The Fibonacci Quarterly

Founded in 1963 by Verner E. Hoggatt, Jr. (1921-1980)
Br. Alfred Brousseau, and I.D. Ruggles

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

FIRST INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS
UNIVERSITY OF PATRAS, GREECE
AUGUST 27-31, 1984

A Report by Karel L. de Bouvère

About fifty mathematicians from thirteen different countries gathered in Patras, on the Peloponnesos in Greece, to exchange knowledge and thoughts on various mathematical topics all with the Fibonacci numbers as a common denominator. Professor A. N. Philippou, chairman of both the international and the local organizational committees, expressed it as follows in his remarks at the opening session: "Most will be lecturing on Number Theory, some will talk on Probability, and still others will present their results on ladder networks in Electric Line Theory and aromic hydrocarbons in Chemistry."

The academic sessions were scheduled, of course, according to the pace of the host country. A morning session from 9:00 A.M. to 1:00 P.M. and an afternoon session from 5:00 P.M. to 8:30 P.M., each session interrupted once by a coffee break. All lectures lasted for 45 minutes and all were in the nature of contributed papers—twenty-four in total. The Conference Proceedings will be published.

The relatively small number of participants made the conference a pleasant affair; in no time everyone knew everyone else. The social atmosphere was enhanced still more by outings and parties, not in the least due to the friendly guidance of the Greek colleagues. And clearly, it is hard to beat an environment that appropriately could be called the cradle of mathematics.

At the end of the final session on August 31, Professor Philippou and his committees and staff were given well deserved praise and applause. It was suggested that similar international conferences should be held every three years and that the University of Santa Clara, in California, U.S.A., "home" of *The Fibonacci Quarterly*, should be the host in 1987, followed in 1990 by an appropriate institution in Pisa, Italy, birthplace of Fibonacci.

The conference was jointly sponsored by the Greek Ministry of Culture and Science, the Fibonacci Association, and the University of Patras.

A Very "Nonscientific" Report by Herta T. Freitag

An announcement of the First International Conference on Fibonacci Numbers and Their Applications to be held at the University of Patras, Greece, August 27-31, 1984, reached me in mid-February. I was overjoyed by the thought that the members of the "Fibonacci-oriented" mathematical community would be able to meet each other on an international scale. Although I consider myself but an amateur in this area compared to the remarkable caliber of my esteemed peers who work in this field, I have long been a devoutly "addicted" member, and have looked forward from one issue of *The Fibonacci Quarterly* to the next ever since The Fibonacci Association was founded in 1963.

Countless hours of planning and work must have gone into the organization of the Conference by the International Committee and the Local Committee, both headed by Professor A. N. Philippou, Vice Rector of the University of Patras, and Chairman of the entire Conference, which was sponsored by the Greek Ministry of Culture and Science, the Fibonacci Association, and the University of Patras. It saddened me to learn that some of the outstanding leaders in our Fibonacci community, among them Professor G. L. Alexanderson, President of the Fibonacci Association, and Professor Gerald E. Bergum, Editor of our *Journal*, could not attend. We felt their presence even from afar. It would have been beautiful to have Verner E. Hoggatt, Jr., in our midst. I know that his spirit was with us!

The Conference well surpassed my fondest expectations. It was professionally inspirational and personally heartwarming. Names that we have held dear for many years became people. Within moments we became a circle of friends. In a very significant sense we were able to speak the same language regardless of our national backgrounds. Our common interest, indeed enthusiasm, affected this miracle.

To hold this first Conference in Greece, cradle of mathematical thought in antiquity, contributed immeasurably. "The Glory that is Greece" — Greece, the country which is indelibly imbedded in the minds, the hearts, and the souls of all educated persons throughout the world! With their inimitable beauty and charm, the surrounding waters, the mountains, those picturesque cypress trees greatly enhanced the atmosphere of our meeting.

The findings presented in the papers were profound and intricate. It seemed to me they not only deepened our conviction of the importance of the Fibonacci sequences and their ramifications, their ever-increasing relevance and applicability; they also significantly contributed to our understanding of specific aspects in this mathematical area. The conspicuous care in the presentations was admirable. The ensuing comments and questions added yet a further dimension. I shall never forget Professor A. Zachariou's deeply searching deliberations.

The Conference was eminently enriching—a uniquely memorable experience. My heartfelt gratitude is extended to all members of our Fibonacci community who have made this Conference possible and who have contributed to its success. And I am truly moved, and most appreciative, that Professor Alexanderson has given me the opportunity to relate my impressions in our *Journal*.

If I may become personal, I would also like to extend a very special "thank you" to Professor Andreas N. Philippou whose wit and warmth immediately set an unforgettable tone for our Conference. Indeed, his intuitive perception led him—at our first encounter—to "recognize" me without ever having seen me. I would like to thank him for the very special courtesies he has extended to The Fibonacci Association, and for allowing me to address the group in my capacity as one of the representatives of our organization.

I believe I speak for all Fibonacci friends across the oceans if I express the hope that this, our First International Conference on Fibonacci Numbers and Their Applications, was but a prelude for those to come.

◆◇◆◇◆

FIBONACCI-TYPE POLYNOMIALS OF ORDER K WITH PROBABILITY APPLICATIONS

ANDREAS N. PHILIPPOU and COSTAS GEORGHIOU
University of Patras, Patras, Greece

GEORGE N. PHILIPPOU
Higher Technical Institute, Nicosia, Cyprus

(Submitted August 1983)

1. INTRODUCTION AND SUMMARY

In this paper, k is a fixed integer greater than or equal to 2, unless otherwise stated, n_i $(1 \leqslant i \leqslant k)$ and n are nonnegative integers as specified, p and x are real numbers in the intervals $(0, 1)$ and $(0, \infty)$, respectively, and $[x]$ denotes the greatest integer in x. Set $q = 1 - p$, let $\{f_n^{(k)}\}_{n=0}^{\infty}$ be the Fibonacci sequence of order k [4], and denote by N_k the number of Bernoulli trials until the occurrence of the k^{th} consecutive success. We recall the following results of Philippou and Muwafi [4] and Philippou [3]:

$$P(N_k = n + k) = p^{n+k} \sum_{\substack{n_1, \ldots, n_k \ni \\ n_1 + 2n_2 + \cdots + kn_k = n}} \binom{n_1 + \cdots + n_k}{n_1, \ldots, n_k} \left(\frac{q}{p}\right)^{n_1 + \cdots + n_k}, \quad n \geqslant 0; \tag{1.1}$$

$$f_{n+1}^{(k)} = \sum_{\substack{n_1, \ldots, n_k \ni \\ n_1 + 2n_2 + \cdots + kn_k = n}} \binom{n_1 + \cdots + n_k}{n_1, \ldots, n_k}, \quad n \geqslant 0; \tag{1.2}$$

$$f_{n+1}^{(k)} = 2^n \sum_{i=0}^{[n/(k+1)]} (-1)^i \binom{n - ki}{i} 2^{-(k+1)i} - 2^{n-1} \sum_{i=0}^{[(n-1)/(k+1)]} (-1)^i \binom{n - 1 - ki}{i} 2^{-(k+1)i}, \quad n \geqslant 1. \tag{1.3}$$

For $p = 1/2$, (1.1) reduces to

$$P(N_k = n + k) = f_{n+1}^{(k)} / 2^{n+k}, \quad n \geqslant 0, \tag{1.4}$$

which relates probability to the Fibonacci sequence of order k. Formula (1.4) appears to have been found for the first time by Shane [8], who also gave formulas for $P(N_k = n)$ $(n \geqslant k)$ and $P(N_k \leqslant x)$, in terms of his polynacci polynomials of order k in p. Turner [9] also derived (1.4) and found another general formula for $P(N_k = n + k)$ $(n \geqslant 0)$, in terms of the entries of the Pascal-T triangle. None of the above-mentioned references, however, addresses the question of whether $\{P(N_k = n + k)\}_{n=0}^{\infty}$ is a proper probability distribution (see Feller [1, p. 309]), and none includes any closed formula for $P(N_k \leqslant x)$.

Motivated by the above results and open questions, we presently introduce a simple generalization of $\{f_n^{(k)}\}_{n=0}^{\infty}$, denoted by $\{F_n^{(k)}(x)\}_{n=0}^{\infty}$ and called a sequence of Fibonacci-type polynomials of order k, and derive appropriate analogs of (1.2)-(1.4) for $F_n^{(k)}(x)$ $(n \geqslant 1)$ [see Theorem 2.1 and Theorem 3.1(a)]. In addition, we show that $\sum_{n=0}^{\infty} P(N_k = n + k) = 1$, and derive a simple and closed formula for the distribution function of N_k [see Theorem 3.1(b)-(c)].

2. FIBONACCI-TYPE POLYNOMIALS OF ORDER K AND MULTINOMIAL EXPANSIONS

In this section, we introduce a sequence of Fibonacci-type polynomials of order k, denoted by $\{F_n^{(k)}(x)\}_{n=0}^{\infty}$, and derive two expansions of $F_n^{(k)}(x)$ $(n \geq 1)$ in terms of the multinomial and binomial coefficients, respectively. The proofs are given along the lines of [3], [5], and [7].

Definition 2.1

The sequence of polynomials $\{F_n^{(k)}(x)\}_{n=0}^{\infty}$ is said to be the sequence of Fibonacci-type polynomials of order k, if

$$F_0^{(k)}(x) = 0,$$

$$F_1^{(k)}(x) = 1,$$

and

$$F_n^{(k)}(x) = \begin{cases} x[F_{n-1}^{(k)}(x) + \cdots + F_0^{(k)}(x)], & \text{if } 2 \leq n \leq k, \\ x[F_{n-1}^{(k)}(x) + \cdots + F_{n-k}^{(k)}(x)], & \text{if } n \geq k+1. \end{cases}$$

It follows from the definition of $\{f_n^{(k)}\}_{n=0}^{\infty}$ and Definition 2.1 that

$$F_n^{(k)}(1) = f_n^{(k)} \quad (n \geq 0).$$

The n^{th} term of the sequence $\{F_n^{(k)}(x)\}$ $(n \geq 1)$ may be expanded as follows:

Theorem 2.1

Let $\{F_n^{(k)}(x)\}_{n=0}^{\infty}$ be the sequence of Fibonacci-type polynomials of order k. Then

$$\text{(a)} \quad F_{n+1}^{(k)}(x) = \sum_{\substack{n_1, \ldots, n_k \ni \\ n_1 + 2n_2 + \cdots + kn_k = n}} \binom{n_1 + \cdots + n_k}{n_1, \ldots, n_k} x^{n_1 + \cdots + n_k}, \; n \geq 0;$$

$$\text{(b)} \quad F_{n+1}^{(k)}(x) = (1+x)^n \sum_{i=0}^{[n/(k+1)]} (-1)^i \binom{n-ki}{i} x^i (1+x)^{-(k+1)i}$$
$$- (1+x)^{n-1} \sum_{i=0}^{[(n-1)/(k+1)]} (-1)^i \binom{n-1-ki}{i} x^i (1+x)^{-(k+1)i}, \quad n \geq 1.$$

We shall first establish the following lemma:

Lemma 2.1

Let $\{F_n^{(k)}(x)\}_{n=0}^{\infty}$ be the sequence of Fibonacci-type polynomials of order k, and denote its generating function by $G_k(s; x)$. Then, for $|s| < 1/(1+x)$,

$$G_k(s; x) = \frac{s - s^2}{1 - (1+x)s + xs^{k+1}} = \frac{s}{1 - xs - xs^2 - \cdots - xs^k}.$$

Proof: We see from Definition 2.1 that

$$F_n^{(k)}(x) = \begin{cases} x(1+x)^{n-2}, & 2 \leqslant n \leqslant k+1, \\ (1+x)F_{n-1}^{(k)}(x) - xF_{n-1-k}^{(k)}(x), & n \geqslant k+2. \end{cases} \tag{2.1}$$

By induction on n, the above relation implies $F_n^{(k)}(x) \leqslant x(1+x)^{n-2}$ $(n \geqslant 2)$, which shows the convergence of $G_k(s;x)$ for $|s| < 1/(1+x)$. Next, by means of (2.1), we have

$$G_k(s;\,x) = \sum_{n=0}^{\infty} s^n F_n^{(k)}(x) = s + \sum_{n=2}^{k+1} s^n x(1+x)^{n-2} + \sum_{n=k+2}^{\infty} s^n F_n^{(k)}(x)$$

and

$$\begin{aligned}\sum_{n=k+2}^{\infty} s^n F_n^{(k)}(x) &= (1+x)\sum_{n=k+2}^{\infty} s^n F_{n-1}^{(k)}(x) - x\sum_{n=k+2}^{\infty} s^n F_{n-1-k}^{(k)}(x) \\ &= [(1+x)s - xs^{k+1}]G_k(s;\,x) - s^2 - \sum_{n=2}^{k+1} s^n x(1+x)^{n-2},\end{aligned}$$

from which the lemma follows.

Proof of Theorem 2.1

First we shall show part (a). Let $|s| < 1/(1+x)$. Then, using Lemma 2.1 and the multinomial theorem, and replacing n by $n - \sum_{i=1}^{k}(i-1)n_i$, we get

$$\begin{aligned}\sum_{n=0}^{\infty} s^n F_{n+1}^{(k)}(x) &= \sum_{n=0}^{\infty}(xs + xs^2 + \cdots + xs^k)^n \\ &= \sum_{n=0}^{\infty} \sum_{\substack{n_1,\ldots,n_k \ni \\ n_1+\cdots+n_k = n}} \binom{n}{n_1,\ \ldots,\ n_k} x^{n_1+\cdots+n_k} s^{n_1+2n_2+\cdots+kn_k} \\ &= \sum_{n=0}^{\infty} s^n \sum_{\substack{n_1,\ldots,n_k \ni \\ n_1+2n_2+\cdots+kn_k = n}} \binom{n_1+\cdots+n_k}{n_1,\ \ldots,\ n_k} x^{n_1+\cdots+n_k},\ n \geqslant 0,\end{aligned}$$

which shows (a).

We now proceed to part (b). Set

$$A_k(x) = \{s \in R;\ |s| < 1/(1+x) \text{ and } |(1+x)s - xs^{k+1}| < 1\},$$

and let $s \in A_k(x)$. Then, using Lemma 2.1 and the binomial theorem, replacing by $n - ki$, and setting

$$b_n^{(k)}(x) = (1+x)^n \sum_{i=0}^{[n/(k+1)]} (-1)^i \binom{n-ki}{i} x^i (1+x)^{-(k+1)i},\ n \geqslant 0,$$

we get

$$\begin{aligned}\sum_{n=0}^{\infty} s^n F_{n+1}^{(k)}(x) &= (1-s)\sum_{n=0}^{\infty}[(1+x)s - xs^{k+1}]^n \\ &= (1-s)\sum_{n=0}^{\infty}\sum_{i=0}^{n}(-1)^i\binom{n}{i}(1+x)^{n-i}x^i s^{n+ki} \\ &= (1-s)\sum_{n=0}^{\infty} s^n \sum_{i=0}^{[n/(k+1)]}(-1)^i\binom{n-ki}{i}(1+x)^{n-(k+1)i}x^i \\ &= (1-s)\sum_{n=0}^{\infty} s^n b_n^{(k)}(x) = 1 + \sum_{n=1}^{\infty} s^n[b_n^{(k)}(x) - b_{n-1}^{(k)}(x)].\end{aligned}$$

The last two relations establish part (b).

3. FIBONACCI-TYPE POLYNOMIALS OF ORDER K AND PROBABILITY APPLICATIONS

In this section we shall establish the following theorem which relates the Fibonacci-type polynomials of order k to probability, shows that

$$\{P(N_k = n + k)\}_{n=0}^{\infty}$$

is a proper probability distribution, and gives the distribution function of N_k.

Theorem 3.1

Let $\{F_n^{(k)}(x)\}_{n=0}^{\infty}$ be the sequence of Fibonacci-type polynomials of order k, denote by N_k the number of Bernoulli trials until the occurrence of the k^{th} consecutive success, and set $q = 1 - p$. Then

(a) $P(N_k = n + k) = p^{n+k}F_{n+1}^{(k)}(q/p)$, $n \geqslant 0$;

(b) $\displaystyle\sum_{n=0}^{\infty} P(N_k = n + k) = 1$;

(c) $$P(N_k \leqslant x) = \begin{cases} 1 - \dfrac{p^{[x]+1}}{q} \displaystyle\sum_{\substack{n_1, \ldots, n_k \ni \\ n_1 + 2n_2 + \cdots + kn_k = [x]+1}} \binom{n_1 + \cdots + n_k}{n_1, \ldots, n_k}\left(\frac{q}{p}\right)^{n_1 + \cdots + n_k}, & x \geqslant k, \\ 0, \text{ otherwise.} \end{cases}$$

We shall first establish the following lemma.

Lemma 3.1

Let $\{F_n^{(k)}(x)\}_{n=0}^{\infty}$ be the sequence of Fibonacci-type polynomials of order k. Then, for any fixed $x \in (0, \infty)$,

(a) $$\lim_{n\to\infty} \frac{F_n^{(k)}(x)}{(1 + x)^n} = 0;$$

(b) $$\sum_{n=0}^{m} \frac{F_{n+1}^{(k)}(x)}{(1 + x)^{n+k}} = 1 - \frac{F_{m+k+2}^{(k)}(x)}{(1 + x)^{m+k}}, \quad m \geqslant 0.$$

Proof: First, we show (a). For any fixed $x \in (0, \infty)$ and $n \geqslant k + 1$, relation (2.1) gives

$$\frac{F_n^{(k)}(x)}{(1 + x)^n} - \frac{F_{n+1}^{(k)}(x)}{(1 + x)^{n+1}} = \frac{(1 + x)F_n^{(k)}(x) - F_{n+1}^{(k)}(x)}{x(1 + x)^{n+1}} = \frac{xF_{n-k}^{(k)}(x)}{(1 + x)^{n+1}} > 0,$$

which implies that $F_n^{(k)}(x)/(1 + x)^n$ converges. Therefore,

$$\lim_{n\to\infty} \frac{xF_{n-k}^{(k)}(x)}{(1+x)^{n+1}} = 0,$$

from which (a) follows.

We now proceed to show (b). For $m = 0$, both the left- and right-hand sides equal $(1 + x)^{-k}$, since $F_{k+2}^{(k)}(x) = x(1 + x)^k - x$ by (2.1). We assume that the lemma holds for some integer $m \geqslant 1$ and we shall show that it is true for $m + 1$. In fact,

$$\sum_{n=0}^{m+1} \frac{F_{n+1}^{(k)}(x)}{(1+x)^{n+k}} = \frac{F_{m+2}^{(k)}(x)}{(1+x)^{m+k+1}} + \sum_{n=0}^{m} \frac{F_{n+1}^{(k)}(x)}{(1+x)^{n+k}}$$

$$= \frac{F_{m+2}^{(k)}(x)}{(1+x)^{m+1+k}} + 1 - \frac{F_{m+k+2}^{(k)}(x)}{x(1+x)^{m+k}}, \text{ by induction hypothesis,}$$

$$= 1 - \frac{(1+x)F_{m+k+2}^{(k)}(x) - xF_{m+2}^{(k)}(x)}{x(1+x)^{m+k+1}}$$

$$= 1 - \frac{F_{m+k+3}^{(k)}(x)}{x(1+x)^{m+k+1}}, \text{ by (2.1).}$$

Proof of Theorem 3.1

Part (a) follows directly from relation (1.1), by means of Theorem 2.1 applied with $x = q/p$. Next, we observe that

$$\sum_{n=0}^{m} P(N_k = n + k) = \sum_{n=0}^{m} p^{n+k}F_{n+1}(q/p), \text{ by Theorem 3.1(a),}$$

$$= \sum_{n=0}^{m} \frac{F_{n+1}^{(k)}(x)}{(1+x)^{m+k}}, \text{ by setting } p = 1/(1+x),$$

$$= 1 - \frac{F_{m+k+2}^{(k)}(x)}{x(1+x)^{m+k}}, \text{ by Lemma 3.1(b),}$$

$$\to 1 \text{ as } m \to \infty, \text{ by Lemma 3.1(a),}$$

which establishes part (b). Finally, we see that

$$P(N_k \leqslant x) = P(\emptyset) = 0, \text{ if } x < k,$$

and

$$P(N_k \leqslant x) = \sum_{n=k}^{[x]} P(N_k = n) = \sum_{n=0}^{[x]-k} P(N_k = n + k)$$

$$= \sum_{n=0}^{[x]-k} p^{n+k}F_{n+1}^{(k)}(q/p), \text{ by Theorem 3.1(a),}$$

$$= 1 - \frac{p^{[x]+1}}{q}F_{[x]+2}^{(k)}(q/p)$$

$$= 1 - \frac{p^{[x]+1}}{q} \sum_{\substack{n_1, \ldots, n_k \ni \\ n_1 + 2n_2 + \cdots + kn_k = [x]+1}} \binom{n_1 + \cdots + n_k}{n_1, \ldots, n_k} \left(\frac{q}{p}\right)^{n_1 + \cdots + n_k}, \quad x \geqslant k,$$

by means of Lemma 3.1(b) and Theorem 2.1(a), both applied with $x = q/p$. The last two relations prove part (c), and this completes the proof of the theorem.

Corollary 3.1

Let X be a random variable distributed as geometric of order k ($k \geqslant 1$) with parameter p [6]. Then the distribution function of X is given by

$$P(X \leqslant x) = \begin{cases} 1 - \dfrac{p^{[x]+1}}{q} \displaystyle\sum_{\substack{n_1, \ldots, n_k \ni \\ n_1 + 2n_2 + \cdots + kn_k = [x]+1}} \binom{n_1 + \cdots + n_k}{n_1, \ldots, n_k} \left(\frac{q}{p}\right)^{n_1 + \cdots + n_k}, & x \geqslant k, \\ 0, \text{ otherwise.} & \end{cases}$$

Proof: For $k = 1$, the definition of the geometric distribution of order k implies that X is distributed as geometric, so that $P(X \leqslant x) = 1 - q^{[x]}$, if $x \geqslant 1$ and 0 otherwise, which shows the corollary. For $k \geqslant 2$, the corollary is true, because of Theorem 3.1(c) and the definition of the geometric distribution of order k.

We end this paper by noting that Theorem 3.1(b) provides a solution to a problem proposed in [2].

REFERENCES

1. W. Feller. *An Introduction to Probability Theory and Its Applications*, I. 3rd ed. New York: Wiley, 1968.
2. A. N. Philippou. Advanced Problem H-348. *The Fibonacci Quarterly* 20, no. 4 (1982):373.
3. A. N. Philippou. "A Note on the Fibonacci Sequence of Order K and the Multinomial Coefficients." *The Fibonacci Quarterly* 21, no. 2 (1983):82-86.
4. A. N. Philippou & A. A. Muwafi. "Waiting for the K^{th} Consecutive Success and the Fibonacci Sequence of Order K." *The Fibonacci Quarterly* 20, no. 1 (1982):28-32.
5. A. N. Philippou & G. N. Philippou. "The Pell Sequence of Order K, Multinomial Coefficients, and Probability." *Bulletin of the Greek Mathematical Society* 22 (1984):74-84.
6. A. N. Philippou, C. Georghiou, & G. N. Philippou. "A Generalized Geometric Distribution of Order K and Some of Its Properties." *Statistics and Probability Letters* 1, no. 4 (1983):171-75.
7. A. N. Philippou, C. Georghiou, & G. N. Philippou. "Fibonacci Polynomials of Order K, Multinomial Expansions, and Probability." *International Journal of Mathematics and Mathematical Sciences* 6, no. 3 (1983):545-50.
8. H. D. Shane. "A Fibonacci Probability Function." *The Fibonacci Quarterly* 11, no. 6 (1973):511-22.
9. S. J. Turner. "Probability via the N^{th}-Order Fibonacci-T Sequence." *The Fibonacci Quarterly* 17, no. 1 (1979):23-28.

◆◇◆◇◆

A NOTE ON INFINITE EXPONENTIALS

I. N. BAKER
Imperial College, London, U.K.

P. J. RIPPON
The Open University, Milton Keynes, U.K.

(Submitted August 1983)

For $a > 0$, the sequence

$$a,\ a^a,\ a^{(a^a)},\ \ldots, \tag{1}$$

is convergent if and only if $a \in I = [e^{-e},\ e^{1/e}]$. This result, which was known to Euler [5], and which has been rediscovered frequently, is capable of generalization in various directions (see [6] for a wide-ranging survey). For instance, Barrow [2] showed that if $a_n \in I$, $n = 1, 2, \ldots$, then the sequence

$$a_1,\ a_1^{a_2},\ a_1^{(a_2^{a_3})},\ \ldots, \tag{2}$$

is convergent also.

More recently [1], we have observed that if a is a complex number and if

$$a^z = \exp[z \log a], \quad (z \in \mathbb{C}),$$

where the principal value of the logarithm is taken, then the sequence (1) converges if a lies in

$$R = \{e^{te^{-t}} : |t| < 1\}.$$

On the boundary of R however, and in its exterior, both convergence and divergence may occur.

The sequence (2) was shown by Thron [7] to be convergent if $|\log a_n| \leqslant 1/e$, $n = 1, 2, \ldots$, but we do not know whether this holds in general if $a_n \in R$, $n = 1, 2, \ldots$.

The aim of the present note is to give a complete discussion of the behaviour of real sequences of the form

$$a,\ a^b,\ a^{(b^a)},\ a^{(b^{(a^b)})},\ \ldots, \quad (a,\ b > 0). \tag{3}$$

Such a sequence is of course a special case of (2), and so Barrow's result guarantees convergence for $(a, b) \in I \times I$, though the full region of convergence is actually much larger. The same problem was discussed and partially solved by Creutz and Sternheimer [4], who also presented considerable computational evidence concerning the region of convergence.

With $a,\ b > 0$, we let $\phi(x) = a^{b^x} (= a^{(b^x)})$, $-\infty < x < \infty$, and

$$\phi^{n+1}(x) = \phi o \phi^n(x) = \phi^n o \phi(x), \quad (n = 1, 2, \ldots).$$

The sequence (3) under consideration is then of the form

$$\phi(0),\ \phi(1),\ \phi^2(0),\ \phi^2(1),\ \ldots\ .$$

Theorem

The following statements are equivalent:

(i) Both

$$\lim_{n\to\infty} \phi^n(0) \quad \text{and} \quad \lim_{n\to\infty} \phi^n(1)$$

exist finitely and are equal.

(ii) The function ϕ has precisely one fixed point c such that $|\phi'(c)| \leqslant 1$.

(iii) We can write

$$\log a = se^{-t} \quad \text{and} \quad \log b = te^{-s}, \quad (|st| \leqslant 1), \tag{4}$$

in a unique way.

The set of points ($\log a$, $\log b$) defined by statement (iii) is shaded in Figure 1 for the reader's convenience. We shall discuss it in more detail once the theorem is proved. Notice that $[-e, 1/e] \times [-e, 1/e]$ lies in the shaded set, as is implied by Barrow's result.

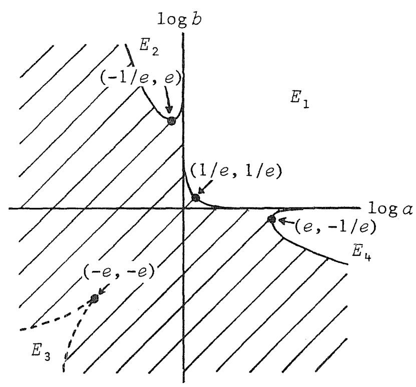

Figure 1

The behavior of the sequence at the remaining points, which will become clear in the course of the proof, is indicated below:

when ($\log a$, $\log b$) $\in E_1$, we have

$$\lim_{n\to\infty} \phi_n(0) = \lim_{n\to\infty} \phi_n(1) = \infty;$$

when ($\log a$, $\log b$) $\in E_2 \cup E_4$, we have

$$\lim_{n\to\infty} \phi^{2n}(0) = \lim_{n\to\infty} \phi^{2n+1}(1) \neq \lim_{n\to\infty} \phi^{2n+1}(0) = \lim_{n\to\infty} \phi^{2n}(1) < \infty,$$

when ($\log a$, $\log b$) $\in E_3$, we have

$$\lim_{n\to\infty} \phi_n(0) < \lim_{n\to\infty} \phi_n(1) < 1.$$

The equivalence of statements (ii) and (iii) is a special case of the following lemma.

Lemma 1

There is a one-to-one correspondence between the fixed points $c = e^s$ of ϕ, such that $|\phi'(c)| \leqslant 1$, and the representations of $(\log a, \log b)$ in the form (4).

Proof: To prove the lemma, note that

$$c = a^{b^c} = \exp(\exp(c \log b)\log a)$$

if and only if $c = e^s$, where

$$s = \exp(c \log b)\log a,$$

and s is of this form if and only if we can write

$$\log a = se^{-t} \text{ and } \log b = te^{-s}.$$

Since we then have

$$\phi'(c) = a^{b^c}b^c \log a \log b = c \exp(c \log b)\log a \log b = st,$$

the proof of the lemma is complete.

We now show that statements (i) and (ii) are equivalent. First we assume that $a, b > 1$ so that ϕ is increasing. Since

$$\phi''(x) = a^{b^x}b^x \log a(\log b)^2(1 + b^x \log a)$$

the function ϕ has no points of inflection and so has at most two fixed points. It is clear that

$$\phi^n(0) < \phi^n(1) < \phi^{n+1}(0), \quad (n = 1, 2, \ldots),$$

and so convergence occurs if and only if ϕ has at least one fixed point, in which case ϕ has exactly one fixed point c such that $|\phi'(c)| \leqslant 1$.

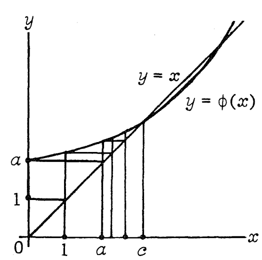

Figure 2

If ϕ has no fixed points, then we clearly have

$$\phi^n(0) \to \infty \quad \text{and} \quad \phi^n(1) \to \infty, \quad (n \to \infty).$$

Next we assume that $0 < a, b < 1$. Once again ϕ is increasing, but now it has one point of inflection, and so there may be one, two, or three fixed points. For $n = 1, 2, \ldots,$ we have

$$\phi^n(0) < \phi^{n+1}(0) < \phi^{n+1}(1) < \phi^n(1),$$

and

$$\lim_{n\to\infty} \phi^n(0) = \lim_{n\to\infty} \phi^n(1) \tag{5}$$

is true if and only if ϕ has exactly one fixed point c. The condition $|\phi'(c)| \leqslant 1$ will then automatically be satisfied.

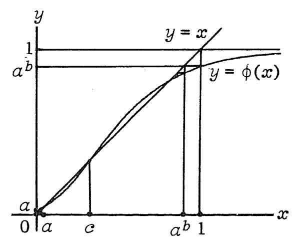

Figure 3

With more than one fixed point, as in Figure 3, both the limits in (5) exist, but they are not equal. This is an example of what Creutz and Sternheimer call "dual convergence."

Since the sequence a, a^b, $a^{(b^a)}$, ... is convergent if and only if the sequence b, b^a, $b^{(a^b)}$, ... is convergent, the cases $0<a<1<b$ and $0<b<1<a$ are equivalent. We may assume then, finally, that $0<a<1<b$. In this case, ϕ is decreasing and has a unique fixed point c.

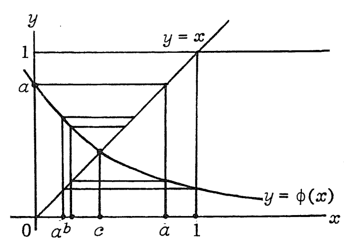

Figure 4

There are now four monotonic subsequences of interest. Indeed, for $n = 1, 2, \ldots$, we have

$$\phi^{2n-1}(1) < \phi^{2n}(0) < \phi^{2n+1}(1) < c < \phi^{2n+1}(0) < \phi^{2n}(1) < \phi^{2n-1}(0), \tag{6}$$

which is easily verified by induction, since $\phi^2 = \phi o \phi$ is increasing and has a fixed point at $x = c$. If $|\phi'(c)| > 1$, then no sequence of the form $\phi^n(x_0)$, $n = 1, 2, \ldots$, $x_0 > 1$, can converge to c, and so in this case we have another (but slightly different) example of dual convergence.

To prove that convergence does occur when $|\phi'(c)| \leqslant 1$, it is enough to show that ϕ^2 has in this case only one fixed point, namely c, since this would imply that

$$\lim_{n\to\infty} \phi^{2n}(0) = c = \lim_{n\to\infty} \phi^{2n}(1).$$

We are, therefore, reduced to proving that, for $0 < x < c$,

$$\phi(x) < \phi^{-1}(x),$$

or

$$a^{b^x} < (\log(\log x/\log a))/\log b.$$

With $\log a = se^{-t}$, $\log b = te^{-s}$, $c = e^s$, and $x = (1-u)e^s$ (cf. the proof of Lemma 1), this becomes, for $0 < u < 1$,

$$\exp[-s(1-e^{-ut})] < 1 + \frac{1}{t}\log\left(1 + \frac{1}{s}\log(1-u)\right), \tag{7}$$

which we must show to be true when $s < 0$, $t > 0$, and $|st| = |\phi'(c)| \leqslant 1$. In fact, it is enough to prove (7) when $s = -1/t$, which we now do.

Lemma 2

For $t > 0$ and $0 < u < 1$, we have

$$\exp\left[\frac{1-e^{-ut}}{t}\right] < 1 + \frac{1}{t}\log\left(1 + t\log\frac{1}{1-u}\right).$$

Proof: To prove the lemma, note that

$$\exp\left[\frac{1-e^{-ut}}{t}\right] < \exp\left[\frac{1}{t}\log(1+ut)\right] = (1+ut)^{1/t}, \quad (t > 0,\ u > 0),$$

and so, since there is equality at $u = 0$, it is enough to show that

$$\frac{d}{du}[(1+ut)^{1/t}] < \frac{d}{du}\left[1 + \frac{1}{t}\log\left(1 + t\log\frac{1}{1-u}\right)\right], \quad (t > 0,\ 0 < u < 1),$$

which is equivalent to

$$1 + t\log\frac{1}{1-u} < \frac{(1+ut)^{1-1/t}}{1-u}, \quad (t > 0,\ 0 < u < 1).$$

Again there is equality at $u = 0$, and so it is enough to show that

$$\frac{d}{du}\left[1 + t\log\frac{1}{1-u}\right] < \frac{d}{du}\left[\frac{(1+ut)^{1-1/t}}{1-u}\right], \quad (t > 0,\ 0 < u < 1),$$

which is equivalent to

$$(1+ut)^{1/t} < \frac{t-1}{t} + \frac{1+ut}{t(1-u)} = \frac{1}{1-u} + \frac{1}{t}\left(\frac{1}{1-u} - 1\right), \tag{8}$$

$$(t > 0,\ 0 < u < 1).$$

However, since

$$(1+ut)^{1/t} < e^u < \frac{1}{1-u}, \quad (t > 0,\ 0 < u < 1),$$

the estimate (8) does in fact hold. This completes the proof of Lemma 2 and also that of our theorem.

We now discuss the mapping $x = se^{-t}$, $y = te^{-s}$, $|st| \leqslant x$, which gives rise to the region in Figure 1. First, it is clear that, for $k = 1, 2, 3, 4$, the k^{th} quadrant in the st-plane is mapped into the k^{th} quadrant of the xy-plane. Next we observe that the mapping is one-to-one for $t > 0$ and $|st| \leqslant 1$. This follows from Lemma 1, if we recall from the proof of the theorem that, for $b > 1$, the function ϕ has a fixed point c with $|\phi'(c)| \leqslant 1$ if and only if this fixed point is unique. By symmetry, the mapping is also one-to-one for $s > 0$.

It is easy to check with a little calculus that the boundary of the image of $\{(s, t) : |st| \leqslant 1\}$ takes the form shown in Figure 1 in the first, second, and fourth quadrants. In the third quadrant, however, the mapping is not one-to-one and a more detailed discussion is required.

If $st = 1$ $(s, t < 0)$ and $x = se^{-t}$, $y = te^{-s}$, then

$$y < x < -e, \quad (s < -1) \quad \text{and} \quad x < y < -e, \quad (s > -1). \tag{9}$$

For instance, if $s < -1$, then the inequality

$$x = se^{-1/s} > s^{-1}e^{-s} = y$$

is equivalent (on putting $\sigma = -s$) to

$$2 \log \sigma < \sigma - 1/\sigma, \quad (\sigma > 1),$$

which is easily verified by differentiation. The maximum value of $se^{-1/s}$ for $s < 0$ occurs when $s = -1$, and so, for $x < -e$, the equation $x = se^{-1/s}$ has two solutions s_1, s_2 with $s_2 < -1 < s_1 < 0$. If $s_1t_1 = 1 = s_2t_2$ and

$$y_1(x) = t_1e^{-s_1}, \; y_2(x) = t_2e^{-s_2}, \quad (x < -e),$$

then y_1, y_2 are smooth functions in $(-\infty, -e)$ and, by (9),

$$y_2(x) < x < y_1(x) < -e, \quad (x < -e).$$

It is easy to check that

$$\lim_{x \to -e} y_1(x) = -e = \lim_{x \to -e} y_2(x)$$

and, using the chain rule, that

$$\lim_{x \to -e} y_1'(x) = 1 = \lim_{x \to -e} y_2'(x).$$

Hence, the image of $st = 1$ has a cusp at $(-e, -e)$.

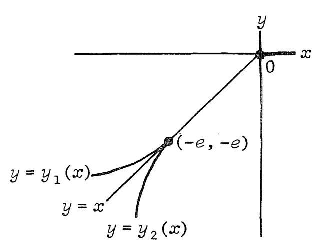

Figure 5

We now claim that the set

$$\{(x, y) : x < -e, \; y_2(x) \leqslant y \leqslant y_1(x)\}$$

is covered twice by the mapping and that the remainder of the third quadrant is covered once. These facts could be verified directly, or we can deduce them from Lemma 1 as follows.

Since, for $0 < a$ and $b < 1$, the maximum value of $\phi'(x)$ is $(-\log b)/e$ (this occurs when $1 + b^x \log a = 0$), we see that ϕ has exactly one fixed point c (and $\phi'(c) \leqslant 1$) if $0 < a < 1$ and $e^{-e} \leqslant b < 1$. This means, by Lemma 1, that

$$\{(x, y) : -\infty < x < 0, -e \leqslant y < 0\}$$

is covered exactly once.

If $0 < b < e^{-e}$, however, then there are numbers a_1 and a_2 with $0 < a_1 < a_2 < e^{-e}$ such that

$$y_1(\log a_1) = \log b = y_2(\log a_2),$$

and then the corresponding functions

$$\phi_1(x) = a_1^{b^x} \quad \text{and} \quad \phi_2(x) = a_2^{b^x}$$

each has a fixed point with derivative 1 (see the proof of Lemma 1). Since $\phi(x) = a^{b^x}$ is strictly monotonic in a when b, x are fixed, we see that for all $a \in [a_1, a_2]$, the function ϕ has two fixed points c such that $\phi'(c) \leqslant 1$. If $a \notin [a_1\ a_2]$, however, the function ϕ has only one such fixed point. By Lemma 1, this establishes the claim.

REFERENCES

1. I. N. Baker & P. J. Rippon. "Convergence of Infinite Exponentials." *Ann. Acad. Sci. Fenn.* Ser. A.I. Math., 8 (1983):179-86.
2. D. F. Barrow. "Infinite Exponentials." *Amer. Math. Monthly* 43 (1936):150-160.
3. M. Creutz & R. M. Sternheimer. "On the Convergence of Iterated Exponentiation—I." *The Fibonacci Quarterly* 18 (1980):341-47.
4. M. Creutz & R. M. Sternheimer. "On the Convergence of Iterated Exponentiation—II." *The Fibonacci Quarterly* 19 (1981):326-35.
5. L. Euler. "De Formulis Exponentialibus Replicatus." *Opera Omnia*, Series Primus XV:268-97; *Acta Academiae Petropolitanae* 1 (1777):38-60.
6. R. A. Knoebel. "Exponentials Reiterated." *Amer. Math. Monthly* 88 (1981): 235-52.
7. W. J. Thron. "Convergence of Infinite Exponentials with Complex Elements." *Proc. Amer. Math. Soc.* 8 (1957):1040-43.

◆◇◆◇◆

EULER'S PARTITION IDENTITY—ARE THERE ANY MORE LIKE IT?

HENRY L. ALDER
University of California, Davis, CA 95616

AMIN A. MUWAFI
American University of Beirut, Beirut, Lebanon

JEFFREY K. LEWIS
University of California, Davis, CA 95616

(Submitted August 1983)

INTRODUCTION

A *partition* of a positive integer n is defined as a way of writing n as a sum of positive integers. Two such ways of writing n in which the parts merely differ in the order in which they are written are considered the same partition. We shall denote by $p(n)$ the number of partitions of n. Thus, for example, since 5 can be expressed by

$$5,\quad 4+1,\quad 3+2,\quad 3+1+1,\quad 2+2+1,\quad 2+1+1+1, \text{ and } 1+1+1+1+1,$$

we have $p(5) = 7$.

The function $p(n)$ is referred to as the number of *unrestricted partitions* of n to make clear that no restrictions are imposed upon the way in which n is partitioned into parts. In this paper, we shall concern ourselves with certain restricted partitions, that is, partitions in which some kind of restriction is imposed upon the parts. Specifically, we shall consider identities valid for all positive integers n of the general type

$$p'(n) = p''(n), \tag{1}$$

where $p'(n)$ is the number of partitions of n where the parts of n are subject to a first restriction and $p''(n)$ is the number of partitions of n where the parts of n are subject to an entirely different restriction.

The most celebrated identity of this type is due to Euler [4], who discovered it in 1748.

Theorem 1 (Euler)

The number of partitions of n into distinct parts is equal to the number of partitions of n into odd parts.

Thus, for example, the partitions of 9 into distinct parts are

$$9,\quad 8+1,\quad 7+2,\quad 6+3,\quad 6+2+1,\quad 5+4,\quad 5+3+1,\quad 4+3+2,$$

that is, there are 8 such partitions, and the partitions of 9 into odd parts are

$$9,\quad 7+1+1,\quad 5+3+1,\quad 5+1+1+1+1,\quad 3+3+3,\quad 3+3+1+1+1,$$
$$3+1+\cdots+1,\quad 1+1+\cdots+1,$$

so that there are also 8 partitions of 9 into odd parts.

For a proof of this theorem by combinatorial methods, see [6], and by means of generating functions, see [2] or [3].

In [2], Alder has given a survey of the existence and nonexistence of generalizations of Euler's partition identity and, in [3], he has shown how to use generating functions to discover and prove the existence and the nonexistence of certain generalizations of this identity.

The use of generating functions, however, is by no means the only method for discovering partition identities or for proving their existence or nonexistence. Other methods, particularly those likely to produce positive results, that is, suggesting the existence of new partition identities, need, therefore, to be developed. Other points of view in looking at the possibility of the existence of such identities need to be encouraged. One such method is used in this paper. It is used to show that a certain generalization of a known partition identity cannot exist. It may well be, however, that as of yet unthought of techniques may prove successful in discovering a generalization.

In 1974 D. R. Hickerson [5] proved the following generalization of Euler's partition identity.

Theorem 2 (Hickerson)

If $f(r, n)$ denotes the number of partitions of n of the form $b_0 + b_1 + b_2 + \cdots + b_s$, where, for $0 \leqslant i \leqslant s - 1$, $b_i \geqslant rb_{i+1}$, and $g(r, n)$ denotes the number of partitions of n where each part is of the form $1 + r + r^2 + \cdots + r^i$ for some $i \geqslant 0$, then

$$f(r, n) = g(r, n). \tag{2}$$

Thus, for example, for $r = 2$, the partitions of 9 of the first type are

$9,\quad 8+1,\quad 7+2,\quad 6+3,\quad 6+2+1,$

so that $f(2, 9) = 5$, and the partitions of 9 of the second type, that is, where each part is chosen from the set $\{1, 3, 7, \ldots\}$, are

$7+1+1,\quad 3+3+3,\quad 3+3+1+1+1,\quad 3+1+\cdots+1,$ and $1+1+\cdots+1,$

so that also $g(2, 9) = 5$.

Hickerson gave a proof of this theorem, both by combinatorial methods and by means of generating functions.

In this paper we are addressing the question: Do there exist identities of the type given by Theorem 2, where the inequality $b_i \geqslant rb_{i+1}$ is replaced by $b_i > rb_{i+1}$?

THE NONEXISTENCE OF CERTAIN TYPES OF PARTITION IDENTITIES OF THE EULER TYPE

We shall consider the question stated above in the following more specific form: If $f(r, n)$ denotes the number of partitions of n of the form $b_0 + b_1 + \cdots + b_s$, where, for $0 \leqslant i \leqslant s - 1$, $b_i > rb_{i+1}$, and $g(r, n)$ denotes the number of partitions of n, where each part is taken from a set of integers S_r, for which r do there exist sets S_r such that $f(r, n) = g(r, n)$?

We know, of course, that for $r = 1$, there exists such a set, since Euler's partition theorem states that S_1 is the set of all positive odd integers. The question—whether there exist other values of r for which there exist sets S_r, so that (2) holds for all positive integers n—was posed at an undergraduate seminar on Number Theory by the first two authors in the Winter quarter 1983, and was answered with proof for all integers $r \geqslant 2$ by Jeffrey Lewis, namely as follows:

Theorem 3 (Lewis)

The number $f(r, n)$ of partitions of n of the form $b_0 + b_1 + \cdots + b_s$, where, for $0 \leqslant i \leqslant s - 1$, $b_i > rb_{i+1}$, r a positive integer, is not, for all n, equal to the number of partitions of n into parts taken from any set of integers whatsoever unless $r = 1$.

Proof of Theorem 3: We shall prove this theorem by contradiction. Let us assume that for some integer $r \geqslant 2$ there exists a set S_r of positive integers—denote the number of partitions of n into parts taken from that set by $g(r, n)$—for which $f(r, n) = g(r, n)$ for all n.

Since $f(r, 1) = 1$, we see that $1 \in S_r$ [otherwise, $g(r, 1) = 0$]. Since $f(r, 2) = 1$, it follows that $2 \notin S_r$ [otherwise, $g(r, 2) = 2$]. Since $f(r, 3) = f(r, 4) = \cdots = f(r, r+1) = 1$, we conclude that $3 \notin S_r$, $4 \notin S_r$, ..., $r + 1 \notin S_r$.

Now $f(r, r+2) = 2$, since the partitions of $r + 2$ for which $b_i > rb_{i+1}$ are $(r+2)$ and $(r+1)+1$. It follows that $r + 2 \in S_r$ [otherwise, $g(r, r+2) = 1$).

Thus, we have verified the entries in Table 1 up to $n = r+2$. We will now complete the construction of this table.

Table 1. Determination of the Elements of S_r for r an Integer $\geqslant 2$

n	$f(r, n)$	$g(r, n)$ if $n \notin S_r$	$g(r, n)$ if $n \in S_r$	Conclusion
1	1	0	1	$1 \in S$
2	1	1	2	$2 \notin S$
3	1	1	2	$3 \notin S$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$r + 1$	1	1	2	$r + 1 \notin S$
$r + 2$	2	1	2	$r + 2 \in S$
$r + 3$	2	2	3	$r + 3 \notin S$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2r + 2$	2	2	3	$2r + 2 \notin S$
$2r + 3$	3	2	3	$2r + 3 \in S$
$2r + 4$	3	4	5	Contradiction

Next we determine the least value of n for which $f(r, n) = 3$. This occurs if n is of either of the forms

$$n = b_0 + b_1 + 1 \quad \text{with} \quad b_0 > rb_1 \quad \text{and} \quad b_1 > r$$

or

$$n = b_0 + 2 \quad \text{with} \quad b_0 > 2r.$$

The least n for which the first can occur is

$$n = (r^2 + r + 1) + (r + 1) + 1 = r^2 + 2r + 3.$$

The least n for which the second can occur is

$$n = (2r + 1) + 2 = 2r + 3.$$

Since $2r + 3 < r^2 + 2r + 3$ for all positive r, it follows that $n = 2r + 3$ is the least value of n for which $f(r, n) = 3$. In that case, the partitions of $2r + 3$ for which $b_i > rb_{i+1}$ are $(2r+3)$, $(2r+2) + 1$, $(2r+1) + 2$. Now, since thus far only $1 \in S_r$ and $r + 2 \in S_r$, it follows that there are only two partitions of $2r + 3$ into parts taken from that set, namely

$$(r + 2) + 1 + \cdots + 1 \quad \text{and} \quad 1 + 1 + \cdots + 1,$$

so that we need $2r + 3 \in S_r$ in order to make $g(r, 2r+3) = 3$.

Now $f(r, 2r+4) = 3$, since the only partitions of $2r + 4$, with $b_i > rb_{i+1}$, are $(2r+4)$, $(2r+3) + 1$, $(2r+2) + 2$. (Note that it is here where we are using the fact that $r \geqslant 2$.) On the other hand, the partitions of $2r + 4$ into parts taken from the set $\{1, r+2, 2r+3\}$ are

$$(2r+3) + 1, \quad (r+2) + (r+2), \quad (r+2) + 1 + 1 + \cdots + 1, \quad 1 + 1 + \cdots + 1,$$

so that $g(r, 2r+3) = 4$ if $2r + 4 \notin S_r$ and $g(r, 2r+3) = 5$ if $2r + 4 \in S_r$, which is a contradiction.

The question arises whether Theorem 3 is true also for all values of $r > 1$. We have some partial answers to this question.

Theorem 4

The nonexistence of sets S_r given in Theorem 3 also applies to all r in any of the intervals $N \leqslant r < N + 1/2$, where N is any integer $\geqslant 2$.

Proof of Theorem 4: This proof is identical to that for Theorem 3, except that, in the construction of Table 1, the entries in the columns for n and the conclusions have to be changed by replacing r in every case by $[r]$, the grestest integer in r. Note that the condition that $r < N + 1/2$ is needed in the determination of the partitions of $2[r] + 3$ with $b_i > rb_{i+1}$, which are

$$(2[r] + 3), \quad (2[r] + 2) + 2, \text{ and } (2[r] + 1) + 2,$$

the latter satisfying the inequality, since

$$2[r] + 1 = 2N + 1 = 2\left(N + \frac{1}{2}\right) > 2r.$$

Now, for values of r for which $N + (1/2) \leqslant r < N + 1$, we have a method for proving the nonexistence of S_r for certain intervals, but have no method which will give a conclusion valid for all such intervals. We illustrate this method for intervals in the range $2.50 \leqslant r < 3.00$.

First we use the same method used in the construction of Table 1 to determine the elements of S_r for $r = 2.50$. (See Table 2.)

Since a contradiction is obtained for $n = 20$, it follows that for $r = 2.50$ no set S_r can exist for which $f(r, n) = g(r, n)$ for all positive integers n.

Next we note that Table 2 applies for all r with $2.50 \leqslant r < x/y$, where x/y is the least rational number > 2.50 for which both x and y appear as parts in a partition counted by $f(r, n)$ in Table 2; that is, we need to find the least rational number $x/y > 2.50$ for which $x + y \leqslant 20$. This clearly is 13/5, since 13 + 5 is a partition of 18 and, therefore, Table 2 would not be applicable for $r = 13/5$ because the partition of $18 = 13 + 5$ would not satisfy $13 > 5r$ for $r = 13/5$.

Thus, Table 2 is applicable for all r with $2.50 \leqslant r < 13/5$, and the nonexistence of the sets S_r follows for all r in this interval.

Table 2. Determination of the Elements of S_r for $r = 2.50$

n	$f(r, n)$	$g(r, n)$ if $n \notin S$	$g(n, r)$ if $n \in S$	Conclusion
1	1	0	1	$1 \in S$
2	1	1	2	$2 \notin S$
3	1	1	2	$3 \notin S$
4	2	1	2	$4 \in S$
5	2	2	3	$5 \notin S$
6	2	2	3	$6 \notin S$
7	2	2	3	$7 \notin S$
8	3	3	4	$8 \notin S$
9	3	3	4	$9 \notin S$
10	3	3	4	$10 \notin S$
11	4	3	4	$11 \in S$
12	5	5	6	$12 \notin S$
13	5	5	6	$13 \notin S$
14	5	5	6	$14 \notin S$
15	6	6	7	$15 \notin S$
16	7	7	8	$16 \notin S$
17	7	7	8	$17 \notin S$
18	8	7	8	$18 \in S$
19	9	9	10	$19 \notin S$
20	9	10	11	Contradiction

We now construct, by programming on a computer, a table similar to Table 2 for $r = 13/5$ (not shown here), obtaining a contradiction for $n = 52$. Next, we note that this table applies to all r with $13/5 \leqslant r < x/y$, where x/y is the least rational number $> 13/5$ for which $x + y \leqslant 52$. This clearly is $34/13$, so that this table is applicable for all r with $13/5 \leqslant r < 34/13$. Constructing a table similar to Table 2 for $r = 34/13$, we obtain a contradiction for $n = 136$ and find that this table is valid for all r with $34/13 \leqslant r < 89/34$. Then, constructing the appropriate table for $r = 89/34$, we were unable to obtain a contradiction on the computer in the time available, that is, for $n \leqslant 181$.

Though we were unable to obtain a contradiction for $r = 89/34 = 2.6176...$, we were able to obtain one for $r = 2.62$, namely for $n = 90$ and, using the previously described method, to determine that this table is valid for all r with $2.62 \leqslant r < 21/8$. Then, considering $r \geqslant 21/8$, we were able to obtain contradictions for all $r < 32/11 = 2.909...$ for the values of n indicated in Table 3.

For values of $r \geqslant 32/11$, the corresponding tables again became so long that the time available on the computer to arrive at a contradiction was exceeded; thus, we have no conclusions for $32/11 \leqslant r < 3$.

For values of r between 1 and 2, the smallest value of r we considered was $r = 1.08$, for which we obtained a contradiction for $n = 54$. Using the same method as used for values of r in the interval $2.50 \leqslant r < 32/11$, it was possible to prove the nonexistence of S_r for all r in the short interval $1.08 \leqslant r < 25/23 = 1.0869...$.

To obtain results valid for larger intervals, we started with $r = 1.25$ and proved the nonexistence of S_r for all r in the interval $1.25 \leqslant r < 23/12 = 1.9166...$, as indicated in Table 4.

Table 3. The Nonexistence of S_r for $2.50 \leqslant r < 89/34 = 2.6176\ldots$ and $2.62 \leqslant r < 32/11 = 2.909\ldots$

Interval	Value of n for Which Contradiction Occurs
$2.50 \leqslant r < 13/5$	20
$13/5 \leqslant r < 34/13$	52
$34/13 \leqslant r < 89/34$	136
$89/34 \leqslant r < 55/21$	No conclusion
$55/21 \leqslant r < 21/8$	90
$21/8 \leqslant r < 8/3$	38
$8/3 \leqslant r < 11/4$	17
$11/4 \leqslant r < 14/5$	21
$14/5 \leqslant r < 17/6$	26
$17/6 \leqslant r < 20/7$	30
$20/7 \leqslant r < 23/8$	34
$23/8 \leqslant r < 26/9$	48
$26/9 \leqslant r < 29/10$	44
$29/10 \leqslant r < 32/11$	48

Table 4. The Nonexistence of S_r for $1.25 \leqslant r < 23/12 = 1.9166\ldots$

Interval	Value of n for Which Contradiction Occurs
$1.25 \leqslant r < 9/7$	18
$9/7 \leqslant r < 4/3$	18
$4/3 \leqslant r < 7/5$	14
$7/5 \leqslant r < 3/2$	14
$3/2 \leqslant r < 5/3$	10
$5/3 \leqslant r < 7/4$	18
$7/4 \leqslant r < 9/5$	18
$9/5 \leqslant r < 11/6$	21
$11/6 \leqslant r < 13/7$	24
$13/7 \leqslant r < 15/8$	28
$15/8 \leqslant r < 17/9$	33
$17/9 \leqslant r < 19/10$	36
$19/10 \leqslant r < 21/11$	39
$21/11 \leqslant r < 23/12$	42

For values of $r < 1.25$, as indicated above, the intervals for which a table similar to Table 2 is valid become very small. Considering the values of $r = 1.08, 1.09, \ldots, 1.20$, separately, we obtained a contradiction for each of them. For values of r close to 1, the time available on the computer to arrive at a contradiction was exceeded. This is not surprising, because we know that, for $r = 1$, we have the Euler identity and, therefore, no contradiction can be obtained. For values of r in the interval $1 < r < 1.25$, except for those listed above and for those in the interval $23/12 \leqslant r < 2$, we have no conclusions.

It is an interesting question whether Theorem 3 can be proved by a method valid for all nonintegral values of $r > 1$.

The authors are greatly indebted to M. Reza Monajjemi for developing the program needed to construct Tables 3 and 4, and for cheerfully spending many hours in helping to prepare them.

REFERENCES

1. H. L. Alder. "The Nonexistence of Certain Identities in the Theory of Partitions and Compositions." *Bull. Amer. Math. Soc.* 54 (1948):712-22.
2. H. L. Alder. "Partition Identities—from Euler to the Present." *Amer. Math. Monthly* 76 (1969):733-46.
3. H. L. Alder. "The Use of Generating Functions To Discover and Prove Partition Identities." *Two-Year College Math. J.* 10 (1979):318-29.
4. L. Euler. "Introductio in Analysin Infinitorium." *Lausanne* 1 (1748):253-275.
5. D. R. Hickerson. "A Partition Identity of the Euler Type." *Amer. Math. Monthly* 81 (1974):627-29.
6. I. Niven & H. S. Zuckerman. *An Introduction to the Theory of Numbers*, 4th ed., p. 268. New York: Wiley, 1980.

◆◇◆◇◆

SOME GENERALIZED LUCAS SEQUENCES

J. H. CLARKE and A. G. SHANNON
The New South Wales Institute of Technology, Sydney, Australia

(Submitted August 1983)

1. INTRODUCTION

In classical usage the *fundamental* and *primordial* second-order recurrences are those of Fibonacci and Lucas, $\{F_n\}$ and $\{L_n\}$, defined by the linear homogeneous recurrence relation

$$U_n = U_{n-1} + U_{n-2}, \quad n > 2, \tag{1.1}$$

with initial conditions $F_1 = 1$, $F_2 = 1$, and $L_1 = 1$, $L_2 = 3$. They are usually generalized by altering the recurrence relation or the initial conditions as described by Horadam [4].

There have been many generalizations of the Fibonacci numbers (cf. Bergum & Hoggatt [1] and Shannon [11]), but fewer published attempts to generalize the corresponding Lucas numbers, though those of Hoggatt and Bicknell-Johnson (cf. [4]) are notable exceptions.

We believe that the following exposition is a useful addition to the literature because, unlike other papers, which concentrate on particular properties, we focus on the unexpected structure of the generalized recurrence relation. This complements the existing literature because the solution of our recurrence relation is the one used by the authors to develop various properties of these sequences. The corresponding approach for the Fibonacci numbers has been applied by Hock and McQuiston [3]. From the simple form of the recurrence relation as revealed here, we specify some particular generalized sequences and two special properties that will be of use to future researchers of the abritrary-order recurrences who utilize the coefficients of the recurrence relation.

We choose here to generalize the Lucas sequence by considering the r^{th}-(arbitrary)-order linear recurrence relation

$$v_n^{(r)} = v_{n-r+1}^{(r)} + v_{n-r}^{(r)}, \quad n \geqslant r > 1, \tag{1.2}$$

and initial conditions $v_n^{(r)} = 0$ if $0 < n < r - 1$, $v_{r-1}^{(r)} = r - 1$ and $v_0^{(r)} = r$. The notation is due to Williams [12] and has been used since then by several authors in studying r^{th}-order recurrences.

Thus, $\{v_n^{(2)}\} \equiv \{L_n\}$, and the accompanying table displays the first 16 terms of $\{v_n^{(r)}\}$ for $r = 2, 3, 4, 5, 6$.

Table 1. Generalized Lucas Numbers for $n \geqslant 0$

$r \backslash n$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	1	3	4	7	11	18	29	47	76	123	199	322	521	843	1364	2207
3	3	0	2	3	2	5	5	7	10	12	17	22	29	39	51	68	90
4	4	0	0	3	4	0	3	7	4	3	10	11	7	13	21	18	20
5	5	0	0	0	4	5	0	0	4	9	5	0	4	13	14	5	4
6	6	0	0	0	0	5	6	0	0	0	5	11	6	0	0	5	16

For example, from the table, we have that

$$v_n^{(4)} = v_{n-3}^{(4)} + v_{n-4}^{(4)} \quad \text{or} \quad 20 = v_{16}^{(4)} = v_{13}^{(4)} + v_{12}^{(4)} = 13 + 7.$$

We propose to consider some of the properties of $\{v_n^{(r)}\}$ that arise from the interesting fact that all but three of the coefficients in the recurrence relation are zero.

2. GENERAL TERMS

The auxiliary equation associated with the recurrence relation (1.2) is

$$x^r - x - 1 = 0, \tag{2.1}$$

which we assume has distinct roots, α_j, $j = 1, 2, \ldots, r$. In fact, $v_n^{(r)}$ is (in the terminology of Macmahon [8]) the homogeneous product sum of weight n of the quantities α_j. It is the sum of a number of symmetric functions formed from a partition of n as elaborated in Shannon [10]. The first three cases are

$$\begin{aligned}
v_1^{(r)} &= P_{r1} &&= \sum \alpha_j \\
v_2^{(r)} &= P_{r1}^2 + P_{r2} &&= \sum \alpha_j^2 + \sum \alpha_i \alpha_j \\
v_3^{(r)} &= P_{r1}^3 + 2P_{r1}P_{r2} + P_{r3} &&= \sum \alpha_j^3 + \sum \alpha_i^2 \alpha_j + \sum \alpha_i \alpha_j \alpha_k
\end{aligned}$$

in which P_{rm} is $(-1)^{m+1}$ times the sum of the α_j taken m at a time as in the theory of equations. More generally,

$$v_n^{(r)} = \sum_{\Sigma\lambda = n} \prod_{i=1}^{r} \alpha_i^{\lambda_i},$$

so that since $P_{rm} = 0$ except for P_{rr} and $P_{r,r-1}$, which are unity, we have

$$v_n^{(r)} = \sum_{j=1}^{r} \alpha_j^n \quad \text{for } n = 1, 2, \ldots, r. \tag{2.2}$$

Then, if we assume the result (2.2) is true for $n = k - 1$:

$$\begin{aligned}
v_k^{(r)} &= v_{k-r+1}^{(r)} + v_{k-r}^{(r)} \\
&= \sum_{j=1}^{r} (\alpha_j^{k-r+1} + \alpha_j^{k-r}) = \sum_{j=1}^{r} \alpha_j^{k-r}(\alpha_j + 1) = \sum_{j=1}^{r} \alpha_j^{k-r}\alpha_j^r = \sum_{j=1}^{r} \alpha_j^k.
\end{aligned}$$

By the Principle of Mathematical Induction, we get

$$v_n^{(r)} = \sum_{j=1}^{r} \alpha_j^n. \tag{2.3}$$

For example,

$$v_n^{(2)} = (1.61803)^n + (-0.61803)^n,$$

the well-known result for the Lucas numbers.

Similarly, for instance, with $i^2 = -1$,

$$v^{(3)} = (1.32472)^n + (-0.66236 + 0.07165i)^n + (-0.66236 - 0.07165i)^n,$$

and

$$v^{(4)} = (1.22075)^n + (-0.7245)^n + (-0.2481 + 1.341i)^n + (-0.2481 - 1.0341i)^n.$$

3. GENERAL PROPERTIES

Among the various properties that can be investigated, we focus on two that follow directly from (2.1) and (1.2).

For odd values of r, (2.1) has the real solution

$$\alpha = (1 + \alpha)^{1/r}$$

which leads to the approximation

$$\alpha \doteqdot r/(r - 1); \tag{3.1}$$

for even values of r, we get

$$\alpha \doteqdot \pm(1 + \alpha/r)$$

or

$$\alpha \doteqdot r/(r \pm 1). \tag{3.2}$$

These are the initial approximate values which, by repeated iterations, converge to the real roots. Furthermore, we observe in (3.1) and (3.2) that as r increases, α approaches unity, which can be confirmed readily with a few numerical examples.

For notational convenience, we assume that u_n exists for $n < 0$. Then, for any $j \in \mathbf{Z}_+$,

$$v_n^{(r)} = \sum_{i=0}^{j} \binom{j}{i} v_{n-rj+1}^{(r)}. \tag{3.3}$$

Proof: We use induction on j. When $j = 1$, (3.3) reduces to the recurrence relation (1.2). Suppose the result is true for $j = 2, 3, \ldots, k - 1$. Then

$$\begin{aligned}\sum_{i=0}^{k} \binom{k}{i} v_{n-rk+i}^{(r)} &= \sum_{i=0}^{k-1} \binom{k-1}{i} v_{n-rk+i}^{(r)} + \sum_{i=1}^{k-1} \binom{k-1}{i-1} v_{n-rk+i}^{(r)} \\ &= \sum_{i=0}^{k-1} \binom{k-1}{i} v_{n-r-r(k-1)+i}^{(r)} + \sum_{i=0}^{k-1} \binom{k-1}{i} v_{n-r-r(k-1)+i+1}^{(r)} \\ &= v_{n-r}^{(r)} + v_{n-r+1}^{(r)} = v_n^{(r)}, \text{ as required.}\end{aligned}$$

4. A DIVISIBILITY RESULT

If we refer to Table 1 again, we observe that 5 divides $v_{10}^{(4)}$, $v_{10}^{(5)}$, and $v_{10}^{(6)}$, 7 divides $v_{14}^{(4)}$, $v_{14}^{(5)}$, and $v_{14}^{(6)}$, etc. More generally, this can be expressed as

$$p \,|\, v_{pr}^{(r+n)} \text{ for } n > 1,\ r > 1, \text{ and prime } p > 2. \tag{4.1}$$

Proof: $v_{pr}^{(r+n)} = \sum_{j=1}^{r+n} \alpha_j^{pr}$

$$\begin{aligned} &= \sum_{j=1}^{r+n} ((\alpha_j + 1)/\alpha_j^2)^p \quad \text{from (2.1)} \\ &= \sum_{j=1}^{r+n} \sum_{k=0}^{p} \binom{p}{k} \alpha_j^{-p-k} \\ &= \sum_{j=1}^{r+n} (\alpha_j^{-p} + \alpha_j^{-2p}) + \text{multiples of } p.\end{aligned}$$

This follows from Hardy and Wright [2, p. 64] and the fact that

$$\binom{p}{k}\sum_{j=1}^{r+n}\alpha_j^{-p-k}$$

is an integer because $\Pi_{j=1}^{r+n}\alpha_j^{-p-k} = \pm 1$. It remains to show that

$$p\,\Big|\,\sum_{j=1}^{r+n}(\alpha_j^{-p} + \alpha_j^{-2p}).$$

The polynomial with zeros $1/\alpha_j$ is

$$f(x) = x^{r+n} + x^{r+n-1} - 1. \tag{4.2}$$

From the theory of equations, we have that

$$\begin{aligned} f'(x)/f(x) &= \sum_{j=1}^{r+n} 1/(x - x_j) \qquad \text{where } x_j = 1/\alpha_j \\ &= \sum_{j=1}^{r+n}\frac{1}{x}\left(1 - \frac{x_j}{x}\right)^{-1} \qquad \text{with } x_j < x. \end{aligned}$$

Thus

$$f'(x)/f(x) = \sum_{j=1}^{r+n}\ \sum_{m=0}^{\infty} x_j^m/x^{m+1} = \sum_{m=0}^{\infty} v_m^{(r+n)}/x^{m+1}. \tag{4.3}$$

Now, $f'(x) = (r+n)x^{r+n-1} + (r+n-1)x^{r+n-2}$ and, by division,

$$f'(x)/f(x) = (r+n)x^{-1} - x^{-2} + x^{-3} - x^{-4} + x^{-5} - \cdots . \tag{4.4}$$

Since p is odd and $2p$ is even, we get from (4.3) and (4.4) that if $\Sigma_{j=1}^{r+n}\alpha_j^{-p} = -1$, then $\Sigma_{j=1}^{r+n}\alpha_j^{-2p} = +1$, and vice versa. Hence,

$$0 = \sum_{j=1}^{r+n}(\alpha_j^{-p} + \alpha_j^{-2p}), \text{ as required.}$$

5. CONCLUDING COMMENTS

The consideration of $v_n^{(r)}$ for $n < 0$ suggests the use of a result from Polyá and Szegö [9] to express the general term on the *negative* side of the sequence. Thus, for $n < 0$,

$$v_n^{(r)} = \sum_{k=0}^{[m/r]} \frac{m}{m - (r-1)k}\binom{m - (r-1)k}{k}(-1)^{m-rk}$$

in which $m = -n$, and $[\cdot]$ represents the greatest integer function.

The first few values are displayed in Table 2.

Table 2. Generalized Lucas Numbers for $n < 0$

$r \backslash n$	-9	-8	-7	-6	-5	-4	-3	-2	-1
2	-76	47	-29	18	-11	7	-4	3	-1
3	-7	5	-1	-2	4	-3	2	1	-1
4	-19	13	-8	7	-6	5	-1	1	-1

For example, when $r = 2$, we get the known result of Lucas [7]:

$$v_n^{(2)} = \sum_{k=0}^{[n/2]} \frac{n}{n-k}\binom{n-k}{k}(-1)^{n-1}. \tag{5.2}$$

The recurrence relation for (5.1) is (with $m = -n$)

$$(-1)^m v_m^{(r)} = (-1)^{m-1} v_{m-1}^{(r)} + (-1)^{m-r} v_{m-r}^{(r)}$$

so that these $v_m^{(r)} = (-1)^m A_m$ of Hock and McQuistan [3] who apply this sequence to a problem on the occupation statistics of lattice spaces in relation to a number of physical phenomena.

Other extensions can be found by developing an associated generalized Fibonacci sequence $\{u_n^{(r)}\}$, related to $\{v_n^{(r)}\}$ by, for instance

$$v_n^{(r)} = n \sum_{\gamma(n)} \frac{(-1)^{k-1}}{k} u_{a_1}^{(r)} \ldots u_{a_k}^{(r)},$$

in which $\gamma(n)$ indicates summation over all the compositions $(a_1, a_2, \ldots, a_k)$ of n as in Shannon [11]. For example, when $r = 2$,

$$\begin{aligned} L_1 &= 1 = f_1, \\ L_2 &= 3 = -\tfrac{2}{2} f_1 f_1 + \tfrac{2}{1} f_2 = -1 + 4, \\ L_3 &= 4 = -\tfrac{3}{2} f_1 f_2 - \tfrac{3}{2} f_2 f_1 + \tfrac{3}{1} f_3 + \tfrac{3}{3} f_1 f_1 f_1 = -3 - 3 + 9 + 1, \end{aligned}$$

where $\{f_n\}$ is the sequence of Fibonacci numbers that satisfy (1.1) with initial conditions $f_1 = 1$, $f_2 = 2$. The use of the lower-case letters for notational convenience ($f_n \equiv F_{n+1}$) is not new (cf. [6]).

Thanks are due to Lambert Wilson [13] for the development of Table 1.

REFERENCES

1. G. E. Bergum & V. E. Hoggatt, Jr. "An Application of the Characteristic of the Generalized Fibonacci Sequence." *The Fibonacci Quarterly* 15, no. 3 (1977):215-20.
2. G. M. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers.* 4th ed. Oxford: Clarendon Press, 1965.
3. J. L. Hock & R. B. McQuistan. "The Occupational Degeneracy for λ-Bell Particles on a Saturated λ × W Lattice Space." *The Fibonacci Quarterly* 21, no. 3 (1983):196-202.
4. V. E. Hoggatt, Jr., & Marjorie Bicknell-Johnson. "Generalized Lucas Sequences." *The Fibonacci Quarterly* 15, no. 2 (1977):131-39.
5. A. F. Horadam. "A Generalized Fibonacci Sequence." *Amer. Math. Monthly* 68 (1971):455-59.
6. A. F. Horadam. "Generating Functions for Powers of a Certain Generalized Sequence of Numbers." *Duke Math. J.* 32 (1965):437-46.
7. Edouard Lucas. "Théorie des fonctions numériques simplement périodiques." *Amer. J. Math.* 1 (1878):184-240.
8. Percy A. Macmahon. *Combinatory Analysis.* Vol. I. Cambridge: University Press, 1915.

9. G. Polyá & G. Szegö. *Aufgaben und Lehrsatze aus der Analysis*. Vol. 2. Berlin: Springer, 1925.
10. A. G. Shannon. "Some Properties of a Fundamental Recursive Sequence of Arbitrary Order." *The Fibonacci Quarterly* 12, no. 4 (1974):327-35.
11. A. G. Shannon. "Fibonacci Analogs of the Classical Polynomials." *Math. Magazine* 48 (1975):123-30.
12. H. C. Williams. "On a Generalization of the Lucas Functions." *Acta Arithmetica* 20 (1972):33-51.
13. L. G. Wilson. Some partial sums divisible by prime n, private communication, 1981.

◆◇◆◇◆

A CHARACTERIZATION OF THE SECOND-ORDER STRONG DIVISIBILITY SEQUENCES

P. HORAK and L. SKULA
J. E. Purkyně University, Brno, Czechoslovakia

(Submitted September 1983)

The Fibonacci numbers satisfy the well-known equation for greatest common divisors (cf. [2], [4]):

$$(F_i, F_j) = F_{(i,j)} \quad \text{for all } i, j \geqslant 1. \tag{1}$$

Equation (1) is also satisfied by some other second-order recurring sequences of integers, e.g., Pell numbers or Fibonacci polynomials evaluated at a fixed integer (cf. [1]). In [3], Clark Kimberling put a question: Which recurrent sequences satisfy the equation (1)? In our paper, we answer this question for a certain class of recurring sequences, namely that of the second-order linear recurrent sequences of integers.

We shall study the sequences $\mathbf{u} = \{u_n : n = 1, 2, \ldots\}$ of integers defined by

$$u_1 = 1, \quad u_2 = b, \quad u_{n+2} = c \cdot u_{n+1} + d \cdot u_n, \quad \text{for } n \geqslant 1,$$

where b, c, d are arbitrary integers. The system of all such sequences will be denoted by U. The system of all the sequences from U, having the property

$$(u_i, u_j) = |u_{(i,j)}| \quad \text{for all } i, j \geqslant 1, \tag{2}$$

will be denoted by D.

The main result of our paper is a complete characterization of all sequences from D. By describing D we solve, in fact, a more general problem of complete characterization of all the second-order, strong-divisibility sequences, i.e., all sequences $\{u_n\}$ of integers defined by

$$u_1 = a, \quad u_2 = b, \quad u_{n+2} = c \cdot u_{n+1} + d \cdot u_n, \quad \text{for } n \geqslant 1,$$

(where a, b, c, d are arbitrary integers) and satisfying equation (2). It is easy to prove that the second-order, strong-divisibility sequences are precisely all integral multiples of sequences from D.

1. CERTAIN SYSTEMS OF SEQUENCES FROM U

Systems U_1, F, F_1, G, G_1, H will be systems of all sequences $\mathbf{u} = \{u_n\}$ from U defined by $u_1 = 1$, $u_2 = b$, and by the recurrence relations (for $n \geqslant 1$):

$$U_1 : u_{n+2} = b \cdot f \cdot u_{n+1} + d \cdot u_n, \quad \text{where } b, d, f \neq 0, F \neq 1, (d, b) = (d, f) = 1;$$

$$F : u_{n+2} = b \cdot u_{n+1} + d \cdot u_n;$$

$$F_1 : u_{n+2} = b \cdot u_{n+1} + d \cdot u_n, \quad \text{where } (d, b) = 1;$$

$$G : u_{n+2} = d \cdot u_n;$$

$$G_1 : u_{n+2} = d \cdot u_n, \quad \text{where } d = 1 \text{ or } d = -1;$$

$$H : u_{n+2} = c \cdot u_{n+1}.$$

It is obvious that $F_1 \subseteq F$ and $G_1 \subseteq G$. Further, we define sequences **a**, **b**, **c**, **d**, **e**, **f** $= \{u_n\} \in U$ by:

$$\mathbf{a}: u_n = 1 \text{ for all } n \geqslant 1 \qquad \mathbf{b}: u_n = \begin{cases} 1 & \text{if } n \text{ is odd} \\ -1 & \text{if } n \text{ is even} \end{cases}$$

$$\mathbf{c}: u_n = \begin{cases} 1 & \text{if } n = 1 \\ -1 & \text{if } n > 1 \end{cases} \qquad \mathbf{d}: u_n = \begin{cases} 1 & \text{if } n = 1 \text{ or } n \text{ is even} \\ -1 & \text{if } n \neq 1 \text{ and } n \text{ is odd} \end{cases}$$

$$\mathbf{e}: u_n = \begin{cases} 1 & \text{if } 3 \nmid n \\ -2 & \text{if } 3 \mid n \end{cases} \qquad \mathbf{f}: u_n = \begin{cases} 1 & \text{if } n \equiv 1, 5 \pmod 6 \\ -1 & \text{if } n \equiv 2, 4 \pmod 6 \\ -2 & \text{if } n \equiv 3 \pmod 6 \\ 2 & \text{if } n \equiv 0 \pmod 6 \end{cases}$$

Let us denote $A = \{\mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{f}\}$. Directly from the definitions we obtain:

1.1 Proposition

1. **a**, **b**, **c**, **d**, **e**, **f** $\in D$, i.e., $A \subseteq D$
2. **a**, **b**, **c**, **d** $\in H$
3. **a**, **b**, **e**, **f** $\in U_1$
4. **a**, **b** $\in F_1 \cap G_1$

1.2 Proposition

Let $\mathbf{u} = \{u_n\} \in G$. Then $\mathbf{u} \in D$ if and only if $\mathbf{u} \in G_1$.

Proof: Let $\mathbf{u} \in D$; then $(u_3, u_4) = 1$ and consequently $\mathbf{u} \in G_1$. Let $\mathbf{u} \in G_1$; then for $k \geqslant 0$ we get $u_{4k+1} = 1$, $u_{4k+2} = b$, $u_{4k+3} = \pm 1$, $u_{4k+4} = \pm b$. Thus, for $i, j \geqslant 1$,

$$(u_i, u_j) = \begin{cases} 1 & \text{if } i \text{ is odd or } j \text{ is odd} \\ |b| & \text{if } i \text{ is even and } j \text{ is even} \end{cases}$$

and therefore, $\mathbf{u} \in D$.

1.3 Proposition

Let $\mathbf{u} = \{u_n\} \in H$. Then $\mathbf{u} \in D$ if and only if $\mathbf{u} \in \{\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}\}$.

Proof: Let $\mathbf{u} \in D$; then $(u_2, u_3) = (u_3, u_4) = 1$ and we get $|b| = 1$, $|c| = 1$, and consequently $\mathbf{u} \in \{\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}\}$. The rest of the proposition follows from 1.1.

1.4 Proposition

Let $\mathbf{u} = \{u_n\} \in U$, such that $c, d \neq 0$. Then, the following statements are equivalent:

(i) $(u_i, u_j) = |u_{(i,j)}|$ for $1 \leqslant i, j \leqslant 4$,

(ii) $\mathbf{u} \in U_1 \cup F_1$.

Proof: Let (i) be true. From $(u_2, u_3) = 1$ we get $(b, d) = 1$. From $u_2 | u_4$ we get $b | c$, $b \neq 0$. Therefore, there is an integer $f \neq 0$, such that $c = bf$. Since $(u_3, u_4) = 1$, we have $(d, f) = 1$ and thus $\mathbf{u} \in U_1 \cup F_1$.

Let $\mathbf{u} \in U_1 \cup F_1$. Then $u_3 = d + b^2 f$, $u_4 = b(d + df + b^2 f^2)$, where $b, f \neq 0$, $(d, b) = (d, f) = 1$. Let p be a prime, $p | u_3$ and $p | u_4$. Obviously $p \nmid b$, and so $d + b^2 f \equiv 0 \pmod p$, $d + df + b^2 f^2 \equiv 0 \pmod p$. Hence $b^2 f \equiv 0 \pmod p$ and consequently $p | f$, $p | d$, a contradiction. Thus $(u_3, u_4) = 1 = |u_1|$. The remaining cases of (i) obviously hold.

2. THE SYSTEM OF SEQUENCES F

The following two results are easily proved by mathematical induction, in the same way as for the Fibonacci numbers (cf. [4]).

2.1 Proposition

Let $\mathbf{u} = \{u_n\} \in F$. Then for any $k \geqslant 2$, $m \geqslant 1$ it holds

$$u_{k+m} = u_k u_{m+1} + d \cdot u_{k-1} u_m.$$

2.2 Proposition

Let $\mathbf{u} = \{u_n\} \in F$ and $k, m \geqslant 1$ be integers. If $k | m$, then $u_k | u_m$.

2.3 Proposition

Let $\mathbf{u} = \{u_n\} \in F$. Then the following statements are equivalent.

(i) $(u_2, u_3) = 1$

(ii) $(u_n, u_{n+1}) = 1$ for all $n \geqslant 1$

(iii) $\mathbf{u} \in D$

(iv) $\mathbf{u} \in F_1$

Proof: Clearly (iii) $\Rightarrow$ (i) and (i) $\Rightarrow$ (iv). Let (iv) be true. Let r be the smallest positive integer such that $(u_r, u_{r+1}) \neq 1$. Then $r \geqslant 2$ and there exists a prime p such that $p | u_r$, $p | u_{r+1}$. But $u_{r+1} = bu_r + du_{r-1}$, and hence $p | d$. Now, it is easy to prove, by induction, that $u_n \equiv b^{n-1} \pmod p$, for all $n \geqslant 1$. Hence, $0 \equiv u_r \equiv b^{r-1} \pmod p$ so that $p | b$, a contradiction, and (iv) $\Rightarrow$ (ii) is proved.

Now, let (ii) be true. We can assume that $i > j > 1$. Let $g = (u_i, u_j)$. Then from 2.2 we get $u_{(i,j)} | g$. It is well known that there exist integers r, s with, say, $r > 0$ and $s < 0$, such that $(i, j) = ri + sj$. Thus, by 2.1, we get

$$u_{ri} = u_{(-s)j + (i,j)} = u_{(-s)j} u_{(i,j)+1} + du_{(-s)j-1} u_{(i,j)}.$$

But by 2.2, $g | u_{(-s)j}$, $g | u_{ri}$, and by (ii), $(g, u_{(-s)j-1}) = 1$, so that $g | du_{(i,j)}$. If p is a prime, $p | g$, $p | d$, then $p | u_i = bu_{i-1} + du_{i-2}$, and so $p | b$. Thus, $(u_2, u_3) > 1$, a contradiction. Hence, $(g, d) = 1$ so that $g | u_{(i,j)}$ and (iii) is true.

3. THE SYSTEM OF SEQUENCES U_1

If $\mathbf{u} = \{u_n\} \in U_1$, then directly from the definition we obtain

$$u_3 = d + b^2 f, \quad u_4 = b(d + df + b^2 f^2)$$

and

$$u_5 = d^2 + 2b^2df + b^2df^2 + b^4f^3, \tag{3}$$

where b, d, $f \neq 0$, $f \neq 1$, and $(d, b) = (d, f) = 1$.

3.1 Proposition

Let $\mathbf{u} = \{u_n\} \in U_1$. Then the following statements are equivalent.

(i) $u_3 | u_6$

(ii) $u_3 \neq 0$ and $f \equiv 1 \pmod{|u_3|}$

Proof:

I: Let $u_3 | u_6$ and let $0 = u_3 = d + b^2 f$. Then $u_6 = bd(d + b^2 f^2) = 0$, and consequently, $f = 1$, a contradiction. Thus, from (i), it follows that $u_3 \neq 0$.

II: Let $u_3 \neq 0$. Since $u_6 \equiv bd(d + b^2 f^2) \pmod{|u_3|}$ and $(bd, u_3) = 1$, we have $u_3 | u_6$ iff $d + b^2 f^2 \equiv 0 \pmod{|u_3|}$. But $d + b^2 f^2 \equiv b^2 f(-1 + f) \pmod{|u_3|}$, and $(f, u_3) = (b, u_3) = 1$, so that $d + b^2 f^2 \equiv 0 \pmod{|u_3|}$ iff $f \equiv 1 \pmod{|u_3|}$.

3.2 Proposition

Let $\mathbf{u} = \{u_n\} \in U_1$. Then the following statements are equivalent.

(i) $u_4 | u_8$

(ii) $d + df + b^2 f^2 \neq 0$ and $f \equiv 1 \pmod{|d + df + b^2 f^2|}$

Proof:

I: Let $u_4 | u_8$ and $d + df + b^2 f^2 = 0$. Then

$$u_4 = 0 \quad \text{and} \quad u_8 = bdf(2d + b^2 f^2) u_3 = 0.$$

But both $2d + b^2 f^2 = 0$ and $u_3 = 0$ lead immediately to a contradiction; thus, from (i) it follows that $d + df + b^2 f^2 \neq 0$.

II: Let $d + df + b^2 f^2 \neq 0$. Clearly, $u_8 \equiv bdf(2d + b^2 f^2) u_3 \pmod{|u_4|}$ and $(df, d + df + b^2 f^2) = 1$, and, from 1.4, we get $(u_3, u_4) = 1$. Hence, $u_4 | u_8$ iff $2d + b^2 f^2 \equiv 0 \pmod{|d + df + b^2 f^2|}$. Trivially,

$$b^2 f^2 \equiv -d - df \pmod{|d + df + b^2 f^2|}$$

and thus,

$$2d + b^2 f^2 \equiv 0 \pmod{|d + df + b^2 f^2|} \text{ iff } f \equiv 1 \pmod{|d + df + b^2 f^2|}.$$

3.3 Lemma

Let $b, d, f \neq 0$, $f \neq 1$ be integers such that $(d, b) = (d, f) = 1$, $d + b^2 f \neq 0$, and $d + df + b^2 f^2 \neq 0$.

Then $f \equiv 1 \pmod{|d + b^2 f|}$ and $f \equiv 1 \pmod{|d + df + b^2 f^2|}$ if and only if one of the following cases occurs:

$b = \pm 1,\ f = -1,\ d = -1$	$b = \pm 1,\ f = -2,\ d = 1, 5$
$b = \pm 1,\ f = -3,\ d = 5$	$b = \pm 1,\ f = -5,\ d = 7$
$b = \pm 1,\ f + d = 1$	$f = \pm b^2,\ d = \mp 1 + b^2 \mp b^4$

Proof: Sufficiency is easy to verify in all of the cases, so we prove necessity. Let us denote $x = d + b^2f$, $y = d + df + b^2f^2$. Clearly, $(x, y) = 1$, $x \equiv y \pmod{|f|}$, and

$$y = x + fx - b^2f \tag{4}$$

$$xy \mid (f - 1). \tag{5}$$

α) Suppose $f > 1$.

Then $x \equiv y \pmod{f}$, and from (5) we get $|x|$, $|y| < f$.

α_1) If $x, y > 0$ or $x, y < 0$, then $x = y$, and hence $b^2 = d + b^2f^2$. So $b \mid d$ and we get $b = \pm1$, $f + d = 1$.

α_2) $x < 0$, $y > 0$ is impossible because of (4).

α_3) If $x > 0$, $y < 0$, then $y = x - f$, where $0 < x < f$.

From (4) we get $x = b^2 - 1$ and from (5) we get $x(f - x) \mid f - 1$. If $x \leqslant (f - 1)/2$, then $f - x > (f - 1)/2$, and hence $f - x = f - 1$. But then $x = 1 = b^2 - 1$, a contradiction. If $x > (f - 1)/2$, then $x = f - 1$. Thus, we get $f = b^2$, $d = -1 + b^2 - b^4$.

β) Suppose $f < 0$.

Denote $t = -f$. Then $x \equiv y \pmod{t}$, and from (5) we get $|x|$, $|y| \leqslant t + 1$.

β_1) If $|x| = t + 1$ or $|y| = t + 1$, then there are four possibilities:

β_{11}) $x = f - 1$, $y = \pm1 = f^2 - b^2f - 1$.

From $1 = f^2 - b^2f - 1$, we get $b = \pm1$, $f = -1$, $d = -1$, and $-1 = f^2 - b^2f - 1$ is impossible, since then we get $f = b^2 > 0$, a contradiction.

β_{12}) $x = -(f - 1)$, $y = \pm1 = -f^2 - b^2f + 1$.

From $1 = -f^2 - b^2f + 1$, we get $f = -b^2$, $d = 1 + b^2 + b^4$, and from $-1 = -f^2 - b^2f + 1$, we get $b = \pm1$, $f = -2$, $d = 5$.

β_{13}) $x = \pm1$, $y = f - 1 = \pm1 \pm f - b^2f$ both lead to a contradiction.

β_{14}) $x = \pm1$, $y = -(f - 1) = \pm1 \pm f - b^2f$.

From $-f + 1 = 1 + f - b^2f$, we get $b^2 = 2$, a contradiction, and from $-f + 1 = -1 - f - b^2f$, we get $b = \pm1$, $f = -2$, $d = 1$.

β_2) If $|x| = t$ or $|y| = t$ and $|x|$, $|y| \neq t + 1$, then $t \mid t + 1$, and hence $f = -1$. We get $b = \pm1$, $f = -1$, $d = 2$, which is a special case of $b = \pm1$, $f + d = 1$.

β_3) If $|x|$, $|y| < t$, then we have the following possibilities:

β_{31}) $x, y > 0$ or $x, y < 0$. Then $x = y$, and in the same way as in α_1), we get $b = \pm1$, $f + d = 1$.

β_{32}) $x < 0$, $y > 0$ is impossible because, then, $x = y + f$, and we get $y = b^2 - f - 1$, so that $x = b^2 - 1 \geqslant 0$, a contradiction.

β_{33}) $x > 0$, $y < 0$. Then $y = x - t = x + f$, and hence $x = b^2 + 1$. From (5), we get $x(t - x) \mid t + 1$, where $0 < x < t$ and $0 < t - x < t$.

If $x < (t + 1)/2$, then $t - x > (t - 1)/2$. From $t - x = t/2$, we get a contradiction, and hence $t - x = (t + 1)/2$, $x = (t - 1)/2$. Now, from $(t - 1)/2 \cdot (t + 1)/2 \mid t + 1$, we get $(t - 1)/2 \mid 2$, and consequently $b = \pm1$, $f = -5$, $d = 7$. If $x \geqslant (t + 1)/2$, then, similarly as above, we get $b = \pm1$, $f = -3$, $d = 5$.

3.4 Proposition

Let $\mathbf{u} = \{u_n\} \in U_1$. Then the following statements are equivalent.

(i) $u_5 | u_{10}$

(ii) $u_5 \neq 0$ and $d^2 + 3b^2df^2 + b^4f^4 \equiv 0 \pmod{|u_5|}$

Proof:

I: Let $u_5 | u_{10}$ and $0 = u_5 = d^2 + 2b^2df + b^2df^2 + b^4f^3$. Then $u_{10} = d(d^2 + 3b^2df^2 + b^4f^4)u_4 = 0$. If $u_4 = 0$, then $0 = d + df + b^2f^2 = d(1 + f) + b^2f^2$ and from (3) we get $u_5(1 + f)^2 = -b^4f^3 \neq 0$, a contradiction. Thus, we have $d^2 + 3b^2df^2 + b^4f^4 = 0$. But then $d^2 = -3b^2df^2 - b^4f^4$ and from $0 = u_5$ we get $b^2f^2 = -2d$, which is a contradiction, since $(d, b) = (d, f) = 1$.

II: Let $u_5 \neq 0$. Then

$$u_{10} \equiv d(d^2 + 3b^2df^2 + b^4f^4)u_4 \pmod{|u_5|}.$$

It is easy to prove that $(u_4, u_5) = 1$ and $(d, u_5) = 1$. Thus, $u_5 | u_{10}$ if and only if $d^2 + 3b^2df^2 + b^4f^4 \equiv 0 \pmod{|u_5|}$.

3.5 Proposition

Let $\mathbf{u} = \{u_n\} \in U_1$. Then the following statements are equivalent.

(i) $u_3 | u_6$, $u_4 | u_8$, $u_5 | u_{10}$

(ii) $\mathbf{u} \in D$

(iii) $\mathbf{u} \in \{\mathbf{a}, \mathbf{b}, \mathbf{e}, \mathbf{f}\}$

Proof: Clearly (iii) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (i). Let (i) be true. According to 3.1 and 3.2, just the cased described in 3.3 can occur for the integers b, d, f.

α) If $b = 1$, $f + d = 1$, then $\mathbf{u} = \mathbf{a}$;
If $b = -1$, $f + d = 1$, then $\mathbf{u} = \mathbf{b}$;
If $b = 1$, $f = -1$, $d = -1$, then $\mathbf{u} = \mathbf{e}$;
If $b = -1$, $f = -1$, $d = -1$, then $\mathbf{u} = \mathbf{f}$.

β) If $f = b^2$, $d = -1 + b^2 - b^4$, then

$$u_5 = -b^6 + b^4 - 2b^2 + 1$$

and

$$\begin{aligned} d^2 + 3b^2df^2 + b^4f^4 &= b^{12} - 3b^{10} + 4b^8 - 5b^6 + 3b^4 - 2b^2 + 1 \\ &= (-b^6 + b^4 - 2b^2 + 1)(-b^6 + 2b^4 + 1) + b^6. \end{aligned}$$

Obviously, $(-b^6 + b^4 - 2b^2 + 1, b^6) = 1$ for every integer b. So, from 3.4, we get $-b^6 + b^4 - 2b^2 + 1 = \pm 1$, and thus $1 = b^2 = f$, a contradiction.

γ) If $f = -b^2$, $d = 1 + b^2 + b^4$, then

$$u_5 = b^6 + b^4 + 2b^2 + 1$$

and

$$\begin{aligned} d^2 + 3b^2df^2 + b^4f^4 &= b^{12} + 3b^{10} + 4b^8 + 5b^6 + 3b^4 + 2b^2 + 1 \\ &= (b^6 + b^4 + 2b^2 + 1)(b^6 + 2b^4) + b^4 + 2b^2 + 1. \end{aligned}$$

But $b^6 + b^4 + 2b^2 + 1 > b^4 + 2b^2 + 1 > 0$ for every nonzero integer b, which contradicts 3.4.

γ) It is easy to prove by direct calculation that the remaining cases of Lemma 3.3 also contradict 3.4.

4. MAIN THEOREM

4.1 Theorem

It holds that $D = A \cup F_1 \cup G_1$.

Proof:

I: Let $\mathbf{u} \in D$. If c, $d \neq 0$ then, by 1.4, 3.5, and 1.1.4, $\mathbf{u} \in F_1$ or $\mathbf{u} \in A$; if $c = 0$, then $\mathbf{u} \in G$ and, by 1.2, $\mathbf{u} \in G_1$; if $d = 0$, then $\mathbf{u} \in H$ and, by 1.3 and 1.1.4, $\mathbf{u} \in F_1$ or $\mathbf{u} \in A$. Hence, $\mathbf{u} \in A \cup F_1 \cup G_1$.

II: Let $\mathbf{u} \in A \cup F_1 \cup G_1$. Then, by 1.1.1, 2.3, and 1.2, we get $\mathbf{u} \in D$.

4.2 Corollary

All the second-order, strong-divisibility sequences are precisely all integral multiples of sequences from D, i.e., of the following sequences:

$\mathbf{c} = \{1, -1, -1, -1, \ldots\}$

$\mathbf{d} = \{1, 1, -1, 1, -1, \ldots\}$

$\mathbf{e} = \{1, 1, -2, 1, 1, -2, \ldots\}$

$\mathbf{f} = \{1, -1, -2, -1, 1, 2, 1, -1, -2, -1, 1, 2, \ldots\}$

$u_1 = 1, \quad u_2 = b, \qquad u_{n+2} = b \cdot u_{n+1} + d \cdot u_n$ where $(d, b) = 1$

$u_1 = 1, \quad u_2 = b, \qquad u_{n+2} = d \cdot u_n$ where $d = \pm 1$.

4.3 Remark

It is easy to prove that the systems A, F_1, G_1 satisfy

$A \cap F_1 = \phi, \quad A \cap G_1 = \phi, \quad F_1 \cap G_1 = \{\mathbf{a}, \mathbf{b}, \mathbf{g}, \mathbf{h}\}$,

where $g = \{1, 0, 1, 0, \ldots\}$, and $h = \{1, 0, -1, 0, 1, 0, -1, 0, \ldots\}$.

REFERENCES

1. M. Bicknell. "A Primer on the Pell Sequence and Related Sequences." *The Fibonacci Quarterly* 13, no. 4 (1975):345-49.
2. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton-Mifflin, 1969; rpt. The Fibonacci Association, Santa Clara, California, 1980.
3. C. Kimberling. "Strong Divisibility Sequences and Some Conjectures." *The Fibonacci Quarterly* 17, no. 1 (1979):13-17.
4. N. N. Vorobyov. *Fibonacci Numbers*. Boston: D. C. Heath, 1963.

◆◇◆◇◆

ON THE DISTRIBUTION OF CONSECUTIVE TRIPLES OF QUADRATIC RESIDUES AND QUADRATIC NONRESIDUES AND RELATED TOPICS

M. G. MONZINGO
Southern Methodist University, Dallas TX 75275

(Submitted September 1983)

In [1], Andrews proves that the number of consecutive triples of quadratic residues, $n(p)$, is equal to $p/8 + Ep$, where $|Ep| < (1/4)\sqrt{p} + 2$. In addition in [1], it is proved* that for $p \equiv 3 \pmod 4$, $|Ep| < 2$.

In this note, $m(p)$ will denote the number of consecutive triples of quadratic nonresidues. In addition to topics related to those presented in [2], $n(p)$ and $m(p)$ will be determined for all odd primes. Also, the number of triples a, $a + 1$, $a + 2$ will be determined for which

$$\left(\frac{a}{p}\right) = \varepsilon, \quad \left(\frac{a+1}{p}\right) = \eta, \quad \text{and} \quad \left(\frac{a+2}{p}\right) = \nu,$$

where ε, η, and ν each take one of the values ± 1. Finally, an elementary proof of Gauss's "Last Entry" will be presented.

In [2], the decomposition of the integers $1, 2, 3, \ldots, p - 1$ into cells is developed as follows: these integers are partitioned into an array according to whether the consecutive integers are (or are not) quadratic residues. For example, for $p = 11$, the quadratic residues are $1, 3, 4, 5, 9$; hence, the array is

$$1 \qquad 2 \qquad 3, 4, 5 \qquad 6, 7, 8 \qquad 9 \qquad 10.$$

The following are also defined in [2]: a *singleton* is an integer in a singleton cell, e.g., 2; a *left* (*right*) *end point* is the first (last) integer in a nonsingleton cell, e.g., 3 (5); and an *interior point* is an integer, not an end point, in a nonsingleton cell, e.g., 4.

Furthermore, as in [2], the following notation will be used: s, e, and i will denote the numbers of singletons, left end points (or right end points), and interior points, respectively. Values for s, e, and i are given in [2], and these values will be cited later. Quadratic residue and quadratic nonresidue will be denoted by *qr* and *qnr*, respectively. The subscript r (n) will be used with s, e, and i to denote the appropriate number of quadratic residues (nonresidues). For example, for $p = 11$, $s_r = 2$ and $e_n = 1$.

Lemma 1

For p an odd prime, $n(p) = i_r$ and $m(p) = i_n$, so that $n(p) + m(p) = i$.

Proof: The middle integer, x, of either type of triple certainly cannot be a singleton or an end point; hence, x must be an interior point. Now, if $a_1, a_2, \ldots, a_k$ are the consecutive interior points of some cell, then there are precisely k consecutive triples: a, a_1, a_2; a_1, a_2, a_3; $\ldots$; a_{k-1}, a_k, b, where a and b are the left and right end points, respectively, of this cell.

---

*This case was solved by E. Jacobsthal, "Anwendungen einer Formel aus der Theorie der Quadratischen Reste," Dissertation (Berlin, 1906), pp. 26-32.

Hence, there is a one-to-one correspondence between the number of triples (of either type) and the number of interior points (of the same type), and the conclusion follows.

The next lemma is proven in [2].

Lemma 2

The results in the following table hold.

$(p = \;)$	$8k + 1$	$8k + 3$	$8k + 5$	$8k + 7$
s	$\frac{p-1}{4}$	$\frac{p+5}{4}$	$\frac{p+3}{4}$	$\frac{p+1}{4}$
e	$\frac{p+3}{4}$	$\frac{p-3}{4}$	$\frac{p-1}{4}$	$\frac{p+1}{4}$
i	$\frac{p-9}{4}$	$\frac{p-3}{4}$	$\frac{p-5}{4}$	$\frac{p-7}{4}$

Theorem 1

Let p be a prime $\equiv 3 \pmod 4$.

(a) If $p \equiv 3 \pmod 8$, then $i_r = i_n = n(p) = m(p) = \frac{p-3}{8}$;

(b) If $p \equiv 7 \pmod 8$, then $i_r = i_n = n(p) = m(p) = \frac{p-7}{8}$.

Proof: It is shown in [2] that the array of integers $1, 2, \ldots, p - 1$ is symmetric, in that a cell of qr corresponds to a cell of qnr of equal length. (This follows from the fact that a is a qr if and only if $p - a$ is a qnr.) So $i_r = i_n$ and, thus, from Lemma 1, $n(p) = m(p) = i/2$. The conclusion follows by applying Lemma 2.

The fact that for $p \equiv 3 \pmod 4$, both i_r and i_n are determined in Theorem 1 gives justification in also determining s_r, s_n, e_r, and e_n. Hence, this shall be done at this point. At the appropriate juncture, these entities will be determined for primes $\equiv 1 \pmod 4$.

Theorem 2

Let p be a prime $\equiv 3 \pmod 4$.

(a) If $p \equiv 3 \pmod 8$, then $s_r = s_n = \frac{p+5}{8}$ and $e_r = e_n = \frac{p-3}{8}$;

(b) If $p \equiv 7 \pmod 8$, then $s_r = s_n = \frac{p+1}{8}$ and $e_r = e_n = \frac{p+1}{8}$.

Proof: As in Theorem 1, use symmetry and apply Lemma 2.

Note: The case $p \equiv 1 \pmod 4$ does not follow so easily. The symmetry of the array used in Theorem 1 does not apply; a cell of qr corresponds to another cell of equal length of qr. (This follows from the fact that a is a qr if and only if $p - a$ is a qr.)

Next, as in [1], $S(1)$ will denote the following sum:

$$\sum_{n=1}^{p-3}\left(\frac{n(n+1)(n+2)}{p}\right).$$

Since Lemma 1 relates to the sum of i_r and i_n, in order to solve for i_r and i_n, it is sufficient to discover $i_r - i_n$. Hence, this shall be our goal.

The proof of the next lemma appears in [1]. [The definition and value of $S(\ell)$ will have no bearing on our results; the fact that $S(\ell)/2$, an integer, exists is sufficient.]

Lemma 3

For p a prime $\equiv 1 \pmod 4$,

$$\left(\frac{S(1)}{2}\right)^2 + \left(\frac{S(\ell)}{2}\right)^2 = p.$$

It is well known that p is uniquely expressed as the sum of squares of two integers (other than with a change in sign, or an interchange of the two integers). Furthermore, the two integers have opposite parity. Ultimately, we shall show that $S(1)$, whose value we seek, is such that $S(1)/2$ is ($\pm$) the odd integer which appears in the expression for p in Lemma 3.

The next lemma lists further results from [2] which will be used in determining the value of $S(1)$.

Lemma 4

For p a prime $\equiv 1 \pmod 4$, the following are identities:

(1) $e_n + s_n = \dfrac{p-1}{4}$ and $e_r + s_r = \dfrac{p+3}{4}$. (These follow from an examination of the number of qr and qnr cells in the array.)

(2) $i_r = s_r - 2$ and $i_n = s_n$. (These follow from an examination of the relationship between a qnr singleton and its multiplicative inverse.)

Next, a further investigation of $S(1)$.

Lemma 5

For p a prime $\equiv 1 \pmod 4$,

$$S(1) = \begin{cases} 4(s_r - s_n) - 2, & \text{if } p \equiv 1 \pmod 8, \\ 4(s_r - s_n) - 6, & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

Proof: First, an examination of $S(1)$ shows that a term in the summation will be positive when $n + 1$ is either a qr singleton, a qnr left or right end point, or a qr interior point. Similarly, the term will be negative when $n + 1$ is either a qnr singleton, a qr left or right end point, or a qnr interior point.

Now, define A and B as follows:

$$\begin{aligned} A &= s_r + 2e_n + i_r \\ &= s_r + 2\left(\frac{p-1}{4} - s_n\right) + (s_r - 2), \quad \text{using Lemma 4;} \end{aligned}$$

$$B = s_n + 2e_r + i_n$$
$$= s_n + 2\left(\frac{p+3}{4} - s_r\right) + s_n, \quad \text{using Lemma 4.}$$

Using the above determination as to when a term is positive or negative, $S(1)$ is almost equal to $A - B$. In the case $p \equiv 5 \pmod 8$, we must subtract 2 from A because 1 and $p - 1$ are singletons counted in s_r which do not appear in the sum (a result of the fact that 1 and $p - 1$ are qr and 2 and $p - 2$ are qnr). Similarly, in case $p \equiv 1 \pmod 8$, we must subtract 2 from B because 1 and $p - 1$ are quadratic residue left and right end points, respectively, which do not appear in the sum (a result of the fact that 1 and $p - 1$ are qr, and, in addition, 2 and $p - 2$ are qr). Finally, incorporating these changes with the appropriate ± 2 to $A - B = 4(s_r - s_n) - 4$, the conclusion follows.

Theorem 3

Let p be a prime $\equiv 1 \pmod 4$ and $p = a^2 + b^2$, where a is positive and odd; then,

$$i_r = n(p) = \begin{cases} \dfrac{p - 15 + 2(-1)^{\frac{a+1}{2}} a}{8}, & \text{if } p \equiv 1 \pmod 8, \\[2ex] \dfrac{p - 7 + 2(-1)^{\frac{a-1}{2}} a}{8}, & \text{if } p \equiv 5 \pmod 8, \end{cases}$$

$$i_n = m(p) = \begin{cases} \dfrac{p - 3 + 2(-1)^{\frac{a-1}{2}} a}{8}, & \text{if } p \equiv 1 \pmod 8, \\[2ex] \dfrac{p - 3 + 2(-1)^{\frac{a+1}{2}} a}{8}, & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

Proof: The case $p \equiv 1 \pmod 8$ will be examined; the case $p \equiv 5 \pmod 8$ follows similarly. As can be seen from Lemma 5, $S(1)/2$ is odd, and by using Lemma 3, the uniqueness of the odd integer in the sum of squares, and Lemma 5,

$$\frac{4(s_r - s_n) - 2}{2} = \pm a.$$

This, along with Lemma 4, implies that

$$i_r - i_n = \frac{\pm a - 3}{2}.$$

The symmetry of the array guarantees that both i_r and i_n are even; hence, $\pm a - 3$ must be divisible by 4. Since a is odd, $a \equiv 1 \pmod 4$ or $a \equiv 3 \pmod 4$. If $a \equiv 1 \pmod 4$, then we must have $-a - 3$; if $a \equiv 3 \pmod 4$, then we must have $a - 3$. The factor $(-1)^{(a+1)/2}$ yields the appropriate sign. Now, from the table in Lemma 2, $i_r + i_n = (p - 9)/4$. By solving the system of linear equations, we have the conclusion.

For example, let $p = 13$; then, since $13 = 3^2 + 2^2$, $a = 3$. Furthermore, $13 \equiv 5 \pmod{13}$; hence, from Theorem 3, $n(13) = i_r = 0$, and $m(13) = i_n = 2$. Specifically, the two qnr triples occur in the middle cell in the decomposition for $p = 13$,

1   2   3, 4   5, 6, 7, 8   9, 10   11   12.

Finally, having found i_r and i_n, we determine s_r, s_n, e_r, and e_n.

Theorem 4

Let p be a prime $\equiv 1 \pmod 4$ and $p = a^2 + b^2$, where a is odd and positive; then,

$$s_r = \begin{cases} \dfrac{p + 1 + 2(-1)^{\frac{a+1}{2}}a}{8}, & \text{if } p \equiv 1 \pmod 8, \\ \dfrac{p + 9 + 2(-1)^{\frac{a-1}{2}}a}{8}, & \text{if } p \equiv 5 \pmod 8, \end{cases}$$

$$s_n = \begin{cases} \dfrac{p - 3 + 2(-1)^{\frac{a-1}{2}}a}{8}, & \text{if } p \equiv 1 \pmod 8) \\ \dfrac{p - 3 + 2(-1)^{\frac{a+1}{2}}a}{8}, & \text{if } p \equiv 5 \pmod 8, \end{cases}$$

$$e_r = \begin{cases} \dfrac{p + 5 + 2(-1)^{\frac{a-1}{2}}a}{8}, & \text{if } p \equiv 1 \pmod 8 \\ \dfrac{p - 3 + 2(-1)^{\frac{a+1}{2}}a}{8}, & \text{if } p \equiv 5 \pmod 8 \end{cases}$$

$$e_n = \begin{cases} \dfrac{p + 1 + 2(-1)^{\frac{a+1}{2}}a}{8}, & \text{if } p \equiv 1 \pmod 8 \\ \dfrac{p + 1 + 2(-1)^{\frac{a-1}{2}}a}{8}, & \text{if } p \equiv 5 \pmod 8 \end{cases}$$

Proof: Use Lemma 4 and Theorem 3.

Theorem 5

Let each of ε, η, and ν take one of the values ± 1, and let T denote the number of triples, a, $a + 1$, $a + 2$, where $a = 1, 2, \ldots, p - 3$, for which

$$\left(\frac{a}{p}\right) = \varepsilon, \quad \left(\frac{a+1}{p}\right) = \eta, \quad \text{and} \quad \left(\frac{a+2}{p}\right) = \nu.$$

Then

$$\begin{aligned} T = \frac{1}{8}\Bigg[(p - 3) &- \varepsilon\left[\left(\frac{-1}{p}\right) + \left(\frac{-2}{p}\right)\right] - \eta\left[1 + \left(\frac{-1}{p}\right)\right] \\ &- \nu\left[1 + \left(\frac{2}{p}\right)\right] - \varepsilon\eta\left[1 + \left(\frac{2}{p}\right)\right] - \varepsilon\nu\left[1 + \left(\frac{-1}{p}\right)\right] \\ &- \eta\nu\left[1 + \left(\frac{2}{p}\right)\right] + \varepsilon\eta\nu S(1)\Bigg]. \end{aligned}$$

Proof: As done with pairs on page 71 of [3] (here, the sums being from 1 to $p - 3$),

$$T = \frac{1}{8}\sum\left[\left(1 + \varepsilon\left(\frac{a}{p}\right)\right)\left(1 + \eta\left(\frac{a+1}{p}\right)\right)\left(1 + \nu\left(\frac{a+2}{p}\right)\right)\right].$$

Next, expand T into eight sums and use the facts that

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0 \quad \text{and} \quad \sum_{a=1}^{p}\left(\frac{a+t}{p}\right)\left(\frac{a+s}{p}\right) = -1 \quad \text{for } (s, t) = 1;$$

then, apply Lemma 5 to substitute for $S(1)$.

We now turn our attention to "The Last Entry," see [4], which refers to the last entry in Gauss's mathematical diary. There, he states:

Theorem (Gauss)

Let p be a prime $\equiv 1 \pmod 4$; then, the number of solutions to

$x^2 + y^2 + x^2y^2 \equiv 1 \pmod p$ is $p + 1 - 2a$,

where $p = a^2 + b^2$, and a is odd.

Note: (1) the sign of a is to be chosen "appropriately," and
(2) there are four points at infinity included in the solution set.

Proof: If either x or y is $\equiv 0 \pmod p$, then the other is $\equiv \pm 1 \pmod p$. In the following, we shall assume that neither x nor y is $\equiv 0 \pmod p$. Now,

(x, y) is a solution $\iff$

$x^2 + y^2 + x^2y^2 \equiv 1 \pmod p \iff$

$(x^2 + 1)y^2 \equiv 1 - x^2 \pmod p \iff$

$x^2 + 1$ and $1 - x^2$ are both qr or qnr $\iff$

$x^2 + 1$ and $x^2 - 1$ are both qr or qnr [since $p \equiv 1 \pmod 4$] $\iff$

$x^2 - 1$, x^2, $x^2 + 1$ is such that x^2 is either a qr singleton or a qr interior point [with the exception that for $p \equiv 5 \pmod 8$ and $x \equiv \pm 1 \pmod p$; these values are qr singletons (± 2 are qnr) which have been taken into account]. Hence, the number of solutions is

$4(s_r + i_r) + 8$ for $p \equiv 1 \pmod 8$,

$4(s_r - 2 + i_r) + 8$ for $p \equiv 5 \pmod 8$,

where the "4 times" is for $(\pm x, \pm y)$, and the 8 is for the 4 points at infinity and the 4 solutions $(0, \pm 1)$, $(\pm 1, 0)$. Simplification yields the solution.

REFERENCES

1. G. E. Andrews. *Number Theory*. Philadelphia: W. B. Saunders, 1971.
2. M. G. Monzingo. "On the Distribution of Quadratic Residues." In *A Collection of Manuscripts Related to the Fibonacci Sequence—18th Anniversary Volume*. Ed. V. E. Hoggatt, Jr., & Marjorie Bicknell-Johnson. Santa Clara, CA: The Fibonacci Association, 1980, pp. 94-97.
3. I. M. Vinogradov. *An Introduction to the Theory of Numbers*. New York: The Pergamon Press, 1955.
4. K. Ireland & M. Rosen. *A Classical Introduction to Modern Number Theory*. New York: Springer-Verlag, 1982, p. 166.

◆◇◆◇◆

LATIN CUBES AND HYPERCUBES OF PRIME ORDER

CHARLES LAYWINE
Brock University, St. Catharines, Ontario L2S 3A1

GARY L. MULLEN
The Pennsylvania State University, University Park, PA 16802

(Submitted September 1983)

1. INTRODUCTION

In [3], the first author obtained an expression for the number of equivalence classes induced on the set of $n \times n$ Latin squares under row and column permutations. The first purpose of this paper is to point out that the results of [3] do not hold for all n, but rather that they hold only if n is a prime.* The second purpose of this paper is, in the case of prime n, to extend the results of [3] to three-dimensional and finally to n-dimensional Latin hypercubes. This is done in Sections 3 and 4.

2. LATIN SQUARES

A Latin square of order n is an $n \times n$ array with the property that each row and each column contains a permutation of the integers 1, 2, ..., n. In [3], two Latin squares were said to be equivalent if one could be obtained from the other by a permutation of the rows and another possibly different permutation of the columns, while a Latin square was said to be stationary if it remained invariant under some nontrivial row and column permutations. Let G be the group of all permutations of rows and columns so that G is isomorphic to $S_n \times S_n$ where S_n is the symmetric group on n letters. A Latin rectangle is an $m \times n$ array $(m \leqslant n)$ in which each row contains a permutation of 1, 2, ..., n and no integer occurs more than once in any column. Denote the number of $m \times n$ Latin rectangles by $L(m, n)$.

---

*We now correct two errors that occur in [3]. In the proof of Lemma 1.2 of [3] it is assumed that if d divides n then the expression $L(kd+1, n)/L(kd, n)$ is always an integer for $k = 0, 1, \ldots, n/d - 1$. That this is not always the case is easily seen in the case when $n = 4$. Let $d = 2$ and $k = 1$, and consider $L(3, 4)/L(2, 4)$. It is easily checked (see, e.g., [2]) that $L(3, 4) = 4!3!4$, while $L(2, 4) = 4!9$, so that $L(3, 4)/L(2, 4) = 8/3$. Lemma 1.2 of [3] is corrected in our Lemma 1.2.

In Theorem 2 of [3], it is indicated that, if n is prime, then there are $(n - 2)!$ classes of stationary Latin squares each of which contains $(n - 1)! \times (n - 2)!$ elements. While the proof of the theorem is correct, the statement contains a typographical error and should read "For n prime, there are $(n - 2)!$ equivalence classes of stationary Latin squares, each of which contains $n! \times (n - 1)!$ elements."

It is now easy to prove

Lemma 1.2

Let $\Pi = (\Pi_r, \Pi_c)$ be a permutation of G such that both Π_r and Π_c consist of either p 1-cycles or 1 p-cycle, where p is a prime. Then there are either $L(p, p)$ or $L(1, p)$ Latin squares invariant under Π.

Proof: Clearly, if Π_r and Π_c both consist of p 1-cycles, then all Latin squares of order p are invariant while in the remaining case the first row can be chosen in $p! = L(1, p)$ ways. Once the first row is completed, the remaining rows are uniquely determined by Π_c.

We now prove

Theorem 1

If p is a prime, then permutations of rows and columns induce

$$\frac{L(p, p)}{(p!)^2} + \frac{(p - 1)!}{p}$$

equivalence classes in the p^{th}-order Latin squares.

Proof: Burnside's lemma gives the number of classes as

$$(1/|G|) \sum_{\Pi \in G} \psi(\Pi)$$

where $\psi(\Pi)$ is the number of squares invariant under Π, from which the theorem follows.

It may be noted that, if ℓ_p denotes the number of reduced Latin squares of order p, then $L(p, p) = p!(p - 1)!\ell_p$ so that the number of equivalence classes thus reduces to $(\ell_p + (p - 1)!)/p$. Moreover, the values of ℓ_p are known if $p \leqslant 9$ (see [1]).

3. LATIN CUBES

In this section we extend the results of [3] to Latin cubes of prime order. A Latin cube C of order p is a $p \times p \times p$ array with the property that each of the p^3 elements c_{ijk} is one of the numbers 1, 2, ..., p and $\{c_{ijk}\}$ ranges over all of the numbers 1, 2, ..., p as one index varies from 1 to p while the other two indices remained fixed. Two Latin cubes of order p are equivalent if one can be obtained from the other by a permutation $\Pi = (\Pi_r, \Pi_c, \Pi_\ell)$, where Π_r is a permutation of the rows, Π_c is a permutation of the columns, and Π_ℓ is a permutation of the levels of C. Let G denote the group of all permutations so that G is isomorphic to S_p^3. We first prove

Lemma 3.1

Given three partitions of a prime p, each into at most $p - 1$ parts and not all into a single part, it is possible to select one part, say s_i, from each partition so that the least common multiple of two of the s_i's is less than $\operatorname{lcm}(s_1, s_2, s_3)$.

Proof: Number the partitions so that the first has more than one part and select as s_1 some part other than 1 from the first partition. Since p is prime, from the second partition we may select as s_2 some part such that $(s_2, s_1) = 1$. Similarly, select s_3 from the third partition so that $(s_3, s_1) = 1$ and, hence, $\operatorname{lcm}(s_2, s_3) < \operatorname{lcm}(s_1, s_2, s_3)$.

Corresponding to Lemma 1 of [3], we have

Lemma 3.2

Let $\Pi = (\Pi_r, \Pi_c, \Pi_\ell) \in G$. A Latin cube of order p a prime is nontrivially invariant under Π only if each component of Π is either a p-cycle or the identity and at least two of the components are p-cycles.

Proof: The permutation Π induces three partitions of p and if s_i is a part from the i^{th} partition for $i = 1, 2, 3$, we may assume that

$$\operatorname{lcm}(s_1, s_2) < \operatorname{lcm}(s_1, s_2, s_3).$$

If $\pi = (\Pi_1, \Pi_2, \Pi_3)$, let $(\ell_{i1}\ell_{i2}\ldots\ell_{is_i})$ be the corresponding cycle of the permutation Π_i. Tracing the effect of the cycles beginning with position $(\ell_{11}, \ell_{21}, \ell_{31})$ we get, after applying the permutation Π $d = \operatorname{lcm}(s_1, s_2)$ times that

$$(\ell_{11}, \ell_{21}, \ell_{31}) \to (\ell_{12}, \ell_{22}, \ell_{32}) \to \cdots \to (\ell_{11}, \ell_{21}, \ell_{3d}),$$

where $\ell_{3d} \neq \ell_{31}$ since $\operatorname{lcm}(s_1, s_2, s_3) > \operatorname{lcm}(s_1, s_2)$. For invariance, the elements in these positions must be equal, a contradiction of the Latin property. Hence all of the s_i must be 1 or p. If only one component contained a p cycle while the other two contained the identity, clearly the cube cannot be invariant without contradicting the Latin property.

Let $L(p, p, p)$ denote the number of Latin cubes of order p a prime. Clearly, if Π is the identity, then $L(p, p, p)$ cubes are invariant under Π, while there are $3[(p-1)!]^2$ permutations $\Pi = (\Pi_r, \Pi_c, \Pi_\ell)$ with the property that one of the components is the identity, while the other two consist of p-cycles. Moreover, each such permutation leaves $L(1, p, p) = L(p, p)$ cubes invariant. In order to count the number of cubes invariant under Π, where Π_r, Π_c, and Π_ℓ all consist of p-cycles, we need the following definitions and lemmas.

Definition 3.1

A *transversal* of a Latin square of order p is a set of p cells, one in each row and one in each column such that no two of the cells contain the same symbol.

Definition 3.2

A Latin square of order p is in *diagonal transversal* form if it consists of p disjoint transversals, one of which is the main diagonal and the remaining transversals are parallel to it, i.e., with addition mod p, cells (i, j) and $(i + 1, j + 1)$ are always in the same transversal.

Let d_p denote the number of Latin squares of order p in diagonal transversal form. We can now prove

Lemma 3.3

A Latin cube of order p a prime is invariant under a permutation $\Pi = (\Pi_r, \Pi_c, \Pi_\ell)$ where Π_r, Π_c, and Π_ℓ are p-cycles only if level one consists of p disjoint transversals.

Proof: Let $\Pi_r = (r_1 r_2 \dots r_p)$ and $\Pi_c = (c_1 c_2 \dots c_p)$. Consider the elements in the p positions $(r_1, c_1, \cdot)$ to be some permutations of 1, 2, ..., p. Repeated applications of Π carries these positions into the positions $(r_2, c_2, \cdot)$, $(r_3, c_3, \cdot)$, ... Since Π_ℓ is a p-cycle, each element occupies the position in level one in exactly one of the p sets of positions, and thus the elements in positions $(r_1, c_1, 1)$, $(r_2, c_2, 1)$, ..., $(r_p, c_p, 1)$ form a transversal. Similarly, successive applications of Π to the p positions $(r_2, c_1, \cdot)$ fixes $(r_3, c_2, \cdot)$, ..., $(r_1, c_p, \cdot)$ so that $(r_2, c_1, 1)$, ..., $(r_1, c_p, 1)$ is a second transversal in the first level. It thus follows that level one consists of p disjoint transversals.

Lemma 3.4

For p a prime there are d_p Latin cubes of order p invariant under a permutation $\Pi = (\Pi_r, \Pi_c, \Pi_\ell)$ where Π_r, Π_c, and Π_ℓ are p-cycles.

Proof: Suppose $\Pi_r = (1 i_2 \dots i_p)$, $\Pi_c = (1 j_2 \dots j_p)$, and $\Pi_\ell = (1 k_2 \dots k_p)$. By the previous lemma, a cube will be invariant under Π only if level one consists of the disjoint transversals

$$\begin{array}{ll} T_1 & (1, 1), (i_2, j_2), \dots, (i_p, j_p), \\ T_2 & (1, j_2), (i_2, j_3), \dots, (i_p, 1), \\ \vdots & \qquad\qquad\vdots \\ T_p & (1, j_p), (i_2, 1), \dots, (i_p, j_{p-1}). \end{array} \tag{3.1}$$

Rearrange the rows and columns by using the permutations

$$\begin{pmatrix} 1 & i_2 & \dots & i_p \\ 1 & 2 & \dots & p \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & j_2 & \dots & j_p \\ 1 & 2 & \dots & p \end{pmatrix}$$

so that level one now consists of the transversals

$$\begin{array}{ll} T_1 & (1, 1), (2, 2), \dots, (p, p), \\ T_2 & (1, 2), (2, 3), \dots, (p, 1), \\ \vdots & \qquad\qquad\vdots \\ T_p & (1, p), (2, 1), \dots, (p, p-1). \end{array}$$

Hence, level one is in diagonal transversal form so that the number of cubes invariant under Π is less than or equal to d_p.

Similarly, if we consider a Latin square of order p in diagonal transversal form and apply the permutations

$$\begin{pmatrix} 1 & 2 & \dots & p \\ 1 & i_2 & \dots & i_p \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 2 & \dots & p \\ 1 & j_2 & \dots & j_p \end{pmatrix}$$

we obtain a square with p disjoint transversals as in (3.1). If we use this square as level one of a cube and allow $\Pi = (\Pi_r, \Pi_c, \Pi_\ell)$ to fix the remaining levels we will have constructed a cube invariant under Π so that d_p is no larger than the number of cubes invariant under Π.

It may be of interest to note that for $p = 2, 3$, and 5, $d_p = (p - 2)p!$. For p prime, one can construct a square in diagonal transversal form by choosing the first row in one of $p!$ ways and then rotating the row one position to the left $p - 1$ times to obtain the remaining rows. By making the $p - 1$ rotations each two positions to the left, one obtains a second diagonal transversal square with a given first row. Similarly, for left rotations of any fixed size up to and including $p - 2$ positions, a new diagonal transversal square is obtained so that $d_p \geqslant (p - 2)p!$. If $p = 7$, the following square

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 7 & 5 & 6 & 1 & 4 \\ 7 & 5 & 4 & 6 & 1 & 2 & 3 \\ 4 & 1 & 6 & 2 & 3 & 7 & 5 \\ 3 & 6 & 5 & 1 & 7 & 4 & 2 \\ 6 & 7 & 2 & 3 & 4 & 5 & 1 \\ 5 & 4 & 1 & 7 & 2 & 3 & 6 \end{matrix}$$

is not obtained by a rotation of the first row so that $d_7 > 5 \cdot 7!$. Moreover, in general, if $p \geqslant 7$, we have $d_p > (p - 2)p!$. It would be of interest to have an exact formula for d_p for all p.

We now apply Burnside's lemma to prove

Theorem 3.1

Permutations of rows, columns, and levels induce

$$N_p = \frac{1}{(p!)^3}[L(p, p, p) + 3((p - 1)!)^2 L(p, p) + ((p - 1)!)^3 d_p]$$

equivalence classes in the set of Latin cubes of order p a prime.

If c_p is the number of reduced Latin cubes of order p, then

$$L(p, p, p) = p!(p - 1)!(p - 1)!c_p,$$

so that N_p may be written in the form

$$N_p = \frac{1}{p^3}[pc_p + 3p!\ell_p + d_p].$$

In [4] it was shown that $c_2 = c_3 = 1$ and $c_5 = 40,246$. Therefore, it is easily checked that $N_2 = N_3 = 1$, while $N_5 = 1774$.

4. HYPERCUBES

In this section we extend our results concerning squares and cubes of prime order to n-dimensional hypercubes of prime order. A Latin hypercube A of dimension n and order p is a $p \times p \times \cdots \times p$ array with the property that each of the p^n elements $a_{i_1 \ldots i_n}$ is one of the numbers $1, 2, \ldots, p$ and $\{a_{i_1 \ldots i_n}\}$ ranges over all of the numbers $1, 2, \ldots, p$ as one index varies from 1 to p, while the remaining indices are fixed. Let $L(n; p)$ be the number of n-dimensional Latin hypercubes of order p. We may generalize the proof of Lemma 3.1 to obtain

Lemma 4.1

Given n partitions of a prime p, each into at most $p - 1$ parts and not all into a single part, it is possible to select one part s_i from each partition so that the least common multiple of $n - 1$ of the s_i's is less than $\operatorname{lcm}(s_1, s_2, \ldots, s_n)$.

Let G be the group that permutes n-dimensional hypercubes by permuting each component so that G is isomorphic to S_p^n. Along the same lines as Lemma 3.2, we may prove

Lemma 4.2

Let $\Pi = (\Pi_1, \ldots, \Pi_n) \in G$. A Latin hypercube of order p a prime is nontrivially invariant under Π only if each Π_i is a p-cycle or the identity and at least two of the Π_i are p-cycles.

Definition 4.1

A *hypertransversal* of an n-dimensional Latin hypercube of order p is a collection of p cells $(i_1^k, \ldots, i_n^k)$, $k = 1, \ldots, p$, such that the corresponding p elements are distinct and among the p n-tuples, the set of p elements in each of the n coordinates is a permutation of $1, 2, \ldots, p$.

By extending the argument used in the proof of Lemma 3.3 to n dimensions, we may prove

Lemma 4.3

An n-dimensional Latin hypercube of order p a prime is invariant under a permutation $\Pi = (\Pi_1, \ldots, \Pi_n)$, where $\Pi_1, \ldots, \Pi_n$ are all p-cycles only if the hypercube possesses a subhypercube of dimension $n - 1$ that is composed of p^{n-2} disjoint hypertransversals.

Definition 4.2

An n-dimensional Latin hypercube of order p is in *parallel hypertransversal* form if it consists of p^{n-1} disjoint hypertransversals

$$(1, i_2, \ldots, i_n),\ (2, i_2 + 1, \ldots, i_n + 1), \ldots, (p, i_2 + p - 1, \ldots, i_n + p - 1),$$

where $(i_2, \ldots, i_n)$ ranges over all p^{n-1} $(n - 1)$-tuples and the additions are mod p.

Let $d(n; p)$ denote the number of n-dimensional Latin hypercubes in parallel hypertransversal form. Analogous to Lemma 3.4, we can prove

Lemma 4.4

For p a prime there are $d(n - 1; p)$ Latin n-dimensional hypercubes of order p invariant under a permutation $\Pi = (\Pi_1, \ldots, \Pi_n)$, where each Π_i is a p-cycle.

Theorem 4.1

Permutations of each coordinate induce

$$N_p = \frac{1}{(p!)^n}\left[L(n;\ p) + \sum_{k=2}^{n-1}\binom{n}{k}((p-1)!)^k L(k;\ p) + ((p-1)!)^n d(n-1;\ p)\right]$$

equivalence classes in the set of n-dimensional Latin hypercubes of order p a prime.

Proof: Clearly, $L(n;\ p)$ hypercubes are invariant under the identity and there are

$$\binom{n}{k}((p-1)!)^k$$

permutations $\Pi = (\Pi_1, \ldots, \Pi_n)$, where $n - k$ of the Π_i are the identity. Moreover, each of these fixes $L(k;\ p)$ k-dimensional hypercubes of order p. Applying Lemma 4.4 and Burnside's lemma yields the result.

REFERENCES

1. J. Dénes & A. D. Keedwell. *Latin Squares and Their Applications.* New York: Academic Press, 1974.
2. J. R. Hamilton & G. L. Mullen. "How Many $i - j$ Reduced Latin Rectangles Are There?" *Amer. Math. Monthly* 87 (1980);392-94.
3. C. Laywine. "An Expression for the Number of Equivalence Classes of Latin Squares Under Row and Column Permutations." *J. Comb. Thy.*, Series A, 30 (1981):317-20.
4. G. L. Mullen & R. E. Weber. "Latin Cubes of Order $\leqslant 5$." *Discrete Math.* 32 (1980):291-97.

◆◇◆◇◆

A COROLLARY TO ITERATED EXPONENTIATION

R. M. STERNHEIMER
Brookhaven National Laboratory, Upton, NY 11973

(Submitted October 1983)

In connection with three previous papers on the convergence of iterated exponentiation by Creutz and Sternheimer [1], [2], [3], and with some earlier work [4], [5], it occurred to me that the problem of the proof of Fermat's Last Theorem might be intimately connected with the properties of the function $F(x, y) \equiv x^y - y^x$, and in particular with the condition that

$$F(x, y) = 0, \tag{1}$$

when x and y are restricted to be positive integers [6]. It can be shown that aside from the trivial solution $x = y$, (1) is satisfied only for $x = 2$, $y = 4$, in which case

$$F(x, y) = 2^4 - 4^2 = 0. \tag{2}$$

In order to prove this property of $F(x, y)$, we consider Figure 1 of [1]. This figure gives the function $f(x)$ defined by the condition

$$x^f = f. \tag{3}$$

In Figure 1 of [1], we consider the continuation of the dashed part of the curve to the right of $f(x) = e$ up to the region of $f(x) = 4$. It is easily seen that the corresponding x is $\sqrt{2}$, since $(\sqrt{2})^4 = 2^2 = 4$ satisfies (3).

We also have $f(x) = 2$ for $x = \sqrt{2}$, as shown by the left-hand part of Figure 1. If we denote the two values of $f(\sqrt{2})$ by f_1 and f_2, we have

$$x^{f_1} = f \ , \ x^{f_2} = f \ , \tag{4}$$

where $x = \sqrt{2}$. We can rewrite (4) as follows:

$$f_1^{1/f_1} = f_2^{1/f_2} = x = \sqrt{2}. \tag{5}$$

From (5), we obtain (by raising to the power $f_1 f_2$):

$$f_1^{f_2} = f_2^{f_1}, \tag{6}$$

i.e., $2^4 = 4^2$.

Thus the two values of $f(x)$ for a given x, namely f_1 and f_2, are the solutions of the equation $f_1^{f_2} = f_2^{f_1}$ (6). We can now set $f_1 = x$, $f_2 = y$ in the notation of (1) (where x is not to be confused with the auxiliary x of Figure 1 of [1]). Now, from Figure 1, it is obvious that one of the f's, say f_1, must be less than e, while the other f, say f_2, must be larger than e. It is also clear that, since the only integer smaller than e and larger than 1 is 2, the equation $f_1^{f_2} = f_2^{f_1}$ can be satisfied only for $f_1 = 2$, $f_2 = 4$, if f_1 and f_2 are restricted to be integers.

This manuscript was authored under Contract No. DE-AC02-76CH00016 with the U.S. Department of Energy.

Incidentally, Figure 2 of [1] shows that, when the ordinate x is less than 1, there is no second branch of the curve of x vs. f, and therefore, for $f_1 < 1$, there is no f_2 such that $f_1^{1/f_1} = f_2^{1/f_2}$.

The fact that $x = 2$, $y = 4$ is the only integer solution of $F(x, y) = 0$ can also be seen by inspection, i.e., by calculating

$$F(2, 3) = -1, \quad F(2, 4) = 0, \quad F(2, 5) = 7, \quad F(2, 6) = 28, \quad F(3, 4) = 17,$$

etc. Also, for arbitrary x and y such that the difference $y - x \equiv \Delta x$ is small, it can be shown by differentiation of x^y with respect to both x and y that

$$F(x, y) = \bar{x}^{\bar{x}}(\ell n\bar{x} - 1)(y - x), \tag{7}$$

where $\bar{x} \equiv (x + y)/2$. In order to prove (7), we note that

$$F(x, y) = x^{x+\Delta x} - (x + \Delta x)^x. \tag{8}$$

Now, if Δx is small, we can expand both terms in the right-hand side of (8) as follows, to first order in Δx:

$$x^{x+\Delta x} = x^x + x^x \ln x\Delta x, \tag{9}$$

where we have used $\partial x^y/\partial y = x^y \ln x$. Moreover,

$$(x + \Delta x)^x = x^x + x^x\Delta x, \tag{10}$$

where we have used

$$\partial x^y/\partial x = yx^{y-1} = \frac{y}{x}x^y \approx x^y. \tag{11}$$

Upon subtracting (10) from (9), one finds:

$$F(x, y) = x^x(\ln x - 1)\Delta x = x^x(\ln x - 1)(y - x). \tag{12}$$

Because of the rapid increase of x^x with increasing x, one will obtain a more accurate result by evaluating the derivatives $\partial x^y/\partial y$ and $\partial x^y/\partial x$ at the midpoint of the interval (x, y), i.e., at the point $\bar{x} = (x + y)/2$. Upon making this substitution in (12), one obtains (7).

Equation (7) shows that for $y - x$ small, x^y is *larger* than y^x for positive Δx if $\bar{x} > e$ and is *smaller* than y^x for positive Δx if $\bar{x} < e$. As an example, $1.6^{1.7} = 2.2233$ is smaller than $1.7^{1.6} = 2.3373$ because $1.6, 1.7 < e$. The difference $F(1.6, 1.7) = -0.1140$ is very well reproduced by (7), which gives, with $\bar{x} = 1.65$:

$$F(1.6, 1.7) = 1.65^{1.65}(\ln 1.65 - 1)(0.1) = -0.1140. \tag{13}$$

As a second example, $2.9^{3.0} = 24.389$ is larger than $3.0^{2.9} = 24.191$ because $2.9, 3.0 > e$. We find $F(2.9, 3.0) = 24.389 - 24.191 = +0.198$, and this difference is very well reproduced by (7), which gives, with $\bar{x} = 2.95$:

$$F(2.9, 3.0) = 2.95^{2.95}(\ln 2.95 - 1)(0.1) = +0.199. \tag{14}$$

Equation (7) again points out the crucial role of the constant e for the sign of $F(x, y)$, since $\ln \bar{x} - 1 = \ln(\bar{x}/e)$. The same equation also shows that for x and y close to e and $x < e$, $y > e$, we must have

$$\bar{x} = (1/2)(x + y) = e \quad \text{for } F(x, y) = 0.$$

Obviously, (7) does not hold when the difference $y - x$ is large, and the previous result $x = 2$, $y = 4$ with $x < e$, $y > e$ can be regarded as an extreme example of (7) when higher derivatives of x^y, i.e., terms in $(\Delta x)^2$, $(\Delta x)^3$, etc., are included.

It is of interest to speculate that $x^n + y^n = z^n$ is solvable only for $n = 1$ and $n = 2$ (with x, y, z = positive integers) because $n = 1$ and $n = 2$ are the only positive integers smaller than e. Here I wish to mention that the Fermat equation $x^n + y^n = z^n$ has solutions both for $n = 1$ and $n = 2$. The case $n = 2$ has been discussed frequently; however, the case $n = 1$ also merits some attention. Thus, if we assume (by definition) that $x \geqslant y$, then $x + y = z$ has $z/2$ distinct solutions when z = even, and it has $(z - 1)/2$ distinct solutions when z = odd. As an example for $z = 11$, we have five distinct solutions:

$$x + y = 6 + 5,\ 7 + 4,\ 8 + 3,\ 9 + 2, \text{ and } 10 + 1.$$

In this connection, I wish to point out that in complete analogy to the exponent n which appears in the Fermat equation, the equation $F(x, y) = 0$, in addition to $F(2, 4) = 0$, also has a valid solution for $x = 1$, namely $F(1, y) = 0$ in the limit in which y approaches infinity. This additional solution will be discussed in detail in a forthcoming paper.

ACKNOWLEDGMENT

This work was supported by the Department of Energy under Contract No. DE-AC02-76CH00016.

REFERENCES

1. M. Creutz & R. M. Sternheimer. "On the Convergence of Iterated Exponentiation—I." *The Fibonacci Quarterly* 18, no. 4 (1980):341-47.
2. M. Creutz & R. M. Sternheimer. "On the Convergence of Iterated Exponentiation—II." *The Fibonacci Quarterly* 19, no. 4 (1981):326-35.
3. M. Creutz & R. M. Sternheimer. "On the Convergence of Iterated Exponentiation—III." *The Fibonacci Quarterly* 20, no. 1 (1982):7-12.
4. R. M. Sternheimer. "On a Set of Non-Associative Functions of a Single Positive Real Variable." Brookhaven Informal Report PD-128; BNL-23081 (June 1977).
5. M. Creutz & R. M. Sternheimer. "On a Class of Non-Associative Functions of a Single Positive Real Variable." Brookhaven Informal Report PD-130; BNL-23308 (September 1977).
6. I have also considered the properties of the function $G(x, y) \equiv x^y + y^x$. It is of interest that $G(2, 6) = 100$.

◆◇◆◇◆

ELEMENTAL COMPLETE COMPOSITE NUMBER GENERATORS

BLAKE RALSTON
2000 Durant Avenue, Berkeley, CA 94704

(Submitted November 1983)

Theorem

There exist arithmetic functions in closed form that are generators of all composite numbers.

Proof: It suffices to produce an example of such a function. Here, the existence of several such functions will be shown. First, consider the following two sequences:

$$2,\ \ 3, 3,\ \ 4, 4, 4,\ \ 5, 5, 5, 5,\ \ 6, 6, 6, 6, 6, \ldots \ (s_1)$$
$$2,\ \ 2, 3,\ \ 2, 3, 4,\ \ 2, 3, 4, 5,\ \ 2, 3, 4, 5, 6, \ldots \ (s_2).$$

(These sequences can be defined by specific recursions, but this will not be done here because the patterns of progression are clear.) It is easy to see that the products of corresponding terms in the sequences s_1 and s_2 constitute all the composite numbers and no prime numbers.

Second, consider the following sequence, H, which progresses

$$1,\ \ 2, 2,\ \ 3, 3, 3,\ \ 4, 4, 4, 4,\ \ 5, 5, 5, 5, 5, \ldots \ (H),$$

whose terms are those of s_1 less one. The n^{th} term of the sequence H is given by

$H(n)$ = the least integer greater than or equal to $\frac{1}{2}(\sqrt{8n+1} - 1)$.

This follows from solving for m in terms of n in the inequality

$$1 + 2 + \cdots + (m - 1) < n \leqslant 1 + 2 + \cdots + m,$$

where each pair of positive integer variables m and n satisfies $H(n) = m$. Now writing

$$H(n) = \left\lceil \frac{1}{2}(\sqrt{8n+1} - 1) \right\rceil, \text{ where } \lceil x \rceil \text{ is ceiling } x,$$

it follows with little difficulty that

$$s_1(n) = H(n) + 1$$
$$s_2(n) = (n + 1) - \frac{1}{2}(H(n) - 1)H(n).$$

To show the second part, one can compare the sequences

$$1,\ \ 2, 3,\ \ 4, 5, 6,\ \ 7, 8, 9, 10,\ \ 11, 12, 13, 14, 15, \ldots \ (N)$$
$$1,\ \ 1, 2,\ \ 1, 2, 3,\ \ 1, 2, 3, 4,\ \ 1, 2, 3, 4, 5, \ldots \ (I).$$

Observe that in the sequence of differences of corresponding terms

$$0,\ \ 1, 1,\ \ 3, 3, 3,\ \ 6, 6, 6, 6,\ \ 10, 10, 10, 10, 10, \ldots \ (n - I(n)),$$

the $(n+1)^{\text{th}}$ block of terms consists of the term $1 + 2 + \cdots + n$, the n^{th} triangular number, repeated a total of $n+1$ times. This implies

$$n - I(n) = \frac{1}{2}(H(n) - 1) \cdot ((H(n) - 1) + 1)$$

or

$$I(n) = n - \frac{1}{2}(H(n) - 1)H(n).$$

Multiplying together the two formulas for $s_1(n)$ and $s_2(n)$, some cancellation of product terms occurs:

$$\begin{aligned} s_1(n) \cdot s_2(n) &= (H(n) + 1) \cdot \left(n + 1 - \frac{1}{2}(H(n) - 1)H(n)\right) \\ &= (H(n) + 1)(n + 1) - \frac{1}{2}(H(n) - 1)H(n)(H(n) + 1) \\ &= nH(n) + n + H(n) + 1 - \frac{1}{2}(H^3(n) - H(n)). \end{aligned}$$

This gives a complete composite number generator

$$\mathsf{C}(n) = s_1(n) \cdot s_2(n) = (n + 1) + \left(n + \frac{3}{2}\right)H(n) - \frac{1}{2}H^3(n).$$

For comparison, a similar function which generates the positive integers—not in their natural order and with repetitions—is

$$\mathsf{N}(n) = H(n) \cdot I(n) = nH(n) + \frac{1}{2}H^2(n) - \frac{1}{2}H^3(n).$$

Alternative arithmetic generators of all the composite numbers can be found by considering sequences such as

$$2,\ 3,\ 2,\ 4,\ 3,\ 2,\ 5,\ 4,\ 3,\ 2,\ 6,\ 5,\ 4,\ 3,\ 2,\ \ldots\ (s_3)$$

[here, $s_2(n) + s_3(n) = s_1(n) + 2$]

and substituting $s_3(n)$ in place of either one of $s_2(n)$ or $s_1(n)$ in the product $s_1(n)s_2(n)$. Following from its relation with $s_2(n)$, an arithmetic functional form for $s_3(n)$ is found to be

$$s_3(n) = (-n + 2) + \frac{1}{2}H(n)(H(n) + 1).$$

Other complete composite number generators in closed arithmetic form are then given by

$$\overline{C}(n) = s_1(n) \cdot s_3(n) = (-n + 2) + \left(-n + \frac{5}{2}\right)H(n) + H^2(n) + \frac{1}{2}H^3(n)$$

$$\overline{\mathsf{C}}(n) = s_2(n) \cdot s_3(n) = (-n^2 + n + 2) + \frac{3}{2}H(n) + \left(n - \frac{1}{4}\right)H^2(n) - \frac{1}{4}H^4(n).$$

◆◇◆◇◆

A NOTE ON A FIBONACCI IDENTITY

NICHOLAS J. ROSE
North Carolina State University, Raleigh, NC 27650

(Submitted November 1983)

The Fibonacci numbers are defined by

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n, \quad n \geqslant 2. \tag{1}$$

The following well-known identity relates F_n to the binomial coefficients:

$$F_n = \sum_{k=0}^{\left[\frac{n-1}{2}\right]} \binom{n-k-1}{k}. \tag{2}$$

In this note we give an interpretation of the individual terms in the identity (2) in terms of the original "rabbit problem":

> *Given a new born pair of rabbits on the first day of a month, find the number of pairs of rabbits at the end of* n *months, assuming that each pair begets a pair each month starting when they are two months old.*

F_n is the number of pairs of rabbits at the end of n months. Now let

$S(n, k)$ = the number of pairs of k^{th} generation rabbits at the end of the n^{th} month.

Here the initial pair of rabbits is called the *zeroeth generation*, the immediate offspring of the initial pair are called *first generation* rabbits, the immediate offspring of the first-generation rabbits are called *second generation* rabbits, and so on.

We can now state our

Theorem

$$S(n, k) = \binom{n-k-1}{k}, \quad 0 \leqslant k \leqslant \left[\frac{n-1}{2}\right].$$

Proof: We have the simple accounting equation:

$$S(n, k) = S(n-1, k) + S(n-2, k-1). \tag{4}$$

This merely states that the number of k^{th} generation pairs at the end of the n^{th} month is equal to the number of such pairs at the end of the $(n-1)^{\text{st}}$ month plus the births of k^{th} generation rabbits during the n^{th} month. However, the births of k^{th} generation rabbits during the n^{th} month must come from $(k-1)^{\text{st}}$ generation rabbits who are at least two months old; there are precisely

$$S(n-2, k-1)$$

such pairs. Since there is only one zeroeth generation pair, we must have

$$S(n, 0) = 1. \tag{5}$$

To complete the proof, it is necessary only to verify that

$$S(n, k) = \binom{n-k-1}{k} \tag{6}$$

satisfies (4) and (5). Putting $k = 0$ in (6) we find $S(n, 0) = 1$. Substituting (6) into (4) we obtain

$$\binom{n - k - 1}{k} = \binom{n - k - 2}{k} + \binom{n - k - 2}{k - 1}$$

However, this is a well-known identity (see, e.g., [1, p. 70]).

For example, if we put $n = 12$ in identity (2), we find

$$F_{12} = 144 = 1 + 10 + 36 + 56 + 35 + 6.$$

Thus, among the 144 pairs of rabbits at the end of 12 months, there are, in addition to the initial pair, 10 first generation, 36 second generation, 56 third generation, 35 fourth generation, and 6 fifth generation pairs.

REFERENCE

1. J. G. Kemeny, J. L. Snell, & G. L. Thompson. *Introduction to Finite Mathematics*. 3rd ed. Englewood Cliffs, N.J.: Prentice-Hall, 1974.

◆◇◆◇◆

GOLDEN CUBOID SEQUENCES

MARSHALL WALKER
Atkinson College, York University
Downsview, Ontario, M3J 2R7, Canada

(Submitted November 1983)

The notion of a golden cuboid as a generalization of a golden rectangle was first introduced by Huntley [1], where it appears as a rectangular parallelepiped with edges 1, ϕ, and ϕ^2. In this paper, we proceed from a somewhat different point of view by first recalling that a golden rectangle may be defined as the unique rectangle with the property that adjunction of a square to the larger side gives a larger rectangle geometrically similar to the first. This definition is generalized to the situation of rectangular parallelepipeds, the results being two new candidates for the title "golden cuboid" (Theorem 1). Theorem 2 establishes a nested sequence of golden cuboids analogous to the well-known sequence of nested golden rectangles. An unexpected application occurs in [2] with the construction of an interpretative model for a disputed passage of Plato's *Timaeus*, lines 31b-32c.

In searching for a generalization of the above-mentioned property of golden rectangles, let R be a rectangular parallelepiped with edges a, b, and c, and suppose $a < b < c$. A larger geometrically similar parallelepiped R' can then always be produced by the adjunction of a single parallelepiped to R, provided $b/a = c/b$. However, as a generalization of the two-dimensional case, if we in addition insist that a cube appear in the adjunction process, then it is clear that at least two adjunctions must occur. This motivates the following definition.

Definition

A rectangular parallelepiped G is golden if there is a rectangular parallelepiped G' geometrically similar to G that is obtained from G by the adjunction of two rectangular parallelepipeds, one of which is a cube.

Continuing the previous discussion, if we wish to adjoin a cube to a rectangular parallelepiped R with edges a, b, and c satisfying $a < b < c$, there must first be a prior adjunction with the effect of making two of the dimensions equal. Adjunction of a cube then retains this property, and thus the result cannot be similar to R. Consequently, we must have

$$a = b < c \quad \text{or} \quad a < b = c.$$

An elementary analysis gives the following theorem.

Theorem 1

Up to geometric similarity, there are precisely two golden cuboids, a *type one golden cuboid* with edges 1, ϕ, and ϕ and a *type two golden cuboid* with edges 1, 1, and ϕ.

Now, consider the situation where A is a type one golden cuboid with edges 1, ϕ, and ϕ, and let C be a golden cuboid of type two with edges ϕ, ϕ, and ϕ^2.

Observe that C is formed from A by the adjunction of a cube B with edge ϕ. Furthermore, if a rectangular parallelepiped D with edges 1, ϕ, and ϕ^2 is adjoined to C, we obtain a rectangular parallelepiped A' similar to A; see Figure 1. Continuing, if a cube B' with edge ϕ^2 is adjoined to A', we obtain C' similar to C. Inductively, we thus obtain the following theorem.

Theorem 2

There exists an infinite increasing sequence of nested golden cuboids,

$A_1, C_1, A_2, C_2, \ldots, A_n, C_n, \ldots,$

in which, for each n, A_n is similar to A, C_n is obtained from A_n by adjunction of a cube and is similar to C, and A_{n+1} is obtained from C_n by adjunction of a parallelepiped similar to D.

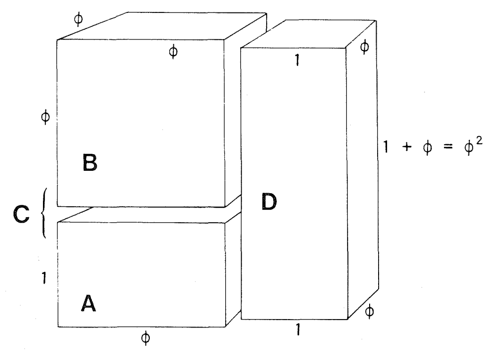

Figure 1

As in the case of golden rectangles, a decreasing sequence may be similarly constructed. We call these sequences *golden cuboid sequences.*

Remark 1: Observe that D is the "golden cuboid" of Huntley [1] but that it is neither of type one nor of type two.

Remark 2: Recall that if C is a golden rectangle and if B is a square excised by a cut parallel with the shorter side, then the remaining piece A is also golden and the areas are related by

$$\frac{\text{area}(C)}{\text{area}(B)} = \frac{\text{area}(B)}{\text{area}(A)} = \phi.$$

Now, consider the cuboid A' of the above discussion and observe that the sequence A, B, C, A' has the analogous property that

$$\frac{\text{volume}(A')}{\text{volume}(C)} = \frac{\text{volume}(C)}{\text{volume}(B)} = \frac{\text{volume}(B)}{\text{volume}(A)} = \phi.$$

REFERENCES

1. H. E. Huntley. "The Golden Cuboid." *The Fibonacci Quarterly* 2, no. 3 (1964):184.
2. M. Walker. "Mean and Extreme Ratio and Plato's *Timaeus*." (Preprint.)

◆◇◆◇◆

A PROPERTY OF CONVERGENTS TO THE GOLDEN MEAN

TONY VAN RAVENSTEIN
GRAHAM WINLEY
KEITH TOGNETTI
University of Wollongong, N.S.W. 2500, Australia

(Submitted November 1983)

If the simple continued fraction expansion of the positive real number α is given by

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}},$$

where a_j is a positive integer, then we denote the continued fraction expansion of α by

$$\{a_0, a_1, a_2, \ldots\}.$$

If

$$\beta = \{b_0, b_1, b_2, \ldots, b_{k-1}, a_k, a_{k+1}, a_{k+2}, \ldots\},$$

then α and β are defined to be equivalent. That is, they have the same tails at some stage.

The j^{th} total convergent to α, C_j, is given by

$$C_j = \{a_0, a_1, \ldots, a_j\},$$

and if we represent the rational number C_j by p_j/q_j, then it can be shown that

$$\begin{aligned} p_j &= p_{j-2} + a_j q_{j-1}, \\ q_j &= q_{j-2} + a_j q_{j-1}, \end{aligned} \tag{1}$$

for $j \geqslant 0$, $p_{-2} = q_{-1} = 0$, and $q_{-2} = p_{-1} = 1$.

It is easily proved (Chrystal [1], Khintchine [2]) that

$$q_{j+1} > q_j > q_{j-1} > \cdots > q_0 = 1,$$

$$C_0 < C_2 < C_4 < \cdots < \alpha < \cdots < C_5 < C_3 < C_1,$$

$$\lim_{j \to \infty} C_j = \alpha.$$

From Le Veque [3] or Roberts [4], we have the following theorems.

Dirichlet's Theorem

If a/b is a rational fraction such that

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$$

then a/b is a total convergent to α.

Hurwitz's Theorem

If α is irrational, then there are infinitely many irreducible rational solutions a/b such that

$$\left|\alpha - \frac{a}{b}\right| < \frac{\beta}{\sqrt{5}b^2} \quad \text{for } \beta = 1.$$

In fact, if we restrict α to be an irrational which is not equivalent to $\tau = (1 + \sqrt{5})/2 = \{1, 1, 1, \ldots\}$ (the Golden Mean), then we are able to find $0 < \beta < 1$ for which there are an infinite number of solutions. For example, if α is equivalent to $\sqrt{2}$, then from Le Veque [3, p. 252] we have $\beta = \sqrt{10}/4$.

Using (1), the convergents to τ are given by

$$C_j = \frac{F_{j+1}}{F_j}, \tag{2}$$

where F_j is a term of the Fibonacci sequence $\{1, 1, 2, 3, 5, \ldots\}$ and

$$F_j = \frac{\tau^{j+1} - (1 - \tau)^{j+1}}{\sqrt{5}} \quad \text{for } j = 0, 1, 2, \ldots . \tag{3}$$

It has been shown in Roberts [4] that in the particular case where $0 < \beta < 1$ there are only finitely many irreducible rational numbers a/b such that

$$\left|\tau - \frac{a}{b}\right| < \frac{\beta}{\sqrt{5}b^2}.$$

Since $0 < \beta < 1$, then $0 < \beta/\sqrt{5} < 1/2$, and so by Dirichlet's theorem there are only finitely many total convergents to τ such that

$$|\tau - C_j| < \frac{\beta}{\sqrt{5}q_j^2}, \tag{4}$$

where C_j is given by (2).

Our purpose is to determine explicitly the finite set of convergents to τ that satisfy (4).

If j is odd ($j = 2k + 1$, $k = 0, 1, 2, \ldots$), then using (2) in (4) we seek positive values of k such that

$$|\tau - C_{2k+1}| = \frac{F_{2k+2}}{F_{2k+1}} - \tau < \frac{\beta}{\sqrt{5}F_{2k+1}^2}. \tag{5}$$

Substituting (3) in (5) and simplifying,

$$[\tau(1 - \tau)]^{2k+2} - [(1 - \tau)^2]^{2k+2} < \frac{\sqrt{5}\beta}{2\tau - 1}.$$

Using $\tau^2 = 1 + \tau$, this becomes $1 - (2 - \tau)^{2k+2} = 1 - (5 - 3\tau)^{k+1} < \beta$ or

$$\frac{1 - \beta}{5 - 3\tau} < (5 - 3\tau)^k.$$

Taking natural logarithms and using $\tau = (1 + \sqrt{5})/2$, we have

$$k > \frac{\ln\left\{\frac{(1 - \beta)(7 + 3\sqrt{5})}{2}\right\}}{\ln\left\{\frac{7 - 3\sqrt{5}}{2}\right\}}. \tag{6}$$

If j is even ($j = 2k$, $k = 0, 1, 2, \ldots$), then substituting (2) in (4) we have

$$|\tau - C_{2k}| = \tau - \frac{F_{2k+1}}{F_{2k}} < \frac{\beta}{\sqrt{5}F_{2k}^2}.$$

By reasoning similar to that which led to (6), we find that

$$k < \frac{\ln\left\{\dfrac{(\beta - 1)(3 + \sqrt{5})}{2}\right\}}{\ln\left\{\dfrac{7 - 3\sqrt{5}}{2}\right\}}. \tag{7}$$

We note that the denominator of the right-hand side of (6) is negative and so positive values of k in (6) exist only if

$$\ln\left\{\frac{(1 - \beta)(7 + 3\sqrt{5})}{2}\right\} < 0,$$

which means $1 > \beta > (3\sqrt{5} - 5)/2$.

Similarly, we see that since $0 < \beta < 1$ there are no positive values of k that satisfy (7).

Hence, there are no convergents to τ that satisfy (4) unless

$$\frac{3\sqrt{5} - 5}{2} < \beta < 1,$$

and in this case the only convergents that do satisfy (4) are given by

$$\left.\begin{aligned} &C_j = \frac{F_{j+1}}{F_j}; \quad j = 1, 3, 5, 7, \ldots, 2[R] + 1, \\ &\text{where} \\ &R = \ln\frac{(1 - \beta)(7 + 3\sqrt{5})}{2} \Big/ \ln\frac{7 - 3\sqrt{5}}{2}, \end{aligned}\right\} \tag{8}$$

and $[R]$ denotes the integer part of R. Consequently, there are $[R] + 1$ convergents to τ that satisfy (4), and these may be determined explicitly from (8).

REFERENCES

1. G. Chrystal. *Algebra.* 2nd ed. Edinburgh: Adam and Charles Black, 1939.
2. A. Ya. Khintchine. *Continued Fractions.* Trans. P. Wynn. Groningen, The Netherlands: P. Noordhoff, 1963.
3. W. J. Le Veque. *Fundamentals of Number Theory.* Reading, Mass.: Addison-Wesley, 1977.
4. J. Roberts. *Elementary Number Theory: A Problem Oriented Approach.* Cambridge, Mass.: The M.I.T. Press, 1977.

GENERATORS OF UNITARY AMICABLE NUMBERS

O. W. McCLUNG

University of San Francisco, San Francisco, CA 94117

(Submitted November 1983)

1. INTRODUCTION

In this paper, unless otherwise stated, lower-case letters denote positive integers with p and q reserved for primes.

Definition

A divisor d of n is a *unitary divisor* if $(n, n/d) = 1$, denoted by $d \| n$.

The sum of all unitary divisors of n will be denoted $\sigma^*(n)$. If

$$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k},$$

then

$$\sigma^*(n) = (1 + p_1^{e_1})(1 + p_2^{e_2}) \cdots (1 + p_k^{e_k}).$$

Hence, σ^* is multiplicative. If $\sigma(n)$ is the sum of all divisors of n, then

$$\sigma(n) = \sigma^*(n) \text{ iff } n \text{ is square-free.}$$

Note that

$$\sigma^*(n) = n \text{ iff } n = 1.$$

Hagis [1] defines a pair of positive integers m and n to be *unitary amicable numbers* if $\sigma^*(m) = \sigma^*(n) = m + n$. If m and n are both square-free, then the pair m, n is amicable (see [2]) iff it is unitary amicable. Independently, Wall [3] studies unitary amicable numbers and finds approximately six hundred pairs that are not amicable pairs. Hagis proves some elementary theorems concerning unitary amicable numbers and gives a table of thirty-two unitary amicable pairs that are not amicable pairs. (A thirty-third such pair,

$$11777220 = 2^2 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 719, \quad 12414780 = 2^2 3^2 5 \cdot 7 \cdot 59 \cdot 167,$$

follows from his theorem 4 and was inadvertently omitted from the table.) This paper generalizes Theorems 4 and 5 of [1] and augments Hagis' list of unitary amicable pairs that are not amicable pairs by twenty-five.

2. THE MAIN RESULTS

In this section, we find conditions on a unitary amicable pair which are sufficient to generate another such pair. The main idea is that of a generator.

Definition

The pair (f, k), where f is a rational number not equal to one and k is an integer, is a *generator* if fk is an integer and $\sigma^*(fk) = f\sigma^*(k)$.

Remark: If $k = 1$ in the above definition, then $\sigma^*(f) = f$, which implies that $f = 1$. Thus $k \neq 1$.

Generators, in conjunction with unitary amicable pairs of a specified form, produce new unitary amicable pairs. In what follows, m and n denote a unitary amicable pair.

Theorem 1

If (f, k) is a generator, $m = km_1$, $n = kn_1$, and $(fk, m_1n_1) = (k, m_1n_1) = 1$, then fkm_1, fkn_1 is a unitary amicable pair.

Proof: $\sigma^*(km_1) = \sigma^*(kn_1) = k(m_1 + n_1)$, since m, n is a unitary amicable pair. Thus,

$$\sigma^*(k)\sigma^*(m_1) = \sigma^*(k)\sigma^*(n_1) = k(m_1 + n_1),$$

since $(k, m_1n_1) = 1$. Hence,

$$f\sigma^*(k)\sigma^*(m_1) = f\sigma^*(k)\sigma\ (n_1) = fk(m_1 + n_1),$$

which yields

$$\sigma^*(fk)\sigma^*(m_1) = \sigma^*(fk)\sigma\ (n_1) = fk(m_1 + n_1),$$

since (f, k) is a generator.

Both f, a rational number, and k can be factored uniquely into a product of primes with nonzero (possibly negative) powers. Let $\pi(f)$ and $\pi(k)$ denote the number of primes in the factorization of f and k, respectively. Subsequent results classify all generators with $\pi(f) \leqslant 2$ and $\pi(k) = 1$.

Definition

The numbers f and k are *relatively prime* if their prime factorizations have no common prime.

Lemma 1

If (f, k) is a generator, then f and k are not relatively prime.

Proof: Suppose that f and k are relatively prime. Then they have distinct primes in their prime factorizations. Since fk is an integer, f is also. Thus,

$$\sigma^*(fk) = \sigma^*(f)\sigma^*(k) = f\sigma^*(k),$$

yielding $\sigma^*(f) = f$, which implies $f = 1$, a contradiction to the definition of a generator.

Theorem 2

There does not exist a generator (f, k) with $\pi(f) = \pi(k) = 1$.

Proof: Suppose that (f, k) is a generator with $\pi(f) = \pi(k) = 1$. By Lemma 1, there is a prime p such that $f = p^a$ and $k = p^b$ for some a and b. Since fk is an integer, $a + b \geqslant 0$. Because $k \neq 1$ in a generator, we must have $b > 0$. Similarly, $f \neq 1$ implies $a \neq 0$.

Case 1: If $a + b = 0$, then

$\sigma^*(fk) = \sigma^*(p^{a+b}) = \sigma^*(1) = 1$

and

$f\sigma^*(k) = p^a\sigma^*(p^b) = p^a(1 + p^b) = p^a + p^{a+b} = p^a + 1.$

Since $\sigma^*(fk) = f\sigma^*(k)$, we have $1 = p^a + 1$ or $p^a = 0$, a contradiction.

Case 2: If $a + b > 0$, then

$\sigma^*(fk) = \sigma^*(p^{a+b}) = 1 + p^{a+b}$

and

$f\sigma^*(k) = p^a + p^{a+b}.$

Thus, $1 + p^{a+b} = p^a + p^{a+b}$, which implies $p^a = 1$ or $a = 0$, a contradiction.

Definition

For the positive rational number f, the prime p *divides* f (written $p|f$) if p occurs in the prime factorization of f.

Lemma 2

Let (f, k) be a generator and p be a prime such that $p^a \| k$ and $p \nmid f$. Then (f, kp^{-a}) is a generator.

Proof: Let $k = p^a r$, where $a > 0$ and $(p, r) = 1$. Then $fk = fp^a r$ is an integer. Since $p \nmid f$, it follows that fr is an integer and that $p \nmid fr$. Hence,

$\sigma^*(fk) = \sigma^*(fp^a r) = (1 + p^a)\sigma^*(fr).$

Also

$f\sigma^*(k) = f\sigma^*(p^a r) = f(1 + p^a)\sigma^*(r).$

Hence, $(1 + p^a)\sigma^*(fr) = (1 + p^a)f\sigma^*(r)$, yielding $\sigma^*(fr) = f\sigma^*(r)$. Thus, (f, r) is a generator.

Therefore, "extraneous" primes may be eliminated from k.

Theorem 3

There does not exist a generator (f, k) with $\pi(f) = 1$ and $\pi(k) = 2$.

Proof: Suppose that (f, k) is a generator with $\pi(f) = 1$ and $\pi(k) = 2$. Then there is a prime p and an integer a with $p^a \| k$ and $p \nmid f$. By Lemma 2, (f, kp^{-a}) is a generator with $\pi(f) = \pi(kp^{-a}) = 1$, a contradiction of Theorem 2.

Theorem 4 characterizes all generators (f, k) with $\pi(f) = 2$ and $\pi(k) = 1$.

Theorem 4

The pair (f, k) is a generator with $\pi(f) = 2$ and $\pi(k) = 1$ iff there are primes p and q and positive integers a, b, and c such that $f = p^b q^c$, $k = p^a$, and $1 + p^{a+b} = q^c(p^b - 1)$.

Proof: Let (f, k) be a generator with $\pi(f) = 2$ and $\pi(k) = 1$. By Lemma 1, there are primes p and q and nonzero integers a, b, and c such that $f = p^b q^c$ and $k = p^a$. Since $k \neq 1$, it follows that $a > 0$. Because fk is an integer, we have $a + b \geqslant 0$ and $c > 0$. We therefore have $fk = p^{a+b}q^c$.

Case 1: If $a + b = 0$, then

$$\sigma^*(fk) = \sigma^*(q^c) = 1 + q^c$$

and

$$f\sigma^*(k) = p^b q^c \sigma^*(p^a) = p^b q^c(1 + p^a) = p^b q^c + p^{a+b}q^c = p^b q^c + q^c.$$

Thus, $1 + q^c = p^b q^c + q^c$, which implies $p^b q^c = 1$. Thus, $b = c = 0$, a contradiction.

Case 2: If $a + b > 0$, then

$$\sigma^*(fk) = \sigma^*(p^{a+b}q^c) = (1 + p^{a+b})(1 + q^c) = 1 + p^{a+b} + q^c + p^{a+b}q^c$$

and

$$f\sigma^*(k) = p^b q^c \sigma^*(p^a) = p^b q^c(1 + p^a) = p^b q^c + p^{a+b}q^c.$$

Therefore,

$$1 + p^{a+b} + q^c + p^{a+b}q^c = p^b q^c + p^{a+b}q^c,$$

yielding

$$1 + p^{a+b} + q^c = p^b q^c.$$

Since $1 + p^{a+b} + q^c$ is an integer, $p^b q^c$ is an integer and, hence, $b \geqslant 0$. If $b = 0$, then $k = p^a$, $f = q^c$, and $(f, k) = 1$, a contradiction of Lemma 1. Thus, $b > 0$ and $1 + p^{a+b} = q^c(p^b - 1)$.

If p and q are primes, and a, b, and c are positive integers such that $f = p^b q^c$, $k = p^a$, and $1 + p^{a+b} = q^c(p^b - 1)$, then clearly fk is an integer. Also

$$\begin{aligned}\sigma^*(fk) = \sigma^*(p^{a+b}q^c) &= (1 + p^{a+b})(1 + q^c) = 1 + p^{a+b} + q^c + p^{a+b}q^c\\ &= q^c(p^b - 1) + q^c + p^{a+b}q^c = p^b q^c + p^{a+b}q^c\\ &= p^b q^c(1 + p^a) = f\sigma^*(k).\end{aligned}$$

Therefore, (f, k) is a generator.

Theorem 5

The equation

$$1 + p^{a+b} = q^c(p^b - 1)$$

has a solution only if $p = 2$ and $b = 1$ or $p = 2$ and $b = 2$ or $p = 3$ and $b = 1$.

Proof: Suppose that $1 + p^{a+b} = q^c(p^b - 1)$ has a solution. Then,

$$p^b - 1 \mid p^{a+b} + 1 \quad \text{or} \quad p^{a+b} = -1 \text{ in } Z(p^b - 1),$$

the ring of integers modulo $p^b - 1$. Since $p^b = 1$ in $Z(p^b - 1)$, we have

$$p^{a+b} = p^a p^b = p^a \text{ in } Z(p^b - 1).$$

Hence,

$$p^a = -1 = p^b - 2 \text{ in } Z(p^b - 1).$$

Since

$$(p,\ p^b - 1) = (p^b - 2,\ p^b - 1) = 1,$$

we see that p and $p^b - 2$ belong to $U(p^b - 1)$, the group of units of $Z(p^b - 1)$. Thus, $p^a = p^b - 2$ in $U(p^b - 1)$. Also, there exist a and b such that

$$p^a = p^b - 2 \text{ iff } p^b - 2 \in \langle p \rangle,$$

the cyclic subgroup generated by p in $U(p^b - 1)$. If $c < b$, then

$$p^c - 1 < p^b - 1 \quad \text{and} \quad p^b - 1 \nmid p^c - 1,$$

so $p^c \neq 1$ in $U(p^b - 1)$. Since $p^b = 1$ in $U(p^b - 1)$, the order of p in $U(p^b - 1)$ is b and $\langle p \rangle = \{1, p, p^2, \ldots, p^{b-1}\}$. Note that

$$\begin{aligned} p^{b-1} < p^b - 2 \ &\text{iff } p^b - p^{b-1} > 2 \\ &\text{iff } p^{b-1}(p - 1) > 2 \\ &\text{iff } p^{b-1} > \frac{2}{p - 1} \\ &\text{iff } b - 1 > \log_p \frac{2}{p - 1} \\ &\text{iff } b > 1 + \log_p \frac{2}{p - 1}. \end{aligned}$$

If $p = 2$, then

$$\log_p \frac{2}{p - 1} = \log_2 \frac{2}{2 - 1} = \log_2 2 = 1.$$

Then

$$\begin{aligned} b > 2 \ &\text{iff } p^{b-1} < p^b - 2 \\ &\text{iff } p^b - 2 \notin \langle p \rangle, \end{aligned}$$

a contradiction. Thus, if $b > 2$, there does not exist a solution to (1).

If $p = 3$, then

$$\log_p \frac{2}{p - 1} = \log_3 1 = 0.$$

Then $b > 1$ iff $p^{b-1} < p^b - 2$. Hence, if $b > 1$, there does not exist a solution to (1).

Also

$$\begin{aligned} \log_p \frac{2}{p - 1} < 0 \ &\text{iff } \log_p 2 - \log_p(p - 1) < 0 \\ &\text{iff } \log_p 2 < \log_p(p - 1) \\ &\text{iff } 2 < p - 1 \\ &\text{iff } p > 3. \end{aligned}$$

Thus, if $p > 3$, then

$$1 + \log_p \frac{2}{p - 1} < 1,$$

which yields

$$b > 1 + \log_p \frac{2}{p - 1} \quad \text{for all } b.$$

Hence, $p^{b-1} < p^b - 2$ and there does not exist a solution to (1).

A computer-assisted search for solutions to (1) for a restricted range of values of a yields Table 1, which also lists the sixteen generators associated with these solutions. When these sixteen generators are applied, iteratively, to the table of thirty-three unitary amicable pairs that are not amicable pairs in [1], the result is the collection of twenty-five pairs in Table 2. Although not in [1], all but the 12th, 17th, and 18th pairs are found in [3].

Table 1

	a	c	q	k	f
$p = 2,\ b = 1,\ 1 \leqslant a \leqslant 31$	1	1	5	2	$2 \cdot 5$
	2	2	3	2^2	$2 \cdot 3$
	3	1	17	2^3	$2 \cdot 17$
	7	1	257	2^7	$2 \cdot 257$
	15	1	65537	2^{15}	$2 \cdot 65537$
$p = 2,\ b = 2,\ 1 \leqslant a \leqslant 30$	1	1	3	2	$2^2 3$
	3	1	11	2^3	$2^2 11$
	5	1	43	2^5	$2^2 43$
	9	1	683	2^9	$2^2 683$
	11	1	2731	2^{11}	$2^2 2731$
	15	1	43691	2^{15}	$2^2 43691$
	17	1	174763	2^{17}	$2^2 173763$
	21	1	2796203	2^{21}	$2^2 2796203$
$p = 3,\ b = 1,\ 1 \leqslant a \leqslant 19$	1	1	5	3	$3 \cdot 5$
	3	1	41	3^3	$3 \cdot 41$
	15	1	21523361	3^{15}	$3 \cdot 21523361$

Table 2. Unitary Amicable Pairs

(1) $1707720 = 2^3 3 \cdot 5 \cdot 7 \cdot 19 \cdot 107$
$2024760 = 2^3 3 \cdot 5 \cdot 47 \cdot 359$

(2) $3951990 = 2 \cdot 3^4 5 \cdot 7 \cdot 17 \cdot 41$
$4974858 = 2 \cdot 3^4 7 \cdot 41 \cdot 107$

(3) $6940890 = 2 \cdot 3^4 5 \cdot 11 \cdot 19 \cdot 41$
$7937190 = 2 \cdot 3^4 5 \cdot 41 \cdot 239$

(4) $29656530 = 2 \cdot 3^4 5 \cdot 19 \cdot 41 \cdot 47$
$29855790 = 2 \cdot 3^4 5 \cdot 29 \cdot 31 \cdot 41$

(5) $58062480 = 2^4 3 \cdot 5 \cdot 7 \cdot 17 \cdot 19 \cdot 107$
$68841840 = 2^4 3 \cdot 5 \cdot 17 \cdot 47 \cdot 359$

(6) $72696690 = 2 \cdot 3^4 5 \cdot 11 \cdot 41 \cdot 199$
$76084110 = 2 \cdot 3^4 5 \cdot 29 \cdot 41 \cdot 79$

(7) $75139680 = 2^5 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 107$
$89089440 = 2^5 3 \cdot 5 \cdot 11 \cdot 47 \cdot 359$

(8) $491170680 = 2^3 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29 \cdot 47$
$553923720 = 2^3 3^2 5 \cdot 7 \cdot 19 \cdot 23 \cdot 503$

Table 2—continued

(9)	1476394920	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 71 \cdot 241$
	6479522280	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 23 \cdot 10163$
(10)	5530444920	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 103 \cdot 149$
	5791411080	=	$2^3 3^2 5 \cdot 7 \cdot 13 \cdot 17 \cdot 10399$
(11)	6365038680	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 1039$
	7221188520	=	$2^3 3^2 5 \cdot 7 \cdot 13 \cdot 53 \cdot 4159$
*(12)	12924024960	=	$2^7 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 43 \cdot 107$
	15323383680	=	$2^7 3 \cdot 5 \cdot 11 \cdot 43 \cdot 47 \cdot 359$
(13)	16699803120	=	$2^4 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29 \cdot 47$
	18833406480	=	$2^4 3^2 5 \cdot 7 \cdot 17 \cdot 19 \cdot 23 \cdot 503$
(14)	74555240760	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 10889$
	83515287240	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 83 \cdot 36299$
(15)	88962742748880	=	$2^4 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 43 \cdot 131 \cdot 1289$
	95916546799920	=	$2^4 3^2 5 \cdot 7 \cdot 11 \cdot 17 \cdot 43 \cdot 139 \cdot 17027$
(16)	209173484520	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 43 \cdot 13499$
	221927955480	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 29 \cdot 359 \cdot 769$
*(17)	214910193960	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 19 \cdot 53 \cdot 7699$
	216191246040	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 17 \cdot 149 \cdot 3079$
*(18)	408774005640	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 191 \cdot 5939$
	418940759160	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 19 \cdot 307 \cdot 2591$
(19)	2534878185840	=	$2^4 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 10899$
	2839519766160	=	$2^4 3^2 5 \cdot 7 \cdot 11 \cdot 17 \cdot 83 \cdot 36299$
(20)	2616551257320	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 43 \cdot 131 \cdot 1289$
	2821074905880	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 43 \cdot 139 \cdot 17027$
(21)	6642948829440	=	$2^8 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 43 \cdot 107 \cdot 257$
	7876219211520	=	$2^8 3 \cdot 5 \cdot 7 \cdot 11 \cdot 43 \cdot 47 \cdot 257 \cdot 359$
(22)	7111898473680	=	$2^4 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 43 \cdot 13499$
	7545550486320	=	$2^4 3^2 5 \cdot 7 \cdot 11 \cdot 17 \cdot 29 \cdot 359 \cdot 769$
(23)	13898316191760	=	$2^4 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 191 \cdot 5939$
	14243985811440	=	$2^4 3^2 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 307 \cdot 2591$
(24)	32583815704440	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 13 \cdot 181 \cdot 499559$
	33402225434760	=	$2^3 3^2 5 \cdot 7 \cdot 13 \cdot 17 \cdot 181 \cdot 229 \cdot 1447$
(25)	106595643389918760	=	$2^3 3^2 5 \cdot 7 \cdot 11 \cdot 19 \cdot 61 \cdot 853 \cdot 3889679$
	106934121830433240	=	$2^3 3^2 5 \cdot 7 \cdot 17 \cdot 19 \cdot 37 \cdot 61 \cdot 853 \cdot 68239$

3. CONJECTURES

A preliminary investigation of generators in which $\pi(f) \geqslant 2$ and $\pi(k) \geqslant 2$ suggests the following.

Conjecture 1

The only generator (f, k) with $\pi(f) = \pi(k) = 2$ is $(3/2, 12)$.

Conjecture 2

There are no generators (f, k) with $\pi(f) > 2$ or $\pi(k) > 2$.

REFERENCES

1. P. Hagis, Jr. "Unitary Amicable Numbers." *Math. of Comp.* 25 (1971):915-18.
2. U. Dudley. *Elementary Number Theory*. San Francisco: W. H. Freeman, 1969.
3. C. R. Wall. "Topics Related to the Sum of Unitary Divisors of an Integer." Ph.D. Dissertation, The University of Tennessee, 1970.

◆◇◆◇◆

A NOTE ON BINOMIAL COEFFICIENTS AND CHEBYSHEV POLYNOMIALS

MAURO BOSCAROL
Università di Trento, Italy

(Submitted December 1983)

In [1] the author gave a demonstration in a slightly different notation of the following property of binomial coefficients: for every integer n, and $k < n$,

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

In this note we shall be concerned with an application of (1) to a problem involving Chebyshev polynomials of the first kind. Remember that the Chebyshev polynomial of the first kind $T_n(x)$ is defined in $-1 \leqslant x \leqslant 1$ as

$$T_n(x) = \cos n(\arccos x).$$

For the sake of convenience we sometimes use the notation T_n instead of $T_n(x)$. We shall use the following two identities (see, e.g., [2] for the proofs):

(a) for every integer n,

$$T_{-n} = T_n; \tag{2}$$

(b) for r, $n > 0$,

$$x^r T_n(x) = 2^{-r} \sum_{i=0}^{r} \binom{r}{i} T_{n-r+2i}(x). \tag{3}$$

Proposition 1

For every integer $n \geqslant 1$, we have

$$\sum_{i=0}^{n-1} x^i T_{n-i-1} = \sum_{i=0}^{n-1} T_{n-2i-1}. \tag{4}$$

Proof: Using (3), we can write the summation on the left as

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

or, changing indexes,

$$S = \sum_{i=0}^{n-1} \sum_{j=0}^{i} 2^{-(n-i+j-1)} \binom{n-i+j-1}{j} T_{-n+2i+1}. \tag{5}$$

We denote by C_i the term involving $T_{-n+2i+1}$ in (5), $i = 0, \ldots, n-1$. Then

$$S = C_0 + C_1 + C_2 + \cdots + C_{n-1} \tag{6}$$

and also, in reverse order,

$$S = C_{n-1} + C_{n-2} + \cdots + C_1 + C_0. \tag{7}$$

Adding (6) and (7) term by term, we can write

$$2S = (C_0 + C_{n-1}) + (C_1 + C_{n-2}) + \cdots + (C_{n-1} + C_0)$$

$$= \sum_{k=0}^{n-1} (C_k + C_{n-k-1}). \tag{8}$$

Now, from (5),

$$C_k = \sum_{j=0}^{k} 2^{-(n-k+j-1)} \binom{n-k+j-1}{j} T_{-n+2k+1}$$

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

Because of (2), $T_{n-2k-1} = T_{-n+2k+1}$. Therefore,

$$C_k + C_{n-k-1} = \left[\sum_{j=0}^{k} 2^{-(n-k+j-1)} \binom{n-k+j-1}{1} \right.$$

$$\left. + \sum_{j=0}^{n-k-1} 2^{-(k+j)} \binom{k+j}{j} \right] T_{n-2k-1}.$$

But the coefficient of T_{n-2k-1} in the above formula is just the expression (1), which is always equal to 2, regardless of the values of n and k. Hence, we can rewrite (8) as

$$2S = \sum_{k=0}^{n-1} 2T_{n-2k-1},$$

and the proposition is thus proved.

Corollary 1

For every integer $n \geqslant 1$,

$$T_n' = n \sum_{i=0}^{n-1} T_{n-2i-1} = n \sum_{i=0}^{n-1} x^i T_{n-i-1}, \tag{9}$$

where T_n' is the first derivative of T_n with respect to x.

Proof: Let $f = \arccos x$ and $\omega = e^{if} = \cos f + i \sin f$. Then, from the definition of $T_n(x)$,

$$\frac{T_n'(x)}{n} = \frac{\sin nf}{\sin f} = \frac{\omega^n - \omega^{-n}}{\omega - \omega^{-1}} = \frac{\omega^{n-1}(1 - \omega^{-2n})}{1 - \omega^{-2}} = \sum_{i=0}^{n-1} \omega^{n-2i-1}$$

$$= \frac{1}{2} \sum_{i=0}^{n-1} (\omega^{n-2i-1} + \omega^{-n+2i+1}) = \sum_{i=0}^{n-1} \cos(n - 2i - 1)f = \sum_{i=0}^{n-1} T_{n-2i-1},$$

and from Proposition 1, the conclusion follows.

A proof of the first equality of (9) is found also in [3].

Remark: Remember that the Chebyshev polynomial of the second kind $U_n(x)$ is defined as

$$U_n(f) = \frac{\sin(n+1)f}{\sin f} \quad \text{(notation as in the proof of Corollary 1).}$$

From Corollary 1 and the known result $T_n' = nU_{n-1}$, it follows that

$$U_n = \sum_{i=0}^{n} T_{n-2i}.$$

ACKNOWLEDGMENT

The author wishes to acknowledge and thank the referee for his useful remarks and thoughtful criticism of the material and terminology in this paper. I am also grateful to Professor Peter Henrici for pointing out a simplification of my previous demonstration of (9).

REFERENCES

1. M. Boscarol. "A Property of Binomial Coefficients." *The Fibonacci Quarterly* **20**, no. 3 (1982):249-51.
2. L. Fox & B. Parker. *Chebyshev Polynomials in Numerical Analysis*. Oxford: Oxford University Press, 1968 (rpt. with correction, 1972).
3. L. Gatteschi. "Funzioni speciali." *UTET*, 1973.

◆◇◆◇◆

RANDOM FIBONACCI-TYPE SEQUENCES

R. DAWSON, G. GABOR, R. NOWAKOWSKI, D. WIENS
Dalhousie University, Halifax, Nova Scotia

(Submitted December 1983)

1. INTRODUCTION

In this paper, we shall study several random variations of Fibonacci-type sequences. The study is motivated in part by a sequence defined by D. Hofstadter and discussed by R. Guy [1]:

$$h_1 = h_2 = 1, \quad h_n = h_{n-h_{n-1}} + h_{n-h_{n-2}}.$$

Although this sequence is completely deterministic, its graph resembles that of the path of a particle fluctuating randomly about the line $h = n/2$. Indeed, there appear to be no results on the quantitative behaviour of this sequence.

Hoggatt and Bicknell [3] and Hoggatt and Bicknell-Johnson [4] studied the behavior of "r-nacci" sequences, in which each term is the sum of the previous r terms. A natural extension of such a sequence is one in which each term is the sum of a fixed number of previous terms, randomly chosen from all previous terms. Heyde [2] investigated martingales whose conditional expectations form Fibonacci sequences, and established almost sure convergence of ratios of consecutive terms to the golden ratio.

We consider three types of sequences:

(i) For fixed positive integers p and q, and values $f_1, \ldots, f_p$; let $F_i = f_i$ with probability one for $i \leqslant p$, and set

$$F_{n+1} = \sum_{i=1}^{q} F_{k_i} \quad \text{for } n > p,$$

where the k_i are randomly chosen, with replacement, from $\{1, 2, \ldots, n\}$. The sequence $\{F_n\}$ is termed a (p, q) sequence.

(ii) If, in the above, the k_i are chosen without replacement, we call $\{F_n\}$ a $(p, q)'$ sequence.

(iii) For given values g_0, g_1, let $G_0 = g_0$, $G_1 = g_1$ with probability one, and set

$$G_{n+1} = X_n G_n + Y_{n-1} G_{n-1},$$

where $\{(X_n, Y_{n-1})'\}$ is a sequence of independent random vectors. We assume that X_n and Y_{n-1} have finite first and second moments independent of n, and are distributed independently of G_n and G_{n-1}.

In Section 2, we derive the sequence of first moments for (p, q) and $(p, q)'$ sequences, and obtain recurrence relations for the sequence of second moments of a (p, q) sequence. In Section 3, similar results are obtained for $\{G_n\}$, and it is shown that, under mild conditions, the sequence of coefficients of variation is unbounded. Section 4 addresses questions concerning the ranges of (p, q) and $(p, q)'$ sequences. Some open problems are discussed in Section 5.

2. MOMENTS OF (p, q) AND $(p, q)'$ SEQUENCES

Theorem 1

For the (p, q) sequence described in the Introduction, the expected value of the n^{th} term, for $n > p$, is

$$E[F_n] = \frac{\binom{n+q-2}{q-1}}{\binom{p+q-1}{q}} \sum_{j=1}^{p} f_j. \tag{2.1}$$

Proof: Given $\mathbf{F}_n \overset{\text{def.}}{\equiv} (F_1, \ldots, F_n)'$, we have

$$F_{n+1} = \sum_{j=1}^{n} F_j X_j,$$

where X_j is the number of times F_j is chosen in the formation of F_{n+1}. Then, $\mathbf{X} \overset{\text{def.}}{\equiv} (X_1, \ldots, X_n)'$ is a multinomially distributed random vector with

$$P\left(\bigcap_{j=1}^{n} (X_j = x_j)\right) = q!n^{-q} \Big/ \prod_{j=1}^{n} x_j!$$

if $0 \leqslant x_j \leqslant q$ and $\sum x_j = q$, zero otherwise. Thus, $E[X_j] = q/n$, so that the conditional expectation of F_{n+1}, given $\mathbf{F}_n$, is

$$E[F_{n+1} | \mathbf{F}_n] = qn^{-1} \sum_{j=1}^{n} F_j.$$

Taking a further expectation over $\mathbf{F}_n$ gives

$$E[F_{n+1}] = qn^{-1} \sum_{j=1}^{n} E[F_j]. \tag{2.2}$$

This leads to the recurrence relation $nE[F_{n+1}] = (n - 1 + q)E[F_n]$ $(n > p)$, from which (2.1) follows. □

Corollary 1

For the $(p, q)'$ sequence described in the Introduction, $E[F_n]$ is again given by (2.1).

Proof: Given $\mathbf{F}_n$, we may define F_{n+1} as

$$\sum_{j=1}^{n} F_j X_j,$$

where now $(X_1, \ldots, X_n)$ is a sequence of $(n - q)$ zeros and q ones, with

$$P\left(\bigcap_{j=1}^{n} (X_j = x_j)\right) = 1 \Big/ \binom{n}{q}, \quad x_j \in \{0, 1\}.$$

Marginally, X_j has a binomial $(1, q/n)$ distribution, with $E[X_j] = q/n$. Thus, (2.1) follows as in the above proof. □

If, as in the deterministic Fibonacci sequence, we place $p = q = 2$, $f_1 = 1$, $f_2 = 2$, then $E[F_n] = n$. In general, $E[F_n]$ is a polynomial in n of degree $q - 1$; this contrasts with the exponential growth of the Fibonacci sequence.

The determination of the sequence of second moments of a (p, q) sequence is somewhat more involved. Define

$$\alpha_n = (2(n-1) + q)(n - 1 + q)/n^2,$$

$$\beta_{n-1} = (n(n-1) + (q-1)(3n + 3q - 4))/n^2,$$

$$\gamma_{n+1} = nq/((q-1)(2q-1)),$$

$$\delta_n = q(n(n - 1 + q) - (q-1)^2)/(n(q-1)(2q-1)),$$

$$\nu_1 = \sum_{j=1}^{p} f_j/p, \quad \nu_2 = \sum_{j=1}^{p} f_j^2/p.$$

Theorem 2

For a (p, q) sequence, if $q = 1$, then

$$E[F_n^2] = \nu_2 \quad \text{for } n > p.$$

If $q > 1$, then

$$\begin{aligned} E[F_{p+1}^2] &= q\nu_2 + q(q-1)\nu_1^2, \\ E[F_{p+2}^2] &= \frac{q}{(p+1)^2}\{(p^2 + p + pq + q^2)\nu_2 + (q-1)(p^2 + 3pq + q^2)\nu_1^2\}; \end{aligned} \tag{2.3}$$

$$E[F_nF_{n+1}] = \gamma_{n+1}E[F_{n+1}^2] - \delta_n E[F_n^2], \quad (n \geqslant p + 1); \tag{2.4}$$

$$E[F_{n+1}^2] = \alpha_n E[F_n^2] - \beta_{n-1}E[F_{n-1}^2], \quad (n \geqslant p + 2). \tag{2.5}$$

Proof: Representing F_{n+1}, given $\mathbf{F}_n$, as in Theorem 1, we find

$$E[F_{n+1}^2] = \frac{q}{n}\sum_{j=1}^{n} E[F_j^2] + \frac{q(q-1)}{n^2}E\left[\left(\sum_{j=1}^{n} F_j\right)^2\right] \tag{2.6}$$

$$= \frac{q(n + q - 1)}{n^2}\sum_{j=1}^{n} E[F_j^2] + \frac{q(q-1)}{n^2}\sum_{i \neq j}^{n} E[F_iF_j], \tag{2.7}$$

$$E[F_nF_{n+1}] = \frac{q}{n}\sum_{j=1}^{n-1} E[F_jF_n] + \frac{q}{n}E[F_n^2]. \tag{2.8}$$

The first statement of Theorem 2, and (2.3), are implied by (2.6). Assume now that $q > 1$. Replacing n by $n - 1$ in (2.7), subtracting the result from (2.7), and using (2.8) gives

$$\begin{aligned} n^2E[F_{n+1}^2] = \{(n-1)^2 + q(n + 1 - q)\}E[F_n^2] \\ + q\sum_{j=1}^{n-1} E[F_j^2] + 2n(q-1)E[F_nF_{n+1}]. \end{aligned} \tag{2.9}$$

Given $\mathbf{F}_n$, we may represent $F_{n+1}F_{n+2}$ as

$$\sum_{j=1}^{n} F_jX_j \cdot \sum_{k=1}^{n+1} F_kY_k,$$

where **X**, **Y** are independent random vectors, **X** is as in Theorem 1, and **Y** is distributed as is **X**, but with n replaced by $n + 1$. We then find

$$E[F_{n+1}F_{n+2}] = \frac{q^2}{n(n+1)} E\left[\left(\sum_{j=1}^{n} F_j\right)^2\right] + \frac{q}{n+1} E[F_{n+1}^2]. \tag{2.10}$$

Combining (2.6) and (2.10), then replacing n by $n - 1$ gives

$$E[F_n F_{n+1}] = \frac{q(n+q-2)}{n(q-1)} E[F_n^2] - \frac{q^2}{n(q-1)} \sum_{j=1}^{n-1} E[F_j^2]. \tag{2.11}$$

Combining (2.9) and (2.11), so as to eliminate $\sum_{j=1}^{n} E[F_j^2]$, yields (2.4). Combining them so as to eliminate $E[F_n F_{n+1}]$ gives

$$n^2 E[F_{n+1}^2] = \{(n-1)^2 + 3q(n-1) + q^2\} E[F_n^2] + (q - 2q^2) \sum_{j=1}^{n-1} E[F_j^2]. \tag{2.12}$$

Replacing n by $n - 1$ in (2.12) and subtracting now yields (2.5). □

Define the "sample" means and variances by

$$\overline{F}_n = \sum_{j=1}^{n} F_j / n, \quad S_n^2 = \sum_{j=1}^{n} (F_j - \overline{F}_n)^2 / n.$$

From (2.2) and (2.8), then from (2.2) and (2.6), we get the interesting relationships

$$\mathrm{cov}[F_{n+1}, F_n] = q\ \mathrm{cov}[F_n, \overline{F}_n], \tag{2.13}$$

$$\mathrm{var}[F_{n+1}] = qE[S_n^2] + q^2 \mathrm{var}[\overline{F}_n]. \tag{2.14}$$

From (2.13) or otherwise, it is clear that F_n and F_{n+1} are positively correlated. Thus, from (2.9) and (2.12),

$$\frac{(n-1)^2 + q(n+1-q)}{n^2} < \frac{E[F_{n+1}^2]}{E[F_n^2]} < \frac{(n-1)^2 + 3q(n-1) + q^2}{n^2},$$

so that

$$\frac{E[F_{n+1}^2]}{E[F_n^2]} \to 1 \quad \text{as } n \to \infty. \tag{2.15}$$

3. THE SEQUENCE $\{G_n\}$

In this section, we investigate the sequence $\{G_n\}$ described in the Introduction. We use the following notation for moments:

$E[X_n] = \mu_x, \quad E[Y_{n-1}] = \mu_y, \quad E[X_n^2] = \tau_x, \quad E[Y_{n-1}^2] = \tau_y, \quad E[X_n Y_{n-1}] = \mu_{xy},$

$\mathrm{var}[X_n] = \sigma_x^2, \quad \mathrm{var}[Y_{n-1}] = \sigma_y^2, \quad \mathrm{cov}[X_n, Y_{n-1}] = \sigma_{xy},$

$E[G_n] = \mu_n, \quad E[G_n^2] = \tau_n, \quad \mathrm{var}[G_n] = \sigma_n^2.$

Taking expectations in the defining relationship $G_{n+1} = X_n G_n + Y_{n-1} G_{n-1}$ and solving the resulting recurrence relationship yields:

Proposition 1

For the sequence $\{G_n\}$, we have

$$\mu_0 = g_0, \quad \mu_1 = g_1, \quad \mu_{n+1} = \mu_x\mu_n + \mu_y\mu_{n-1},$$

so that if k_1, k_2 are the zeros of $k^2 - \mu_x k - \mu_y$;

$$\mu_n = \begin{cases} \dfrac{(g_1 - k_1g_0)k_2^n - (g_1 - k_2g_0)^n}{k_2 - k_1}, & k_1 \neq k_2 \\[2ex] n\left(\dfrac{\mu_x}{2}\right)^{n-1} g_1 - (n - 1)\left(\dfrac{\mu_x}{2}\right)^n, & k_1 = k_2. \end{cases}$$

A direct expansion of the defining relationship gives

$$\tau_{n+1} = \tau_x\tau_n + 2\mu_{xy}E[G_nG_{n-1}] + \tau_y\tau_{n-1} \tag{3.1}$$

$$= \tau_x\tau_n + (2\mu_{xy}\mu_x + \tau_y)\tau_{n-1} + 2\mu_{xy}\mu_yE[G_{n-2}G_{n-1}]. \tag{3.2}$$

Replacing n by $n - 1$ in (3.1), then combining with (3.2) yields

$$\tau_{n+1} = A\tau_n + B\tau_{n-1} + C\tau_{n-2} \quad (n \geqslant 2), \tag{3.3}$$

where

$$A = \tau_x + \mu_y, \quad B = 2\mu_{xy}\mu_x + \tau_y - \tau_x\mu_y, \quad C = -\tau_y\mu_y. \tag{3.4}$$

Solving this recurrence relation gives

Theorem 3

If the zeros λ_1, λ_2, λ_3 of $\lambda^3 - A\lambda^2 - B\lambda - C$ are distinct, then

$$\tau_n = \sum_{i=1}^{3} \omega_i\lambda_i^n \quad (n > 2);$$

where

$$\omega_i = \left(\tau_2 - \left(\sum_{j \neq i} \lambda_j\right)\tau_1 + \left(\prod_{j \neq i} \lambda_j\right)\tau_0\right) \Big/ \prod_{j \neq i} (\lambda_j - \lambda_i), \tag{3.5}$$

$$\tau_0 = g_0^2, \quad \tau_1 = g_1^2, \quad \tau_2 = \tau_x g_1^2 + 2\mu_{xy}g_0g_1 + \tau_y g_0^2.$$

Example 1: If $g_0 = 0$, $g_1 = 1$, $\mu_x = \mu_y = \mu_{xy} = 1$, $\tau_x = \tau_y = 2$, then μ_n is the n^{th} Fibonacci number and

$$\tau_n = (-8(-1)^n + 7\sqrt{2}(2 + \sqrt{2})^n + 2(4 - \sqrt{2})(2 - \sqrt{2})^n)/28.$$

Example 2: If $g_0 = g_1 = 1$, $\mu_x = 0 = \mu_{xy}$, $\mu_y = 1$, $\sigma_x^2 = \sigma_y^2 = 1$, then $\mu_n = 1$ and

$$\tau_n = \left[\frac{2^{n+1} + 1}{3}\right] \quad \text{(greatest integer function).}$$

Deterministic Fibonacci-type sequences are sometimes used to model the growth of certain physical processes. In such applications, the coefficients of the defining recurrence relation might more properly be viewed as random variables—e.g., gestation periods of rabbits. The usefulness of such random models for predictive purposes, hence of the deterministic models as well, is cast into doubt by the next theorem. Note that in the examples above, the coefficients of variation σ_n/μ_n are unbounded. We shall show that this is quite generally the case.

First define matrices

$$M = \begin{bmatrix} A & B & C \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad N = \begin{bmatrix} D & E & F \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad P = M \oplus (M - N),$$

where A, B, C are as at (3.4), $D = \sigma_x^2$, $E = \sigma_y^2 - \sigma_x^2\mu_y + 2\sigma_{xy}\mu_x$, $F = -\sigma_y^2\mu_y$. Relation (3.3) becomes

$$(\tau_{n+1}, \tau_n, \tau_{n-1})' = M(\tau_n, \tau_{n-1}, \tau_{n-2})',$$

and a parallel development yields

$$(\mu_{n+1}^2, \mu_n^2, \mu_{n-1}^2)' = (M - N)(\mu_n^2, \mu_{n-1}^2, \mu_{n-2}^2)'.$$

Theorem 4

If the characteristic roots of P are real and distinct, then $\sigma_n/|\mu_n| \to \infty$ as $n \to \infty$.

Proof: It suffices to show that $\tau_n/\mu_n^2 \to \infty$. Put

$$\ell_n = \tau_n/\mu_n^2, \quad k_n = \mu_n^2/\mu_{n+1}^2, \quad r_n = \tau_n/\tau_{n-1}.$$

Note that $\ell_n \geqslant 1$, and that $\ell_n/\ell_{n-1} = r_n k_{n-1}$. We claim that r_n, k_n have nonnegative, finite limits r and k, and that $rk \neq 1$. Then $\ell_n/\ell_{n-1} \to rk$, so that $rk > 1$, else $\ell_n \to 0$. But then $\ell_n \to \infty$, completing the proof.

That r exists is clear from (3.5) and the assumption of the theorem, since the roots of P are those of M together with those of $M - N$. The roots of M, in turn, are the λ_i of Theorem 3. Thus, $r = \lambda_0$, where λ_0 is the root λ_i of largest absolute value, such that $\omega_i \neq 0$. Clearly, $r \geqslant 0$. Similarly, $k_n \to k = \nu_0^{-1} \geqslant 0$, where ν_0 is the root of $M - N$ with properties analogous to those of λ_0. Thus, $0 \leqslant rk = \lambda_0/\nu_0 \neq 1$. □

The assumption and conclusion of Theorem 4 fail if $\sigma_x^2 = \sigma_y^2 = 0$, i.e., if the sequence is deterministic. In this case, $N = 0$, $P = M \oplus M$, $\sigma_n/\{|\mu_n|\} \equiv 1$. We conjecture that $\{\sigma_n/|\mu_n|\}$ is bounded iff $\sigma_x^2 = \sigma_y^2 = 0$.

4. THE RANGES OF (p, q) AND $(p, q)'$ SEQUENCES

For a (p, q) or $(p, q)'$ sequence, any number which can be formed from $f_1, \ldots, f_p$ in the manner used to generate the sequence is, with positive probability, in the range of $\{F_n\}$. The following result is the natural counterpart to this observation.

Theorem 5

Let S be the range of a (p, q) or $(p, q)'$ sequence. If $n \notin \{f_1, \ldots, f_p\}$ and $P(F_{p+1} = n) < 1$, then $P(n \notin S) > 0$.

Proof: Assume that $q > 1$; the result is obvious otherwise. Assume also, w.l.o.g., that $|f_1| \geqslant |f_2| \geqslant \cdots \geqslant |f_p|$. Consider any sequence of the form

$$S_0 = \{f_1, \ldots, f_p, f_{p+1} = qf_1, \ldots, f_{p+k} = q^k f_1, f_{p+k+1}, f_{p+k+2}, \ldots\}$$

where $|f_{p+k+j}| > |n|$ for $j \geqslant 1$, and k is chosen so that $|f_{p+k-1}| < |n| < |f_{p+k}|$. If $|n| = q^\ell |f_1|$ for some integer ℓ, then omit $f_{p+\ell}$ from S_0. Let S_* be the set of all such sequences. We shall show that $P(S \in S_*) > 0$. Since no $S_0 \in S_*$ contains n, this will complete the proof.

Let S_j, $S_{0,j}$ be the initial j-element segments of S and S_0, respectively, and define E_j to be the event "$S_j = S_{0,j}$ for some $S_0 \in S_*$". The sequence $\{E_j\}$ is decreasing, and

$$P(S \in S_*) = P\left(\bigcap_{j=1}^{\infty} E_j\right) = \lim_{j\to\infty} P(E_j).$$

Clearly, $P(E_{p+k}) > 0$. For $\ell \geqslant 1$,

$$P(E_{p+k+\ell})/P(E_{p+k+\ell-1}) = P(E_{p+k+\ell}|E_{p+k+\ell-1}) \geqslant P$$

(at least one element from $\{f_{p+k}, \ldots, f_{p+k+\ell-1}\}$ is chosen in the formation of $f_{p+k+\ell}$). This last term cannot be less than

$$1 - \left(\frac{p+k-1}{p+k+\ell-1}\right)^q,$$

so that for $j \geqslant 1$,

$$P(E_{p+k+j}) \geqslant P(E_{p+k}) \prod_{\ell=1}^{j}\left(1 - \left(\frac{p+k-1}{p+k+\ell-1}\right)^q\right).$$

With $c = p + k - 1$, we then have

$$P(S \in S_*) \geqslant P(E_{p+k}) \prod_{\ell=1}^{\infty}\left(1 - \left(\frac{c}{c+\ell}\right)^q\right),$$

so that it remains only to show that the infinite product is positive. But this is equivalent to the convergence of the series

$$-\sum_{\ell=1}^{\infty} \log\left(1 - \left(\frac{c}{c+\ell}\right)^q\right),$$

whose terms are eventually dominated by those of

$$2\sum_{\ell=1}^{\infty}\left(\frac{c}{c+\ell}\right)^q \leqslant 2c^q \sum_{\ell=1}^{\infty} \ell^{-q} < \infty. \quad \square$$

5. OPEN PROBLEMS

1. Do any of the sequences considered here, properly normalized, have limiting distributions? If so, what are they? Monte Carlo simulations have indicated that the (p, q) sequence $\{F_n\}$, for $q > 1$, has a limiting log-normal distribution. This leads to the conjecture that, with $\mu_n = E[F_n]$ and $\tau_n = E[F_n^2]$,

$$\frac{\log F_n - \log \dfrac{\mu_n^2}{\sqrt{\tau_n}}}{\left(\log \dfrac{\tau_n}{\mu_n^2}\right)^{1/2}} \xrightarrow{L} N(0, 1).$$

Numerical investigations also lead to the conjecture that for such a sequence, $\tau_n = 0(n^{2q-2}(\log n)^{\alpha})$, where $\alpha(q) \in [0, 1]$ is an increasing function of q. Note that this holds for $q = 1$, with $\alpha(1) = 0$. These conjectures together imply that the coefficient of variation of F_n is $O((\log n)^{\alpha})$, while that of $\log F_n$ tends to zero.

2. A simple consequence of Theorem 5 is that any finite set N, no member of which is forced to be the $(p+1)^{\text{th}}$ element of a (p, q) or $(p, q)'$ sequence is, with positive probability, disjoint from the range of such a sequence. Is the same true of infinite sets? Preliminary investigations indicate that it is true for countable sets if, when the elements of such a set are arranged as an increasing sequence, the sequence diverges sufficiently quickly. Definitive results have yet to be obtained.

REFERENCES

1. R. K. Guy. "Problem E31." In *Unsolved Problems in Number Theory*. Berlin: Springer-Verlag, 1981.
2. C. C. Heyde. "On a Probabilistic Analogue of the Fibonacci Sequence." *J. Appl. Prob.* 17 (1980):1079-82.
3. V. E. Hoggatt, Jr., & M. Bicknell. "Generalized Fibonacci Polynomials and Zeckendorf's Theorem." *The Fibonacci Quarterly* 11, no. 5 (1973):399-428.
4. V. E. Hoggatt, Jr., & M. Bicknell-Johnson. "Lexicographic Ordering and Fibonacci Representations." *The Fibonacci Quarterly* 20, no. 3 (1982):193-218.

◆◇◆◇◆

EUCLID'S ALGORITHM AND THE FIBONACCI NUMBERS

P. W. EPASINGHE
University of Colombo, Colombo 3, Sri Lanka

(Submitted December 1983)

The number of steps in Euclid's algorithm for the natural number pair (a, b) with $a > b$ is discussed. If the number of steps is k, then the least possible value for a is F_{k+2}. If the number of steps exceeds k, then $a \geqslant F_{k+3}$. If the number of steps is k and $a = F_{k+2}$, then $b = F_{k+1}$. If $b = F_{k+1}$ and the number of steps is k, then $a = F_k + nF_{k+1}$ where n is any natural number. (F_k is the k^{th} Fibonacci number.)

Given two natural numbers a, b, Euclid's algorithm produces the greatest common divisor of a and b. The Fibonacci numbers are defined by the recurrence relation $F_{n+2} = F_{n+1} + F_n$ where n is a natural number, with $F_1 = F_2 = 1$. Various interesting properties of these numbers can be found in the literature. In the following, we shall demonstrate an extremal property of the Fibonacci numbers in relation to Euclid's algorithm.

If the n^{th} quotient and n^{th} remainder in Euclid's algorithm are q_n and r_n, respectively, and the algorithm consists of at least k steps, then the sequence of steps up to and including the k^{th} step can be written algebraically as follows:

$$\left.\begin{array}{l} r_{n-2} = q_n r_{n-1} + r_n, \quad n = 1, 2, 3, \ldots, k; \\ \text{where } r_{-1} = a, \quad r_0 = b. \end{array}\right\} \tag{1}$$

Further, all the quantities r_{n-2}, r_{n-1}, r_n, q_n are natural numbers except r_k, which may also be zero.

Therefore, given any two natural numbers a, b with $a > b$, there is a unique natural number $e(a, b)$ associated with them where $e(a, b)$ is the number of operations in Euclid's algorithm for the greatest common divisor of a and b. We have, for example, $e(a, 1) = 1$ for all natural numbers a (> 1).

Given any natural number k, it is possible to determine a pair of natural numbers a, b with $a > b$ such that $e(a, b) = k$. This is not obvious for all k, but will be seen in a little while to be true. As special cases—$e(2, 1) = 1$, $e(3, 2) = 2$, $e(5, 3) = 3$, and $e(8, 5) = 4$—and it can be shown that all these number pairs are consecutive Fibonacci numbers. As a generalization, it follows that

$$e(F_{k+2}, F_{k+1}) = k. \tag{2}$$

Given k, the number of pairs (a, b) such that $e(a, b) = k$ is nonfinite because, for all natural numbers n, $e(a + nb, b) = e(a, b)$. As a special consequence, we also have

$$e(F_{k+3}, F_{k+1}) = k. \tag{3}$$

It now follows that, given a natural number k,

$$\{a \mid e(a, b) = k \text{ for some natural number } b < a\}$$

is not bounded above, but being a subset of the set of natural numbers should have a least element. It is convenient to denote this least element by $e(k + 2)$

with $e(1) = e(2) = 1$. We will also call $e(k)$ the Euclid number of k. The main result that justifies the title of this note is:

"The Euclid number of the natural number k is the k^{th} Fibonacci number."

Before proving this result, we need an equation that we shall be using over and over again. We multiply the equation in (1) corresponding to each value of n by F_n and sum over all the values of n. This yields

$$\sum_{n=1}^{k} F_n r_{n-2} = \sum_{n=1}^{k} F_n r_{n-1} q_n + \sum_{n=1}^{k} F_n r_n.$$

$$\therefore\ F_1 a + F_2 b + \sum_{n=1}^{k-2} F_{n+2} r_n = bq_1 + \sum_{n=1}^{k-2} F_{n+1} r_n q_{n+1} + F_k r_{k-1} q_k$$
$$+ \sum_{n=1}^{k-2} F_n r_n + F_{k-1} r_{k-1} + F_k r_k \quad \text{if } k \geqslant 3.$$

That is,

$$a = b(q_1 - 1) + \sum_{n=1}^{k-2} F_{n+1} r_n (q_{n+1} - 1) + F_k r_{k-1} q_k + F_{k-1} r_{k-1} + F_k r_k,$$

where we have used the fact that $F_{n+2} = F_{n+1} + F_n$ when $n = 1, 2, \ldots, k-2$.

$$\therefore\ a - F_{k+1} = b(q_1 - 1) + \sum_{n=1}^{k-2} F_{n+1} r_n (q_{n+1} - 1)$$
$$+ F_k r_{k-1} q_k + F_{k-1}(r_{k-1} - 1) + F_k(r_k - 1);$$

$$\therefore\ a - F_{k+1} = b(q_1 - 1) + \sum_{n=1}^{k-1} F_{n+1} r_n (q_{n+1} - 1)$$
$$+ F_{k+1}(r_{k-1} - 1) + F_k r_k. \tag{4}$$

Equation (4) has been obtained only when $k \geqslant 3$. However, it is easily verified to be true even when $k = 2$.

Property 1

If the number of steps in Euclid's algorithm for the pair of natural numbers a, b, where $a > b$, is exactly k, then

$$a \geqslant F_{k+2}.$$

The case when $k = 1$ is trivial. When $k \geqslant 2$, we have $r_k = 0$ and $q_k \geqslant 2$. Also, $q_n \geqslant 1$, $n = 1, 2, \ldots, k-1$, and $r_n \geqslant 1$, $n = 1, 2, \ldots, k-1$. Hence, by equation (4),

$$a - F_{k+1} \geqslant F_k$$
$$\therefore\quad a \geqslant F_{k+2}.$$

Thus, the least value of a is $F_{k+2} = e(k+2)$. This proves the main result as stated earlier.

Property 2

If the number of steps in Euclid's algorithm for the pair of natural numbers a, b, where $a > b$, is greater than k, then $a \geqslant F_{k+3}$.

Here again, the case when $k = 1$ is trivial. When $k \geqslant 2$, we have $r_k \geqslant 1$ and $r_{k-1} \geqslant 2$. Also, $q_n \geqslant 1$, $n = 1, 2, \ldots, k$. Equation (4) now gives

$$a - F_{k+1} \geqslant F_{k+1} + F_k = F_{k+2}$$

$$\therefore \quad a \geqslant F_{k+1} + F_{k+2} = F_{k+3}.$$

Property 3

If the number of steps in Euclid's algorithm for the pair of natural numbers F_{k+2}, b, where $F_{k+2} > b$, is exactly k, then

$$b = F_{k+1}.$$

Here again, the case $k = 1$ is trivial. When $k \geqslant 2$, $a = F_{k+2}$, $r_k = 0$, and $q_k \geqslant 2$, whereas $q_n \geqslant 1$ and $r_n \geqslant 1$ when $n = 1, 2, \ldots, k - 1$. Equation (4) now gives

$$0 = b(q_1 - 1) + \sum_{n=1}^{k-2} F_{n+1} r_n (q_{n+1} - 1) + F_{k+1}(r_{k-1} - 1) + F_k[r_{k-1}(q_k - 1) - 1] \quad \text{if } k \geqslant 2,$$

with obvious modifications if $k = 1$. Since this is the sum of a number of terms, each of which is nonnegative, each term should be zero.

$$\therefore\ q_n = 1,\ n = 1, 2, \ldots, k - 1; \quad r_{k-1} = 1 \quad \text{and} \quad q_k = 2.$$

Equation set (1) now reduces to

$$\left.\begin{aligned} r_{n-2} &= r_{n-1} + r_n,\ n = 1, 2, \ldots, k - 1, \\ r_{k-2} &= 2, \\ F_{k+2} &= r_{-1}. \end{aligned}\right\} \tag{5}$$

This set of equations has a unique solution with

$$r_n = F_{k+1-n},\ n = -1, 0, 1, \ldots, k - 2.$$

In particular, $r_0 = F_{k+1}$.

Property 4

If the number of steps in Euclid's algorithm for the pair a, F_{k+1}, where $a > F_{k+1}$, is k, then $a = F_k + nF_{k+1}$, where n is any natural number.

Here, too, the case when $k = 1$ is trivial. When $k \geqslant 2$, we can use Eq. set (1) directly. Leaving the equation corresponding to $n = 1$ out for the moment, the other $k - 1$ equations would correspond to a $(k - 1)$-step Euclid algorithm for the number pair F_{k+1}, r_1, where $r_1 < F_{k+1}$.
By an application of Property 3, $r_1 = F_k$.

$$\therefore\ a = bq_1 + r_1 = F_k + q_1 F_{k+1}, \text{ where } q_1 \text{ is any natural number.}$$

This proves the result.

◆◇◆◇◆

LETTER FROM THE EDITOR

Dear Readers:

Recently, an expository Master's thesis was written by Mr. John Spraggon under the guidance of Professor A. F. Horadam on the mathematical research of V. E. Hoggatt, Jr.

The editor has read this thesis and considers it to be a very well written and extensive analysis of the works of our former editor.

Anyone interested in purchasing this thesis can do so by sending a request to:

INTER LIBRARY LOANS LIBRARIAN,
DIXSON LIBRARY
UNIVERSITY OF NEW ENGLAND,
ARMIDALE, N.S.W. 2351
AUSTRALIA

The title of Mr. Spraggon's thesis is "Special Aspects of Combinatorial Number Theory: Being As Exposition of the Mathematical Research of V. E. Hoggatt, Jr." M.A. (Hons), 1982, U.N.E.

Payment will be requested before the thesis is sent, and the cost, depending on the method of mail route chosen, is between $27.00 (Ordinary Mail) and $43.00 (Airmail).

Sincerely,

Gerald E. Bergum

ELEMENTARY PROBLEMS AND SOLUTIONS

Edited by
A. P. HILLMAN

Assistant Editors
GLORIA C. PADILLA and CHARLES R. WALL

Please send all communications regarding ELEMENTARY PROBLEMS AND SOLUTIONS to PROFESSOR A. P. HILLMAN; 709 SOLANO DR., S.E.; ALBUQUERQUE, NM 87108. Each problem or solution should be on a separate sheet (or sheets). Preference will be given to those typed with double spacing in the format used below. Proposed problems should be accompanied by their solutions. Solutions should be received within four months of the publication date.

DEFINITIONS

The Fibonacci numbers F_n and Lucas numbers L_n satisfy

$$F_{n+2} = F_{n+1} + F_n, \quad F_0 = 0, \quad F_1 = 1,$$

and

$$L_{n+2} = L_{n+1} + L_n, \quad L_0 = 2, \quad L_1 = 1.$$

PROBLEMS PROPOSED IN THIS ISSUE

B-544 *Proposed by Herta T. Freitag, Roanoke, VA*

Show that $F_{2n+1}^2 \equiv L_{2n+1}^2 \pmod{12}$ for all integers n.

B-545 Proposed by Herta T. Freitag, Roanoke, VA

Show that there exist integers a, b, and c such that

$$F_{4n} \equiv an \pmod{5} \quad \text{and} \quad F_{4n+2} \equiv bn + c \pmod{5}$$

for all integers n.

B-546 *Proposed by Stuart Anderson, East Texas State University, Commerce, TX and John Corvin, Amoco Research, Tulsa, OK*

For positive integers a, let S_a be the finite sequence $a_1, a_2, \ldots, a_n$ defined by

$$a_1 = a,$$
$$a_{i+1} = a_i/2 \text{ if } a_i \text{ is even}, \quad a_{i+1} = 1 + a_i \text{ if } a_i \text{ is odd},$$

the sequence terminates with the earliest term that equals 1.

For example, S_5 is the sequence 5, 6, 3, 4, 2, 1, of six terms. Let K_n be the number of positive integers a for which S_a consists of n terms. Does K_n equal something familiar?

B-547 *Proposed by Philip L. Mana, Albuquerque, NM*

For positive integers p and n with p prime, prove that

$$L_{np} \equiv L_n L_p \pmod{p}.$$

B-548 *Proposed by Valentina Bakinova, Rondout Valley, NY*

Let $D(n)$ be defined inductively for nonnegative integers n by $D(0) = 0$ and $D(n) = 1 + D(n - [\sqrt{n}]^2)$, where $[x]$ is the greatest integer in x. Let n_k be the smallest n with $D(n) = k$. Then

$$n_0 = 0, \quad n_1 = 1, \quad n_2 = 2, \quad n_3 = 3, \quad \text{and} \quad n_4 = 7.$$

Describe a recursive algorithm for obtaining n_k for $k \geqslant 3$.

B-549 *Proposed by George N. Philippou, Nicosia, Cyprus*

Let H_0, H_1, ... be defined by $H_0 = q - p$, $H_1 = p$, and $H_{n+2} = H_{n+1} + H_n$ for $n = 0, 1, \ldots$. Prove that, for $n \geqslant m \geqslant 0$,

$$H_{n+1}H_m - H_{m+1}H_n = (-1)^{m+1}[pH_{n-m+2} - qH_{n-m+1}].$$

SOLUTIONS

Coded Multiplication Modulo 10 or 12

B-520 *Proposed by Charles R. Wall, Trident Technical College, Charleston, SC*

(a) Suppose that one has a table for multiplication (mod 10) in which a, b, ..., j have been substituted for 0, 1, ..., 9 in some order. How many decodings of the substitution are possible?

(b) Answer the analogous question for a table of multiplication (mod 12).

Solution by the proposer.

(a) There are two ways to decode the substitution. The letters representing 0 and 1 are easy to find, since $x \cdot 0 = 0$ and $x \cdot 1 = x$ for all x; then 9 is easily found as the unique solution to $x^2 - 1$ with $x \neq 1$. The letter representing 5 is identifiable, and the letters are easily sorted as odd or even, because $5 \cdot x = 5$ if x is odd and $5 \cdot x = 0$ if x is even. Then 6 is identified from $6 \cdot x = x$ if x is even, and 4 is identified from $x^2 = 6$ with $x \neq 6$. Still unidentified are 2, 3, 7, and 8, but $2^2 = 8^2 = 4$ and $3^2 = 7^2 = 9$. so there are two choices for 3. Once 3 is chosen, 7 is forced, and so are 2 and 8, since $3 \cdot 4 = 2$ and $3 \cdot 6 = 8$.

(b) The substitution is unique. As in (a), 0 and 1 are easily identified. Then 6 is easily found, and the letters can be classified as odd or even, because $6 \cdot x = 6$ if x is odd and $6 \cdot x = 0$ if x is even. Now, 4 is the only nonzero even solution of $x^2 = x$. If x and y are both even, then $x \cdot y$ is 0, 4, or 8, and since 0 and 4 are already known, 8 is easily identified, leaving only 2 and 10 unknown among the even numbers. But $8 \cdot 2 = 4$ and $8 \cdot 10 = 8$, so 2 and 10 can be determined. Among the odd numbers, 9 is the only solution to $x^2 = x$ with $x \neq 1$, so 9 is easily identified. If x is odd, then $9 \cdot x$ is either 3 or 9, so 3 is determined. Then 7 is identified using the fact that $7 \cdot x = x$ if x is even. To identify 5 and 11, we use the fact that $3 \cdot 5 = 3$, while $3 \cdot 11 = 9$.

Also solved by Paul S. Bruckman and by L. Kuipers & P. A. J. Scheelbeek.

Unique Decoding

B-521 *Proposed by Charles R. Wall, Trident Technical College, Charleston, SC*

See the previous problem. Find all moduli $m > 1$ for which the multiplication (mod m) table can be decoded in only one way.

Solution by the proposer.

Suppose the multiplication (mod m) table can be decoded uniquely. Then it is easy to see that if $k|m$, the multiplication (mod k) table can also be decoded in only one way.

If $p \geqslant 5$ is prime, there are at least two distinct primitive roots (mod p), say g and h; replacing g^n by h^n for each n yields an equivalent substitution, so the multiplication (mod p) table cannot be decoded uniquely, and hence $p \nmid m$.

The multiplication (mod 9) table cannot be decoded uniquely, because 3 and 6 may be interchanged, and in the multiplication (mod 8) table, 2 and 6 may be switched.

Therefore, $m = 2^a 3^b$ with $a \leqslant 2$ and $b \leqslant 1$. Since the multiplication (mod 12) table can be decoded in only one way, $m = 2, 3, 4, 6$, or 12.

Also solved by Paul S. Bruckman and by L. Kiupers & P. A. J. Scheelbeek.

Alternating Even and Odd

B-522 *Proposed by Joan Tomescu, University of Bucharest, Romania*

Find the number $A(n)$ of sequences $(a_1, a_2, \ldots, a_k)$ of integers a_i satisfying $1 \leqslant a_i < a_{i+1} \leqslant n$ and $a_{i+1} - a_i \equiv 1 \pmod 2$ for $i = 1, 2, \ldots, k - 1$. [Here k is variable but, of course, $1 \leqslant k \leqslant n$. For example, the three allowable sequences for $n = 2$ are (1), (2), and $(1, 2)$.]

Solution by J. Suck, Essen, Germany

$$A(n) = F_{n+3} - 2.$$

Proof by Double Induction

Let $B(n)$ be the number of sequences of the said type with $a_k = n$. I claim that $B(n) = F_{n+1}$. This is so for $n = 1, 2$. Suppose it is true for $\nu = 1, \ldots, n - 1 \geqslant 1$. The sequences with $a_k = n$, except (n), consist of those with $a_{k-1} = n - 1$ or $n - 3$ or $n - 5 \ldots$. Thus

$$B(m) = 1 + F_n + F_{n-2} + \cdots + \begin{cases} F_2 & \text{for } n \text{ even} \\ F_3 & \text{for } n \text{ odd} \end{cases}$$

$$= F_{n+1} \text{ in any case by Hoggatt's } I_5 \text{ or } I_6.$$

Now, $A(1) = 1 = F_4 - 2$, and, clearly,

$$A(n) = A(n-1) + B(n) = F_{n+2} - 2 + F_{n+1} = F_{n+3} - 2 \quad \text{for } n > 1.$$

Also solved by Paul S. Bruckman, Laszlo Cseh, L. A. G. Dresel, Herta T. Freitag, L. Kuipers, J. Metzger, W. Moser, Sahib Singh, and the proposer.

Reversing Coefficients of a Polynomial

B-523 *Proposed by Laszlo Cseh and Imre Merenyi, Cluj, Romania*

Let p, a_0, a_1, ..., a_n be integers with p a positive prime such that

$$\gcd(a_0, p) = 1 = \gcd(a_n, p).$$

Prove that in $\{0, 1, \ldots, p-1\}$ there are as many solutions of the congruence

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$$

as there are of the congruence

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \equiv 0 \pmod{p}.$$

Solution by Sahib Singh, Clarion University of Pennsylvania, Clarion, PA

Since $\gcd(a_0, p) = \gcd(a_n, p) = 1$, it follows that both polynomials associated with the given congruences are of n^{th} degree and that zero is not a solution of any one of these congruences. If α is a solution of the first congruence, then α^{-1} is a solution of the second congruence where α^{-1} denotes the unique multiplicative inverse of α in Z_p.

Thus, we conclude that if $\alpha_1, \alpha_2, \ldots, \alpha_t$ are the solutions of the first congruence in Z_p, then $\alpha_1^{-1}, \alpha_2^{-1}, \ldots, \alpha_t^{-1}$ are precisely the solutions of the second congruence in Z_p.

Also solved by Paul S. Bruckman, L. A. G. Dresel, L. Kuipers, J. M. Metzger, Bob Prielipp, and the proposer.

Disguised Fibonacci Squares

B-524 *Proposed by Herta T. Freitag, Roanoke, VA*

Let

$$S_n = F_{2n-1}^2 + F_nF_{n-1}(F_{2n-1} + F_n^2) + 3F_nF_{n+1}(F_{2n-1} + F_nF_{n-1}).$$

Show that S_n is the square of a Fibonacci number.

Solution by Paul S. Bruckman, Fair Oaks, CA

Let $a = F_n$, $b = F_{n-1}$. Note that $F_{2n-1} = a^2 + b^2$, $F_{n+1} = a + b$. Then

$$\begin{aligned} S_n &= (a^2 + b^2)^2 + ab(a^2 + b^2 + a^2) + 3a(a + b)(a^2 + b^2 + ab) \\ &= a^4 + 2a^2b^2 + b^4 + 2a^3b + ab^3 + 3a^4 + 6a^3b + 6a^2b^2 + 3ab^3 \\ &= 4a^4 + 8a^3b + 8a^2b^2 + 4ab^3 + b^4 \\ &= (2a^2 + 2ab + b^2)^2. \end{aligned}$$

Now $2a^2 + 2ab + b^2 = a^2 + (a + b)^2 = F_n^2 + F_{n+1}^2 = F_{2n+1}$. Hence, $S_n = F_{2n+1}^2$.

Also solved by L. A. G. Dresel, L. Kuipers, Imre Merenyi, J. M. Metzger, Bob Prielipp, Sahib Singh, J. Suck, and the proposer.

Diophantine Equation

B-252 *Proposed by Walter Blumberg, Coral Springs, FL*

Let x, y, and z be positive integers such that $2^x - 1 = y^z$ and $x > 1$. Prove that $z = 1$.

Solution by Leonard A. G. Dresel, University of Reading, England

Since $x > 1$, we have $y^z = 2^x - 1 \equiv -1 \pmod 4$. Hence, $y \equiv -1 \pmod 4$ and z is odd, so that we have the identity

$$y^z + 1 = (y + 1)(y^{z-1} - y^{z-2} + \cdots - y + 1).$$

Hence, $y + 1$ divides $y^z + 1 = 2^x$, so that $y + 1 = 2^u$, $u \leqslant x$, and

$$\begin{aligned} 2^{x-u} &= y^{z-1} - y^{z-2} + \cdots - y + 1 \\ &\equiv 1 + 1 + \cdots + 1 + 1 \pmod 4 \\ &\equiv z \text{ (since there are } z \text{ terms)} \\ &\equiv 1 \text{ modulo 2, since } z \text{ is odd.} \end{aligned}$$

Therefore, we must have $x - u = 0$, and $y^z = y$, and since $y^z > 1$ it follows that $z = 1$.

Note by Paul S. Bruckman

This is apparently a well-known result, indicated by S. Ligh and L. Neal in "A Note on Mersenne Numbers," *Math. Magazine* 47, no. 4 (1974):231-33. The result indicated in that reference is that a Mersenne number cannot be a power (greater than one) of an integer.

Also solved by Paul S. Bruckman, Odoardo Brugia & Piero Filipponi, Laszlo Cseh, L. Kuipers, Imre Merenyi, J. M. Metzger, Bob Prielipp, E. Schmutz & H. Klauser, Sahib Singh, J. Suck, and the proposer.

◆◇◆◇◆

ADVANCED PROBLEMS AND SOLUTIONS

Edited by
RAYMOND E. WHITNEY

Please send all communucations 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-385 *Proposed by M. Wachtel, Zurich, Switzerland*

Solve the following system of equations:

I. $U^2_{f(n)} + V^2_{g(n)} - 3 \cdot U_{f(n)}V_{g(n)} = 1;$

II. $3 \cdot U_{h(n)}V_{i(n)} - (U^2_{h(n)} + V^2_{i(n)}) = 1.$

H-386 *Proposed by Paul S. Bruckman, Fair Oaks, CA*

Define the multiple-valued *Fibonacci function* ${}^mF : \mathbf{C} \to \mathbf{C}$ as follows:

1. $${}^mF(z) = \frac{1}{\sqrt{5}}(\exp Lz - \exp L'z), \quad z \in \mathbf{C},\ m \in \mathbb{Z},$$

where $L = \log \alpha$, $\alpha = \frac{1}{2}(1 + \sqrt{5})$, $L' = (2m + 1)i\pi - L$, and "log" denotes the principal logarithm.

a. Show that ${}^mF(n) = F_n$ for all integers m and n.

b. Prove the multiplication formula

2. $$\prod_{m=0}^{n-1} {}^mF\left(k + \frac{r}{n}\right) = 5^{-\frac{1}{2}(n-1)}F_{nk+r},$$ where n, k, r are integers with $0 < r < n$.

c. With m fixed, find the zeros of ${}^mF$.

H-387 *Proposed by Lawrence Somer, Washington, D.C.*

Let $\{w_n\}_{n=0}^{\infty}$ be a second-order linear integral recurrence defined by the recursion relation

$$w_{n+2} = aw_{n+1} + bw_n,$$

where $b \neq 0$. Show the following:

(i) If p is an odd prime such that $p \nmid b$ and $w_1^2 - w_0w_2$ is a quadratic nonresidue of p, then

$$p \nmid w_{2n} \quad \text{for any } n \geq 0.$$

(ii) If p is an odd prime such that $(-b)(w_1^2 - w_0w_2)$ is a quadratic nonresidue of p, then

$$p \nmid w_{2n+1} \quad \text{for any } n \geqslant 0.$$

(iii) If p is an odd prime such that $-b$ is a nonzero quadratic residue of and $w_1^2 - w_0w_2$ is a quadratic nonresidue of p, then

$$p \nmid w_n \quad \text{for any } n \geqslant 0.$$

H-388 *Proposed by Piero Filipponi, Rome, Italy*

This problem arose in the determination of the diameter of a class of locally restricted digraphs [1].

For a given integer $n \geqslant 2$, let $P_1 = \{p_{1,1}, p_{1,2}, \ldots, p_{1,k_1}\}$ be a nonempty (i.e., $k_1 \geqslant 1$) increasing sequence of positive integers such that $p_{1,k_1} \leqslant n - 1$. Let $P_2 = \{p_{2,1}, p_{2,2}, \ldots, p_{2,k_2}\}$ be the increasing sequence containing all nonzero distinct values given by $p_{1,i} + p_{1,j} \pmod n$ $(i, j = 1, 2, \ldots, k_1)$. In general let $P_h = \{p_{h,1}, p_{h,2}, \ldots, p_{h,k_h}\}$ be the increasing sequence containing all nonzero distinct values given by $p_{h-1,i} + p_{1,j} \pmod n$ $(i = 1, 2, \ldots, k_{n-1}, j = 1, 2, \ldots, k_1)$. Furthermore, let B_m $(m = 1, 2, \ldots)$ be the increasing sequence containing all values given by

$$\bigcup_{j=1}^{m} P_j.$$

Find, in terms of $n, p_{1,1}, \ldots, p_{1,k_1}$, the smallest integer t such that

$$B_t = \{1, 2, \ldots, n - 1\}.$$

Remark: The necessary and sufficient condition for t to exist (i.e., to be finite) is given in [1]:

$$\gcd(n, p_{1,1}, \ldots, p_{1,k_1}) = 1.$$

In such a case we have $1 \leqslant t \leqslant n - 1$. It is easily seen that

$$k_1 = 1 \Longleftrightarrow t = n - 1$$

$$k_1 = n - 1 \Longleftrightarrow t = 1;$$

furthermore, it can be conjectured that either $t = n - 1$ or $1 \leqslant t \leqslant [n/2]$.

Reference

1. P. Filipponi. "Digraphs and Circulant Matrices." *Ricerca Operativa*, no. 17 (1981):41-62.

An Example

$$\begin{aligned} n = 8 \quad & P_1 = \{3, 5\} & &\to B_1 = \{3, 5\} \\ & P_2 = \{2, 6\} & &\to B_2 = \{2, 3, 5, 6\} \\ & P_3 = \{1, 3, 5, 7\} & &\to B_3 = \{1, 2, 3, 5, 6, 7\} \\ & P_4 = \{2, 4, 6\} & &\to B_4 = \{1, 2, 3, 4, 5, 6, 7\}; \text{ hence, we have } t = 4. \end{aligned}$$

SOLUTIONS

A Note to Solutions of H-350, H-354 by Paul Bruckman

H-350

Although the published solution is apparently correct, it can be considerably simplified. In the course of solving H-372, it occurred to the solver that the same method of solution could have been applied to solve H-350 (but was not). As noted in the published solution, the given equation:

$$5y^2 - Ax^2 = 1 \quad (\text{where } A \equiv 5a^2 + 5a + 1) \tag{1}$$

has general solutions

$$x_n = \frac{u^{2n-1} - v^{2n-1}}{2\sqrt{A}}, \; y_n = \frac{u^{2n-1} + v^{2n-1}}{2\sqrt{5}}, \quad n = 1, 2, \ldots, \\ \text{where } u \equiv (2a+1)\sqrt{5} + 2\sqrt{A}, \quad v \equiv (2a+1)\sqrt{5} - 2\sqrt{A}. \tag{2}$$

Note $uv = 1$. From (2), we could easily have derived the following relations:

$$5y_n y_{n+1} - Ax_n x_{n+1} = B \equiv 40a^2 + 40a + 9; \tag{3}$$

$$x_{n+1}y_n - x_n y_{n+1} = 4(2a + 1). \tag{4}$$

Dividing (3) and (4) throughout by $y_n y_{n+1}$ would have yielded the following:

$$5 - Ar_n r_{n+1} = B/y_n y_{n+1}, \quad r_{n+1} - r_n = 4(2a + 1)/y_n y_{n+1},$$

or

$$5 - Ar_n r_{n+1} = \frac{B}{4(2a + 1)}(r_{n+1} - r_n),$$

which yields:

$$r_{n+1} = \frac{Br_n + 20(2a + 1)}{4A(2a + 1)r_n + B}, \text{ with } r_1 = 2/(2a + 1). \tag{5}$$

The expression given by (5) is a recursion of the first order (though modular rather than linear), which is considerably simpler than the cumbersome third-order recursion published as the solution. The published third-order recursion follows from (5) (after some computation), but not vice-versa.

H-354

The published "solution" is not a solution (or even an attempted solution) of the original problem, as submitted. The original problem asked for necessary and sufficient conditions for a solution in integers (x, y) to exist for the equation:

$$ax^2 - by^2 = c, \tag{1}$$

where a, b, c are pairwise relatively prime positive integers such that ab is not a perfect square. It is already known that if a solution of (1) exists, then infinitely many such solutions exist. Moreover, an explicit formula for all such solutions is known, in terms of the one known solution (if any).

In the published "solution" to the problem, as *altered*, Wächtel changed the notation to the following equation,

$$By^2 - Ax^2 = C, \tag{2}$$

which in itself is not a substantive modification; however, he also indicated that C is to be *dependent* on A and B. Nothing of the sort was intended by the proposer; in the original problem, a, b, and c are *independently arbitrary*, subject only to the conditions noted above. Moreover, Wächtel attempted *construction* of the solutions to particular cases. This again was not the intent of the proposer, although admittedly the construction of the *minimal* solution, if possible, would go a long way toward solving the problem.

The only progress made by the proposer toward solution of the original problem may be summarized as follows:

I. *Necessary* conditions for a solution of (1) to exist are the following, in terms of the generalized Legendre symbols:

$$\left(\frac{ac}{b}\right) = \left(\frac{-bc}{a}\right) = \left(\frac{ab}{c}\right) = 1. \tag{3}$$

That the conditions in (3) are not sufficient may be demonstrated from the counter-example: $a = 1$, $b = 17$, $c = 2$, in this case, $x^2 - 17y^2 = 2$ has no solution, yet the conditions in (3) are satisfied.

II. The *construction* of a minimal solution to (1) seems to depend somehow on the simple continued fraction expansion of $\sqrt{b/a}$ (or equivalently, of $\sqrt{a/b}$). It is however *false*, in general, that for any solution (x, y) of (1), x/y is a convergent of the simple continued fraction expansion for $\sqrt{b/a}$. Nevertheless, a finite algorithm exists for finding the minimal solution (x_0, y_0), if any, of (1). By solving the congruence

$$-by^2 \equiv c \pmod{a} \tag{4}$$

implied by (3), and also using the inequality

$$0 < y_0 < \sqrt{cu_1/2b}, \tag{5}$$

where (u_1, v_1) is the minimal *nontrivial* solution of the auxiliary equation

$$u^2 - abv^2 = 1, \tag{6}$$

[the trivial one is $(u_0, v_0) = (1, 0)$], we may determine in a finite number of trials if a solution exists. It would be far more desirable, however, to construct such a minimal solution of (1) *directly*, rather than by trial and error.

III. Given that (x_0, y_0) is the minimal solution of (1), and (u_n, v_n) the solutions of the auxiliary equation in (6) (which latter solutions are known to exist in all cases, and for which several constructive algorithms are known), then *all* solutions of (1) are given by:

$$x_n = x_0u_n + by_0v_n, \quad y_n = y_0u_n + ax_0v_n, \quad n \in \mathbb{Z}. \tag{7}$$

Note that the solutions (u_n, v_n) of (6) are given by:

$$u_n = \frac{1}{2}(p^n + q^n), \quad v_n = \frac{1}{2\sqrt{ab}}(p^n - q^n), \quad n \in \mathbb{Z}, \tag{8}$$

where

$$p = u_1 + v_1\sqrt{ab}, \quad q = u_1 - v_1\sqrt{ab}. \tag{9}$$

IV. We note that $u_{-n} = u_n$, $v_{-n} = -v_n$ for all $n \in \mathbb{Z}$. From this it may be deduced that $x_n > 0$ for all n, while y_n has the same sign as n. This eliminates trivial variations in solutions due to sign, and makes the theory more elegant.

* * *

Correction to H-382

The left-hand side of (3) should read F_{n+2}, and the left-hand side of (4) should read F_{n+2}.

Correction to H-381

Equation (ii) should read

$$\text{(ii)} \qquad \beta(2m-1) = \sum_{i=1}^{m-1} \frac{(-)^{i+1}u^{2i}}{2^{2i}(2i)!}\beta(2m-2i-1), \quad m \geqslant 2.$$

Ring around the Lucas!

H-362 *Proposed by Stanley Rabinowitz, Merrimack, NH*
(Vol. 21, no. 4, November 1983)

Let Z_n be the ring of integers modulo n. A *Lucas number* in this ring is a member of the sequence $\{L_k\}$, $k = 0, 1, 2, \ldots$, where

$$L_0 = 2,\ L_1 = 1, \text{ and } L_{k+2} \equiv L_{k+1} + L_k \quad \text{for } k \geqslant 0.$$

Prove that for $n > 14$, all members of Z_n are Lucas numbers if and only if n is a power of 3.

Remark: A similar, but more complicated, result is known for Fibonacci numbers. See [1]. I do not have a proof of the above proposal, but I suspect a proof similar to the result in [1] is possible; however, it should be considerably simpler because there is only one case to consider rather than seven cases.

To verify the conjecture, I ran a computer program that examined Z_n for all n between 2 and 10,000 and found that the only cases where all members of Z_n were Lucas numbers were powers of 3 and the exceptional values $n = 2, 4, 6, 7$, and 14 (the same exceptions found in [1]). This is strong evidence for the truth of the conjecture.

Reference

1. S. A. Burr. "On Moduli for Which the Fibonacci Sequence Contains a Complete System of Residues." *The Fibonacci Quarterly* 9, no. 5 (1971):497.

Solution by Paul S. Bruckman, Fair Oaks, CA

We generalize and modify the definition of *defectiveness* indicated in [1]. Given a positive integer n, let $R_n = \{0, 1, 2, \ldots, n-1\}$ denote a complete residue class (mod n), and consider the (periodic) sequence

$$(L_r \pmod n)_{r=0}^{\infty} = (L_r')_{r=0}^{\infty}$$

with elements in R_n. Let $k = k(n)$ denote the period of this sequence. We say n is *Lucas-defective* if $R_n \not\subset \{L_0', L_1', L_2', \ldots, L_k'\}$, i.e., if there exists $j \in R_n$ such that $L_i \not\equiv j \pmod n$ for all $i \geqslant 0$. Let LD denote the set of all Lucas-defective numbers. A comparable definition using Fibonacci numbers instead of Lucas numbers may be made, with FD denoting the comparable set of *Fibonacci-defective* numbers; these were simply called *defective* numbers in Burr's paper [1]. Let LD^* and FD^* denote the complements of LD and FD, respectively, with respect to $\mathbb{N} = \{1, 2, 3, \ldots\}$, i.e.,

$$LD^* = \mathbb{N} - LD, \quad FD^* = \mathbb{N} - FD.$$

We recall the main result of Burr:

Theorem 1

FD^* consists of the following numbers:

$$5^u, \quad 2 \cdot 5^u, \quad 4 \cdot 5^u, \quad 6 \cdot 5^u, \quad 7 \cdot 5^u, \quad 14 \cdot 5^u, \quad 3^v \cdot 5^u, \quad u \geqslant 0, \quad v \geqslant 1.$$

We will establish Rabinowitz' conjecture, namely:

Theorem 2

LD^* consists of the following numbers:

$$1, 2, 4, 6, 7, 14, 3^v, \quad v \geqslant 1.$$

Note that 1 is (trivially) LD^*, as well as FD^*, although Rabinowitz did not specifically mention this. We will require some preliminary lemmas.

Lemma 1

If $n \in LD$, then $kn \in LD$ for all $k \in \mathbb{N}$.

Proof of Lemma 1: Since $n \in LD$, there exists an integer $j \in R$ such that $L_i \not\equiv j \pmod{n}$ for all $i \geqslant 0$. Therefore, $L_i \not\equiv j \pmod{kn}$ for all $k \in \mathbb{N}$ and for all $i \geqslant 0$. Hence, $kn \in LD$ for all $k \in \mathbb{N}$.

Lemma 2

(a) $1, 2, 4, 6, 7, 14 \in LD^*$;

(b) $5 \in LD$.

Proof of Lemma 2: This follows from a simple, but trite, tabulation of the residues of the sequences $(L_r \pmod{n}))_{r=0}^{k-1}$ for the various stated values of n, leading to the indicated results by inspection.

Note that Lemma 1 and Lemma 2(b) imply that no multiple of 5 can be in LD^*.

Lemma 3

$LD^* \subset FD^*$.

Proof of Lemma 3: Suppose $n \in LD^*$. Then there exists $j \in R_n$ such that $L_j \equiv 0 \pmod{n}$. Since $\gcd(L_j, L_{j+1}) = 1$, we have $\gcd(n, L_{j+1}) = 1$; hence, $L_{j+1}^{-1} \pmod{n}$ exists. Define the sequence $\theta_r \equiv L_{j+1}^{-1} \cdot L_r \pmod{n}$, $r = 0, 1, 2, \ldots$. Note that the θ_r's are equal to a constant integer $(L_{j+1}^{-1} \pmod{n})$ times the L_r's $\pmod{n}$, and therefore satisfy the basic Fibonacci recursion. Moreover, $\theta_j \equiv 0$, $\theta_{j+1} \equiv 1 \pmod{n}$, which are the initial values of the standard Fibonacci sequence. Hence, $(\theta_r)_{r=0}^{\infty}$ is the Fibonacci sequence $\pmod{n}$, except in a cyclically permuted order. Since $n \in LD^*$, the sequence of L_r's contains R_n in some order. Since $\gcd(L_{j+1}^{-1} \pmod{n}, n) = 1$, we see that multiplying the elements of R_n throughout by $L_{j+1}^{-1} \pmod{n}$ regenerates R_n in some permuted order. Hence, $(F_r \pmod{n}))_{r=0}^{\infty}$ contains R_n, i.e., $n \in FD^*$. Thus, $LD^* \subset FD^*$. Combining the results of Lemmas 1, 2, and 3, we see that LD^* consists of all the numbers in

FD^* (as stated in Theorem 1), *except* all multiples of 5, and *possibly* further excepting powers of 3. It therefore suffices to prove one more result, namely:

Lemma 4

$3^v \in LD^*, \quad v \in \mathbb{N}.$

Proof of Lemma 4: Given $v \in \mathbb{N}$, let $m = 3^{v-1}$. We indicate the main result of [3] below:

$$\alpha^{3m} \equiv \beta^m, \quad \beta^{3m} \equiv \alpha^m \pmod{3m}. \tag{*}$$

This is an instance of an identity in the "calculus of complex residues" explained in [3], whereby we may manipulate the quantities $\alpha \equiv \frac{1}{2}(1 + \sqrt{5})$ and $\beta = \frac{1}{2}(1 - \sqrt{5}) \pmod{3m}$ as we would ordinarily manipulate complex numbers; in this case, however, the object $\sqrt{5}$ (rather than $\sqrt{-1}$) is "imaginary," since 5 is a quadratic nonresidue of $3m$. Note that (*) implies $\alpha^{2m} \equiv -\beta^{2m} \pmod{3m}$, i.e., $L_{2m} \equiv 0 \pmod{3m}$. Also, we have

$$\alpha^{2m+1} \equiv \beta^{2m-1}, \quad \beta^{2m+1} \equiv \alpha^{2m-1} \pmod{3m},$$

which implies $F_{2m+1} \equiv -F_{2m-1} \pmod{3m}$. Therefore, $F_{2m+1} \equiv F_{2m} - F_{2m+1} \pmod{3m}$, or

$$F_{2m} \equiv 2F_{2m+1} \pmod{3m}. \tag{**}$$

Since $\gcd(F_r, F_{r+1}) = 1$ for all r, we must therefore have $\gcd(F_{2m}, 3m) = 1$; hence, $F_{2m}^{-1} \pmod{3m}$ exists. The rest of the proof is similar to that of Lemma 3. Define the sequence $\Psi_r \equiv 2F_{2m}^{-1}F_r \pmod{3m}$, $r = 0, 1, 2, \ldots$. Then the Ψ_r's satisfy the Fibonacci recursion. Moreover, $\Psi_{2m} \equiv 2$ and $\Psi_{2m+1} \equiv 1 \pmod{3m}$, using (**); these are the initial values of the Lucas sequence. Thus, $(\Psi_r)_{r=0}^{\infty}$ is the Lucas sequence $\pmod{3m}$, except in a cyclically permuted order. From Theorem 1, $3m \in FD^*$; hence, the sequence $(F_r \pmod{3m}))_{r=0}^{\infty}$ contains R_{3m} in some permuted order. Since $\gcd(2F_{2m}^{-1} \pmod{3m}, 3m) = 1$, multiplying the elements of R_{3m} throughout by $2F_{2m}^{-1} \pmod{3m}$ regenerates R_{3m} in some permuted order; hence, $3m \in LD^*$. Q.E.D.

This completes the proof of Theorem 2 (Rabinowitz' Conjecture).

References

1. S. A. Burr. "On Moduli for Which the Fibonacci Sequence Contains a Complete System of Residues." *The Fibonacci Quarterly* 9, no. 5 (1971):497-504.
2. A. P. Shah. "Fibonacci Sequence Modulo m." *The Fibonacci Quarterly* 6, no. 2 (1968):139-41.
3. P. S. Bruckman. "Some Divisibility Properties of Generalized Fibonacci Sequences." *The Fibonacci Quarterly* 17, no. 1 (1979):42-49.

Also solved by L. Somer.

◆◇◆◇◆

SUSTAINING MEMBERS

*A.L. Alder
S. Ando
*J. Arkin
B.I. Arthur, Jr.
L. Bankoff
C.A. Barefoot
Frank Bell
M. Berg
J.G. Bergart
G. Bergum
G. Berzsenyi
*M. Bicknell-Johnson
C. Bridger
Br. A. Brousseau
J.L. Brown, Jr.
P.S. Bruckman
P.F. Byrd
G.D. Chakerian
J.W. Creely
P.A. DeCaux
M.J. DeLeon
J. Desmond
H. Diehl
J.L. Ercolano
D.R. Farmer
F.F. Frey, Jr.
C.L. Gardner
A.A. Gioia
R.M. Giuli
I.J. Good
*H.W. Gould
W.E. Greig
H.E. Heatherly
A.P. Hillman
*A.F. Horadam
F.T. Howard
R.J. Howell
R.P. Kelisky
C.H. Kimberling
J. Lahr
*C.T. Long
*J. Maxwell
L. Miller
M.G. Monzingo
S.D. Moore, Jr.
K. Nagasaka
F.J. Ossiander
S. Rabinowitz
E.M. Restrepo
E.D. Robinson
S.E. Schloth
J.A. Schumaker
H.G. Simms
J. Sjoberg
L. Somer
M.N.S. Swamy
L. Taylor
*D. Thoro
R. Vogel
C.C. Volpe
M. Waddill
*L.A. Walker
J.E. Walton
G. Weekly
R.E. Whitney
B.E. Williams

*Charter Members

INSTITUTIONAL MEMBERS

THE BAKER STORE EQUIPMENT COMPANY
Cleveland, Ohio

CALIFORNIA STATE UNIVERSITY, SACRAMENTO
Sacramento, California

GENERAL BOOK BINDING COMPANY
Chesterland, Ohio

PRINCETON UNIVERSITY
Princeton, New Jersey

SAN JOSE STATE UNIVERSITY
San Jose, California

SCIENTIFIC ENGINEERING INSTRUMENTS, INC.
Sparks, Nevada

TRI STATE UNIVERSITY
Angola, Indiana

UNIVERSITY OF CALIFORNIA, SANTA CRUZ
Santa Cruz, California

UNIVERSITY OF GEORGIA
Athens, Georgia

UNIVERSITY OF REDLANDS
Redlands, California

UNIVERSITY OF SANTA CLARA
Santa Clara, California

UNIVERSITY OF TORONTO
Toronto, Canada

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 Majorie Bicknell and Verner E. Hoggatt, Jr. FA, 1972.

Fibonacci's Problem Book. Edited by Majorie Bicknell and Verner E. Hoggatt, Jr. FA, 1974.

The Theory of Simply Periodic Numerical Functions by Edouard Lucas. Translated from the French by Sidney Kravitz. Edited by Douglas Lind. FA, 1969.

Linear Recursion and Fibonacci Sequences by Brother Alfred Brousseau. FA, 1971.

Fibonacci and Related Number Theoretic Tables. Edited by Brother Alfred Brousseau. FA, 1972.

Number Theory Tables. Edited by Brother Alfred Brousseau. FA, 1973.

Recurring Sequences by Dov Jarden. Third and enlarged edition. Riveon Lematematika, Israel, 1973.

Tables of Fibonacci Entry Points, Part One. Edited and annotated by Brother Alfred Brousseau. FA, 1965.

Tables of Fibonacci Entry Points, Part Two. Edited and annotated by Brother Alfred Brousseau. FA, 1965.

A Collection of Manuscripts Related to the Fibonacci Sequence — 18th Anniversary Volume. Edited by Verner E. Hoggatt, Jr. and Marjorie Bicknell-Johnson. FA, 1980.