The Fibonacci Quarterly

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

TABLE OF CONTENTS

On Glaisher's Infinite Sums Involving the Inverse Tangent Function ... *Allen R. Miller and H.M. Srivastava* 290

Author and Title Index ... 294

Complete Fibonacci Sequences in Finite Fields ... *Owen J. Brison* 295

Fourth International Conference Proceedings ... 304

The Diophantine Equation $x^2 + a^2y^m = z^{2n}$ With $(x, ay) = 1$ ... *Konstantine Dabmian Zelator* 305

On the (2, F) Generalizations of the Fibonacci Sequence ... *W.R. Spickerman, R.N. Joyner, and R.L. Creech* 310

A Short History on Lucas ... 314

Fibonacci Numbers and the Numbers of Perfect Matchings of Square, Pentagonal, and Hexagonal Chains ... *Ratko Tošic and Ivan Stojmenovic* 315

On a Digraph Defined by Squaring Modulo n ... *Earle L. Blanton, Jr., Spencer P. Hurd and Judson S. McCranie* 322

The Fibonacci Conference in Scotland ... *Herta T. Freitag* 334

On the Distribution of Pythagorean Triples ... *Edward K. Hinson* 335

Generating M-Strong Fibonacci Pseudoprimes ... *Adina Di Porto and Piero Filipponi* 339

On Sequences Having Same Minimal Elements in the Lemonie-Kátai Algorithm ... *Jukka Pihko* 344

A Generalization of Kummer's Congruences and Related Results ... *Frank S. Gillespie* 349

Elementary Problems and Solutions ... *Edited by Stanley Rabinowitz* 368

Advanced Problems and Solutions ... *Edited by Raymond E. Whitney* 376

Volume Index ... 383

VOLUME 30 NOVEMBER 1992 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 FIBONACCI QUARTERLY.** They should be typewritten or reproduced typewritten copies, that are clearly readable, double spaced with wide margins and on only one side of the paper. The full name and address of the author must appear at the beginning of the paper directly under the title. Illustrations should be carefully drawn in India ink on separate sheets of bond paper or vellum, approximately twice the size they are to appear in print. Since the Fibonacci Association has adopted $F_1 = F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$, $n \geq 2$ and $L_1 = 1$, $L_2 = 3$, $L_{n+1} = L_n + L_{n-1}$, $n \geq 2$ as the standard definitions for The Fibonacci and Lucas sequences, these definitions *should not* be a part of future papers. However, the notations *must* be used. One to three *complete* A.M.S. classification numbers *must* be given directly after references or on the bottom of the last page. Papers without classification numbers will be returned.

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 57007-1596.**

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 $35 for Regular Membership, $45 for Sustaining Membership, and $70 for Institutional Membership; foreign rates, which are based on international mailing rates, are somewhat higher than domestic rates; please write for details. **THE FIBONACCI QUARTERLY** is published each February, May, August and November.

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

The Fibonacci Quarterly

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

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

ON GLAISHER'S INFINITE SUMS INVOLVING THE INVERSE TANGENT FUNCTION

Allen R. Miller
George Washington University, Washington, DC 20052

H. M. Srivastava
University of Victoria, Victoria, British Columbia V8W 3P4, Canada

(Submitted November 1990)

1. Introduction

In 1878, J. W. L. Glaisher [1] derived a number of results about certain infinite sums involving the inverse tangent function; in particular, he showed for complex θ $(0 < |\theta| < \infty)$, that

$$\sum_{n=1}^{\infty} \arctan \frac{2\theta^2}{n^2} = \frac{\pi}{4} - \arctan\left(\frac{\tanh \pi\theta}{\tan \pi\theta}\right). \tag{1}$$

This equation appears again in 1908 as an exercise in T. J. I'a. Bromwich's book [2, p. 259]. Generalizations of (1) are found in [3], [4, p. 276], and [5, p. 749].

Letting $\theta \to 1-$ in (1), Glaisher also obtained the elegant result:

$$\sum_{n=1}^{\infty} \arctan \frac{2}{n^2} = \frac{3}{4}\pi. \tag{2}$$

A very simple derivation of (2) and a history of this series appeared recently in [6].

It is easy to see that the two members of (1) may differ by an integer multiple of π; this pathology occurs often in many results of this type, since the inverse tangent function is a multiple-valued function. Hence, if we use only the principal value of the inverse tangent function, we must write (1) in the form

$$\sum_{n=1}^{\infty} \arctan \frac{2\theta^2}{n^2} = \left(\frac{1}{4} + m\right)\pi - \arctan\left(\frac{\tanh \pi\theta}{\tan \pi\theta}\right) \tag{3}$$

for some $m \in \mathbb{Z} \equiv \{0, \pm 1, \pm 2, \ldots\}$.

In this paper we shall derive computationally more useful results than (3); our results will yield some interesting corollaries not available heretofore. Indeed we shall show, for complex θ $(0 < |\theta| < \infty)$, that

$$\sum_{n=1}^{\infty} \arctan \frac{2\theta^2}{n^2} = \left(\theta - \frac{1}{4}\right)\pi - \arctan\left(\frac{\sin 2\pi\theta}{\cos 2\pi\theta - \exp 2\pi\theta}\right) \tag{4}$$

where, here and in what follows, the principal value of the inverse tangent function is assumed. We shall also show that (3) and (4) are, in fact, equivalent. We shall then give (in Section 5) some generalizations of (4). Finally, in Section 6, we deduce some interesting particular cases of one of the general summation formulas which we obtain in Section 5.

2. Derivation of the Summation Formula (4)

To derive (4), we shall use the Euler-Maclaurin summation formula ([7, p. 27]; see also [8, p. 521])

$$\sum_{k=0}^{n} f(k) = \int_0^n f(x)dx + \frac{1}{2}f(0) + \frac{1}{2}f(n) + \int_0^n P(x)f'(x)dx$$

where $P(x)$, for real x, is a saw-tooth function: $P(x) = x - [x] - 1/2$. Letting $f(x) = \arctan(2\theta^2/x^2)$ and $n \to \infty$, we obtain

$$\sum_{k=0}^{\infty} \arctan \frac{2\theta^2}{k^2} = \int_0^{\infty} \arctan \frac{2\theta^2}{x^2}dx + \frac{\pi}{4} - 4\theta^2\int_0^{\infty} P(x)\frac{xdx}{4\theta^4 + x^4}.$$

Assuming $0 < \theta < \infty$ and making simple transformations in the integrals, we have

$$(5) \qquad \sum_{k=1}^{\infty} \arctan \frac{2\theta^2}{k^2} = -\frac{\pi}{4} + \theta\int_0^{\infty} \arctan \frac{2}{x^2}dx - 2\int_0^{\infty} P(\theta\sqrt{2}x)\frac{xdx}{1 + x^4}.$$

The first integral on the right side of (5) can be evaluated in a number of ways or by using tables of integrals (cf. [5] and [9]). We omit the details and give the result:

$$(6) \qquad \int_0^{\infty} \arctan(2/x^2)dx = \pi.$$

The saw-tooth function $P(x)$ is a sectionally (piecewise) smooth periodic function with unit period. It can be represented by a Fourier series which is given by

$$(7) \qquad P(x) = -\frac{1}{\pi}\sum_{k=1}^{\infty} \frac{1}{k} \sin(2\pi kx).$$

The series given in (7) converges uniformly in every closed interval where $P(x)$ is continuous. The saw-tooth function and its Fourier series representation are discussed in detail, for example, in [10, pp. 107-24].

To evaluate the second integral in (5), we use (7) and interchange the sum and integral, thus giving:

$$(8) \qquad \int_0^{\infty} P(\theta\sqrt{2}x)\frac{xdx}{1 + x^4} = -\frac{1}{\pi}\sum_{k=1}^{\infty} \frac{1}{k}\int_0^{\infty} \sin(2\sqrt{2}\theta\pi kx)\frac{xdx}{1 + x^4}.$$

Using [9, p. 408, Sec. 3.727, Eq. (4)], we find that

$$(9) \qquad \int_0^{\infty} \sin(2\sqrt{2}\theta\pi kx)\frac{xdx}{1 + x^4} = \frac{\pi}{2} \exp(-2\theta\pi k)\sin(2\theta\pi k).$$

Hence, from (5), (6), (8), and (9), we obtain

$$\sum_{k=1}^{\infty} \arctan \frac{2\theta^2}{k^2} = \left(\theta - \frac{1}{4}\right)\pi + \sum_{k=1}^{\infty} \frac{1}{k} \exp(-2\theta\pi k)\sin(2\theta\pi k);$$

and now, using [5, p. 740, Eq. (5)], we can write the sum on the right in closed form, thus giving (4), provided that $0 < \theta < \infty$.

It can easily be shown that the right member of (4) is indeed an even function of θ and that, as θ approaches zero, it vanishes. Hence, (4) is valid for real θ and (by appealing to the principle of analytic continuation) it is valid for complex θ. This evidently completes the derivation of the summation formula (4).

3. Equivalence of the Sums (3) and (4)

Defining

$$\xi(x) \equiv \frac{\sin 2x}{\cos 2x - \exp 2x},$$

we note the easily verified identity

$$\frac{\tan x}{\tanh x} = \frac{\tan x - \xi(x)}{1 + \xi(x) \tan x}.$$

Since $\tan x = \tan(x - m\pi)$, for all $m \in \mathbb{Z}$, this gives

$$\frac{\tan x}{\tanh x} = \frac{\tan(x - m\pi) - \xi(x)}{1 + \xi(x)\tan(x - m\pi)}.$$

Taking the inverse tangent of both members of this equation and observing that

$$\arctan u - \arctan v = \arctan((u - v)/(1 + uv)),$$

we obtain

$$\arctan\left(\frac{\tan x}{\tanh x}\right) = (x - m\pi) - \arctan \xi(x).$$

Now, using $\arctan x = \pi/2 - \arctan 1/x$, we deduce from this the identity

$$\frac{\pi}{2} - \arctan\left(\frac{\tanh x}{\tan x}\right) + m\pi = x - \arctan\left(\frac{\sin 2x}{\cos 2x - \exp 2x}\right) \tag{10}$$

for some $m \in \mathbb{Z}$. Replacing x by $\theta\pi$, (10) shows that the results in (3) and (4) are indeed equivalent.

4. Special Cases of Equation (4)

In (4), if we set $\theta = k$ and $\theta = k/2$ $(k = 1, 2, 3, \ldots)$, we obtain

$$\sum_{n=1}^{\infty} \arctan \frac{2k^2}{n^2} = \left(k - \frac{1}{4}\right)\pi \tag{11}$$

and

$$\sum_{n=1}^{\infty} \arctan \frac{k^2}{2n^2} = \left(k - \frac{1}{2}\right)\frac{\pi}{2}, \tag{12}$$

respectively; now, splitting the sum in (11) into even and odd terms, and using (12), we deduce also that

$$\sum_{n=0}^{\infty} \arctan \frac{2k^2}{(2n + 1)^2} = \frac{\pi}{2}k. \tag{13}$$

Equation (2) follows from (11) when $k = 1$. Equations (12) and (13) were also derived by Glaisher for $k = 1$. Ramanujan (circa 1903) derived (11), (12), and (13) for $k = 1$ [11, Ch. 2].

5. Generalizations of the Summation Formula (4)

Letting $f(x) = \arctan(z^{2n}/x^{2n})$ in the Euler-Maclaurin summation formula (cited already in Section 2), but now using [9, p. 608, Sec. 4.532, Eq. (2)] and [5, p. 396, Eq. (2)] to compute the two integrals, in basically the same way as (4) was obtained, we can derive the result

$$\sum_{k=1}^{\infty} \arctan \frac{z^{2n}}{k^{2n}} = \left(z \sec \frac{\pi}{4n} - \frac{1}{2}\right)\frac{\pi}{2} + \sum_{k=1}^{n} (-1)^k \arctan\left(\frac{\sin \xi}{\cos \xi - \exp \eta}\right) \tag{14}$$

$$(0 < |z| < \infty;\ n = 1, 2, 3, \ldots),$$

where

$$\xi = 2\pi z \cos \frac{2k - 1}{4n}\pi, \quad \eta = 2\pi z \sin \frac{2k - 1}{4n}\pi.$$

For $n = 1$ and $z = \sqrt{2}\theta$, (14) reduces to (4). For $n = 2$, setting $\alpha = \pi x \cos \pi/8$ and $\beta = \pi x \sin \pi/8$, we get

$$\sum_{k=1}^{\infty} \arctan \frac{x^4}{k^4} = \left[\alpha - \arctan\left(\frac{\sin 2\alpha}{\cos 2\alpha - \exp 2\beta}\right)\right] - \left[\beta - \arctan\left(\frac{\sin 2\beta}{\cos 2\beta - \exp 2\alpha}\right)\right] - \frac{\pi}{4}. \tag{15}$$

Glaisher [1] obtained, modulo an integer multiple of π, that

$$(16)\qquad \sum_{k=1}^{\infty} \arctan \frac{x^4}{k^4}$$
$$= \arctan\left(\frac{\tan\alpha \tanh\alpha - \tan\beta \tanh\beta - \tan\alpha \tan\beta - \tanh\alpha \tanh\beta}{\tan\alpha \tanh\alpha - \tan\beta \tanh\beta + \tan\alpha \tan\beta + \tanh\alpha \tanh\beta}\right).$$

Hence, the difference of the right members of (15) and (16) is an integer multiple of π.

By splitting the left member of (14) into even and odd terms, we easily find that

$$(17)\qquad \sum_{k=0}^{\infty} \arctan \frac{z^{2n}}{(2k+1)^{2n}} = \frac{\pi z}{4} \sec \frac{\pi}{4n}$$
$$+ \sum_{k=1}^{n} (-1)^k \left[\arctan\left(\frac{\sin\xi}{\cos\xi - \exp\eta}\right) - \arctan\left(\frac{\sin\xi/2}{\cos\xi/2 - \exp\eta/2}\right)\right]$$
$$(n = 1, 2, 3, \ldots).$$

Glaisher [1] also obtained results, modulo an integer multiple of π, for the left member of (17) in the special cases when $n = 1$ and $n = 2$.

We note here that, in general, when an infinite sum of arctangent functions is given modulo an integer multiple of π, the Euler-Maclaurin summation formula appears to be helpful in attempting to derive computationally more useful results.

By using (14) and (17), we have, in addition,

$$\sum_{k=1}^{\infty} (-1)^{k+1} \arctan \frac{z^{2n}}{k^{2n}} = \frac{\pi}{4}$$
$$+ \sum_{k=1}^{n} (-1)^k \left[\arctan\left(\frac{\sin\xi}{\cos\xi - \exp\eta}\right) - 2\arctan\left(\frac{\sin\xi/2}{\cos\xi/2 - \exp\eta/2}\right)\right].$$

In particular, letting $n = 1$ and $z = \sqrt{2}\theta$, we get

$$(18)\qquad \sum_{k=1}^{\infty} (-1)^{k+1} \arctan \frac{2\theta^2}{k^2} = \frac{\pi}{4} - \arctan\left(\frac{\sin 2\pi\theta}{\cos 2\pi\theta - \exp 2\pi\theta}\right)$$
$$+ 2\arctan\left(\frac{\sin\pi\theta}{\cos\pi\theta - \exp\pi\theta}\right).$$

By using [4, p. 277, Eq. (42.1.10)], (18) may be written equivalently as

$$(19)\qquad \sum_{k=1}^{\infty} (-1)^{k+1} \arctan \frac{2\theta^2}{k^2} = \arctan\left(\frac{\sinh\pi\theta}{\sin\pi\theta}\right) - \frac{\pi}{4}.$$

6. A Special Case of Formula (18)

In (18) or (19), if we set $\theta = \ell$ ($\ell = 1, 2, 3, \ldots$), we deduce the intesting result:

$$(19)\qquad \sum_{k=1}^{\infty} (-1)^{k+1} \arctan \frac{2\ell^2}{k^2} = \frac{\pi}{4} \quad (\ell = 1, 2, 3, \ldots),$$

from which it easily follows that

$$\sum_{k=1}^{\infty} (-1)^{k+1} \arctan\left[\frac{2(\ell^2 - m^2)k^2}{k^4 + 4\ell^2 m^2}\right] = 0 \quad (m = 1, 2, 3, \ldots)$$

and

$$\sum_{k=1}^{\infty} (-1)^{k+1} \arctan\left[\frac{2(\ell^2 + m^2)k^2}{k^4 - 4\ell^2 m^2}\right] = \frac{\pi}{2} \quad (m = 1, 2, 3, \ldots),$$

ℓ being a positive integer.

Equation (19) apparently was first derived by Ramanujan for the special case $\ell = 1$ [11, Ch. 2] and it is also derived for $\ell = 1$ by Wheelon [12, p. 46].

Acknowledgments

The present investigation was supported, in part, by the Natural Sciences and Engineering Research Council of Canada under Grant OGP0007353.

References

1. J. W. L. Glaisher. "A Theorem in Trigonometry." *Quart. J. Math.* *15* (1878): 151-57.
2. T. J. I'a. Bromwich. *An Introduction to the Theory of Infinite Series*. London: Macmillan, 1908; 2nd. ed., 1926.
3. M. L. Glasser & M. S. Klamkin. "On Some Inverse Tangent Summations." *Fibonacci Quarterly* *14.4* (1976):385-88.
4. E. R. Hansen. *A Table of Series and Products*. Englewood Cliffs: Prentice-Hall, 1975.
5. A. P. Prudnikov, Yu. A. Brychkov, & O. I. Marichev. *Integrals and Series*. Vol. I (trans. from the Russian by N. M. Queen). New York: Gordon and Breach, 1986.
6. N. Schaumberger. "Problem 399: An Old Arctangent Series Reappears." *College Math. J.* *21* (1990):253-54.
7. E. D. Rainville. *Special Functions*. New York: Macmillan, 1960.
8. K. Knopp. *Theory and Application of Infinite Series*. Glasgow: Blackie and Son, 1928.
9. I. S. Gradshteyn & I. M. Ryzhik. *Table of Integrals, Series, and Products*. New York: Academic Press, 1980.
10. H. Sagan. *Boundary and Eigenvalue Problems in Mathematical Physics*. New York: John Wiley, 1961.
11. B. C. Berndt. *Ramanujan's Notebooks, Part I*. New York: Springer-Verlag, 1985.
12. A. D. Wheelon. *Tables of Summable Series and Integrals Involving Bessel Functions*. San Francisco: Holden-Day, 1968.

AMS Classification number: 42A24

*****

Author and Title Index for *The Fibonacci Quarterly*

Currently, Dr. Charles K. Cook of the University of South Carolina at Sumter is working on an AUTHOR index, TITLE index and PROBLEM index for *The Fibonacci Quarterly*. In fact, these three indices are already completed. We hope to publish these indices in 1993 which is the 30th anniversary of *The Fibonacci Quarterly*. Dr. Cook and I feel that it would be very helpful if the publication of the indices also had AMS classification numbers for all articles published in *The Fibonacci Quarterly*. We would deeply appreciate it if all authors of articles published in *The Fibonacci Quarterly* would take a few minutes of their time and send a list of articles with primary and secondary classification numbers to

PROFESSOR CHARLES K. COOK
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SOUTH CAROLINA AT SUMTER
1 LOUISE CIRCLE
SUMTER, S.C. 29150

At their summer meeting, the board of directors voted to publish the indices on a 3.5-inch high density disk. The price will be $40.00 to nonmembers and $20.00 to members plus postage. Disks will be available for use on the MacIntosh or any IBM compatible machine using Word Perfect, Word, First Choice or any of a number of other word processors. More on this will appear in the February 1993 issue.

Gerald E. Bergum, Editor

COMPLETE FIBONACCI SEQUENCES IN FINITE FIELDS

Owen J. Brison
Faculdade de Ciências, Rua Ernesto de Vasconcelos, Bloco C1, Piso 3, 1700 Lisbon, Portugal
(Submitted November 1990)

1. Introduction

In certain finite fields $\mathbb{F}_p$ of prime order p, it is possible to write the set of nonzero elements, without repetition, in such an order that they form a closed Fibonacci-type sequence. For example, in $\mathbb{F}_{11}$ we may write

1, 8, 9, 6, 4, 10, 3, 2, 5, 7,

which evidently has the required property. In [1], a similar example is given for $\mathbb{F}_{109}$. It is implicit in [1], [12], that such sequences exist in $\mathbb{F}_p$ if $\mathbb{F}_p$ contains a so-called Fibonacci Primitive Root, or FPR: see below for definitions. Here we show (Theorem 4.2) that such sequences exist in $\mathbb{F}_p$ if and only if $\mathbb{F}_p$ contains an FPR; moreover, when $\mathbb{F}_p$ does contain an FPR, we show that the only such sequences to exist are the "natural" ones: that is, the sequences of successive powers of FPRs. Of course, it was shown in [1] that if the sequence of successive powers of an element is to have this Fibonacci property, then the element in question must be an FPR, but here we allow for any sequence of elements.

We also prove (Theorem 4.4) analogous results for Fibonacci-type sequences of the set of (nonzero) squares of $\mathbb{F}_p$. In this context, the sequence

1, 4, 5, 9, 3,

is a Fibonacci-type sequence of the squares of $\mathbb{F}_{11}$.

It will be shown that, except for the fields $\mathbb{F}_4$ and $\mathbb{F}_9$, these phenomena only occur in the fields of prime order.

We wish to thank the referee for pointing out several references, and in particular for the information that part of Theorem 2.5 below is proved in [10].

2. Preliminaries

In this section we collect some preliminaries from [3], [7], [8], [14], and [15]; p will always denote a prime, q will stand for a power of p, $\mathbb{F}_q$ will denote the field of order q, $\mathbb{F}_q^*$ will denote the multiplicative group of $\mathbb{F}_q$, while F_n and L_n will, respectively, denote the n^{th} Fibonacci and n^{th} Lucas number. In addition, if z is an integer, then $\bar{z}$ will denote the image of z in $\mathbb{F}_p$ (in situations where the prime p is understood). If g is an element of a group, then $|g|$ will denote the order of g.

A Φ-sequence in a finite field $\mathbb{F}$ is defined to be a sequence

$$\mathfrak{S} = (s_0, s_1, s_2, \ldots) \quad (s_i \in \mathbb{F}),$$

where

$$s_{n+2} = s_{n+1} + s_n \text{ for } n = 0, 1, 2, \ldots .$$

Any Φ-sequence in $\mathbb{F}_q$ is periodic with period $r \le q^2 - 1$: see [7, Th. 8.7]. This means that

$$s_{n+r} = s_n \text{ for } n = 0, 1, 2, \ldots,$$

and that r is the least natural number for which this holds. Following Wall [15], we write $k(p)$ for the period of the Fibonacci sequence (mod p); note that De Leon [3] writes $A(p)$ for this number, while Vajda [14] writes $P(p, F)$.

Theorem 2.1: ([7, Th. 8.16]). If r is the period of some Φ-sequence in $\mathbb{F}_q$, where $q = p^n$, then $r \mid k(p)$. □

Theorem 2.2: (Wall, [15]; see also [14, p. 91]). Let p be a prime. Then

(a) $k(p) \mid p - 1$ if $p \equiv \pm 1 \pmod 5$.

(b) $k(p) \mid 2(p + 1)$ if $p \equiv \pm 2 \pmod 5$. □

The polynomial $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t]$ is what is called [7, p. 198], the *characteristic polynomial* of a Φ-sequence. We have

Theorem 2.3: ([7, Th. 8.21]). Let $p \neq 5$ be a prime. Let s_0, s_1, ..., be a Φ-sequence in $\mathbb{F}_q$. Let $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t]$ and suppose that g, h are the roots of $f(t)$ in a splitting field $\mathbb{F} \supset \mathbb{F}_q$. Then there exist α, $\beta \in \mathbb{F}$ such that

$$s_i = \alpha g^i + \beta h^i, \text{ for } i = 0, 1, 2, \ldots . \quad \square$$

Lemma 2.4: Let p be an odd prime and let $n \in \mathbb{N}$ be such that

$$(p^n - 1)/2 \mid 2(p + 1).$$

Then $p \leq 5$ and $n \leq 2$.

Proof: We have

$$(p - 1)(p^{n-1} + \cdots + 1) \; 4(p + 1).$$

But $(p - 1, p + 1) = 2$, because p is odd. Thus $(p - 1) \mid 8$, and so $p \in \{3, 5\}$. If $n \geq 3$ we may easily derive a contradiction, and the assertion follows.

The first four parts of the following theorem are a combination of results from [3], [10], [11], and [12] (but note that we are working in an extension field $\mathbb{F} \supset \mathbb{F}_p$ rather than in $\mathbb{F}_p$). Proofs of parts (a)-(c) can be found in Phong [10, pp. 68-69], or can be extracted from a careful reading of De Leon [3], together with Wall's result that $k(p)$ is even for $p > 2$: [11, Th. 4]. Part (d) is proved by Shanks [12, p. 164]. We supply proofs for completeness.

Theorem 2.5: Let $p \geq 7$ be a prime. Let g, h be the roots, in a suitable extension field $\mathbb{F} \supseteq \mathbb{F}_p$, of the polynomial

$$f(t) = t^2 - t - 1 \in \mathbb{F}_p[t].$$

Then

(a) Not both $|g|$ and $|h|$ can be odd. If, say, $|h|$ is odd, then $|g| = 2|h|$.

(b) If both $|g|$, $|h|$ are even, then $|g| = |h|$ is divisible by 4.

(c) If $|g|$, say, is even, then $|g| = k(p)$. In particular, $k(p)$ is even.

(d) We have g, $h \in \mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod 5$.

(e) If $|g|$, say, is of the form $p^n - 1$ or $(p^n - 1)/2$, for $n \in \mathbb{N}$, then $n = 1$, $g \in \mathbb{F}_p$, and $p \equiv \pm 1 \pmod 5$.

Proof: Since g, h are the roots of $f(t) = t^2 - t - 1$, then $g = -1/h$. Write $|g| = a$ and $|h| = b$.

(a) Suppose that b is odd, and note that $b = |1/h|$. Since $|-1| = 2$, it follows that $|g| = 2|1/h|$, and thus that $a = 2b$.

(b) Suppose that a, b are both even. Then we have

$$1 = g^a = (-1)^a/h^a = 1/h^a$$

and so $h^a = 1$. Similarly, $g^b = 1$, and so $a = b$. Suppose that $a = 2d$ with d odd. Then $|g^d| = 2$ and so $g^d = -1$, the unique element of order 2 in $\mathbb{F}_p^*$. But then

$$h^d = (-1)^d/g^d = -1/-1 = 1,$$

and so b is odd, contrary to hypothesis. Assertion (b) now follows.

(c) We adapt the proof of [3, Lem. 1]. It follows by induction that $g^n = \overline{F}_n g + \overline{F}_{n-1}$ for any natural number n (and similarly for h^n). Since $\overline{F}_{k(p)} = 0$ and $\overline{F}_{k(p)-1} = 1$, it follows that $g^{k(p)} = 1$ and thus that $a|k(p)$. Similarly, $b|k(p)$. In particular, $k(p)$ must be even. If $\overline{F}_a = 0$, then $1 = g^a = \overline{F}_{a-1}$; thus, $k(p)|a$ and so $k(p) = a$. Similarly, if $\overline{F}_b = 0$, then $k(p) = b$. Suppose then that $\overline{F}_a \neq 0$ and $\overline{F}_b \neq 0$. Then $1 = g^a = \overline{F}_a g + \overline{F}_{a-1}$ and so $g = (1 - \overline{F}_{a-1})/\overline{F}_a$. Thus, as in [3], we have

$$\begin{aligned} 0 &= (g^2 - g - 1)\overline{F}_a^2 \\ &= -(\overline{F}_a^2 - \overline{F}_a\overline{F}_{a-1} - \overline{F}_{a-1}^2) - (\overline{F}_a + 2\overline{F}_{a-1}) + 1 \\ &= (-1)^a - \overline{L}_a + 1. \end{aligned}$$

Thus, $\overline{L}_a = 1 + (-1)^a$. Similarly, $\overline{L}_b = 1 + (-1)^b$.

Now, if a is even, then $\overline{L}_a = 2$. But $\overline{L}_a^2 - 5\overline{F}_a^2 = 4$ and so $\overline{F}_a = 0$, a contradiction. Thus, a must be odd. Similarly, b must also be odd. But this is in contradiction to (a). It follows that at least one of $\overline{F}_a$, $\overline{F}_b$ must be zero, and assertion (c) follows.

(d) We have $(2g - 1)^2 = 5 \in \mathbb{F}_p$. On the other hand, if $w \in \mathbb{F}_p$ satisfies $w^2 = 5$, then $(1 \pm w)/2$ are the roots of $f(t)$. Thus, $g, h \in \mathbb{F}_p$ if and only if the element 5 is a square in $\mathbb{F}_p$, and this occurs if and only if $p \equiv \pm 1 \pmod 5$, by the quadratic reciprocity law [5, Ths. 97 and 98].

(e) Suppose that $|g| = p^n - 1$ or $(p^n - 1)/2$. Then $|g|$ divides $k(p)$ by (a) and (c) above. Suppose that $p \equiv \pm 2 \pmod 5$. Then $k(p)|2(p + 1)$ by 2.2(b). Thus, in either case, $(p^n - 1)/2|2(p + 1)$. This is impossible by Lemma 2.4, because $p \geq 7$. Therefore, we must have $p \equiv \pm 1 \pmod 5$, and so $g \in \mathbb{F}_p$ by (d). But now $k(p)|(p - 1)$ by 2.2(a), whence $(p^{n-1} + \cdots + 1)|2$ and it follows that $n = 1$. □

3. Fibonacci Primitive Roots

Definition 3.1: Let $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t] \subset \mathbb{F}_q[t]$ where q is a power of p. Suppose that $g \in \mathbb{F}_q$ is a root of $f(t)$.

(a) (Shanks, [12]). We call g a *Fibonacci Primitive Root* (*FPR*) *in* $\mathbb{F}_q$ if $|g| = q - 1$; that is, if g is a primitive root in $\mathbb{F}_q$.

(b) We call g a *Fibonacci Square-Primitive Root* (*FSPR*) *in* $\mathbb{F}_q$ if g generates the subgroup of squares in $\mathbb{F}_q$; if q is odd, this means that

$$|g| = (q - 1)/2.$$

Fibonacci Primitive Roots and related topics have an extensive literature: see, for example, references [1], [3], [6], and [9]-[15].

In part (b) of the following result, the criterion for the existence of an FPR is proved in Theorem 1 of De Leon [3], while the assertions on the number of FPRs are proved by Shanks [15, pp. 164-65]. The exceptional cases to this theorem ($p < 7$) will be dealt with in 3.3 below.

Theorem 3.2: Let $p \geq 7$ be a prime and let $q = p^n$ where $n \in \mathbb{N}$.

(a) If $\mathbb{F}_q \supset \mathbb{F}_p$ possesses an FPR or an FSPR, then $\mathbb{F}_q = \mathbb{F}_p$ and $p \equiv \pm 1 \pmod 5$.

(b) $\mathbb{F}_p$ possesses an FPR iff $k(p) = p - 1$. Further, if $k(p) = p - 1$, then
- (i) if $p \equiv 1 \pmod 4$, there are two FPRs;
- (ii) if $p \equiv -1 \pmod 4$, there is just one FPR (and one FSPR).

(c) $\mathbb{F}_p$ possesses an FSPR iff either

(i) $k(p) = p - 1$ and $p \equiv -1 \pmod 4$, when there is a unique FSPR; or

(ii) $k(p) = (p - 1)/2$. In this case, we must have $p \equiv 1 \pmod 4$, then

(α) if $p \equiv 1 \pmod 8$ there are two FSPRs;

(β) if $p \equiv 5 \pmod 8$, there is a unique FSPR.

Proof: Again write $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t]$, and suppose that g, h are the roots of $f(t)$ in the field $\mathbb{F}_q \supset \mathbb{F}_p$.

(a) Suppose that g is an FPR or an FSPR in $\mathbb{F}_q$. Then $|g| = p^n - 1$ or $(p^n - 1)/2$, and so by 2.5(e), $p \equiv \pm 1 \pmod 5$ and $n = 1$. Thus, $\mathbb{F}_q = \mathbb{F}_p$.

(b) If g is an FPR in $\mathbb{F}_p$, then $|g| = p - 1$ is even and so $k(p) = p - 1$ by 2.5(c). Further, $p \equiv \pm 1 \pmod 5$ by 2.5(d).

Conversely, suppose $k(p) = p - 1$. Let g be an even-order root of $f(t)$; then $|g| = p - 1$, by 2.5(c), and so $g \in \mathbb{F}_p$ by 2.5(e). Thus, g is an FPR in $\mathbb{F}_p$. Now, if $p \equiv 1 \pmod 4$, then $4 | p - 1$, whence $|g| = |h|$ by 2.5(c), and so g, h are both FPRs. However, if $p \equiv -1 \pmod 4$, then $p - 1$ is twice an odd number. Thus, by 2.5(a) and 2.5(c), g has order $p - 1$, and so is an FPR, while $h \in \mathbb{F}_p$ has order $(p - 1)/2$, and so is an FSPR.

(c) Suppose that $h \in \mathbb{F}_p$ is an FSPR. Then $|h| = (p - 1)/2$, and so

$$k(p) \in \{p - 1, (p - 1)/2\}$$

by 2.5(a) and 2.5(c). Suppose that $k(p) = p - 1$. Then, by part (b), $\mathbb{F}_p$ possesses an FPR, which must be the other root g of $f(t)$. But then g is a non-square in $\mathbb{F}_p$, while h is a square and $g = -1/h$. Thus, -1 is a non-square in $\mathbb{F}_p$ and $p \equiv -1 \pmod 4$ by quadratic reciprocity. This proves the "only if" part of (c).

If $k(p) = p - 1$ and $p \equiv -1 \pmod 4$, then there is a unique FSPR in $\mathbb{F}_p$ by (b). Suppose that $k(p) = (p - 1)/2$. Since $k(p)$ is even by 2.5, then $p \equiv 1 \pmod 4$.

(α) If $p \equiv 1 \pmod 8$, then $(p - 1)/2$ is divisible by 4 and so both roots of $f(t)$ have order $(p - 1)/2$ by 2.5(a)-(c). These roots belong to $\mathbb{F}_p$ by 2.5(e), and so there are two FSPRs in $\mathbb{F}_p$.

(β) If $p \equiv 5 \pmod 8$, then $(p - 1)/2$ is twice an odd number. By 2.5(a)-(c), one root of $f(t)$ has order $(p - 1)/2$ while the other has order $(p - 1)/4$. Again by 2.5(e), these roots belong to $\mathbb{F}_p$, and so there is a unique FSPR in $\mathbb{F}_p$.

Assertion (c) now follows, and the proof is complete. □

The following proposition lists a collection of easily-verifiable facts concerning FPRs for primes $p < 7$.

Proposition 3.3: We have

(a) $k(2) = 3$. Let ζ be a root in $\mathbb{F}_4$ of $f(t) = t^2 + t + 1 \in \mathbb{F}_2[t]$. Then $1 + \zeta$ is the other root of $f(t)$. We have $|\zeta| = |1 + \zeta| = 3$, and so ζ and $1 + \zeta$ are both FPRs in $\mathbb{F}_4$; they are also FSPRs because all elements of $\mathbb{F}_4$ are squares.

(b) $k(3) = 8$. Let ζ be a root in $\mathbb{F}_9$ of $p(t) = t^2 + 1 \in \mathbb{F}_3[t]$. Then $f(t) = t^2 - t - 1 \in \mathbb{F}_3[t]$ has roots $g = \eta - 1$ and $h = -\eta - 1$ in $\mathbb{F}_9$. Further, $|g| = |h| = 8$, and so g, h are FPR's in $\mathbb{F}_9$.

(c) $k(5) = 20$. Because $(t - 3)^2 = t^2 - t - 1 \in \mathbb{F}_5[t]$, then the element $3 \in \mathbb{F}_5$ is a double root of $f(t)$ in $\mathbb{F}_5$. Further, $|3| = 4$, so that 3 is the unique FPR in $\mathbb{F}_5$. Note that 2.5(c) definitely fails for $p = 5$. □

It should be noted that Brousseau [1] lists the FPR's for those primes $p < 300$ that possess such, while Wall [15] gives the values of $k(p)$ for all primes $p < 2000$. In section 5 below, we list the FPRs and FSPRs for those primes $p < 2000$ that possess such.

It is proved in [11], on the assumption of certain Riemann hypotheses, that, asymptotically, the proportion $C = 0.2657...$ of all primes possess an FPR; since, apart from $p = 5$, the only eligible primes p satisfy $p \equiv \pm 1 \pmod 5$, then we are to expect that over half of these possess an FPR. It might be of interest to determine the proportion of primes that possess an FSPR. For example, there are 146 primes $p < 2000$ with $p \equiv \pm 1 \pmod 5$, of which 80 possess FPRs and 76 possess FSPRs (see the table in section 5).

4. Complete Φ-Sequences

Let p be a prime and let q be a power of p. Let $\mathfrak{S} = (s_0, s_1, s_2, \ldots)$ be a Φ-sequence of period r in $\mathbb{F}_q$. We call $\mathfrak{S}$ a *complete Φ-sequence in $\mathbb{F}_q$* if $r = q - 1$ and if $\{s_0, s_1, \ldots, s_{r-1}\}$ is precisely the set of nonzero elements of $\mathbb{F}_q$. If $\{s_0, s_1, \ldots, s_{r-1}\}$ is precisely the set of nonzero squares of $\mathbb{F}_q$, so that $r = (q-1)/2$ if q is odd, then $\mathfrak{S}$ is called a *square-complete Φ-sequence in $\mathbb{F}_q$*.

Lemma 4.1: Let $f(t) = t^2 - t - 1 \in \mathbb{F}[t]$ and let g be a root of $f(t)$ in a field $\mathbb{F} \supset \mathbb{F}_p$. Then the Φ-sequence $\mathfrak{S} = (s_0, s_1, \ldots)$ in $\mathbb{F}$ with $s_0 = 1$, $s_1 = g$ has period $a = |g|$, and

$$\{s_0, s_1, \ldots, s_{a-1}\} = \{1, g, \ldots, g^{-1}\}.$$

In particular, if g is an FPR, or FSPR, in $\mathbb{F}$, then $\mathfrak{S}$ is a complete- or square-complete Φ-sequence in $\mathbb{F}$, respectively.

Proof: This is clear. □

We now give our characterization of complete Φ-sequences for primes $p \geq 7$; the cases $p < 7$ are exceptional and will be dealt with later. It is worth observing that if $\mathfrak{S}$ is a complete Φ-sequence in $\mathbb{F}_p$, then the sequence formed by multiplying the terms of $\mathfrak{S}$ by a fixed nonzero element of $\mathbb{F}_p$ is essentially the same sequence $\mathfrak{S}$ with the terms all shifted by a fixed amount; we will thus not distinguish between such multiples.

Theorem 4.2: Let $p \geq 7$ be a prime and let $q = p^n$ where $n \in \mathbb{N}$. Then there is a complete Φ-sequence in $\mathbb{F}_q$ if and only if there is an FPR in $\mathbb{F}_q$, and for this to happen we must have $q = p$. Further, any complete Φ-sequence in $\mathbb{F}_p$ has the form $(1, j, j^2, \ldots)$ where j is an FPR in $\mathbb{F}_p$, and conversely.

Proof: Let $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t]$, let g, h be the roots of $f(t)$ in a splitting field $\mathbb{F} \supset \mathbb{F}_q$. Suppose without loss that $|g|$ is even; then $|g| = k(p)$ by 2.5(c).

If j is an FPR in $\mathbb{F}_q$, then the Φ-sequence $(1, j, j^2, \ldots)$ is complete (in $\mathbb{F}_q$) by Lemma 4.1.

Suppose now that $\mathfrak{S}$ is a complete Φ-sequence in $\mathbb{F}_q$. Then $\mathfrak{S}$ has period $q - 1$ and so $q - 1 | k(p)$ by 4.1. If $p \equiv \pm 2 \pmod 5$, then $k(p) | 2(p + 1)$ by 2.2. Thus, $q - 1 | 2(p + 1)$, which is impossible by 2.4 because $p \geq 7$. Therefore, we may assume that $p \equiv \pm 1 \pmod 5$. Then $k(p) | p - 1$ by 2.2; thus, $q - 1 | p - 1$, and so $q = p$ and $k(p) = p - 1$. Thus, g is an FPR in $\mathbb{F}_p$. Note now that $f(t)$ splits in $\mathbb{F}_p$. By 2.3, there exist $\alpha, \beta \in \mathbb{F}_p$ such that

$$\mathfrak{S} = (\alpha + \beta, \alpha g + \beta h, \alpha g^2 + \beta h^2, \ldots),$$

and because $\mathfrak{S}$ is complete,

$$\mathbb{F}_p^* = \{\alpha g^i + \beta h^i : 0 \leq i \leq p - 2\}.$$

But $h = -1/g = g^{(p-1)/2}g^{p-2} = g^{(3p-5)/2}$. Thus, the map

$$g^i \mapsto \alpha g^i + \beta g^{i(3p-5)/2}, \; 0 \le i \le p-2,$$

is a permutation of $\mathbb{F}_p^*$. But then the polynomial

$$p(t) = \alpha t + \beta t^{(3p-5)/2} \in \mathbb{F}_p[t]$$

is a permutation polynomial of $\mathbb{F}_p$. But now Hermite's criterion for permutation polynomials (see [4, §84] or [7, Th. 7.4]) implies that, in particular, the reduction, $P(t)$ say, of $(p(t))^4 \pmod{t^p - t}$ has degree $d < p - 1$. A certain amount of calculation reveals that

$$P(t) = 6\alpha^2\beta^2 t^{p-1} + Q(t),$$

where $Q(t) \in \mathbb{F}_p[t]$ has degree $e \le p - 2$. It follows that $\alpha\beta = 0$, and so the only possibilities for $\mathfrak{G}$ are (nonzero multiples of):

$$(1, g, g^2, \ldots),$$

and if, also, $|h| = p - 1$,

$$(1, h, h^2, \ldots).$$

This completes the proof. □

The next theorem characterizes the square-complete Φ-sequences for $p \ge 7$; again, the exceptional cases ($p < 7$) are dealt with later. The characterization is almost a word-for-word "translation" of the previous result, but there are a number of technical differences in the proof. Hermite's criterion is not directly applicable here, but we can apply ideas from its proof to get what we need. We will also need to know that the smallest prime $p \equiv \pm 1 \pmod 5$ for which $k(p) < p - 1$ is $p = 29$. This fact is given in Wall [15], but may easily be calculated by hand: we need only check the Fibonacci sequences mod 11 and mod 19.

First we need a lemma; it is not new (see [4, §74]) but we indicate a proof.

Lemma 4.3: Let G be a subgroup of $\mathbb{F}_q^*$ with $|G| = m$. Then

(a) $\sum_{g \in G} g^m = m$ (considered as an element of $\mathbb{F}_q^*$), and

(b) $\sum_{g \in G} g^j = 0$, for $1 \le j \le m - 1$.

Proof:

(a) This follows because $g^m = 1$ for all $g \in G$.

(b) The elements of G are precisely the roots of $t^m - 1 \in \mathbb{F}_q[t]$. Then

$$\sum_{g \in G} g^j$$

is the sum of the j^{th} powers of these roots, and the assertion follows by Newton's formula [4, §74] and [7, Th. 1.75]. □

Theorem 4.4: Let $p \ge 7$ be a prime and let $q = p^n$ where $n \in \mathbb{N}$. Then there is a square-complete Φ-sequence in $\mathbb{F}_q$ if and only if there is an FSPR in $\mathbb{F}_q$, and for this to happen we must have $q = p$. Further, any square-complete Φ-sequence in $\mathbb{F}_p$ has the form $(1, j, j^2, \ldots)$ where j is an FSPR in $\mathbb{F}_p$, and conversely.

Proof: Let $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t]$, let g, h be the roots of $f(t)$ in a splitting field $\mathbb{F} \supset \mathbb{F}_q$. Suppose without loss that $|g|$ is even; then $|g| = k(p)$ by 2.5(c).

If j is an FSPR in $\mathbb{F}_q$, then the Φ-sequence $(1, j, j^2, \ldots)$ is square-complete (in $\mathbb{F}_q$) by Lemma 4.1.

Suppose now that $\mathfrak{S}$ is a square-complete Φ-sequence in $\mathbb{F}_q$. Then $\mathfrak{S}$ has period $(q - 1)/2$, and so $(q - 1)/2 | k(p)$ by 4.1. If $p \equiv \pm 2 \pmod 5$, then $k(p) | 2(p + 1)$ by 2.2. Thus $(q - 1)/2 | 2(p + 1)$, which is impossible by 2.4 because $p \geq 7$. We may therefore assume that $p \equiv \pm 1 \pmod 5$, and so $g, h \in \mathbb{F}_p$. Then $k(p) | p - 1$ by 2.2; thus $q - 1 | 2(p - 1)$, and so $q = p$ and

$$k(p) \in \{p - 1, (p - 1)/2\}.$$

By 2.3, there exist $\alpha, \beta \in \mathbb{F}_p$ such that

$$\mathfrak{S} = (\alpha + \beta, \alpha g + \beta h, \alpha g^2 + \beta h^2, \ldots).$$

We consider separately the two possibilities for $k(p)$.

(i) Suppose that $k(p) = p - 1$. Since $\mathfrak{S}$ has period $(p - 1)/2$, then

$$\alpha + \beta = \alpha g^{(p-1)/2} + \beta h^{(p-1)/2}.$$

But $|g| = p - 1$ and so $g^{(p-1)/2} = -1$. If also $|h| = p - 1$, then $h^{(p-1)/2} = -1$, and so $\alpha + \beta = -(\alpha + \beta) = 0$. But then $\mathfrak{S}$ contains the element 0, and so cannot be square-complete, a contradiction. Therefore $|h| = (p - 1)/2$, by 2.5, and so $\alpha + \beta = -\alpha + \beta$. Thus $\alpha = 0$, and so $\mathfrak{S}$ must be (a nonzero, square multiple of)

$$(1, h, h^2, \ldots),$$

and h is an FSPR in $\mathbb{F}_p$.

(ii) Suppose that $k(p) = (p - 1)/2$. By the Remark before Lemma 4.3, we may assume that $p \geq 29$. Since $|g| = k(p)$, then g is an FSPR in $\mathbb{F}_p$. By 3.2(c), $p \equiv 1 \pmod 4$, and so -1 is a square in $\mathbb{F}_p$. We then have $g^{-1} = g^{(p-3)/2}$ and $-1 = g^{(p-1)/4}$, whence $h = -1/g = g^{(3p-7)/4}$. Write Q for the subgroup of squares in $\mathbb{F}_p^*$; then $|Q| = (p - 1)/2$. Since $\mathfrak{S}$ is square-complete, we have

$$\begin{aligned} Q &= \{\alpha g^i + \beta h^i : 0 \leq i \leq (p - 1)/2\} \\ &= \{\alpha g^i + \beta g^{i(3p-7)/4} : 0 \leq i \leq (p - 1)/2\} \\ &= \{\alpha c + \beta c^{(3p-7)/4} : c \in Q\}. \end{aligned}$$

Calculation now reveals that

$$(\alpha c + \beta c^{(3p-7)/4})^8 = x(c),$$

where $x(t) \in \mathbb{F}_p[t]$ is a polynomial of degree at most $(p - 3)/2$ with constant term $70\alpha^4\beta^4$. There are certain points that require care in the calculation here; for example, the second term in the expansion is

$$\begin{aligned} 8\alpha^7\beta c^7 c^{(3p-7)/4} &= 8\alpha^7\beta c^{(3p+21)/4} \\ &= 8\alpha^7\beta c^{(p-1)/2} c^{(p+23)/4}. \end{aligned}$$

Now $c^{(p-1)/2} = 1$ because $c \in Q$, while $1 \leq (p + 23)/4 < (p - 1)/2$ is the upper bound because $p \geq 29 > 25$. Thus, we obtain a term whose degree in c lies between 1 and $(p - 3)/2$. The constant term arises naturally as the "middle" term of the expansion, and all other terms have degree between 1 and $(p - 3)/2$. Now 4.3 gives both the first [since $(p - 3)/2 \geq 8$] and the last equality in the following chain:

$$0 = \sum_{c \in Q} c^8 = \sum_{c \in Q} (\alpha c + \beta c^{(3p-7)/4})^8 = \sum_{c \in Q} x(c) = ((p - 1)/2)70\alpha^4\beta^4.$$

It follows (because $p \geq 29$ cannot divide 70) that $\alpha\beta = 0$. Thus, the only possible square-complete Φ-sequences in $\mathbb{F}_p$ are (nonzero square multiples of)

$$(1, g, g^2, \ldots),$$

and if, also, h is an FSPR,

$$(1,\ h,\ h^2,\ \ldots).$$

This completes the proof. □

The following result mirrors Proposition 3.3, and deals with the primes 2, 3, and 5.

Proposition 4.5:

(a) The field $\mathbb{F}_2$ possesses neither a complete Φ-sequence nor a square-complete Φ-sequence. If ζ is as in 3.3(a), then

$$1,\ \zeta,\ 1+\zeta, \quad \text{and} \quad 1,\ 1+\zeta,\ \zeta$$

are the only complete Φ-sequences in $\mathbb{F}_4$; they are also square-complete because all elements of $\mathbb{F}_4^*$ are squares.

(b) The field $\mathbb{F}_3$ possesses neither a complete Φ-sequence nor a square-complete Φ-sequence. If ω is any element in $\mathbb{F}_9$ that is *not* in $\mathbb{F}_3$ then the Φ-sequence with $s_0 = 1$, $s_1 = \omega$:

$$1,\ \omega,\ 1+\omega,\ 1+2\omega,\ 2,\ 2\omega,\ 2+2\omega,\ 2+\omega,$$

is in $\mathbb{F}_9$, but there are no square-complete Φ-sequences.

(c) The sequence 1, 3, 4, 2 is the unique complete Φ-sequence in $\mathbb{F}_5$, while this field possesses no square-complete Φ-sequence.

(d) If q is any of 2^n, $n \geq 3$, or 3^n, $n \geq 3$, or 5^n, $n \geq 2$, then $\mathbb{F}_q$ possesses neither a complete Φ-sequence nor a square-complete Φ-sequence.

Proof: Most of these assertions are straightforward to verify. For part (d), we use 2.1. □

5. List of FPRs and FSPRs for Primes $p < 2000$

We finish with a table of FPRs and FSPRs for those primes $p < 2000$ that possess such; as we have seen, the prime 5 is "singular" and we set it apart in the list. By 3.2, the only primes $p < 5$ eligible are those with $p \equiv \pm 1 \pmod 5$ and $k(p) \in \{p-1, (p-1)/2\}$; all other primes are thus omitted from the list. For each eligible prime, we give the respective root(s) in $\mathbb{F}_p$ of $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t]$ when they are either primitive (denoted by P) or square-primitive (denoted by Q). We omit those roots that are not either primitive or square-primitive.

Information on the values of $k(p)$ necessary to find the eligible primes was taken from Wall [15]. Certain of the calculations were performed by computer using the finite field facility in the Group Theory Language CAYLEY [2], although much of the work was carried out using nothing more than a pocket calculator.

p	FPR (P) or FSPR (Q)		p	FPR (P) or FSPR (Q)	
5	3P				
11	8P	4Q	19	15P	5Q
29	6Q		31	13P	19Q
41	7P	35P	59	34P	26Q
61	18P	44P	71	63P	9Q
79	30P	50Q	89	10Q	80Q
101	23Q		109	11P	99P
131	120P	12Q	149	41P	109P
179	105P	75Q	181	168Q	
191	89P	103Q	229	148Q	
239	224P	16Q	241	52P	190P
251	134P	118Q	269	72P	198P

p	FPR (P) or FSPR (Q)		p	FPR (P) or FSPR (Q)	
271	255P	17Q	311	59P	253Q
349	206Q		359	106P	254Q
379	360P	20Q	389	152P	238P
401	112Q	290Q	409	130P	280P
419	399P	21Q	431	341P	91Q
439	370P	70Q	449	166P	284P
479	229P	251Q	491	74P	418Q
499	275P	225Q	509	388Q	
569	337P	233P	571	298P	274Q
599	575P	25Q	601	137P	465P
631	110P	522Q	641	279P	363P
659	201P	459Q	701	27P	675P
719	330P	390Q	739	119P	621Q
751	541P	211Q	761	92Q	670Q
821	213P	609P	839	498P	342Q
929	31P	899P	941	228Q	
971	798P	174Q	1019	526P	494Q
1021	458Q		1039	287P	753Q
1051	73P	979Q	1061	602Q	
1091	212P	880Q	1109	703Q	
1129	328P	802P	1171	1058P	114Q
1181	534P	648P	1201	78P	1124P
1229	745Q		1249	405Q	845Q
1259	1224P	36Q	1301	268P	1034P
1319	920P	400Q	1321	453P	869P
1361	83Q	1279Q	1399	240P	1160Q
1409	125Q	1285Q	1429	547P	883P
1439	701P	739Q	1451	283P	1169Q
1459	1293P	167Q	1481	39P	1443P
1489	681P	809P	1499	1291P	209Q
1531	88P	1444Q	1549	1020Q	
1559	1520P	40Q	1571	1044P	568Q
1609	636P	974P	1619	855P	765Q
1621	1446Q		1669	136Q	
1709	601Q		1741	321Q	
1759	859P	901Q	1789	1554Q	
1801	427P	1375P	1811	186P	1626Q
1831	1053P	779Q	1861	1498Q	
1879	1457P	423Q	1889	824P	1066P
1901	98P	1804P	1931	988P	944Q
1949	789P	1161P	1979	1935P	45Q

Acknowledgments

The author wishes to acknowledge partial support from "Projecto 87463 da JNICT" and from the "Centro de Algebra da Universidade de Lisboa do INIC."

References

Note that Chapter 8 of [7] corresponds closely to Chapter 6 of [8], to the extent that Theorem 8.n of [7] corresponds to Theorem 6.n of [8]; in the text we have thus limited the relevant references to [7].

1. Brother Alfred Brousseau. "Table of Indices with a Fibonacci Relation." *Fibonacci Quarterly* 10 (1972):182-84.
2. John J. Cannon. "An Introduction to the Group Theory Language, Cayley." In *Computational Group Theory*, ed. Michael D. Atkinson. London, Orlando: Academic Press, 1984, pp. 145-83.
3. M. J. De Leon. "Fibonacci Primitive Roots and the Period of the Fibonacci Numbers Modulo p." *Fibonacci Quarterly* 15 (1977):353-55.
4. Leonard Eugene Dickson. *Linear Groups with an Exposition of the Galois Field Theory*. Leipzig: Teubner, 1901; New York: Dover, 1958.
5. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*. 5th ed. Oxford: Clarendon Press, 1979.
6. P. Kiss & B. M. Phong. "On the Connection between the Rank of Apparition of a Prime p in Fibonacci Sequence and the Fibonacci Primitive Roots." *Fibonacci Quarterly* 15 (1977):347-49.
7. Rudolf Lidl & Harald Niederreiter. *Finite Fields*. Reading, Mass: Addison-Wesley, 1983; Cambridge: Cambridge University Press, 1984.
8. Rudolf Lidl & Harald Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge: Cambridge University Press, 1986.
9. M. E. Mays. "A Note on Fibonacci Primitive Roots." *Fibonacci Quarterly* 20 (1982):111.
10. B. M. Phong. "Lucas Primitive Roots." *Fibonacci Quarterly* 29 (1991):66-71.
11. J. W. Sander. "On Fibonacci Primitive Roots." *Fibonacci Quarterly* 28 (1990):79-80.
12. Daniel Shanks. "Fibonacci Primitive Roots." *Fibonacci Quarterly* 10 (1972): 162-68.
13. Daniel Shanks & Larry Taylor. "An Observation on Fibonacci Primitive Roots." *Fibonacci Quarterly* 11 (1973):159-60.
14. S. Vajda. *Fibonacci & Lucas Numbers, and the Golden Section: Theory and Application*. Chichester: Ellis Horwood Ltd., 1989.
15. D. D. Wall. "Fibonacci Series Modulo m." *Amer. Math. Monthly* 67 (1960): 525-532.

*****

THE DIOPHANTINE EQUATION $x^2 + a^2y^m = z^{2n}$ WITH $(x, ay) = 1$

Konstantine Dabmian Zelator (formerly K. Spyropoulos)
Carnegie Mellon University, Pittsburgh, PA 15213
(Submitted December 1990)

As it is well known, the equation

(1) $$x^2 + y^4 = z^4$$

has no solutions in the set of positive integers (one can find this equation in a number of sources including Dickson's *History of the Theory of Numbers* [2]). The equation $x^2 + y^4 = z^4$ serves as a classic result in the history of diophantine analysis, and one of the first known examples where Fermat's method of infinite descent is employed.

Therefore, if $m \equiv 0 \pmod 4$ and n is even, the equation $x^2 + y^m = z^{2n}$ has no solution in positive integers x, y, and z.

Now consider the diophantine equation $x^2 + a^2y^m = z^{2n}$ with m even. We will show that if a is a positive odd integer and if it has a prime divisor $p \equiv \pm 3 \pmod 8$, then the above equation has no solution with $(x, ay) = 1$ and y odd, provided that $n \equiv 0 \pmod 2$. This author has shown in [3] that the equation $x^4 + p^2y^4 = z^2$, p a prime with $p \equiv 5 \pmod 8$, has no solution in the set of positive integers. It is known, however, that for certain primes of the form $p \equiv 1$, 3, or $7 \pmod 8$, the latter equation does have a solution over the set of positive integers (for fruther details, refer to [3]).

To start, we have

Theorem 1: Let a be a positive odd integer with a prime factor p of the form $p \equiv \pm 3 \pmod 8$. Also, let m and n be positive integers with m and n both even. Then the diophantine equation $x^2 + a^2y^m = z^{2n}$ with $(x, ay) = 1$ and y odd has no solution in the set of positive integers.

Proof: Assume (x, y, z) to be a solution to the equation

(2) $$x^2 + a^2y^m = z^{2n}$$

with $(x, ay) = 1$.

Since m is even, $m = 2k$, the equation

(3) $$x^2 + a^2y^{2k} = z^{2n},$$

describes a Pythagorean triangle with side lengths x, ay^k, and z^n. Accordingly, there must exist positive integers t and ℓ of different parity, i.e., $t + \ell \equiv 1 \pmod 2$, with $(t, \ell) = 1$ (t and ℓ relatively prime), such that

(4) $$x = 2t\ell, \quad ay^k = t^2 - \ell^2, \quad z^n = t^2 + \ell^2.$$

From the second equation of (4), we obtain

(5) $$ay^k = (t - \ell)(t + \ell).$$

In view of the fact that the integers t and ℓ are relatively prime and of different parity, we conclude that $t - \ell$ and $t + \ell$ must be relatively prime and both odd; thus, (5) implies

(6) $$t - \ell = a_1y_1^k, \quad t + \ell = a_2y_2^k$$

with y_1, y_2 both odd and $(y_1, y_2) = 1 = (a_1, a_2)$ and $a_1a_2 = a$.

Equations (6) yield

$$t = \frac{a_1y_1^k + a_2y_2^k}{2}, \quad \ell = \frac{a_2y_2^k - a_1y_1^k}{2}$$

and by substituting in the third equation of (4), we obtain

$$2z^n = a_1^2y_1^{2k} + a_2^2y_2^{2k}.$$

By the hypothesis of the Theorem, n is even, $n = 2\beta$, and so we obtain

$$2z^{2\beta} = a_1^2y_1^{2k} + a_2^2y_2^{2k}. \tag{7}$$

According to the general solution of the diophantine equation

$$2Z^2 = X^2 + Y^2 \text{ with } (X, Y) = 1$$

(refer to [2] and also to the Remark at the end of the proof for comment on this equation), (7) implies

$$z^\beta = r^2 + s^2, \quad a_1y_1^k = r^2 + 2rs - s^2, \quad a_2y_2^k = -r^2 + 2rs + s^2 \tag{8}$$

with $(r, s) = 1$ (and, in fact, r and s are of different parity).

According to the hypothesis of the Theorem, $a = a_1a_2$ is divisible by a prime $p \equiv \pm 3 \pmod 8$. Thus, a_1 or a_2 is divisible by p, say a_1. Then the second equation in (8) gives $r^2 + 2rs - s^2 \equiv 0 \pmod p$; $(r + s)^2 - 2s^2 \equiv 0$; and so

$$(r + s)^2 \equiv 2s^2 \pmod p. \tag{9}$$

But s and $r + s$ are relatively prime, since r and s are; thus, neither of them is divisible by p [by (9)] and so congruence (9) shows that 2 is a quadratic residue modulo p, which is impossible according to the quadratic reciprocity law and since $p \equiv \pm 3 \pmod 8$ [recall that $p \equiv \pm 1 \pmod 8$ iff 2 is a quadratic residue mod p]. The argument is identical when a_2 is divisible by p; the congruence that yields the contradiction is

$$(r + s)^2 \equiv 2r^2 \pmod p.$$

Remark: Given two positive integers a and b which are relatively prime, it can be shown through elementary means that every solution (with X, Y, and Z relatively prime) (X, Y, Z) in $\mathbb{Z}$, to the diophantine equation

$$(a^2 + b^2)Z^2 = X^2 + Y^2,$$

must satisfy

$$X = \frac{-am^2 + 2bmn + an^2}{D}, \quad Y = \frac{bm^2 + 2amn - bn^2}{D}, \quad Z = \frac{m^2 + n^2}{D},$$

where D is the greatest common divisor of the three numerators and where the integers m and n are relatively prime. In the case of the equation

$$2Z^2 = X^2 + Y^2$$

we have, of course, $a = b = 1$; so the parametric solution takes the form

$$X = -m^2 + 2mn + n^2, \quad Y = m^2 + 2mn - n^2, \quad Z = m^2 + n^2$$

with $(X, Y) = 1$, $(m, n) = 1$, and m, n of different parity. If we set $a = b = 1$ in the above formulas and require $(X, Y) = 1$, then it is not hard to see that $D = 1$ or 2 according to whether m and n are of different parity or both odd with $(m, n) = 1$; but the case $D = 2$ reduces to $D = 1$ when m and n are both odd. To see this, we may set $m = m' - n'$ and $n = m' + n'$ with $(m', n') = 1$ and m', n' of different parity. By solving the above formulas for m' and n' in terms of m and n, substituting for $a = b = 1$ and $D = 2$ in the above formulas, we do see indeed that the case $(m, n) = 1$ and $m + n \equiv 0 \pmod 2$ reduces to that of $(m, n) = 1$ and $m + n \equiv 1 \pmod 2$ (and so $D = 1$).

These elementary derivations of parametric solutions make essential use of the fact that the equation $(a^2 + b^2)Z^2 = X^2 + Y^2$ is homogeneous. For further reading, you may refer to [1].

Corollary 1: If a satisfies the hypothesis of Theorem 1, there is no primitive Pythagoran triangle (primitive means that any two sides are relatively prime) whose odd perpendicular side is divisible by a and whose hypotenuse is an integer square.

Proof: Suppose, to the contrary, that there is such a primitive Pythagorean triple, say (x_1, y_1, z_1), so that $x_1^2 + y_1^2 = z_1^2$, $(x_1, y_1) = 1$, y_1 odd. Then we must, accordingly, have $y_1 = ay$ and $z_1 = z^2$, where y and z are positive integers. Substituting into the above equation, we obtain $x_1^2 + a^2y^2 = z^4$; since y_1 is odd, so must be y in view of $y_1 = ay$. But $(x_1, y_1) = (x_1, ay) = 1$, which, together with the last equation, violate Theorem 1 for $n = m = 2$. Thus, a contradiction.

Comment: It is not very difficult to show that, given any positive integer ρ, there is an infinitude of Pythagorean triangles with a perpendicular side being a ρ^{th} integer power; or with the hypotenuse a ρ^{th} integer power. A construction of such families of Pythagorean triangles can be done elementarily and explicitly. Specifically, if a and b are odd positive integers which are relatively prime, define the positive integers

$$M = \frac{a^\rho + b^\rho}{2} \quad \text{and} \quad N = \frac{a^\rho - b^\rho}{2}; \quad a > b.$$

Then the triple $(M^2 - N^2, 2MN, M^2 + N^2)$ is a primitive Pythagorean triple such that $M^2 - N^2$ is the ρ^{th} power of an integer. That the triple is Pythagorean is well known and established by a straightforward computation. To show that it is primitive, it is enough to observe that, in view of the fact that a and b are both odd (and so are a^ρ and b^ρ), M and N must have different parity (to see this, consider $a^\rho + b^\rho$ and $a^\rho - b^\rho$ modulo 4). If p is a prime divisor of M and N one easily shows that p must divide both a^ρ and b^ρ, an impossibility in view of $(a, b) = 1$. This establishes that $(M, N) = 1$. Finally, a computation shows $M^2 - N^2 = a^\rho b^\rho = (ab)^\rho$.

To construct a primitive Pythagorean triangle whose even side is the ρ^{th} power of an integer, it would suffice to take $M = a^\rho$ and $N = 2^{\rho-1}\cdot b^\rho$ (or vice versa), with $(a, b) = 1$, a and b positive integers and a odd. Here we assume $\rho \geq 2$ (for $\rho = 1$ the problem is trivial, in which case one must assume b to be even). By inspection, we have $(M, N) = 1$. And $2MN = 2a^\rho \cdot 2^{\rho-1}b^\rho = (2ab)^\rho$; the triangle $(M^2 - N^2, 2MN, M^2 + N^2)$ is a primitive one whose even side is a ρ^{th} integer power.

Now, let us discuss the construction of a primitive Pythagorean triangle whose hypotenuse is the ρ^{th} power of an integer. In the special case $\rho = 2^n$, the following procedure can be applied. We form the sequence

$$(x_0, y_0, z_0), \ldots, (x_n, y_n, z_n)$$

by first defining

$$x_0 = M_0^2 - N_0^2, \quad y_0 = 2M_0N_0, \quad z_0 = M_0^2 + N_0^2,$$

where M_0 and N_0 are given positive integers, relatively prime, of different parity, and $M_0 > N_0$. Then recursively define

$$M_i = M_{i-1}^2 - N_{i-1}^2 \quad \text{and} \quad N_i = 2M_{i-1}N_{i-1}, \text{ for } i = 1, \ldots, n.$$

It can easily be shown by induction that $(M_i, N_i) = 1$ and that (x_i, y_i, z_i) is a Pythagorean triple, where

$$x_i = M_i^2 - N_i^2, \quad y_i = 2M_iN_i, \quad z_i = M_i^2 + N_i^2.$$

It is also easily shown that $z_i = z_{i-1}^2$, which eventually leads to $z_n = z_0^{2n}$. The Pythagorean triple (x_n, y_n, z_n) would then be a primitive one, with z_n the ρ^{th}

power of an integer $\rho = 2^n$. More generally, if $\rho \geq 2$ is any integer, a primitive Pythagorean triangle can be constructed such that the hypotenuse is the ρ^{th} power of a prime $p \equiv 1 \pmod 4$.

Specifically, if p is any prime such that $p = 1 \pmod 4$, then $p = a^2 + b^2$, where the relatively prime integers a and b are uniquely determined.

We have

$$p^2 = p \cdot p = (a^2 + b^2)(a^2 + b^2) = (a^2 - b^2)^2 + (2ab)^2;$$

one can easily check that $a^2 - b^2$ and $2ab$ must be relatively prime. Now, suppose that $p^{\rho-1} = M^2 + N^2$, $\rho \geq 3$, for some positive integers M and N such that $(M, N) = 1$.

We have

$$\begin{aligned} p^{\rho} = p^{\rho-1} \cdot p = (M^2 + N^2)(a^2 + b^2) &= (Mb - Na)^2 + (Ma + Nb)^2 \\ &= (Mb + Na)^2 + (Ma - Nb)^2. \end{aligned}$$

We claim that

$$(Mb - Na, Ma + Nb) = 1 \quad \text{or} \quad (Mb + Na, Ma - Nb) = 1.$$

For, otherwise, there would be a prime q dividing $Mb - Na$ and $Ma + Nb$ and a prime r dividing $Mb + Na$ and $Ma + Nb$. But then, according to the above equation, both q and r would divide p^{ρ}; hence, $q = r = p$. But this would imply that p must divide $2Mb$, $2Na$, $2Ma$, and $2Nb$; consequently, p must divide (since p is odd) Mb, Na, Ma, and Nb; however, this is impossible by virtue of $(M, N) = (a, b) = 1$. Thus, we have shown that, for given $\rho \geq 2$ and prime $p \equiv 1 \pmod 4$, there exist integers M, N, $(M, N) = 1$ such that $p^{\rho} = M^2 + N^2$. Then the desired Pythagorean triple is $(M^2 - N^2, 2MN, p^{\rho})$.

Corollary 2: If in a primitive Pythagorean triangle the hypotenuse is an integer square, then each prime factor p of its odd perpendicular side must be congruent to ± 1 modulo 8.

Proof: The result is an immediate consequence of Corollary 1. Indeed, if it were otherwise, that is, if the odd perpendicular side y had a prime factor $p = \pm 3 \pmod 8$, then by setting $y = py_1$, we would obtain

$$x^2 + p^2 \cdot y_1^2 = z^2, \text{ with } (x, py_1) = 1.$$

But $z = R^2$ by hypothesis, and so the last equation produces

$$x^2 + p^2 y_1^2 = R^4,$$

which is contrary to Corollary 1 with $a = p$.

Theorem 2: Let m be a (positive) even integer, $m = 2k$, with k odd, $k \geq 3$, and n even. Also, let a be an odd positive integer that contains a prime divisor $p \equiv \pm 3 \pmod 8$, and assume that b is a non-k^{th} residue modulo q, while 2 is a k^{th} residue of q, where q is some prime divisor of a; b some positive integer relatively prime to a. Moreover, assume that each divisor ρ of a/q^e, where q^e is the highest power of q dividing a, is a k^{th} residue modulo q. Then the diophantine equation

$$b^2x^m + a^2y^m = z^{2n}; \; (bx^k)^2 + (ay^k)^2 = (z^n)^2$$

has no solution in positive integers x, y, z with $(bx, ay) = 1$.

Proof: By Theorem 1, there is nothing to prove when y is odd. If, on the other hand, y is even and x odd, with $(bx, ay) = 1$ and $b^2x^m + a^2y^m = z^{2n}$, we see that bx^k, ay^k, and z^n form a primitive Pythagorean triple, where $k = m/2$. In that case, of course, bx is odd and ay is even, and so we must have

(10) $\quad bx^k = M^2 - N^2, \quad ay^k = 2MN, \quad z^n = M^2 + N^2$

with $(M, N) = 1$ and M, N being positive integers of different parity.

Let q be the prime divisor of a, as stated in the hypothesis. The second equation of (10) shows that q must divide M or N. Certainly the above coprimeness conditions show that q does not divide bx. On the other hand, by virtue of the fact that k is odd, we have $(-1)^k = -1$. First, suppose $M \equiv 0 \pmod{q}$. Then, if q^e is the highest power of q dividing a, then since $(M, N) = 1$, the second equation in (1) shows that q^e divides M; and

$$N = N_1^k \rho 2^f,$$

where ρ is a divisor of a/q^e and the exponent f equals 0 or $k - 1$, depending on whether N is odd or even, respectively. Thus,

$$N^2 = N_1^{2k} \rho^2 \cdot 2^{2f};$$

but ρ is a k^{th} residue of q by hypothesis; hence, so is ρ^2. Also 2^{k-1} is a k^{th} residue of q, since 2 is (by hypothesis) and $2 \cdot 2^{k-1} = 2^k$. Consequently, N^2 is a k^{th} residue and since $(-1)^k = -1$, the first equation in (10) clearly implies that b is also a k^{th} residue of q, contrary to the hypothesis.

A similar argument settles the case $N \equiv 0 \pmod{q}$.

Example: Take $k = 3$, and so $m = 6$, $p = 29$, $q = 31$, $e = 1$, and $a = p \cdot q = 899$; then $p \equiv 5 \pmod{8}$ and the cubic residues of 31 are ±1, ±2, ±4, ±8, and ±15; $p = 29$ is a cubic residue of q. Thus, if $b \not\equiv \pm1, \pm2, \pm4, \pm15 \pmod{31}$, the diophantine equation $(bx^3)^2 + (899y^3)^2 = z^4$ has no solution over the set of positive integers.

Corollary 3 (to Th. 2): Let a, b, and k be positive integers satisfying the hypothesis of Theorem 2. Then, there is no primitive Pythagorean triangle with one perpendicular side equal to a times a k^{th} integer power, the other b times a k^{th} power, and the hypotenuse a perfect square.

Proof: Apply Theorem 2 with $m = n = 2$. We omit the details.

References

1. L. J. Mordell. *Diophantine Euqations*. London: Academic Press, 1969.
2. L. E. Dickson. *History of the Theory of Numbers*, Vol. II. New York: Chelsea, 1952.
3. K. Spyropoulos. "On a Property of Pythagorean Triangles and Its Application to Two Diophantine Equations." *Congressus Numerantium* 57 (March 1987):281-88.
4. W. Sierpinski. *Elementary Theory of Numbers*. Warsaw, 1964.

AMS Classification number: 11NT (number theory)

*****

ON THE (2, F) GENERALIZATIONS OF THE FIBONACCI SEQUENCE

W. R. Spickerman, R. N. Joyner, and R. L. Creech
East Carolina University, Greenville, NC 27858
(December 1990)

A generalization of the Fibonacci sequence to vectors was defined in Atanassov, Atanassova, & Sasselov [1]. In a later article, Atanassov [2] defined the four distinct (2, F) generalizations of the Fibonacci sequence and determined a solution for one of the cases in terms of the greatest integer function. Subsequently Lee & Lee [3] published solutions for all four (2, F) generalizations using the function $f(n) = t_j$, where $j = n \bmod(k) + 1$ and t_j is the j^{th} element of an ordered k-tuple $[t_1, t_2, \ldots, t_k]$. The purpose of this paper is to present a solution to each of the four (2, F) generalizations of the Fibonacci sequence as

(1) A linear combination of two second-order recursive sequences, and
(2) a polynomial in α and β and sometimes ω and $\overline{\omega}$, where $\alpha = (1 + \sqrt{5})/2$, $\beta = (1 - \sqrt{5})/2$, and ω and $\overline{\omega}$ are the usual complex cube roots of 1.

In order to find a solution to the four (2, F) generalizations of the Fibonacci sequence, the following lemma is used.

Lemma: Let $p(x) = 1 \mp x \mp x^2$. The four recursive sequences defined by the four possible generating functions $1/p(x)$ have the properties given in Table 1 below, where ω and $\overline{\omega}$ are the complex cube roots of unity and $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$.

Table 1

Generating Function	General Term	Generated Series	Recursion Relation
$\dfrac{1}{1 - x - x^2}$	$F_n = \dfrac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}$	$\sum_{n=0}^{\infty} F_n x^n$	$F_{n+2} = F_{n+1} + F_n$
$\dfrac{1}{1 + x + x^2}$	$T_n = \dfrac{\omega^{n+1} - \overline{\omega}^{n+1}}{\omega - \overline{\omega}}$	$\sum_{n=0}^{\infty} T_n x^n$	$-T_{n+2} = T_{n+1} + T_n$
$\dfrac{1}{1 - x + x^2}$	$S_n = (-1)^n \dfrac{\omega^{n+1} - \overline{\omega}^{n+1}}{\omega - \overline{\omega}}$	$\sum_{n=0}^{\infty} S_n x^n$	$S_{n+2} = S_{n+1} - S_n$
$\dfrac{1}{1 + x - x^2}$	$G_n = (-1)^n \dfrac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}$	$\sum_{n=0}^{\infty} G_n x^n$	$G_{n+2} = -G_{n+1} + G_n$

The proof of the lemma is not shown; however, the lemma can be proved by separating the generating functions into fractions with linear denominators and then applying the binomial theorem for negative exponents. Note that, in the table,

$$F_0 = 1,\ F_1 = 1, \text{ and } F_{n+2} = F_{n+1} + F_n \text{ for } n = 2, 3, 4, \ldots .$$

From the table, it is immediate that

$$G_n = (-1)^n F_n \quad \text{and} \quad S_n = (-1)^n T_n.$$

It is also true that all four sequences may be extended to negative indices.

Theorem: Let $P_n^1 = (X_n, Y_n)$ and $P_n^2 = (Y_n, X_n)$. Then the difference equation

$$P_{n+2}^1 = P_{n+1}^j + P_n^k,\ n \geq 0; \text{ for } j,\ k \in \{1,\ 2\}$$

with the initial conditions $P_0^1 = (a, c)$, $P_1^1 = (b, d)$, where a, b, c, and d are arbitrary real numbers, defines the four distinct (2, F) generalizations of the Fibonacci sequence.

Proof of the Theorem: The four distinct cases are considered separately.

Case 1: Let $j = 1$ and $k = 1$. The system is

$$X_{n+2} = X_{n+1} + X_n, \quad n \geq 0,$$
$$Y_{n+2} = Y_{n+1} + Y_n, \quad n \geq 0, \text{ with}$$
$$P_0^1 = (a, c) \text{ and } P_1^1 = (b, d).$$

Here, the system is separable into two independent difference equations with each equation defining a generalized Fibonacci sequence. The required solution is

$$X_n = aF_{n-2} + bF_{n-1} \quad \text{and} \quad Y_n = cF_{n-2} + dF_{n-1} \quad \text{for } n \geq 0.$$

Binet's formulas are

$$X_n = a\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} + b\frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad Y_n = c\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} + d\frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Case 2: Let $j = 1$ and $k = 2$. The system is

$$X_{n+2} = X_{n+1} + Y_n, \quad n \geq 0,$$
$$Y_{n+2} = Y_{n+1} + X_n, \quad n \geq 0, \text{ with}$$
$$P_0^1 = (a, c) \text{ and } P_1^1 = (b, d).$$

Assuming a solution of the form

$$X = f(x) = \sum_{i=0}^{\infty} X_i x^i, \quad Y = g(x) = \sum_{i=0}^{\infty} Y_i x^i,$$

and substituting into the above system yields the system

$$(1 - x)f(x) - x^2 g(x) = a + (b - a)x$$
$$-x^2 f(x) + (1 - x)g(x) = c + (d - c)x$$

defining $f(x)$ and $g(x)$. Solving this system and applying partial fractions results in the following generating functions for $f(x)$ and $g(x)$:

$$f(x) = \frac{1}{2}\left[\frac{(a + c) + (-a - c + b + d)x}{1 - x - x^2} + \frac{(a - c) + (-a + c + b - d)x}{1 - x + x^2}\right],$$

$$g(x) = \frac{1}{2}\left[\frac{(a + c) + (-a - c + b + d)x}{1 - x - x^2} + \frac{(-a + c) + (a - c - b + d)x}{1 - x + x^2}\right].$$

Applying the lemma and collecting terms, the equations are

$$f(x) = \frac{1}{2}\sum_{i=0}^{\infty}[(a + c)F_{i-2} + (-a + c)S_{i-2} + (b + d)F_{i-1} + (b - d)S_{i-1}]x^i$$

and

$$g(x) = \frac{1}{2}\sum_{i=0}^{\infty}[(a + c)F_{i-2} + (a - c)S_{i-2} + (b + d)F_{i-1} + (-b + d)S_{i-1}]x^i.$$

Consequently,

$$X_n = \frac{1}{2}[(a + c)F_{n-2} + (-a + c)S_{n-2} + (b + d)F_{n-1} + (b - d)S_{n-1}],$$

$$Y_n = \frac{1}{2}[(a + c)F_{n-2} + (a - c)S_{n-2} + (b + d)F_{n-1} + (-b + d)S_{n-1}].$$

Substituting

$$F_n = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} \quad \text{and} \quad S_n = (-1)^n \frac{\omega^{n+1} - \overline{\omega}^{n+1}}{\omega - \overline{\omega}}$$

from the Lemma yields the analogs of Binet's formulas:

$$X_n = \frac{1}{2}\left[(a + c)\left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right) + (b + d)\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)\right.$$
$$\left. + (-a + c)(-1)^{n-2}\left(\frac{\omega^{n-1} - \overline{\omega}^{n-1}}{\omega - \overline{\omega}}\right) + (b - d)(-1)^{n-1}\left(\frac{\omega^n - \overline{\omega}^n}{\omega - \overline{\omega}}\right)\right]$$

and

$$Y_n = \frac{1}{2}\left[(a + c)\left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right) + (b + d)\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)\right.$$
$$\left. + (a - c)(-1)^{n-2}\left(\frac{\omega^{n-1} - \overline{\omega}^{n-1}}{\omega - \overline{\omega}}\right) + (-b + d)(-1)^{n-1}\left(\frac{\omega^n - \overline{\omega}^n}{\omega - \overline{\omega}}\right)\right].$$

Case 3: For $j = 2$ and $k = 1$, the system is

$$X_{n+2} = Y_{n+1} + X_n, \quad n \geq 0,$$
$$Y_{n+2} = X_{n+1} + Y_n, \quad n \geq 0, \text{ with}$$
$$P_0^1 = (a, c) \text{ and } P_1^1 = (b, d).$$

Assuming a solution of the form

$$X = f(x) = \sum_{i=0}^{\infty} X_i x^i, \qquad Y = g(x) = \sum_{i=0}^{\infty} Y_i x^i,$$

substituting into the system, solving for $f(x)$ and $g(x)$ and then applying partial fractions gives the generating functions in the following forms:

$$f(x) = \frac{1}{2}\left[\frac{(a + c) + (-a - c + b + d)x}{1 - x - x^2} + \frac{(a - c) + (a - c + b - d)x}{1 + x - x^2}\right],$$

$$g(x) = \frac{1}{2}\left[\frac{(a + c) + (-a - c + b + d)x}{1 - x - x^2} + \frac{(-a + c) + (-a + c - b + d)x}{1 + x - x^2}\right].$$

Applying the Lemma, collecting terms, and using the recursion relations from the Lemma yields the following forms for the generating functions:

$$f(x) = \frac{1}{2}\sum_{i=0}^{\infty}[(a + c)F_{i-2} + (a - c)G_{i-2} + (b + d)F_{i-1} + (b - d)G_{i-1}]x^i,$$

$$g(x) = \frac{1}{2}\sum_{i=0}^{\infty}[(a + c)F_{i-2} + (c - a)G_{i-2} + (b + d)F_{i-1} + (d - b)G_{i-1}]x^i.$$

Consequently,

$$X_n = \frac{1}{2}[(a + c)F_{n-2} + (a - c)G_{n-2} + (b + d)F_{n-1} + (b - d)G_{n-1}]$$

and

$$Y_n = \frac{1}{2}[(a + c)F_{n-2} + (c - a)G_{n-2} + (b + d)F_{n-1} + (d - b)G_{n-1}].$$

Substituting for F_n and G_n in terms of α and β gives the following analogs of Binet's formulas:

$$X_n = \frac{1}{2}\left[(a + c)\left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right) + (a - c)(-1)^n\left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right)\right.$$
$$\left. + (b + d)\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right) + (b - d)(-1)^{n-1}\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)\right],$$

and

$$Y_n = \frac{1}{2}\left[(a + c)\left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right) + (a - c)(-1)^{n-1}\left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right)\right.$$
$$\left. + (b + d)\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right) + (b - d)(-1)^n\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)\right].$$

Note that $G_i = (-1)^i F_i$. Collecting terms in a, b, c, and d gives

$$X_n = \frac{1}{2}[aF_{n-2}[1 + (-1)^n] + cF_{n-2}[1 - (-1)^n]$$
$$+ bF_{n-1}[1 + (-1)^{n-1}] + dF_{n-1}[1 - (-1)^{n-1}]]$$

and a similar form for Y_n.

Case 4: For $j = 2$ and $k = 2$, the system is

$$X_{n+2} = Y_{n+1} + Y_n, \quad n \geq 0,$$
$$Y_{n+2} = X_{n+1} + X_n, \quad n \geq 0, \text{ with}$$
$$P_0^1 = (a, c) \text{ and } P_1^1 = (b, d).$$

Again, assuming a solution of the form

$$X = f(x) = \sum_{i=0}^{\infty} X_i x^i, \qquad Y = g(x) = \sum_{i=0}^{\infty} Y_i x^i,$$

substituting into the system, solving for $f(x)$ and $g(x)$, and using partial fractions gives the following forms of the generating functions:

$$f(x) = \frac{1}{2}\left[\frac{(a + c) + (-a - c + b + d)x}{1 - x - x^2} + \frac{(a - c) + (a - c + b - d)x}{1 + x + x^2}\right],$$

$$g(x) = \frac{1}{2}\left[\frac{(a + c) + (-a - c + b + d)x}{1 - x - x^2} + \frac{(-a + c) + (-a + c - b + d)x}{1 + x + x^2}\right].$$

Applying the series from the Lemma, collecting terms, and using the recursion relations from the Lemma to combine terms gives

$$f(x) = \frac{1}{2}\sum_{i=0}^{\infty}[(a + c)F_{i-2} + (-a + c)T_{i-2} + (b + d)F_{i-1} + (b - d)T_{i-1}]x^i,$$

$$g(x) = \frac{1}{2}\sum_{i=0}^{\infty}[(a + c)F_{i-2} + (a - c)T_{i-2} + (b + d)F_{i-1} + (-b + d)T_{i-1}]x^i.$$

Thus,

$$X_n = \frac{1}{2}[(a + c)F_{n-2} + (-a + c)T_{n-2} + (b + d)F_{n-1} + (b - d)T_{n-1}]$$

and

$$Y_n = \frac{1}{2}[(a + c)F_{n-2} + (a - c)T_{n-2} + (b + d)F_{n-1} + (-b + d)T_{n-1}].$$

Substituting for F_n and T_n in terms of α, β, ω, and $\overline{\omega}$ gives the analogs of Binet's formulas:

$$X_n = \frac{1}{2}\left[(a + c)\left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right) + (-a + c)\left(\frac{\omega^{n-1} - \overline{\omega}^{n-1}}{\omega - \overline{\omega}}\right)\right.$$
$$\left. + (b + d)\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right) + (b - d)\left(\frac{\omega^n - \overline{\omega}^n}{\omega - \overline{\omega}}\right)\right]$$

and

$$Y_n = \frac{1}{2}\left[(a + c)\left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right) + (a - c)\left(\frac{\omega^{n-1} - \overline{\omega}^{n-1}}{\omega - \overline{\omega}}\right)\right.$$
$$\left. + (b + d)\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right) + (-b + d)\left(\frac{\omega^n - \overline{\omega}^n}{\omega - \overline{\omega}}\right)\right].$$

In this paper we have expressed the solutions to the (2, F) generalizations of the Fibonacci sequence as a linear combination of the terms of two recursive sequences of order 2. Since the coefficients of the terms of the recursive sequences are linear functions of the initial terms of the (2, F) sequences, it is possible to rearrange the solutions into the form of a linear combination of the initial terms, where coefficients are functions of the terms of the second-order sequences involved.

References

1. K. T. Atanassov, L. C. Atanassova, & D. D. Sasselov. "A New Perspective to the Generalization of the Fibonacci Sequence." *Fibonacci Quarterly 23.1* (1985):21-28.
2. K. T. Atanassov. "On a Second New Generalization of the Fibonacci Sequence." *Fibonacci Quarterly 24.4* (1986):362-65.
3. J. Lee & J. Lee. "Some Properties of the Generalization of the Fibonacci Sequence." *Fibonacci Quarterly 25.2* (1987):111-17.

AMS Classification numbers: 40, 11

*****

A Short History on Edouard Lucas

In "Pascals's Triangle and the Tower of Hanoi" by Andreas M. Hinz, The American Mathematical Monthly, Vol 99.6 (1992) pages 538-544, one can find a very short but well written history on Edouard Lucas. It is certainly worth reading.

Gerald E. Bergum, Editor

FIBONACCI NUMBERS AND THE NUMBERS OF PERFECT MATCHINGS OF SQUARE, PENTAGONAL, AND HEXAGONAL CHAINS*

Ratko Tošić
Institute of Mathematics, University of Novi Sad, Novi Sad, Yugoslavia

Ivan Stojmenović
Computer Science Department, University of Ottawa, Ottawa, Canada
(Submitted December 1990)

1. Some Preliminaries

Let G be a finite graph. A *perfect matching* in G is a selection of edges in G such that each vertex of G belongs to exactly one selected edge. Therefore, if the number of vertices in G is odd, then there is no perfect matching. We denote by $K(G)$ the number of perfect matchings of G, and refer to it as the *K number* of G.

By a polygonal *chain* $P_{k,s}$ we mean a finite graph obtained by concatenating s k-gons in such a way that any two adjacent k-gons (cells) have exactly one edge in common, and each cell is adjacent to exactly two other cells, except the first and last cells (end cells) which are adjacent to exactly one other cell each. It is clear that different polygonal chains will result, according to the manner in which the cells are concatenated.

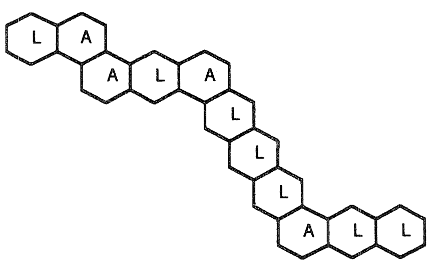


Figure 1

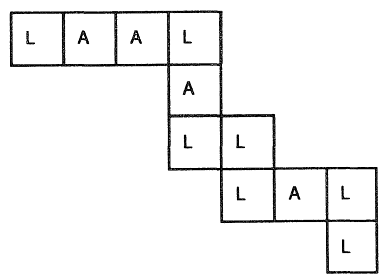


Figure 2

Figure 1 shows a hexagonal chain $P_{6,11}$. The *LA-sequence* of a hexagonal chain is defined in [11] as follows. A hexagonal chain $P_{6,s}$ is represented by a word of the length s over the alphabet $\{A, L\}$. The i^{th} letter is A (and the corresponding hexagon is called a *kink*) iff $1 < i < s$ and the i^{th} hexagon has an edge that does not share a common vertex with any of two neighbors. Otherwise, the i^{th} letter is L. For instance, the hexagonal chain in Figure 1 is represented by a word $LAALALLLALL$, or, in abbreviated form $LA^2LAL^3AL^2$. The LA-sequence of a hexagonal chain may always be written in the form

$$P_6\langle x_1, \ldots, x_n\rangle = L^{x_1}AL^{x_2}A \ldots AL^{x_n},$$

where $x_1 \ge 1$, $x_n \ge 1$, $x_i \ge 0$, for $i = 2, 3, \ldots, n - 1$. For instance, the LA-sequence of the hexagonal chain in Figure 1 may be written in the form

$$P_6\langle 1, 0, 1, 3, 2\rangle = LAL^0ALAL^3AL^2.$$

It is well known that the number of a hexagonal chain is entirely determined by its LA-sequence, no matter which way the kinks go ([1], [10], [12]). In [1]

*Work partially supported by the NSERC of Canada.

the term "isoarithmicity" for this phenomenon is coined. Thus,

$$P_6\langle x_1,\ x\ ,\ \ldots,\ x_n\rangle$$

represents a class of isoarithmic hexagonal chains.

Figure 2 above shows a square chain $P_{4,11}$. We introduce a representation of square chains in order to establish a mapping between square and hexagonal chains that will enable us to obtain the K numbers for square chains. A square chain $P_{4,s}$ is represented by a word of the length s over the alphabet $\{A, L\}$, also called its *LA-sequence*. The i^{th} letter is A iff each vertex of the i^{th} square also belongs to an adjacent square. Otherwise, the i^{th} letter is L. For instance, the square chain in Figure 2 above is represented by the word $LAALALLLALL$, or, in abbreviated form $LA^2LAL^3AL^2$. Clearly, the LA-sequence of a square chain may always be written in the form

$$P_4\langle x_1,\ \ldots,\ x_n\rangle = L^{x_1}AL^{x_2}A\ \ldots\ AL^{x_n},$$

where $x_1 \geq 1$, $x_n \geq 1$, $x_i \geq 0$, for $i = 2, 3, \ldots, n - 1$. For example, the LA-sequence of the square chain in Figure 2 may be written in the form

$$P_4\langle 1,\ 0,\ 1,\ 3,\ 2\rangle = LAL^0ALAL^3AL^2.$$

We show below that all square chains of the form

$$P_4\langle x_1,\ \ldots,\ x_n\rangle$$

are isoarithmic.

We will draw pentagonal chains so that each pentagon has two vertical edges and a horizontal one which is adjacent to both vertical edges. The common edge of any two adjacent pentagons is drawn vertical. We shall call such a way of drawing a pentagonal chain the *horizontal representation* of that pentagonal chain. From the horizontal representation of a pentagonal chain one can see that it is composed of a certain number (≥ 1) of segments; namely, two adjacent pentagons belong to the same segment iff their horizontal edges are adjacent. We denote by

$$P_5\langle x_1,\ x_2,\ \ldots,\ x_n\rangle$$

the pentagonal chain consisting of n segments of lengths $x_1, x_2, \ldots, x_n$, where the segments are taken from left to right. Figure 4a below shows

$$P_5\langle 3,\ 2,\ 4,\ 8,\ 5\rangle.$$

Notice that one can assume that $x_1 > 1$ and $x_n > 1$.

Among all polygonal chains, the hexagonal chains were studied the most extensively, since they are of great importance in chemistry, namely, benzenoid hydrocarbon chains. Each perfect matching of a hexagonal chain corresponds to a Kekulé structure of the corresponding benzenoid hydrocarbon. The stability and other properties of these hydrocarbons have been found to correlate with their K numbers. The classical paper [10] contains a general algorithm for the enumeration of Kekulé structures (K numbers) of benzenoid chains and branched catacondensed benzenoids. The algorithm is modified in [6]. An alternative derivation for the case of unbranched chains is described in [4]. In [17] Tošić proposed an algorithm of time complexity $O(n)$ for calculating the number of Kekulé structures of an arbitrary benzenoid chain composed from n linearly condensed segments. The explicit formulas, in terms of the Fibonacci numbers, for the number of Kekulé structures for a zigzag chain were given in [20], [3], and [5]. We will re-derive the formula for K numbers of zigzag chains as a special case of a new general formula. A treatise on three connections between Fibonacci numbers and Kekulé structures is presented in [2] and [15]. A procedure for producing algebraic formulas for the K number of an arbitrary catacondensed benzenoid is elaborated in [1]. Two different explicit formulas for the K number of an arbitrary benzenoid chain are given in [18] and [19]. A whole recent book [7] is devoted to Kekulé structures in benzenoid hydrocarbons. It contains a list of other references on the problem of finding the "Kekulé structure count" for hydrocarbons.

In [14] Gutman & Cyvin investigated the connection between the square and hexagonal chains, and derived the number of a graph $Q_{p,q}$, which is a chain composed of $p+q+1$ squares, and, in our notation, is denoted by

$$LA^{p-1}LA^{q-1}L\colon\ K(Q_{p,q}) = F_{p+q+2} + F_{p+1}F_{q+1}.$$

In the present paper, we investigate the K number of an arbitrary square chain; the above formula will follow as a special case of a general result.

In [8] and [9] Farrell investigated the K numbers of pentagonal chains of particular forms. The obtained results are special cases of a general formula which will be deduced here.

2. K Numbers of Hexagonal Chains

Recently Tošić and Bodroza [18] proved a recurrence relation and a formula for the K numbers of hexagonal chains using a notation that counts every kink twice. Motivated by the possibility of mapping square and pentagonal chains to hexagonal ones, here we use a different notation that leads to a new recurrence relation and formula. The proofs are omitted because they can be obtained along the same lines as the proofs of Theorems 1 and 2 from [18].

The K formula for a single linear chain (polyacene) of x_1 hexagons, i.e., $P_6\langle x_1\rangle$ is deduced in [10] and [7]. We define $P_6\langle\ \rangle$ as the hexagonal chain with "no hexagons."

Theorem 1: $K(P_6\langle\ \rangle) = 1$, $K(P_6\langle x_1\rangle) = 1 + x_1$,

$$K(P_6\langle x_1, \ldots, x_{n-1}, x_n\rangle) = (x_n + 1)K(P_6\langle x_1, \ldots, x_{n-1}\rangle) + K(P_6\langle x_1, \ldots, x_{n-2}\rangle) \text{ for } n \ge 2.$$

Theorem 2: $K(P_6\langle x_1, \ldots, x_{n-1}, x_n\rangle) =$

$$F_{n+1} + \sum_{0<i_1<\cdots<i_k\le n,\ 1\le k\le n} F_{n+1-i_k}F_{i_k-i_{k-1}}\cdots F_{i_2-i_1}F_{i_1}x_{i_1}x_{i_2}\cdots x_{i_k}.$$

3. K Number of a Square Chain

Theorem 3: $K(P_4\langle x_1, \ldots, x_{n-1}, x_n\rangle) = K(P_6\langle x_1, \ldots, x_{n-1}, x_n\rangle)$.

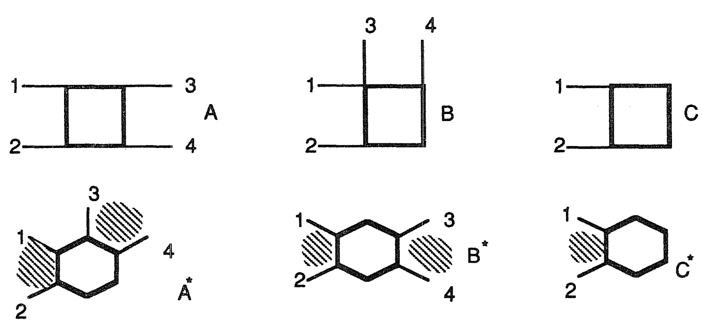


Figure 3

Proof: Referring to Figure 3, it is easy to see that if in a square chain some (or all) structural details of the type A, B, and C are replaced by A*, B*, and C*, respectively, the K number will remain the same. By accomplishing such replacements, each square chain can be transformed into a hexagonal chain with the same LA-sequence. Therefore, a square chain and corresponding hexagonal chain represented by the same LA-sequence have the same K number. For example, the square chain in Figure 2 can be transformed into the hexagonal chain in Figure 1. Note that the corner squares of a square chain correspond to the linear hexagons, and vice versa, in this transformation. □

Thus, the K numbers for square chains are also given by Theorem 2. It is clear that all other properties concerning the K numbers of square chains can be derived from the corresponding results for hexagonal chains and that the investigation of square chains as a separate class from that point of view is of no interest.

Note that the formula

$$K(Q_{p,q}) = F_{p+q+2} + F_{p+1}F_{q+1}$$

of Gutman & Cyvin [14] for the chain $LA^{p-1}LA^{q-1}L$ can be derived from Theorem 2 as a special case. Namely, in the LA-sequence of $Q_{p,q}$, we have

$$n = p + q - 1; \quad x_1 = x_p = x_{p+q-1} = 1; \quad x_i = 0 \text{ for } i \neq 1, p, p+q-1,$$

and

$$\begin{aligned} K(Q_{p,q}) &= F_{p+q} + F_{p+q-1}F_1 + F_qF_p + F_1F_{p+q-1} + F_qF_{p-1}F_1 + F_1F_{p+q-2}F_1 \\ &\qquad + F_1F_{q-1}F_p + F_1F_{q-1}F_{p-1}F_1 \\ &= (F_{p+q} + 2F_{p+q-1} + F_{p+q-2}) + (F_p + F_{p-1})F_q + (F_p + F_{p-1})F_{q-1} \\ &= F_{p+q+2} + F_{p+1}F_q + F_{p+1}F_{q-1} \\ &= F_{p+q+2} + F_{p+1}F_{q+1}. \end{aligned}$$

K Number of a Pentagonal Chain

First, recall a general result concerning matchings of graphs. Let G be a graph and u, x, y, v its distinct vertices, such that ux, xy, yv are edges of G, u and v are not adjacent, and x and y have degree two. Let the graph H be obtained from G by deleting the vertices x and y and by joining u and v. Conversely, G can be considered as obtained from H by inserting two vertices (x and y) into the edge of uv. We say that G can be *reduced* to H, or that G is reducible to H; clearly $K(G) = K(H)$ [13].

Theorem 4: If $x_1 + x_2 + \cdots + x_n$ is odd, then

$$K(P_5\langle x_1, \ldots, x_n\rangle) = 0.$$

Otherwise (i.e., if the sequence $x_1, x_2, \ldots, x_n$ contains an even number of odd integers), let

$$s(j_1),\ s(j_2),\ \ldots,\ s(j_t) \quad (j_1 < j_2 < \cdots < j_t)$$

be the odd numbers in the sequence

$$s(r) = x_1 + \cdots + x_r \quad (r = 1, 2, \ldots, n),$$

and let $s(j_0) = -1$ and $s(j_{t+1}) = s_n + 1$; then

$$K(P_5\langle x_1, \ldots, x_n\rangle)$$

$$= F_{t+2} + \sum_{\substack{0 = i_0 < i_1 < \cdots < i_r \le t+1 \\ 1 \le r \le t+1}} (F_{t+2-i_r})/2^r \prod_{\ell=1}^{r} (s(j_{i_\ell}) - s(j_{i_\ell - 1}) - 2)F_{i_\ell - i_{\ell-1}}.$$

Proof: Clearly a pentagonal chain consisting of p pentagons has $3p+2$ vertices. Hence, a pentagonal chain with an odd number of pentagons has no perfect matching. Therefore, we assume that it has an even number of segments of odd length.

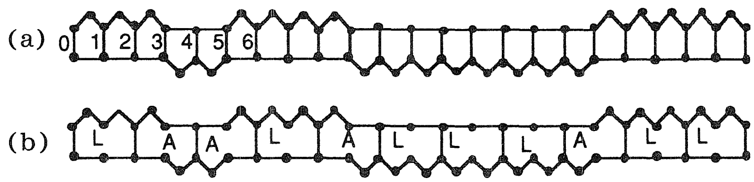


Figure 4

Consider a horizontal representation of $P\langle x_1, x_2, \ldots, x_n\rangle$ (Fig. 4a). Label the vertical edges 0, 1, ..., s_n, from left to right. Clearly no edge labeled by an odd number can be included in any perfect matching of $P_5\langle x_1, x_2, \ldots, x_n\rangle$ since there are an odd number of vertices on each side of such an edge. By removing all edges labeled with odd numbers, we obtain an octagonal chain consisting of $s_n/2$ octagons (Fig. 4b). This octagonal chain can be reduced to a hexagonal chain with $s_n/2$ hexagons (Fig. 1). It is evident that in the process of reduction, each octagon obtained from the two adjacent pentagons of the same segment becomes an L mode hexagon, while each octagon obtained from the two adjacent pentagons of different segments becomes a kink. The number of kinks is t, since each kink corresponds to an odd $s(r)$. It means that this hexagonal chain consists of $t+1$ segments. Let y_i be the number of L mode hexagons in the i^{th} segment. Then

$$y_1 = (s(j_1) - 1)/2 = (s(j_1) - s(j_0) - 2)/2$$

$$y_{t+1} = (s(n) - s(j_t) - 1)/2 = (s(j_{t+1}) - s(j_t) - 2)/2,$$

and, for $2 \le i \le t$,

$$y_i = (s(j_i) - s(j_{i-1}) - 2)/2.$$

Since reducibility preserves K numbers, it follows that

$$K(P_5\langle x_1, x_2, \ldots, x_n\rangle) = K(P_6\langle y_1, y_2, \ldots, y_{t+1}\rangle)$$

$$= F_{t+2} + \sum_{\substack{0=i_0<i_1<\cdots<i_r\le t+1 \\ 1\le r\le t+1}} F_{t+2-i_r} \prod_{\ell=1}^{r} y_{i_\ell} F_{i_\ell - i_{\ell-1}},$$

which gives, by taking into account the values for y_i, the expression in Theorem 4. □

Now we shall consider some special cases of Theorem 4 in order to derive some useful consequences. As a first specialization, we shall take the regular pentagonal chains, defined as follows. If all segments of a pentagonal chain are of the same length $m(x_1 = x_2 = \cdots = x_n = m)$, we say that it is a *regular pentagonal chain* and denote it by $P_5\langle m^n\rangle$ (similar notation will be used for a regular subchain of a chain).

Theorem 5: Let m and n be positive integers, m odd and n even ≥ 6. Then

$$K(P_5\langle m^n\rangle) = (m+1)^2(F_{n/2} + Q_{(n-2)\,2}(m-1))/4 + (m+1)(F_{(n-2)/2} + Q_{(n-4)/2}(m-1)) + F_{(n-4)/2} + Q_{(n-6)/2}(m-1),$$

where

$$Q_n(m) = \sum_{\substack{0=i_0<i_1<\cdots<i_r<i_{r+1}\le n+1 \\ 1\le r\le n}} m^r \prod_{\ell=1}^{r+1} F_{i_\ell - i_{\ell-1}} \quad \text{for } n \ge 1 \text{ and } Q_0(m) = 0.$$

Proof: Let $m = 2k + 1$, $n = 2p$. Then $t = p + 1$ and $y_1 = y_{p+1} = k$, $y_i = 2k$, for $i = 2, 3, \ldots, t$. Hence

$$K(P_5\langle m^n \rangle) = K(P_5\langle k, 2k^{p-1}, k\rangle).$$

Applying Theorem 1 and property $K(P_5\langle x_1, \ldots, x_n\rangle) = K(P_5\langle x_n, \ldots, x_1\rangle)$ we obtain

$$K(P_5\langle k, 2k^{p-1}, k\rangle) = (k + 1)K(P_5\langle 2k^{p-1}, k\rangle) + K(P_5\langle 2k^{p-2}, k\rangle),$$

$$K(P_5\langle 2k^{p-1}, k\rangle) = (k + 1)K(P_5\langle 2k^{p-1}\rangle) + K(P_5\langle 2k^{p-2}\rangle),$$

and

$$K(P_5\langle 2k^{p-2}, k\rangle) = (k + 1)K(P_5\langle 2k^{p-2}\rangle) + K(P_5\langle 2k^{p-3}\rangle).$$

It follows that

$$K(P_5\langle k, 2k^{p-1}, k\rangle) = (k + 1)^2K(P_5\langle 2k^{p-1}\rangle) + 2(k + 1)K(P_5\langle 2k^{p-2}\rangle) + K(P_5\langle 2k^{p-3}\rangle).$$

Thus,

$$K(P_5\langle m^n\rangle) = 1/4(m + 1)^2K(P_5\langle m - 1^{(n-2)/2}\rangle) + (m + 1)K(P_5\langle m - 1^{(n-4)/2}\rangle) + K(P_5\langle m - 1^{(n-6)/2}\rangle).$$

The statement follows by applying Theorem 2. □

We note that all results by Farrell in [9] and other papers concerning the numbers of perfect matchings of pentagonal chains are very special cases of Theorem 5 (which is a special case of Theorem 4).

Corollary 1: $K(P_5\langle 1^{2k}\rangle) = F_{k+2}$.

Proof: Follows as a special case of Theorem 5 when $m = 1$. Then, obviously, $Q_n(1) = 0$ and we have, for $n = 2k$,

$$K(P_5\langle 1^{2k}\rangle) = F_k + 2F_{k-1} + F_{k-2} = F_{k+2}. \quad \square$$

Clearly, in this special case, the process of reduction results in a zigzag hexagonal chain, with the LA-sequence $LA^{k-2}L$. This is in accordance with the previously known result for the number of zigzag hexagonal chains derived in [20], [3], and [5].

Corollary 2: Let $x_1, x_2, \ldots, x_n$ be all even positive integers, $n \geq 1$. Then

$$K(P_5\langle x_1, \ldots, x_n\rangle) = (x_1 + \cdots + x_n)/2 + 1.$$

Proof: Since all partial sums $s(r)$ in Theorem 4 are even, no kink is obtained in the process of reduction to a hexagonal chain. Thus, a linear hexagonal chain consisting of $h = (x_1 + x_2 + \cdots + x_n)/2$ hexagons is obtained (i.e., $P_6\langle h\rangle = L^h$). According to [7], we have $K(P_6\langle h\rangle) = h + 1$; hence,

$$K(P_5\langle x_1, \ldots, x_n\rangle) = h + 1. \quad \square$$

In the special case of Corollary 2, when $n = 1$, we obtain a *uniform* pentagonal chain, i.e., a pentagonal chain consisting of only one segment. Several results concerning the matchings of the uniform pentagonal chains, including the K number, are deduced in [8] by application of matching polynomials, which, in the case when the perfect matchings are in question, is a very involved technique. Here we generalize the result by deriving the formula for the K number of an arbitrary pentagonal chain, using a much simpler technique.

Corollary 3: Let m be an odd positive integer >1. Then

$$K(P_5\langle m^2\rangle) = (m^2 + 2m + 5)/4; \quad K(P_5\langle m^4\rangle) = (m^3 + 2m^2 + 5m + 4)/4.$$

Proof: Follows as a special case of Theorem 5.

Acknowledgment

We wish to thank the referee for suggestions that led to an improved presentation of the paper.

References

1. A. T. Balaban & I. Tomescu. "Algebraic Expressions for the Number of Kekulé Structure of Isoarithmic Catacondensed Benzenoid Polycyclic Hydrocarbons." *MATCH* *14* (1983):155-82.
2. A. T. Balaban & I. Tomescu. "Chemical Graphs—XL—Three Relations between the Fibonacci Sequence and the Numbers of Kekulé Structures for Non-Branched Catacondensed Polycyclic Aromatic Hydrocarbons." *Croat. Chem. Acta* *57.3* (1984):391-404.
3. D. Cvetkovic & I. Gutman. "Kekulé Structures and Topology—II—Catacondensed Systems." *Croat. Chem. Acta* *46* (1974):15.
4. S. J. Cyvin. "Number of Kekulé Structures of Single-Chain Aromatics." *Monatsh. Chem.* *114* (1983):13-20.
5. S. J. Cyvin. "Kekulé Structures and the Fibonacci Series." *Acta Chim. Hung.* *112* (1983):281.
6. S. J. Cyvin & I. Gutman. "Topological Properties of Benzenoid Systems—Part XXXVI—Algorithm for the Number of Kekulé Structures in Some Pericondensed Benzenoids." *MATCH* *19* (1986):229-42.
7. S. J. Cyvin & I. Gutman. *Kekulé Structures in Benzenoid Hydrocarbons, Lecture Notes in Chemistry 46*. Berlin: Springer-Verlag, 1988.
8. E. J. Farrell & S. A. Wahid. "Matchings in Pentagonal Chains." *Discr. Appl. Math.* *7* (1984):31-40.
9. E. J. Farrell. "On the Occurrences of Fibonacci Sequences in the Counting of Matchings in Linear Polygonal Chains." *Fibonacci Quarterly* *24.3* (1986): 238-46.
10. M. Gordon & W. H. T. Davison. "Resonance Topology of Fully Aromatic Hydrocarbons." *J. Chem. Phys.* *20* (1952):428-35.
11. I. Gutman. "Topological Properties of Benzenoid Systems—An Identity for the Sextet Polynomial." *Theor. Chim. Acta* *45* (1977):309.
12. I. Gutman. "Topological Properties of Benzenoid Systems—XXI—Theorems, Conjectures, Unsolved Problems." *Croat. Chem. Acta* *56.3* (1983):365-74.
13. I. Gutman. "Perfect Matchings in a Class of Bipartite Graphs." *Publ. de l'Inst. Math.* (Belgrade), Nouvelle serié *45.59* (1989):11-15.
14. I. Gutman & S. J. Cyvin. "A Result on 1-Factors Related to Fibonacci Numbers." *Fibonacci Quarterly* *28.1* (1990):81-84.
15. H. Hosoya. "Topological Index and Fibonacci Numbers with Relation to Chemistry." *Fibonacci Quarterly* *11.3* (1973):255-69.
16. L. Lovacz & M. D. Plummer. *Matching Theory*. Budapest: Akademiai Kiado, 1986
17. R. Tosić. "A Fast Algorithm for Calculating the Number of Kekulé Structures of Unbranched Benzenoid Chains." *MATH/CHEM/COMP 1988*. Proc. Int. Course and Conf. on Interfaces between Math., Chem. and Comp. Sci., Dubrovnik, June, 1988. Elsevier Publishers B.V., 1989, pp. 123-26.
18. R. Tosić & O. Bodroza. "An Algebraic Expression for the Number of Kekulé Structures of Benzenoid Chains." *Fibonacci Quarterly* *29.1* (1991):7-11.
19. R. Tosić & O. Bodroza. "On the Number of Kekulé Structures of Unbranched Benzenoid Chains." *MATCH* *24* (1989):311-16.
20. T. F. Yen. "Resonance Topology of Polynuclear Aromatic Hydrocarbons." *Theor. Chim. Acta* *20* (1971):399.

AMS Classification numbers: 05C70, 05B50, 05A15

*****

ON A DIGRAPH DEFINED BY SQUARING MODULO n

Earle L. Blanton, Jr.
Box 754, Moultrie, GA 31768

Spencer P. Hurd
The Citadel, Charleston, SC 29409

Judson S. McCranie
1503 East Park Avenue, Apt. V-11, Valdosta, GA 31602

1. Introduction

Let us begin by defining the digraph G_n. We identify the vertices of G_n with the set $\{0, 1, 2, \ldots, n - 1\}$. The ordered pair (a, b) is an edge of G_n if and only if $a^2 \equiv b$ modulo n. Our general aim is to show how the number-theoretic properties of n and $n - 1$ are closely associated with certain "geometric" properties of the digraph G_n. The most fundamental results for prime moduli are established in Section 2. In Section 3 we are able to extend these results and at the same time to give a framework in which to view a series of theorems about primitive roots. In the last section we determine the cycle structure for G_p for an arbitrary prime p, and we use this structure to classify primes according to their cycle "signature."

Some examples of these digraphs are shown in the diagrams. For the digraph G_{13} (which is more or less typical since the sequence $a, a^{2^1}, a^{2^2}, \ldots, a^{2^k}, \ldots$ mod n must eventually repeat for any a and any n), we observe that there are 3 connected components which vary in size. Each component consists of a directed cycle and a tree or "tail" appended to some or all of the elements in the cycle. The tail is called a complete binary tree if it has a greatest vertex, called the node, if every vertex in the tail has indegree 0 or 2, and if each directed path from an extremity of the tail to the cycle has the same length. In G_{13}, the cycle vertex 9 has a tail $\{10, 6, 7\}$ with node 10.

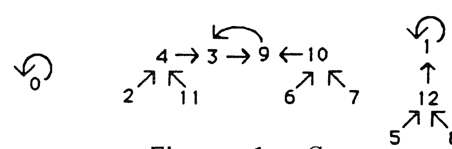


Figure 1. G_{13}

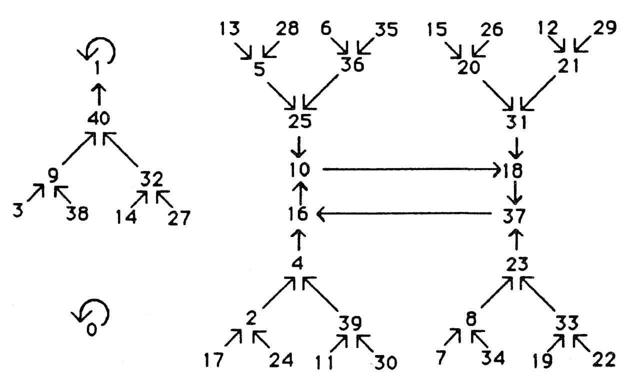


Figure 2. G_{41}

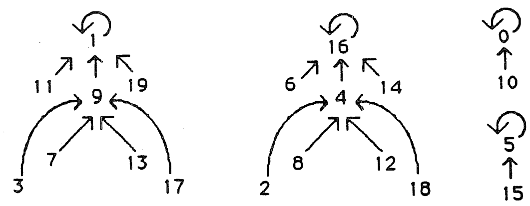


Figure 3. G_{20}

The component of G_{13} containing 0 is a singleton. If $y \equiv y^2 \pmod{n}$, then (y, y) is an edge, and we call y a loop or sink. The vertices 0 and 1 are always sinks. There are many questions one might ask. We will consider the following:

1. Given an n, which vertices in G_n are in a cycle and which are in a tail?
2. How many components has G_n? What are the various cycle sizes? Why are the sizes different?
3. How and why do the tails differ?
4. Are there other sinks besides 0 and 1?
5. To what extent do the digraphs characterize n?

2. The Prime Modulus Case

In what follows, p will always denote an odd prime. A few observations are immediate. The congruence $x^2 \equiv b \pmod{p}$ has 2 solutions, say a and $p - a$, or no solutions [4, p. 84]. This has useful and interesting consequences.

Lemma 0: (a, b) is an edge of G_p if and only if $(p - a, b)$ is an edge. Put another way, if (a, b) and (a', b) are different edges, then $a + a' = p$.

Proposition 1: Every vertex in G_p except 0 has indegree 2 or indegree 0. Whether n is prime or not, every vertex in G_n has outdegree 1.

Proposition 2: If y is any vertex in a cycle of G_p, then the tail for y is empty or is a complete binary tree.

If $y = 0$, then obviously y has both indegree and outdegree 1 and has no tail. Otherwise, as y is in a cycle and $y \neq 0$, there is an edge, say (a, y), with a also in the cycle (this a is the same as y if y is a sink, that is, if $y^2 \equiv y$). But, in any case, this means $(p - a, y)$ is a new edge and $p - a$ is not in the cycle. Thus, $p - a$ is the node of the tail of y. There are no other edges into y since p is prime. By Proposition 1, either $p - a$ has indegree 0 and the tail consists only of $p - a$ itself, or $p - a$ has indegree 2 and there are vertices b_1 and b_2 so that $(b_1, p - a)$ and $(b_2, p - a)$ are edges. But now Proposition 1 applies in turn to b_1 and b_2 in the same way as for $p - a$.

Finally, we recall the theorem that, if p is a prime and if $\gcd(v, p) = 1$, then $x^k \equiv v \pmod{p}$ has either $\gcd(k, p - 1)$ solutions or no solutions at all [7, p. 49]. It follows from this theorem, by induction on the distance from the node, that at every level, say distance w from the node, there are 2^w vertices in the tail at that level. Therefore, it follows that all vertices of indegree zero (the extremities of the tail) are at the same bottom level. Thus, the tail is a complete binary tree. □

These propositions are false if n is not prime (see G_{20}, for example).

Let us recall some standard terminology. If p is an odd prime, and if $x^2 \equiv a \pmod{p}$ has a solution (resp., has no solution), then a is called a quadratic residue (resp., nonresidue) mod p, and satisfies $a^{(p-1)/2} \equiv 1 \pmod{p}$, (resp., $\equiv -1$). In our situation, the numbers at the extremities of the tails are all quadratic nonresidues. We call them *sources*, and there are $(p - 1)/2$ of them.

We need a few additional ideas from number theory. Let ϕ denote the usual Euler totient function. (All of the following can be found in [4, Chs. 9-12].) Euler's Theorem says that, if $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$. Suppose now that $\gcd(a, n) = 1$. Then there is a least positive exponent, say t, such that $a^t \equiv 1 \pmod{n}$. One says "t is the order of a mod n" or "t is the exponent to which a belongs mod n." Further, it follows, for any exponent s with $a^s \equiv 1 \pmod{n}$, that $t|s$. In particular, $t|\phi(n)$. If the exponent t to which a belongs mod n is $\phi(n)$ itself, then a is called a primitive root of n. Every prime number p has exactly $\phi(p - 1)$ primitive roots.

Now suppose that g is a primitive root mod p. Then g, as a vertex of G_p, is a source and lies at the extremity of a tail for some vertex, say h, which is an element of a cycle. Note that $h = g^{2^y}$ for some "minimal" y. We say that y is the length of the tail. It follows from Proposition 2 that there are 2^{y-1} sources in the tail for h and that there are altogether $2^y - 1$ vertices in the tail. Suppose now that the cycle has length x. Then there is a directed path, along the directed edges, in which a repetition first occurs, as follows:

$$g \to g^2 \to \cdots \to g^{2^y} \equiv h \to h^2 \to \cdots \to h^{2^x} \equiv h.$$

Since $h^{2^x} \equiv h \pmod{p}$, we have $h^{2^x-1} \equiv 1 \pmod{p}$. Combining results,

$$g^{2^y(2^x-1)} \equiv 1 \pmod{p}. \tag{2}$$

Clearly, as the repetition did not occur sooner, the numbers y and x are the smallest possible such that (2) is true.

Proposition 3: If $p - 1 = 2^w q$ for some odd number q, then every tail in G_p with a primitive root at its extremity has length w.

Proof: Suppose g is a primitive root for p and that $p - 1 = 2^w q$ for some odd number q. Then g belongs to the exponent $p - 1$, and, by (2) and the discussion above, it follows that $2^y(2^x - 1)$ is a multiple of $p - 1$. Necessarily, then, $q|2^x - 1$ and $2^w|2^y$, and $w \le y$. However, it is impossible that $w < y$, as this implies that the path beginning with g would be at least one step shorter than it actually is. Hence, $w = y$. □

Proposition 4: Suppose that $p - 1 = 2^w q$ for some odd number q. Let h be a vertex of G_p in a cycle of length x as in path (1) with a primitive root for a source. Then,

(a) h has order q.
(b) $2^x - 1$ is the smallest Mersenne number divisible by q.
(c) $q = \gcd(2^x - 1, \phi(p))$.
(d) $x|\phi(q)$, and $x = q - 1$ if q is prime and 2 is a primitive root for q.

Proof: Part (a) follows on untangling quantities:

$$1 \equiv g^{\phi(n)} = g^{2^w q} = [g^{2^w}]^q = h^q.$$

Part (b) is argued above, since x is the smallest integer making the path (1) repeat a vertex. Also, from (a) and (b),

$$q = \gcd(2^x - 1, q) = \gcd(2^x - 1, \phi(p)).$$

This proves part (c). For part (d),

$$q|2^x - 1 \Rightarrow 2^x \equiv 1 \pmod{q}.$$

Now by part (b), x is the order of 2 mod q, and so the rest follows by Euler's Theorem mod q. □

Proposition 4 summarizes parts of the earlier comments and emphasizes the connection between q in the factorization of $p - 1$ and the cycle length x. Let us give another application of this factorization to show that all tails have the same length when n is prime.

Proposition 5: Suppose $p - 1 = 2^w q$ for some odd number q. If $h \neq 0$ is any vertex in a cycle for G_p, then the order of h (mod p) is odd and w is the length of the tail for h. All vertices in the same cycle have the same order. Conversely, if the order mod p of a vertex f in G_p is odd, then f is in a cycle for G_p.

Proof: Since $h \neq 0$, h has a source by the argument in Proposition 2. So let c be a source for h. Note that c is necessarily an odd power of some primitive root, since an even power could not be a source because it would have a square root. Then, by replacing g by c in (1) and (2), it follows that the order of h is odd and that the tail for h has length at least w. But if the tail were longer, then the repetition in (2) would occur at least one step sooner, a contradiction. Now suppose h and j are any two vertices in the same cycle. Say h has order t and j has order s. Note that $h^{2^u} \equiv j \pmod p$ for some u. Therefore,

$$j^t \equiv [h^{2^u}]^t \equiv [h^t]^{2^u} \equiv 1 \pmod p.$$

This shows $s|t$. A symmetric argument shows $t|s$. Hence, $s = t$, and it follows that all vertices in the cycle with h have the same order.

Suppose that the vertex f has odd order d (mod p). Then $q = dv$ for some odd integer v. Let g be a primitive root for p. Then, for some least positive integer r, $f \equiv g^r \pmod p$. Thus, $1 \equiv f^d \equiv g^{rd} \pmod p$. This implies rd is a multiple of $2^w q$, and so r is a multiple of $2^w v$. Thus,

$$r = 2^{w+k} \cdot sv, \text{ for } k \geq 0,\ s \text{ odd}.$$

Now let $c = g^{sv}$. Since sv is odd, c is a source for a cycle vertex, say h. Thus, since the tail length is w, $c^{2^w} \equiv h \pmod p$. It follows that

$$h^{2^k} \equiv [c^{2^w}]^{2^k} \equiv [g^{sv}]^{2^{w+k}} \equiv g^r \equiv f \pmod p.$$

This shows that f is in a cycle, k steps away from h. A different argument for this converse gives a little additional information. Note that $2^{\phi(d)} \equiv 1$ (mod d), by Euler's theorem, since $\gcd(d, 2) = 1$. This means $2^{\phi(d)} - 1 = ds$ for some integer s. Then

$$f^{2^{\phi(d)}-1} \equiv [f^d]^s \equiv 1 \pmod p.$$

But on multiplying by f, we obtain $f^{2^{\phi(d)}} \equiv f \pmod p$. This congruence shows that f is in a cycle, and moreover, that the cycle has length less or equal to $\phi(d)$. This completes the proof. □

We note that if n is not prime, then the tails in G_n need not all have the same length (e.g., see G_{20}).

3. Some Applications

The next few propositions explore the extent to which the digraph G_p determines or characterizes w or q, where $p - 1 = 2^w q$. Along the way, we obtain not only relatively easy proofs of some familiar results about primitive roots, but also a framework which the digraphs provide for illustrating and investigating questions about primitive roots.

We refer the reader to Table 1 which contains cycle data for G_p with $5 \leq p \leq 79$, and $p = 2^w q + 1$, for q odd. A cycle of maximum length will be called a long cycle. From Propositions 4 and 5, we suspect that these long cycles are cycles with primitive roots for sources, and this usually turns out to be the case. For those examples in which q is also prime, the cycle structure is simpler. Further, if $w = 1$ (that is, $p = 2q + 1$), the number of primitive roots is $q - 1$, and there are only q quadratic nonresidues (sources). Except for the tail $p - 1$ for the sink 1, the tails consist of the primitive roots alone. Thus, there are $q - 1$ primitive roots and $q - 1$ vertices in the cycles containing them. Are these $2q - 2$ vertices in the same component? That is, is there only one long cycle? Sometimes, yes, as for G_7, G_{11}, G_{23}, and G_{59}. But sometimes not, as in G_{47}. What splits the long cycle into parts?

Table 1. Cycle Data for G_p

		Cycles				Cycles	
p	$p-1=2^kq$	Length	Qty	p	$p-1=2^kq$	Length	Qty
5	2^2	1	2	43	2(3)(7)	1	2
						2	1
7	2(3)	1	2			3	2
		2	1			6	2
11	2(5)	1	2	47	2(23)	1	2
		4	1			11	2
13	$2^2(3)$	1	2	53	$2^2(13)$	1	2
		2	1			12	1
17	2^4	1	2	59	2(29)	1	2
						28	1
19	$2(3^2)$	1	2				
		2	1	61	$2^2(3)(5)$	1	2
		6	1			2	1
						4	3
23	2(11)	1	2				
		10	1	67	2(3)(11)	1	2
						2	1
29	$2^2(7)$	1	2			10	3
		3	2				
				71	2(5)(7)	1	2
31	2(3)(5)	1	2			3	2
		2	1			4	1
		4	3			12	2
37	$2^2(3^2)$	1	2	73	$2^3(3^2)$	1	2
		2	1			2	1
		6	1			6	1
41	$2^3(5)$	1	2	79	2(3)(13)	1	2
		4	1			2	1
						12	3

Proposition 6: Suppose $p = 2^w q + 1$ for some odd prime q. Then G_p has 3 cycles if and only if 2 is a primitive root for q. More precisely, if x is the exponent to which 2 belongs mod q, then x is the length of a long cycle, and there are $(q - 1)/x$ cycles of this maximal length. The total number of cycles is $2 + (q - 1)/x$, and the only cycle lengths that occur are 1 and x.

Proof: First, we prove that there are exactly q vertices in cycles which have tails. In each tail, the "bottom row" consists of sources, and in all the tails there are $(p - 1)/2$ of these; the next row is half as large, and so on. The total number of vertices in tails is

$$\begin{aligned}(p-1)/2 + (p-1)/4 + \cdots + (p-1)/2^w &= 2^w q(1/2 + \cdots + 1/2^w)\\ &= q(2^{w-1} + 2^{w-2} + \cdots + 1)\\ &= 2^w q - q.\end{aligned}$$

Now $n - (2^w q - q) = q + 1$. So all but $q + 1$ vertices are in tails. There are no sources (or tails) for the trivial sink 0. The sink 1 has a tail. The other $q - 1$ vertices which have tails are in non-sink cycles.

Now, the number of quadratic nonresidues (sources) which are not primitive roots is

$$\begin{aligned}(p-1)/2 - \phi(p-1) &= 2^w q/2 - \phi(2^w q)\\ &= 2^{w-1}q - 2^{w-1}(q-1) = 2^{w-1}.\end{aligned}$$

This is precisely the number of sources for the sink 1, and, by Proposition 4(a), none of these are primitive roots, since the cycle vertex 1 does not have order q. All other sources are primitive roots and thus lead to vertices in cycles of the same length x as in path (1). The number of such cycles is $(q - 1)/x$ since there are exactly $q - 1$ vertices in the remaining cycles, by the first argument. We have shown that two cycles are the two loops 0 and 1 and that the rest have the same size x. □

Corollary 7: If q is prime and $p = 2^w q + 1$, $w \geq 1$, then the sources which are not primitive roots all lie in the tail for the sink 1.

In 1852, V. A. Lebesgue put Corollary 7 differently. He said any quadratic nonresidue, say g, is a primitive root for p unless $g^{2^{w-1}} + 1 \equiv 0 \pmod{p}$; the congruence would imply, in our context, that the source g leads to the node $p - 1$ and, of course, in one more step to the loop 1. A list of historical references appears in the last section.

Question: Suppose that all of the non-sink cycles of G_p have the same size. Then must $p = 2^w q + 1$ for some odd prime q?

The answer to the question is "no." The prime $p = 2^6 \cdot 23 \cdot 89 + 1 = 131009$ gives a counterexample. G_{131009} has 2 cycles of length 1 (the two sinks) and 186 cycles of length 11. This is the smallest counterexample. The largest prime counterexample we found has 1252 digits. Full details of these examples appear in the next section.

The counting arguments in Proposition 6 can easily be extended to prove the following proposition.

Proposition 8: Suppose q is odd, and $p = 2^w q + 1$. Then

(a) The number of primitive roots for p is $2^{w-1}\phi(q)$.

(b) The number of nonresidues for p is $2^{w-1}q$.

(c) The number of sources that are not primitive roots is $2^{w-1}(q - \phi(q))$.

(d) The number of sources in each tail is 2^{w-1}. The number of vertices in each tail is $2^w - 1$. The number of vertices in tails is $2^w q - q$.

(e) The number of vertices in non-sink cycles is $q - 1$.

Proposition 9: Suppose $p \equiv 3 \pmod 4$, i.e., that $p = 2q + 1$ for q odd. Then r is a quadratic residue for p if and only if $p - r$ is a quadratic nonresidue.

Proof: If r is a residue, it is in a cycle, since tails have length 1. Thus, $p - r$ is the node (source) for the vertex r^2 which is in the cycle with r. □

Proposition 10: G_p has exactly two components if and only if p is a Fermat prime.

Proof: If G_p has exactly two components, then one consists of the sink 0. All the other vertices must be in the other component and necessarily lead to the sink 1. Now 2 is in the tail somewhere. Therefore, there is a path starting with 2 and terminating at the node $p - 1$. But then $p - 1$ is congruent to a power of two [and the power is a power of two as in path (1)]. Thus, p divides $2^{2^t} + 1$ for some $t \geq 0$. On the other hand, for some w, there are $2^w - 1$ vertices in the tail for 1. Thus, G_p consists of the sink 0, the sink 1, and the $2^w - 1$ vertices in the tail for 1. It follows that $p = 2^w + 1$. In order that there be no remainder in this long division,

$$2^w + 1 \overline{\big)\, 2^{2^t} + 1}^{\;Q},$$

some partial remainder in the division such as $-2^{2^t - kw} + 1$ is zero. Therefore, for some k, $2^t - kw = 0$. It follows that w is a power of 2. This means p is a Fermat prime: $p = 2^w + 1$ and w is a power of 2.

For the converse, suppose p is a prime and $p = 2^{2^t} + 1$ for some $t \geq 0$. Then, by Proposition 8, the tail for the sink 1 has $2^{2^t} - 1$ elements. The whole component containing 1 has 2^{2^t} elements. It follows that the component containing 1 and the sink 0 comprise all of G_p. □

The next two corollaries are well known, but the proofs are nice applications of the digraphs.

Corollary 11: If $p = 2^w + 1$ is prime, then w is a power of 2.

Proof: By Propositions 5 and 8, tails for G_p have length w and there are $2^w - 1$ vertices in the tail for 1. The vertices for G_p include the sink 0, the sink 1, and the tail for 1. This gives $1 + 1 + (2^w - 1) = 2^w + 1 = p$ vertices. As all of G_p is accounted for, we see that there are only two components. By Proposition 10, p is a Fermat prime, and so w is a power of 2.

Corollary 12: Every source of G_p is a primitive root if and only if p is a Fermat prime.

Proof: First, suppose all sources are primitive roots. If g is a source for 1, then the order of g is a power of two, and the desired result follows by Corollary 11. Conversely, when p is a Fermat prime, there are only two components by Proposition 10. Thus, all the sources (and all the primitive roots) are sources for the sink 1. Let g be any source. Then $g^{2^w} \equiv 1 \pmod{p}$; so g has order a power of two, some divisor of 2^w. But if $g^{2^y} \equiv 1 \pmod{p}$ and $y < w$, then the path from g to 1 would be shorter, a contradiction. Hence, $y = w$ and g is a primitive root. □

Proposition 13: Exactly one source of G_p fails to be a primitive root for p if and only if $p = 2q + 1$ for some odd prime q and $p - 1$ is the source not a primitive root.

Proof: The second direction follows from Proposition 8(c) and Corollary 7. Now suppose only one source, say g', is not a primitive root. Then g' must lead to the loop 1 as, otherwise, some other source g'' leading to 1 would be a primitive root with order a power of two, and by the previous results, p would be a Fermat prime, and every source would be a primitive root, a contradiction. This same argument shows that the tail to which the source g' belongs must have only one source. Thus, the tail consists of only the node. Since all the tails have the same length, by Proposition 5, $p - 1 = 2q$ for some odd number q. Hence, there are q sources, and by hypothesis, $q - 1$ of them are primitive roots. There are also q residues of which $q - 1$ are in non-sink cycles. If h is any of these vertices in non-sink cycles, by Proposition 4, the order of h

is q. Therefore, the non-zero vertices of G_p have only the orders 1 (the sink 1), 2 (the nonresidue $p - 1 = g'$), 2 (the $q - 1$ primitive roots), and q (the $q - 1$ vertices in non-sink cycles). This accounts for all the non-zero vertices of G_p and none has order some proper divisor of q. However, if g is a primitive root, then g has order $2q$. If $kj = q$ for $1 < k, j < q$, then the element g^{2k} would have order j, a proper divisor of q. But there is no such vertex. It follows that q is prime. □

We now give a new proof of a result of Baum [2]. Like Wilansky [15], we will not use quadratic reciprocity. The argument is made easier using the representation for G_p. We assume familiarity with the Legendre symbol and its properties (see [4], [7]).

Proposition 14: Suppose $p = 2q + 1$ and that q is an odd prime. It follows that:

(a) If $q \equiv 1 \pmod 4$, then 2 and $q + 1$ are primitive roots for p (and $p - 2$ and q are residues).

(b) If $q \equiv 3 \pmod 4$, then $p - 2$ and q are primitive roots for p (and 2 and $q + 1$ are residues).

(c) In either case, $2(-1)^{(q-1)/2}$ is a primitive root for p.

Proof: (a) Using the Legendre symbol and noting that $p \equiv 3 \pmod 8$ in this case so that $(2|p) = -1$, we have

$$1 = (1|p) = (2q + 2|p) = (2(q + 1)|p) = (2|p)(q + 1|p).$$

It follows that $q + 1$, like 2, is a quadratic nonresidue mod p. By Proposition 9, since $q + 1$ is a source, q is a residue; likewise, as 2 is a source, $p - 2$ is a residue. But by Proposition 13, these sources are primitive roots since, clearly, neither is $p - 1$. The proof for (b) is similar, and (c) follows from (a) and (b).

Proposition 15: Suppose q is odd and $p = 2^w q + 1$, $w \geq 2$. Then it follows that:

(a) g is a primitive root mod p if and only if $p - g$ is also, and b is a source but not a primitive root if and only if $p - b$ is also.

(b) If $w \geq 3$, then ± 2 and $\pm 2^m q$ $(0 \leq m \leq w)$ are never primitive roots for p.

(c) If $w = 2$ and if q is prime (that is, $p = 4q + 1$), then 2, $p - 2$, $2q$, and $2q + 1$ are primitive roots for p; also, q and $3q + 1$ are residues.

Proof: For (a), since $w \geq 2$, tails have length at least two, and so the tails are not merely nodes. Thus, by Lemma 0, the sources come in pairs a and $p - a$ with $a^2 \equiv (p - a)^2 \pmod p$, and both lead to the same cycle vertex. By Proposition 4, sources which are primitive roots lead to cycles in which each vertex has order q. There are $\phi(q)$ such vertices, each of which has a tail with 2^{w-1} sources. But by, Proposition 8, there are altogether $2^{w-1}\phi(q)$ primitive roots. Thus, no source which is not a primitive root could also lead to a vertex of order q. Therefore, if one member of a pair a and $p - a$ is a primitive root (or is a source not a primitive root), then so is the other.

For (b), since $p \equiv 1 \pmod 8$, we have $(2|p) = 1$. Thus, 2 and $p - 2$ are not sources. Now,

$$1 = (1|p) = (-2^w q|p) = (2^w|p)(-q|p) = (-q|p).$$

So $-q$ is a residue, and by part (a) so is q. It follows that $\pm 2^m q$ is a residue for $0 \leq m \leq w$.

For (c), $(2|p) = -1$, since $p \equiv 5 \pmod 8$. Thus, 2 is a source. By Corollary 7, 2 must be a primitive root because, otherwise, 2 is a source for the sink 1, and then we would have $2^2 = p - 1 = 4q$ = the node for 1, an impossibility. It follows from part (a) that $p - 2$ is also a primitive root. Now

$$(2|p)(2q + 1|p) = (p + 1|p) = 1.$$

Thus, $2q + 1$ is a source and clearly must be a primitive root for, otherwise, by Corollary 7 again,

$$(2q + 1)^2 = 4q^2 + 4q + 1 \equiv 4q^2 \equiv p - 1 = 4q,$$

which would imply $q \equiv 1$, an impossibility. By part (a) again, $2q$ is a primitive root. Since tails have length 2, $p - 1$ is not a source. Hence,

$$1 = (p - 1|p) = (4q|p) = (q|p).$$

Thus, q is a residue, and by part (a) so is $3q + 1$. □

4. Cycles and Signatures for Arbitrary Prime Moduli

In this section we consider an arbitrary prime p with $p = 2^w q + 1$ where q is odd, $w \geq 1$, and begin with a nice generalization of Propositions 4 and 6.

Proposition 16: Suppose $p = 2^w q + 1$ and q is odd. If d is a divisor of q, then there are $\phi(d)$ vertices in G_p, all in cycles of length $x = x(d)$, where x is determined from $2^x - 1$, the smallest Mersenne number divisible by d. The number of cycles corresponding to d of length $x(d)$ is

$$\phi(d)/x(d).$$

For any cycle length y, the number of cycles of length y is

$$\sum\{\phi(d)/x(d) : \exists d,\ x(d) = y\}.$$

The total number of cycles of G_p is

$$1 + \sum\{\phi(d)/x(d) : d|q\}.$$

Proof: For each divisor d of q, there are $\phi(d)$ vertices of order d (mod p) [4, p. 80], and by Proposition 5, they are all together in the same cycle or cycles. It follows that there are $\phi(d)/x(d)$ cycles containing these vertices. Since

$$\sum\{\phi(d) : d|q\} = q,$$

this accounts for all of the q vertices in cycles with tails (Proposition 8). The only other cycle is the sink 0. It follows that there are altogether

$$1 + \sum\{\phi(d)/x(d) : d|q\}$$

cycles. □

We are now in a position to explain all the data in Table 1. For example, for $p = 61$, we have $d = 1, 3, 5$, and 15. For $d = 1$, the corresponding cycle is the sink 1. For $d = 3$, the corresponding cycle has length $\phi(3) = 2$, and both cycle vertices have order 3 mod 61. For $d = 5$, the corresponding cycle has length $\phi(5) = 4$. The remaining eight cycle vertices are in the other two cycles of length 4, corresponding to $d = 15$, and $\phi(15) = 8$. The sources for these eight vertices are the primitive roots of 61. Since, in this last case, there are two cycles of length 4 instead of one of length 8, we know that $2^4 - 1$ is the smallest Mersenne number divisible by 15.

The example of the prime $p = 2^6 \cdot 23 \cdot 89 + 1 = 131009$, referred to in section 3, is of special interest. Cycle data for this p is summarized in Table 2.

Table 2. Cycle Data for G_{131009}

$p = 1 + 2^6 \cdot 23 \cdot 89 = 131009$

d, an odd divisor of $p - 1$	$\phi(d)$, the number of vertices of order d	Number of cycles	Order of 2 mod d (cycle length)
1	1	1	1
23	22	2	11
89	88	8	11
23(89)	22(88)	176	11

There is one additional tailless cycle for the sink 0.

By Proposition 8, there are $q = 23(89) = 2047$ vertices in cycles with tails. These are the nonzero elements of G_{131009} of odd order. By Proposition 16, for each divisor d of q, there are $\phi(d)$ elements with order d. These d are listed in Table 2. Since the smallest Mersenne number divisible by 23 (i.e., $2^{11} - 1$) is also the smallest Mersenne number divisible by 89, there are only two cycle lengths, 1 (2 cycles) and 11 (186 cycles), but q is not prime. Therefore, the converse to Proposition 6 does not hold. In the example, all non-sink cycles must have the same length

$$11 = x(23) = x(89) = x(q),$$

but the ten cycles corresponding to $d = 89$ and to $d = 23$ have sources which are not primitive roots.

We were interested in whether counterexamples to a possible converse of Proposition 6 were rare. Therefore, in Table 3, we give a list of all primes of the form $1 + 2^w \cdot 23 \cdot 89$ which have fewer than 1300 digits. Each of them has the same 188 cycles (two sinks and the rest of length 11)—the tails get large!

All our computer data was generated by the third author (J. S. M., correspondence welcome) on a Dell 310 microcomputer with a 20 mHz 80386 CPU.

Table 3. A List of Primes of the Form $1 + 2^w \cdot 23 \cdot 89$

w	Number of digits	Computer time in seconds
80	28	1
296	93	1
354	110	1
428	133	2
2118	641	68
2856	864	159
2960	895	176

Note: values of w were checked up to $w = 4332$.

Prime numbers were obtained also for $w = 6$, 14, 18, 48, 60.

Our first algorithm to check for primality proceeded in three steps, each of which used UBASIC [8] routines for handling large integers. First, we checked for small prime factors less than or equal to 131071. If n passed this test, we applied Fermat's Theorem in step 2. That is, pick a prime, say p, and see if $p^{n-1} \equiv 1 \pmod{n}$. If 1 is not the result, then n is certainly composite, but n can pass this test and be composite. If n passes step 2, then step 3 uses the method of Lucas & Lehmer [6, §4.5.4]: "if there is a number x for which the order of x modulo n is equal to $n - 1$, then n is prime. . . . The order of x will be $n - 1$ iff (i) x^{n-1} (mod n) = 1; and (ii) $x^{(n-1)/p}$ (mod n) is not 1 for all primes $p | n - 1$."

This test is convenient because we know the factorization of $n - 1$; nevertheless, we reduced the time factor for larger n by using Proth's test instead of steps 2 and 3 (see [3], p. 92, or [10]): "Let $n = 2^w q + 1$, where $w > 1$, $0 < q < 2$, and $3 \nmid q$. Then n is prime if and only if $3^{(n-1)/2} \equiv -1 \pmod{n}$." In this test, 3 can be replaced by any quadratic nonresidue of n. The time lengths in Table 3 correspond to the use of Proth's test (when $q < 2^w$).

Since $2^{23} - 1 = 47(178481)$ and since the order of 2 is 23 with respect to 47 and 178481, another set of numbers of the form $1 + 2^w \cdot 47 \cdot 178481$ was investigated. This form gives primes for w = 6, 24, 42, 134, 204, 806, 3660, and no other if $w < 4352$. The prime number corresponding to $w = 3660$ has 1109 digits.

One last set of examples concerns primes of the form $1 + 2^w \cdot 233 \cdot 1103 \cdot 2089$ (which correspond in similar fashion to $2^{29} - 1$). Primes occur for w = 12, 144, 312, 548, 644, 3284, and 4128, and for no other $w < 4364$. If $w = 4128$, then the prime number has 1252 digits. Although ours is a respectably large prime to be both discovered and proved prime on a standard (unmodified) microcomputer, the current record has over 2000 digits (personal correspondence, S. Yates; see also [16]).

Proposition 17: Suppose $p = 2^w q + 1$ and q is odd. The length $x(q)$ of the longest cycle of G_p is the least common multiple of the set of cycle lengths.

Proof: Suppose $x(d_1)$ and $x(d_2)$ are the orders of 2 mod d_1 and mod d_2, respectively. If $d_1 | 2^m - 1$, that is, if $2^m \equiv 1 \pmod{d_1}$, then m is a multiple of $x(d_1)$, and likewise for d_2. Clearly, if

$$m = \operatorname{lcm}(x(d_1), x(d_2)),$$

then $2^m - 1$ is the smallest Mersenne number divisible by d_1 and d_2. The proposition now follows by induction on the set of divisors of q. □

For each entry $p = 2^w q + 1$ in Table 1, let us call the corresponding two-column matrix for the length and quantity of cycles the *signature* of p corresponding to q. Since the two columns are determined only by the factorization of q, we will suppress (notationally) the mention of p and will denote this matrix by $S(q)$. In Table 1, we observe that 19, 37, and 73 have the same signature $S(9)$. The primes listed in Table 3 all have the same signature $S(q)$ for $q = 23(89)$.

It is convenient to use the notation $S(q)$ even if there are no primes corresponding to a particular q. In this case, we say the signature $S(q)$ is "empty." If the matrix $S(q)$ has, say, m rows and entries s_{ij}, then

$$\sum_{i=1}^{m} s_{i1} s_{i2} = q + 1.$$

There is a natural equivalence relation, say S, on the set of primes defined by $p_1 S p_2$ if and only if p_1 and p_2 have the same signature. It will cause no confusion if we associate nonempty signatures with the corresponding equivalence class.

Whether any of these equivalence classes of S is infinite is an interesting and apparently open question. Perhaps the most closely examined class in this regard is that with signature $S(1)$, the Fermat primes. Sierpinski asked whether there were infinitely many primes of the form $2^w 3^x + 1$ for some w and x [12]. If not, then there are infinitely many x such that the signatures $S(3^x)$ are empty. This problem is still unsettled.

Interestingly, Sierpinski has proved that infinitely many other signatures are indeed empty [1], [5], [13]. In particular, if

$$q \equiv 1 \pmod{[2^{32} - 1] \cdot 641} \quad \text{and} \quad q \equiv -1 \pmod{6700417},$$

then every integer in the sequence $\{2^w q + 1 : w = 1, 2, \ldots\}$ is divisible by at least one of the primes in the "covering set" {3, 5, 17, 257, 641, 65537, 6700417}. Numbers q such that $S(q)$ is empty are called Sierpinski numbers, and discovering the smallest such q is an open problem [5]. The smallest known Sierpinski number is $q = 78557$, with covering set {3, 5, 7, 13, 19, 37, 73}. Are there any Sierpinski numbers that do not have a finite covering set?

The idea of iteratively squaring some integer (or iterating a quadratic function), and reducing modulo n each time, occurs in computer-generated sequences of random or pseudorandom numbers [6] and in certain factorization methods [9]. Also, D. Shanks [11] suggests using a "cycle graph" (not digraph) to analyze the multiplicative group of least positive residues prime to n. Later Shanks suggests constructing a digraph somewhat similar to ours but with edges $(a, a^2 - 2)$. However, we have not seen the digraphs used here in the literature.

Many of our results about primitive roots were known 140-160 years ago. From Chapter VII of [3] we find that in 1830 M. A. Stern proved that, if q and $p = 2q + 1$ are odd primes, then 2 or -2 is a primitive root of p according to whether $p = 8n + 3$ or $8n + 7$, and that, if $n = 4q + 1$, then ± 2 are primitive roots (rediscovered by P. L. Tchebychev in 1845 and V. Bouniakowski in 1867. See also Shanks [11, Ths. 38-40]). F. J. Richelot in 1832 (and later M. Frolov in 1893) proved that, if $p = 2^m + 1$ is prime, then every quadratic nonresidue is a primitive root.

E. Desmarest and V. A. Lebesgue separately proved in 1852 (and later G. Wertheim in 1894) that, if q and $p = 2^w q + 1$ are odd primes, then any quadratic nonresidue g of p is a primitive root unless $g^{2^{w-1}} + 1 \equiv 0 \pmod{p}$. F. Landry in 1854 also proved this and added that, if $p = 2m + 1$, where m is prime, then the quadratic nonresidue h was a primitive root of p if $h \neq p - 1$. Allegret in 1857 proved that, if q is odd, then q is not a primitive root of $2^{2^x} q + 1$. More recently, Baum [2] and Wilansky [15] proved most of our Proposition 14, having observed Propositions 9 and 13 also. Corollary 11 is well known (see p. 58 of Stewart [14]).

If the modulus is not prime, then most of our results fail to be true. Tails need not have the same lengths. In fact, the length of a tail must be redefined. Since a cycle vertex may have indegree greater than 2, tails need not have nodes. The sink 0 can have a tail longer than that for vertices in non-sink cycles. Given any $k \geq 1$, there are infinitely many n so that G_n has 2^k sinks. All the cycles can be sinks. A single long cycle is rare. These and other facts will be explored in a later paper.

References

1. R. Baillie, G. Cormack, & H. C. Williams. "The Problem of Sierpinski Concerning $k \cdot 2^n + 1$." *Math. of Comp.* *37* (1981):229-31.
2. John D. Baum. "A Note on Primitive Roots." *Math. Mag.* *38* (1965):12-14.
3. Leonard E. Dickson. *History of the Theory of Numbers*. Vol. I: *Divisibility and Primality*. New York: Chelsea, 1952 (rpt. of the 1919 ed., Carnegie Institute).
4. Underwood Dudley. *Elementary Number Theory*. 2nd ed. New York: W. H. Freeman and Company, 1978.
5. G. Jaeschke. "On the Smallest k Such That $k \cdot 2^n + 1$ Are Composite." *Math. of Comp.* *40* (1983):381-84.
6. Donald E. Knuth. *Seminumerical Algorithms: The Art of Computer Programming*. Vol. 2. Reading, Mass.: Addison-Wesley, 1969.
7. Ivan Niven & Herbert S. Zuckerman. *An Introduction to the Theory of Numbers*. 3rd ed. New York: Wiley, 1972.

8. Walter D. Neumann. "UBASIC: A Public Domain BASIC for Mathematics." *Notices of the A.M.S.* *36.5* (1989):557-59.
9. J. M. Pollard. "Monte Carlo Methods for Index Computation (mod p)." *Math. of Comp.* *32* (1978):918-24.
10. Raphael M. Robinson. "The Converse of Fermat's Theorem." *Amer. Math. Monthly* *64* (1957):703-10.
11. Daniel Shanks. *Solved and Unsolved Problems in Number Theory*. Washington, D.C.: Spartan Books, 1962.
12. W. Sierpinski. *A Selection of Problems in the Theory of Numbers*. New York: Pergamon Press, Macmillan, 1964.
13. W. Sierpinski. "Sur un probleme concernant les nombres $k \cdot 2^n + 1$." *Elem. Math.* *15* (1960):73-74; "Corrigendum," *ibid.* *17* (1962):85.
14. B. M. Stewart. *Theory of Numbers*. 2nd ed. New York: Macmillan, 1964.
15. Albert Wilansky. "Primitive Roots without Quadratic Reciprocity." *Math. Mag.* *49* (1976):146.
16. Samuel Yates. *Known Primes with 1000 or More Digits*. October 1990. Published annually by the author.

AMS Classification Numbers: 05C20, 11A07, 05C75.

*****

THE FIBONACCI CONFERENCE IN SCOTLAND

Herta T. Freitag

Ever since our previous Meeting at Wake Forest University in North Carolina, the 1992 Conference had been awaited with keen anticipation. Finally, the announcement appeared: "sponsored jointly by The Fibonacci Association and The University of St. Andrews, THE FIFTH INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS will be held at The University of St. Andrews, Scotland, from July 20th to July 24th 1992. Co-chairmen of the Local Committee are George M. Phillips and Colin M. Campbell, whereas the International Committee is co-chaired by A. N. Philippou and A. F. Horadam."

The participation, 80 in number, 12 of whom are women mathematicians, practically doubled previous attendances. All five continents were represented. From Europe there were 36; 29 came from America, 10 from Asia, 4 from Australia, and 1 from Africa. Among the 24 countries represented by Conference participants, the United States provided the largest contingent of 25 followed by Scotland and England, each with 8, and four countries—Austria, Canada, Italy, and Japan—each providing four registrants.

In all our Conferences do we greatly appreciate A. N. Philippou, "FATHER OF OUR INTERNATIONAL CONFERENCES," as he had initiated our FIRST meeting at Patras University in Greece in 1984. And in all our Conferences (and I do hope that in his proverbial modesty he will not censure this remark) we always cherish our conviction that a program, designed by our esteemed and beloved editor, Professor G. E. Bergum, spells excellence, even if—alas—this time double sessions would become necessary.

What caused the big increase in attendance?

It may have been the fact that The University of St. Andrews is held in high esteem the world over. It may have been the magnetism, mathematical as well as personal, of the set of co-chairmen.

Soul-searching choice decisions had to be made for the overlapping sessions as there were 68 papers, 6 of them presented by women mathematicians who hailed from Bulgaria, China, Italy, Scotland, and (two of them) from the U.S. At least three "non-mathematicians" gave papers, one a research astronomer, two electrical engineers. The ages ranged from 33– to 83+, an age span of 50 years! And the distance traveled by speakers ranged from zero (four St. Andrews faculty members gave papers) to approximately 12,000 miles (the journey from New Zealand).

Please turn to page 367

ON THE DISTRIBUTION OF PYTHAGOREAN TRIPLES

Edward K. Hinson
University of New Hampshire, Durham, NH 03824

(Submitted January 1991)

1. Introduction

A triple (a, b, c) of natural numbers is a *pythagorean triple* if $a^2 + b^2 = c^2$, that is, if there exists a right triangle whose sides are lengths a, b, and c. If $\gcd(a, b) = 1$, then the triple is *primitive*. The family of such triples was among the earliest mathematical objects to be completely characterized.

Theorem 1: Every primitive pythagorean triple (x, y, z) with x even and x, y, $z > 0$ is given by

$$x = 2st, \quad y = s^2 - t^2, \quad z = s^2 + t^2$$

for positive integers s, t such that $\gcd(s, t) = 1$ and $s \not\equiv t \pmod 2$. Conversely, each such pair s, t gives a primitive pythagorean triple by the formula.

In this paper we pursue alternate descriptions of the family of pythagorean triples. We approach this by way of functions which map the set of triples into subsets of $\mathbf{R}$ in which their distribution can be represented topologically and algebraically.

2. The Counting Function ν

We wish to characterize pythagorean triples in terms of two parameters: the positive differences between the lengths of the hypotenuse and the respective legs. In order that this be unambiguous, we must verify that any pair (a, b) in $\mathbf{N} \times \mathbf{N}$, $a \le b$, corresponds to at most one triple. But this amounts to showing that the quadratic equation

$$(1) \qquad x^2 + (x + a)^2 = (x + b)^2$$

has at most one natural number solution—an easy exercise using the quadratic formula. Thus, we have a function

$$\nu_0 : (\mathbf{N} \cup \{0\}) \times \mathbf{N} \to \{0, 1\},$$

where $\nu_0(a, b) = 1$ if and only if there exists a natural number solution for the equation (1).

One can formulate this more concisely. Let $S = \mathbf{Q} \cap [0, 1)$, the set of all rational points in the unit interval except the right endpoint 1. Define

$$\nu : S \to \{0, 1\}$$

by

$$\nu(a/b) = \nu_0(a, b).$$

For ν to be well defined, it suffices that, for all a, b, d in $\mathbf{N}$, we have

$$\nu_0(a, b) = \nu_0(ad, bd).$$

But this holds since

$$(b - a) + \sqrt{2b(b - a)} \in \mathbf{N}$$

if and only if

$$d(b - a) + d\sqrt{2b(b - a)} = (db - da) + \sqrt{2(db)(db - da)} \in \mathbf{N}.$$

Note that any common divisor of x, $x + a$, and $x + b$ must divide both a and b. Since every fraction can be represented in lowest terms, it follows that a one-to-one correspondence exists between the elements of $\nu^{-1}(1)$ and the primitive pythagorean triples. Considering S to have the topology induced by the usual one on $\mathbf{R}$ we may use ν to represent the primitive triples in S and study them from a topological viewpoint.

For example, consider the infinite family of triples

$$(2n + 1,\ 2n^2 + 2n,\ 2n^2 + 2n + 1),\ n \in \mathbf{N}. \tag{2}$$

Under ν these correspond to the rational numbers

$$q_n = \frac{2n^2 - 1}{2n^2},\ n \geq 1.$$

Thus, in the real unit interval $I = [0, 1]$, the accumulation point 1 of the set $\nu^{-1}(1)$ reflects the asymptotic equality of the longer leg and the hypotenuse in the family (2).

We shall use the following basic property of ν in the next section.

Proposition 2: Let a, b be natural numbers. If a is even and b is odd, then $\nu(a/b) = 0$.

Proof: It suffices to show that $\sqrt{2b(b - a)}$ cannot be an integer. Under the hypotheses, both b and $b - a$ are odd; thus, there is not the second factor of 2 necessary in $2b(b - a)$ for it to be a square.

3. A Density Theorem for ν

Most of the easily represented families of triples yield sequences in I converging to 1; e.g.,

$$(2n,\ n^2 - 1,\ n^2 + 1),$$
$$(4n^2,\ n^4 - 4,\ n^4 + 4),$$
$$(2n + 1,\ 2n^2 + 2n,\ 2n^2 + 2n + 1).$$

But there may be many other accumulation points of $\nu^{-1}(1)$. We can use Theorem 1 to determine the inverse images of the counting function ν.

Theorem 3: The sets $\nu^{-1}(0)$ and $\nu^{-1}(1)$ are both dense in the real unit interval I with respect to the usual metric.

Proof: We shall use Proposition 2 to show the density of $\nu^{-1}(0)$. Since $\nu(0) = \nu(1) = 0$, choose r in $(0, 1)$ and $\varepsilon > 0$. Choose b to be an even natural number satisfying $1/(b^2 + 1) < \varepsilon/2$. Now for some nonnegative integer a the interval $(r - \varepsilon, r + \varepsilon)$ contains both $a/(b^2 + 1)$ and $(a + 1)/(b^2 + 1)$. Exactly one of a and $a + 1$ is even (say it's a), and now $\nu(a/(b^2 + 1)) = 0$ by Proposition 2. Since ε is arbitrary we have r in the closure of $\nu^{-1}(0)$.

To show the density of $\nu^{-1}(1)$ in I it suffices to show that every neighborhood in I contains some a/b with $\nu(a/b) = 1$. Choose r and ε from $(0, 1)$ such that $0 < \varepsilon < \min\{r, 1 - r\}$. We can restrict ourselves (thus slightly strengthening the result) to those triples whose longer leg has even length, i.e., for which $2st > s^2 - t^2$ in the characterization of Theorem 1. Solving the quadratic inequality resulting from the substitution $\gamma = s/t$ gives $s < (1 + \sqrt{2})t$ as a necessary and sufficient condition for this restriction. Thus, by Theorem 1, we wish to find relatively prime s and t, exactly one of which is even, so that

$$r - \varepsilon < \frac{2st - (s^2 - t^2)}{(s^2 + t^2) - (s^2 - t^2)} < r + \varepsilon. \tag{3}$$

Again using $\gamma = s/t$ and the quadratic formula, and setting $R = 1 - r - \varepsilon$, we have (3) if and only if

$$\text{(4)} \qquad \sqrt{R} < \frac{1}{\sqrt{2}}\left(\frac{s}{t} - 1\right) < \sqrt{R + 2\varepsilon}.$$

The density of $\mathbf{Q}$ in $\mathbf{R}$ insures that relatively prime s_0 and t_0 exist which satisfy (4). Furthermore, $\sqrt{R + 2\varepsilon} < 1$ implies that $s_0 < (1 + \sqrt{2})t_0$. If exactly one of s_0 and t_0 is even, we may take $s = s_0$, $t = t_0$ and be done. If s_0 and t_0 are both odd, choose $N > 0$ odd and large enough so that

$$\sqrt{R} < \frac{1}{\sqrt{2}}\left(\frac{Ns_0 + 1}{Nt_0} - 1\right) < \sqrt{R + 2\varepsilon}.$$

Let s and t be the numerator and denominator, respectively, of the lowest terms representation of $(Ns_0 + 1)/Nt_0$; it follows from the choice of N that s is even and t is odd. In this way we can construct a rational a/b with $\nu(a/b) = 1$ and $|(a/b) - r| < \varepsilon$, and the theorem is proved.

4. A Representation in the Multiplicative Positive Rationals

There is another formulation of the counting function which is of interest. Define a function

$$\eta : \mathbf{Q}^+ \to \{0, 1\}$$

by

$$\eta(a/b) = \nu(a/(a + b))$$

and note that it, too, is well defined. There is again a one-to-one correspondence between primitive triples and the elements of $\eta^{-1}(1)$. Realizing η as $\nu \circ f$, where $f : \mathbf{Q}^+ \to [0, 1)$ is given by $f(x) = x/(1 + x)$, allows one to deduce from the continuity of f that $\eta^{-1}(0)$ and $\eta^{-1}(1)$ are both dense in $\mathbf{Q}^+$.

The natural multiplicative closure in $\mathbf{Q}^+$ suggests the possibility of an induced closure in $\eta^{-1}(0)$, $\eta^{-1}(1)$, or related subsets. But direct calculations yield

$$\eta(7) = \eta\left(\frac{1}{8}\right) = 1, \quad \eta\left(\frac{7}{8}\right) = \eta\left(\frac{1}{2}\right) = \eta\left(\frac{1}{4}\right) = 0,$$

which taken together show the failure of closure in $\eta^{-1}(0)$ and $\eta^{-1}(1)$. One may observe some slight structure, however, from the following point of view. Let

$$I = \left\{\frac{p}{q} \in \mathbf{Q}^+ : \eta\left(\frac{p}{q}\right) = \eta\left(\frac{q}{p}\right) = 1\right\}$$

and

$$I' = \left\{\frac{p}{q} \in \mathbf{Q}^+ : \eta\left(\frac{p}{q}\right) = \eta\left(\frac{q}{p}\right)\right\}.$$

Clearly, I contains 1, and thus one has a chain $I \subseteq I' \subseteq \mathbf{Q}^+$ of nonempty sets. In fact, we can further characterize the elements of I.

Proposition 4: Let p and q be in $\mathbf{Z}^+$ with $\gcd(p, q) = 1$. Then p/q is in I if and only if $\eta(p/q) \cdot \eta(q/p) = 1$ if and only if p and q are each squares and $p + q$ is twice a square.

Proof: The first equivalence is immediate. Note that

$$f(p/q) = p/(p + q) \quad \text{and} \quad f(q/p) = q/(p + q)$$

and so $\eta(p/q) \cdot \eta(q/p) = 1$ if and only if both

$$\sqrt{2(p + q)q} \quad \text{and} \quad \sqrt{2(p + q)p}$$

are integers. Suppose that p, q, and $(p + q)/2$ are each squares. Then the above radicals are clearly integers. Conversely, if

$$\sqrt{2(p + q)q} \quad \text{and} \quad \sqrt{2(p + q)q}$$

are both integers, then so is

$$\sqrt{2(p+q)q} \cdot \sqrt{2(p+q)p} = 2(p+q)\sqrt{pq}$$

and thus pq is a square. Moreover, since they are relatively prime, each of p and q must be a square. Letting p be a square, it follows from the integrality of $\sqrt{2(p+q)p}$ that $(p+q)/2$ is also a square, as required.

One sees as a corollary that a given p/q from $\eta^{-1}(1)$ is in I if and only if p and q are squares. This observation is useful in proving the following result.

Proposition 5: Let p, p_i, q, and q_i be positive integers.

(i) If p_i/q_i is in I, $i = 1, 2$, then p_1p_2/q_1q_2 is in I';

(ii) for any positive rational p/q, I' contains $(p/q)^2$;

(iii) if p/q is in I, then $(p/q)^n$ is in I' for all $n \geq 1$.

Proof: If, under the hypothesis of (i), $p_1p_2 + q_1q_2$ is twice a square, then p_1p_2/q_1q_2 is in I by Proposition 4. If $p_1p_2 + q_1q_2$ is not twice a square then

$$\eta(p_1p_2/q_1q_2) \cdot \eta(q_1q_2/p_1p_2) = 0;$$

but each factor must be 0 since, otherwise, the above remark would force their product to be 1. A similar argument proves (ii) immediately, and (iii) follows from (ii) using Proposition 4.

As in the previous section, one may wish to know the accumulation points of I and I' in the nonnegative half-line $\mathbf{R}^+ \cup \{0\}$.

Theorem 6: The sets I and I' are dense in $\mathbf{R}^+$.

Proof: The density of I' will follow from that of I by the inclusion $I \subseteq I'$. We know from Proposition 4 that p/q is in I if and only if p and q are squares and $p + q$ is twice a square. Note that such p/q, in lowest terms, correspond to the primitive solutions of the diophantine equation $u^2 + v^2 = 2w^2$ when $p = u^2$ and $q = v^2$. One may calculate that

$$(b-a)^2 + (b+a)^2 = 2c^2$$

if and only if (a, b, c) is a pythagorean triple. Thus, it will suffice to show that as a and b vary among primitive pythagorean triples (a, b, c) the fractions $(b-a)/(b+a)$ are dense in the interval $(0, 1)$. We argue as in Theorem 3. Characterizing the primitive triples as in Theorem 1, restricting our attention to those triples in which $2st > s^2 - t^2$ and setting $\gamma = s/t$ gives

$$\frac{b-a}{b+a} = \frac{2\gamma - \gamma^2 + 1}{2\gamma + \gamma^2 - 1}.$$

But now, differentiating this expression with respect to the real variable γ shows that its range on the restricted domain $(\sqrt{2} - 1, \sqrt{2} + 1)$ is all of $\mathbf{R}^+$; as in Theorem 3, the restriction above on s and t holds in this interval. We complete the proof by using the technique of Theorem 3 to produce s/t corresponding to primitive pythagorean triples arbitrarily close to any rational in $(0, 1)$.

Acknowledgment

The author gratefully acknowledges the referee's observation of the result in Theorem 6.

AMS Classification number: 10A99

*****

GENERATING M-STRONG FIBONACCI PSEUDOPRIMES

Adina Di Porto and Piero Filipponi
Fondazione Ugo Bordoni, Via B. Castiglione, 59, I-00142 Roma, Italy
(Submitted January 1991)

1. Introduction and Generalities

One of the most important problems to be faced when using public-key cryptosystems (see [7] for background material) is to generate a large number of large ($\geq 10^{100}$) prime numbers. This hard to handle problem has been elegantly by-passed by submitting randomly generated odd integers n (which are, of course, of unknown nature) to one or more *probabilistic primality tests*. If n fails a test, then it is *surely* composite, whereas, if n passes the tests, then it is said to be a *probable prime* and is accepted as a prime. More precisely, the term "probable prime" stands for prime number candidates until their primality (or compositeness) has been established [6, p. 92].

In [2] we proposed a simple method for finding large probable primes. To make this paper self-contained, we recall briefly both this method and the definitions given in [2] and [3] of which this paper is an extension.

Let the generalized Lucas numbers $V_n(m)$ (or simply V_n) be defined as

$$(1.1) \qquad V_n = \alpha^n + \beta^n,$$

where

$$(1.2) \qquad \begin{cases} \alpha = -1/\beta = (m + \Delta)/2 \\ \Delta = (m^2 + 4)^{1/2}. \end{cases}$$

It is known (e.g., see [2]) that the congruence

$$(1.3) \qquad V_n \equiv m \pmod{n}$$

holds if n is prime. In [2] we analyzed some properties of the *m-Fibonacci Pseudoprimes* (m-F.Psps.), defined as the *odd* composites satisfying (1.3) for a given value of m, and proposed to accept an integer n of unknown nature as a prime if (1.3) is fulfilled for $m = 1, 2, \ldots, M$, where M is an integer somehow depending on the order of magnitude of n.

The above mentioned method is rather efficient from the point of view of the amount of calculations involved but traps are laid for it by the existence of *M-strong Fibonacci Pseudoprimes* (M-sF.Psps.) defined in [3] as the odd composites n which satisfy (1.3) for $1 \leq m \leq M$.

A correct use of this method for cryptographic purposes would imply the knowledge of the largest M for which at least one M-sF.Psp. exists below a given limit (say, 10^{100}). An attempt in this direction is made by the authors in this paper (see also [3]) by finding formulas for generating M-sF.Psps. for arbitrarily large M (section 3). In section 4 some numerical results are presented from which we could get the hang of the order of magnitude of such largest value of M.

2. Preliminaries

Let us rewrite the quantity Δ [cf. (1.2)] as

$$(2.1) \qquad \Delta = \Big(\prod_j 2^d p_j^{a_j}\Big)^{1/2} = \prod_j 2^s p_j^{b_j} \Big(\prod_j 2^r p_j^{c_j}\Big)^{1/2} \ (d \in \{0, 2, 3\};\ r, c_j \in \{0, 1\}),$$

where p_j are distinct odd primes. Both the power to which they are raised in the canonical decomposition of Δ^2 and the value of d depend, obviously, on m.

First, we state the following lemmas.

Lemma 1: p_j is of the form $4k + 1$ ($k \in \mathbb{N} = \{1, 2, \ldots\}$) for any j (and m).

Proof (reductio ad absurdum): Let us assume that the congruence

(2.2) $\quad \Delta^2 = m^2 + 4 \equiv 0 \pmod{4k + 3}$,

where $4k + 3$ is a prime, holds. The congruence (2.2) implies that $m^2 \equiv -4 \pmod{4k + 3}$, that is, it implies that -4 is a quadratic residue modulo $4k + 3$. Now, by using the properties of the Legendre symbol, we have

$$\left(\frac{-4}{4k+3}\right) = \left(\frac{(-1)4}{4k+3}\right) = \left(\frac{-1}{4k+3}\right)\left(\frac{2^2}{4k+3}\right) = (-1)^{(4k+2)/2} \cdot 1 = -1,$$

which contradicts the assumption. Q.E.D.

Lemma 2: p_j is a quadratic residue modulo any prime of the form $kp_j + 1$.

Proof: From Lemma 1 and [4, Th. 99, p. 76], we can write

$$\left(\frac{p_j}{kp_j + 1}\right) = \left(\frac{kp_j + 1}{p_j}\right) = \left(\frac{1}{p_j}\right) = 1. \quad \text{Q.E.D.}$$

Then, let us state the following

Theorem 1: Let q_i be odd rational primes such that [cf. (2.1)]

(2.3) $\quad q_i \equiv 1 \left(\bmod\ 8^r \prod_j p_j^{c_j}\right)$

and let

(2.4) $\quad n = \prod_i q_i^a \quad (a \in \{0, 1\})$

be an odd (square-free) composite. Moreover, define $\Lambda(n)$ as

(2.5) $\quad \Lambda(n) = \operatorname{lcm}(q_i - 1)_i$.

If $n - 1 \equiv 0 \pmod{\Lambda(n)}$, then $V_n \equiv m \pmod{n}$, that is n is an m-F.Psp.

Proof: By considering congruences defined over quadratic fields [4, Ch. XII], from the definition of α and (2.1) we have

$$2\alpha = m + \prod_j 2^s p_j^{b_j} \left(\prod_j 2^r p_j^{c_j}\right)^{1/2}$$

whence, due to the primality of q_i, the congruence

(2.6) $\quad (2\alpha)^{q_i} = 2^{q_i}\alpha^{q_i} \equiv m^{q_i} + \left(\prod_j 2^s p_j^{b_j}\right)^{q_i} \left(\prod_j 2^r p_j^{c_j}\right)^{q_i/2} \pmod{q_i}$

can be written. By using Fermat's little theorem, (2.6) becomes

(2.7) $\quad 2\alpha^{q_i} \equiv m + \prod_j 2^s p_j^{b_j} \left(\prod_j 2^r p_j^{c_j}\right)^{(q_i - 1)/2} \left(\prod_j 2^r p_j^{c_j}\right)^{1/2} \pmod{q_i}$.

From (2.3), Lemma 2, and [4, Th. 95, p. 75], (2.7) can be rewritten as

$$2\alpha^{q_i} \equiv m + \prod_j 2^s p_j^{b_j} \left(\prod_j 2^r p_j^{c_j}\right)^{1/2} = 2\alpha \pmod{q_i},$$

whence, we have

(2.8) $\quad \alpha^{q_i} \equiv \alpha \pmod{q_i}, \quad \alpha^{q_i - 1} \equiv 1 \pmod{q_i}$.

By hypothesis [i.e., $n - 1 \equiv 0 \pmod{q_i - 1}$] and (2.8), we have

$$\alpha^{n-1} \equiv 1 \pmod{q_i}$$

and, consequently,

$$\alpha^{n-1} \equiv 1 \left(\bmod\ \prod_i q_i\right) \quad (\text{i.e., mod } n),$$

whence

(2.9) $\alpha^n \equiv \alpha \pmod{n}$.

Analogously, it can be proved that

(2.10) $\beta^n \equiv \beta \pmod{n}$.

Finally, from (2.9) and (2.10) we have

$$V_n(m) = \alpha^n + \beta^n \equiv \alpha + \beta = m \pmod{n}. \quad \text{Q.E.D.}$$

3. Generating M-sF.Psps.

In this section a simple method for generating M-sF.Psps., which are also Carmichael numbers, is discussed.

Let us consider any expression [5, p. 99] of the form

(3.1) $$n(T) = \prod_{i=1}^{h}(k_iT + 1) = \prod_{i=1}^{h} P_i \quad (h \geq 3;\ k_i,\ T \in \mathbb{N})$$

which gives Carmichael numbers $n(T)$ for all values of T such that P_i ($i = 1, 2, \ldots, h$) is prime.

For $n(T)$ to be an m-F.Psp. by Theorem 1, we must impose that

(3.2) $$P_i \equiv 1 \left(\text{mod } 8^r \prod_j p_j(m)\right) \quad (i = 1, 2, \ldots, h),$$

where [cf. (2.1)] the primes $p_j(m)$ (with $c_j = 1$) are all distinct *odd* primes which appear in the canonical decomposition of $m^2 + 4$ raised to an *odd power* and $r = 1$ (0) if $d = 3$ ($\neq 3$), that is, if $m - 2$ is (is not) divisible by 4.

Due to the particular structure of the factors P_i, (3.2) can be fulfilled by simply imposing that

(3.3) $$T = 8^r \prod_j p_j(m)t \quad (t \in \mathbb{N})$$

so that

(3.4) $$n(t) = \prod_{i=1}^{h} P_i = \prod_{i=1}^{h}\left(k_i 8^r \prod_j p_j(m)t + 1\right).$$

Recalling that the congruence $n(t) - 1 \equiv 0 \pmod{\operatorname{lcm}(P_i - 1)_i}$ holds by construction, Theorem 1 ensures that $n(t)$ is an m-F.Psp. (and a Carmichael number) for all values of t such that P_i is prime ($i = 1, 2, \ldots, h$).

Now, it is clear that if we wish to construct an M-sF.Psp. ($M \geq 2$), we must simply multiply $8k_i$ by the least common multiple of all distinct primes $p_j(m)$ ($m = 1, 2, \ldots, M$).

(3.6) $$C_M = \operatorname{lcm}(p_j(m))_{j,\, 1 \leq m \leq M}$$

thus, getting the number

(3.7) $$n_M(t) = \prod_{i=1}^{h}(8C_M k_i t + 1)$$

which is an M-sF.Psp. (and a Carmichael number) for all values of t such that all the h factors in the product (3.7) are prime.

An Important Remark: An M-sF.Psp. constructed by using the above method may be an $(M + a)$-sF.Psp. ($a \geq 1$) as well. For this to happen (see also [2, Th. 6]) it suffices that either

(3.8) $$C_{M+a} = C_M$$

or

(3.9) $$t_0 \equiv 0 \pmod{\operatorname{lcm}(p_j(m))_{j,\, M+1 \leq m \leq M+a}},$$

where t_0 is any value of t such that [cf. (3.7)] $8C_M k_i t + 1$ is prime ($i = 1, 2, \ldots, h$).

It should be noted that a so-obtained M-sF.Psp. may be an $(M + a)$-sF.Psp. even though (3.8) and/or (3.9) are not satisfied. This fact will be investigated in a further work. Some numerical examples of the said occurrences will be shown in section 4.

4. Numerical Results

Some simple expressions of the form (3.1) are

(4.1) $\quad n(T) = (6T + 1)(12T + 1)(18T + 1),$

(4.2) $\quad n'(T) = n(T)(36T + 1),$

(4.3) $\quad n''(T) = (12T + 1)(24T + 1)(36T + 1)(72T + 1)(144T + 1).$

A computer experiment to find M-sF.Psps. was carried out on the basis of the simplest among them [namely, (4.1)] which was discovered by Chernick [6] in 1939.

According to the procedure discussed in section 3 [cf. (3.7)], we see that, since for $m = 1$ we have $\Delta = \sqrt{5}$, the numbers

(4.4) $$\begin{aligned} n_2(t) &= (5 \cdot 8 \cdot 6t + 1)(5 \cdot 8 \cdot 12t + 1)(5 \cdot 8 \cdot 18t + 1) \\ &= (240t + 1)(480t + 1)(720t + 1) \end{aligned}$$

are 2-sF.Psps. (and Carmichael numbers) for all values of t such that all three factors on the right-hand side of (4.4) are prime. The smallest among them is $n_2(20) = 663{,}805{,}468{,}801$.

Following this procedure, we sought numbers $n_M(t)$ $(M = 3, 4, \ldots)$ which are M-sF.Psps. not exceeding 10^{100}.

The number of digits (#d) of the smallest M-F.Psps. found in this way is shown against M in Table 1.

Table 1

M	#d	M	#d	M	#d
		10	29	29	76
1	8	11	29	21	61
2	12	12	36	22	61
3	16	13	45	23	61
4	16	14	45	24	61
5	18	15	51	25	61
6	18	16	51	26	61
7	29	17	51	27	95
8	29	18	65	28	98
9	29	19	71	29	98

By means of our experiment we could not find any 30-sF.Psp. below 10^{100}.

Just as an illustration, and for the delight of lovers of large numbers, we show the smallest (98 digits) 29-sF.Psp. found by us:

41,703,652,779,296,795,260,673,920,462,490,602,986,625,330,278,308,
957,565,652,181,464,065,185,928,126,878,406,976,583,823,233,761.

This remarkable number is, as previously mentioned, also a Carmichael number. Its canonical factorization (three 33-digit prime factors) is available upon request. This number [namely, $n_{28}(23)$] has been constructed to be a 28-sF.Psp. [see An Important Remark above and paragraph (vi) of the Remark below). The authors would be deeply grateful to anyone bringing to their knowledge a 29-sF.Psp. smaller than $n_{23}(23)$ and/or a 30-sF.Psp. $< 10^{100}$.

Remark: It must be noted that (cf. Table 1), due to the fulfillment of (3.8),

(i) the numbers $n_3(t)$ [cf. (3.7)] which are 3-sF.Psps. are 4-sF.Psps. as well,

(ii) the numbers $n_5(t)$ which are 5-sF.Psps. are 6-sF.Psps. as well,

(iii) the numbers $n_8(t)$ which are 8-sF.Psps. are 11-sF.Psps. as well,

(iv) the numbers $n_{15}(t)$ which are 15-sF.Psps. are 16-sF.Psps. as well,

(v) the numbers $n_{22}(t)$ which are 22-sF.Psps. are 26-sF.Psps. as well,

(vi) the numbers $n_{28}(t)$ which are 28-sF.Psps. are 29-sF.Psps. as well.

Moreover, due to the fulfillment of (3.9), the smallest $n_{21}(t)$ which is a 21-sF.Psp. [namely, $n_{21}(488)$] is a 22-sF.Psp. Therefore, by (v), it is a 26-sF.Psp. as well.

Finally, the smallest $n_{15}(t)$ which is a 15-sF.Psp. [and, by (iv), a 16-sF.-Psp.] is, rather surprisingly, a 17-sF.Psp. This number [namely, $n_{15}(378)$] has 51 digits and is the smallest 17-sF.Psp. with which we are acquainted.

Acknowledgment

This work has been carried out in the framework of an agreement between the Italian PT Administration and the Fondazione Ugo Bordoni.

Addendum

Professor W. Müller (Universität Klagenfurt, Austria) communicated to us that on March 30, 1992, Dr. R. Pinch (University of Cambridge, UK) proved the existence of the ∞-sF.Psps. These *exceptional* numbers satisfy the congruence (1.3) for *all* values of the parameter m. The smallest among them is

$$443372888629441 = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331.$$

References

1. J. Chernick. "On Fermat's Simple Theorem." *Bull. Amer. Math. Soc.* 45 (1939): 269-74.
2. A. Di Porto & P. Filipponi. "A Probabilistic Primality Test Based on the Properties of Certain Generalized Lucas Numbers." *Lecture Notes on Computer Science 330*, pp. 211-23. Berlin: Springer-Verlag, 1988.
3. A. Di Porto, P. Filipponi, & E. Montolivo. "On the Generalized Fibonacci Pseudoprimes." *Fibonacci Quarterly 28.4* (1990):347-54.
4. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers.* 2nd ed. Oxford: Clarendon Press, 1945.
5. P. Ribenboim. *The Book of Prime Number Records.* New York: Springer-Verlag, 1988.
6. H. Riesel. *Prime Numbers and Computer Methods for Factorization.* Boston: Birkäuser, 1985.
7. R. L. Rivest, A. Shamir, & L. Adleman. "A Method for Obtaining Digital Signature and Public-Key Cryptosystems." *Comm. ACM 21.2* (1978):120-26.

AMS Classification numbers: 11A51, 11A07. 11B39

*****

ON SEQUENCES HAVING SAME MINIMAL ELEMENTS IN THE LEMOINE-KATAI ALGORITHM

Jukka Pihko
University of Helsinki, Hallituskatu 15, SF-00100 Helsinki, Finland
(Submitted February 1991)

1. Introduction

Let $1 = a_1 < a_2 < \cdots$ be an infinite strictly increasing sequence of positive integers. Let n be a positive integer. We write

(1.1) $\quad n = a_{(1)} + a_{(2)} + \cdots + a_{(s)},$

where $a_{(1)}$ is the greatest element of the sequence $\leq n$, $a_{(2)}$ is the greatest element $\leq n - a_{(1)}$, and, generally, $a_{(i)}$ is the greatest element $\leq n - a_{(1)} - a_{(2)} - \cdots - a_{(i-1)}$. This algorithm for additive representation of positive integers was introduced in 1969 by Kátai ([2], [3], [4]). Lemoine had earlier considered the special cases $a_i = i^k$, $k \geq 2$ ([5], [6]), and $a_i = i(i+1)/2$ ([7]). (See [10] for further information and note also [1].) The above algorithm is, in turn, a special case of a more general algorithm introduced by Nathanson ([9]) in 1975.

The following basic definitions and results are taken from [8] and [10]. We denote here the set of positive integers by $\mathbf{N}$.

Let $1 = a_1 < a_2 < \cdots$ be an infinite strictly increasing sequence of positive integers with the first element equal to 1. We call it an *A-sequence* and denote by A the sequence itself or sometimes the set consisting of the elements of the sequence. We denote the number s of terms in (1.1) by $h(n)$. If the set $\{n \in \mathbf{N} \mid h(n) = m\}$ is nonempty for some $m \in \mathbf{N}$, we say that *y_m exists* and define y_m to be the *smallest* element of this set. If y_m exists for every $m \in \mathbf{N}$, we say that the *Y-sequence exists* and we denote the sequence $1 = y_1 < y_2 < \cdots$ by Y. The elements y_m are also called *minimal elements*.

Theorem 1.1 (Lord): Let y_k be given ($k \in \mathbf{N}$). Then y_{k+1} exists if and only if there exists a number $n \in \mathbf{N}$ such that

$$a_{n+1} - a_n - 1 \geq y_k.$$

Furthermore, if y_{k+1} exists, then $y_{k+1} = y_k + a_m$, where m is the smallest number in the set

$$\{n \in \mathbf{N} \mid a_{n+1} - a_n - 1 \geq y_k\}.$$

Proof: [8], [10, p. 9]. □

It follows that the Y-sequence exists if and only if the set

$$\{a_{n+1} - a_n \mid n \in \mathbf{N}\}$$

is not bounded.

For technical reasons, we sometimes wish to start the A-sequences and Y-sequences with an element $a_0 = 0$ or $y_0 = 0$, respectively. The following result is from [10, p. 14].

Theorem 1.2: Suppose that $B: 0 = b_0 < 1 = b_1 < b_2 < \cdots$ is an infinite sequence of nonnegative integers. Then B is the Y-sequence for some A-sequence if and only if it satisfies the following conditions:

(a) For every $n \in \mathbf{N}$, either

(1) $b_{n+1} - b_n = b_n - b_{n-1}$, or
(2) $b_{n+1} \ge 2b_n + 1$.

(b) The condition (2) in (a) holds for infinitely many $n \in \mathbf{N}$.

In section 2 of this paper we determine, given a sequence B satisfying the conditions (a) and (b) above, *all* A-sequences A such that $Y = B$ (Theorem 2.1). In section 3 we establish *how many* such A-sequences there are (Theorem 3.5). Fibonacci numbers make their appearance there (after Definition 3.1). For other connections of Fibonacci numbers with the Lemoine-Kátai algorithm we refer to [11] and especially to [12], which also provides part of the motivation for this paper.

2. Determination of All A-Sequences Having a Given Y-Sequence

Theorem 2.1: Let the sequence $B: 0 = b_0 < 1 = b_1 < b_2 < \cdots$ satisfy the conditions (a) and (b) of Theorem 1.2. For the A-sequence $A: 1 = a_1 < a_2 < \cdots$, we have $Y = B$ if and only if the following conditions hold:

(a) $A \cap [b_1, b_2] = \{1, 2, \ldots, b_2 - 1\}$.

(b) Let $n > 1$. If $b_{n+1} - b_n = b_n - b_{n-1}$, then $A \cap [b_n, b_{n+1}] = \emptyset$.

(c) Let $n > 1$. If $b_{n+1} \ge 2b_n + 1$, then $A \cap [b_n, b_{n+1}] = \{a_s, \ldots, a_t\}$, where $a_s < \cdots < a_t$, and

(2.1) $\quad b_n + 1 \le a_s \le 2b_n - b_{n-1}$,

(2.2) $\quad a_{i+1} - a_i \le b_n$, $i = s, \ldots, t - 1$ (if $t > s$),

(2.3) $\quad a_t = b_{n+1} - b_n$.

Proof: The "if" part can be proved in almost exactly the same fashion as the corresponding part in the proof of Theorem 1.2. In fact, we only have to suppress "= 0" on page 16, line 7 in [10]. Notice also that the condition

$$a_s \le 2b_n - b_{n-1}$$

in (2.1) means that (2.2) holds also for $i = s - 1$. To see this, observe that

(2.4) $\quad a_{s-1} = b_n - b_{n-1}$,

which follows easily using conditions (a), (b), and (c).

To prove the "only if" part we suppose now that $A: 1 = a_1 < a_2 < \cdots$ is an A-sequence such that $Y = B$. We must prove that conditions (a), (b), and (c) hold. Condition (a) is trivial. Let $n > 1$ and suppose that

$$b_{n+1} - b_n = b_n - b_{n-1}.$$

From our definitions, it follows easily that

(2.5) $\quad A \cap B = \{1\}$.

Suppose that condition (b) is not true. Then, using (2.5) and $B = Y$, we would get

$$\{y_n + 1, y_n + 2, \ldots, y_n + (y_n - y_{n-1})\} \cap A$$
$$= \{b_n + 1, \ldots, b_{n+1}\} \cap A \ne \emptyset,$$

and so, by [10, Th. 1.13, p. 13],

$$b_{n+1} \ge 2b_n + 1,$$

a contradiction.

Suppose now that $n > 1$ and $b_{n+1} \geq 2b_n + 1$. Suppose further that (a) holds and that (b) and (c) hold for all $n' \in \mathbf{N}$, $1 < n' < n$ if $n > 2$. We prove that (c) holds for n. Since $b_n + 1 \leq b_{n+1} - b_n < b_{n+1}$ and since, by Theorem 1.1, $y_{n+1} - y_n = b_{n+1} - b_n \in A$, we see that

$$A \cap [b_n, b_{n+1}] = \{a_s, \ldots, a_t\}$$

with $a_s < \cdots < a_t$ and $b_{n+1} - b_n = a_h$ for some h, $s \leq h \leq t$. We must prove that $h = t$. By Theorem 1.1 and the definition of h, we get

$$a_{h+1} - a_h - 1 \geq b_n.$$

If $h < t$, then we would get

$$a_{h+1} - a_h - 1 \leq b_{n+1} - (b_{n+1} - b_n) - 1 = b_n - 1 < b_n,$$

a contradiction. It follows that (2.3) holds.

If we had $a_{i+1} - a_i > b_n$ for some i, $s - 1 \leq i \leq t - 1$, then we would have $a_{i+1} - a_i - 1 \geq b_n$ and so, by Theorem 1.1,

$$b_{n+1} \leq b_n + a_i < b_n + a_t = b_{n+1},$$

a contradiction. This proves (2.2). Finally, (2.1) follows from (2.5) and the case $i = s - 1$ above, noticing that using our induction hypothesis we get (2.4) as before. Theorem 2.1 is now proved. □

3. The Number of A-Sequences Having a Given Y-Sequence

Suppose that $B: 0 = b_0 < 1 = b_1 < b_2 < \cdots$ satisfies conditions (a) and (b) of Theorem 1.2. Let $n > 1$ and suppose that $b_{n+1} \geq 2b_n + 1$. Let $I(n)$ be the number of different sequences $a_s < \cdots < a_t$ satisfying conditions (2.1), (2.2), and (2.3). We are going to evaluate $I(n)$. For that, we need the following

Definition 3.1: Let $j \in \mathbf{N}$. Let $u_i^{(j)}$, $i = 1, 2, \ldots$, be such that

$$u_i^{(j)} = \begin{cases} 2^{i-1} & \text{for } i = 1, 2, \ldots, j, \\ u_{i-1}^{(j)} + \cdots + u_{i-j}^{(j)} & \text{for } i > j. \end{cases}$$

In particular, we have $u_i^{(1)} = 1$, $i = 1, 2, \ldots$, and $u_i^{(2)} = F_{i+1}$, $i = 1, 2, \ldots$ (where F_{i+1} denotes the Fibonacci number).

Lemma 3.2: Let $a, b \in \mathbf{Z}$, $a < b$, $j \in \mathbf{N}$. The number of all possible sets $\{c_1, \ldots, c_k\}$ (k is *not* fixed), where

$$a = c_1 < c_2 < \cdots < c_k = b, \; c_i \in \mathbf{Z}, \; i = 1, \ldots, k,$$

and

$$c_{i+1} - c_i \leq j, \; i = 1, \ldots, k - 1,$$

is $u_{b-a}^{(j)}$.

Proof: If $b - a \leq j$, then any subset of the set $\{a + 1, \ldots, b - 1\}$, arranged as a sequence $c_2 < \cdots < c_{k-1}$, gives rise to a permissible sequence

$$a = c_1 < c_2 < \cdots < c_k = b.$$

There are $b - a - 1$ members in the set $\{a + 1, \ldots, b - 1\}$.

If $b - a > j$, then c_2 must be one of the numbers $a + 1, a + 2, \ldots, a + j$, and we use induction. □

Theorem 3.3: Let $n > 1$ and $b_{n+1} \geq 2b_n + 1$.

(a) $I(n) = 2^{b_{n+1} - 2b_n - 1}$, if $2b_n - b_{n-1} \geq b_{n+1} - b_n$.

(b) $I(n) = \sum_{i=g}^{h} u_i^{(b_n)}$, if $2b_n - b_{n-1} < b_{n+1} - b_n$, where

$$g = b_{n+1} - 3b_n + b_{n-1} \quad \text{and} \quad h = b_{n+1} - 2b_n - 1.$$

(c) In case (b), if $(b_{n+1} - b_n) - (b_n + 1) \le b_n$, then

$$I(n) = 2^{b_{n+1} - 2b_n - 1} - 2^{b_{n+1} - 3b_n + b_{n-1} - 1}.$$

Proof: These results follow easily from Theorem 2.1, the definition of $I(n)$, and the use of Lemma 3.2. □

Corollary 3.4: Let $n > 1$ and $b_{n+1} \ge 2b_n + 1$. We have $I(n) = 1$ if and only if

(a) $b_{n+1} = 2b_n + 1$, or

(b) $b_{n+1} = 2b_n + 2$ and $b_n = b_{n-1} + 1$.

Proof: The "if" part is clear. To prove the "only if" part, we suppose that neither (a) nor (b) holds. Then we must have $b_{n+1} \ge 2b_n + 2$.

(1) If $b_{n+1} = 2b_n + 2$, we must have $b_n - b_{n-1} \ge 2$. It follows that

$$2b_n - b_{n-1} \ge b_n + 2 = b_{n+1} - b_n.$$

According to Theorem 3.3, we have

$$I(n) = 2^{b_{n+1} - 2b_n - 1} = 2^{2-1} = 2.$$

(2) Let $b_{n+1} \ge 2b_n + 3$. If $2b_n - b_{n-1} \ge b_{n+1} - b_n$, then, according to Theorem 3.3, we have

$$I(n) = 2^{b_{n+1} - 2b_n - 1} \ge 2^{3-1} = 4.$$

On the other hand, if $2b_n - b_{n-1} < b_{n+1} - b_n$, then, again by Theorem 3.3,

$$I(n) \ge u_h^{(b_n)} = u_{b_{n+1} - 2b_n - 1}^{(b_n)} \ge u_{3-1}^{(b_n)} = u_2^{(b_n)} > 1.$$

In the last inequality, we use the fact that $b_n > 1$, which follows from $n > 1$, and the proof is complete. □

Theorem 3.5: Let $B: 0 = b_0 < 1 = b_1 < b_1 < \cdots$ be an infinite sequence of nonnegative integers satisfying the conditions (a) and (b) of Theorem 1.2. Let $I(B)$ denote the number of different A-sequences for which $Y = B$. Then $I(B)$ is finite if and only if there exists $n_0 \in \mathbf{N}$ such that $b_{n+1} \le 2b_n + 1$ for all $n \ge n_0$. In that case

$$I(B) = \prod_{\substack{1 \le n \le n_0 \\ b_{n+1} \ge 2b_n + 1}} I(n) \quad [\text{we define } I(1) = 1]. \tag{3.1}$$

Proof: From Theorem 2.1 it is clear that $I(B)$ is finite if and only if for some point on we always have $I(n) = 1$ for n satisfying $b_{n+1} \ge 2b_n + 1$. From Corollary 3.4 we know exactly when $I(n) = 1$. It remains to observe that condition (b) of Corollary 3.4 can hold for at most one n. □

Examples 3.6:

(a) ([10, p. 16], [12, p. 296]) Let B be defined by $b_0 = 0$, $b_{n+1} = 2b_n + 1$, $n = 0, 1, \ldots$. Then $b_n = 2^n - 1$ for every $n \in \mathbf{N}$ and by (3.1) we get $I(B) = 1$. The only A-sequence A satisfying $Y = B$ is given by $a_n = 2^{n-1}$, $n = 1, 2, \ldots$.

(b) Let us modify the example given above by taking B: 0, 1, 3, 10, 17, 24, 31, 63, 127, ..., $2^n - 1$, ... Using (3.1) and Theorem 3.3 [we can use (b) or (c)], we get $I(B) = I(2) = 6$. The six A-sequences for which $Y = B$ are given by

1, 2, 4, 5, 6, 7, 32, 64, ..., 2^n, ...,
1, 2, 4, 6, 7, 32, 64, ..., 2^n, ...,
1, 2, 4, 5, 7, 32, 64, ..., 2^n, ...,
1, 2, 4, 7, 32, 64, ..., 2^n, ...,
1, 2, 5, 6, 7, 32, 64, ..., 2^n, ...,
1, 2, 5, 7, 32, 64, ..., 2^n, ...

(c) We modify the examples given above and take $B: 0, 1, 3, 17, 31, 63, 127, \ldots$. We again obtain $I(B) = I(2)$. This time we have to use part (b) of Theorem 3.3 to calculate $I(2)$. The result is

$$I(B) = I(2) = u_9^{(3)} + u_{10}^{(3)} = 149 + 274 = 423.$$

Acknowledgments

This research was done while I spent the Fall term 1988 at the University of Bergen, Norway. I wish to express my sincere gratitude to Ernst S. Selmer for his interest and for carefully reading the manuscript. I thank NAVF for financial support.

References

1. A. S. Fraenkel. "Systems of Numeration." *Amer. Math. Monthly* *92* (1985):105-114.
2. I. Kátai. "Some Algorithms for the Representation of Natural Numbers." *Acta Sci. Math.* (Szeged) *30* (1969):99-105.
3. I. Kátai. "On an Algorithm for Additive Representation of Integers by Prime Numbers." *Ann. Univ. Sci. Budapest, Eötvös Sect. Math.* *12* (1969):23-27.
4. I. Kátai. "On Additive Representation of Integers." *Ann. Univ. Sci. Budapest, Eötvös Sect. Math.* *13* (1970):77-81.
5. E. Lemoine. "Décomposition d'un nombre entier N en ses puissances n^ièmes maxima." *C. R. Paris* *XCV* (1882):719-22.
6. E. Lemonie. "Sur la décomposition d'un nombre en ses carrés maxima." *Assoc. Franc. Tunis* *25* (1896):73-77.
7. E. Lemoine. "Note sur deus nouvèles décompositions des nombres entiers." *Assoc. Franc. Paris* *29* (1900):72-74.
8. G. Lord. "Minimal Elements in an Integer Representing Algorithm." *Amer. Math. Monthly* *83* (1976):193-95.
9. M. B. Nathanson. "An Algorithm for Partitions." *Proc. Amer. Math. Soc.* *52* (1975):121-24.
10. J. Pihko. "An Algorithm for Additive Representation of Positive Integers." *Ann. Acad. Sci. Fenn. Ser. A. I Math. Dissertationes No.* *46* (1983):1-54.
11. J. Pihko. "On Fibonacci and Lucas Representations and a Theorem of Lekkerkerker." *Fibonacci Quarterly* *26.3* (1988):256-61.
12. J. Pihko. "Fibonacci Numbers and an Algorithm of Lemoine and Kátai." In *Applications of Fibonacci Numbers*. Ed. G. E. Bergum et al. Kluwer: Academic Publishers, 1990, pp. 287-97.

AMS Classification numbers: 11B37, 11A67

*****

A GENERALIZATION OF KUMMER'S CONGRUENCES AND RELATED RESULTS

Frank S. Gillespie
Southwest Missouri State University, Springfield, MO 65804
(Submitted February 1991)

1. Introduction

Euler's ϕ-function $\phi(m)$ for m a natural number is defined to be the number of natural numbers not exceeding m which are relatively prime to m. Euler's Theorem states: If m is a natural number and a is an integer such that $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$. It is well known that if $m > 1$ and

$$m = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t}$$

is m's unique representation as a product of pairwise distinct prime numbers, then

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_t}\right).$$

For a discussion of Euler's ϕ-function, see [19], pages 180-83 and 185-90. For clarity of notation,

$$\mathrm{GCD}(a, b) = (a, b)$$

occasionally will be used for the greatest common divisor of a and b. Also,

$$\mathrm{LCM}[a_1, a_2, \dots, a_t]$$

will be used for the least common multiple of $a_1, a_2, \dots, a_t$. As will be seen, the ϕ-function is useful for generating sequences of rational numbers which are used to construct generalized Kummer congruences.

This paper is concerned with sequences $\{u_j\}_{j=0}^{\infty}$ of rational numbers. It will be supposed that each such rational number is written as a quotient of relatively prime integers. A rational number so written is said to be in *standard form*. It is immaterial for this discussion whether the denominator be positive or negative.

The purpose of this paper is to develop a method which will generate sequences of rational numbers (e_n-sequences) which satisfy Kummer's congruence (see line 9 in Definition 3) and especially Theorem 7. The sequences are manifold: they include Bernoulli, Euler, and Tangent numbers as well as Bernoulli and Euler polynomials. Some additional applications will also be given. For example, Kummer's congruences involving reciprocals of Bernoulli (Theorem 9) and Euler numbers (Theorem 8) will be given. A ring structure for some of these sequences will be observed (section 7), and finally some additional examples will be given (section 8).

The Bernoulli polynomials $\{B_j(x)\}_{j=0}^{\infty}$ are defined by

$$\frac{te^{xt}}{e^t - 1} = \sum_{j=0}^{\infty} B_j(x)\frac{t^j}{j!}, \tag{1}$$

and the Bernoulli numbers $\{B_j\}_{j=0}^{\infty}$ are defined by the generating function

$$\frac{x}{e^x - 1} = \sum_{j=0}^{\infty} B_j \frac{x^j}{j!}. \tag{2}$$

See [21], pages 167 and 35.

A rational number a in standard form is a *p-integer* for the prime number p provided the denominator of a is relatively prime to p. See [1], pages 22 and 385. *Kummer's congruence* says: If p is a prime number and $k \not\equiv 0 \pmod{p-1}$ where k is an even natural number, then B_k/k is a p-integer and

$$\frac{B_{k+p-1}}{k+p-1} \equiv \frac{B_k}{k} \pmod{p}. \tag{3}$$

In the paper [11] Fermat's Little Theorem was generalized to sequences $\{u_j\}_{j=0}^{\infty}$ of rational numbers which include sequences of the form $\{a^j\}_{j=0}^{\infty}$ where a is a rational. Basically, [11] investigated sequences $\{u_j\}_{j=0}^{\infty}$ having the property $u_p \equiv u_1 \pmod{p}$ for p a prime number. It is to be observed that $u_p \equiv u_1 \pmod{p}$ can be formed umbrally from $a^p \equiv a \pmod{p}$ by identifying superscripts with subscripts and changing a to u. Here congruences $(\bmod\ m^n)$ are investigated with $m > 1$ a natural number.

Definition 1: Let $m > 1$ be a natural number and let a be a rational number in standard form. The rational number a is said to be an *m-integer* or to be *m-integral* provided the denominator of a is relatively prime to m. If m is a prime number, then of course a is simply a p-integer.

The main results of this paper follow Theorem 1. However, Theorem 1 is important for Definition 3. See the remarks immediately following Definition 3.

Definition 2: Let $m > 1$ be a natural number and suppose $m = p_1^{a_1}p_2^{a_2} \ldots p_t^{a_t}$ is its unique representation as a produce of pairwise distinct prime numbers. The *height h(m) of m* is defined to be

$$h(m) = \max_{1 \le j \le t} (a_j). \tag{4}$$

If $m = 1$, then $h(m)$ is defined to be 0.

Theorem 1 follows from results in [9] or can be easily proved directly.

Theorem 1: Let $m > 1$ be a natural number and suppose a is an m-integer. Then

$$a^{\phi(m)+h(m)} - a^{h(m)} \equiv 0 \pmod{m}. \tag{5}$$

If $m = p$ a prime number, then

$$h(m) = h(p) = 1 \quad \text{and} \quad \phi(m) = \phi(p) = p - 1$$

so that Theorem 1 says $a^p - a \equiv 0 \pmod{p}$, which is Fermat's Theorem. If $(a, m) = 1$, then Theorem 1 is Euler's Theorem.

Using Euler's Theorem, if a is an m-integer, r an integer, g a natural number, and if r is negative $1/a$ is also an m-integer, Theorem 1 and induction give

$$a^{r[\phi(m)+h(m)]^g} - a^{r[h(m)]^g} \equiv 0 \pmod{m}. \tag{6}$$

To see this, note that a^r is an m-integer whether r is positive or negative.

From (6) for n a natural number with r and k integers,

$$a^k\left(a^{r[\phi(m)+h(m)]^g} - a^{r[h(m)]^g}\right)^n \equiv 0 \pmod{m^n}. \tag{7}$$

(See the second paragraph after Definition 4.)

Here, a and $1/a$ are both m-integers if either k or r is negative. This says that

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} a^{(n-j)r[\phi(m)+h(m)]^g + r[h(m)]^g j + k} \equiv 0 \pmod{m^n}. \tag{8}$$

Viewing (8) umbrally gives the inspiration for the following Definition.

Definition 3: Let $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$ where $m_1, m_2, \ldots, m_t$ are natural numbers. The sequence $\{u_j\}_{j=0}^{\infty}$ of rational numbers written in standard form such that each element of

$$\left\{u_{(n-j)\alpha(m)+\beta(m)j+\gamma(m)}\right\}_{j=0}^{n}$$

is an m-integer where $\alpha(m)$, $\beta(m)$, and $\gamma(m)$ are integers such that

$$f(n, j) = (n - j)\alpha(m) + \beta(m)j + \gamma(m) \geq 0$$

is an *e_n-sequence with shift* $(\alpha(m), \beta(m), \gamma(m))$ *with respect to m provided*

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}u_{f(n,j)} \equiv 0 \pmod{m_1^{n_1}m_2^{n_2}\ldots m_t^{n_t}}, \tag{9}$$

where $n_1, n_2, \ldots, n$ are whole numbers such that $n_1 + n_2 + \cdots + n_t = n$. This is, of course, equivalent to

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}u_{f(n,n-j)} \equiv 0 \pmod{m_1^{n_1}m_2^{n_2}\ldots m_t^{n_t}}.$$

In other words, $n_1, n_2, \ldots, n_t$ forms a whole number partition of the natural number n. (See the comments immediately following Theorem 8 and Definition 4.) It is easy to see that (9) can be replaced with the modulus

$$\{\text{LCM}[m_1, m_2, \ldots, m_t]\}^n.$$

(See the third paragraph below.) It is this form of (9) that will be used.

To say, for two rational numbers a and b, that $a \equiv b \pmod m$ for $m > 1$ a natural number simply means $(a - b)/m$ is an m-integer.

Theorem 1 does, as seen above, generalize Euler's Theorem. However, Theorem 1 is not the main generalization with which this paper is concerned. A sequence that is an e_n-sequence with shift $(\alpha(m), \beta(m), \gamma(m))$ could be called a *generalized Euler sequence*. Thus, this paper is not so much concerned with congruences of the form $a^{r+s} \equiv a^r \pmod m$ (see [5], [7], [9], [15]) as it is with sequences that satisfy (9). Kummer's congruences are related to congruences of the type (9) with the modulus

$$\{\text{LCM}[m_1, m_2, \ldots, m_t]\}^n = m^n.$$

Because of the special role that Euler's ϕ-function plays in finding many such congruences, it seems appropriate to refer to sequences named by Definition 3 as generalized Euler sequences.

In light of (8), one possible choice for $\alpha(m)$ and $\beta(m)$ is

$$\alpha(m) = r\alpha_1(m) \quad \text{and} \quad \beta(m) = r\beta_1(m)$$

where r is an integer and $\alpha_1(m)$ and $\beta_1(m)$ are such that, for some integers $r_1, r_2, \ldots, r_t$; $s_1, s_2, \ldots, s_t$ and some natural numbers $g_1, g_2, \ldots, g_t$;

$$\begin{aligned} r_1[\phi(m_1) + h(m_1)]^{g_1} + s_1 &= r_2[\phi(m_2) + h(m_2)]^{g_2} + s_2 \\ &= \cdots = r_t[\phi(m_t) + h(m_t)]^{g_t} + s_t = \alpha_1(m) \end{aligned}$$

and

$$\begin{aligned} r_1[h(m_1)]^{g_1} + s_1 &= r_2[h(m_2)]^{g_2} + s_2 \\ &= \cdots = r_t[h(m_t)]^{g_t} + s_t = \beta_1(m). \end{aligned}$$

To keep this shift from being trivial, $\alpha_1(m)$, $\beta_1(m)$, $r \neq 0$, and $\alpha_1(m) \neq \beta_1(m)$. This shift $(\alpha(m), \beta(m), \gamma(m))$ is a *natural shift*. It is clear that for a natural shift

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}a^{f(n,j)} \equiv 0 \pmod{m_1^{n_1}m_2^{n_2}\ldots m_t^{n_t}} \quad \text{for an } m\text{-integer}.$$

The reason for this is

$$(a^{\alpha(m)} - a^{\beta(m)})^{n_i} \equiv 0 \pmod{m_i^{n_i}}$$

so that

$$\prod_{i=1}^{t} (a^{\alpha(m)} - a^{\beta(m)})^{n_i} = (a^{\alpha(m)} - a^{\beta(m)})^{n_1+n_2+\cdots+n_t}$$

$$= \sum_{j=0}^{n} (-1)^j \binom{n}{j} a^{f(n,j)} \equiv 0 \pmod{m_1^{n_1} m_2^{n_2} \ldots m_t^{n_t}},$$

where $n_1, n_2, \ldots, n_t$ are whole numbers such that $n_1 + n_2 + \cdots + n_t = n$. Note that $\alpha(m)$ and $\beta(m)$ depend upon $m_1, m_2, \ldots, m_t$; $r_1, r_2, \ldots, r_t$; $s_1, s_2, \ldots, s_t$; and $g_1, g_2, \ldots, g_t$. Special care is needed when any of the r's or s's are negative. Note also, since the expression is divisible by $m_1^{n_1} m_2^{n_2} \ldots m_t^{n_t}$ for any whole number partition of $n = n_1 + n_2 + \cdots + n_t$, it will be divisible by $[\mathrm{LCM}[m_1, m_2, \ldots, m_t]]^n$ so that $\{u_j\}_{j=0}^{\infty}$ being an e_n-sequence with respect to $m = \mathrm{LCM}[m_1, m_2, \ldots, m_t]$ implies that

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} u_{f(n,j)} \equiv 0 \pmod{\{\mathrm{LCM}[m_1, m_2, \ldots, m_t]\}^n}$$

and conversely. Thus, for each way of writing m as $\mathrm{LCM}[m_1, m_2, \ldots, m_t]$ there is the possibility of a separate congruence (mod m^n). The simplest way of satisfying this is, of course, $m = \mathrm{LCM}[m]$. From now on, m will denote $\mathrm{LCM}[m_1, m_2, \ldots, m_t]$ for some natural numbers $m_1, m_2, \ldots, m_t$. As will be seen, other ways of writing m besides $m = \mathrm{LCM}[m]$ do indeed lead to different expressions $\equiv 0 \pmod{m^n}$. See section 8 for some examples. $[m_1, m_2, \ldots, m_t]$ is called an *LCM-partition of* m when $m = \mathrm{LCM}[m_1, m_2, \ldots, m_t]$ and $m_1, m_2, \ldots, m_t$ are all natural numbers > 1.

Definition 4: Let $\{u_j\}_{j=0}^{\infty}$ be a sequence of rational numbers written in standard form such that each element of $\{u_{(n-j)\alpha(m)+\beta(m)j+\gamma(m)}\}_{j=0}^{\infty}$ is an m-integer where $\alpha(m)$, $\beta(m)$, and $\gamma(m)$ are integers such that

$$f(n, j) = (n - j)\alpha(m) + \beta(m)j + \gamma(m) \geq 0.$$

If

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} u_{f(n,j)} \equiv 0 \pmod{m^n}, \text{ where } m = \mathrm{LCM}[m_1, m_2, \ldots, m_t] > 1$$

for some natural numbers $m_1, m_2, \ldots, m_t$, then this congruence is a *generalized Kummer congruence*.

From the above, if $\{u_j\}_{j=0}^{\infty}$ is an e_n-sequence with shift $(\alpha(m), \beta(m), \gamma(m))$ with respect to m, then it satisfies a generalized Kummer congruence.

A remark on $\phi(m)$ and $h(m)$ is needed: these functions are convenient to use; however, if for some natural number $m > 1$ there exist $A(m)$ and $B(m)$ such that for every m-integer a, $a^{A(m)} - a^{B(m)} \equiv 0 \pmod{m}$, then $A(m)$ could be used in place of $\phi(m) + h(m)$, and $B(m)$ in place of $h(m)$. Consequently, many of the results in this paper can be generalized somewhat by just such a consideration. However, because of the convenience of finding and working with $\phi(m)$ and $h(m)$, the results are stated in terms of these two functions. Furthermore, some of the parity properties of $\phi(m)$ are used in the proof of Theorem 2, so it was felt that it was better to state the results in terms of natural shifts.

There exist sequences $\{u_j\}_{j=0}^{\infty}$ with shifts other than the natural shift

$$(r[\phi(m) + h(m)]^g, r[h(m)]^g, \gamma(m)).$$

For example, using Theorem 5, if p is an odd prime and a is a p-integer such that

$$(a, p) = 1 \quad \text{and} \quad \left\{\frac{1}{(i - j)a^p + aj}\right\}_{j=0}^{n} \text{ for } 1 \leq i \leq n$$

are all p-integers, then the sequence $\{1/j\}_{j=1}^{\infty}$ is an e_n-sequence with shift $(a^p, a, 0)$ with respect to p. The condition

$$\frac{1}{(i-j)a^p + aj} \text{ is a } p\text{-integer for } 1 \le i \le n$$

is equivalent to $p > n$. Thus $\{1/j\}_{j=1}^{\infty}$ is an e_n-sequence with shift $(a^p, a, 0)$ when $p > n$. Here $m = \text{LCM}[p]$.

From the above definition, it is clear that linear combinations of e_n-sequences with common shift $(\alpha(m), \beta(m), \gamma(m))$ with respect to the same natural number $m > 1$ are also e_n-sequences with shift $(\alpha(m), \beta(m), \gamma(m))$ when the coefficients defining the linear combinations are all m-integers. In particular, multiplying each term of an e_n-sequence by an m-integer gives an e_n-sequence.

It is possible to couch condition (9) in terms of the difference operator Δ, here defined by $\Delta u_x = u_{x+t} - u_x$. If

$$x = n\beta(m) + \gamma(m) \quad \text{and} \quad t = \alpha(m) - \beta(m),$$

then it turns out that

$$\Delta^n u_x = \sum_{j=0}^{n} (-1)^j \binom{n}{j} u_{f(n,j)}.$$

Note that if

$$\alpha(m) = \phi(m) + h(m) \quad \text{and} \quad \beta(m) = h(m),$$

then the increment t is just $\phi(m)$. This will be returned to later in connection with the Factor and Product Theorems.

Let $\{L_j\}_{j=0}^{\infty}$ be the sequence of Lucas numbers. It is well known that

$$(10) \qquad L_j = \left(\frac{1+\sqrt{5}}{2}\right)^j + \left(\frac{1-\sqrt{5}}{2}\right)^j, \; j \ge 0. \quad \text{(See [13], page 26.)}$$

Although (10) represents L_j in the form $\alpha^j + \beta^j$, neither α nor β is rational. By the main theorem of [11], $\{L_j\}_{j=0}^{\infty}$ is an e_1-sequence for any prime number p with shift $(p, 1, 0)$; i.e., for p a prime number, $L_p \equiv L_1 \pmod{p}$. However, simply because L_j is the sum of powers of $(1+\sqrt{5})/2$ and $(1-\sqrt{5})/2$, this is not sufficient for $\{L_j\}_{j=0}^{\infty}$ to be an e_n-sequence with arbitrary shift. Indeed, $\{L_j\}_{j=0}^{\infty}$ is not even an e_2-sequence with shift $(p, 1, 0)$ for the prime number $p = 3$ since $L_6 - 2L_4 + L_2 \not\equiv 0 \pmod{3^2}$. Hence, it does not follow that if each term of the sequence $\{u\}_{j=0}^{\infty}$ of rationals is of the form

$$u_j = x_1^j + x_2^j + \cdots + x_t^j$$

then the sequence is an e_n-sequence with even reasonable shifts.

2. Euler Polynomials and Numbers

The Euler polynomials $E_n(x)$ of degree n and argument x are given by the generating function

$$(11) \qquad \frac{2e^{xt}}{1+e^t} = \sum_{j=0}^{\infty} \frac{E_j(x)t^j}{j!}. \quad \text{(See [21], page 175.)}$$

A well-known formula involving the Euler polynomials is

$$(12) \qquad \sum_{i=1}^{N} (-1)^{N-i} i^n = \frac{1}{2}\{E_n(N+1) + (-1)^N E_n(0)\},$$

where $n = 1, 2, 3, \ldots,$ and $N = 1, 2, 3, \ldots$. (See [16], page 30.)

Using the notation introduced in Definition 3, replace n by $f_j = f(n, j)$ in (12) so that

$$\sum_{i=1}^{N}(-1)^{N-i}i^{f_j} = \frac{1}{2}\{E_{f_j}(N+1) + (-1)^N E_{f_j}(0)\}. \tag{13}$$

To (13), apply the operator

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}a^{f_j}$$

so that

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}\sum_{i=1}^{N}(-1)^{N-i}a^{f_j}i^{f_j} \tag{14}$$

$$= \frac{1}{2}\sum_{j=0}^{n}(-1)^j\binom{n}{j}a^{f_j}E_{f_j}(N+1) + \frac{1}{2}(-1)^N\sum_{j=0}^{n}(-1)^j\binom{n}{j}a^{f_j}E_{f_j}(0).$$

Expanding the left side of (14) gives

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}(-1)^{N-1}[a^{f_j} - (2a)^{f_j} + (3a)^{f_j} - + \cdots + (-1)^{N-1}(Na)^{f_j}] \tag{15}$$

$$= (-1)^{N-1}\{a^{\gamma(m)}[a^{\alpha(m)} - a^{\beta(m)}]^n - (2a)^{\gamma(m)}[(2a)^{\alpha(m)} - (2a)^{\beta(m)}]^n$$

$$+ - \cdots + (-1)^{N-1}(Na)^{\gamma(m)}](Na)^{\alpha(m)} - (Na)^{\beta(m)}]^n\}.$$

Now if $\alpha(m)$ and $\beta(m)$ are such that

$$[(ia)^{\alpha(m)} - (ia)^{\beta(m)}]^n \equiv 0 \pmod{m^n} \text{ for } i = 1, 2, \ldots, N$$

where $m = \mathrm{LCM}[m_1, m_2, \ldots, m_t]$, which they will be for the natural shift $(\alpha(m), \beta(m), \gamma(m))$, then by (7) for $a^{\gamma(m)}$, $(ia)^{\alpha(m)}$, $(ia)^{\beta(m)}$ all m-integral for $i = 1, 2, 3, \ldots, N$, (15) will be $\equiv 0 \pmod{m^n}$. Because of the conditions needed for all these numbers to be m-integers, it is supposed that $r \geq 0$ and $\gamma(m) \geq 0$.

Suppose that $\alpha(m) = r\alpha_1(m)$ and $\beta(m) = r\beta_1(m)$. For $m_i = 2$ where $i = 1, 2, \ldots, t$, the parity of $f(n, j)$ is the parity of $rr_1 j + \gamma + nrs_1$, which will be even if r and $\gamma(m)$ are both even. On the other hand, if $m_i > 2$ for some $i = 1, 2, \ldots, t$, all of the numbers $f(n, j)$, $0 \leq j \leq n$, have the same parity. To see this, use the fact that $\phi(m_i)$ is even when $m_i > 2$. From (15) and (14),

$$\frac{1}{2}\sum_{j=0}^{n}(-1)^i\binom{n}{j}a^{f(n,j)}E_{f(n,j)}(N+1) + \frac{1}{2}(-1)^N\sum_{j=0}^{n}(-1)^j\binom{n}{j}a^{f(n,j)}E_{f(n,j)}(0) \equiv 0 \pmod{m^n}. \tag{16}$$

It is well known that, for $f(n, j)$ even, $E_{f(n,j)}(0) = 0$. (See [21], page 179.) Now $f(n, j)$ is even when $\beta_1(m)$ is odd and $nr + \gamma(m)$ is even when $\beta_1(m)$ is even and $\gamma(m)$ is even.

Next, suppose that m is odd so that $1/2$ is m-integral. In this case, for $N \equiv -(1/2) \pmod{m^n}$ and $f(n, j)$ odd, then

$$E_{f(n,j)}\left(\frac{1}{2}\right) = 0,$$

whereas, if $f(n, j)$ is even

$$E_{f(n,j)}(1) = 0 \quad [\text{letting } N \equiv 0 \pmod{m^n}]. \quad \text{(See [21], page 179.)}$$

Hence, in (14),

$$\sum_{j=0}^{n}(-1)^i\binom{n}{j}E_{f(n,j)}(0) \equiv 0 \pmod{m^n}$$

when $f(n, j)$ is even or when m is odd. Since n is a natural number in (12) and $f(n, j)$ replaces n, it follows that $f(n, j) \geq 1$. This establishes the following theorem.

Theorem 2: Let $m = \mathrm{LCM}[m_1, m_2, \ldots, m_t] > 1$ with $m_1, m_2, \ldots, m_t$ all natural numbers and a, $\gamma(m)$, and x all m-integers. Suppose

$$f(n, j) = (n - j)r\alpha_1(m) + r\beta_1(m)j + \gamma(m) \geq 1 \quad \text{for } 0 \leq j \leq n,$$

where $r \geq 0$ and $\gamma(m) \geq 0$. Assume one of the following statements holds:

(1) $m_i = 2$ for $i = 1, 2, \ldots, t$, and r and $\gamma(m)$ are both even;
(2) m is even and $m_i > 2$ for some $i = 1, 2, \ldots, t$, $\beta_1(m)$ and $\gamma(m)$ are both even;
(3) m is even and $m_i > 2$ for some $i = 1, 2, \ldots, t$, and $nr + \gamma(m)$ is even but $\beta_1(m)$ is odd;
(4) m is odd.

Then $\{a^{f(n,j)}E_{f(n,j)}(x)\}_{j=0}^{n}$ are all m-integers and $\{a^jE_j(x)\}_{j=0}^{\infty}$ is an e_n-sequence with the natural shift $(\alpha(m), \beta(m), \gamma(m))$.

The hypothesis of Theorem 2 cannot be weakened to simply: $m > 1$ is a natural number. To see this, let $m = 4 = \mathrm{LCM}[4]$, $n = 1$, $g = r = \gamma(m) = 1$. None of the four hypotheses is satisfied if $r_1 = 1$ and $s_1 = 0$. If the weakened hypothesis is valid, then

$$(17) \qquad \sum_{j=0}^{1}(-1)^j\binom{1}{j}E_{5-2j}(x) = E_5(x) - E_3(x) = \left(x^5 - \frac{5x^4}{2} + \frac{5x^2}{2} - \frac{1}{2}\right) - \left(x^3 - \frac{3x^2}{2} + \frac{1}{4}\right) \equiv 0 \pmod 4$$

which is false.

For $m > 2$ and m odd, the coefficients of the Euler polynomials are all m-integers. To see this, use

$$(18) \qquad E_n(x) = 2^{-n}\sum_{j=0}^{n}\binom{n}{j}(2x - 1)^{n-j}E_j,$$

where $\{E_j\}_{j=0}^{\infty}$ is the sequence of Euler numbers. The Euler numbers are all integers and, furthermore, $E_t = 2^tE_t(1/2)$. (See [21], pages 177, 39, and 42.)

The above observations along with Theorem 2 establish Theorem 3.

Theorem 3: Let $m = \mathrm{LCM}[m_1, m_2, \ldots, m_t] > 1$ with $m_1, m_2, \ldots, m_t$ all natural numbers and a an m-integer. Suppose

$$f(n, j) = (n - j)r\alpha_1(m) + r\beta_1(m)\,j + \gamma(m) \geq 1 \quad \text{for } 0 \leq j \leq n,$$

where $r \geq 0$ and $\gamma(m) \geq 0$. Then $\{a^jE_j\}_{j=0}^{\infty}$ is an e_n-sequence with the natural shift $(\alpha(m), \beta(m), \gamma(m))$.

The Euler numbers form secant coefficients since

$$\sec x = \sum_{j=0}^{\infty}(-1)^j\frac{E_{2j}x^{2j}}{(2j)!},$$

which is convergent for $|x| < \pi/2$. The number $E_{2n+1} = 0$ for $n \geq 0$. (See [18], pages 202 and 203.)

3. Bernoulli Numbers and Polynomials

The above results open the way to exploration of Bernoulli polynomials and Bernoulli numbers with respect to forming e_n-sequences. A useful relationship is

$$(19) \qquad E_n(x) = \frac{2^{n+1}}{n+1}\left[B_{n+1}\left(\frac{x+1}{2}\right) - B_{n+1}\left(\frac{x}{2}\right)\right] \quad \text{for } n = 0, 1, 2, \ldots .$$

(See [21], page 177.) Using this and the hypothesis of Theorem 2, we have

$$(20) \qquad \left\{\frac{2^{j+1}a^j}{j+1}\left[B_{j+1}\left(\frac{x+1}{2}\right) - B_{j+1}\left(\frac{x}{2}\right)\right]\right\}_{j=0}^{\infty}$$

is an e_n-sequence with natural shift $(\alpha(m), \beta(m), \gamma(m))$ for the natural number $m = \mathrm{LCM}[m_1, m_2, \ldots, m_t] > 1$. Here, both a and x are m-integers.

In (20) let $x = 0$ so that

$$B_{j+1}\left(\frac{1}{2}\right) = \left(\frac{2}{2^{j+1}} - 1\right)B_{j+1} \quad \text{and} \quad B_{j+1}(0) = B_{j+1}, \text{ for } j = 1, 3, 5, \ldots .$$

(See [21], page 171.)

After simplification and using $B_{2j+1} = 0$ for $j = 1, 2, 3, \ldots$, (20) gives

Theorem 4: Let $m = \mathrm{LCM}[m_1, m_2, \ldots, m_t] > 1$ with $m_1, m_2, \ldots, m_t$ all natural numbers and let a be an m-integer. Suppose

$$f(n, j) = (n - j)\alpha(m) + \beta(m)j + \gamma(m) \geq 1 \quad \text{for } 0 \leq j \leq n,$$

where $r \geq 0$ and $\gamma(m) \geq 0$. If m is odd, then

$$\left\{\left(2^{f(n,j)+1} - 1\right)a^{f(n,j)+1}\frac{B_{f(n,j)+1}}{f(n, j) + 1}\right\}_{j=0}^{n}$$

are all m-integers and

$$\left\{\left(2^{j+1} - 1\right)a^{j+1}\frac{B_{j+1}}{j + 1}\right\}_{j=0}^{\infty} \tag{21}$$

is an e_n-sequence with the natural shift $(\alpha(m), \beta(m), \gamma(m))$.

It is important in working with these e_n-sequences to *first* put the terms in standard form and *then* reduce the expression (mod m^n).

Theorem 4 generalizes some well-known results. With the hypotheses of Theorem 4, (21) says

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}\frac{\left(2^{[r[\phi(m)+h(m)]^g - r[h(m)]^g]j+k} - 1\right)B_{[r[\phi(m)+h(m)]^g - r[h(m)]^g]j+k}}{[r[\phi(m) + h(m)]^g - r[h(m)]^g]j + k} \equiv 0 \pmod{m^n}, \tag{22}$$

where $k = r[\phi(m)]^g n + \gamma(m) + 1$. Here $m = \mathrm{LCM}[m]$. This last condition is equivalent to saying $k > r[\phi(m)]^g n$. If $m = p$ (a prime number), $r = g = 1$, then (22) gives

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}\frac{\left(2^{(p-1)j+k} - 1\right)B_{(p-1)j+k}}{(p - 1)j + k} \equiv 0 \pmod{p^n},\ k > (p - 1)n. \tag{23}$$

The Bernoulli, Genocchi, Lucas, and Euler numbers are closely related (see [14]). In particular,

$$G_n = 2(1 - 2^n)B_n \quad \text{and} \quad R_n = (1 - 2^{n-1})B_n, \tag{24}$$

where G_n and R_n are the Genocchi and Lucas numbers, respectively. With the same hypothesis as Theorem 4, $m = p = \mathrm{LCM}[p]$ and $r = g = 1$ gives as examples

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}\frac{G_{(p-1)j+k}}{(p - 1)j + k} \equiv 0 \pmod{p^n}, \text{ and} \tag{25}$$

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}\frac{(2^{(p-1)j+k} - 1)R_{(p-1)j+k}}{(1 - 2^{(p-1)j+k-1})((p - 1)j + k)} = 0 \pmod{p^n}.$$

For a further discussion of these numbers, see [6] and [25].

4. The Factor and Product Theorems

In (21) it is clear that $\{2^{j+1} - 1\}_{j=0}^{\infty}$ is an e_n-sequence with natural shift $(\alpha(m), \beta(m), \gamma(m))$ for the natural number $m = \mathrm{LCM}[m_1, m_2, \ldots, m_t]$. This suggests the possibility of "factoring" a sequence of the form $\{u_j v_j\}_{j=0}^{\infty}$. To that end, consider

$$\Delta^n u_x v_x = \sum_{i=0}^{n} \binom{n}{i} (\Delta^{n-i} u_x)(\Delta^i v_{x+(n-i)t}), \tag{26}$$

where

$$\Delta^n u_x = \sum_{j=0}^{n} (-1)^j \binom{n}{j} u_{x+(n-j)t}. \tag{27}$$

Here, the difference operator is defined by $\Delta u_x = u_{x+t} - u_x$. (See [10], pages 6 and 1, respectively.) Rewriting (26) using (27) gives

$$\begin{aligned} &\sum_{j=0}^{n} (-1)^j \binom{n}{j} u_{x+(n-j)t} v_{x+(n-j)t} \\ &= \sum_{i=0}^{n} \binom{n}{i} \left(\sum_{j=0}^{n-i} (-1)^j \binom{n-i}{j} u_{x+(n-i-j)t} \right) \left(\sum_{j=0}^{i} (-1)^j \binom{i}{j} v_{x+(n-j)t} \right). \end{aligned} \tag{28}$$

To express this in a form needed for e_i-sequences, let

$$x + (n - j)t = (n - j)\alpha(m) + \beta(m)j + \gamma(m), \text{ so that} \tag{29}$$

$$x = n\beta(m) + \gamma(m) \quad \text{and} \quad t = \alpha(m) - \beta(m).$$

Substituting these in (28) yields

$$\begin{aligned} &\sum_{j=0}^{n} (-1)^j \binom{n}{j} u_{(n-j)\alpha(m)+\beta(m)j+\gamma(m)} v_{(n-j)\alpha(m)+\beta(m)j+\gamma(m)} \\ &= \sum_{i=0}^{n} \left[\binom{n}{i} \left(\sum_{j=0}^{n-i} (-1)^j \binom{n-i}{j} u_{(n-i-j)\alpha(m)+\beta(m)j+\beta(m)i+\gamma(m)} \right) \right. \\ &\qquad \left. \cdot \left(\sum_{j=0}^{i} (-1)^j \binom{i}{j} v_{(n-j)\alpha(m)+\beta(m)j+\gamma(m)} \right) \right]. \end{aligned} \tag{30}$$

Using this, the Factor Theorem is obtained.

Theorem 5 (Factor Theorem): Let $m = \text{LCM}[m_1, m_2, \ldots, m_t]$ with $m_1, m_2, \ldots, m_t$ natural numbers. If

(a) $\{u_j v_j\}_{j=0}^{\infty}$ is an e_n-sequence with shift $(\alpha(m), \beta(m), \gamma(m))$; and

(b) $\{v_j\}_{j=0}^{\infty}$ is an e_i-sequence with shift $(\alpha(m), \beta(m), (n - i)\alpha(m) + \gamma(m))$, for $i = 1, 2, \ldots, n - 1$; and

(c) $\{u_j\}_{j=0}^{\infty}$ is an e_{n-i}-sequence with shift $(\alpha(m), \beta(m), \beta(m)i + \gamma(m))$ for $i = 1, 2, \ldots, n - 1$, then

1) If $(m, v_{n\alpha(m)+\gamma(m)}) = 1$ and $\{v_j\}_{j=0}^{\infty}$ is an e_n-sequence with shift $(\alpha(m), \beta(m), \gamma(m))$, then $\{u_j\}_{j=0}^{\infty}$ is an e_n-sequence with shift $(\alpha(m), \beta(m), \gamma(m))$;

2) If $(m, u_{n\beta(m)+\gamma(m)}) = 1$ and $\{u_j\}_{j=0}^{\infty}$ is an e_n-sequence with shift $(\alpha(m), \beta(m), \gamma(m))$, then $\{v_j\}_{j=0}^{\infty}$ is an e_n-sequence with shift $(\alpha(m), \beta(m), \gamma(m))$.

An examination of identity (30) also leads to the Product Theorem.

Theorem 6 (Product Theorem): Let $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$ with $m_1, m_2, \ldots, m_t$ natural numbers. If

(a) $\{u_j\}_{j=0}^{\infty}$ is an e_{n-i}-sequence with shift $(\alpha(m), \beta(m), \beta(m)i + \gamma(m))$ for $i = 0, 1, 2, \ldots, n - 1$; and

(b) $\{v_j\}_{j=0}^{\infty}$ is an e_i-sequence with shift $(\alpha(m), \beta(m), (n - i)\alpha(m) + \gamma(m))$ for $i = 1, 2, \ldots, n$; thus, $\{u_j v_j\}_{j=0}^{\infty}$ is an e_n-sequence with shift $(\alpha(m), \beta(m), \gamma(m))$.

Using $m > 1$ being odd and $\gamma(m) \geq 0$ arbitrary, Theorem 4 together with the Factor Theorem and Theorem 1 yields

Theorem 7: Let $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$ with $m_1, m_2, \ldots, m_t$ all natural numbers. If

(a) $f(n, j) = (n - j)r\alpha_1(m) + r\beta_1(m) + \gamma(m)$ is an odd natural number for $0 \leq j \leq n$; and

(b) $r \geq 0$, $\gamma(m) \geq 0$, g is a natural number; and

(c) $\text{GCD}\left(m,\ 2^{ir\alpha_1(m) + \gamma(m) + 1} - 1\right) = 1$ or, equivalently $\text{GCD}\left(m,\ 2^{ir\beta_1(m) + \gamma(m) + 1} - 1\right) = 1$ for $i = 1, 2, \ldots, n$,

then $\left\{\dfrac{B_{f(n, j) + 1}}{f(n, j) + 1}\right\}_{j=0}^{n}$ are all m-integers and $\left\{\dfrac{B_{j+1}}{j + 1}\right\}_{j=0}^{\infty}$ is an e_n-sequence with the natural shift $(\alpha(m), \beta(m), \gamma(m))$.

In Theorem 7 let $m = p = \text{LCM}[p]$ be an odd prime number and suppose $r = g = 1$ and $k = n + \gamma + 1$. Then (c) becomes

$$(p,\ 2^{i+k-n} - 1) = 1, \quad i = 1, 2, \ldots, n.$$

If $(p, 2^k - 1) = 1$, then $k \not\equiv 0 \pmod{p - 1}$ since $p \mid (2^{p-1} - 1)$ by Fermat's Little Theorem. Theorem 7 gives

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} \frac{B_{(p-1)j+k}}{(p - 1)j + k} \equiv 0 \pmod{p^n}. \tag{31}$$

This congruence is well known (see [3], [4], [18], [22], [23], [24], [26]). The paper [22] has many references to these and related congruences. It is clear that Theorem 7 with $m = p = \text{LCM}[p]$ does not remove the restriction $k \not\equiv 0 \pmod{p - 1}$.

In Theorem 7 let $m = p^t$, where p is an odd prime number and t is a natural number. Then

$$\phi(m) = \phi(p^t) = p^{t-1}(p - 1) \quad \text{and} \quad h(m) = h(p^t) = t.$$

Further, suppose that $\gamma(m) = \gamma(p^t) \geq 0$, $r \geq 0$, g is a natural number and $n = 1$. Then Theorem 7 gives

$$\frac{B_{r[p^{t-1}(p-1)+t]^g + \gamma + 1}}{r[p^{t-1}(p - 1) + t]^g + \gamma + 1} \equiv \frac{B_{rt^g + \gamma + 1}}{rt^g + \gamma + 1} \pmod{p^t}, \tag{32}$$

when $(p, 2^{t+\gamma+1} - 1) = 1$. In (32) let $t = 1$ and $\gamma = 2k - 2$. This then is Kummer's congruence with the hypothesis $(p, 2^{2k} - 1) = 1$. Similar congruences immediately follow from Theorem 7 for $m = p^t$ and n an arbitrary natural number.

Repeated use of the Product Theorem allows for variations of the previous results. Thus, for $m > 1$ an odd natural number $\{\alpha^j E_{j+b_1}^{a_1} E_{j+b_2}^{a_2} \cdots E_{j+b_t}^{a_t}\}_{j=0}^{\infty}$ is an e_n-sequence with shift $(r[\phi(m) + h(m)]^g,\ r[h(m)]^g,\ \gamma(m))$ where $r \geq 0$, $\gamma(m) \geq 0$, $a_1, a_2, \ldots, a_t$; $b_1, b_2, \ldots, b_t$ are whole numbers and α is an m-integer. One application of this is to let

$$a_1 = a_2 = \cdots = a_t = 1 \quad \text{and} \quad b_1 = b_2 = \cdots = b_t = 0$$

so that $\{E_j^t\}_{j=0}^{\infty}$ is an e_n-sequence. For example, let $m = p = \text{LCM}[p]$ be an odd prime number and let $n = 2$. Then, for t any natural number,

$$E_{2p+\gamma}^t - 2E_{p+\gamma+1}^t + E_{\gamma+2}^t \equiv 0 \pmod{p^2}.$$

Here, $\gamma = \gamma(p) \geq 1$ and $r = 1$. For example, letting $p = 7$ and $\gamma = 2$, this says, after reduction, for every n a whole number

$$40^n - 2 \cdot 47^n + 5^n \equiv 0 \pmod{49}.$$

It is possible to combine both the Factor Theorem and the Product Theorem. Since $\{1\}_{j=0}^{\infty}$ is an e_n-sequence with respect to the odd natural number $m > 1$ and for j even, $E_j(1/E_j) = 1$, it follows that for the natural shift with $r \geq 0$, $\gamma(m) \geq 0$, and $f(n, j)$ even, for $0 \leq j \leq n$ and $\{1/E_{f(n,j)}\}_{j=0}^{n}$ consisting of m-integers, then $\{1/E_j\}_{j \text{ even}}$, is an e_n-sequence. From Theorem 3 it follows that

$$E_{f(n,j+1)} \equiv E_{f(n,j)} \pmod{m} \text{ for } 0 \leq j+1 \leq n,$$

so that if $(m, E_{f(n,j)}) = 1$ for any $j = 0, 1, 2, \ldots, n$, then $\{1/E_{f(n,j)}\}_{j=0}^{n}$ consists of m-integers. This establishes

Theorem 8: Let $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$ with $m_1, m_2, \ldots, m_t$ natural numbers be an odd natural number. Suppose

$$f(n, j) = (n - j)r\alpha_1(m) + r\beta_1(m) + \gamma(m)$$

is an even natural number where $r \geq 0$ and $\gamma(m) \geq 0$. If $(m, E_{f(n,j)}) = 1$ for at least one $j = 0, 1, 2, \ldots, n$, then the sequence $\{1/E_j\}_{j \text{ even}}$ is an e_n-sequence for the natural shift $(\alpha(m), \beta(m), \gamma(m))$.

In Theorem 8, what is meant by saying $\{1/E_j\}_{j \text{ even}}$ is an e_n-sequence? For that matter, what is meant by saying $\{u_j\}_{j \text{ of the form } F}$ is an e_n-sequence? This simply means:

(a) $f(n, j)$ is of the form F for $0 \leq j \leq n$,

(b) $\{u_{f(n,j)}\}_{j=0}^{n}$ are all m-integers, and

(c) $\sum_{j=0}^{n} (-1)^j \binom{n}{j} u_{f(n,j)} \equiv 0 \pmod{m^n}$ where $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$ with $m_1, m_2, \ldots, m_t$ natural numbers.

Since

$$\left\{\frac{B_{j+1}}{j+1} \cdot \frac{j+1}{B_{j+1}}\right\}_{j \text{ odd}}$$

is an e_n-sequence with shift $(r\alpha_1(m), r\beta_1(m), \gamma(m))$, $r \geq 0$ and $\gamma(m) \geq 0$ for the odd natural number $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$, Theorem 7 gives conditions for $\{B_{j+1}/(j+1)\}_{j \text{ odd}}$ to be an e_n-sequence, and $[f(n, j) + 1]/(B_{f(n,j)+1})$ will be an m-integer when

$$\text{GCD}\left(m, \frac{B_{f(n,j)+1}}{f(n, j) + 1}\right) = 1.$$

This implies

Theorem 9: Let $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$ with $m_1, m_2, \ldots, m_t$ all natural numbers and m odd. If

(a) $f(n, j) = (n - j)r\alpha_1(m) + r\beta_1(m) + \gamma(m)$ is an odd natural number for $0 \leq j \leq n$; and

(b) $r \geq 0$ and $\gamma(m) \geq 0$; and

(c) $\text{GCD}\left(m, 2^{ir\alpha_1(m)+\gamma(m)+1} - 1\right) = 1$ or, equivalently,
$\text{GCD}\left(m, 2^{ir\beta_1(m)+\gamma(m)+1} - 1\right) = 1$ for $i = 1, 2, \ldots, n$; and

(d) $\left(m, \frac{B_{f(n,j)+1}}{f(n, j) + 1}\right) = 1$ for at least one $j = 0, 1, 2, \ldots, n$, then $\left\{\dfrac{f(n, j) + 1}{B_{f(n, j)+1}}\right\}_{j=0}^{n}$ are all m-integers and $\left\{\dfrac{j+1}{B_{j+1}}\right\}_{j=0}^{\infty}$ is an e_n-sequence with natural shift $(\alpha(m), \beta(m), \gamma(m))$.

5. The Tangent Numbers

The *tangent numbers* $\{T_j\}_{j=0}^{\infty}$ are defined by the generating function

$$\tan x = \sum_{j=0}^{\infty} \frac{T_j x^j}{j!}. \tag{33}$$

It is well known that $T_{2j} = 0$, $j \geq 0$, and

$$T_{2n-1} = (-1)^{n-1} 4^n (4^n - 1)\frac{B_{2n}}{2n} \text{ is a positive integer.} \tag{34}$$

For a discussion of these numbers, see [12], page 273. Theorem 4 together with these observations gives

Theorem 10: Let $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$ with $m_1, m_2, \ldots, m_t$ natural numbers be an odd number and suppose

$$f(n, j) = (n - j)r\alpha_1(m) + r\beta_1(m)j + \gamma(m) \geq 1$$

for $0 \leq j \leq n$, $r \geq 0$, and $\gamma(m) \geq 0$. Then $\{(-1)^{(j-1)/2}\, T_j\}_{j \text{ odd}}$ is an e_n-sequence with the natural shift $(r\alpha_1(m), r\beta_1(m), \gamma(m))$.

6. Miscellaneous Results

A formula analogous to (12) for Bernoulli polynomials is

$$\sum_{i=1}^{N} i^n = \frac{1}{n+1}(B_{n+1}(N+1) - B_{n+1}), \tag{35}$$

where both n and N are natural numbers (see [16], page 26). Let

$$f(n, j) = f_j = (n - j)r\alpha_1(m) + r\beta_1(m) + \gamma(m),$$

where $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$ and $m_1, m_2, \ldots, m_t$ are natural numbers. In (35), replace n by f_j (so that $f_j \geq 0$) and to this apply the operator

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j}$$

so that

$$\sum_{i=1}^{N} \sum_{j=0}^{n} (-1)^i \binom{n}{j} i^{f_j} = \sum_{j=0}^{n} (-1)^j \binom{n}{j} \left[\frac{B_{f_j+1}\ (N+1) - B_{f_j+1}}{f_j+1}\right]. \tag{36}$$

Using Theorem 1, this implies

Theorem 11: Let $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$ with $m_1, m_2, \ldots, m_t$ natural numbers, and let

$$f_j = f(n, j) = (n - j)r\alpha_1(m) + r\beta_1(m) + \gamma(m) \geq 1$$

for $0 \leq j \leq n$, $r \geq 0$, and $\gamma(m) \geq 0$. If x is an m-integer, then

$$\left\{\frac{B_{f_j+1}(x) - B_{f_j+1}}{f_j + 1}\right\}_{j=0}^{\infty}$$

are all m-integers and

$$\left\{\frac{B_{j+1}(x) - B_{j+1}}{j+1}\right\}_{j=0}^{\infty}$$

is an e_n-sequence with the natural shift $(\alpha(m), \beta(m), \gamma(m))$. Here, n is a natural number.

Now $B_{2k+1} = 0$ for $k = 1, 2, 3, \ldots$, so that, if $f(n, j) + 1 \geq 3$ is an odd number, then

$$\left\{\frac{B_{f(n,j)+1}}{f(n, j) + 1}\right\}_{j=0}^{n} \text{ are all } m\text{-integers and } \left\{\frac{B_{j+1}(x)}{j + 1}\right\}_{j=0}^{n} \text{ is an } e_n\text{-sequence.}$$

With these observations, Theorems 11 and 7 yield

Theorem 12: Let $m = \mathrm{LCM}[m_1, m_2, \ldots, m_t] > 1$ with $m_1, m_2, \ldots, m_t$ natural numbers, and suppose

$$f(n, j) = (n - j)r\alpha_1(m) + r\beta_1(m) + \gamma(m) \geq 1$$

for $0 \leq j \leq n$, $r \geq 0$, and $\gamma(m) \geq 0$. Suppose also that x is an m-integer. If $f(n, j) + 1 \geq 3$ and $f(n, j)$ is even for $0 \leq j \leq n$, or if

$$\mathrm{GCD}\left(m, 2^{ir\alpha_1(m)+\gamma(m)+1} - 1\right) = 1 \text{ or, equivalently, } \mathrm{GCD}\left(m, 2^{ir\beta_1(m)+\gamma(m)+1} - 1\right) = 1$$

for $1 \leq i \leq n$, then

$$\left\{\frac{B_{f(n,j)+1}(x)}{f(n, j) + 1}\right\}_{j=0}^{\infty} \text{ are all } m\text{-integers}$$

and

$$\left\{\frac{B_{j+1}(x)}{j + 1}\right\}_{j=0}^{\infty}$$

is an e -sequence with natural shift $(r\alpha_1(m), r\beta_1(m), \gamma(m))$. Here, n is a natural number.

Varieties using these results can easily be made. For example, in Theorem 12, since x is an m-integer, $-x$ is also an m-integer, and it follows that

$$\left\{\frac{B_{j+1}(x) - B_{j+1}(-x)}{j + 1}\right\}_{j=0}^{\infty}$$

is an e_n-sequence. Here, the even powers of x are missing since

$$\frac{B_{j+1}(x) - B_{j+1}(-x)}{j + 1}$$

is an odd function of x. By the same reasoning

$$\left\{\frac{B_{j+1}(x) + B_{j+1}(-x)}{j + 1}\right\}_{j=0}^{\infty}$$

is an e_n-sequence. Here, the odd powers of x are missing since

$$\frac{B_{j+1}(x) + B_{j+1}(-x)}{j + 1}$$

is an even function of x. Similar remarks can, of course, be made concerning the Euler polynomials.

7. Binomial Rings

As has been seen, the Product Theorem allows for various combinations involving e-sequences. This will now be investigated.

Definition 5: A sequence $\{w_j\}_{j=0}^{\infty}$ is said to be *well behaved to* k where k is a natural number with respect to $m > 1$ and α and β integers provided for every natural number $n \leq k$ it is an e_{n-i}-sequence with shift $(\alpha, \beta, \beta i + \gamma)$ for $i = 0, 1, 2, \ldots, n - 1$ and it is an e_i-sequence with shift $(\alpha, \beta, (n - i)\alpha + \gamma)$

for $i = 1, 2, \ldots, n$ where the conditions to be a shift are satisfied in each instance and γ is arbitrary. This means that γ is chosen from the set of all integers S which is such that if $\gamma_0 \in S$, $\beta i + \gamma_0 \in S$ for $i = 0, 1, 2, \ldots, n - 1$ and $(n - i)\alpha + \gamma_0 \in S$ for $i = 1, 2, \ldots, n$ and the shift conditions are satisfied for all values $\gamma \in S$ for the given values α and β.

Note that if $\{w_j\}_{j=0}^{\infty}$ is a well-behaved sequence to k and if $k_1 < k$ is any natural number, then $\{w_j\}_{j=0}^{\infty}$ is also well behaved to k_1. When the phrase "$\{w_j\}_{j=0}^{\infty}$ is a well-behaved sequence" is used, it will be supposed "to arbitrary k a natural number." Unless otherwise stated, the shift that will be used for well-behaved sequences is $(r\alpha_1(m), r\beta_1(m), \gamma(m))$ where r and $\gamma(m)$ are whole numbers.

One of the examples of a well-behaved sequence for any k a natural number that has been given is the sequence $\{E_j\}_{j=0}^{\infty}$ of Euler numbers with the shift $(r\alpha_1(m), r\beta_1(m), \gamma(m))$ for r a fixed whole number and γ an arbitrary whole number with $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$ with $m_1, m_2, \ldots, m_t$ natural numbers.

It is clear by the Product Theorem that the "product"

$$(\{u_j\}_{j=0}^{\infty}\{v_j\}_{j=0}^{\infty} = \{u_j v_j\}_{j=0}^{\infty})$$

of well-behaved sequences all with respect to m, $\alpha(m)$ and $\beta(m)$ is also a well-behaved sequence. Indeed, it is this that motivated Definition 5.

Definition 6: Let k, $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$ and $m_1, m_2, \ldots, m_t$ be natural numbers. Let

$$R\binom{k}{m} = \{(x_0, x_1, \ldots, x_k) \mid x_0, x_1, \ldots, x_k \text{ are all } m\text{-integers}\}$$

and suppose

$$(x_0, x_1, \ldots, x_k), (y_0, y_1, \ldots, y_k) \in R\binom{k}{m}.$$

Then

(a) $(x_0, x_1, \ldots, x_k) = (y_0, y_1, \ldots, y_k)$ provided $x_i \equiv y_i \pmod{m^k}$ for $0 \le i \le k$;

(b) $(x_0, x_1, \ldots, x_k) + (y_0, y_1, \ldots, y_k) = (x_0 + y_0, x_1 + y_1, \ldots, x_k + y_k)$;

(c) $(x_0, x_1, \ldots, x_k) \cdot (y_0, y_1, \ldots, y_k) = (x_0 y_0, x_1 y_1, \ldots, x_k y_k)$;

(d) If α is any m-integer, $\alpha(x_0, x_1, \ldots, x_k) = (\alpha x_0, \alpha x_1, \ldots, \alpha x_k)$;

(e) Let n be any integer. If $x_1^n, x_2^n, \ldots, x_k^n$ all exist $\pmod{m^k}$, then $(x_0, x_1, \ldots, x_k)^n = (x_0^n, x_1^n, \ldots, x_k^n)$.

It is clear that $R\binom{k}{n}$ is a commutative ring with identity $e = (1, 1, \ldots, 1)$. $R\binom{k}{m}$ is called the ring of $(k + 1)$-*tuples of m-integers* $\pmod{m^k}$ and, furthermore, by the Product Theorem, there exist subrings $B\binom{k}{m}$ of $R\binom{k}{m}$ such that if $(x_0, x_1, \ldots, x_k) \in B\binom{k}{m}$ then

$$\sum_{j=0}^{k} (-1)^i \binom{k}{j} x_j \equiv 0 \pmod{m^k}. \tag{37}$$

Any such subring of $R\binom{k}{m}$ is called a *binomial ring*.

Let $\{w_j\}_{j=0}^{\infty}$ be a well-behaved sequence. It is clear that

$$(w_{f(k,0)}, w_{f(k,1)}, \ldots, w_{f(k,k)})$$

generates a binomial ring. These observations establish

Theorem 13: Let $\{x_{ij}\}_{j=0}^{\infty}$ for $1 \le i \le t$ all be well-behaved sequences to k with respect to $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$ and fixed $\alpha(m)$ and $\beta(m)$. Let $g(x_1, x_2, \ldots, x_t)$ be a polynomial with m-integer coefficients. Let $y_{ij} = x_{if(k,j)}$. Then

$(g(y_{10}, y_{20}, \ldots, y_{t0}), g(y_{11}, y_{21}, \ldots, y_{t1}), \ldots, g(y_{1k}, y_{2k}, \ldots, y_{tk}))$ is an element of a binomial ring.

Definition 7: An element $(x_0, x_1, \ldots, x_k) \in R\binom{k}{m}$ is said to be *principal* provided $(x_0x_1 \ldots x_k, m) = 1$.

It is clear that if $x = (x_0, x_1, \ldots, x_k)$ is a principal element of $R\binom{k}{m}$, then $\{x, x^2, x^3, \ldots\}$ is a cyclic group under multiplication. Furthermore, it is the principal elements that have multiplicative inverses.

Suppose that $\{w_j\}_{j=0}^{\infty}$ is a well-behaved sequence to k with respect to $m = \text{LCM}[m_1, m_2, \ldots, m_t] > 1$, $\alpha(m)$, and $\beta(m)$. Suppose also that $\{a_i\}$, $\{b_i\}$, and $\{i_q\}$ are all sequences of whole numbers. Then $\{w_{j+b_{i_q}}\}_{j=0}^{\infty}$ is a well-behaved sequence to k. Let α_i, β_i, c_i, d, and g_i be any m-integers. It follows that

$$\left\{\left(\left(\sum_i \prod_q \left(a_{i_q}^j b_{i_q} w_{j+b_{i_q}}^{a_{iq}} + g_i\right)\right) + d + fc_i\right)^n\right\}_{j=0}^{\infty} \tag{38}$$

is well behaved to k with respect to m, α, and β. Here, the sum and the product are finite and $f \equiv 0 \pmod{m^k}$. Other variations besides (38) can, of course, be given.

As has been seen, $\{E_j\}_{j=0}^{\infty}$ is well behaved to any k a natural number for $m > 1$ an odd number with shift $(r\alpha_1(m), r\beta_1(m), \gamma(m))$ for r and $\gamma(m)$ whole numbers.

As an example of a binomial ring constructed from the Euler numbers, let $m = 5 = \text{LCM}[5]$ and $k = 3$. Here, using the natural shift

$$f(3, j) = (3 - j)r(\phi(5) + h(5)]^g + r[h(5)]^g j + \gamma(5)$$
$$= (3 - j)5 + j + 1 = 16 - 4j,$$

where $r = g = \gamma = 1$. Here, γ was chosen to be 1 since, for even γ, the corresponding Euler number is 0, and this is trivial. Other choices can, of course, be made for r, g, and $\gamma(m)$. For the above choices,

$$E_{16} = 1\ 9\ 3\ 9\ 1\ 5\ 1\ 2\ 1\ 4\ 5 \equiv 20 \pmod{5^3},$$
$$E_{12} = 2\ 7\ 0\ 2\ 7\ 6\ 5 \equiv 15 \pmod{5^3},$$
$$E_8 = 1\ 3\ 8\ 5 \equiv 10 \pmod{5^3},$$
$$E_4 = 5 \equiv 5 \pmod{5^3}.$$

Thus,

$$(20, 15, 10, 5) \text{ is a member of a binomial ring } B\binom{3}{5}.$$

Since (x, x, x, x) is also a member, it follows that

$$(20 + x)^n - 3(15 + x)^n + 3(10 + x)^n - (5 + x)^n \equiv 0 \pmod{125}$$

for n any whole number and x any integer.

To construct another element of such a $B\binom{3}{5}$, let $r = g = 1$ and $\gamma = 3$. Then $f(3, j) = 18 - 4j$, so that

$$E_{18} = -2\ 4\ 0\ 4\ 8\ 7\ 9\ 6\ 7\ 5\ 4\ 4\ 1 \equiv 59 \pmod{125},$$
$$E_{14} = -1\ 9\ 9\ 3\ 6\ 0\ 9\ 8\ 1 \equiv 19 \pmod{125},$$
$$E_{10} = -5\ 0\ 5\ 2\ 1 \equiv 104 \pmod{125},$$
$$E_6 = -6\ 1 \equiv 64 \pmod{125}.$$

Thus,

$$(59, 19, 104, 64) \text{ is a member of a } B\binom{3}{5}.$$

Combining this with the previous element, for x and y any integers, m and n any whole numbers,

$$(20+x)^m(59+y)^n - 3(15+x)^m(19+y)^n + 3(10+x)^m(104+y)^n - (5+x)^m(64+y)^n \equiv 0 \pmod{125}.$$

This can actually be made a little stronger. If

$$(20+x,\ 15+x,\ 10+x,\ 5+x) \text{ and } (59+y,\ 19+y,\ 104+y,\ 64+y)$$

are both principal, then m and n can be any integers.

8. Some Additional Results with $(\bmod\{\mathrm{LCM}[m_1, m_2, \ldots, m_t]\}^n)$

The examples in this paper have been concerned with congruences $(\bmod\ m^n)$. The case, with $m = p = \mathrm{LCM}[p]$ and p a prime number, is, of course, well known in connection with Kummer's congruences. Some additional examples will be given here.

The natural shift $(\alpha(m), \beta(m), \gamma(m))$ with $m = \mathrm{LCM}[m_1, m_2, \ldots, m_t]$ will be used. Here

(39) $$\alpha(m) = r\alpha_1(m),\ \beta(m) = r\beta_1(m),$$

with

(40) $$\alpha_1(m) = r_1[\phi(m_1) + h(m_t)]^{g_1} + s_1 = r_2[\phi(m_2) + h(m_2)]^{g_2} + s_2 = \cdots = r_t[\phi(m_t) + h(m_t)]^{g_t} + s_t$$

and

(41) $$\beta_1(m) = r_1[h(m_1)]^{g_1} + s_1 = r_2[h(m_2)]^{g_2} + s_2 = \cdots = r_t[h(m_t)]^{g_t} + s_t,$$

for some integers $r_1, r_2, \ldots, r_t, s_1, s_2, \ldots, s_t$, and some natural numbers $g_1, g_2, \ldots, g_t$. As was remarked earlier, special care is needed for any of the r's or s's to be negative. It will be supposed that $\alpha_1(m)$, $\beta_1(m)$, $r \neq 0$ and $\alpha_1(m) \neq \beta_1(m)$ to keep the results from being trivial.

First, an example using Theorem 3 will be given. Let $m = 15 = \mathrm{LCM}[3, 5]$ and $n = 3$. In this case, $\phi(3) = 2$ and $\phi(5) = 4$ so that $r_1, r_2;\ s_1, s_2;\ g_1, g_2$ are required such that

(42) $$r_1[2+1]^{g_1} + s_1 = r_2[4+1]^{g_2} + s_2 \text{ and } r_1 \cdot 1^{g_1} + s_1 = r_2 \cdot 1^{g_2} + s_2.$$

Clearly, a choice is $r_1 = 2$, $r_2 = 1$; $s_1 = 0$, $s_2 = 1$; $g_1 = g_2 = 1$ and $r = 1$ so that $\alpha(m) = 6$ and $\beta(m) = 2$ so that $f(3, j) = (3 - j)\cdot 6 + 2j + \gamma = 18 - 4j + \gamma$ so that Theorem 3 gives

(43) $$\sum_{j=0}^{3} (-1)^i \binom{3}{j} E_{18-4j+\gamma} \equiv 0 \pmod{15^3} \text{ where } \gamma \text{ is a whole number.}$$

Evidently, other choices for $r_1, r_2, s_1, s_2, g_1, g_2$ in (41) can be made.

On the other hand, if $m = 15 = \mathrm{LCM}[15]$, then

$$f(3, j) = (3 - j)r[\phi(15) + h(15)]^g + r[h(15)]^g_j + \gamma.$$

Let $r = g = 1$ so that

$$f(3, j) = (3 - j)(9) + j + \gamma = 27 - 8j + \gamma$$

and

(44) $$\sum_{j=0}^{3} (-1)^i \binom{3}{j} E_{27-8j+\gamma} \equiv 0 \pmod{15^3}.$$

An example using Theorem 7 is given by $m = 35 = \mathrm{LCM}[5, 7]$. Here, $\phi(5) = 4$, $h(5) = 1$, $\phi(7) = 6$, and $h(7) = 1$ so that r_1, r_2, s_1, and s_2 are needed such that

(45) $$5r_1 + s_1 = 7r_2 + s_2,\quad r_1 + s_1 = r_2 + s_2. \quad \text{(Here, } g_1 = g_2 = 1.)$$

A choice for these numbers is $r_1 = 3$, $r_2 = 2$, $s_1 = 0$, and $s_2 = 1$. This gives $\alpha_1(m) = 15$ and $\beta_1(m) = 3$. Choose $r = 1$. From Theorem 7, it is required that $(35, 2^{3+\gamma+1} - 1) = 1$ and $(1 - j)15 + 3j + \gamma + 1$ is even. In this case, $n = 1$. A choice for $\gamma = \gamma(m)$ satisfying this is $\gamma = 6$. Thus, Theorem 7 says that

$$\left\{\frac{B_{22-12j}}{22 - 12j}\right\}_{j=0}^{1} \text{ are both 35-integers and } \sum_{j=0}^{1}(-1)^j\binom{1}{j}\frac{B_{22-12j}}{22 - 12j} \equiv 0 \pmod{35}.$$

Notice that another congruence (mod 35) can easily be given by letting $m = 35 = \text{LCM}[35]$. In this case, $\phi(35) = 24$ and $h(35) = 1$. Thus, a choice of $\alpha(35) = 25$ and $\beta(35) = 1$. To satisfy the hypothesis of Theorem 7, it is required that $(35, 2^{1+\gamma+1} - 1) = 1$ and $(1 - j)\cdot 25 + j + \gamma + 1 = 26 - 24j +$ be even. $\gamma = 0$ works. Thus, according to Theorem 7,

$$\left\{\frac{B_{26-24j}}{26 - 24j}\right\}_{j=0}^{1} \text{ are 35-integers and } \sum_{j=0}^{1}(-1)^j\binom{1}{j}\frac{B_{26-24j}}{26 - 24j} \equiv 0 \pmod{35}.$$

More generally, let a and b be natural numbers such that $m = \text{LCM}[a, b] > 1$ is odd. Then it is required to find r_1, r_2, s_1, s_2, for $g_1 = g_2 = 1$ such that

$$\begin{aligned} &r_1[\phi(a) + h(a)] + s_1 = r_2[\phi(b) + h(b)] + s_2, \\ &r_1 h(a) + s_1 = r_2 h(b) + s_2. \end{aligned} \tag{46}$$

A choise for r_1 and s_1 satisfying this is

$$r_1 = \frac{\text{LCM}[\phi(a),\ \phi(b)]}{\phi(a)} \text{ and } s_1 = 0.$$

For this choice,

$$\alpha(m) = \frac{r\ \text{LCM}[\phi(a),\ \phi(b)][\phi(a) + h(a)]}{\phi(a)}$$

and

$$\beta(m) = \frac{r\ \text{LCM}[\phi(a),\ \phi(b)]h(a)}{\phi(a)},$$

so that, by Theorem 7, if

$$\left(\text{LCM}[a,\ b],\ 2^{\frac{ir\ \text{LCM}[\phi(a),\ \phi(b)]\ h(a)}{\phi(a)} + \gamma + 1} - 1\right) = 1 \quad \text{for } i = 1, 2, 3, \ldots, n,$$

then

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}\frac{B_{\left\{r\,\text{LCM}[\phi(a),\,\phi(b)]j + \frac{nr\ \text{LCM}[\phi(a),\,\phi(b)]\ h(a)}{\phi(a)} + \gamma + 1\right\}}}{r\ \text{LCM}[\phi(a),\ \phi(b)]j + \dfrac{nr\ \text{LCM}[\phi(a),\ \phi(b)]h(a)}{\phi(a)} + \gamma + 1} \tag{48}$$

$$\equiv 0 \pmod{\{\text{LCM}[a,\ b]\}^n}. \quad [\text{Here, } \gamma = j(m)].$$

Notice that since there exist a and b such that

$$\text{LCM}[\phi(a),\ \phi(b)] \neq \phi(\text{LCM}[a,\ b])$$

(for example, $a = 15$ and $b = 35$) it follows that (48) is essentially different from what would be obtained simply by letting $m = \text{LCM}[m]$ for $m = \text{LCM}[a, b]$.

The reader might enjoy examining the congruences obtained from

$$\begin{aligned} m &= 105 = \text{LCM}[105] = \text{LCM}[3, 5, 7] = \text{LCM}[15, 7] = \text{LCM}[21, 5] \\ &= \text{LCM}[3, 35] = \text{LCM}[15, 35] = \text{LCM}[21, 35] = \text{LCM}[15, 21] \end{aligned}$$

for these various LCM-partitions of 105.

Acknowledgment

The author would like to thank an anonymous referee for numerous helpful suggestions.

References

1. Z. I. Borevich & I. R. Shafarevial. *Number Theory*. New York and London: Academic Press, 1966.
2. L. Carlitz. "Some Congruences for the Bernoulli Numbers." *Amer. J. Math.* *75* (1953):163-71.
3. L. Carlitz. "Some Theorems on Kummer's Congruences." *Duke Math. J. 20* (1953):423-31.
4. L. Carlitz. "Kummer's Congruence for the Bernoulli Numbers." *Portegaliae Mathematica 19* (1960):203-10.
5. L. Carlitz. "An Extension of the Fermat Theorem." *Amer. Math. Monthly 70* (1963):247-50.
6. L. Carlitz. "Some Unusual Congruences for the Bernoulli and Genocchi Numbers." *Duke Math. J. 35.3* (1968):563-66.
7. D. G. Duncan. "A Generalization of the Euler-Fermat Theorem." *Amer. Math. Monthly 62* (1955):241.
8. H. M. Edwards. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*. Berlin: Springer-Verlag, 1977.
9. A. Eker. "Comment on the Note: 'The Congruence $a^{r+s} \equiv a^r \pmod{m}$' by A. E. Livingston and M. L. Livingston." *Amer. Math. Monthly 87* (1980):811-14.
10. T. Fort. *Finite Differences and Difference Equations in the Real Domain*. Oxford: At the Clarendon Press, 1948.
11. F. S. Gillespie. "A Generalization of Fermat's Little Theorem." *Fibonacci Quarterly 27.2* (1989):109-15.
12. R. L. Graham, D. E. Knuth, & O. Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. New York: Addison-Wesley, 1989.
13. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin, 1969.
14. D. H. Lehmer. "Lacunary Recurrence Formulas for the Numbers of Bernoulli and Euler." *Annals of Math. 36.3* (1935):637-49.
15. A. E. Livingston & M. L. Livingston. "The Congruence $a^{r+s} \equiv a^r \pmod{m}$." *Amer. Math. Monthly 85* (1978):97-100.
16. W. Magnus, F. Oberbettinger, & R. P. Soni. *Formulas and Theorems for the Special Functions of Mathematical Physics*. New York: Springer-Verlag, 1966.
17. L. J. Mordell. *Three Lectures on Fermat's Last Theorem*. New York: Chelsea, 1962.
18. P. Ribenboim. *13 Lectures on Fermat's Last Theorem*. New York: Springer-Verlag, 1979.
19. K. H. Rosen. *Elementary Number Theory and Its Applications*. 2nd ed. New York: Addison-Wesley, 1988.
20. D. Shanks. *Solved and Unsolved Problems in Number Theory*. New York: Chelsea, 1985.
21. J. Spanier & K. B. Oldham. *An Atlas of Functions*. New York: Hemisphere Publishing, 1987.
22. H. R. Stevens. "Bernoulli Numbers and Kummer's Criterion." *Fibonacci Quarterly 24.2* (1986):154-59.
23. J. V. Uspensky & M. A. Heaslet. *Elementary Number Theory*. New York: McGraw-Hill, 1939.

24. H. S. Vandiver. "Certain Congruences Involving the Bernoulli Numbers." *Duke Math. J.* 5 (1939):548-51.
25. H. S. Vandiver. "On Developments in an Arithmetic Theory of the Bernoulli and Allied Numbers." *Scripta Math.* 25 (1961):273-303.
26. L. C. Washington. *Introduction to Cyclotomic Fields*. New York: Springer-Verlag, 1982.

AMS Classification numbers: 11B68, 11B48, 11B80

*****

Continued from page 334

Our home during the Conference was a University dormitory. John Burnet Hall, formerly a hotel, and still providing the comfort of such. Colleges and Universities have the reputation of offering dull, institutionalized fare. Our food, taken at the dorm's cafeteria, constituted an enjoyable counterexample.

St Andrews is an ancient institution. And during its nearly six centuries of existence, it has maintained vigorous scholarly impact across the whole academic spectrum. St. Andrews has been called "a gem of a University"—uniquely Scottish by history and beautiful location, yet unusually cosmopolitan.

The Conference's social events rounded off, and enhanced, our academic sessions. The traditional mid-conference's afternoon excursion took us to Falkland, a Renaissance Palace, which grew out of the medieval Falkland Castle. At once did we get lured into the quaintness of an historically rich palace and became enchanted by the charming multi-coloredness of the garden.

To convey the congenial and happy atmosphere at our Conference—dinner adequately would require a vocabulary far richer than mine. Interspersed with inspirational short talks and remarks, animated by delicious banquet fare and, most of all, by having our whole group gathered together, it was simply delightful.

And, finally, the Conference itself.

Erudite and always carefully prepared papers ranged over the heights and depths of "purity" and "applicability," once more illustrating the startling way in which these two facets of mathematics are duals of each other. And while we speak with many different accents, we understand each other on a much more significant level. Almost immediately, friendships blossomed or ripened, as the love of our discipline and the enthusiasm for it were written over all the faces of the "Fibonaccians" as some of us like to refer to ourselves. That one week in Scotland, kindled by the serenity of the Scottish landscape and enhanced by the spirit of our Scottish hosts and co-mathematicians, gave us experiences which were both mentally enriching and personally heartwarming.

Finally, it was "farewell." But it is with much happiness that we can say: "*Auf Wiedersehen* in two years at Pullman, Washington."

*****

ELEMENTARY PROBLEMS AND SOLUTIONS

Edited by

Stanley Rabinowitz

Please send all material for ELEMENTARY PROBLEMS AND SOLUTIONS to Dr. STANLEY RABINOWITZ; 12 VINE BROOK RD; WESTFORD, MA 01886-4212 USA. Correspondence may also be sent to the problem editor by electronic mail to 72717.3515@compuserve.com *on Internet. All correspondence will be acknowledged.*

Each solution should be on a separate sheet (or sheets) and must be received within six months of publication of the problem. Solutions typed in the format used below will be given preference. Proposers of problems should normally include solutions.

Dedication. This year's column is dedicated to **Dr. A. P. Hillman** in recognition of his 27 years of devoted service as editor of the Elementary Problems Section.

BASIC FORMULAS

The Fibonacci numbers F_n and the Lucas numbers L_n satisfy

$$F_{n+2} = F_{n+1} + F_n,\ F_0 = 0,\ F_1 = 1;$$

$$L_{n+2} = L_{n+1} + L_n,\ L_0 = 2,\ L_1 = 1.$$

Also, $\alpha = (1 + \sqrt{5})/2$, $\beta = (1 - \sqrt{5})/2$, $F_n = (\alpha^n - \beta^n)/\sqrt{5}$, and $L_n = \alpha^n + \beta^n$.

PROBLEMS PROPOSED IN THIS ISSUE

B-724 *Proposed by Larry Taylor, Rego Park, NY*

Dedicated to Dr. A. P. Hillman

Let n be a positive integer. Prove that the numbers $L_{n-1}L_{n+1}$, $5F_n^2$, L_{3n}/L_n, L_{2n}, F_{3n}/F_n, L_n^2, $5F_{n-1}F_{n+1}$ are in arithmetic progression and find the common difference.

B-725 *Proposed by Russell Jay Hendel, Patchogue, NY and Herta T. Freitag, Roanoke, VA*

Dedicated to Dr. A. P. Hillman

(a) Find an infinite set of right triangles each of which has a hypotenuse whose length is a Fibonacci number and an area that is the product of four Fibonacci numbers.

(b) Find an infinite set of right triangles each of which has a hypotenuse whose length is the product of two Fibonacci numbers and an area that is the product of four Lucas numbers.

B-726 *Proposed by Florentin Smarandache, Phoenix, AZ*

Dedicated to Dr. A. P. Hillman

Let $d_n = P_{n+1} - P_n$, $n = 1, 2, 3, \ldots$, where P_n is the n^{th} prime. Does the series

$$\sum_{n=1}^{\infty} \frac{1}{d_n}$$

converge?

B-727 *Proposed by Ioan Sadoveanu, Ellensburg, WA*

Dedicated to Dr. A. P. Hillman

Find the general term of the sequence (a_n) defined by the recurrence

$$a_{n+2} = \frac{a_{n+1} + a_n}{1 + a_{n+1}a_n}$$

with initial values $a_0 = 0$ and $a_1 = (e^2 - 1)/(e^2 + 1)$, where e is the base of natural logarithms.

B-728 *Proposed by Leonard A. G. Dresel, Reading, England*

Dedicated to Dr. A. P. Hillman

If $p > 5$ is a prime and n is an even integer, prove that

(a) if $L_n \equiv 2 \pmod{p}$, then $L_n \equiv 2 \pmod{p^2}$;
(b) if $L_n \equiv -2 \pmod{p}$, then $L_n \equiv -2 \pmod{p^2}$.

B-729 *Proposed by Lawrence Somer, Catholic University of America, Washington, D.C.*

Dedicated to Dr. A. P. Hillman

Let (H_n) denote the second-order recurrence defined by

$$H_{n+2} = aH_{n+1} + bH_n,$$

where $H_0 = 0$, $H_1 = 1$, and a and b are integers. Let p be a prime such that $p \nmid b$. Let k be the least positive integer such that $H_k \equiv 0 \pmod{p}$. (It is well-known that k exists.) If $H_n \not\equiv 0 \pmod{p}$, let $R_n \equiv H_{n+1}H_n^{-1} \pmod{p}$.

(a) Show that $R_n + R_{k-n} \equiv a \pmod{p}$ for $1 \le n \le k - 1$.
(b) Show that $R_nR_{k-n-1} \equiv -b \pmod{p}$ for $1 \le n \le k - 2$.

Acknowledgment

The editor of Elementary Problems and Solutions wishes to thank Clark Kimberling for his help in proofreading material for this section.

SOLUTIONS

A Radical Limit

B-698 *Proposed by Richard André-Jeannin, Sfax, Tunisia*

Consider the sequence of real numbers $a_1, a_2, \ldots$, where $a_1 > 2$ and

(1) $$a_{n+1} = a_n^2 - 2 \quad \text{for } n \ge 1.$$

Find $\lim\limits_{n\to\infty} b_n$, where

(2) $$b_n = \frac{a_{n+1}}{a_1a_2\ldots a_n} \quad \text{for } n \ge 1.$$

Solution 1 by Hans Kappus, Rodersdorf, Switzerland

We claim that

$$\lim_{n\to\infty} b_n = \sqrt{a_1^2 - 4}.$$

This follows from the formula

$$b_n^2 = \frac{(a_1^2 - 4)a_{n+1}^2}{a_{n+1}^2 - 4} \tag{3}$$

and the obvious fact that $\{a_n\}$ is an increasing sequence so $\lim_{n\to\infty} a_n = \infty$.

To prove (3), we proceed by mathematical induction. We have

$$b_1^2 = \frac{a_2^2}{a_1^2} = \frac{(a_1^2 - 4)a_2^2}{(a_1^2 - 4)a_1^2} = \frac{(a_1^2 - 4)a_2^2}{(a_1^2 - 2)^2 - 4} = \frac{(a_1^2 - 4)a_2^2}{a_2^2 - 4}$$

so formula (3) is true for $n = 1$. Assume now that (3) holds for some integer $n = k - 1$. Then, from $b_k = b_{k-1}a_{k+1}/a_k^2$, we have

$$b_k^2 = \frac{b_{k-1}^2 a_{k+1}^2}{a_k^4} = \frac{(a_1^2 - 4)a_{k+1}^2}{(a_k^2 - 4)a_k} = \frac{(a_1^2 - 4)a_{k+1}^2}{(a_k^2 - 2)^2 - 4} = \frac{(a_1^2 - 4)a_{k+1}^2}{a_{k+1}^2 - 4},$$

which completes the induction.

Solution 2 by Ioan Sadoveanu, Ellensburg, WA

Using the recurrence relation in the form

$$a_{n+1} - a_n = (a_n + 1)(a_n - 2)$$

implies, by induction, that $a_{n+1} > a_n > 2$ for all $n \geq 1$.

Let x_n be defined by

$$a_n/2 = \cosh x_n. \tag{4}$$

This is possible since the hyperbolic cosine defined on $(0, \infty)$ and valued in $(1, \infty)$ is a one-to-one function.

We recall some facts concerning hyperbolic functions [1]:

$$\cosh z = \frac{e^z + e^{-z}}{2} \tag{5}$$

$$\sinh z = \frac{e^z - e^{-z}}{2} \tag{6}$$

$$\cosh^2 z - \sinh^2 z = 1 \tag{7}$$

$$\sinh 2z = 2 \sinh z \cosh z \tag{8}$$

$$\cosh 2z = 2 \cosh^2 z - 1 \tag{9}$$

$$\coth z = \frac{\cosh z}{\sinh z} \tag{10}$$

Applying (4) to (1) gives

$$2 \cosh x_n = (2 \cosh x_{n-1})^2 - 2$$

or

$$\cosh x_n = 2 \cosh^2 x_{n-1} - 1 = \cosh 2x_{n-1}$$

by (7). Thus, $x_n = 2x_{n-1}$. Repeated application of this formula yields

$$x_n = 2^{n-1}x_1.$$

Now

$$a_1 a_2 \cdots a_n = (2 \cosh x_1)(2 \cosh 2x_1) \cdots (2 \cosh 2^{n-1}x_1)$$

$$= \frac{\sinh 2x_1}{\sinh x_1} \frac{\sinh 4x_1}{\sinh 2x_1} \cdots \frac{\sinh 2^n x_1}{\sinh 2^{n-1}x_1} = \frac{\sinh 2^n x_1}{\sinh x_1}$$

using (6) and cancelling. Therefore,

$$b_n = \frac{a_{n+1}}{a_1 a_2 \cdots a_n} = \frac{\sinh x_1 (2 \cosh x_{n+1})}{\sinh 2^n x_1}$$

$$= \frac{\sinh x_1}{\sinh x_{n+1}}(2 \cosh x_{n+1}) = 2 \sinh x_1 \coth x_{n+1}.$$

But

$$\lim_{x \to \infty} \coth x = \lim_{x \to \infty} \frac{e^x + e^{-x}}{e^x - e^{-x}} = \lim_{x \to \infty} \frac{1 + \frac{1}{e^{2x}}}{1 - \frac{1}{e^{2x}}} = \frac{1 + 0}{1 - 0} = 1.$$

Thus,

$$\lim_{n \to \infty} b_n = 2 \sinh x_1 \lim_{n \to \infty} \coth x_{n+1} = 2 \sinh x_1$$

$$= 2\sqrt{\cosh^2 x_1 - 1} = \sqrt{4 \cosh^2 x_1 - 4} = \sqrt{a_1^2 - 4}.$$

Reference

1. Abramowitz & Stegun. *Handbook of Mathematical Functions*. National Bureau of Standards, Washington, DC, 1966.

Also solved by Paul S. Bruckman, Blagoj S. Popov, and the proposer.

A Solution Using Periodic Orbits

B-699 *Proposed by Larry Blaine, Plymouth State College, Plymouth, NH*

Let a be an integer greater than 1. Define a function $p(n)$ by

$$p(1) = a - 1 \quad \text{and} \quad p(n) = a^n - 1 - \sum p(d) \quad \text{for } n \geq 2,$$

where $\sum$ denotes the sum over all d with $1 \leq d < n$ and $d|n$.

Prove or disprove that $n|p(n)$ for all positive integers n.

Solution by the proposer

Consider the function $f:[0, 1) \to [0, 1)$ defined by

$$f(x) \equiv ax \pmod 1,$$

i.e.,

$$f(x) = ax - k \text{ for } k/a \leq x < (k + 1)/a, \; k = 0, 1, \ldots, a - 1.$$

We use the customary notation

$$f^1(x) = f(x), \quad f^{n+1}(x) = f(f^n(x)) \quad \text{for } n = 1, 2, \ldots,$$

and for $x \in [0, 1)$ we define the orbit of x to be the sequence

$$x_0 = x, \quad x_n = f^n(x) \quad \text{for } n = 1, 2, \ldots .$$

We say that x is an n-periodic point if $x_0 = x_n$, but $x_0 \neq x_i$ for $i = 1, 2, \ldots, n - 1$.

Now, if x is n-periodic, then $f^n(x) = x$. The converse is not quite true: $f^n(x) = x$ if and only if x is d-periodic for some positive integer d for which $d|n$ (including, of course, $d = 1$ and $d = n$). An easy calculation shows that there are exactly $a - 1$ 1-periodic points and $a^n - 1$ points for which $f^n(x) = x$. It follows by induction that $p(n)$ is the number of n-periodic points. Since these points fall into equivalence classes (periodic orbits) of the form $\{x_0, x_1, \ldots, x_{n-1}\}$, it follows that $n|p(n)$ in all cases.

Also solved by Paul S. Bruckman and Russell Jay Hendel.

The proposer asks whether a proof can be given using elementary number theoretic techniques. Although our two other solvers gave proofs using "elementary" number theory, their proofs were not as simple as the proposer's. Hendel's proof ran for three pages and Bruckman's proof involved the Möbius inversion formula and a generalized form of Fermat's Little Theorem.

But It Doesn't Look Symmetric

B-700 *Proposed by Herta T. Freitag, Roanoke, VA*

Prove that for positive integers m and n,

$$\alpha^m(\alpha L_n + L_{n-1}) = \alpha^n(\alpha L_m + L_{m-1}).$$

Solution by Paul S. Bruckman, Edmonds, WA

Let $f(m, n) = \alpha^m(\alpha L_n + L_{n-1})$. Using $\alpha\beta = -1$, we find that

$$\begin{aligned}\alpha L_n + L_{n-1} &= \alpha(\alpha^n + \beta^n) + \alpha^{n-1} + \beta^{n-1}\\ &= \alpha^{n+1} - \beta^{n-1} + \alpha^{n-1} + \beta^{n-1}\\ &= \alpha^n(\alpha - \beta) = \alpha^n\sqrt{5}.\end{aligned}$$

Therefore, $f(m, n) = \alpha^{m+n}\sqrt{5}$, from which we see that $f(m, n) = f(n, m)$.

Solvers found various methods of showing that $f(m, n)$ is symmetric:
Melham showed that $f(m, n) = \alpha^{m+n+1} + \alpha^{m+n-1}$.
Singh showed that $f(m, n) = \alpha^{m+n-1}(\alpha^2 + 1)$.
Brown notes that the result follows from problem B-538 ($\sqrt{5}\alpha^n = \alpha L_n + L_{n-1}$).
Haukkanen generalized by showing that the following are symmetric in m and n:

$$\beta^m(\beta L_n + L_{n-1}), \quad \alpha^m(\alpha F_n + F_{n-1}), \quad \beta^m(\beta F_n + F_{n-1}).$$

Also solved by Michel Ballieu, Brian D. Beasley, Glenn Bookhout, Scott H. Brown, Russell Euler, C. Georghiou, Pentti Haukkanen, Russell Jay Hendel, Joseph J. Kostal, Graham Lord, Ray Melham, Blagoj S. Popov, Bob Prielipp, H.-J. Seiffert, Sahib Singh, Lawrence Somer, and the proposer.

A Pair of Triangles with Common Sides

B-701 *Proposed by Herta T. Freitag, Roanoke, VA*

In triangles ABC and DEF, $AC = DF = 5F_{2n}$, $BC = L_{n+2}L_{n-1}$, $EF = L_{n+1}L_{n-2}$, and $AB = DE = 5F_{2n+1} - L_{2n+1} + (-1)^{n-1}$. Prove that $\angle ACB = \angle DFE$.

Solution by the proposer

Let $L_{n+1} = x$, $L_n = y$, $b = 5F_{2n}$, $c = AB$, $a = L_{n+2}L_{n-1}$, $d = L_{n+1}L_{n-2}$, $e = DF$, and $f = DE$. Since

$$L_{n+2}L_{n-1} = (L_{n+1} + L_n)(L_{n+1} - L_n),$$
$$5F_{2n} = 5F_nL_n = (L_{n+1} + L_{n-1})L_n = (2L_{n+1} - L_n)L_n,$$
$$L_{n+1}L_{n-2} = L_{n+1}(2L_n - L_{n+1}),$$

and

$$5F_{2n+1} - L_{2n+1} + (-1)^{n-1} = L_{2n} + L_{2n+2} - L_{2n+1} + (-1)^{n-1},$$

and where, furthermore,

$$L_{2n} + L_{2n+2} = L_{n+1}^2 + L_n^2 \quad \text{and} \quad L_{2n+1} + (-1)^n = L_{n+1}L_n,$$

we therefore have

$$a = x^2 - y^2, \quad b = y(2x - y) = e, \quad c = x^2 - xy + y^2 = f, \quad d = x(2y - x).$$

Now, using the Law of Cosines for triangle ABC, we find

$$\cos C = \frac{a^2 + b^2 - c^2}{2ab}.$$

However, $a^2 + b^2 - c^2 = 2x^3y - x^2y^2 - 2xy^3 + y^4 = ab$. Thus, $\cos C = 1/2$; hence $\angle C = \pi/3$.

Similarly, for triangle DEF,

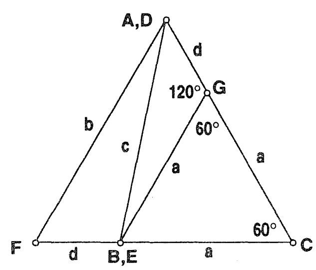
$$d^2 + e^2 - f^2 = -2x^3y + 5x^2y^2 - 2xy^3 = de,$$

from which we get $\cos F = 1/2$; hence $\angle F = \angle C = \pi/3$.

Comment by the editor:

With the same notation as in Solution 1, it is straightforward to show that $c^2 = a^2 + ad + d^2$ and $a + d = b$.

By the Law of Cosines, this tells us that there is a triangle ABG with sides of length $AB = c$, $BG = a$, and $GA = d$ and that $\angle AGB = 120°$.



Extend side AG past G for a distance a to the point C. Then, since $\angle BGC = 60°$, triangle BGC is equilateral and $BC = a$. Draw a line through A parallel to BG. and meeting CB extended at F. Thus, $\angle AFC = \angle GBC = 60°$; therefore, $\triangle AFC$ is also equilateral. Thus $BF = d$ and $AF = a + d = b$.

Giving labels D and E to points A and B, respectively, we thus see our two triangles ABC and DEF of the problem proposal and have also shown that $\angle ACB = \angle DFE = 60°$.

Also solved by Paul S. Bruckman, C. Georghiou, Russell Jay Hendel, Ray Melham, Bob Prielipp, and H.-J. Seiffert. A wonderful 6-page solution (with 7 lemmas) was also received, but the solver forgot to print his or her name on the solution sheets, so proper credit cannot be assigned.

A Comparison of Continued Fractions

B-702 *Proposed by L. Kuipers, Sierre, Switzerland*

For n a positive integer, let

$$x_n = F_n + \cfrac{1}{L_n + \cfrac{1}{F_n + \cfrac{1}{L_n + \ddots}}} \quad \text{and} \quad y_n = F_n + \cfrac{1}{F_{n+1} + \cfrac{1}{F_n + \cfrac{1}{F_{n+1} + \ddots}}}.$$

(a) Find closed form expressions for x_n and y_n.
(b) Prove that $x_n < y_n$ when $n > 1$.

Solution to part (a) by C. Georghiou, University of Patras, Patras, Greece

Assuming convergence, we have

$$x_n = F_n + \cfrac{1}{L_n + \cfrac{1}{x_n}} \quad \text{and} \quad y_n = F_n + \cfrac{1}{F_{n+1} + \cfrac{1}{y_n}}.$$

Solving these equations for x_n and y_n, respectively, we find

$$x_n = \frac{F_n}{2}\left[1 + \sqrt{1 + \frac{4}{F_nL_n}}\right] \quad \text{and} \quad y_n = \frac{F_n}{2}\left[1 + \sqrt{1 + \frac{4}{F_nF_{n+1}}}\right].$$

(The negative roots of the quadratics must be rejected since x_n and y_n are clearly positive.)

Solution to part (b) by Sahib Singh, Clarion University of Pennsylvania, Clarion, PA

It is obvious that $x_1 = y_1$. For $n > 1$, from the well-known formula $L_n = F_{n+1} + F_{n-1}$, we see that $F_{n+1} < L_n$. Applying this inequality to the formulas for x_n and y_n shows that $y_n > x_n$ when $n > 1$.

Most solvers ignored the question of convergence. Unless you know that the continued fractions converge, the operations above cannot be justified.

Proof of convergence by H.-J. Seiffert, Berlin, Germany

For positive integers a and b, let

$$z = a + \cfrac{1}{b + \cfrac{1}{a + \cfrac{1}{b + \ddots}}}$$

If p_k/q_k denotes the k^{th} convergent of z, then, for all positive integers k:

$$p_0 = a, \quad p_1 = ab + 1, \quad q_0 = 1, \quad q_1 = b,$$
$$p_{2k} = ap_{2k-1} + p_{2k-2}, \quad p_{2k+1} = bp_{2k} + p_{2k-1},$$
$$q_{2k} = aq_{2k-1} + q_{2k-2}, \quad q_{2k+1} = bq_{2k} + q_{2k-1}.$$

It follows that the sequences (p_{2k}) and (q_{2k}) satisfy

$$p_0 = a, \quad p_2 = a(ab + 2), \quad p_{2k} = (ab + 2)p_{2k-2} - p_{2k-4},$$
$$q_0 = 1, \quad q_2 = ab + 1, \quad q_{2k} = (ab + 2)q_{2k-2} - q_{2k-4}.$$

These are second-order linear recurrences; and using standard methods, we find that

$$p_{2k} = a(t_1^{k+1} - t_2^{k+1})/D \quad \text{and} \quad q_{2k} = ((t_1 - 1)t_1^k - (t_2 - 1)t_2^k)/D$$

where $t_1 = (ab + 2 + D)/2$ and $t_2 = (ab + 2 - D)/2$ are the roots of $t^2 - (ab + 2)t + 1 = 0$ and $D = \sqrt{ab(ab + 4)}$.

Since $t_1 > t_2 > 0$, we find that

$$\lim_{k\to\infty} \frac{p_{2k}}{q_{2k}} = \lim_{k\to\infty} \frac{a(t_1^{k+1} - t_2^{k+1})}{(t_1 - 1)t_1^k - (t_2 - 1)t_2^k} = \lim_{k\to\infty} \frac{a\left(1 - \left(\frac{t_2}{t_1}\right)^{k+1}\right)}{(t_1 - 1)\frac{1}{t_1} - \frac{t_2 - 1}{t_1}\left(\frac{t_2}{t_1}\right)^k}$$
$$= \frac{a}{1 - \frac{1}{t_1}} = \frac{at_1}{t_1 - 1}.$$

In a similar manner, we find that

$$\lim_{k\to\infty} \frac{p_{2k+1}}{q_{2k+1}}$$

has this same value. Thus,

$$\lim_{k\to\infty} \frac{p_k}{q_k}$$

exists and the continued fraction converges to this value.

One could also have noted convergence by quoting from a standard text on continued fractions, such as Theorem 3.5 from [1], which states that any simple continued fraction (positive entries and 1's in the numerators) converges. Seiffert's proof, though, not only proves convergence and finds the limit, but also gives the value of all the convergents.

Reference

1. C. D. Olds. *Continued Fractions*. Washington, D.C.: Mathematical Association of America (New Mathematics Library), 1963.

Also solved by Charles Ashbacher, Paul S. Bruckman, Russell Euler, Herta T. Freitag, C. Georghiou, Russell Jay Hendel, Hans Kappus, Carl Libis, Graham Lord, Ray Melham, Bob Prielipp, H.-J. Sieffert, 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-471 *Proposed by Andrew Cusumano & Marty Samberg, Great Neck, NY*

Starting with a sequence of four ones, build a sequence of finite differences where the number of finite differences taken at each step is the term of the sequence. That is,

S_1

```
  1   1   1   1
1   2   3   4   5
```

S_2

```
      1   1   1   1
    1   2   3   4   5
  1   2   4   7  11  16
```

S_3

```
         1   1   1   1
       1   2   3   4   5
     1   2   4   7  11  16
   1   2   4   8  15  26  42
```

Now, reverse the procedure but start with the powers of the last row of differences and continue until differences are constant. For example, if the power is two, we have

```
1   4   9  16  25          1   4  16  49  121  256   etc.
  3   5   7   9              3  12  33  72  135
    2   2   2                  9  21  39  63
                                12  18  24
                                   6   6
```

The sequence of constants obtained when the power is two is

$$2, 6, 20, 70, \ldots,$$

while the sequence of constants when the power is three is

$$6, 90, 1680, 34650, \ldots .$$

Let N be the number of the term in the original difference sequence and M be the power used in forming the reversed sequence. Show that the constant term is

$$X(N, M) = \frac{(N \cdot M)!}{(N!)^M}, \quad N = 1, 2, 3, \ldots, \quad M = 2, 3, 4, \ldots .$$

For example,

$$x(2, 3) = \frac{6!}{2^3} = 90.$$

H-472 *Proposed by Paul S. Bruckman, Edmonds, WA*

Let $Z(n)$ denote the Fibonacci entry-point of the natural number n, that is, the smallest positive index t such that $n \mid F_t$. Prove that $n = Z(n)$ if and only if $n = 5$ or $n = 12 \cdot 5$, for some $u \geq 0$.

H-473 *Proposed by A. G. Schaake & J. C. Turner, Hamilton, New Zealand*

Show that the following [1, p. 98] is equivalent to Fermat's Last Theorem.

"For $n > 2$ there does not exist a positive integer triple (a,b,c) such that the two rational numbers r/s, p/q, with

$$r = c - a, \qquad p = b - 1,$$
$$s = \sum_{i=1}^{n} b^{n-i}, \qquad q = \sum_{i=1}^{n} a^{i-1}c^{n-i},$$

are penultimate and final convergents, respectively, of the simple continued fraction (having an odd number of terms) for p/q."

Reference

1. A. G. Schaake & J. C. Turner. *New Methods for Solving Quadratic Diophantine Equations (Part I and Part II)*. Research Report No. 192, Department of Mathematics and Statistics, University of Waikato, New Zealand, 1989.

Editorial comment: Please note that in the May 1992 issue of this quarterly, the first solution (A Triggy Problem), which is actually Problem 446, was erroneously identified as Problem 466.

SOLUTIONS

Sum Problem

H-435 *Proposed by Ratko Tošič, University of Novi Sad, Yugoslavia (Vol. 27, no. 5, November 1989)*

(a) Prove that, for $n \geq 1$,

$$F_{n+1} + \sum_{\substack{0 < i_1 < \cdots < i_k \leq n \\ 1 \leq k \leq n}} F_{n+1-i_k} F_{i_k - i_{k-1}} \cdots F_{i_2 - i_1} F_{i_1}$$
$$= \sum_{k=0}^{\lfloor \frac{n+1}{2} \rfloor} \binom{n+1}{2k+1} \cdot 2^k,$$

where $\lfloor x \rfloor$ is the greatest integer $\leq x$.

(b) Prove that, for $n \geq 3$,

$$\sum_{\substack{0 < i_1 < \cdots < i_k \leq n \\ 1 \leq k \leq n}} (-1)^{n-k} F_{n-1-i_k} F_{i_k - i_{k-1}} \cdots F_{i_2 - i_1} F_{i_1 - 2} \cdot 2^k$$
$$= F_{n+3} + (-1)^{n+1} F_{n-3}.$$

Solution by Y. H. Harris Kwong, SUNY College at Fredonia, Fredonia, NY

(a) Let S_n denote the sum on the left of the given identity. Note that S_n can be rewritten as $\sum_{k=0}^{n} S_{n,k}$, where

$$S_{n,k} = \sum_{\substack{j_1, \ldots, j_{k+1} > 0 \\ j_1 + \cdots + j_{k+1} = n+1}} F_{j_1} F_{j_2} \cdots F_{j_{k+1}},$$

which is precisely the coefficient of x^{n+1} in

$$\left(\sum_{i=1}^{\infty} F_i x_i\right)^{k+1} = \left(\frac{x}{1 - x - x^2}\right)^{k+1}.$$

Therefore, S_n is the coefficient of x^{n+1} in

$$\sum_{k=0}^{\infty} \left(\frac{x}{1 - x - x^2}\right)^{k+1} = \frac{x}{1 - 2x - x^2} = \frac{1}{2\sqrt{2}}\left(\frac{1}{1 + (1 - \sqrt{2})x} - \frac{1}{1 - (1 - \sqrt{2})x}\right)$$

$$= \frac{1}{2\sqrt{2}} \sum_{n=0}^{\infty} [(1 + \sqrt{2})^n - (1 - \sqrt{2})^n]x^n.$$

Hence, we conclude that

$$S_n = \frac{1}{2\sqrt{2}} \sum_{j=0}^{n+1} \binom{n+1}{j} [\sqrt{2}^j - (-\sqrt{2})^j] = \sum_{k=0}^{\left\lfloor \frac{n+1}{2} \right\rfloor} \binom{n+1}{2k+1} 2^k.$$

(b) Let T_n denote the sum on the left of the given identity, then

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

where

$$T_{n,k} = \sum_{\substack{j_1, j_{k+1} \geq -1, j_2, \ldots, j_k > 0 \\ j_1 + \cdots + j_{k+1} = n-3}} F_{j_1} (-2F_{j_2}) \cdots (-2F_{j_k}) F_{j_{k+1}},$$

which is exactly the coefficient of x^{n-3} in

$$\left(\sum_{j=-1}^{\infty} F_j x^j\right)^2 \left(\sum_{i=1}^{\infty} -2F_i x^i\right)^{k-1} = \left(\frac{1}{x} + \frac{x}{1 - x - x^2}\right)^2 \left(\frac{-2x}{1 - x - x^2}\right)^{k-1}$$

Hence, we have

$$\sum_{n=0}^{\infty} (-1)^{n+1} T_n x^n = 2x^3 \left(\frac{1}{x} + \frac{x}{1 - x - x^2}\right)^2 \sum_{k=1}^{\infty} \left(\frac{-2x}{1 - x - x^2}\right)^{k-1}$$

$$= \frac{2x(1 - x)^2}{(1 - x - x^2)(1 + x - x^2)} = \frac{2 - 3x}{1 - x - x^2} - \frac{2 - x}{1 + x - x^2}.$$

It is clear that

$$\frac{1}{1 + x - x^2} = \frac{1}{(1 + \alpha x)(1 + \beta x)} = \frac{1}{\alpha - \beta}\left[\frac{\alpha}{1 + \alpha x} - \frac{\beta}{1 + \beta x}\right],$$

where $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. Thus,

$$\frac{1}{1 + x - x^2} = \sum_{n=0}^{\infty} \frac{(-1)^n [\alpha^{n+1} - \beta^{n+1}]}{\alpha - \beta} x^n = \sum_{n=0}^{\infty} (-1)^n F_{n+1} x^n,$$

which implies that

$$\frac{2 - 3x}{1 - x - x^2} - \frac{2 - x}{1 + x - x^2} = \sum_{n=0}^{\infty} [(2F_{n+1} - 3F_n) + (-1)^{n+1}(2F_{n+1} + F_n)]x^n.$$

Therefore, we conclude that for $n \geq 0$,

$$T_n = (2F_{n+1} + F_n) + (-1)^{n+1}(2F_{n+1} - 3F_n) = F_{n+3} + (-1)^{n+1} F_{n-3}.$$

Also solved by N. A. Volodin.

Mix and Match

H-454 *Proposed by Larry Taylor, Rego Park, NY (Vol. 29, no. 2, May 1991)*

Construct six distinct Fibonacci-Lucas identities such that

(a) Each identity consists of three terms;
(b) Each term is the product of two Fibonacci numbers;
(c) Each subscript is either a Fibonacci or a Lucas number.

Solutions by Stanley Rabinowitz, Westford, MA

Solution Set 1

Here are six identities that meet the requested conditions, although they are probably not what the proposer intended:

$$F_{F_2}F_{F_n} + F_{F_3}F_{F_n} = F_{F_4}F_{F_n}$$
$$F_{F_2}F_{L_n} + F_{F_3}F_{L_n} = F_{F_4}F_{L_n}$$
$$F_{F_3}F_{F_n} + F_{F_4}F_{F_n} = F_{L_3}F_{F_n}$$
$$F_{F_3}F_{L_n} + F_{F_4}F_{L_n} = F_{L_3}F_{L_n}$$
$$F_{F_4}F_{F_n} + F_{L_3}F_{F_n} = F_{F_5}F_{F_n}$$
$$F_{F_4}F_{L_n} + F_{L_3}F_{L_n} = F_{F_5}F_{L_n}$$

Solution Set 2

If numerical identities are acceptable, then we have the following identities (found by computer search):

$$F_2F_3 + F_4F_8 = F_5F_7$$
$$F_2F_8 + F_5F_{11} = F_3F_{13}$$
$$F_2F_{18} + F_5F_{11} = F_7F_{13}$$
$$F_3F_7 + F_4F_8 = F_2F_{11}$$
$$F_3F_{13} + F_8F_{18} = F_5F_{21}$$
$$F_5F_{21} + F_8F_{34} = F_{13}F_{29}$$
$$F_8F_{18} + F_{11}F_{21} = F_3F_{29}$$
$$F_{13}F_{29} + F_{18}F_{34} = F_5F_{47}$$

where all the subscripts are distinct in each example.

Solution Set 3

The numerical identities in Solution Set 2 suggest the following identities involving one parameter, i:

$$\begin{cases} F_{F_{i+4}}F_{L_{i+1}} + F_{F_{i+2}}F_{L_{i+2}} = F_{F_i}F_{L_{i+3}} & \text{if } i \text{ is not divisible by } 3 \\ F_{F_{i+4}}F_{L_{i+1}} = F_{F_{i+2}}F_{L_{i+2}} + F_{F_i}F_{L_{i+3}} & \text{if } 3\mid i. \end{cases}$$

We will prove these by proving the equivalent single condition:

(1) $$F_{F_{i+4}}F_{L_{i+1}} - (-1)^{F_i}F_{F_{i+2}}F_{L_{i+2}} = F_{F_i}F_{L_{i+3}}.$$

To verify identity (1), we apply the known transformation

$$5F_mF_n = L_{m+n} - (-1)^n L_{m-n}$$

to get:

$$L_{F_{i+4}+L_{i+1}} - (-1)^{L_{i+1}} L_{F_{i+4}-L_{i+1}} - (-1)^{F_i}[L_{F_{i+2}+L_{i+2}} - (-1)^{L_{i+2}} L_{F_{i+2}-L_{i+2}}] - L_{F_i+L_{i+3}} + (-1)^{L_{i+3}} L_{F_i-L_{i+3}} = 0.$$

This identity can be shown to be true because, of the six terms, it can be grouped into pairs of terms that cancel. Specifically,

(2) $$L_{F_{i+4}+L_{i+1}} = L_{F_i+L_{i+3}}$$

(3) $$(-1)^{L_{i+1}} L_{F_{i+4}-L_{i+1}} = (-1)^{F_i}(-1)^{L_{i+2}} L_{F_{i+2}-L_{i+2}}$$

(4) $$(-1)^{F_i} L_{F_{i+2}+L_{i+2}} = (-1)^{L_{i+3}} L_{F_i-L_{i+3}}$$

Equation (2) follows from the identity

$$F_{i+4} + L_{i+1} = F_i + L_{i+3},$$

which is straightforward to prove.

To prove equation (3), we use the fact that $L_{-n} = (-1)^n L_n$, so that

$$L_{F_{i+2}-L_{i+2}} = L_{-F_{i+2}+L_{i+2}}$$

since a simple parity argument shows that $F_{i+2} - L_{i+2}$ is always even. Then we note that $F_i + L_{i+2} \equiv L_{i+1} \pmod 2$, which also follows from a simple parity argument. Thus,

$$(-1)^{L_{i+1}} = (-1)^{F_i+L_{i+2}}$$

and we see that equation (3) is equivalent to

$$F_{i+4} - L_{i+1} = -F_{i+2} + L_{i+2},$$

which we again leave as a simple exercise for the reader.

For equation (4), we have similarly that $F_i \equiv L_{i+3} \pmod 2$, and hence equation (4) is equivalent to the easily proven

$$F_{i+2} + L_{i+2} = -F_i + L_{i+3},$$

where again we note that $F_i - L_{i+3}$ is always even.

Finally, we note a second identity analogous to (1):

(5) $$F_{F_{i+1}} F_{L_{i+1}} - (-1)^{F_i} F_{F_{i-1}} F_{F_{i+2}} = F_{F_i} F_{F_{i+3}}$$

whose proof is similar and is omitted.

Equations (1) and (5) appear to generate all the numerical examples I have found. If we let i have the forms $3k - 1$, $3k$, and $3k + 1$, we get the six identities:

$$F_{F_{3k+3}} F_{L_{3k}} + F_{F_{3k+1}} F_{L_{3k+1}} = F_{F_{3k-1}} F_{L_{3k+2}}$$
$$F_{F_{3k+4}} F_{L_{3k+1}} = F_{F_{3k+2}} F_{L_{3k+2}} + F_{F_{3k}} F_{L_{3k+3}}$$
$$F_{F_{3k+5}} F_{L_{3k+2}} + F_{F_{3k+3}} F_{L_{3k+3}} = F_{F_{3k+1}} F_{L_{3k+4}}$$
$$F_{F_{3k}} F_{L_{3k}} + F_{F_{3k-2}} F_{F_{3k+1}} = F_{F_{3k-1}} F_{F_{3k+2}}$$
$$F_{F_{3k+1}} F_{L_{3k+1}} = F_{F_{3k-1}} F_{F_{3k+2}} + F_{F_{3k}} F_{F_{3k+3}}$$
$$F_{F_{3k+2}} F_{L_{3k+2}} + F_{F_{3k}} F_{F_{3k+3}} = F_{F_{3k+1}} F_{F_{3k+4}}$$

which are probably the ones the proposer had in mind.

Also solved by P. Bruckman and the proposer.

Squared Magic

H-455 *Proposed by T. V. Padma Kumar, Trivandrum, South India (Vol. 29, no. 3, August 1991)*

Characterize, as completely as possible, all "Magic Squares" of the form

a_1	a_2	a_3	a_4
b_1	b_2	b_3	b_4
c_1	c_2	c_3	c_4
d_1	d_2	d_3	d_4

subject to the following constraints:

1. Rows, columns, and diagonals have the same sum
2. $a_1 + a_4 + d_1 + d_4 = b_2 + b_3 + c_2 + c_3 = a_1 + b_1 + a_4 + b_4 = K$
3. $c_1 + d_1 + c_4 + d_4 = a_2 + a_3 + b_2 + b_3 = c_2 + c_3 + d_2 + d_3 = K$
4. $a_1 + a_2 + b_1 + b_2 = c_1 + c_2 + d_1 + d_2 = a_3 + a_4 + b_3 + b_4 = K$
5. $c_3 + c_4 + d_3 + d_4 = c_1 + d_2 + a_3 + b_4 = a_1 + a_2 + d_1 + d_2 = K$
6. $a_3 + a_4 + d_3 + d_4 = b_1 + b_2 + c_1 + c_2 = b_3 + b_4 + c_3 + c_4 = K$
7. $a_2 + a_3 + d_2 + d_3 = b_1 + c_1 + b_4 + c_4 = K$
8. $a_1 + b_1 + c_1 + a_2 + b_2 + a_3 = b_4 + c_3 + c_4 + d_2 + d_3 + d_4 = 3K/2$
9. $b_1 + c_1 + d_1 + c_2 + d_2 + d_3 = a_2 + a_3 + a_4 + b_3 + b_4 + c_4 = 3K/2$
10. $a_2^2 + a_3^2 + d_2^2 + d_3^2 = b_1^2 + c_1^2 + b_4^2 + c_4^2$
11. $c_1^2 + c_2^2 + d_1^2 + d_2^2 = a_3^2 + b_3^2 + a_4^2 + b_4^2$
12. $c_3^2 + c_4^2 + d_3^2 + d_4^2 = a_1^2 + b_1^2 + a_2^2 + b_2^2$
13. $a_1^2 + a_2^2 + a_3^2 + a_4^2 + b_1^2 + b_2^2 + b_3^2 + b_4^2 = M$
14. $c_1^2 + c_2^2 + c_3^2 + c_4^2 + d_1^2 + d_2^2 + d_3^2 + d_4^2 = M$
15. $a_1^2 + b_1^2 + c_1^2 + d_1^2 + a_2^2 + b_2^2 + c_2^2 + d_2^2 = M$
16. $a_3^2 + b_3^2 + c_3^2 + d_3^2 + a_4^2 + b_4^2 + c_4^2 + d_4^2 = M$
17. $a_1 + b_2 + c_3 + d_4 + d_1 + c_2 + b_3 + a_4 = b_1 + c_1 + a_2 + d_2 + a_3 + d_3 + b_4 + c_4$
18. $a_1a_2 + a_3a_4 + b_1b_2 + b_3b_4 = c_1c_2 + c_3c_4 + d_1d_2 + d_3d_4$
19. $a_1b_1 + c_1d_1 + a_2b_2 + c_2d_2 = a_3b_3 + c_3d_3 + a_4b_4 + c_4d_4$

Solution by Paul S. Bruckman, Edmonds, WA

We first apply constraints 1-9 and 17, which are linear in nature. We find that these constraints are satisfied with 4 degrees of freedom, that is, with 4 of the 16 unknown quantities still undetermined. We may choose any 4 of the 16 quantities as arbitrary and determine the other 12 from these, so as to satisfy 1-9 and 17. For example, if we leave a_1, a_2, a_3, and b_1 as arbitrary, our magic square will look as follows:

a_1	a_2	a_3	$k - a_1 - a_2 - a_3$
b_1	$k - a_1 - a_2 - b_1$	$a_1 + b_1 - a_3$	$a_2 + a_3 - b_1$
$\frac{k}{2} - a_3$	$a_1 + a_2 + a_3 - \frac{k}{2}$	$\frac{k}{2} - a_1$	$\frac{k}{2} - a_2$
$\frac{k}{2} - a_1 - b_1 + a_3$	$\frac{k}{2} - a_2 - a_3 + b_1$	$\frac{k}{2} - b_1$	$a_1 + a_2 + b_1 - \frac{k}{2}$

It is a tedious but trivial exercise to verify that the quantities shown above satisfy constraints 1-9 and 17, and also constraints 10-12, 18, and 19. As for constraints 13-16, we may also verify that these are satisfied by the above quantities, provided the following single condition holds:

$$(*)\qquad M = 2k^2 - 2k(2a_1 + 2a_2 + a_3 + b_1) + 4b_1^2 + 4b_1(a_1 - a_3) + 4a_2(a_1 + a_3) + 4(a_1^2 + a_2^2 + a_3^2).$$

The condition in (*) removes one additional degree of freedom, thereby leaving only 3 undetermined quantities, say a_1, a_2, and a_3. If we require that the magic square's entries be *integers*, this imposes additional constraints on the entries, subject to the Diophantine solutions of (*). If, in addition, we require that the entries be *distinct*, further restrictions apply.

As may be shown, the corner entries of any 3×3 square contained within the large square must add up to k, as well as the corner entries of the large square itself. Moreover, the entries of any 2×2 square contained within the large square must total k.

An example which satisfies all 19 conditions (though not the condition that the entries be distinct) is the following, taking $k = 18$, $M = 208$, $a_1 = 4$, $a_2 = 3$, and $a_3 = 5$:

4	3	5	6
2	9	1	6
4	3	5	6
8	3	7	0

If we take $k = 34$, $M = 748$, $a_1 = 5$, $a_2 = 11$, $a_3 = 8$, we obtain a "conventional" magic square (where all entries are integers; in fact, the integers from 1-16). There are many such magic squares possible; this is only one such:

5	11	8	10
16	2	13	3
9	7	12	6
4	14	1	15

Also solved by the proposer.

*****

VOLUME INDEX

ANDO, Shiro (coauthor: Calvin T. Long). "Another Generalization of Gould's Star of David Theorem," 30(3): 251-55.

ANDRADE, Ana (coauthor: S. P. Pethe). "On the r^{th}-Order Nonhomogeneous Recurrence Relation and Some Generalized Fibonacci Sequences," 30(3):256-62.

ANDRÉ-JEANNIN, Richard. "The Equations $U_n = U_q x^2$, Where q Is Odd, and $V_n = V_q x^2$ Where q Is Even," 30(2):133-35."Recurrent Formulas of the Generalized Fibonacci and Tribonacci Sequences," 30(1):77-79.

BAILEY, D. F. "More Binomial Coefficient Congruences," 30(2):121-25.

BESLIN, Scott (coauthor: Steve Ligh). "GCD-Closed Sets and the Determinants of GCD Matrices," 30(2):157-60.

BLANTON, Earle L., Jr. (coauthors: Spencer P. Hurd & Judson S. McCranie). "On a Digraph Defined by Squaring Modulo n," 30(4):322-34.

BOYD, A. V. "Bounds for the Catalan Numbers," 30(2):136-38.

BRISON, Owen J. "Complete Fibonacci Sequences in Finite Fields," 30(4):295-304.

BUNDER, M. W. "Zeckendorf Representations Using Negative Fibonacci Numbers," 30(2):111-15.

CHUAN, Wai-fong. "Fibonacci Words," 30(1):68-76.

CREECH, R. L. (coauthors: W. R. Spickerman & R. N. Joyner). "On the (2, F) Generalizations of the Fibonacci Sequence," 30(4):310-14.

D'AMICO, A. (coauthors: G. Ferri & M. Faccio). "Fibonacci Numbers and Ladder Network Impedance," 30(1): 62-67.

DeTEMPLE, Duane W. "The Triangle of Smallest Perimeter Which Circumscribes a Semicircle," 30(3):274.

DEZA, Michel (coauthor: Monique Laurent). "The Fibonacci and Parachute Inequalities for ℓ_1-Metrics," 30(1): 54-61.

DiPORTO, Adina (coauthor: Piero Filipponi). "Generating M-Strong Fibonacci Pseudoprimes," 30(4):339-43.

EWELL, John A. "On Representations of Numbers by Sums of Two Triangular Numbers," 30(2):175-78.

FACCIO, M. (coauthors: G. Ferri & A. D'Amico). "Fibonacci Numbers and Ladder Network Impedance," 30(1): 62-67.

FERRI, G. (coauthors: M. Faccio & A. D'Amico). "Fibonacci Numbers and Ladder Network Impedance," 30(1): 62-67.

FILIPPONI, Piero. "Waring's Formula, The Binomial Formula, and Generalized Fibonacci Matrices," 30(3):225-31.

FILIPPONI, Piero (coauthor: Adina DiPorto). ""Generating M-Strong Fibonacci Pseudoprimes," 30(4):339-43.

FREITAG, Herta. "The Fibonacci Conference in Scotland," 30(4):334, 367.

GILLESPIE, Frank S. "A Generalization of Kummer's Congruences and Related Results," 30(4):349-67.

GRIFFIN, Peter. "Acceleration of the Sum of Fibonacci Reciprocals," 30(2):178-81.

HILLMAN, A. P., ed. (coeditor: Stanley Rabinowitz). "Elementary Problems and Solutions," 30(1):85-89; 30(2): 182-86.

HINSON, Edward K. "On the Distribution of Pythagorean Triples," 30(4):335-38.

HLEBARSKA, J. (coauthors: K. Atanassov & S. Mihov). "Recurrent Formulas of the Generalized Fibonacci and Tribonacci Sequences," 30(1):77-79.

HODGSON, Bernard R. "On Some Number Sequences Related to the Parity of Binomial Coefficients," 30(1):35-47.

HORADAM, A. F. "Negative Order Genocchi Polynomials," 30(1):21-34; "Generation of Genocchi Polynomials of First Order by Recurrence Relations," 30(3):239-43.

HORAK, Pavel. "Strong Divisibility Linear Recurrences of Third Order," 30(2):98-102.

HORIBE, Yasuichi. "A Fibonacci Theme on Balanced Binary Trees," 30(3):244-250.

HURD, Spencer P. (coauthors: Earle L. Blanton, Jr., & Judson S. McCranie). "On a Digraph Defined by Squaring Modulo n," 30(4):322-34.

JACOBSON, Eliot T. "Distribution of the Fibonacci Numbers Mod 2^k," 30(3):211-15.

JONES, J. P. (coauthor: P. G. Tsangaris). "An Old Theorem on the GCD and Its Application to Primes," 30(3): 194-98.

JOYNER, R. N. (coauthors: W. R. Spickerman & R. L. Creech). "On the (2, F) Generalizations of the Fibonacci Sequence," 30(4):310-14.

KELLY, John B. "Schur Functions and Fibonacci Identities," 30(2):148-56.

KISS, Péter (co-authors; Béla Zay). "On a Generation of a Recursive Sequence," 30(2):103-09.

KNOPFMACHER, Arnold. "Elementary Properties of the Subtractive Euclidean Algorithm," 30(1):80-83.

KNOX, Steven W. "Fibonacci Sequence in Finite Groups," 30(2):116-20.

KUHN, Steven T. (coauthor: Andrew Vogt). "Numbers Without Ones," 30(1):48-53.

LANG, Wolfdieter. "A Combinatorial Problem in the Fibonacci Number System and Two-Variable Generalizations of Chebyshev's Polynomials," 30(3):199-210.

LAURENT, Monique (coauthor: Michel Deza). "The Fibonacci and Parachute Inequalities for ℓ_1-Metrics," 30(1):54-61.

LEE, Jack Y. "The Golden-Fibonacci Equivalence," 30(3):216-20.

LIGH, Steve (coauthor: Scott Beslin). "GCD-Closed Sets and the Determinants of GCD Matrices," 30(2):157-60.

LIU, Bolian. "A Matrix Method To Solve Recurrences With Constant Coefficients," 30(1):2-8.

LONG, Calvin T. (coauthor: Shiro Ando). "Another Generalization of Gould's Star of David Theorem," 30(3): 251-55.

McCRANIE, Judson S. (coauthors: Earle L. Blanton, Jr., & Spencer P. Hurd). "On a Digraph Defined by Squaring Modulo n," 30(4):322-34.

McNEILL, R. B. "On a Theorem of Monzingo Characterizing the Prime Divisors of Certain Sequences of Integers," 30(2):110.

MIHOV, S. (coauthors: K. Atanassov & J. Hlebarska). "Recurrent Formulas of the Generalized Fibonacci and Tribonacci Sequences," 30(1):77-79.

MILLER, Allen R. (coauthor: H. M. Srivastava). "On Glaisher's Infinite Sums Involving the Inverse Tangent Function," 30(4):290-94.

MILLER, Gordon L. (coauthor: Mary T. Whalen). "Armstrong Numbers: $153 = 1^3 + 5^3 + 3^3$," 30(3):221-24.

MINQIANG, Huang (coauthor: Dai Zongduo). "Projective Maps of Linear Recurring Sequences With Maximal p-adic Periods," 30(2):139-43.

MOORE, Thomas E. "On the Least Absolute Remainder Euclidean Algorithm," 30(2):161-65.

PAGE, Warren (coauthor: K. R. S. Sastry). "Area-Bisecting Polygonal Paths," 30(3):263-73.

PETHE, S. P. (coauthor: Ana Andrade). "On the r^{th}-Order Nonhomogeneous Recurrence Relation and Some Generalized Fibonacci Sequences," 30(3):256-62.

PIHKO, Jukka. "On Sequences Having Same Minimal Elements in the Lemoine-Kátai Algorithm," 30(4):344-48.

RABINOWITZ, Stanley, ed. "Elementary Problems and Solutions," 30(1):85-89; 30(2):182-86; 30(3):275-81; 30(4):368-75.

SASTRY, K. R. S. (coauthor: Warren Page). "Area-Bisecting Polygonal Paths," 30(3):263-73.

SPICKERMAN, W. R. (coauthors: R. N. Joyner & R. L. Creech). "On the $(2, F)$ Generalizations of the Fibonacci Sequence," 30(4):310-14.

SPYROPOULOS, K. (see Zelator).

SRIVASTAVA, H. M. (coauthor: Allen R. Miller). "On Glaisher's Infinite Sums Involving the Inverse Tangent Function," 30(4):290-94.

STOJMENOVIĆ, Ivan (coauthor: Ratko Tošić). "Fibonacci Numbers and the Numbers of Perfect Matchings of Square, Pentagonal, and Hexagonal Chains," 30(4):315-21.

TOŠIĆ, Ratko (coauthor: Ivan Stojmenović). "Fibonacci Numbers and the Numbers of Perfect Matchings of Square, Pentagonal, and Hexagonal Chains," 30(4):315-21.

TSANGARIS, P. G. (coauthor J. P. Jones). "An Old Theorem on the GCD and Its Application to Primes," 30(3): 194-98.

VOGT, Andrew (coauthor: Steven T. Kuhn). "Numbers Without Ones," 30(1):48-53.

WADDILL, Marcellus E. "The Tetranacci Sequence and Generalizations," 30(1):9-20; "Some Properties of the Tetranacci Sequence Modulo m," 30(3):232-38.

WATERHOUSE, William C. "Continued Fractions and Pythagorean Triples," 30(2):144-47.

WHALEN, Mary T. (coauthor: Gordon L. Miller). "Armstrong Numbers: $153 = 1^3 + 5^3 + 3^3$," 30(3):221-24.

WHITNEY, Raymond E., ed. "Advanced Problems and Solutions," 30(1):90-96; 30(2):187-92; 30(3):282-88; 30(4):376-82.

YOUNG, Anne Ludington. "k-Reverse Multiples," 30(2):126-32; "Trees for k-Reverse Multiples," 30(2):166-74.

ZAY, Béla (coauthor: Péter Kiss). "On a Generation of a Recursive Sequence," 30(2):103-09.

ZELATOR, Konstantine (formerly K. Spyropoulos). "The Diophantine Equation $x^2 + a^2y^m = z^{2n}$ With $(x, ay) = 1$," 30(4): 305-09.

ZONGDUO, Dai (coauthor: Huang Minqiang). "Projective Maps of Linear Recurring Sequences With Maximal p-adic Periods," 30(2):139-43.

SUSTAINING MEMBERS

I. Adler
*H.L. Alder
G.L. Alexanderson
S. Ando
R. Andre-Jeannin
J. Arkin
D.C. Arney
C. Ashbacher
M.K. Azarian
N. Balasubramania
L. Bankoff
M. Berg
J.G. Bergart
G. Bergum
G. Berzsenyi
*M. Bicknell-Johnson
P. Bien
P.S. Bruckman
M.F. Bryn
G.D. Chakerian
C. Chouteau
W.S. Clary
C.K. Cook
J.W. Creely
P.A. DeCaux
M.J. DeLeon
J. Desmond
V. Dudley
T.H. Engel
M. Faccio
D.R. Farmer
D.C. Fielder
F. Firoozbakht
Emerson Frost
Anthony Gioia
*H.W. Gould
P. Hagis, Jr.
H. Harborth
Y. Harris Kwong
P. Haukkanen
*A.P. Hillman
*A.F. Horadam
F.T. Howard
R.J. Howell
S. Howell
J.P. Jones
R.E. Kennedy
C.H. Kimberling
A. Knopfmacher
R.P. Kovach
J. Lahr
J.C. Lagarias
L.H. Lange
*C.T. Long
Chris Long
G. Lord
Br. J.M. Mahon
*J. Maxwell
F.U. Mendizabal
M.G. Monzingo
J.F. Morrison
K. Nagasaka
S.A. Obaid
D.J. Pedwell
A. Prince
S. Rabinowitz
S. Sato
J.A. Schumaker
A.G. Shannon
L.W. Shapiro
J.R. Siler
D. Singmaster
J. Sjoberg
L. Somer
W.R. Spickerman
M.N.S. Swamy
*D. Thoro
J.C. Turner
T.P. Vaughan
K. Velupiliai
J.N. Vitale
M. Waddill
J.E. Walton
G. Weekly
R.E. Whitney
B.E. Williams

*Charter Members

INSTITUTIONAL MEMBERS

ACADIA UNIVERSITY LIBRARY
Wolfville, Nova Scotia

THE BAKER STORE EQUIPMENT COMPANY
Cleveland, Ohio

CALIFORNIA STATE UNIVERSITY SACRAMENTO
Sacramento, California

ETH-BIBLIOTHEK
Zurich, Switzerland

FERNUNIVERSITAET HAGEN
Hagen, West Germany

HOWELL ENGINEERING COMPANY
Bryn Mawr, California

KLEPCO, INC.
Sparks, Nevada

MATHEMATICS SOFTWARE COMPANY
Evansville, Indiana

MISSOURI SOUTHERN STATE COLLEGE
Joplin, Missouri

PRINCETON UNIVERSITY
Princeton, New Jersey

SAN JOSE STATE UNIVERSITY
San Jose, California

SANTA CLARA UNIVERSITY
Santa Clara, California

UNIVERSITY OF NEW ENGLAND
Armidale, N.S.W. Australia

UNIVERSITY OF ROMA "LA SAPIENZA"
Roma, Italy

UNIVERSITY OF TECHNOLOGY
Sydney, N.S.W. Australia

WAKE FOREST UNIVERSITY
Winston-Salem, North Carolina

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.

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.

Applications of Fibonacci Numbers, Volumes 2 and 3. Edited by A.N. Philippou, A.F. Horadam and G.E. Bergum.

Please write to the Fibonacci Association, Santa Clara University, Santa Clara CA 95053, U.S.A., for current prices.