiv n(-1)^n \pmod{F_n}$.

Solution by C. Georghiou, Univ. of Patras, Patras, Greece

We will show that $S_n \equiv n(-1)^{n+1} \pmod{F_n}$.

Let $f(x) = x + x^2 + \cdots + x^n$ and $g(x) = 1^2x + 2^2x^2 + 3^2x^3 + \cdots + n^2x^n$. We then have $g(x) = x^2f''(x) + xf'(x)$ and, therefore,

$$S_n = (g(\alpha^2) + g(\beta^2) - 2g(-1))/5$$
$$= \frac{1}{5}[(n-1)^2L_{2n+1} + (2n-1)L_{2n-1} - n(n+1)(-1)^n]$$

and by using the identity

$$L_{2n-1} = 5F_nF_{n-1} - (-1)^n,$$

we get

$$S_n = (n-1)^2F_n^2 + (n^2+2)F_nF_{n-1} - n(-1)^n,$$

from which the assertion follows.

Note: The solver corrected back to the proposer's $S_n \equiv n(-1)^{n+1}$.

Also solved by Paul S. Bruckman, Herta T. Freitag, Hans Kappus, L. Kuipers, Bob Prielipp, H.-J. Seiffert, Sahib Singh, and the proposer.

◆◇◆◇◆

ADVANCED PROBLEMS AND SOLUTIONS

Edited by
RAYMOND E. WHITNEY

Please send all communications concerning ADVANCED PROBLEMS AND SOLUTIONS to RAYMOND E. WHITNEY, MATHEMATICS DEPARTMENT, LOCK HAVEN UNIVERSITY, LOCK HAVEN, PA 17745. This department especially welcomes problems believed to be new or extending old results. Proposers should submit solutions or other information that will assist the editor. To facilitate their consideration, all solutions should be submitted on separate signed sheets within two months after publication of the problems.

PROBLEMS PROPOSED IN THIS ISSUE

H-425 *Proposed by Stanley Rabinowitz, Littleton, MA*

Let $F_n(x)$ be the n^{th} Fibonacci polynomial

$$F_1(x) = 1,\ F_2(x) = x,\ F_{n+2}(x) = xF_{n+1}(x) + F_n(x).$$

Evaluate:

(a) $\displaystyle\int_0^1 F_n(x)dx$; (b) $\displaystyle\int_0^1 F_n^2(x)dx$.

H-426 *Proposed by Larry Taylor, Rego Park, NY*

Let j, k, m, and n be integers. Prove that

$$(F_nF_{m+k-j} - F_mF_{n+k-j})(-1)^m = (F_kF_{j+n-m} - F_jF_{k+n-m})(-1)^j.$$

H-427 *Proposed by Piero Filipponi, Rome, Italy*

Let $C(n,\ k) = C_1(n,\ k)$ denote the binomial coefficient $\binom{n}{k}$.

Let $C_2(n,\ k) = C[C(n,\ k),\ k]$ and, in general,

$$C_i(n,\ k) = C(C\{\ldots[C(n,\ k),\ k]\}).$$

For given n and i, is it possible to determine the value k_0 of k for which

$$C_i(n,\ k_0) > C_i(n,\ k) \quad (k = 0,\ 1,\ \ldots,\ n;\ k \neq k_0)?$$

SOLUTIONS

Some Triple Sum

H-404 *Proposed by Andreas N. Philippou and Frosso S. Makri, Patras, Greece (Vol. 24, no. 4, November 1986)*

Show that

$$\text{(a)} \sum_{r=0}^{n}\sum_{i=0}^{1}\sum_{\substack{n_1,\ {}_2\ \ni \\ n_1+2n_2=n-i \\ n_1+n_2=n-r}}\binom{n_1+n_2}{n_1,\ n_2} = F_{n+2},\ n \geq 0;$$

$$\text{(b)} \sum_{r=0}^{n}\sum_{i=0}^{k-1} \sum_{\substack{n_1,\ldots,n_k \ni \\ n_1+2n_2+\cdots+kn_k=n-i \\ n_1+\cdots+n_k=n-r}} \binom{n_1+\cdots+n_k}{n_1,\ldots,n_k} = F_{n+2}^{(k)},\ n \geq 0,\ k \geq 2,$$

where $n_1, \ldots, n_k$ are nonnegative integers and $\{F_n^{(k)}\}$ is the sequence of Fibonacci-type polynomials of order k [1].

[1] A. N. Philippou, C. Georghiou, & G. N. Philippou, "Fibonacci-Type Polynomials of Order K with Probability Applications," *The Fibonacci Quarterly* *23*, no. 2 (1985):100-105.

Solution by Tad P. White, Student, UCLA, Los Angeles, CA

(a) Although this is a special case of (b), it can be solved in a slightly simpler manner since the simultaneous equations

$$n_1 + 2n_2 = n - i$$
$$n_1 + n_2 = n - r$$

can be explicitly solved to obtain $n_1 = n + i - 2r$ and $n_2 = r - i$; thus the sum becomes

$$\sum_{r=0}^{n}\sum_{i=0}^{1}\binom{n-r}{r-i} = \sum_{r=0}^{n}\binom{n+1-r}{r},$$

and it is well known that the right-hand side sums to F_{n+2} for $n \geq 0$. However, the details can be omitted since this case is treated in part (b).

(b) Fix $k \geq 2$; we prove this equality in two steps. Let $f(n)$ denote the left-hand side of the equation in question, for our fixed k. First, we show that both sides of the equation are equal for $0 \leq n < k$, and then we show that both sides obey the same kth-order recursion relation, namely

$$f(n) = \sum_{1 \leq l \leq k} f(n-l);$$

we are off to a good start because we know already that $F_n^{(k)}$, and hence $F_{n+2}^{(k)}$, obey this relation.

Assuming first that $0 \leq n \leq k-1$, the upper limit of the summation over i can be replaced with n, since if $i > n$, the condition $n_1 + \cdots + kn_k = n - i$ is not satisfied by any k-tuple $(n_1, \ldots, n_k)$. Also, the condition that $n_1 + \cdots + n_k = n - r$ for some r with $0 \leq r \leq n$ is vacuously satisfied by every k-tuple $(n_1, \ldots, n_k)$ satisfying $n_1 + \cdots + kn_k = n - i$ for some $i \leq n$, so we may remove both this condition and the summation over r. Therefore,

$$\begin{aligned} f(n) &= \sum_{i=0}^{n} \sum_{\substack{n_1,\ldots,n_k \ni \\ n_1+2n_2+\cdots+kn_k=n-i}} \binom{n_1+\cdots+n_k}{n_1,\ldots,n_k} \\ &= \sum_{i=0}^{n} \sum_{\substack{n_1,\ldots,n_k \ni \\ n_1+2n_2+\cdots+kn_k=i}} \binom{n_1+\cdots+n_k}{n_1,\ldots,n_k} \\ &= \sum_{i=0}^{n} F_{i+1}^{(k)}. \end{aligned}$$

Since $F_{n+1}^{(k)} = \sum_{i=1}^{n} F_i^{(k)}$ for $n \leq k$, we conclude that $f(n) = F_{n+2}^{(k)}$ for $0 \leq n \leq k-1$.

We now derive a recursion relation for $f(n)$. We make use of the following property of multinomial coefficients:

$$\binom{n_1+\cdots+n_k}{n_1,\ldots,n_k} = \sum_{1 \leq l \leq k}\binom{n_1+\cdots+n_k-1}{n_1,\ldots,n_{l-1},n_l-1,n_{l+1},\ldots,n_k}.$$

We will follow the convention that a multinomial coefficient vanishes when any entry is negative, so that this identity remains valid whenever each n_k is nonnegative. Substituting this in the formula defining $f(n)$, we find

$$f(n) = \sum_{1\le l\le k}\sum_{r=0}^{n}\sum_{i=0}^{k-1}\sum_{\substack{n_1,\ldots,n_k \ni \\ n_1+2n_2+\cdots+kn_k=n-i \\ n_1+\cdots+n_k=n-r}} \binom{n_1+\cdots+n_k-1}{n_1,\ldots,n_{l-1},n_l-1,n_{l+1},\ldots,n_k}$$

Letting m_i denote n_i for $i \neq l$ and $m_l = n_l - 1$, this becomes

$$= \sum_{1\le l\le k}\sum_{r=0}^{n}\sum_{i=0}^{k-1}\sum_{\substack{m_1,\ldots,m_k \ni \\ m_1+2m_2+\cdots+km_k=n-l-i \\ m_1+\cdots+m_k=n-1-r}} \binom{m_1+\cdots+m_k}{m_1,\ldots,m_k}$$

Letting s now denote $r+1-l$,

$$= \sum_{1\le l\le k}\sum_{s=1-l}^{n+1-l}\sum_{i=0}^{k-1}\sum_{\substack{m_1,\ldots,m_k \ni \\ m_1+2m_2+\cdots+km_k=n-l-i \\ m_1+\cdots+m_k=n-l-s}} \binom{m_1+\cdots+m_k}{m_1,\ldots,m_k}$$

The terms with $s < 0$ and $s = n+1-l$ contribute zero to the sum, so we may eliminate them to obtain

$$= \sum_{1\le l\le k}\left[\sum_{s=0}^{n-l}\sum_{i=0}^{k-1}\sum_{\substack{m_1,\ldots,m_k \ni \\ m_1+2m_2+\cdots+km_k=n-l-i \\ m_1+\cdots+m_k=n-l-s}} \binom{m_1+\cdots+m_k}{m_1,\ldots,m_k}\right]$$

$$= \sum_{1\le l\le k} f(n-l).$$

Thus $f(n)$ and $F_{n+2}^{(k)}$ obey the same kth order recursion relation, and agree for $0 \le n \le k-1$. Thus $f(n) = F_{n+2}^{(k)}$ for all $k \ge 2$ and $n \ge 0$.

Also solved by P. Bruckman, C. Georghiou, and the proposers.

General Ize

H-405 *Proposed by Piero Filipponi, Rome, Italy*
(Vol. 24, no. 4, November 1986)

(i) Generalize Problem B-564 by finding a closed form expression for

$$\sum_{n=1}^{N} [\alpha^k F_n], \quad (N = 1, 2, \ldots; k = 1, 2, \ldots)$$

where $\alpha = (1+\sqrt{5})/2$, F_n is the n^{th} Fibonacci number, and $[x]$ denotes the greatest integer not exceeding x.

(ii) Generalize the above sum to negative values of k.

(iii) Can this sum be further generalized to any rational value of the exponent of α?

Remark: As to (iii), it can be proved that

$$[\alpha^{1/k}F_n] = F_n, \text{ if } 1 \leqslant n \leqslant [(\ln\sqrt{5} - \ln(\alpha^{1/k}-1))/\ln\alpha].$$

References

1. V. E. Hoggatt, Jr., & M. Bicknell-Johnson, "Representation of Integers in Terms of Greatest Integer Functions and the Golden Section Ratio," *The Fibonacci Quarterly* 17, no. 4 (1979):306-318.
2. V. E. Hoggatt, Jr., *Fibonacci and Lucas Numbers* (Boston: Houghton Mifflin Company, 1969).

Partial solution by the proposer

First, recall that [1, Lemma 2]

$$[\alpha^k F_n] = \begin{cases} F_{n+k} & (n \text{ odd}) \\ F_{n+k} - 1 & (n \text{ even}). \end{cases} \quad (k \geqq 2;\ n \geqq k) \tag{1}$$

It can be noted that, since the relationship [1, Lemma 1]

$$[\alpha F_n] = \begin{cases} F_{n+1} & (n \text{ odd}) \\ F_{n+1} - 1 & (n \text{ even}) \end{cases} \quad (n \geqq 2) \tag{2}$$

clearly holds also for $n = 1$, (a) holds for $k = 1$ as well.

Then, we find an expression for $[\alpha^k F_n]$ in the case of $1 \leqq n \leqq k - 1$. Using the Binet form, the equality

$$\alpha^k F_n = F_{k+n} - \beta^n F_k \tag{3}$$

can be proved [1, Lemma 3]. Again, using the Binet form, we obtain

$$\beta^n F_k = \frac{\beta^n(\alpha^k - \beta^k)}{\sqrt{5}} = \frac{(-1)^n \alpha^{k-n} - \beta^{k+n}}{\sqrt{5}} + \frac{(-1)^n(\beta^{k-n} - \beta^{k-n})}{\sqrt{5}}$$

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

Since it is readily seen that

$$\begin{cases} 0 < x < 1 & (k \text{ even}) \\ -1 < x < 0 & (k \text{ odd}), \end{cases} \quad (1 \leqq n \leqq k - 1) \tag{4}$$

from (3) and (4), we can write

$$[\alpha^k F_n] = \begin{cases} F_{k+n} - F_{k-n} - 1 & (n \text{ even}, k \text{ even}) \\ F_{k+n} - F_{k-n} & (n \text{ even}, k \text{ odd}) \\ F_{k+n} + F_{k-n} - 1 & (n \text{ odd}, k \text{ even}) \\ F_{k+n} + F_{k-n} & (n \text{ odd}, k \text{ odd}) \end{cases} \quad (1 \leqq n \leqq k - 1)$$

from which, by Hoggatt's I_{24} and I_{22} [2], we get

$$[\alpha^k F_n] = \begin{cases} L_k F_n & (k \text{ odd}) \\ L_k F_n - 1 & (k \text{ even}). \end{cases} \quad (1 \leqq n \leqq k - 1) \tag{5}$$

Now, let us distinguish the following two cases.

Case 1: $k > N$

From (5) and Hoggatt's I_1 [2], we have

$$\sum_{n=1}^{N} [\alpha^k F_n] = \begin{cases} L_k \sum_{n=1}^{N} F_n = L_k(F_{N+2} - 1) & (k \text{ odd}) \\ L_k \sum_{n=1}^{N} F_n - N = L_k(F_{N+2} - 1) - N & (k \text{ even}) \end{cases}$$

which can be rewritten in the following more compact form:

$$\sum_{n=1}^{N} [\alpha^k F_n] = L_k(F_{N+2} - 1) - N \frac{(-1)^k + 1}{2} \quad (\text{if } k > N). \tag{6}$$

Case 2: $1 \leqq k \leqq N$

From (6), we can write

$$\begin{aligned}\sum_{n=1}^{N} [\alpha^k F_n] &= \sum_{n=1}^{k-1} [\alpha^k F_n] + \sum_{n=k}^{N} [\alpha^k F_n] \\ &= L_k(F_{k+1} - 1) - (k - 1)\frac{(-1)^k + 1}{2} + \sum_{n=k}^{N} [\alpha^k F_n].\end{aligned} \tag{7}$$

From (1) we have

$$\sum_{n=k}^{N} [\alpha^k F_n] = \sum_{n=1}^{N-k+1} F_{2k+n-1} - \begin{cases} \left[\dfrac{N - k + 1}{2}\right] & (k \text{ odd}) \\ \left[\dfrac{N - k + 2}{2}\right] & (k \text{ even}), \end{cases}$$

which, by Hoggatt's I_1 [2] can be rewritten as (cf. Prob. B-564, for $k = 1$)

$$\sum_{n=k}^{N} [\alpha^k F_n] = F_{N+k+2} - F_{2k+1} - \left[\frac{2N - 2k + 3 + (-1)^k}{4}\right] \tag{8}$$

Combining (7) and (8), we obtain

$$\begin{aligned}\sum_{n=1}^{N} [\alpha^k F_n] &= L_k(F_{k+1} - 1) + F_{N+k+2} - F_{2k+1} \\ &\quad - (k - 1)\frac{(-1)^k + 1}{2} - \left[\frac{2N - 2k + 3 + (-1)^k}{4}\right],\end{aligned}$$

that is,

$$\begin{aligned}\sum_{n=1}^{N} [\alpha^k F_n] &= L_k(F_{k+1} - 1) + F_{N+k+2} - F_{2k+1} \\ (\text{if } 1 \leqq k \leqq N) &\quad - \frac{2N + (2k - 1)(-1)^k + (-1)^N}{4}.\end{aligned} \tag{9}$$

The problem can be further generalized to negative values of the exponent k. The proof can be obtained by reasoning similar to the preceding and is omitted for the sake of brevity. Se we offer the following

Conjecture: For N and k positive integers,

$$\sum_{n=1}^{N}[\alpha^{-k}F_n] = \begin{cases} F_{N-k+2} - \left[\dfrac{N-k+3}{2}\right], & \text{if } N > k+1 \\ 0, & \text{if } N \leq k+1. \end{cases}$$

Also partially solved by P. Bruckman.

◆◇◆◇◆

BOOK REVIEW

by A.F. Horadam, University of New England, Armidale, Australia 2351

Leonardo Pisano (Fibonacci)—The Book of Squares

(an annotated translation into modern English)—L.E. Sigler, Academic Press 1987.

This is the first complete translation into English of Fibonacci's masterpiece, *Liber quadratorum* ("The Book of Squares"), which was written in 1225. Until the nineteenth century when he acquired the nickname Fibonacci, the author, who was born in Pisa and christened Leonardo, was universally known as Leonardo Pisano. He is better-known for his *Liber abbaci* in which the Fibonacci numbers first appear.

The volume under review consists of three main parts, namely; a short biographical sketch of Fibonacci, an English translation of *Liber quadratorum,* and a commentary on this translation ("The Book of Squares"). The Latin text followed by Sigler is that used by Boncompagni who found the MS in the Ambrosian Library in Milan when preparing the first printed edition of Fibonacci's writings in 1857-62.

Sigler's commentary is particularly useful as it provides in detail an explanation of Fibonacci's text in modern mathematical notation and terminology. Fibonacci had no algebraic symbolism to help him. Following Euclid, he represented numbers geometrically as line-segments. It is truly remarkable how far he could progress with this limited mathematical equipment. His achievements in this book justly confirm him as the greatest exponent of number theory, particularly in indeterminate analysis, in the Middle Ages.

A representative, and famous, problem posed and solved in the text is: Find a square number from which, when 5 is added or subtracted, there always arises a square number.

According to the translator, "a knowledge of secondary school mathematics, algebra and geometry ought to be adequate preparation for the reading and understanding of this book."

We are indebted to Sigler for making this English translation available. For many, it could open up a new world of delight.

VOLUME INDEX

SUSTAINING MEMBERS

*Charter Members

*A.L. Alder	P.A. DeCaux	R.J. Howell	E.D. Robinson
S. Ando	M.J. DeLeon	H. Ibstedt	S.E. Schloth
R. Andre-Jeannin	J. Desmond	R.P. Kelisky	J.A. Schumaker
*J. Arkin	H. Diehl	C.H. Kimberling	A.G. Shannon
M.K. Azarian	T.H. Engel	J. Lahr	D. Singmaster
L. Bankoff	D.R. Farmer	N. Levine	J. Sjoberg
F. Bell	P. Flanagan	C.T. Long	L. Somer
M. Berg	F.F. Frey, Jr.	Br. J.M. Mahon	M.N.S. Swamy
J.G. Bergart	Emerson Frost	*J. Maxwell	*D. Thoro
G. Bergum	Anthony Gioia	F.U. Mendizabal	J.C. Turner
G. Berzsenyi	R.M. Giuli	L. Miller	R. Vogel
*M. Bicknell-Johnson	I.J. Good	M.G. Monzingo	J.N. Vitale
*Br. A. Brousseau	*H.W. Gould	S.D. Moore, Jr.	M. Waddill
P.S. Bruckman	H. Harborth	J.F. Morrison	J.E. Walton
M.F. Bryn	H.E. Heatherly	K. Nagaska	G. Weekly
P.F. Byrd	A.P. Hillman	F.G. Ossiander	R.E. Whitney
G.D. Chakerian	*A.F. Hordam	A. Prince	B.E. Williams
J.W. Creely	F.T. Howard	S. Rabinowitz	A.C. Yanoviak

INSTITUTIONAL MEMBERS

THE BAKER STORE EQUIPMENT COMPANY
Cleveland, Ohio

BOSTON COLLEGE
Chestnut Hill, Massachusetts

BUCKNELL UNIVERSITY
Lewisburg, Pennsylvania

CALIFORNIA STATE UNIVERSITY, SACRAMENTO
Sacramento, California

ETH-BIBLIOTHEK
Zurich, Switzerland

FERNUNIVERSITAET HAGEN
Hagen, West Germany

HOWELL ENGINEERING COMPANY
Bryn Mawr, California

NEW YORK PUBLIC LIBRARY GRAND CENTRAL STATION
New York, New York

NORTHWESTERN UNIVERSITY
Evanston, Illinois

PRINCETON UNIVERSITY
Princeton, New Jersey

SAN JOSE STATE UNIVERSITY
San Jose, California

SANTA CLARA UNIVERSITY
San Jose, California

KLEPKO, INC.
Sparks, Nevada

SYRACUSE UNIVERSITY
Syracuse, New York

TECHNOLOGICAL EDUCATION INSTITUTE
Larissa, Greece

UNIVERSITY OF SALERNO
Salerno, Italy

UNIVERSITY OF CALIFORNIA, SANTA CRUZ
Santa Cruz, California

UNIVERSITY OF GEORGIA
Athens, Georgia

UNIVERSITY OF NEW ENGLAND
Armidale, N.S.W. Australia

WASHINGTON STATE UNIVERSITY
Pullman, Washington

BOOKS AVAILABLE THROUGH THE FIBONACCI ASSOCIATION

Introduction to Fibonacci Discovery by Brother Alfred Brousseau. Fibonacci Association (FA), 1965.

Fibonacci and Lucas Numbers by Verner E. Hoggatt, Jr. FA, 1972.

A Primer for the Fibonacci Numbers. Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1972.

Fibonacci's Problem Book. Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1974.

The Theory of Simply Periodic Numerical Functions by Edouard Lucas. Translated from the French by Sidney Kravitz. Edited by Douglas Lind. FA, 1969.

Linear Recursion and Fibonacci Sequences by Brother Alfred Brousseau. FA, 1971.

Fibonacci and Related Number Theoretic Tables. Edited by Brother Alfred Brousseau. FA, 1972.

Number Theory Tables. Edited by Brother Alfred Brousseau. FA, 1973.

Recurring Sequences by Dov Jarden. Third and enlarged edition. Riveon Lematematika, Israel, 1973.

Tables of Fibonacci Entry Points, Part One. Edited and annotated by Brother Alfred Brousseau. FA, 1965.

Tables of Fibonacci Entry Points, Part Two. Edited and annotated by Brother Alfred Brousseau. FA, 1965.

A Collection of Manuscripts Related to the Fibonacci Sequence—18th Anniversary Volume. Edited by Verner E. Hoggatt, Jr. and Marjorie Bicknell-Johnson. FA, 1980.

Fibonacci Numbers and Their Applications. Edited by A.N. Philippou, G.E. Bergum and A.F. Horadam.

Please write to the Fibonacci Association, Santa Clara University, Santa Clara, CA 95053, U.S.A., for current prices.