The Fibonacci Quarterly

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

TABLE OF CONTENTS

VOLUME 27 MAY 1989 NUMBER 2

PURPOSE

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

EDITORIAL POLICY

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

SUBMITTING AN ARTICLE

Articles should be submitted in the format of the current issues of the **THE FIBONACCI QUARTERLY.** They should be typewritten or reproduced typewritten copies, that are clearly readable, double spaced with wide margins and on only one side of the paper. The full name and address of the author must appear at the beginning of the paper directly under the title. Illustrations should be carefully drawn in India ink on separate sheets of bond paper or vellum, approximately twice the size they are to appear in print.

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

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

SUBSCRIPTIONS, ADDRESS CHANGE, AND REPRINT INFORMATION

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

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

Annual domestic Fibonacci Association membership dues, which include a subscription to **THE FIBONACCI QUARTERLY**, are $30 for Regular Membership, $40 for Sustain Membership, and $67 for Institutional Membership; foreign rates, which are based on international mailing rates, are somewhat higher than domestic rates; please write for details. **THE FIBONACCI QUARTERLY** is published each February, May, August and November.

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

The Fibonacci Quarterly

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

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

ON TRIANGULAR FIBONACCI NUMBERS

Luo Ming
Chongqing Teachers' College, China
(Submitted February 1987)

1. Introduction and Results

Vern Hoggatt (see [1]) conjectured that 1, 3, 21, 55 are the only triangular numbers [i.e., positive integers of the form $\frac{1}{2}m(m+1)$] in the Fibonacci sequence

$$u_{n+2} = u_{n+1} + u_n,\ u_0 = 0,\ u_1 = 1,$$

where n ranges over all integers, positive or negative. In this paper, we solve Hoggatt's problem completely and obtain the following results.

Theorem 1: $8u_n + 1$ is a perfect square if and only if $n = \pm 1, 0, 2, 4, 8, 10$.

Theorem 2: The Fibonacci number u_n is triangular if and only if $n = \pm 1, 2, 4, 8, 10$.

The latter theorem verifies the conjecture of Hoggatt.

The method of the proofs is as follows. Since u_n is a triangular number if and only if $8u_n + 1$ is a perfect square greater than 1, it is sufficient to find all n's such that $8u_n + 1$ is square. To do this, we shall find, for each nonsquare $8u_n + 1$, an integer w_n such that the Jacobi symbol

$$\left(\frac{8u_n + 1}{w_n}\right) = -1.$$

Using elementary congruences we can show that, if $8u_n + 1$ is square, then

$$n \equiv \pm 1 \pmod{2^5 \cdot 5} \text{ if } n \text{ is odd, and}$$

$$n \equiv 0, 2, 4, 8, 10 \pmod{2^5 \cdot 5^2 \cdot 11} \text{ if } n \text{ is even.}$$

We develop a special Jacobi symbol criterion with which we can further show that each congruence class above contains exactly one value of n such that $8u_n + 1$ is a perfect square, i.e., $n = \pm 1, 0, 2, 4, 8, 10$, respectively.

2. Preliminaries

It is well known that the Lucas sequence

$$v_{n+2} = v_{n+1} + v_n,\ v_0 = 2,\ v_1 = 1,$$

where n denotes an integer, is closely related to the Fibonacci sequence, and that the following formulas hold (see [2]):

$$u_{-n} = (-1)^{n+1}u_n,\ v_{-n} = (-1)^n v_n; \tag{1}$$

$$2u_{m+n} = u_m v_n + u_n v_m,\ 2v_{m+n} = 5u_m u_n + v_m v_n; \tag{2}$$

$$u_{2n} = u_n v_n,\ v_{2n} = v_n^2 + 2(-1)^{n+1}; \tag{3}$$

$$v_n^2 - 5u_n^2 = 4(-1)^n; \tag{4}$$

$$u_{2kt+n} \equiv (-1)^t u_n \pmod{v_k}; \tag{5}$$

where n, m, t denote integers and $k \equiv \pm 2 \pmod 6$.

Moreover, since $x = \pm u_n$, $y = \pm v_n$ are the complete set of solutions of the Diophantine equations $5x^2 - y^2 = \pm 4$, the condition $u_n = \frac{1}{2}m(m+1)$ is equivalent to finding all integer solutions of the two Diophantine equations

$$5m^2(m+1)^2 - 4y^2 = \pm 16,$$

i.e., finding all integer points on these two elliptic curves. These problems are also solved in this paper.

3. A Jacobi Symbol Criterion and Its Consequences

In the first place we establish a Jacobi symbol criterion that plays a key role in this paper and then give some of its consequences.

Criterion: If a, n are positive integers such that $n \equiv \pm 2 \pmod 6$, $(a, v_n) = 1$, then

$$\left(\frac{\pm 4au_{2n} + 1}{v_{2n}}\right) = -\left(\frac{8au_n \pm v_n}{64a^2 + 5}\right)$$

whenever the right Jacobi symbol is proper.

Proof: Since $n \equiv \pm 2 \pmod 6$ implies $v_n \equiv 3 \pmod 4$ and $2n \equiv \pm 4 \pmod{12}$ implies $v_{2n} \equiv 7 \pmod 8$, we have

$$\left(\frac{\pm 4au_{2n} + 1}{v_{2n}}\right) = \left(\frac{\pm 8au_{2n} + 2}{v_{2n}}\right) = \left(\frac{\pm 8au_n v_n + v_n^2}{v_{2n}}\right) \quad \text{by (3)}$$

$$= \left(\frac{v_{2n}}{8au_n v_n \pm v_n^2}\right) \quad \text{since } a,\ n > 0 \text{ imply } 8au_n \pm v_n > 0$$

$$= \left(\frac{v_{2n}}{v_n}\right)\left(\frac{v_{2n}}{8au_n \pm v_n}\right) = \left(\frac{-2}{v_n}\right)\left(\frac{\frac{1}{2}(5u_n^2 + v_n^2)}{8au_n \pm v_n}\right) \quad \text{by (2)}$$

$$= -\left(\frac{2}{v_n}\right)\left(\frac{a}{8au_n \pm v_n}\right)\left(\frac{40au_n^2 + 8av_n^2}{8au_n \pm v_n}\right) = -\left(\frac{2}{v_n}\right)\left(\frac{a}{8au_n \pm v_n}\right)\left(\frac{\lambda(64a^2 + 5)u_n v_n}{8au_n \pm v_n}\right)$$

$$= \pm\left(\frac{2}{v_n}\right)\left(\frac{a}{8au_n \pm v_n}\right)\left(\frac{8au_n \pm v_n}{64a^2 + 5}\right)\left(\frac{u_n v_n}{8au_n \pm v_n}\right).$$

If $u_n \equiv 1 \pmod 4$, then

$$\left(\frac{u_n}{8au_n \pm v_n}\right) = \left(\frac{8au_n \pm v_n}{u_n}\right) = \left(\frac{v_n}{u_n}\right) = \left(\frac{u_n}{v_n}\right);$$

If $u_n \equiv 3 \pmod 4$, then

$$\left(\frac{u_n}{8au_n \pm v_n}\right) = \mp\left(\frac{8au_n \pm v_n}{u_n}\right) = -\left(\frac{v_n}{u_n}\right) = \left(\frac{u_n}{v_n}\right).$$

Hence, we always have $\left(\frac{u_n}{8au_n \pm v_n}\right) = \left(\frac{u_n}{v_n}\right)$.

Since $\left(\frac{v_n}{8au_n \pm v_n}\right) = \mp\left(\frac{8au_n \pm v_n}{v_n}\right) = \lambda\left(\frac{2a}{v_n}\right)\left(\frac{u_n}{v_n}\right)$, we get

$$\left(\frac{\pm 4au_{2n}+1}{v_{2n}}\right) = -\left(\frac{a}{v_n}\right)\left(\frac{a}{8au_n \pm v_n}\right)\left(\frac{8au_n \pm v_n}{64a^2+5}\right) = -\left(\frac{a}{8au_{2n} \pm v_n^2}\right)\left(\frac{8au_n \pm v_n}{64a^2+5}\right).$$

Moreover, put $a = 2^s b$, $s \geq 0$, $2 \nmid b$. If $b \equiv 1 \pmod 4$, then

$$\left(\frac{a}{8au_{2n} \pm v_n^2}\right) = \left(\frac{b}{8au_{2n} \pm v_n^2}\right) = \left(\frac{8au_{2n} \pm v_n^2}{b}\right) = 1;$$

If $b \equiv 3 \pmod 4$, then

$$\left(\frac{a}{8au_{2n} \pm v_n^2}\right) = \left(\frac{b}{8au_{2n} \pm v_n^2}\right) = \pm\left(\frac{8au_{2n} \pm v_n^2}{b}\right) = 1,$$

the same as above, so we finally obtain

$$\left(\frac{\pm 4au_{2n}+1}{v_{2n}}\right) = -\left(\frac{8au_n \pm v_n}{64a^2+5}\right).$$

The proof is complete. □

Now we derive some consequences of this criterion.

Lemma 1: If $n \equiv \pm 1 \pmod{2^5 \cdot 5}$, then $8u_n + 1$ is a square only for $n = \pm 1$.

Proof: We first consider the case $n \equiv 1 \pmod{2^5 \cdot 5}$. If $n \neq 1$, put

$$n = \delta(n-1) \cdot 3^r \cdot 2 \cdot 5m + 1,$$

where $\delta(n-1)$ denotes the sign of $n - 1$, and $r \geq 0$, $3 \nmid m$, then $m > 0$ and $m \equiv \pm 16 \pmod{48}$. We shall carry out the proof in two cases depending on the congruence class of $\delta(n-1) \cdot 3^r \pmod 4$.

Case 1: $\delta(n-1) \cdot 3^r \equiv 1 \pmod 4$. Let $k = 5m$ if $m \equiv 16 \pmod{48}$ or $k = m$ if $m \equiv 32 \pmod{48}$, then we always have $k \equiv 32 \pmod{48}$. Using (5) and (2), we obtain

$$8u_n + 1 \equiv 8u_{2k+1} + 1 \equiv 4(u_{2k} + v_{2k}) + 1 \equiv 4u_{2k} + 1 \pmod{v_{2k}}.$$

Using the Criterion, we get (evidently the conditions are satisfied)

$$\left(\frac{8u_n + 1}{v_{2k}}\right) = \left(\frac{4u_{2k}+1}{v_{2k}}\right) = -\left(\frac{8u_k + v_k}{69}\right)$$

Take modulo 69 to $\{8u_n + v_n\}$, the sequence of the residues has period 48, and $k \equiv 32 \pmod{48}$ implies $8u_k + v_k \equiv 38 \pmod{69}$, then we get

$$\left(\frac{8u_n + 1}{v_k}\right) = -\left(\frac{38}{69}\right) = -1$$

so that $8u_n + 1$ is not a square in this case.

Case 2: $\delta(n-1) \cdot 3^r \equiv 3 \pmod 4$. In this case, let $k = m$ if $m \equiv 16 \pmod{48}$ or $k = 5m$ if $m \equiv 32 \pmod{48}$ so that $k \equiv 16 \pmod{48}$ always. Similarly, by (5), (2), and the Criterion, we have

$$\left(\frac{8u_n + 1}{v_{2k}}\right) = \left(\frac{-4u_{2k}+1}{v_{2k}}\right) = -\left(\frac{8u_k - v_k}{69}\right).$$

Since the sequence of residues of $\{8u_n - v_n\}$ (mod 69) has period 48 and $k \equiv 16 \pmod{48}$ implies $8u_k - v_k \equiv 31 \pmod{69}$, we get

$$\left(\frac{8u_n + 1}{v_{2k}}\right) = -\left(\frac{31}{69}\right) = -1.$$

Hence $8u_n + 1$ is also not a square in this case.

Secondly, if $n \equiv -1 \pmod{2^5 \cdot 5}$ and $n \neq -1$, by (1) we can write

$$8u_n + 1 = 8u_{-n} + 1.$$

Since $-n \equiv 1 \pmod{2^5 \cdot 5}$ and $-n \neq 1$, it cannot possibly be a square according to the argument above.

Finally, when $n = \pm 1$, both give $8u_n + 1 = 3^2$, which completes the proof. □

In the remainder of this section we suppose that n is even. Note that if n is negative and even, then $8u_n + 1$ is negative, so it cannot be a square; hence, we may assume that $n \geq 0$.

Lemma 2: If $n \equiv 0 \pmod{2^2 \cdot 5^2}$, then $8u_n + 1$ is a square only for $n = 0$.

Proof: If $n > 0$, put $n = 2 \cdot 5^2 \cdot 2^s \cdot \ell$, $2 \nmid \ell$, $s \geq 1$, and let

$$k = \begin{cases} 2^s & \text{if } s \equiv 0 \pmod{3}, \\ 5^2 \cdot 2^s & \text{if } s \equiv 1 \pmod{3}, \\ 5 \cdot 2^s & \text{if } s \equiv 2 \pmod{3}, \end{cases}$$

then $k \equiv \pm 6 \pmod{14}$. Since $(2, v_k) = 1$, $k \equiv \pm 2 \pmod{6}$, by (5) and the Criterion we get

$$\left(\frac{8u_n + 1}{v_{2k}}\right) = \left(\frac{\pm 8u_{2k} + 1}{v_{2k}}\right) = -\left(\frac{16u_k \pm v_k}{9 \cdot 29}\right) = -\left(\frac{16u_k \pm v_k}{29}\right).$$

[It is easy to check that $(16u_n \pm v_n, 3) = 1$ for any even n.]

Simple calculations show that both of the residue sequences $\{16u_n \pm v_n\}$ modulo 29 have period 14. If $k \equiv 6 \pmod{14}$, then

$$16u_k + v_k \equiv 1 \pmod{29},\quad 16u_k - v_k \equiv -6 \pmod{29};$$

if $k \equiv -6 \pmod{14}$, then

$$16u_k + v_k \equiv 6 \pmod{29},\quad 16u_k - v_k \equiv -1 \pmod{29}.$$

Since $(\pm 1/29) = (\pm 6/29) = 1$, we obtain

$$\left(\frac{8u_n + 1}{v_{2k}}\right) = -1,$$

so that $8u_n + 1$ is not a square.

The case $n = 0$ gives $8u_n + 1 = 1^2$, which completes the proof. □

Lemma 3: If $n \equiv 2 \pmod{2^5 \cdot 5^2}$, then $8u + 1$ is a square only for $n = 2$.

Proof: If $n > 2$, put $n = 3^r \cdot 2 \cdot 5^2 \cdot \ell + 2$, $3 \nmid \ell$, $\ell > 0$, then $\ell \equiv \pm 16 \pmod{48}$. Let $k = \ell$ or 5ℓ or $5^2\ell$, which will be determined later. Since $4 \mid k$ implies $(3, v_k) = 1$, and clearly $k \equiv \pm 2 \pmod{6}$, we obtain, using (5), (2), and the Criterion

$$\left(\frac{8u_n + 1}{v_{2k}}\right) = \left(\frac{\pm 8u_{2k+2} + 1}{v_{2k}}\right) = \left(\frac{\pm 12u_{2k} + 1}{v_{2k}}\right) = -\left(\frac{24u_k \pm v_k}{581}\right).$$

Taking $\{24u_n \pm v_n\}$ modulo 581, we obtain two residue sequences with the same period 336 and having the following table:

n (mod 336)	80	112	128	208	224	256
$24u_n + v_n$ (mod 581)	65	401	436	359	261	170
$24u_n - v_n$ (mod 581)	411	320	222	145	180	516

It is easy to check that

$$\left(\frac{24u_n \pm v_n}{581}\right) = 1$$

for all six of these residue classes n (mod 336).

Since $336 = 48 \cdot 7$, we see that $\ell \equiv \pm 16 \pmod{48}$ are equivalent to $\ell \equiv 16$, 32, 64, 80, 112, 128, 160, 176, 208, 224, 256, 272, 304, 320 (mod 336). We choose k as follows:

$$k = \begin{cases} \ell & \text{if } \ell \equiv 80,\ 112,\ 128,\ 208,\ 224,\ 256 \pmod{336} \\ 5\ell & \text{if } \ell \equiv 16,\ 160,\ 176,\ 320 \pmod{336} \\ 5^2\ell & \text{if } \ell \equiv 32,\ 64,\ 272,\ 304 \pmod{336}. \end{cases}$$

With this choice k must be congruent to one of 80, 112, 128, 208, 224, and 256 modulo 336. Thus, we get

$$\left(\frac{8u_n + 1}{v_{2k}}\right) = -\left(\frac{24u_k \pm v_k}{581}\right) = -1,$$

so that $8u_n + 1$ is not a square.

Finally, the case $n = 2$ gives $8u_n + 1 = 3^2$. The proof is complete. □

Lemma 4: If $n \equiv 4 \pmod{2^5}$, then $8u_n + 1$ is a square only for $n = 4$.

Proof: If $n > 4$, we put $n = 2 \cdot 3^r \cdot k + 4$, $3 \nmid k$, then $k \equiv \pm 16 \pmod{48}$. According to (5), we have

$$8u_n + 1 \equiv -8u_4 + 1 \equiv -23 \pmod{v_k}.$$

Simple calculations show that the sequence of residues $\{v_k\}$ modulo 23 has period 48 and that $k \equiv \pm 16 \pmod{48}$ implies that $v_k \equiv -1 \pmod{23}$. Hence,

$$\left(\frac{8u_n + 1}{v_k}\right) = \left(\frac{-23}{v_k}\right) = \left(\frac{v_k}{23}\right) = \left(\frac{-1}{23}\right) = -1,$$

so that $8u_n + 1$ is not a square in this case.

When $n = 4$, $8u_n + 1 = 5^2$. The proof is complete. □

Lemma 5: If $n \equiv 8 \pmod{2^5 \cdot 5}$, then $8u_n + 1$ is a square only for $n = 8$.

Proof: If $n > 8$, we put $n = 2 \cdot 3^r \cdot 5\ell + 8$, $3 \nmid \ell$, then $\ell \equiv \pm 16 \pmod{48}$. Let $k = \ell$ or 5ℓ, which will be determined later. For both cases, we have, by (5),

$$8u_n + 1 \equiv -8u_8 + 1 \equiv -167 \pmod{v_k}.$$

The sequence $\{v_n\}$ modulo 167 is periodic with period 336, and the following table holds.

n (mod 336)	±32	±64	±80	±112	±160
v_n (mod 167)	125	91	17	166	120

It is easy to verify that all values in the second row are quadratic nonresidues modulo 167. Let A denote the set consisting of the residue classes in the first row. We now choose k such that its residue modulo 336 is in A.

The condition $\ell \equiv \pm 16 \pmod{48}$ is equivalent to $\ell \equiv 16, 32, 64, 80, 112, 128, 160, 176, 208, 224, 256, 272, 304, 320 \pmod{336}$, and all of these residue classes, except four classes, are in A. For these classes, we let $k = \ell$. The four exceptions are $\ell \equiv 16, 128, 208, 320 \pmod{336}$, for which we choose $k = 5\ell$ so that $k \equiv 80, -32, 32, -80 \pmod{336}$, respectively, which are also in A. Thus, for every choice of k, v_k is a quadratic nonresidue modulo 167. Hence,

$$\left(\frac{8u_n + 1}{v_k}\right) = \left(\frac{-167}{v_k}\right) = \left(\frac{v_k}{167}\right) = -1,$$

and $8u_n + 1$ is not a square.

Finally, for $n = 8$, $8u_n + 1 = 13^2$, which completes the proof. □

Lemma 6: If $n \equiv 10 \pmod{2^2 \cdot 5 \cdot 11}$, then $8u_n + 1$ is a square only for $n = 10$.

Proof: In the first place, by taking $\{v_n\}$ modulo 439 we get a sequence of residues with period 438 and having the following table:

$n \pmod{438}$	2	8	16	44	56	64	94	178	230	256	296	302	332	356	376
$v_n \pmod{439}$	3	47	12	306	54	407	395	24	79	101	394	202	184	135	74

Let B denote the set consisting of all fifteen residue classes modulo 438 in the first row. Simple calculations show that, for each n in B, v_n is a quadratic nonresidue modulo 439.

Now suppose that $8u_n + 1$ is a square. If $n > 10$, put $n = 2 \cdot \ell \cdot 5 \cdot 11 \cdot 2^t + 10$, $2 \nmid \ell$, $t \geq 1$. The sequence $\{2^t\}$ modulo 438 is periodic with period 18 with respect to t and we obtain the following table:

$t \pmod{18}$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$2^t \pmod{438}$	$\underline{2}$	4	$\underline{8}$	$\underline{16}$	32	$\underline{64}$	128	$\underline{256}$	74	148	$\underline{296}$	154	308	$\underline{178}$	$\underline{356}$	274	110	220
$5 \cdot 2^t \pmod{438}$										$\underline{302}$		$\underline{332}$				$\underline{56}$		
$11 \cdot 2^t \pmod{438}$		$\underline{44}$					$\underline{94}$		$\underline{376}$									$\underline{230}$
$5 \cdot 11 \cdot 2^t \pmod{438}$					$\underline{8}$								$\underline{296}$				$\underline{356}$	

where the underlined residue classes modulo 438 are in B. If we take k as follows:

$$k = \begin{cases} 2^t & \text{if } t \equiv 1, 3, 4, 6, 8, 11, 14, 15 \pmod{18} \\ 5 \cdot 2^t & \text{if } t \equiv 10, 12, 16 \pmod{18} \\ 11 \cdot 2^t & \text{if } t \equiv 0, 2, 7, 9 \pmod{18} \\ 5 \cdot 11 \cdot 2^t & \text{if } t \equiv 5, 13, 17 \pmod{18}, \end{cases}$$

then the residue of k modulo 438 is in B, that is, v_k is a quadratic nonresidue modulo 439. Thus, by (5), we get

$$8u_n + 1 \equiv -8u_{10} + 1 \equiv -439 \pmod{v_k},$$

and

$$\left(\frac{8u_n + 1}{v_k}\right) = \left(\frac{-439}{v_k}\right) = \left(\frac{v_k}{439}\right) = -1,$$

so $8u_n + 1$ is not a square. In the remaining case $n = 10$, we have $8u_n + 1 = 21^2$. The proof is complete. □

Lemmas 2 to 6 immediately imply the following result:

Corollary 1: Assume that $n \equiv 0, 2, 4, 8, 10 \pmod{2^5 \cdot 5^2 \cdot 11}$, then $8u_n + 1$ is a square only for $n = 0, 2, 4, 8, 10$. □

4. Some Lemmas Obtained by Congruent Calculations

The lemmas in this section provide a system of necessary conditions for $8u_n + 1$ to be a square. We prove them mainly by the following process of calculation: First we study $\{8u_n + 1\}$ modulo a_1. We get a sequence with period k_1 (with respect to n), in which we eliminate every residue class modulo k_1 of n for which $8u_n + 1$ is a quadratic nonresidue modulo a_1. Next we study $\{8u_n + 1\}$ modulo a_2, and get a sequence with period k_2. For our purpose, a_2 will be chosen in such a way so that $k_1 | k_2$. Then we eliminate every residue class modulo k_2 of n from those left in the preceding step, for which $8u_n + 1$ is a quadratic nonresidue modulo a_2. We repeat this procedure until we reach the desired results.

Remark: Most of the a_i will be chosen to be prime and the calculations may then be carried out directly from the recurrence relation

$$8u_{n+2} + 1 = (8u_{n+1} + 1) + (8u_n + 1) - 1.$$

Lemma 7: If $8u_n + 1$ is a square, then $n \equiv \pm 1, 0, 2, 4, 8, 10 \pmod{2^5 \cdot 5}$.

Proof:

(i) Modulo 11. The sequence of residues of $\{8u_n + 1\}$ has period 10. We can eliminate $n \equiv 3, 5, 6, 7 \pmod{10}$ since they imply, respectively,

$$8u_n + 1 \equiv 6, 8, 10, 6 \pmod{11},$$

all of which are quadratic nonresidues modulo 11, so there remain $n \equiv \pm 1, 0, 2, 4, 8 \pmod{10}$.

For brevity, we shall omit the sentences about periods in what follows since they can be inferred from the other information given, e.g., mod 10 in the above step.

(ii) Modulo 5. Eliminate $n \equiv 9, 11, 12, 14, 18 \pmod{20}$, which imply

$$8u_n + 1 \equiv \pm 2 \pmod 5,$$

which are quadratic nonresidues modulo 5, so there remain $n \equiv \pm 1, 0, 2, 4, 8, 10 \pmod{20}$.

(iii) Modulo 3. Eliminate $n \equiv 3, 5, 6 \pmod 8$, which imply

$$8u_n + 1 \equiv 2 \pmod 3,$$

which is a quadratic nonresidue modulo 3, so eliminate $n \equiv 19, 21, 22, 30 \pmod{40}$ and there remain $n \equiv \pm 1, 0, 2, 4, 8, 10, 20, 24, 28 \pmod{40}$.

(iv) Modulo 2161. Eliminate $n \equiv 28, 39, 41, 42, 44, 60, 68 \pmod{80}$ since they imply, respectively,

$$8u_n + 1 \equiv 1153, 2154, 2154, 2154, 2138, 2067, 1010 \pmod{2161},$$

which are quadratic nonresidues modulo 2161, so there remain $n \equiv \pm 1, 0, 2, 4, 8, 10, 20, 24, 40, 48, 50, 64 \pmod{80}$.

(v) Modulo 3041. Eliminate $n \equiv 24, 40, 50, 64, 79, 81, 82, 84, 88, 90, 100, 104, 120, 128 \pmod{160}$ since they imply, respectively,

$$8u_n + 1 \equiv -57, 2590, 2613, 1815, -7, -7, -7, -23, 2874, 2602, 619, 59, 447, 1500 \pmod{3041},$$

which are quadratic nonresidues modulo 3041.

Modulo 1601. Eliminate $n \equiv 130, 144 \pmod{160}$ since they imply, respectively,

$$8u_n + 1 \equiv 639, 110 \pmod{1601},$$

which are quadratic nonresidues modulo 1601.

Hence, there remain $n \equiv \pm 1, 0, 2, 4, 8, 10, 20, 48, 80 \pmod{160}$.

(vi) Modulo 2207. Eliminate $n \equiv 48, 80, 208, 240 \pmod{320}$ since they imply

$$8u_n + 1 \equiv 933 \text{ or } 1276 \pmod{2207},$$

both of which are quadratic nonresidues modulo 2207, so eliminate $n \equiv 48$ and $80 \pmod{160}$ and there remain $n \equiv \pm 1, 0, 2, 4, 8, 10, 20 \pmod{160}$.

(vii) Now we eliminate $n \equiv 20 \pmod{160}$ by the following calculation. Put $n = 160m + 20$, since $80 \equiv 2 \pmod 6$; by (5), $u_{160m+20} \equiv \pm u_{20} \pmod{v_{80}}$, where the sign + or - depends on whether m is even or odd. Using (3) and (4), we get

$$\left(\frac{8u_{20} + 1}{v_{80}}\right) = \left(\frac{v_{80}}{8u_{20} + 1}\right) = \left(\frac{(v_{20}^2 - 2)^2 - 2}{8u_{20} + 1}\right) = \left(\frac{(5u_{20}^2 + 2)^2 - 2}{8u_{20} + 1}\right)$$

$$= \left(\frac{(5 \cdot (8u_{20})^2 + 2 \cdot 8^2)^2 - 2 \cdot 8^4}{8u_{20} + 1}\right)$$

$$= \left(\frac{(5 + 2 \cdot 8^2)^2 - 2 \cdot 8^4}{8u_{20} + 1}\right) = \left(\frac{9497}{8u_{20} + 1}\right) = \left(\frac{9497}{54121}\right) = -1.$$

Similarly,

$$\left(\frac{-8u_{20} + 1}{v_{80}}\right) = \left(\frac{v_{80}}{8u_{20} - 1}\right) = \left(\frac{9497}{8u_{20} - 1}\right) = \left(\frac{9497}{54119}\right) = -1.$$

Hence $8u_n + 1$ must not be a square when $n \equiv 20 \pmod{160}$, and, finally, there remain $n \equiv \pm 1, 0, 2, 4, 8, 10 \pmod{160}$. This completes the proof. □

In the following two lemmas, we suppose that n is even.

Lemma 8: If n is even and $8u_n + 1$ is a square, then we have $n \equiv 0, 2, 4, 8, 10 \pmod{2^2 \cdot 5^2}$.

Proof: We begin from the second step of the proof of Lemma 7. Note that since n is even, there remain $n \equiv 0, 2, 4, 8, 10 \pmod{20}$.

(i) Modulo 101. Eliminate $n \equiv 12, 18, 20, 24, 32, 38, 40, 42, 44, 48 \pmod{50}$ since they imply, respectively,

$$8u_n + 1 \equiv 42, 69, 86, 73, 34, 61, 66, 35, 38, 94 \pmod{101},$$

which are quadratic nonresidues modulo 101.

Modulo 151. Eliminate $n \equiv 22, 28, 34 \pmod{50}$ since they imply, respectively,

$$8u_n + 1 \equiv 51, 102, 108 \pmod{151},$$

which are quadratic nonresidues modulo 151.

Hence, there remain $n \equiv 0, 2, 4, 8, 10, 30, 50, 60, 64, 80 \pmod{100}$.

(ii) Modulo 3001. Eliminate $n \equiv 60$ and $80 \pmod{100}$ since they imply, respectively,

$$8u_n + 1 \equiv 2562 \text{ and } 2900 \pmod{3001},$$

both of which are quadratic nonresidues modulo 3001.

Modulo 25. Eliminate $n \equiv 64 \pmod{100}$ since it implies

$$8u_n + 1 \equiv 10 \pmod{25},$$

which is a quadratic nonresidue modulo 25.
Hence, there remain $n \equiv 0, 2, 4, 8, 10, 30, 50 \pmod{100}$.

(iii) Modulo 401. Eliminate $n \equiv 30, 50, 130, 150 \pmod{200}$ since they imply, respectively,

$$8u_n + 1 \equiv 122, 165, 281, 238 \pmod{401},$$

which are quadratic nonresidues modulo 401. Hence, at last, there remain $n \equiv 0, 2, 4, 8, 10 \pmod{100}$, which completes the proof. □

Lemma 9: If n is even and $8u_n + 1$ is a square, then we have $n \equiv 0, 2, 4, 8, 10 \pmod{2^2 \cdot 5 \cdot 11}$.

Proof:

(i) Modulo 199. Eliminate $n \equiv 16, 18, 20 \pmod{22}$ since they imply, respectively,

$$8u_n + 1 \equiv 136, 176, 192 \pmod{199},$$

which are quadratic nonresidues modulo 199. There remain $n \equiv 0, 2, 4, 6, 8, 10, 12, 14 \pmod{22}$.

(ii) Modulo 89. Eliminate $n \equiv 6, 24, 26, 28, 32, 34 \pmod{44}$ since they imply, respectively,

$$8u_n + 1 \equiv 65, 82, 66, 26, 6, 6 \pmod{89},$$

which are quadratic nonresidues modulo 89, so there remain $n \equiv 0, 2, 4, 8, 10, 12, 14, 22, 30, 36 \pmod{44}$.

(iii) In the first two steps of the proof of Lemma 7 we have shown that it is necessary for $n \equiv 0, 2, 4, 8, 10 \pmod{20}$, so that there further remain $n \equiv 0, 2, 4, 8, 10, 22, 30, 44, 48, 80, 88, 90, 100, 102, 110, 124, 140, 142, 144, 168, 180, 184, 188, 190 \pmod{220}$.

(iv) Modulo 661. Eliminate $n \equiv 44, 48, 124, 144, 180, 184 \pmod{220}$ since they imply, respectively,

$$8u_n + 1 \equiv 544, 214, 290, 447, 379, 546 \pmod{661},$$

which are quadratic nonresidues modulo 661.
Modulo 331. Eliminate $n \equiv 30, 58, 88, 102 \pmod{110}$ since they imply, respectively,

$$8u_n + 1 \equiv 242, 231, 312, 164 \pmod{331},$$

which are quadratic nonresidues modulo 331. Thus, we can eliminate $n \equiv 30, 88, 102, 140, 168 \pmod{220}$.
Modulo 474541. Eliminate $n \equiv 80, 90, 142, 188 \pmod{220}$ since they imply, respectively,

$$8u_n + 1 \equiv 12747, 54121, 131546, 131546 \pmod{474541},$$

which are quadratic nonresidues modulo 474541.
Hence there remain $n \equiv 0, 2, 4, 8, 10, 22, 100, 110, 190 \pmod{220}$.

(v) Modulo 307. Eliminate $n \equiv 14, 22, 58, 66 \pmod{88}$ since they imply, respectively,

$$8u_n + 1 \equiv 254, 162, 55, 147 \pmod{307},$$

which are quadratic nonresidues modulo 307. These are equivalent to $n \equiv 14$, 22 (mod 44), so that we can eliminate $n \equiv 22$, 110, 190 (mod 220) from those left in the foregoing step and then there remain $n \equiv 0$, 2, 4, 8, 10, 100 (mod 220).

(vi) Modulo 881. Eliminate $n \equiv 12$, 56, 100, 144 (mod 176) since they imply, respectively,

$$8u_n + 1 \equiv 272,\ 293,\ 611,\ 590 \pmod{881},$$

which are quadratic nonresidues modulo 881. These are equivalent to $n \equiv 12$ (mod 44), so that we can eliminate $n \equiv 100$ (mod 220).

Finally, there remain $n \equiv 0$, 2, 4, 8, 10 (mod 220). This completes the proof. □

From Lemmas 7 to 9, we can derive the following corollary.

Corollary 2: If n is even, and if $8u_n + 1$ is a square, then $n \equiv 0$, 2, 4, 8, 10 (mod $2^5 \cdot 5^2 \cdot 11$).

Proof: Suppose that $8u_n + 1$ is a square, n is even. According to Lemmas 7 to 9, n must satisfy the following congruences simultaneously:

$$\begin{cases} n \equiv c_1 & \pmod{2^5 \cdot 5} \\ n \equiv c_2 & \pmod{2^2 \cdot 5^2} \\ n \equiv c_3 & \pmod{2^2 \cdot 5 \cdot 11} \end{cases} \qquad c_1, c_2, c_3 \in \{0, 2, 4, 8, 10\}.$$

Because the greatest common divisor of the three modulos is 20 and the absolute value of the difference of any two numbers in $\{0, 2, 4, 8, 10\}$ cannot exceed 10, we conclude that $c_1 = c_2 = c_3$. Moreover, since the least common multiple of the three modulos is $2^5 \cdot 5^2 \cdot 11$, we finally obtain $n \equiv 0$, 2, 4, 8, 10 (mod $2^5 \cdot 5^2 \cdot 11$). The proof is complete. □

5. Proofs of Theorems

Now we give the proofs of the theorems in Section 1.

Proof of Theorem 1: Suppose $8u_n + 1$ is a square, the conclusion follows from Lemma 7 and Lemma 1 when n is odd, and from Corollary 2 and Corollary 1 when n is even. □

Proof of Theorem 2: The proof follows immediately from Theorem 1, by excluding $u_0 = 0$, since a triangular number is positive.

In fact,

$$u_{\pm 1} = u_2 = 1 \cdot 2/2,\ u_4 = 2 \cdot 3/2,\ u_8 = 6 \cdot 7/2,\ u_{10} = 10 \cdot 11/2. \ \square$$

Finally, we give two corollaries as the Diophantine equation interpretations of Theorem 2.

Corollary 3: The Diophantine equation

$$5x^2(x + 1)^2 - 4y^2 = 16 \tag{6}$$

has only the integer solutions $(x, y) = (-2, \pm 1)$, $(1, \pm 1)$.

Proof: According to (4) and the explanation at the end of Section 2, equation (6) implies $\frac{1}{2}x(x + 1) = u_n$ and n is odd, thus it follows from Theorem 2 that $\frac{1}{2}x(x + 1) = 1$, which gives $x = -2$ or 1. □

Corollary 4: The Diophantine equation

$$5x^2(x + 1)^2 - 4y^2 = -16 \tag{7}$$

has only the integer solutions $(x, y) = (-1, \pm 2)$, $(0, \pm 2)$, $(-2, \pm 3)$, $(1, \pm 3)$, $(-3, \pm 7)$, $(2, \pm 7)$, $(-7, \pm 47)$, $(6, \pm 47)$, $(-11, \pm 123)$, and $(10, \pm 123)$.

Proof: With the same reason as in Corollary 3, equation (7) implies $\frac{1}{2}x(x + 1) = u_n$ and n is even, so $\frac{1}{2}x(x + 1) = 0, 1, 3, 21$, or 55 by Theorem 2 (adding $u_0 = 0$). Thus, we get $x = -1, 0, -2, 1, -3, 2, -7, 6, -11, 10$, which give all integer solutions of equation (7). □

Acknowledgment

The author wishes to thank Professor Sun Qi for his great encouragement.

References

1. R. K. Guy. *Unsolved Problems in Number Theory*. New York: Springer-Verlag, 1981, p. 106.
2. J. H. E. Cohn. "On Square Fibonacci Numbers." *J. London Math. Soc.* 39 (1964):537-541.

*****

A GENERALIZATION OF FERMAT'S LITTLE THEOREM

Frank S. Gillespie
Southwest Missouri State University, Springfield, MO 65804
(Submitted February 1987)

A rational number r is said to be divisible by a prime number p provided the numerator of r is divisible by p. Here it is assumed that all rational numbers are written in standard form. That is, the numerators and denominators are relatively prime integers and the denominators are positive.

Certain sequences $\{u_n\}_{n=1}^{\infty}$ of rational numbers have the property that if p is any prime number, then $u_p \equiv u_1 \pmod{p}$. A sequence $\{u_n\}_{n=1}^{\infty}$ having this property is said to be a *Fermat sequence* or to possess the *Fermat property*.

The obvious example of a sequence that has the Fermat property is $\{a^n\}_{n=1}^{\infty}$ with a being an integer. Indeed Fermat's Little Theorem states that if a is any integer and if p is a prime number, then $a^p \equiv a \pmod{p}$.

There are sequences $\{u_n\}_{n=1}^{\infty}$ that have the Fermat property other than $\{a^n\}_{n=1}^{\infty}$. An example of a sequence that has the Fermat property for odd primes is the sequence $\{T_n(x)\}_{n=1}^{\infty}$ where x is an integer and $T_n(x)$ is a Tchebycheff polynomial of the first kind.

It is the purpose of this paper to give a class of sequences (of rational numbers) all having the Fermat property. The following theorem is related to Newton's formulas. Let

$$f(x) = x^k + A_1x^{k-1} + \cdots + A_{k-1}x + A_k$$

be a polynomial with real or complex coefficients. The sequence $\{u_n\}_{n=1}^{\infty}$ is defined in the following way: The first k terms of the sequence are given by Newton's formulas, namely,

$$\begin{aligned} &u_1 + A_1 = 0, \\ &u_2 + A_1u_1 + 2A_2 = 0, \\ &u_3 + A_1u_2 + A_2u_1 + 3A_3 = 0, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &u_k + A_1u_{k-1} + A_2u_{k-2} + \cdots + A_{k-1}u_1 + kA_k = 0. \end{aligned} \tag{1}$$

After the initial k terms are given, the rest of the terms are generated by the difference equation

$$u_n + A_1u_{n-1} + A_2u_{n-2} + \cdots + A_ku_{n-k} = 0, \tag{2}$$

for $n \geq k + 1$, which is formed from the polynomial $f(x)$. It is well known that the sequence $\{u_n\}_{n=1}^{\infty}$ given above is the sequence of the sum of the powers of the roots of $f(x)$. Thus, if

$$f(x) = (x - x_1)(x - x_2) \ldots (x - x_k),$$

then

$$u_n = x_1^n + x_2^n + \cdots + x_k^n, \text{ for } n = 1, 2, 3, \ldots .$$

In this paper it is supposed that $x_1x_2 \ldots x_k \neq 0$. See [6], pages 260-262.

The Corollary to Theorem 1 solves the difference equation defined by (1) and (2) with appropriate adjustments in the way $f(x)$ is factored.

Theorem 1: Let $c_1, c_2, \ldots, c_k$ and $x_1, x_2, \ldots, x_k$ be any real or complex numbers. Let

$$\prod_{i=1}^{k}(1 + x_i x)^{c_i} = 1 + \sum_{i=1}^{\infty} A_i x^i. \tag{3}$$

Then

$$c_1 x_1^n + c_2 x_2^n + \cdots + c_k x_k^n \tag{4}$$

$$= \frac{n \sum_{j_1=0}^{n-1} (-1)^{j_1} \sum_{j_2=0}^{j_1} \binom{n - j_1}{j_2} A_1^{n-j_1-j_2} \sum_{j_3=0}^{j_2} \binom{j_2}{j_3} A_2^{j_2-j_3} \cdots}{n - j_1}$$

$$\frac{\sum_{j_{n-1}=0}^{j_{n-2}} \binom{j_{n-2}}{j_{n-1}} A_{n-2}^{j_{n-2}-j_{n-1}} \binom{j_{n-1}}{j_1 - j_2 - \cdots - j_{n-1}} A_{n-1}^{j_{n-1} - (j_1 - j_2 - \cdots - j_{n-1})} A_n^{j_1 - j_2 - \cdots - j_{n-1}}}{},$$

where n is a natural number.

Proof: The argument is formal. Take $\ln x$ of both sides of (3). Then, for the left side,

$$\ln \prod_{i=1}^{k}(1 + x_i x)^{c_i} = \sum_{i=1}^{k} c_i \ln(1 + x_i x). \tag{4}$$

The expansion

$$\ln(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - + \cdots + \frac{(-1)^{n-1}x^n}{n} + \cdots, \tag{5}$$

$|x| < 1$ is well known.

Let $\text{Coe}_{x^r} f(x)$ denote the coefficient of x^r when $f(x)$ is expanded as a power series in x. Then

$$\text{Coe}_{x^n} \sum_{i=1}^{k} c_i \ln(1 + x_i x) = \sum_{i=1}^{k} \frac{c_i (-1)^{n-1} x_i^n}{n} = \frac{(-1)^{n-1}[c_1 x_1^n + c_2 x_2^n + \cdots + c_k x_k^n]}{n}. \tag{6}$$

To find the coefficient of x^n on the right side of (3) after $\ln x$ is taken, the following argument is given. Since the coefficient of x^n is to be determined, it follows that only

$$\ln\left(1 + \sum_{i=1}^{n} A_i x^i\right)$$

need be considered. Thus, the required coefficient is

$$\text{Coe}_{x^n} \ln\left(1 + \sum_{i=1}^{n} A_i x^i\right) \tag{7}$$

$$= \text{Coe}_{x^n}\left[\frac{\sum_{i=1}^{n} A_i x^i}{1} - \frac{\left(\sum_{i=1}^{n} A_i x^i\right)^2}{2} + - \cdots + \frac{(-1)^{n-j-1}\left(\sum_{i=1}^{n} A_i x^i\right)^{n-j}}{n - j} + \cdots\right].$$

Since each term in this expansion has x as a factor, it is not necessary to consider terms for which $n - j > n$. Thus, $n - j \le n$ so that $j \ge 0$. Also, the only ones that are needed to be considered are those which do have some term with x^n in its expansion. Now each term that has x^n in its expansion satisfies $n(n - j) \geq n$ or $n - j \geq 1$ or $n - 1 \geq j$. Thus, the largest value for j needed is $n - 1$. Hence,

$$\text{Coe}_{x^n} \ln\left(1 + \sum_{i=1}^{n} A_i x^i\right) = \text{Coe}_{x^n} \sum_{j_1=0}^{n-1} \frac{(-1)^{n-j_1-1}\left(\sum_{i=1}^{n} A_i x^i\right)^{n-j_1}}{n - j_1} \tag{8}$$

$$= \sum_{j_1=0}^{n-1} \frac{(-1)^{n-j_1-1}\text{Coe}_{x^{j_1}}\left(A_1 + \sum_{i=2}^{n} A_i x^{i-1}\right)^{n-j_1}}{n - j_1}$$

$$= \sum_{j_1=0}^{n-1} \frac{(-1)^{n-j_1-1}\text{Coe}_{x^{j_1}} \sum_{j_2=0}^{n-j_1} \binom{n - j_1}{j_2} A_1^{n-j_1-j_2}\left(\sum_{i=2}^{n} A_i x^{i-1}\right)^{j_2}}{n - j_1}$$

$$= \sum_{j_1=0}^{n-1} \frac{(-1)^{n-j_1-1} \sum_{j_2=0}^{n-j_1} \binom{n - j_1}{j_2} A_1^{n-j_1-j_2}\,\text{Coe}_{x^{j_1-j_2}}\left(A_2 + \sum_{i=3}^{n} A_i x^{i-2}\right)^{j_2}}{n - j_1}.$$

Continuing this pattern with a simple induction completes the proof. □

An important special case of Theorem 1 occurs when $c_1 = c_2 = \cdots = c_k = 1$. In this case, in (7),

$$\text{Coe}_{x^n} \ln\left(1 + \sum_{i=1}^{k} A_i x^i\right) = \text{Coe}_{x^n} \ln\left(1 + \sum_{i=1}^{k} \sigma_i x^i\right), \tag{9}$$

where $\sigma_1, \sigma_2, \ldots, \sigma_k$ are the elementary symmetric functions of $x_1, x_2, \ldots, x_k$. Thus,

$$\begin{aligned}\sigma_1 &= x_1 + x_2 + \cdots + x_k,\\ \sigma_2 &= x_1x_2 + x_1x_3 + x_1x_4 + \cdots + x_2x_3 + \cdots\\ &\quad + \cdots + x_{k-1}x_k, \ \ldots, \ \sigma_k\\ &= x_1x_2 \ldots x_k.\end{aligned}$$

The only terms in the expansion (9) that need be considered are those which actually do have some term with x^n in its expansion. Now each term which has x^n in its expansion satisfies $k(n - j) \geq n$, or $(k - 1)n \geq kj$, [see line (8)]. Let $h_k(n)$ be the largest whole number t such that $(k - 1)n \geq kt$. Thus, $0 \leq j \leq h_k(n)$. With this change, the following is a corollary to Theorem 1.

Corollary to Theorem 1: Let n be a natural number and let $x_1, x_2, \ldots, x_k$ be a set of real or complex numbers.

Then,

$$x_1^n + x_2^n + \cdots + x_k^n = n \sum_{j_1=0}^{h_k(n)} \frac{(-1)^{j_1} \sum_{j_2=0}^{j_1} \binom{n - j_1}{j_2} \sigma_1^{n-j_1-j_2} \sum_{j_3=0}^{j_2} \binom{j_2}{j_3} \sigma_2^{j_2-j_3} \cdots \sum_{j_{k-1}=0}^{j_{k-2}} \binom{j_{k-2}}{j_{k-1}} \sigma_{k-2}^{j_{k-2}-j_{k-1}} \binom{j_{k-1}}{j_1 - j_2 - \cdots - j_{k-1}} \sigma_{k-1}^{j_{k-1}-(j_1-j_2-\cdots-j_{k-1})} \sigma_k^{j_1-j_2-\cdots-j_{k-1}}}{n - j_1}, \tag{10}$$

where $\sigma_1, \sigma_2, \ldots, \sigma_k$ are the elementary symmetric functions of $x_1, x_2, \ldots, x_k$ and $h_k(n)$ is the largest whole number t such that $(k-1)n \geq kt$.

Using (10), with appropriate simplifications for $k = 2$ and $k = 3$, gives:

$$x_1^n + x_2^n = n \sum_{j=0}^{[n/2]} (-1)^j \frac{\binom{n-j}{j}}{n-j} (x_1 + x_2)^{n-2j}(x_1x_2)^j, \tag{11}$$

and

$$x_1^n + x_2^n + x_3^n \tag{12}$$
$$= \frac{n \sum_{j=0}^{[2n/3]} (-1)^j \sum_{\ell=[(j+1)/2]}^{j} \binom{n-j}{\ell}\binom{\ell}{j-\ell}(x_1 + x_2 + x_3)^{n-j-\ell}}{n-j} \cdot \frac{(x_1x_2 + x_2x_3 + x_3x_1)^{2\ell-j}(x_1x_2x_3)^{j-\ell}}{},$$

where [ ] is the greatest integer function.

The identity (11) is known. It is reported on in [2], p. 80, in the article on G. Candido's use of this identity.
For a discussion of formal arguments, see [3].

Theorem 1 can now be used to establish

Theorem 2: Let $c_1, c_2, \ldots, c_k$ and $x_1, x_2, \ldots, x_k$ be any real or complex numbers and if the coefficients $A_1, A_2, A_3, \ldots$ in

$$\prod_{i=1}^{k} (1 + x_i x)^{c_i} = 1 + \sum_{i=1}^{\infty} A_i x^i$$

are all rational numbers, then:

(1) The sequence $\{u_n\}_{n=1}^{\infty}$, $u_n = c_1x_1^n + c_2x_2^n + \cdots + c_kx_k^n$, is a sequence of rational numbers; and

(2) If for any prime number p, p is relatively prime to each of the denominators of $A_1, A_2, \ldots, A_p$, then the sequence $\{u_n\}_{n=1}^{\infty}$ has the Fermat property.

Proof: From Theorem 1, it is clear that u_n is a rational number if $A_1, A_2, \ldots, A_n$ are all rationals. Also, if p is a prime number, from Theorem 1 and the fact that the denominators of $A_1, A_2, \ldots, A_p$ are all relatively prime to p, $u_p \equiv u_1 \pmod{p}$. Here, $u_1 = A_1$. □

L. E. Dickson established a result somewhat reminiscent of Theorem 2. He showed that if Z_n is the sum of the n^{th} powers of the roots of the polynomial

$$x^m + a_1x^{m-1} + \cdots + a_k = 0,$$

where $a_1 = 0$ and $a_1, a_2, \ldots, a_k$ are all integers, then $Z_p \equiv 0 \pmod{p}$ when p is a prime. See [1]. This result is of course a corollary of Theorem 2.

Example 1: For the Tchebycheff polynomials it is known that

$$2T_n(x) = (x + \sqrt{x^2-1})^n + (x - \sqrt{x^2-1})^n.$$

(See [5], p. 5.) Letting

$$y_1 = x + \sqrt{x^2 - 1}$$

and

$$y_2 = x - \sqrt{x^2 - 1}$$

and

$$(1 + y_1 y)(1 + y_2 y) = 1 + 2xy + y^2$$

so that, by Theorem 2, for x an integer $\{2T_n(x)\}_{n=1}^{\infty}$ is a Fermat sequence. Thus, if p is a prime number $2T_p(x) \equiv 2x \pmod{p}$. Hence, if $p > 2$, $\{T\ (x)\}_{n=1}^{\infty}$ has the Fermat property.

It is possible to give examples of sequences $\{u\ \}_{n=1}^{\infty}$ in (1) of Theorem 2 where the c's are irrational or even complex. However, if the x 's are irrational, then it is not obvious that $u_n \equiv u_1 \pmod{p}$ for p being a prime number. The position taken here is that no irrational number is divisible by any prime number. The arithmetic of this paper is the arithmetic of the real rational integers. Thus,

$$\left(\frac{1 + \sqrt{5}}{2}\right)^p \not\equiv \frac{1 + \sqrt{5}}{2} \pmod{p},$$

but as Theorem 2 shows

$$\left(\frac{1 + \sqrt{5}}{2}\right)^p + \left(\frac{1 - \sqrt{5}}{2}\right)^p \equiv \frac{1 + \sqrt{5}}{2} + \frac{1 - \sqrt{5}}{2} \pmod{p}.$$

Thus, for $x_1, x_2, \ldots, x_k$, the roots of a polynomial over the rationals

$$x_1^p + x_2^p + \cdots + x_k^p \equiv x_1 + x_2 + \cdots + x_k \pmod{p}$$

is a generalization of Fermat's Little Theorem.

From Theorem 1 it is clear that if the u's are all rational numbers, then all the A's in Theorem 2 are also rational. Thus, the following corollary is established.

Corollary to Theorem 2: Let $c_1, c_2, \ldots, c_k$ and $x_1, x_2, \ldots, x_k$ be any real or complex numbers. Then a necessary and sufficient condition for the coefficients $A_1, A_2, A_3, \ldots$ in

$$\prod_{i=1}^{k}(1 + x_i x)^{c_i} = 1 + \sum_{i=1}^{\infty} A_i x^i, \tag{13}$$

to be rational numbers is for the sequence

$$\{u_n\}_{n=1}^{\infty},\ u_n = c_1 x_1^n + c_2 x_2^n + \cdots + c_k x_k^n,$$

to be a sequence of rationals.

Example 3: Let a and b be rationals and suppose that b is not the square of a rational. Consider the power series

$$(1 + (a + \sqrt{b})x)^{a-\sqrt{b}}(1 + (a - \sqrt{b})x)^{a+\sqrt{b}} = 1 + \sum_{i=1}^{\infty} A_i x^i. \tag{14}$$

By the corollary, the power series will have rational coefficients provided

$$u_n = (a + \sqrt{b})(a - \sqrt{b})^n + (a - \sqrt{b})(a + \sqrt{b})^n,$$

is rational for $n = 1, 2, 3, \ldots$. Now

$$u_n = (a^2 - b)[(a - \sqrt{b})^{n-1} + (a + \sqrt{b})^{n-1}] \tag{15}$$

$$= (a^2 - b)\sum_{i=0}^{n-1}\binom{n-1}{i}a^{n-1-i}b^{i/2}[(-1)^i + 1],$$

which is clearly rational.

For example,

$$(1 + \omega x)^{\omega^2}(1 + \omega^2 x)^{\omega} = 1 + \sum_{i=1}^{\infty} A_i x^i, \tag{16}$$

is such that A_i is rational for $i = 1, 2, 3, \ldots$ when $1, \omega, \omega^2$ are the cube roots of unity.

Example 4: Define the sequence $\{u_n\}_{n=1}^{\infty}$ by the formula

$$u_n = \sum_{j=1}^{m} \sec^{2n} \frac{2j-1}{4m}\pi.$$

Here m is an arbitrary natural number. Then $\{u_n\}_{n=1}^{\infty}$ is a sequence of integers which has the Fermat property.

To see this, consider the product

$$f(y) = \prod_{j=1}^{m}\left(1 - \left[\sec^2 \frac{2j-1}{4m}\pi\right] y\right). \tag{17}$$

Multiply this by $\prod_{j=1}^{m} \cos^2 \frac{2j-1}{4m}\pi$ so that

$$f(y)\prod_{j=1}^{m} \cos^2 \frac{2j-1}{4m}\pi = \prod_{j=1}^{m}\left(\cos^2 \frac{2j-1}{4m}\pi - y\right). \tag{18}$$

Replace y by x^2 so that

$$f(x^2)\prod_{j=1}^{m} \cos^2 \frac{2j-1}{4m}\pi = \prod_{j=1}^{m}\left(\cos^2 \frac{2j-1}{4m}\pi - x^2\right), \tag{19}$$

$$\left[(-1)^m \prod_{j=1}^{m} \cos^2 \frac{2j-1}{4m}\pi\right] f(x^2) = \prod_{j=1}^{m}\left(x - \cos \frac{2j-1}{4m}\pi\right)\left(x + \cos \frac{2j-1}{4m}\pi\right). \tag{20}$$

Thinking of $\cos[(2j-1)/4m]\Pi$ along the unit circle for $j = 1, 2, \ldots, m$, it is in the first quadrant so that, by symmetry,

$$\left[(-1)^m \prod_{j=1}^{m} \cos^2 \frac{2j-1}{4m}\pi\right] f(x^2) = \prod_{j=1}^{2m}\left(x - \cos \frac{2j-1}{4m}\pi\right). \tag{21}$$

A well-known identity is

$$x^{2n} + 1 = \prod_{j=1}^{n}\left(x^2 - 2x \cos \frac{2j-1}{2n}\pi + 1\right). \tag{22}$$

In (22), let $n = 2m$ and $x = i$ so that

$$2 = (-1)^m 2^{2m} \prod_{j=1}^{2m} \cos^2 \frac{2j-1}{4m}\pi. \tag{23}$$

Now, by symmetry around the unit circle,

$$\prod_{j=1}^{2m} \cos \frac{2j-1}{4m}\pi = (-1)^m \prod_{j=1}^{m} \cos^2 \frac{2j-1}{4m}\pi = \frac{(-1)^m}{2^{2m-1}}. \tag{24}$$

Using (24) and (21) yields

$$f(x^2) = (-1)^m 2^{2m-1} \prod_{j=1}^{2m}\left(x - \cos\frac{2j-1}{4m}\pi\right). \tag{25}$$

It is well known that

$$T_{2m}(x) = 2^{2m-1}\prod_{j=1}^{2m}\left(x - \cos\frac{2j-1}{4m}\pi\right),$$

where $T_{2m}(x)$ is the $2m^{\text{th}}$ Tchebycheff polynomial (see [4], pp. 86-90). This follows from the fact that $T_n(x) = \cos(n\arccos x)$. Now $x = \sqrt{y}$, so that

$$f(y) = (-1)^m T_{2m}(\sqrt{y}), \tag{26}$$

which is a polynomial in y with integer coefficients.

Since $\sec^2[(2j-1)/4m]\pi$ for $j = 1, 2, 3, \ldots, m$ are the roots of

$$(-1)^m y^m T_{2m}(1/\sqrt{y})$$

and the coefficients of this polynomial are all integers and the leading coefficient is $(-1)^m$, it follows from the corollary to Theorem 2 that $\{u_n\}_{n=1}^{\infty}$ is a sequence of integers satisfying the Fermat property.

References

1. *Amer. Math. Monthly* 15 (1908):209.
2. L. E. Dickson. *History of the Theory of Numbers*. Vol. I: *Divisibility and Primality*. New York: Chelsea, 1952.
3. Ian P. Goulden & David M. Jackson. *Combinatorial Enumeration*. New York: Wiley & Sons, 1983.
4. Kenneth S. Miller & John B. Walsh. *Advanced Trigonometry*. New York: Krieger, 1977.
5. Theodore J. Rivlin. *The Chebyshev Polynomials*. New York: Wiley-Interscience, 1974.
6. J. V. Uspensky. *Theory of Equations*. New York: McGraw-Hill, 1948.

*****

A SIMPLE METHOD WHICH GENERATES INFINITELY MANY CONGRUENCE IDENTITIES

Bau-Sen Du
Institute of Mathematics, Academia Sinica, Taipei, Taiwan 11529, ROC
(Submitted March 1987)

1. Introduction

Let $\phi(m)$ be an integer-valued function defined on the set of all positive integers. If $m = p_1^{k_1}p_2^{k_2} \ldots p_r^{k_r}$, where the p_i's are distinct prime numbers, r and the k_i's are positive integers, we define $\Phi_1(1, \phi) = \phi(1)$ and

$$\Phi_1(m, \phi) = \phi(m) - \sum_{i=1}^{r} \phi(m/p_i) + \sum_{i_1 < i_2} \phi(m/(p_{i_1} p_{i_2}))$$
$$- \sum_{i_1 < i_2 < i_3} \phi(m/(p_{i_1} p_{i_2} p_{i_3})) + \cdots + (-1)^r \phi(m/(p_1 p_2 \ldots p_r)),$$

where the summation $\sum_{i_1 < i_2 < \cdots < i_j}$ is taken over all integers $i_1, i_2, \ldots, i_j$ with $1 \le i_1 < i_2 < \cdots < i_j \le r$.

If $m = 2^{k_0}p_1^{k_1}p_2^{k_2} \ldots p_r^{k_r}$, where the p_i's are distinct odd prime numbers, and $k_0 \ge 0$, r, and the k_i's ≥ 1 are integers, we define, similarly,

$$\Phi_2(m, \phi) = \phi(m) - \sum_{i=1}^{r} \phi(m/p_i) + \sum_{i_1 < i_2} \phi(m/(p_{i_1} p_{i_2}))$$
$$- \sum_{i_1 < i_2 < i_3} \phi(m/(p_{i_1} p_{i_2} p_{i_3})) + \cdots + (-1)^r \phi(m/(p_1 p_2 \ldots p_r)).$$

If $m = 2^k$, where $k \ge 0$ is an integer, we define

$$\Phi_2(m, \phi) = \phi(m) - 1.$$

If, for some integer $n \ge 2$, we have $\phi(m) = n^m$ for all positive integers m, then we denote $\Phi_i(m, \phi)$ by $\Phi_i(m, n)$, $i = 1, 2$, to emphasize the role of this integer n.

On the other hand, let S be a subset of the real numbers and let f be a function from S into itself. For every positive integer n, we let f^n denote the n^{th} iterate of f: $f^1 = f$ and $f^n = f \circ f^{n-1}$ for $n \ge 2$. For every $x_0 \in S$, we call the set $\{f^k(x_0) \mid k \ge 0\}$ the orbit of x_0 under f. If x_0 satisfies $f^m(x_0) = x_0$ for some positive integer m, then we call x_0 a periodic point of f and call the smallest such positive integer m the minimal period of x_0 and of the orbit of x_0 (under f). Note that, if x_0 is a periodic point of f with minimal period m, then, for every integer $1 \le k \le m$, $f^k(x_0)$ is also a periodic point of f with minimal period m and they are all distinct, so every periodic orbit of f with minimal period m consists of exactly m distinct points. Since it is obvious that distinct periodic orbits of f are pairwise disjoint, the number (if finite) of distinct periodic points of f with minimal period m is divisible by m and the quotient equals the number of distinct periodic orbits of f with minimal period m. This observation, together with a standard inclusion-exclusion argument, gives the following well-known result.

Theorem 1: Let S be a subset of the real numbers and let $f: S \to S$ be a mapping with the property that, for every positive integer m, the equation $f^m(x) = x$ (or $-x$, respectively) has only finitely many distinct solutions. Let $\phi(m)$ (or $\psi(m)$, respectively) denote the number of these solutions. Then, for every positive integer m, the following hold.

(i) The number of periodic points of f with minimal period m is $\Phi_1(m, \phi)$. So $\Phi_1(m, \phi) \equiv 0 \pmod{m}$.

(ii) If $0 \in S$ and f is odd, then the number of symmetric periodic points (i.e., periodic points whose orbits are symmetric with respect to the origin) of f with minimal period $2m$ is $\Phi_2(m, \psi)$. Thus, $\Phi_2(m, \psi) \equiv 0 \pmod{2m}$.

Successful applications of the above theorem depend of course on a knowledge of the function ϕ or ψ. For example, if we let S denote the set of all real numbers and, for every integer $n \geq 2$ and every odd integer $t = 2k + 1 > 1$, let

$$f_n(x) = a_n \cdot \prod_{j=1}^{n} (x - j)$$

and let

$$g_t(x) = b_t \cdot x \prod_{j=1}^{k} (x^2 - j^2),$$

where a_n and b_t are fixed sufficiently large positive numbers depending only on n and t, respectively. Then it is easy to see that, for every positive integer m, the equation $f_n^m(x) = x$ [$g_t^m(x) = -x$, resp.] has exactly n^m (t^m, resp.) distinct solutions in S. Therefore, if $\phi(m, n) = n^m$ and $\psi(m, t) = t^m$, then we have as a consequence of Theorem 1 the following well-known congruence identities which include Fermat's Little Theorem as a special case.

Corollary 2: (i) Let $m \geq 1$ and $n \geq 2$ be integers. Then $\Phi_1(m, n) \equiv 0 \pmod{m}$.

(ii) Let $m \geq 1$ be an integer and let $n > 1$ be an odd integer. Then $\phi_2(m, n) \equiv 0 \pmod{2m}$.

In this note, we indicate that the method introduced in [1] can also be used to recursively define infinitely many ϕ and ψ and thus produce infinitely many families of congruence identities related to Theorem 1. In Section 2, we will review this method, and to illustrate it we will prove the following result in Section 3.

Theorem 3: For every positive integer $n \geq 3$, let ϕ_n be the integer-valued function on the set of all positive integers defined recursively by letting $\phi_n(m) = 2^m - 1$ for all $1 \leq m \leq n - 1$ and

$$\phi_n(n + k) = \sum_{j=1}^{n-1} \phi_n(n + k - j), \text{ for all } k \geq 0.$$

Then, for every positive integer m, $\Phi_1(m, \phi_n) \equiv 0 \pmod{m}$. Furthermore,

$$\lim_{m \to \infty} [\log \Phi_1(m, \phi_n)]/m = \lim_{m \to \infty} [\log \phi_n(m)]/m = \log \alpha_n,$$

where α_n is the (unique) positive (and the largest in absolute value) zero of the polynomial

$$x^{n-1} - \sum_{k=0}^{n-2} x^k.$$

Note that in the above theorem these numbers $\phi_n(m)$, $m \geq 1$, are generalized Fibonacci numbers [3, 4] and when $n = 3$, these numbers $\phi_3(m)$, $m \geq 1$, are the well-known Lucas numbers: 1, 3, 4, 7, 11, 18, 29, ...

Just for comparison, we also include the following two results which can be verified numerically. The rigorous proofs of these two results which are similar to that of Theorem 3 below can be found in [1, Theorem 2] and [2, Theorem 3], respectively.

Theorem 4: For every positive integer $n \geq 2$, let sequences

$$\langle b_{k,1,j,n} \rangle,\ \langle b_{k,2,j,n} \rangle,\ 1 \leq j \leq n,$$

be defined recursively as follows:

$$b_{1,1,j,n} = 0,\quad 1 \leq j \leq n,$$
$$b_{2,1,j,n} = 1,\quad 1 \leq j \leq n,$$
$$b_{1,2,j,n} = b_{2,2,j,n} = 0,\quad 1 \leq j \leq n-1,$$
$$b_{1,2,n,n} = b_{2,2,n,n} = 1.$$

For $i = 1$ or 2, and $k \geq 1$,

$$b_{k+2,i,j,n} = b_{k,i,1,n} + b_{k,i,j+1,n},\quad 1 \leq j \leq n-1,$$
$$b_{k+2,i,n,n} = b_{k,i,1,n} + b_{k+1,i,n,n}.$$

Let $b_{k,1,j,n} = 0$ for all $-2n + 3 \leq k \leq 0$ and $1 \leq j \leq n$, and for all positive $n$integers m, let

$$\phi_n(m) = b_{m,2,n,n} + 2 \cdot \sum_{j=1}^{n} b_{m+2-2j,1,j,n}.$$

Then, for every positive integer m, $\Phi_1(m, \phi_n) \equiv 0 \pmod{m}$. Furthermore,

$$\lim_{m \to \infty}[\log \Phi_1(m, \phi_n)]/m = \lim_{m \to \infty}[\log \phi_n(m)]/m = \log \beta_n,$$

where β_n is the (unique) positive (and the largest in absolute value) zero of the polynomial $x^{2n+1} - 2x^{2n-1} - 1$.

Remark 1: For all positive integers m and n, let

$$A_{m,n} = \Phi_1(2m-1, \phi_n)/(2m-1),$$

where ϕ_n is defined as in Theorem 3 for $n = 1$ and as in Theorem 4 for $2 \leq n$. Table 1 lists the first 31 values of $A_{m,n}$ for $1 \leq n \leq 6$. It seems that $A_{m,n} = 2^{m-n-1}$ for $n + 1 \leq m \leq 3n + 2$ and $A_{m,n} > 2^{m-n-1}$ for $m > 3n + 2$. If, for all positive integers m and n, we define sequences $\langle B_{m,n,k} \rangle$ by letting

$$B_{m,n,1} = A_{m+3n+2,n} - 2A_{m+3n+1,n}$$

and

$$B_{m,n,k} = B_{m+2n+1,n,k-1} - B_{m+2n+1,n+1,k-1}$$

for $k > 1$, then more extensive numerical computations seem to show that, for all positive integers k, we have

(i) $B_{1,n,k} = 2$ for all $n \geq 1$,

(ii) $B_{2,n,k} = 4k$ for all $n \geq 1$,

(iii) $B_{3,n,k}$ is a constant depending only on k, and

(iv) for all $1 \leq m \leq 2n + 1$, $B_{m,n,k} = B_{m,j,k}$ for all $j \geq n \geq 1$.

Theorem 5: Fix any integer $n \geq 2$. For all integers i, j, and k with $i = 1, 2$, $1 \leq |j| \leq n$, and $k \geq 1$, we define $c_{k,i,j,n}$ recursively as follows:

$$c_{1,1,n,n} = 1 \text{ and } c_{1,1,j,n} = 0 \quad \text{for } j \neq n,$$
$$c_{1,2,1,n} = 1 \text{ and } c_{1,2,j,n} = 0 \quad \text{for } j \neq 1.$$

For $i = 1, 2$, and $k \geq 1$,

$$c_{k+1,i,1,n} = c_{k,i,1,n} + c_{k,i,-n,n} + c_{k,i,n,n},$$
$$c_{k+1,i,j,n} = c_{k,i,j-1,n} + c_{k,i,n,n} \quad \text{for all } 2 \leq j \leq n,$$
$$c_{k+1,i,-1,n} = c_{k,i,-1,n} + c_{k,i,-n,n} + c_{k,i,n,n},$$
$$c_{k+1,i,-j,n} = c_{k,i,-j+1,n} + c_{k,i,-n,n} \quad \text{for all } 2 \leq j \leq n.$$

Let $c_{k,1,j,n} = 0$ for all integers k, j with $4 - n \leq k \leq 0$ and $1 \leq |j| \leq n$, and, for all positive integers m, let

$$\phi_n(m) = 2\sum_{k=1}^{n-1} c_{m+2-k,1,n+1-k,n} + 2c_{m+1,2,1,n} - 1$$

and

$$\psi_n(m) = 2\sum_{k=1}^{n-1} c_{m+2-k,1,k-n-1,n} + 2c_{m+1,2,-1,n} + 1.$$

Then, for every positive integer m,

$$\Phi_1(m, \phi_n) \equiv 0 \pmod{m} \quad \text{and} \quad \Phi_2(m, \psi_n) \equiv 0 \pmod{2m}.$$

Furthermore,

$$\lim_{m\to\infty}[\log \Phi_1(m, \phi_n)]/m = \lim_{m\to\infty}[\log \phi_n(m)]/m = \lim_{m\to\infty}[\log \psi_n(m)]/m$$
$$= \lim_{m\to\infty}[\log \Phi_2(m, \psi_n)]/m = \log \gamma_n,$$

where γ_n is the (unique) positive (and the largest in absolute value) zero of the polynomial $x^n - 2x^{n-1} - 1$.

Remark 2: For all integers $m \geq 1$ and $n \geq 2$, let

$$D_{m,n} = \Phi_2(m, \psi_n)/(2m),$$

where the ψ_n's are defined as in the above theorem. Table 2 lists the first 25 values of $D_{m,n}$ for $2 \leq n \leq 6$. It seems that $D_{m,n} = 2^{m-n}$ for $n \leq m \leq 3n$, and $D_{m,n} > 2^{m-n}$ for $m > 3n$. If, for all integers $m \geq 1$ and $n \geq 2$, we define the sequences $\langle E_{m,n,k}\rangle$ by letting

$$E_{m,n,1} = D_{m+3n,n} - 2D_{m+3n-1,n}$$

and

$$E_{m,n,k} = E_{m+2n,n,k-1} - E_{m+2n,n+1,k-1}$$

for $k > 1$, then more extensive computations seem to show that, for all positive integers k, we have

(i) $E_{1,n,k} = 2$ for all $n \geq 2$,

(ii) $E_{2,n,k} = 4k$ for all $n \geq 2$,

(iii) $E_{3,n,k}$ and $E_{4,n,k}$ are constants depending only on k, and

(iv) for all $1 \leq m \leq 2n$, $E_{m,n,k} = E_{m,j,k}$ for all $j \geq n \geq 2$.

See Tables 1 and 2 below.

TABLE 1

m	$A_{m,1}$	$A_{m,2}$	$A_{m,3}$	$A_{m,4}$	$A_{m,5}$	$A_{m,6}$
1	1	1	1	1	1	1
2	1	1	1	1	1	1
3	1	0	0	0	0	0
4	1	1	1	1	1	1
5	2	1	0	0	0	0
6	2	2	2	2	2	2
7	4	2	1	0	0	0
8	5	3	3	3	3	3
9	8	4	2	1	0	0
10	11	6	6	6	6	6
11	18	8	4	2	1	0
12	25	11	9	9	9	9
13	40	16	8	4	2	1
14	58	23	18	18	18	18
15	90	32	16	8	4	2
16	135	46	32	30	30	30
17	210	66	32	16	8	4
18	316	94	61	56	56	56
19	492	136	64	32	16	8
20	750	195	115	101	99	99
21	1164	282	128	64	32	16
22	1791	408	224	191	186	186
23	2786	592	258	128	64	32
24	4305	856	431	351	337	335
25	6710	1248	520	256	128	64
26	10420	1814	850	668	635	630
27	16264	2646	1050	512	256	128
28	25350	3858	1673	1257	1177	1163
29	39650	5644	2128	1026	512	256
30	61967	8246	3328	2402	2220	2187
31	97108	12088	4320	2056	1024	512

TABLE 2

m	$D_{m,2}$	$D_{m,3}$	$D_{m,4}$	$D_{m,5}$	$D_{m,6}$
1	0	0	0	0	0
2	1	0	0	0	0
3	2	1	0	0	0
4	4	2	1	0	0
5	8	4	2	1	0
6	16	8	4	2	1
7	34	16	8	4	2
8	72	32	16	8	4
9	154	64	32	16	8
10	336	130	64	32	16
11	738	264	128	64	32
12	1632	538	256	128	64
13	3640	1104	514	256	128
14	8160	2272	1032	512	256
15	18384	4692	2074	1024	512
16	41616	9730	4176	2050	1024
17	94560	20236	8416	4104	2048
18	215600	42208	16980	8218	4096
19	493122	88288	34304	16464	8194
20	1130976	185126	69376	32992	16392
21	2600388	389072	140458	66132	32794
22	5992560	819458	284684	132608	65616
23	13838306	1729296	577592	265984	131296
24	32016576	3655936	1173040	533672	262740
25	74203112	7742124	2384678	1071104	525824

2. Symbolic Representation for Continuous Piecewise Linear Functions

In this section, we review the method introduced in [1]. Throughout this section, let g be a continuous piecewise linear function from the interval $[c, d]$ into itself. We call the set $\{(x_i, y_i) | i = 1, 2, \ldots, k\}$ a set of nodes for (the graph of) $y = g(x)$ if the following three conditions hold:

(1) $k \geq 2$,
(2) $x_1 = c$, $x_k = d$, $x_1 < x_2 < \cdots < x_k$, and
(3) g is linear on $[x_i, x_{i+1}]$ for all $1 \leq i \leq k - 1$ and $y_i = g(x_i)$ for all $1 \leq i \leq k$.

For any such set, we will use its y-coordinates $y_1, y_2, \ldots, y_k$ to represent its graph and call $y_1y_2 \ldots y_k$ (in that order) a (symbolic) representation for (the graph of) $y = g(x)$. For $1 \leq i < j \leq k$, we call $y_iy_{i+1} \ldots y_j$ the representation for $y = g(x)$ on $[x_i, x_j]$ obtained by restricting $y_1y_2 \ldots y_k$ to $[x_i, x_j]$. For convenience, we will also call every y_i in $y_1y_2 \ldots y_k$ a node. If $y_i = y_{i+1}$ for some i (i.e., g is constant on $[x_i, x_{i+1}]$), we will simply write

$$y_1 \cdots y_iy_{i+2} \cdots y_k$$

instead of

$$y_1 \cdots y_iy_{i+1}y_{i+2} \cdots y_k.$$

That is, we will delete y_{i+1} from the (symbolic) representation $y_1y_2 \ldots y_k$. Therefore, every two consecutive nodes in a (symbolic) representation are distinct. Note that a continuous piecewise linear function obviously has more than one (symbolic) representation. However, as we will soon see that there is no need to worry about that.

Now assume that $\{(x_i, y_i) | i = 1, 2, \ldots, k\}$ is a set of nodes for $y = g(x)$ and $a_1a_2 \ldots a_r$ is a representation for $y = g(x)$ with

$$\{a_1, a_2, \ldots, a_r\} \subset \{y_1, y_2, \ldots, y_k\}$$

and $a_i \neq a_{i+1}$ for all $1 \leq i \leq r - 1$. If

$$\{y_1, y_2, \ldots, y_k\} \subset \{x_1, x_2, \ldots, x_k\},$$

then there is an easy way to obtain a representation for $y = g^2(x)$ from the one $a_1a_2 \ldots a_r$ for $y = g(x)$. The procedure is as follows: First, for any two distinct real numbers u and v, let $[u : v]$ denote the closed interval with endpoints u and v. Then let $b_{i,1}b_{i,2} \ldots b_{i,t_i}$ be the representation for $y = g(x)$ on $[a_i : a_{i+1}]$ which is obtained by restricting $a_1a_2 \ldots a_r$ to $[a_i : a_{i+1}]$. We use the following notation to indicate this fact:

$$a_ia_{i+1} \to b_{i,1}b_{i,2} \cdots b_{i,t_i} \text{ (under } g\text{) if } a_i < a_{i+1},$$

or

$$a_ia_{i+1} \to b_{i,t_i} \cdots b_{i,2}b_{i,1} \text{ (under } g\text{) if } a_i > a_{i+1}.$$

The above representation on $[a_i : a_{i+1}]$ exists since

$$\{a_1, a_2, \ldots, a_r\} \subset \{x_1, x_2, \ldots, x_k\}.$$

Finally, if $a_i < a_{i+1}$, let $z_{i,j} = b_{i,j}$ for all $1 \leq j \leq t_i$. If $a_i > a_{i+1}$, let

$$z_{i,j} = b_{i,t_i+1-j} \text{ for all } 1 \leq j \leq t_i.$$

Let

$$Z = z_{1,1} \cdots z_{1,t_1}z_{2,2} \cdots z_{2,t_2} \cdots z_{r,2} \cdots z_{r,t_r}.$$

(Note that $z_{i,t_i} = z_{i+1,1}$ for all $1 \leq i \leq r - 1$.) Then it is easy to see that Z is a representation for $y = g^2(x)$. It is also obvious that the above procedure can be applied to the representation Z for $y = g^2(x)$ to obtain one for $y = g^3(x)$, and so on.

3. Proof of Theorem 3

In this section we fix an integer $n \geq 3$ and let $f_n(x)$ be the continuous function from the interval $[1, n]$ onto itself defined by

$$f_n(x) = x + 1 \quad \text{for } 1 \leq x \leq n - 1$$

and

$$f_n(x) = -(n - 1)x + n^2 - n + 1 \quad \text{for } n - 1 \leq x \leq n.$$

Using the notations introduced in Section 2, we have the following result.

Lemma 6: Under f_n, we have

$$k(k + 1) \to (k + 1)(k + 2), \ 2 \leq k \leq n - 2, \text{ if } n > 3,$$

$$(k + 1)k \to (k + 2)(k + 1), \ 2 \leq k \leq n - 2, \text{ if } n > 3,$$

$$(n - 1)n \to n(1), \ n(n - 1) \to (1)n,$$

$$n(1) \to (1)n(n - 1) \ldots 432, \ (1)n \to 234 \ldots (n - 1)n(1).$$

In the following, when we say the representation for $y = f_n^k(x)$, we mean the representation obtained, following the procedure as described in Section 2, by applying Lemma 6 to the representation $234 \ldots (n - 1)n(1)$ for $y = f_n(x)$ successively until we get to the one for $y = f_n^k(x)$.

For every positive integer k and all integers i, j with $1 \leq i, j \leq n - 1$, let $a_{k,i,j,n}$ denote the number of uv's and vu's in the representation for $y = f_n^k(x)$ whose corresponding x-coordinates are in the interval $[i, i + 1]$, where $uv = 1n$ if $j = 1$, and $uv = j(j + 1)$ if $2 \leq j \leq n - 1$. It is obvious that

$$a_{1,i,i+1,n} = 1 \text{ for all } 1 \leq i \leq n - 2,$$

$$a_{1,n-1,1,n} = 1, \text{ and } a_{1,i,j,n} = 0 \text{ elsewhere.}$$

From the above lemma, we find that these sequences $\langle a_{k,i,j,n} \rangle$ can be computed recursively.

Lemma 7: For every positive integer k and all integers i with $1 \leq i \leq n-1$, we have

$$a_{k+1,i,1,n} = a_{k,i,1,n} + a_{k,i,n-1,n},$$

$$a_{k+1,i,2,n} = a_{k,i,1,n},$$

$$a_{k+1,i,j,n} = a_{k,i,1,n} + a_{k,i,j-1,n}, \ 3 \leq j \leq n - 1 \text{ if } n > 3.$$

It then follows from the above lemma that the sequences $\langle a_{k,i,j,n} \rangle$ can all be computed from the sequences $\langle a_{k,n-1,j,n} \rangle$.

Lemma 8: For every positive integer k and all integers j with $1 \leq j \leq n-1$, we have

$$a_{k,n-1,j,n} = a_{k+i,n-1-i,j,n}, \ 1 \leq i \leq n - 2.$$

For every positive integer k, let

$$c_{k,n} = \sum_{i=1}^{n-1} a_{k,i,1,n} + \sum_{i=2}^{n-1} a_{k,i,i,n}.$$

Then it is easy to see that $c_{k,n}$ is exactly the number of distinct solutions of the equation $f_n^k(x) = x$ in the interval $[1, n]$. From the above lemma, we also have, for all $k \geq 1$, the identities:

$$c_{k,n} = \sum_{i=0}^{n-2} a_{k-i,\, n-1,\, 1,\, n} + \sum_{i=0}^{n-3} a_{k-i,\, n-1,\, n-1-i,\, n}$$

provided that $a_{m,n-1,j,n} = 0$ for all $m \le 0$ and $j > 0$. Since, for every positive integer k,

$$\begin{aligned} a_{k,\, n-1,\, 1,\, n} &= a_{k-1,\, n-1,\, 1,\, n} + a_{k-1,\, n-1,\, n-1,\, n} \\ &= a_{k-1,\, n-1,\, 1,\, n} + a_{k-2,\, n-1,\, 1,\, n} + a_{k-2,\, n-1,\, n-2,\, n} \\ &= a_{k-1,\, n-1,\, 1,\, n} + a_{k-2,\, n-1,\, 1,\, n} + a_{k-3,\, n-1,\, 1,\, n} \\ &\qquad + a_{k-3,\, n-1,\, n-3,\, n} \\ &= \cdots \\ &= \sum_{i=1}^{n-1} a_{k-i,\, n-1,\, 1,\, n} \end{aligned}$$

and

$$\begin{aligned} c_{k,n} &= \sum_{i=0}^{n-2} a_{k-i,\, n-1,\, 1,\, n} + \sum_{i=0}^{n-3} a_{k-i,\, n-1,\, n-1-i,\, n} \\ &= a_{k,\, n-1,\, 1,\, n} + a_{k-1,\, n-1,\, 1,\, n} + \sum_{i=2}^{n-2} a_{k-i,\, n-1,\, 1,\, n} \\ &\qquad + a_{k-1,\, n-1,\, 1,\, n} + a_{k-1,\, n-1,\, n-2,\, n} \\ &\qquad + \sum_{i=1}^{n-3} a_{k-i,\, n-1,\, n-1-i,\, n} \\ &= a_{k,\, n-1,\, 1,\, n} + 2a_{k-1,\, n-1,\, 1,\, n} + \sum_{i=2}^{n-2} a_{k-i,\, n-1,\, 1,\, n} \\ &\qquad + 2a_{k-1,\, n-1,\, n-2,\, n} + \sum_{i=2}^{n-3} a_{k-i,\, n-1,\, n-1-i,\, n} \\ &= \cdots \\ &= \sum_{i=0}^{n-2} (i+1) a_{k-i,\, n-1,\, 1,\, n} \end{aligned}$$

provided that $a_{m,n-1,1,n} = 0$ if $m \le 0$, we obtain that $c_{k,n} = 2^k - 1$ for all $1 \le k \le n - 1$ and

$$c_{k,n} = \sum_{i=1}^{n-1} c_{k-i,n} \text{ for all integers } k \ge n.$$

If, for every positive integer m, we let $\phi_n(m) = c_{m,n}$, then, by Theorem 1, we have $\Phi_1(m, \phi_n) \equiv 0 \pmod{m}$. The proof of the other statement of Theorem 3 is easy and omitted (see [3] and [4]). This completes the proof of Theorem 3.

References

1. Bau-Sen Du. "The Minimal Number of Periodic Orbits of Periods Guaranteed in Sharkovskii's Theorem." *Bull. Austral. Math. Soc.* *31* (1985):89-103.
2. Bau-Sen Du. "Symmetric Periodic Orbits of Continuous Odd Functions on the Interval." *Bull. Inst. Math. Acad. Sinica* *16* (1988):1-48.
3. Hyman Gabai. "Generalized Fibonacci k-Sequences." *Fibonacci Quarterly 8.1* (1970):31-38.
4. E. P. Miles, Jr. "Generalized Fibonacci Numbers and Associated Matrices." *Amer. Math. Monthly* *67* (1960):745-52.

*****

Announcement

FOURTH INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS

Monday through Friday, July 30-August 3, 1990

Department of Mathematics and Computer Science

Wake Forest University

Winston-Salem, North Carolina 27109

International Committee

Horadam, A.F. (Australia), *Co-Chairman*
Philippou, A.N. (Cyprus), *Co-Chairman*
Ando, S. (Japan)
Bergum, G. (U.S.A.)
Johnson, M. (U.S.A.)
Kiss P. (Hungary)
Filipponi, Piero (Italy)
Campbell, Colin (Scotland)

Local Committee

Fred T. Howard, *Co-Chairman*
Marcellus E. Waddill, *Co-Chairman*
Elmer K. Hayashi
Theresa Vaughan
Deborah Harrell

CALL FOR PAPERS

The FOURTH INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS will take place at Wake Forest University, Winston-Salem, N.C., from July 30 to August 3, 1990. This conference is sponsored jointly by the Fibonacci Association and Wake Forest University.

Papers on all branches of mathematics and science related to the Fibonacci numbers as well as recurrences and their generalizations are welcome. Abstracts are to be submitted by March 15, 1990. Manuscripts are requested by May 1, 1990. Abstracts and manuscripts should be sent to G.E. Bergum (address below). Invited and contributed papers will appear in the Conference Proceedings, which are expected to be published.

The program for the Conference will be mailed to all participants, and to those individuals who have indicated an interest in attending the conference, by June 15, 1990. All talks should be limited to one hour or less.

For further information concerning the conference, please contact Gerald Bergum, *The Fibonacci Quarterly*, Department of Computer Science, South Dakota State University, P.O. Box 2201, Brookings, South Dakota 57007-0194.

ON ANDREWS' GENERALIZED FROBENIUS PARTITIONS

Padmavathamma
University of Mysore, Manasagangotri, Mysore-570 006, India
(Submitted March 1987)

1. Introduction

A generalized Frobenius partition or simply an F-partition of an integer n greater than 0 is a two-rowed array of nonnegative integers

$$\begin{pmatrix} a_1 & \dots & a_r \\ b_1 & \dots & b_r \end{pmatrix}$$

where each row is arranged in nonincreasing order and

$$n = r + \sum_{i=1}^{r} (a_i + b_i).$$

Let $c\phi_{k,h}(n)$ denote the number of those F-partitions of n in which each part is repeated at most h times and is taken from k copies of the nonnegative integers which are ordered as follows: $m_i < n_j$ if $m < n$ or if $m = n$ and $i < j$, where i and j denote the copy of the nonnegative integers. $c\phi_{k,h}(n)$ is called the number of F-partitions of n with k colors and h repetitions. Let $C\phi_{k,h}(q)$ be the generating function of $c\phi_{k,h}(n)$ so that

$$C\phi_{k,h}(q) = \sum_{n=0}^{\infty} c\phi_{k,h}(n)q^n.$$

For example, the F-partitions enumerated by $c\phi_{2,2}(1)$ are

$$\begin{pmatrix} 0_1 \\ 0_1 \end{pmatrix}\begin{pmatrix} 0_2 \\ 0_1 \end{pmatrix}\begin{pmatrix} 0_1 \\ 0_2 \end{pmatrix}\begin{pmatrix} 0_2 \\ 0_2 \end{pmatrix}$$

and those enumerated by $c\phi_{2,2}(2)$ are

$$\begin{pmatrix} 1_1 \\ 0_1 \end{pmatrix}\begin{pmatrix} 1_2 \\ 0_1 \end{pmatrix}\begin{pmatrix} 1_1 \\ 0_2 \end{pmatrix}\begin{pmatrix} 1_2 \\ 0_2 \end{pmatrix}\begin{pmatrix} 0_1 \\ 1_1 \end{pmatrix}\begin{pmatrix} 0_1 \\ 1_2 \end{pmatrix}\begin{pmatrix} 0_2 \\ 1_1 \end{pmatrix}\begin{pmatrix} 0_2 \\ 1_2 \end{pmatrix}$$

$$\begin{pmatrix} 0_2 & 0_1 \\ 0_2 & 0_1 \end{pmatrix}\begin{pmatrix} 0_2 & 0_2 \\ 0_2 & 0_2 \end{pmatrix}\begin{pmatrix} 0_2 & 0_2 \\ 0_2 & 0_1 \end{pmatrix}\begin{pmatrix} 0_2 & 0_2 \\ 0_1 & 0_1 \end{pmatrix}\begin{pmatrix} 0_2 & 0_1 \\ 0_2 & 0_2 \end{pmatrix}$$

$$\begin{pmatrix} 0_2 & 0_1 \\ 0_1 & 0_1 \end{pmatrix}\begin{pmatrix} 0_1 & 0_1 \\ 0_2 & 0_1 \end{pmatrix}\begin{pmatrix} 0_1 & 0_1 \\ 0_1 & 0_1 \end{pmatrix}\begin{pmatrix} 0_1 & 0_1 \\ 0_2 & 0_2 \end{pmatrix}$$

and

$$c\phi_{2,2}(q) = 1 + 4q + 17q^2 + \cdots .$$

Similarly,

$$C\phi_{3,2}(q) = 1 + 9q + 54q^2 + \cdots .$$

George E. Andrews [2] has studied extensively the two functions

$$c\phi_{1,k}(n) = \phi_k(n) \quad \text{and} \quad c\phi_{k,1}(n) = c\phi_k(n).$$

The former function enumerates the F-partitions of n in which the parts repeat at most k times and the latter enumerates those F-partitions of n in which the parts are distinct and are colored with k given colors. Andrews [2] has obtained infinite product representations for

$$C\phi_{1,1}(q) = \phi_1(q), \quad C\phi_{1,2}(q) = \phi_2(q),$$
$$C\phi_{1,3}(q) = \phi_3(q), \quad C\phi_{2,1}(q) = C\phi_2(q)$$

and has expressed $C\phi_{3,1}(q) = C\phi_3(q)$ as a sum of two infinite products. The purpose of this paper is to outline a method of obtaining such representations for $C\phi_{k,h}(q)$ for arbitrary positive integers k and h. We first consider in §2 the typical cases $C\phi_{2,2}(q)$ and $C\phi_{2,3}(q)$ and sketch in §3 how the methods of §2 can be extended for $C\phi_{k,h}(q)$ for arbitrary positive integers k and h. Throughout, we use the notations

$$(a)_\infty = (a, q)_\infty = \prod_{n=0}^{\infty}(1 - aq^n)$$

for complex numbers a and q with $|q| < 1$.

2. Representations of $C\phi_{2,2}(q)$ and $C\phi_{2,3}(q)$

Theorem 1: For $|q| < 1$,

$$C\phi_{2,2}(q) = A_0(q)^2(q^4;\, q^4)_\infty(-q^2;\, q^4)_\infty^2 + 2q^{-1}[qB_0(q)]^2(q^4;\, q^4)_\infty(-q^4;\, q^4)_\infty^2, \tag{1}$$

where $A_0(q) = \phi_2(q)$ and $qB_0(q)$ is the generating function for symbols

$$\begin{pmatrix} \alpha_1 & \cdots & \alpha_r\alpha_{r+1} \\ \beta_1 & \cdots & \beta_r \end{pmatrix} \tag{2}$$

That is, this is subject to the same rules as the original generalized Frobenius symbols related to $\phi_2(q)$ but there is one more element in the top now. This sort of generalization of the Frobenius symbol has been studied at length by James Propp in a forthcoming article in the *Journal of Combinatorial Theory*.

Proof: To prove (1) we first make use of the following result of Andrews [3, Lemma 3]:

$$\begin{aligned}(z\alpha q)_\infty(z\beta q)_\infty(z^{-1}\alpha^{-1})_\infty(z^{-1}\beta^{-1})_\infty \\ = A_0(\alpha, \beta, q)\sum_{n=-\infty}^{\infty} q^{n^2+n}\alpha^n\beta^n z^{2n} \\ - \beta^{-1}A_0(\alpha q, \beta, q)\sum_{n=-\infty}^{\infty} q^{n^2}\alpha^n\beta^n z^{2n-1},\end{aligned} \tag{3}$$

where z, α, β are nonzero, $|q| < 1$, and

$$A_0(\alpha, \beta, q) = (-q)_\infty(-\alpha\beta^{-1}q;\, q^2)_\infty(-\alpha^{-1}\beta q;\, q^2)_\infty(q)_\infty^{-1}. \tag{4}$$

Choosing $\alpha = \omega$, $\beta = \omega^2$ in (3) where $\omega = \exp(2\pi i/3)$ and observing that

$$\prod_{n=1}^{\infty}(1 - q^{2n-1} + q^{4n-2}) = \frac{(-q^3;\, q^6)_\infty}{(-q;\, q^2)_\infty}$$

we obtain

$$\prod_{n=0}^{\infty}(1 + zq^{n+1} + z^2q^{2n+2})(1 + z^{-1}q^n + z^{-2}q^{2n}) \tag{5}$$
$$= A_0(q)\sum_{n=-\infty}^{\infty} q^{n^2+n}z^{2n} - B_0(q)\sum_{n=-\infty}^{\infty} q^{n^2}z^{2n-1},$$

where

$$A_0(q) = \frac{(-q^2;\ q^2)_\infty(-q^3;\ q^6)_\infty}{(q)_\infty} = \phi_2(q) \tag{6}$$

$$B_0(q) = -\frac{(-q;\ q^2)_\infty(-q^6;\ q^6)_\infty}{(q)_\infty}. \tag{7}$$

From the General Principle of Andrews [2, p. 5], it immediately follows that $C\phi_{2,2}(q)$ is the constant term in

$$\prod_{n=0}^{\infty}(1 + zq^{n+1} + z^2q^{2n+2})^2(1 + z^{-1}q^n + z^{-2}q^{2n})^2.$$

Squaring (5) and equating the constant terms, we get

$$C\phi_{2,2}(q) = \phi_2(q)^2\sum_{n=-\infty}^{\infty} q^{2n^2} + [qB_0(q)]^2\sum_{n=-\infty}^{\infty} q^{2n^2-2n-1}. \tag{8}$$

Now, using Jacobi's triple product identity [1, p. 21]:

$$\sum_{n=-\infty}^{\infty} q^{n^2}z^n = (q^2;\ q^2)_\infty(-qz;\ q^2)_\infty(-qz^{-1};\ q^2)_\infty \tag{9}$$

for $z \neq 0$, $|q| < 1$ for the two summations in (8) we get (1).

From the proof of Theorem 1, it immediately follows that $C\phi_{2,2}(q)$ has the following representation.

Corollary 1: For $|q| < 1$,

$$C\phi_{2,2}(q) = \frac{(-q^2;\ q^2)_\infty^2(-q^3;\ q^6)_\infty^2(q^4;\ q^4)_\infty(-q^2;\ q^4)_\infty^2}{(q)_\infty^2} \tag{10}$$
$$+ 2q\frac{(-q;\ q^2)_\infty^2(-q^6;\ q^6)_\infty(q^4;\ q^4)_\infty(-q^4;\ q^4)_\infty^2}{(q)_\infty^2}.$$

Theorem 2: For $|q| < 1$,

$$C\phi_{2,3}(q) = A_1(q)^2(q^6;\ q^6)_\infty(-q^3;\ q^6)_\infty^2 \tag{11}$$
$$+ q^{-5}[qB_1(q)][q^2C_1(q)](q^6;\ q^6)_\infty(-q;\ q^6)_\infty(-q^5;\ q^5)_\infty,$$

where $A_1(q) = \phi_3(q)$, $qB_1(q)$ is the generating function for symbols (2) where a part can be repeated at most three times on each row and $q^2C_1(q)$ is the generating function for symbols

$$\begin{pmatrix}\alpha_1 & \ldots & \alpha_r\alpha_{r+1}\alpha_{r+2}\\ \beta_1 & \ldots & \beta_r\end{pmatrix}$$

which has two more elements in the top row than the original generalized Frobenius symbol.

Proof: Proof of (11) is similar to the proof of (1) and we give only a sketch. First, for α, β, γ, z nonzero and $|q| < 1$, we can obtain the Laurent expansion of the product

$$(z\alpha q)_\infty (z\beta q)_\infty (z\gamma q)_\infty (z^{-1}\alpha^{-1})_\infty (z^{-1}\beta^{-1})_\infty (z^{-1}\gamma^{-1})_\infty \tag{3'}$$

in the same way the analogous Andrews' identity (3) above is derived [3, Lemma 3]. Then, substituting $\alpha = i$, $\beta = -i$, and $\gamma = -1$ in that Laurent expansion, we obtain in analogy with (5)

$$\prod_{n=0}^{\infty}(1 + zq^{n+1} + z^2q^{2n+2} + z^3q^{3n+3})(1 + z^{-1}q^n + z^{-2}q^{2n} + z^{-3}q^{3n}) \tag{5'}$$

$$= \frac{(q^2;\, q^2)_\infty (q;\, q^2)_\infty^2 (q^6;\, q^6)_\infty}{(q)_\infty^3}\Bigg[(-q^3;\, q^6)_\infty^2 \sum_{n=-\infty}^{\infty} q^{\frac{1}{2}(3n^2+3n)} z^{3n}$$

$$+ q(-q;\, q^6)_\infty (-q^5;\, q^6)_\infty \sum_{n=-\infty}^{\infty} q^{\frac{1}{2}(3n^2+5n)} z^{3n+1}$$

$$+ q^3(-q^{-1};\, q^6)_\infty (-q^7;\, q^6)_\infty \sum_{n=-\infty}^{\infty} q^{\frac{1}{2}(3n^2+7n)} z^{3n+2}\Bigg]$$

$$= A_1(q)\Sigma_1 + B_1(q)\Sigma_2 + C_1(q)\Sigma_3, \text{ say.}$$

From the General Principle [2, p. 5], it is clear that $C\phi_{2,3}(q)$ is a constant term in

$$\prod_{n=0}^{\infty}(1 + zq^{n+1} + z^2q^{2n+2} + z^3q^{3n+3})^2(1 + z^{-1}q^n + z^{-2}q^{2n} + z^{-3}q^{3n})^2.$$

Squaring (5′) and equating the constant terms, we find

$$C\phi_{2,3}(q) = A_1(q)^2 \sum_{n=-\infty}^{\infty} q^{3n^2} + [qB_1(q)][q^2C_1(q)] \sum_{n=-\infty}^{\infty} q^{3n^2+2n-5}. \tag{8'}$$

Finally, using (9) for the two summations in (8′), we obtain (11).

From the proof of Theorem 2, we obtain the following representation of $C\phi_{2,3}(q)$.

Corollary 2: For $|q| < 1$,

$$C\phi_{2,3}(q) = \frac{(q^2;\, q^2)_\infty^2 (q;\, q^2)_\infty^4 (q^6;\, q^6)_\infty^3}{(q)_\infty^6}[(-q^3;\, q^6)_\infty^6 + \tag{12}$$

$$+ 2q^2(-q;\, q^6)_\infty^2 (-q^5;\, q^6)_\infty^2 (-q^{-1};\, q^6)_\infty (-q^7;\, q^6)_\infty].$$

3. Representation of $C\phi_{k,h}(q)$ in General

The representation of $C\phi_{k,h}(q)$ for arbitrary positive integers k and h is obtained in Theorem 3 in the same way we obtain the special cases (1) and (11), but after suitable generalizations of the methods. Lemma 1 furnishes a result which plays the role played by Jacobi's triple product identity in passing from (8) to (1) and from (8′) to (11). Due to the mechanical nature of the steps, we only sketch our proofs and avoid lengthy expressions.

Lemma 1: For $a > 0$, $a_1, \ldots, a_{k-1}$ integers and $|q| < 1$, the series

$$\sum_{n_1, \ldots, n_{k-1} = -\infty}^{\infty} q^{a\left(\sum_{i=1}^{k-1} n_i^2 + \sum_{1 \le i < j \le k-1} n_i n_j\right) + \sum_{i=1}^{k-3} a_i n_i} \tag{9$'$}$$

can be expressed as a sum of $2^{k-2}3^{k-3}4^{k-4} \ldots (k-1)^{k-(k-1)}$ infinite products.

Proof: First Step. By grouping terms with $n_1, \ldots, n_{k-2}$ even and $n_1, \ldots, n_{k-2}$ odd separately, the series (9$'$) can be written as the sum of 2^{k-2} series, each of which will be of the form

$$q^{m_1} \sum_{n_1, \ldots, n_{k-2} = -\infty}^{\infty} q^{a\left(3n_1^2 + \cdots + 3n_{k-2}^2 + 2 \sum_{1 \le i < j \le k-2} n_i n_j\right) + \sum_{i=1}^{k-2} b_i n_i} \times \sum_{n_{k-1} = -\infty}^{\infty} q^{an_{k-1}^2 + bn_{k-1} + b'},$$

where $m_1, b_1, \ldots, b_{k-2}, b, b'$ are integers. Here, the second series can be written as an infinite product by Jacobi's triple product identity (9). Thus, it suffices to express the first series as a product.

Second Step: By grouping terms with $n_1, \ldots, n_{k-3} \equiv r \pmod 3$, $r = 0, 1, 2$, the first series of the first step can be written as the sum of 3^{k-3} series, each of which will be of the form

$$q^{m_2} \sum_{n_1, \ldots, n_{k-3} = -\infty}^{\infty} q^{a\left(24n_1^2 + \cdots + 24n_{k-3}^2 + 12 \sum_{1 \le i < j \le k-3} n_i n_j\right) + \sum_{i=1}^{k-3} c_i n_i} \times \sum_{n_{k-2} = -\infty}^{\infty} q^{3an_{k-2}^2 + cn_{k-2} + c'},$$

where $m_2, c_1, \ldots, c_{-3}, c, c'$ are all integers.

Proceeding similarly, we arrive at the $(k-2)^{\text{th}}$ step, namely,

$(k-2)^{th}$ Step: By grouping terms with $n_1 \equiv r \pmod{k-1}$, $r = 0, 1, 2, \ldots, k-2$, separately, the first series of the $(k-3)^{\text{th}}$ step can be written as a sum of $(k-1)^{k-(k-1)} = k-1$ series, each of which will be of the form

$$q^{m_{k-2}} \sum_{n_1 = -\infty}^{\infty} q^{\alpha_1 n_1^2 + \beta_1 n_1 + \gamma_1} \sum_{n_2 = -\infty}^{\infty} q^{\alpha_2 n_2^2 + \beta_2 n_2 + \gamma_2},$$

(where m_{k-2}, α_i, β_i, γ_i for $i = 1, 2$ are integers), which are explicit infinite products by (9).

Conclusion: From Steps 1 to $(k-2)$, it is clear that the series (9$'$) can be written as a sum of $2^{k-2}3^{k-3}4^{k-4} \ldots (k-1)$ infinite products. This proves Lemma 1.

Theorem 3: For arbitrary positive integers k and h, $C\phi_{k,h}(q)$ can be expressed as a sum of infinite products.

Proof: For $z, \alpha_1, \ldots, \alpha_h$ all nonzero and $|q| < 1$, we consider the product

$$(z\alpha_1 q)_\infty (z\alpha_2 q)_\infty \ldots (z\alpha_h q)_\infty (z^{-1}\alpha_1^{-1})_\infty (z^{-1}\alpha_2^{-1})_\infty \ldots (z^{-1}\alpha_h^{-1})_\infty, \tag{3$''$}$$

which, on using (9), can be written as

$$(q)_\infty^{-h} \sum_{n_1=-\infty}^{\infty} (-1)^{n_1} q^{\frac{n_1^2+n_1}{2}} \alpha_1^{n_1} z^{n_1} \ \ldots \ \sum_{n_h=-\infty}^{\infty} (-1)^{n_h} q^{\frac{n_h^2+n_h}{2}} \alpha_h^{n_h} z^{n_h}. \tag{13}$$

It is not difficult to realize a procedure for obtaining the Laurent expansion of the product (13). For instance, consider, for arbitrary integers a, b, c, d, e, f and nonzero z, α, β and $|q| < 1$, the product

$$\sum_{m=-\infty}^{\infty} q^{am^2+bm} \alpha^m z^{cm} \sum_{n=-\infty}^{\infty} q^{dn^2+en} \beta^n z^{fn}. \tag{14}$$

In this, let

$$x = \frac{c}{(c,\ f)} \quad \text{and} \quad y = \frac{f}{(c,\ f)}.$$

By grouping terms with $m \equiv r \pmod{y}$, $r = 0, 1, \ldots, y-1$, separately, and then changing n to $n - xm$, (14) can be written as sum of y number of series of the form

$$\sum_{m=-\infty}^{\infty} S(\beta,\ z,\ q,\ m) \sum_{n=-\infty}^{\infty} q^{an^2-bmn+cn} \alpha^n. \tag{15}$$

Now grouping terms with $m \equiv r \pmod{e}$, $r = 0, 1, \ldots, e-1$, where $2ad - be = 0$ with $(d, e) = 1$ in (15), we obtain the Laurent expansion of (14).

By applying the above procedure successively, we obtain the Laurent expansion of (13). Substituting $\alpha_1 = \omega, \ldots, \alpha_h = \omega^h$, where $\omega = \exp(2\pi i/h + 1)$ in that Laurent expansion, multiplying the resulting identity k times, and equating the constant terms, we find $C\phi_{k,h}(q)$ to be a sum of series of the form (9′) which, by Lemma 1, is a sum of $2^{k-2}3^{k-3} \ldots (k-1)$ infinite products.

It would be interesting to obtain combinatorial proofs of equations (8) and (8′) which might throw more light on this subject.

Acknowledgments

The results of this paper form a part of the author's doctoral dissertation at the University of Mysore under the guidance of Professor S. Bhargava. She wishes to express her deep sense of gratitude to him and to Professor George E. Andrews for their valuable suggestions and comments in preparing this paper. She is also grateful to the referee of this paper for his useful comments.

References

1. G. E. Andrews. "The Theory of Partitions." In *Encyclopedia of Math and Its Applications*, Vol. II. Reading, Mass.: Addison-Wesley, 1976.
2. G. E. Andrews. "Generalised Frobenius Partitions." *Memoirs of the Amer. Math. Soc. 49* (1984):1-44.
3. G. E. Andrews. "Hecke Modular Forms and the Kac-Peterson Identities." *Trans. Amer. Math. Soc. 283.2* (1984):451-458.

*****

RECURSIONS FOR CARLITZ TRIPLES

Paul Duvall and Theresa P. Vaughan
University of North Carolina at Greensboro, Greensboro, NC 27412
(Submitted March 1987)

1. Introduction

In [1], using the properties of the reciprocity law for Dedekind sums, L. Carlitz proved that the system

$$\begin{aligned} hh' &\equiv 1 \pmod{k}, & hh' &\equiv 1 \pmod{k'} \\ kk' &\equiv 1 \pmod{h}, & kk' &\equiv 1 \pmod{h'} \end{aligned} \tag{*}$$

has no positive integral solutions unless either $k = k'$ or $h = h'$.

In [2], M. DeLeon studied (essentially) solutions of the system (*). He defines a Carlitz four-tuple (a, b, c, c) by: a, b, c are integers (not required to be positive), $ab \equiv 1 \pmod{c}$, $c^2 \equiv 1 \pmod{a}$, and $c^2 \equiv 1 \pmod{b}$. He introduces the notion of a primitive Carlitz four-tuple (a, b, c, c), that is, one with the property that there exists no integer $m > 1$ such that one also has that $(a/m, bm, c, c)$ is a Carlitz four-tuple. We mention here two of his results, which are basic to our work in this paper: the Carlitz four-tuple (a, b, c, c) is primitive if and only if the greatest common divisor

$$\gcd(a, (c^2 - 1)/b) = 1,$$

and secondly, if (a, b, c, c) is primitive, then a divides b.

In this paper we consider only the positive integral solutions of the system (*). Since at most three different integers are involved, we use the notation (a, b, c) for a solution, with $ab \equiv 1 \pmod{c}$, $c^2 \equiv 1 \pmod{a}$, and $c^2 \equiv 1 \pmod{b}$; we call this a Carlitz triple (CT). The results of [2] of course apply to these triples. A primitive CT will be called a PCT.

In Section 2, we first prove some elementary arithmetic properties of a PCT, and then prove the following conjecture from [2]:

If (a, b, c) is a PCT with $a \neq b$, $c > 1$, $c \neq ab - 1$, then we have: $0 < a < c < b$.

In Section 3, we show that the set of all PCT's (a, ax, c) with $c > 2$, and for a fixed integer $x > 3$, satisfy a recursive relation. The original recursions (resulting directly from a study of these PCT's) are not very pretty, but they reduce to a surprisingly simple form.

In Section 4, we give the generating functions associated with the recurrences from Section 3; these are rational functions whose denominator is quadratic.

The reader will notice that many of our results are stated with assorted minor restrictions (e.g., $c > 1$, or $a < b$, and so on). In Section 5, we discuss the reasons for such restrictions. It is then seen that only one interesting case [out of all possible positive solutions to the system (*)] is not covered. This is the case of those PCT's of the form (a, a, c), to which, of course, the conjecture of DeLeon does not apply. We hope to say more about these in a later paper.

2. Elementary Properties

In this section we first develop some of the arithmetic consequences of the definition of a PCT (a, b, c). Recall that a CT is a triple of positive integers a, b, c satisfying:

$$a \le b$$

$$ab \equiv 1 \pmod{c}$$
$$c^2 \equiv 1 \pmod{a}$$
$$c^2 \equiv 1 \pmod{b}.$$

The PCT triples also satisfy the additional conditions

$$a \mid b$$

$$\gcd(a, (c^2 - 1)/b) = 1.$$

Lemma 2.1: Let (a, b, c) be a PCT with $c > 1$.

Then there exist integers x, r, u so that $x > 0$, $u > 0$, $r \ge 0$, and

(i) $b = ax$

(ii) $c^2 - 1 = ax(uc - a)$, $(a, u) = (a, uc - a) = 1$

(iii) $a^2x = 1 + rc$.

Proof: Since $a \mid b$, (i) is true for some $x > 0$. Then $ab = a^2x$ and (iii) follows since $ab \equiv 1 \pmod{c}$. We know that $b = ax$ divides $c^2 - 1$, that is, $c^2 - 1 = axt$ for some integer t; $t > 0$ since $c > 1$. Since $axt \equiv -1 \pmod{c}$ and $a^2x \equiv 1 \pmod{c}$, then $t \equiv -a \pmod{c}$. We claim that $t = uc - a$ with u a positive integer. If $c = 2$, this is seen directly: $c^2 - 1 = 3 = axt$ implies that a, x, and t can only take on the values 1 or 3. If $a = x = 1$, then $u = 2$; if $a = 3$, $x = 1$, $t = 1$, then $u = 2$; if $a = 1$, $x = 3$, $t = 1$, then $u = 1$. If $c > 2$, then since $t \equiv -a \pmod{c}$ and t, a, and c are all positive, then $t = uc - a$ for some $u > 0$. Note that r can be 0 if and only if $a = b = x = 1$; otherwise $r > 0$. □

Corollary 2.1: Let (a, b, c) be a PCT with $c > 1$, and suppose the integers x, r, u are given as in Lemma 2.1. Then $(uc - a, x(uc - a), c)$ is also a PCT with $c > 1$. □

Remark: Later on, for a given $x > 3$, we will be considering the set of all PCT's (a, b, c) for which $b/a = x$. It will be useful to note that, if (a, ax, c) is a PCT with $c > 2$, then one of the two PCT's (a, ax, c) and $(uc - a, x(uc - a), c)$ has its left-most member less than c. [This follows from Lemma 2.1(ii); $a(uc - a)$ divides $c^2 - 1$, so one of the factors must be less than c.]

Lemma 2.2: Let (a, b, c) be a PCT with $c > 1$, and suppose the integers x, r, u are given as in Lemma 2.1. Then

(i) $c = axu - r$

(ii) $(ru - a)c = ar - u$

(iii) $(a^2 - u^2)(r^2 - 1) = (c^2 - 1)(ru - a)^2$.

Proof: From the proof of Lemma 2.1, we have $x = b/a$, $r = (ab - 1)/c$, and $u = (c^2 - 1 + ab)/bc$. The result follows easily from these equalities. □

Theorem 2.1: Let (a, b, c) be a PCT with $a > 1$ and $c > 1$, and suppose the integers x, r, u are given as in Lemma 2.1. Then $r > 1$, and (a, b, r) is a PCT.

Proof: First, since $a > 1$, then $a^2x = 1 + rc > 1$ [Lemma 2.1(iii)] and so $r > 0$. Now consider Lemma 2.2(ii) with $r = 1$. It reduces to $(u - a)c = a - u$. We have $c > 0$, so this implies $a = u$. But $(a, u) = 1$ by Lemma 2.1(ii), and so $u = 1$ and $a = 1$, contradicting the assumption that $a > 1$; thus $r > 1$. Next, since $a^2x = 1 + rc$ and $c = axu - r$, then

$$a^2x = 1 + r(axu - r) = 1 + (uax)r - r^2$$

$$ax(a - ur) = 1 - r^2$$

and so $r^2 \equiv 1 \pmod{a}$ and $r^2 \equiv 1 \pmod{b}$ (since $b = ax$).

From Lemma 2.1(iii) we already have $ab = a^2x \equiv 1 \pmod{r}$. It remains to show that (a, b, r) is primitive, that is (see [2]), that

$$\gcd(a, (r^2 - 1)/ax) = \gcd(a, ru - a) = 1.$$

From Lemma 2.1(ii) and the fact that (a, b, c) is primitive, we have

$$\gcd(a, u) = 1.$$

Lemma 2.1(iii) implies that

$$\gcd(a, r) = 1.$$

Then $\gcd(a, ru - a) = 1$ also. □

The following theorem settles the conjecture of DeLeon in the affirmative.

Theorem 2.2: Let (a, b, c) be a PCT with $0 < a < b$ and $c > 1$. If $a < c$, then $b > c$.

Proof: First, if $a = 1$, then we have, by Lemma 2.1(iii), that $a^2x = x = 1 + rc$. Since $b = ax$, and $b > 1$, then $r > 0$ and so $b \geq c + 1$. Thus, the theorem is true for $a = 1$ and $c > 2$. For $a > 1$, the proof is by descent. (We use the notation of Lemma 2.1.) Suppose the contrary, and let c be the smallest positive integer such that there exist integers a, x so that, with $b = ax$, one has that (a, b, c) is a PCT with $a < c$ and $b < c$, $a < b$ and $c > 1$. Note now that, since we have $b > a$, then $x > 1$. Since $ax < c$, then $a^2x < ac$. Then

$$a^2x = 1 + rc < ac,$$

and hence $r < a$. By Theorem 2.1, (a, ax, r) is also a PCT and has $r > 1$, and by Corollary 2.1, $(a', b', c') = (ru - a, x(ru - a), r)$ is a PCT. Since $a > r$, and since $r^2 - 1 = ax(ru - a)$ then $x(ru - a) < r$. Thus,

$$a' < c',\ b' < c',\ a' < b', \text{ and } r > 1.$$

We have $r < a \leq ax < c$, which contradicts the minimality of c. This completes the proof. □

Corollary 2.2: Let (a, b, c) be a PCT with $0 < a < b$, and with $c > 1$, and suppose the integers x, r, u are given as in Lemma 2.1. Assume that $a < c$. Then $u = 1$.

Proof: By Theorem 2.2, $ax > c$, so from Lemma 2.1(ii) it follows that

$$0 < uc - a < c.$$

Since $a < c$, then it must be that $u = 1$. □

3. The Recursion for PCT's

Consider the set $S(t)$ of all PCT's of the form $(a, a(t+1), c)$, where $c > 2$ and $t > 2$. In this section, we show that for each $t > 2$, $S(t)$ is a recursively defined sequence of triples, with initial element $(1, t+1, t)$.

These conditions of course imply that Theorem 2.2 and its Corollary will apply to all these PCT's. In particular, in the notation of Lemma 2.1, for any PCT (a, b, c) in this section we will always have $u = 1$.

Lemma 3.1: Let (a, b, c) be a PCT with $a < b$ and $c > 2$, and r as defined in Lemma 2.1. If $a < c/2$, then $r \le c - 2$; if $a > c/2$, then $r > c$.

Proof: We use the notation of Lemma 2.1. Note that

$$(r+1)(c+1) = rc + 1 + r + c.$$

By Corollary 2.2, $u = 1$ and so, from Lemma 2.2(i), $ax = r + c$.

By Lemma 2.1(iii), $a^2x = rc + 1$. Hence, we have

$$(r+1)(c+1) = a^2x + ax = ax(a+1).$$

If $a < c/2$, then $a + 1 \le c - a$. Then,

$$(r+1)(c+1) \le ax(c-a) = c^2 - 1,$$

which implies that $r \le c - 2$; similarly, if $c/2 < a < c$, then $a + 1 > c - a$, and then $r > c - 2$. Note that $a = c/2$ is not possible if c is odd; if c is even and $c > 2$, then $(a, c) = 1$ implies that $a \ne c/2$. [Lemma 2.1(iii) implies that $(a, c) = 1$.] By Lemma 2.2(ii), since $u = 1$, we have

$$(r-a)c = ar - 1,$$

so that $(r, c) = 1$ and hence $r \ne c$. It remains to show that $r \ne (c-1)$. Suppose to the contrary that $r = c - 1$. By Lemma 2.2(i) then, $ax = 2c - 1 > 3$. Since ax must divide $c^2 - 1$, while $\gcd(2c-1, c-1) = 1$, then $2c - 1$ must divide $c + 1$; this is impossible for $c > 2$. Thus, $r \ne c - 1$, and it follows that $r > c$. □

Lemma 3.2: Suppose that (a, ax, r) and (a, ax, k) are both PCT's with $r, k > 2$ and $x > 3$, and that $r \ne k$. Then $a^2x = 1 + rk$, and $r + k = ax$.

Proof: By Corollary 2.2, $u = 1$. Then, from Lemmas 2.1 and 2.2, we must have:

$$r^2 - 1 = ax(r-a)$$
$$a^2x = 1 + rm \text{ (for some positive integer } m)$$
$$r + m = ax$$
$$k^2 - 1 = ax(s-a)$$
$$a^2x = 1 + kn \text{ (for some positive integer } n)$$
$$k + n = ax.$$

Then

$$a^2x = 1 + m(ax - m) = 1 + n(ax - n),$$

and then

$$(m-n)ax = m^2 - n^2,$$

which gives $ax = m + n$. Then $k = m$ and $r = n$. □

Lemma 3.3: If (a, ax, c) is a PCT with $c > 2$ and $x > 3$, and if $a^2x = 1 + rc$, then $r \ne c$.

Proof: If $r = 1$, clearly $r \neq c$. Suppose $r > 1$. Since $a^2x = 1 + rc$ implies that $(a, r) = 1$ and $r > 1$, then $r \neq a$. By Lemma 2.2 and Corollary 2.2,

$$(r - a)c = ra - 1.$$

Thus, r and c must be relatively prime. Since $c > 1$, then $r \neq c$. □

Corollary 3.3: Suppose that (a, ax, c) is a PCT with $c > 2$ and $x > 3$, and with $a^2x = 1 + rc$ and $a > c/2$. Then the PCT (a, ax, r) has $r > c$ and $a < r/2$.

Proof: For the PCT (a, b, c), Lemma 3.1 says that $r > c$. Applying Lemma 3.1 to the PCT (a, b, r) completes the proof. □

Remark: Observe that, given any PCT (a, b, c) with $b/a = x > 3$ and $c > 2$, there are two more PCT's particularly associated with it, in which the quotient of the second element by the first is also x, namely

$$(c - a, (c - a)x, c) \quad \text{and} \quad (a, b, r).$$

By Lemmas 3.1 and 3.2, there are exactly two such triples, and, in the lexicographic ordering of all triples, one of these associated triples is "less than" (a, b, c), and the other one is "greater."

Example: $x = 5$; $c_0 = 4 = x - 1$; $a = 1$. Then $(1, 5, 4)$ is a PCT;

$$a^2x = 5 = 1 + 4.$$

Also $(3, 15, 4)$ is a PCT so we have $a = 3$ and

$$a^2x = 45 = 1 + 4 \times 11.$$

[Note that $3 = c_0 - 1$, and $11 = c_0^2 - c_0 - 1 = c_1$.]

Now $(3, 15, 11)$ is a PCT (Theorem 2.1). Wishing still to go up, use the related PCT $(8, 40, 11)$ (Corollary 2.1); then $a = 8$ and we have

$$a^2x = 1 + 11 \times 29.$$

Put $c_2 = 29$.

[Note that $8 = 11 - 3 = (c_1 - c_0 + 1)$.]

We now have that $(8, 40, 29)$ and $(21, 5 \times 21, 29)$ are PCT's. With $a = 21$, then

$$a^2x = 1 + 29 \times 76.$$

Put $c_3 = 76$.

[Note that $21 = c_2 - c_1 + c_0 - 1$.]

For convenience, we state this rather commonplace observation as a theorem.

Theorem 3.1: The set $S(t)$ of all PCT's $(a, a(t + 1), c)$ with $a > 0$, $c > 2$, $t > 2$, is linearly ordered by the lexicographic order:

$$A_0, A_1, A_2, \ldots,$$

where $A_0 = (1, t + 1, t)$, and if $A_n = (a, a(t + 1), c)$ with $a < c/2$, then

$$A_{n+1} = (c - a, (c - a)(t + 1), c);$$

if $A_n = (a, a(t + 1), c)$ with $a > c/2$, then

$$A_{n+1} = (a, a(t + 1), (a^2(t + 1) - 1)/c). \quad □$$

The first few members of $\{A_i\}$ are:

$$A_0 = (1,\ t + 1,\ t)$$
$$A_1 = (t - 1,\ (t - 1)(t + 1),\ t)$$
$$A_2 = (t - 1,\ (t - 1)(t + 1),\ t^2 - t - 1)$$
$$A_3 = (t^2 - 2t,\ (t^2 - 2t)(t + 1),\ t^2 - t - 1).$$

Let $(x_0, x_1, x_2, \ldots)$ be the sequence of the left-hand entries of the A_i, and define a sequence (a_n) as follows:

$$a_0 = 1,\ a_1 = t - 1,$$

and then, for all $i > 1$, $a_i = x_{2i-1}$. That is, (a_n) is the sequence of the distinct left-hand entries of the triples A_i. We proceed similarly on the right; it will be convenient to furnish this sequence with an "extra" initial term:

$$c_0 = 1,\ c_1 = t,\ c_2 = t^2 - t - 1,\ \ldots .$$

From the definition, we have that

$$a_n = c_n - a_{n-1} \quad \text{and} \quad c_{n+1} = (a_n^2 (t + 1) - 1)/c_n.$$

Theorem 3.2: For fixed t, $t > 2$, the sequences $\{a_n\}$ and $\{c_n\}$ defined above satisfy

(i) $a_n = c_n - c_{n-1} + \cdots + (-1)^j c_{n-j} + \cdots + (-1)^n \quad (n \geq 0)$

(ii) $c_{n+1} = (t + 1)c_n - 2(t + 1)a_{n-1} + c_{n-1} \quad (n \geq 1)$.

Proof: Since $a_0 = 1 = (-1)^0$, then (i) follows by induction from the definition of $\{A_i\}$.

We have $c_0 = 1$, and $c_1 = t$, so

$$c_2 = t^2 - t - 1 = (t + 1)c_1 - 2(t + 1)a_0 + c_0.$$

From the definition of $\{A_i\}$, if $n > 2$, we have

$$\begin{aligned} c_n &= \{(t + 1)(c_{n-1} - c_{n-2} + \cdots + (-1)^n)^2 - 1\}/c_{n-1} \\ &= [(t + 1)\ c_{n-1}^2 + 2c_{n-1}(-c_{n-2} + c_{n-3} - \cdots + (-1)^n \\ &\qquad + (-c_{n-2} + c_{n-3} + \cdots + (-1)^n)^2 - 1]/c_{n-1} \\ &= (t + 1)c_{n-1} + 2(t + 1)(-c_{n-2} + c_{n-3} - \cdots + (-1)^n) \\ &\qquad + \{(t + 1)(-c_{n-2} + c_{n-3} - \cdots + (-1)^n)^2 - 1\}/c_{n-1} \\ &= (t + 1)c_{n-1} + 2(t + 1)(-a_{n-1}) + \{(t + 1)(a_{n-2})^2 - 1\}/c_{n-1}. \end{aligned}$$

From the definition of $\{A_i\}$, we know that

$$\{(t + 1)(a_{n-2})^2 - 1\}/c_{n-2} = c_{n-1},$$

and this proves (ii). □

Using this result, one can establish that the sequences $\{a_n\}$ and $\{c_n\}$ do in fact satisfy recursions of a much simpler nature.

Theorem 3.3: For fixed t, $t > 2$, the sequences $\{a_n\}$ and $\{c_n\}$ satisfy, for $n \geq 1$:

(i) $c_{n-1} + c_n = (t + 1)a_{n-1}$

(ii) $a_{n+1} = (t - 1)a_n - a_{n-1}$

(iii) $c_{n+1} = (t - 1)c_n - c_{n-1}$.

Proof: It is easy to verify that (i), (ii), (iii) are all true for $n = 1, 2, 3$. Suppose they are true for all k, $1 \le k \le n$. From Theorem 3.2 and the inductive hypothesis, we have

$$\begin{aligned} c_{n+1} &= (t + 1)c_n + 2(t + 1)(-a_{n-1}) + c_{n-1} \\ &= (t + 1)c_n - 2(c_n + c_{n-1}) + c_{n-1} \\ &= (t - 1)c_n - c_{n-1}. \end{aligned}$$

It then follows that

$$\begin{aligned} c_{n+1} + c_n &= tc_n - c_{n-1} = (t + 1)c_n - c_n - c_{n-1} \\ &= (t + 1)(c_n - a_{n-1}) = (t + 1)a_n. \end{aligned}$$

Since $a_n = c_n - a_{n-1}$, statement (ii) follows from (iii); this completes the proof. □

4. Generating Functions

It is well known that recursive sequences like $\{a_n\}$ and $\{c_n\}$ are naturally associated with generating functions, which may be found and described in a standard way. In this section we give the generating functions and the corresponding Binet formulas without proof.

Let t be a fixed integer, $t > 2$, and consider the sequences $\{a_n\}$ and $\{c_n\}$ defined in Section 3. Define two formal power series by

$$F(z) = \sum_{i=0}^{\infty} c_i z^i; \quad G(z) = \sum_{i=0}^{\infty} a_i z^i.$$

Theorem 4.1: The series defined above satisfy

$$F(z) = (1 + z)/(1 + (1 - t)z + z^2); \quad G(z) = F(z)/(1 + z). \ \square$$

If $t = 3$, then

$$z^2 + z(1 - t) + 1 = (z - 1)^2,$$

while, if $t > 3$, then $z^2 + z(1 - t) + 1$ has irrational roots. Thus, we consider two cases separately.

Theorem 4.2: If $t = 3$, then

$$F(z) = \sum(i + 1)z^i;$$

$a_n = n + 1$ and $c_n = 2n + 1$. □

Theorem 4.3: Let $t > 3$, and let α, β be the two roots of $z^2 + (1 + t)z + 1$. Then $\alpha \ne \beta$, and we have

$$a_n = (\alpha^{n+1} - \beta^{n+1})/(\alpha - \beta)$$

and

$$c_n = (\alpha^{n+1} + \alpha_n - \beta^{n+1} - \beta_n)/(\alpha - \beta). \ \square$$

5. Some Exceptions

In this section we discuss the reasons for the restrictive conditions attached to some of our results. Throughout we use the notation of Lemma 2.1; (a, b, c) is a PCT, a, b, c are positive integers, and so on.

A. If $c = 1$: For all positive a, b, $(a, b, 1)$ is a CT and is primitive if and only if $a = 1$.

B. If $c = 2$: The only PCT's with $c = 2$ are $(1, 1, 2)$, $(1, 3, 2)$, and $(3, 3, 2)$.

C. If $c > 2$, there are no PCT's of the form $(a, 2a, c)$ or $(a, 3a, c)$.

D. There are PCT's of the form (a, a, c), for instance $(8, 8, 3)$. However, these seem to differ from those with $a < b$ in various essential ways; in particular, they do not appear to fit into a single recurrence scheme. Note that DeLeon's conjecture does not apply to these PCT's.

Statements (A) and (B) are easily checked. To see (C), suppose first that $(a, 2a, c)$ is a PCT with $c > 2$. Then, by Theorem 2.2, we have $a < c < 2a$; and by Corollary 2.2 and Lemma 2.1, we can write

$$c^2 - 1 = 2a(c - a) = 2ac - 2a^2.$$

Rearranging, we get

$$c^2 - 2ac + a^2 = 1 - a^2$$

$$(c - a)^2 = 1 - a^2.$$

Since $c > a$, this is positive, contradicting the fact that $a > 0$. Therefore, $(a, 2a, c)$ can only be a PCT if $c = 1, 2$.

Proceeding similarly with a PCT of the form $(a, 3a, c)$ with $c > 2$, we get $a < c < 3a$ and

$$c^2 - 1 = 3a(c - a)$$

$$(c - a)^2 = 1 + a(c - 2a).$$

Since $c > a$, this is positive, so $c \geq 2a$. Rearranging the first equation in another way, we get

$$c^2 - 3ac + 2a^2 = 1 - a^2$$

$$(c - a)(c - 2a) = 1 - a^2.$$

Since $c \geq 2a$, we must have $a = 1$. A CT (a, b, c) must satisfy $ab \equiv 1 \pmod{c}$ and $c^2 \equiv 1 \pmod{a, b}$. Here we have $a = 1$, $b = 3$; then $ab \equiv 1 \pmod{c}$ implies $c \leq 2$. Thus, there are no PCT's with $c > 2$ and the form $(a, 3a, c)$.

References

1. L. Carlitz. "An Application of the Reciprocity Theorem for Dedekind Sums." *Fibonacci Quarterly* *22* (1984).
2. M. J. DeLeon. "Carlitz Four-Tuples." *Fibonacci Quarterly* (to appear).

*****

NIVEN REPUNITS AND $10^n \equiv 1 \pmod{n}$

Robert E. Kennedy and Curtis N. Cooper
Central Missouri State University, Warrensburg, MO 64093
(Submitted March 1987)

1. Introduction

A positive integer which is divisible by its digital sum is called a Niven number. This concept was introduced in [1], and was investigated in greater detail in [2], [3], and [4]. A variety of results and open questions were presented in these articles. One problem, however, that was not completely resolved was a characterization of Niven repunits. That is, Niven numbers whose decimal representation is all ones. For example, the repunits 1, 111, 111111111, and 111111111111111111111111111 (27 ones) are the first four Niven repunits. Here, we will give a complete characterization of such integers. In addition, it will be pointed out how all Niven repunits can be constructed from a certain list of primes.

To facilitate the following discussion, we use the notation $R(n)$ to represent the repunit made up of n ones. Thus

$$R(n) = \frac{1}{9}(10^n - 1)$$

and so, we wish to determine under which conditions

$$R(n) \equiv 0 \pmod{n}. \tag{1.1}$$

2. A Useful Lemma

A particular instance of the following lemma will be useful in proving a characterization theorem for Niven repunits.

Lemma 2.1: Let a, b, m, and n be positive integers. If $a \equiv b \pmod{m^n}$, then

$$a^{m^k} \equiv b^{m^k} \pmod{m^{k+n}}$$

for each nonnegative integer k.

Proof: By observing the factorization,

$$a^{m^{k+1}} - b^{m^{k+1}} = (a^{m^k} - b^{m^k})[(a^{m^k})^{m-1} + (a^{m^k})^{m-2}(b^{m^k}) + \cdots + (b^{m^k})^{m-1}],$$

the proof follows by induction on k.

For convenience, we state a special case of Lemma 2.1 as Lemma 2.2.

Lemma 2.2: Let m, n, and t be positive integers. Then $10^t \equiv 1 \pmod{m^n}$ implies that

$$(10^t)^{m^k} \equiv 1 \pmod{m^{k+n}}$$

for each nonnegative integer k.

3. The Characterization Theorem

Using Lemma 2.2, we can now prove the following theorem, which gives necessary and sufficient conditions in order that (1.1) is true.

Theorem: Let n and 10 be relatively prime. Denote the order of 10 (mod n) by $e_n(10)$. Then the following statements are equivalent.

(1) $R(n)$ is a Niven repunit.

(2) $10^n \equiv 1 \pmod{n}$.

(3) $n \equiv 0 \pmod{e_n(10)}$.

(4) $n \equiv 0 \pmod{e_p(10)}$ for each prime factor p of n.

Proof: That (1) ⇒ (2) ⇒ (3) ⇒ (4) is a direct application of congruence arithmetic and Fermat's Theorem. Thus, we need only prove that (4) ⇒ (1).

Suppose that $n \equiv 0 \pmod{e_p(10)}$ for each prime factor p of n. Let m be the least prime factor of n. Then, since $e_m(10) < m$ and, by the hypothesis $e_m(10)$ is also a factor of n, we have that $e_m(10)$ must be 1. This can only occur when $m = 3$.

So, we may write the prime factorization of n in the form

$$3^k \prod_{i=1}^{t} p_i^{k_i}, \text{ where } 3 < p_1 < p_2 < p_3 < \cdots < p_t.$$

Thus, $n \equiv 0 \pmod{e_{p_i}(10)}$ for $i = 1, 2, 3, \ldots, t$ and since

$$10^{e_{p_i}(10)} \equiv 1 \pmod{p_i}$$

for each i, we have that $10^n \equiv 1 \pmod{p_i}$ for each i. But by Fermat's Theorem,

$$10^{p_i - 1} \equiv 1 \pmod{p_i}$$

and so, $e_{p_i}(10)$ divides $p_i - 1$ for each i. Thus,

$$10^{(n,\, p_i - 1)} \equiv 1 \pmod{p_i}$$

for each i where, as usual, $(n, p_i - 1)$ denotes the greatest common factor of n and $p_i - 1$. But, since $(n, p_i - 1)$ is a factor of $n/p_i^{k_i}$, we have

$$10^{n/p_i^{k_i}} \equiv 1 \pmod{p_i}$$

for each i. Noting that

$$10^{n/3^k} \equiv 1 \pmod{3^2},$$

we have, by Lemma 2.2, that

$$(10^{n/p_i^{k_i}})^{p_i^{k_i}} \equiv 1 \pmod{p_i^{k_i+1}}$$

for each i, and

$$(10^{n/3^k})^{3^k} \equiv 1 \pmod{3^{k+2}}.$$

Therefore,

$$10^n \equiv 1 \pmod{p_i^{k_i}}$$

for each i, and

$$10^n \equiv 1 \pmod{3^{k+2}}.$$

It follows that $10^n \equiv 1 \pmod{3^2 n}$ and so

$$\frac{1}{9}(10^n - 1) \equiv 0 \pmod{n}.$$

Therefore, $R(n)$ is a Niven repunit, and we have that (4) $\Rightarrow$ (1).

An immediate corollary to the theorem is that $R(3^t)$ is a Niven repunit for every nonnegative integer t. This follows from the fact that $e_3(10) = 1$ and statement (4) of the theorem. In fact, statement (4) gives the most useful characterization of Niven repunits.

4. Generation of Niven Repunits

Using statement (4) of the theorem, we can construct all n such that $R(n)$ is Niven by determining which primes, p, are such that every prime factor of $e_p(10)$ also satisfies the condition of statement (4). For example, since $e_3(10) = 1$, as has already been pointed out every power of 3 is a Niven repunit. But since $e_7(10) = 6$ has a factor of 2, it follows that no multiple of 7 can satisfy statement (4). That is, $R(7m)$ can never be a Niven repunit. In fact, the first prime larger than 3 that can be a factor of an n that satisfies statement (4) is 37. This follows because $e_{37}(10) = 3$ and, as stated above, 3 is a prime that must be a factor of every n that satisfies statement (4) of the theorem.

Similarly, it is found that the next two primes, after 37, which could possibly be factors of an n such that $R(n)$ is Niven are 163 and 757 since

$$e_{163}(10) = 3^4 \quad \text{and} \quad e_{757}(1) = 3^3.$$

The first column in the following table gives all primes, less than 50,000, which could possibly be factors of an n that satisfies statement (4). The second column gives the corresponding $e_p(10)$.

TABLE 4.1

prime p	$e_p(10)$
3	1
37	3
163	$81 = 3^4$
757	$27 = 3^3$
1999	$999 = (3^3)(37)$
5477	$1369 = 37^2$
8803	$1467 = (3^2)(163)$
9397	$81 = 3^4$
13627	$6813 = (3^2)(757)$
15649	$489 = (3)(163)$
36187	$18093 = (3)(37)(163)$
40879	757

It should be noted that an infinitude of such primes exist, since $e_p(10)$ is a power of 3 infinitely often. As an example, suppose that 757 is the largest prime factor of n. Then in order that $R(n)$ be a Niven repunit, n would have to be of the form

$$3^{n_1}37^{n_2}163^{n_3}757^{n_4}$$

where the exponents are necessarily interdependent. That is, if $n_3 \neq 0$, then, by inspection of the right column of Table 4.1, $n_1 \geq 4$. So, a list of generators of Niven repunits can be continuously constructed by consideration of Table 4.1. The first few of such a list is given in Table 4.2.

TABLE 4.2

3
(3)(37)
(3^4)(163)
(3^3)(757)
(3^3)(37)(1999)
(3)(37^2)(5477)
(3^4)(163)(8803)
(3^4)(9397)
(3^3)(757)(13627)
(3)(163)(15649)

For example, the product $(3^4)(163)(8803)$ is in the list given by Table 4.2 because

$$e_{8803}(10) = 1467 = (3^2)(163)$$

and each of its prime factors is in the list given by Table 4.1. So, if 8803 is the largest admissible prime factor of n, 163 would also have to be a factor which, in turn, forces 3^4 to be a factor of n. The phrase, ". . . generators of Niven repunits . . ." is used because *increasing the exponents of any of the prime factors of the least common multiple of any collection chosen from the list given in Table 4.2 will be an* n *such that* R(n) *is a Niven repunit.* For example

$$\text{lcm}((3^4)(163), (3^3)(757), (3^3)(757)(13627)) = (3^4)(163)(757)(13627)$$

and so

$$R(3^{n_1}163^{n_2}757^{n_3}13627^{n_4})$$

will be a Niven repunit for any $n_1 \geq 4$, $n_2 \geq 1$, $n_3 \geq 1$, and $n_4 \geq 1$.

5. Concluding Remarks

As pointed out, the list of primes given by Table 4.1 can be extended by inspecting $e_p(10)$ for primes p. A useful reference for finding such primes has been published by Yates [5]. For example, he has calculated that, for the prime 333667,

$$e_{333667}(10) = 9 = 3^2.$$

Hence, 333667 may be added to the list given by Table 4.1 since 3 is already listed in Table 4.1.

Finally, it should be mentioned that since, for any decimal digit $d \neq 0$,

$$\frac{d}{9}(10^n - 1) \equiv 0 \pmod{dn}$$

if and only if $R(n) \equiv 0 \pmod{n}$, the characterization theorem for repunits also gives a complete characterization for what could be called "Niven repdigits."

References

1. R. E. Kennedy, T. A. Goodman, & C. H. Best. "Mathematical Discovery and Niven Numbers." *MATYC Journal* *14* (1980):21-25.
2. R. E. Kennedy & C. N. Cooper. "On the Natural Density of the Niven Numbers." *College Math. Journal* *15* (1984):309-312.
3. C. N. Cooper & R. E. Kennedy. "On an Asymptotic Formula for the Niven Numbers." *Internat. J. Math. & Math. Sci.* *8* (1985):537-543.

4. C. N. Cooper & R. E. Kennedy. "A Partial Asymptotic Formula for the Niven Numbers." *Fibonacci Quarterly* 26.2 (1988):163-168.
5. S. Yates. *Prime Period Lengths*. 1975.

*****

OPERATIONS ON GENERATORS OF UNITARY AMICABLE PAIRS

Rudolph M. Najar
University of Wisconsin-Whitewater, Whitewater, WI 53190
(Submitted March 1987)

0. Introduction

McClung [3] defined a *generator* (of unitary amicable pairs) as a pair (f, k) where f is a rational not one and k and fk are integers such that

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

The utility of this concept arises in that if $m = km'$ and $n = kn'$ are unitary amicable numbers with

$$(k, m'n') = 1 = (fk, m'n'),$$

then fkm' and fkn' are also unitary amicable numbers. McClung found sixteen generators which he applied to the unitary amicable pairs in the Hagis list [1] to produce 25 unitary amicable pairs of which 3 are new.

In Section 1, properties of generators are investigated. An equivalence relation is defined on the set of generators. A product of two generators is defined, but not everywhere, which is consistent with the equivalence relation and so yields a product of classes, also not everywhere defined.

Section 2 is devoted to methods of producing generators. The action of classes of generators on unitary amicable pairs is defined and the properties are examined. The section closes with a table of generators.

Section 3 briefly indicates how the methods of Section 2 apply to unitary sociable sets, defined in [2].

H. J. J. te Riele, [5], [6], used number pairs (a, b), satisfying

$$\sigma^*(a)/a = \sigma^*(b)/b,$$

to generate hundreds of new unitary amicable pairs. One can define a binary operation and an equivalence relation on the set of all such pairs which yield stuctures isomorphic to those developed here for generators. Both te Riele [7] and McClung [4] were aware of the equivalence of the two methods. Apparently, neither developed the structures of the te Riele pairs to the extent this paper does for the McClung generators.

A paper in progress will extend and generalize this one.

1. Properties and Operations

It is assumed that the reader is familiar with McClung's results and notation [3]. To avoid confusion, $\gcd(a, b)$ wil denote the greater common divisor of a and b. $\operatorname{gucd}(a, b)$ will denote the greatest unitary common divisor. The notation (f, k) will be reserved for generators.

A prime p divides f if it divides either the numerator or the denominator of f. The expression "p is (not) in f" means that "p does (not) divide f." m is said to be relatively prime to f, i.e., $\gcd(m, f) = 1$, if no prime p divides both m and f.

If a prime p is relatively prime to fk but not to k, then it divides f.

Extend the definition of a generator as follows.

Definition 1: A pair of integers of the form $(1, k)$ will be called a *trivial generator*.

When applied to a given unitary amicable pair, a trivial generator does not generate a different unitary amicable pair. The two integers of a trivial generator are relatively prime. So on eliminating extraneous primes, one gets $(1, 1)$.

Theorem 1: a. (f, k) is a generator iff $(1/f, fk)$ is a generator.

b. Let p be a prime which does not divide f. Then, (f, kp^a) is a generator for all positive integers a.

Proof: a. f is a rational not one and k and fk are integers.

$$\sigma^*(fk) = f\sigma^*(k) \text{ iff } \sigma^*(k) = (1/f)\sigma^*(fk)$$
$$\text{iff } \sigma^*((1/f)(fk)) = (1/f)\sigma^*(fk).$$

$1/f$ is a rational not one and fk and $(1/f)(fk) = k$ are both integers. $(1/f, fk)$ is a generator. The argument is reversible.

b. If $p \nmid k$,

$$\sigma^*(fkp^a) = \sigma^*(fk)\sigma^*(p^a) = f\sigma^*(k)\sigma^*(p^a) = f\sigma^*(kp^a).$$

If $p \mid k$, set $k = k'p^b$, $\gcd(k', p) = 1$. By McClung's Lemma 2, (f, k') is a generator. By the previous case,

$$(f, kp^a) = (f, k'p^{a+b})$$

is a generator. □

Compare with McClung's Lemma 2. In effect, for any prime p which does not divide f, one can divide or multiply k by any power of p that yields an integer and thereby produce a new generator.

Since there are countably infinitely many primes p and prime powers p^a, each generator (f, k) has countably infinitely many generators (f, kp^a), $p \nmid f$, associated to it.

Definition 2: For (f, k), the generator $(1/f, fk)$ is called the *inverse* or *reciprocal generator* and is written $(f, k)^{-1}$.

Note that $(1, k)^{-1} = (1, k)$ and that $(1/f, fk)^{-1} = (f, k)$. Trivial generators are their own inverses. The inverse of the inverse is the initial generator.

Definition 3: A generator (f_1, k_1) is said to be *related* to a generator (f_2, k_2) iff (a) $f_1 = f_2$; and (b) there exist integers m and n both relatively prime to f_1, so that $mk_1 = nk_2$.

Theorem 2: The relation of Definition 3 is an equivalence relation.

Proof: Obvious. □

Definition 4: A generator (f, k) is said to be *primitive* if there does not exist a prime p, $p^a \| k$, $p \nmid f$, such that (f, kp^{-a}) is a generator.

Essentially, a generator is primitive iff k has no extraneous primes. Several properties are immediate consequences of Definition 3, Theorem 2, and Definition 4.

Trivial generators form an equivalence class.

Each generator (f, k) has a unique primitive generator associated to it by eliminating extraneous primes.

Each equivalence class has one and only one primitive generator.

For a primitive generator, if $p|k$, then $p|f$. Thus, $\pi(k) \le \pi(f)$.

$$(f, k) \text{ is primitive iff } (1/f, fk) = (f, k)^{-1} \text{ is primitive.}$$

Primitive generators are the natural representatives for the equivalence classes. Upper case letters (F, K) will be used for primitive generators. The primitive generator associated to an arbitrary generator (f, k) will be denoted by $\underline{(f, k)}$; the equivalence class, by $\langle (f, k) \rangle$. Arbitrary equivalence classes will be denoted by C_i.

McClung's conjectures can be stated in stronger form by using reciprocals and primitives. Even then, they are false.

Conjecture 1: Up to reciprocals, the only primitive generator (F, K) with $\pi(F) = \pi(K) = 2$ is $(3/2, 12)$.

$$\left(\frac{1}{2 \cdot 17}, 2^4 \cdot 17\right) \text{ is a counterexample.}$$

Conjecture 2: There are no primitive generators (F, K) with $\pi(F) > 2$ or $\pi(K) > 2$.

$$\left(\frac{2^3 \cdot 3 \cdot 5 \cdot 11 \cdot 43}{17}, 2^4 \cdot 3 \cdot 17\right) \text{ is a counterexample.}$$

Definition 5: Let (f_1, k_1) and (f_2, k_2) be two generators such that $k_2 = f_1 k_1$. Then the *product* of (f_1, k_1) and (f_2, k_2), in that order, is defined and given by

$$(f_1, k_1) \times (f_2, k_2) = (f_1 f_2, k_1).$$

Lemma 1: The product $(f_1 f_2, k_1)$ of two generators (f_1, k_1) and (f_2, k_2) is a generator. The product is trivial iff the factors are reciprocals.

Proof: k_1 and $f_1 f_2 k_1 = f_2 k_2$ are integers. We must show that

$$\sigma^*(f_1 f_2 k_1) = f_1 f_2 \sigma^*(k_1);$$

$$\sigma^*(f_1 f_2 k_1) = \sigma^*(f_2 k_2) = f_2 \sigma^*(k_2) = f_1 f_2 \sigma^*(k_1).$$

If the factors are reciprocals, the product is obviously trivial. Suppose the product is trivial. Then, $f_1 f_2 = 1$ and $f_2 = 1/f_1$. Substituting, the factors become (f_1, k_1) and $(1/f_1, f_1 k_1)$. □

From Definition 5, it is obvious that the product is not defined for every pair of generators. The product of $(2 \cdot 5, 2)$ and $(3 \cdot 41, 3^3)$ does not exist in either order. When the product does exist, it need not be commutative.

$$(2 \cdot 17, 2^3) \times \left(\frac{2 \cdot 11}{17}, 2^4 \cdot 17\right) = (2^2 \cdot 11, 2^3)$$

but is not defined in the opposite order.

For a generator (f, k), the trivial generator $(1, k)$ is a left identity, and $(1, fk)$ is a right identity.

Where sufficiently defined, the product is associative. Let (f_i, k_i), $i = 1, 2, 3$ be generators such that the products $(f_1, k_1) \times (f_2, k_2)$ and $(f_2, k_2) \times (f_3, k_3)$ exist. Then the product of the three is associative; i.e.,

$$((f_1, k_1) \times (f_2, k_2)) \times (f_3, k_3) = (f_1, k_1) \times ((f_2, k_2) \times (f_3, k_3)).$$

It is a simple matter to follow both sides through to $(f_1f_2f_3, k_1)$. The conditions necessary for each intermediate step obtain.

The reciprocal of a product is the product of the reciprocals in the reverse order.

$$((f_1, k_1) \times (f_2, k_2))^{-1} = (f_1f_2, k_1)^{-1} = (1/f_1f_2, f_1f_2k_1);$$
$$(f_2, k_2)^{-1} \times (f_1, k_1)^{-1} = (1/f_2, f_2k_2) \times (1/f_1, f_1k_1)$$
$$= (1/f_1f_2, f_2k_2) = (1/f_1f_2, f_1f_2k_1).$$

The equality $f_1k_1 = (1/f_2)(f_2k_2)$ must hold for the product of the reciprocals to exist. But $f_1k_1 = k_2 = (1/f_2)(f_2k_2)$. The product is defined!

Lemma 2: Let (f_i, k_i), $i = 1, 2, 3, 4$, be generators such that:

a. (f_1, k_1) is equivalent to (f_2, k_2); (f_3, k_3) to (f_4, k_4); and

b. the products $(f_1, k_1) \times (f_3, k_3)$ and $(f_2, k_2) \times (f_4, k_4)$ exist. Then, the products are equivalent.

Proof: By Definition 3, $f_1 = f_2$ and $f_3 = f_4$, so $f_1f_3 = f_2f_4$. Also, there exist integers m and n, both relatively prime to f_1 so that $mk_1 = nk_2$, and p and q, both relatively prime to f_3, so that $pk_3 = qk_4$. Assume m and n are relatively prime and p and q also. Otherwise, divide out the gcd's. As $k_3 = f_1k_1$ and $k_4 = f_2k_2$, $pf_1k_1 = qf_2k_2$ and $pk_1 = qk_2$. $k_1 = (q/p)k_2$ and $m(q/p)k_2 = nk_2$. $mq = pn$. m must divide p. Say $p = am$. $mq = amn$ and $q = an$. Thus, a divides $\gcd(p, q) = 1$, $a = 1$, $q = n$, and $p = m$. m and n are then relatively prime to both f_1 and f_3, hence to f_1f_3, and satisfy the condition for equivalence. □

Definition 6: Let C_1 and C_2 be two equivalence classes such that for (f_1, k_1) in C_1 and for (f_2, k_2) in C_2, the product $(f_1, k_1) \times (f_2, k_2)$ exists. Then, we say that the *product* of the two classes C_1 and C_2, in that order, exists and is given by:

$$C_1 \times C_2 = \langle (f_1, k_1) \times (f_2, k_2) \rangle.$$

The product is not everywhere defined. Where it is defined, by Lemma 2, it is well defined. Where it is defined, it is not necessarily commutative. It does have some nice properties which we list in the following theorem. No proofs are given as they follow from the preceding discussion.

Theorem 3: a. The class of trivial generators is a two-sided identity.

b. Each class has a two-sided inverse, or reciprocal, given by

$$\langle (f, k) \rangle^{-1} = \langle (f, k)^{-1} \rangle.$$

c. The reciprocal of a product is the product of the reciprocals in the reverse order.

d. The product is associative; that is, let C_i, $i = 1, 2, 3$, be classes such that the products $C_1 \times C_2$ and $C_2 \times C_3$ exist, then

$$(C_1 \times C_2) \times C_3 = C_1 \times (C_2 \times C_3).$$

The reciprocal of a class C will be denoted by C^{-1}. $(C^{-1})^{-1} = C$.

To form products, class representatives cannot be chosen at random. Even primitive generators are not necessarily good choices. The product

$$(2 \cdot 5, 2) \times (3 \cdot 41, 3^3)$$

is not defined. Equivalent generators yield

$$(2 \cdot 5,\ 2 \cdot 3^3) \times (3 \cdot 41,\ 2^3 \cdot 3^3 \cdot 5) = (2 \cdot 3,\ 5 \cdot 41,\ 2 \cdot 3^3).$$

Thus

$$\langle(2 \cdot 5)\rangle \times \langle(3 \cdot 41,\ 3^3)\rangle = \langle(2 \cdot 3,\ 5 \cdot 41,\ 2 \cdot 3^3)\rangle.$$

Lemma 3: Let C_1, C_2 be classes such that for respective generators (f_1, k_1) and (f_2, k_2), f_1, f_2 have no primes in common. Then the product $C_1 \times C_2$ exists and is commutative.

Proof: Let (f_1, K_1), (f_2, K_2) be the corresponding primitives. Since f_1, f_2 have no primes in common, neither do f_1, K_2 nor f_2, K_1 nor K_1, K_2. Then the products, in both orders, can be defined using equivalent generators. Specifically,

$$(f_1,\ K_1K_2) \times (f_2,\ f_1K_1K_2) = (f_1f_2,\ K_1K_2) = (f_2,\ K_2K_1) \times (f_1,\ f_2K_1K_2).$$

Thus,

$$C_1 \times C_2 = C_2 \times C_1. \ \square$$

The converse of Lemma 3 is an open question. The following is given without proof.

Corollary 1: Let C_1, C_2 be two classes such that for the respective primitives (F_1, K_1), (F_2, K_2), F_1, F_2 have no primes in common. Then the product exists, is commutative, and is given by $\langle(F_1F_2,\ K_1K_2)\rangle$.

Except for the fact that the product is not everywhere defined, the set of classes would form a group. The product fails to exist in one significant case so that the properties of the product as described set bounds on the best possible situation.

Lemma 4: With the exception of the identity class, the square of a class does not exist.

Proof: It is a direct calculation to show that the square of the identity is the identity. Let (F, K) be the primitive for any nonidentity class, $F \neq 1$. For the product to be defined there must be integers m and n, relatively prime to F so that the product $(F, Km) \times (F, Kn)$ exists; that is, so that $FKm = Kn$, $Fm = n$. Since m and n are relatively prime to F, either $F = 1$ or $m = n$, which forces $F = 1$. $\square$

Lemma 4 also implies that, with the exception of the identity class, the powers of a class do not exist. The full characterization of which products exist (or do not exist) is an open question.

2. Generators and Unitary Amicable Pairs

There are at least three methods of producing generators. McClung found sixteen in a limited computer search. Briefly, he characterized generators with $\pi(f) = 2$ and $\pi(k) = 1$ and searched for generators of the forms

$$(2 \cdot p,\ 2^a),\ (2^2 \cdot p,\ 2^b),\ \text{and}\ (3 \cdot p,\ 3^c).$$

He found five, eight, and three, respectively. By the nature of the characterization, all are primitive.

The characterization of other generator forms remains a fertile area of endeavor. It appears, for example, that in the case $\pi(f) = \pi(k) = 2$, f is not an integer.

The examination of known unitary amicable pairs yields generators. Before discussing the method, a brief review will be useful to allow the introduction of notation.

Two numbers m and n form a unitary amicable pair if

$$\sigma^*(m) = \sigma^*(n) = m + n.$$

Let $T = \text{gucd}(m, n)$. Write $m = TM$ and $n = TN$. Assume, for convenience, that $M < N$. Notation for the unitary amicable pair m, n will be $U = (T; M, N)$.

The action of a generator (f, k) on U to produce a new unitary amicable pair U' takes the following form. If k is a unitary divisor of T such that

$$\gcd(fk, (T/k)MN) = 1 = \gcd(k, (T/k)MN),$$

then the unitary amicable pair produced is $U' = (fT; M, N)$.

Use right function notation:

$$(f, k) : (T; M, N) \mapsto (fT; M, N) \quad \text{and} \quad (T; M, N)(f, k) = (fT; M, N).$$

Lemma 5: Let (f_1, k_1) and (f_2, k_2) be two generators which act on the unitary amicable pair $(T; M, N)$ to produce the same unitary amicable pair U'. Then one has that (f_1, k_1) is equivalent to (f_2, k_2).

Proof: Since $(T; M, N)(f_1, k_1) = (f_1T; M, N)$ and $(T; M, N)(f_2, k_2) = (f_2T; M, N)$,

$$(f_1T; M, N) = (f_2T; M, N) \text{ and } f_1T = f_2T.$$

Thus, $f_1 = f_2$. k_1 and k_2 are unitary divisors of T. There exist numbers a, b, also unitary divisors of T so that $ak_1 = T = bk_2$.

$$\gcd(a, k_1) = 1 = \gcd(b, k_2).$$

We must show that a and b are relatively prime to f_1. Suppose p is a prime dividing both a and f_1. Since $a = (T/k_1)$ and $\gcd(f_1k_1, (T/K_1)MN) = 1$, p does not divide f_1k_1. Thus, p must occur to a negative power in f_1 and a positive in k_1. However, since $\gcd(k_1, (T/k_1)MN) = 1$, it does not. Thus, p does not divide f_1. So a, and similarly b, is relatively prime to f_1. Therefore, one has that (f_1, k_1) and (f_2, k_2) are equivalent. □

Definition 7: Two unitary amicable pairs

$$U_1 = (T_1; M_1, N_1) \quad \text{and} \quad U_2 = (T_2; M_2, N_2)$$

are said to be *in the same family* iff $M_1 = M_2$ and $N_1 = N_2$.

Lemma 6: The relation of being in the same family is an equivalence relation.

Proof: Left to the reader. □

Since the action of a generator class on a unitary amicable pair $(T; M, N)$ leaves M and N unchanged, the classes cycle pairs within the family. Lemma 5 leads to the following statement.

Definition 8: A generator class C is said to *act on a unitary amicable pair* U to yield another pair U' if there is a generator (f, k) in C such that

$$U(f, k) = U'.$$

Notation will be $C : U \mapsto U'$ or $UC = U'$.

If C is the identity class, $UC = U$ for any U. If $UC = U'$, $U'C^{-1} = U$.

Theorem 4: Let U and U' be unitary amicable pairs in the same family. Then there is a class C so that $UC = U'$.

Proof: Let $U = (T; M, N)$ and $U' = (T'; M, N)$. It suffices to find a generator (f, k) so that $U(f, k) = U'$. $C = \langle(f, k)\rangle$. Let $f = T'/T$ and $k = T$. If $T' = T$, (f, k) is a trivial generator with the desired action. Assume $T' \neq T$. k and fk are integers.

$$\gcd(k, MN) = \gcd(T, MN) = 1 \quad \text{and} \quad \gcd(fk, MN) = \gcd(T', MN) = 1.$$

To verify that $f\sigma^*(k) = \sigma^*(fk)$, note that the relation $\sigma^*(TM) - TM = TN$, yields

$$\sigma^*(T)/T = (M + N)/\sigma^*(M).$$

Thus,

$$\sigma^*(T)/T = \sigma^*(T')/T';$$

$$\begin{aligned} f\sigma^*(k) &= (T'/T)\sigma^*(T) = (T'/T')\sigma^*(T') = \sigma^*(T'') \\ &= \sigma^*((T'/T)T) = \sigma^*(fk). \end{aligned}$$

Finally,

$$U(f, k) = (T; M, N)(T'/T, T) = ((T'/T)T; M, N) = (T'; M, N) = U'. \ \square$$

Corollary: The cardinality of the set of classes is at least as large as the cardinality of the largest family of unitary amicable pairs.

Theorem 5: Let (f_1, k_1) and (f_2, k_2) be generators, and let U_1, U_2, and U_3 be unitary amicable pairs in the same family, satisfying:

1. The product $(f_1, k_1) \times (f_2, k_2)$ exists;
2. $U_1(f_1, k_1) = U_2$;
3. $U_2(f_2, k_2) = U_3$.

Then $U_1((f_1, k_1) \times (f_2, k_2)) = U_3$.

Proof: By (1) the product

$$(f_1, k_1) \times (f_2, k_2) = (f_1f_2, k_1)$$

exists. The action $U_1(f_1f_2, k_1)$ is defined if k_1 is a unitary divisor of T_1 as given in (2). It suffices to evaluate $f_1f_2T_1$. From (2) and (3),

$$f_1f_2T_1 = f_2(f_1T_1) = f_2T_2 = T_3.$$

Thus,

$$U_1(f_1f_2, k_1) = (T_3; M, N) = U_3. \ \square$$

Let C_1, C_2 be classes, and let U_1, U_2, U_3 be unitary amicable pairs in the same family, satisfying:

1. The product $C_1 \times C_2$ is defined;
2. $U_1C_1 = U_2$;
3. $U_2C_2 = U_3$.

Then, $U_1(C_1 \times C_2) = U_3$.

A brief list of primitive generators is given in the table below. Sources include McClung's list [3] and the results of applying Theorem 4 to the unitary amicable pairs in Hagis [1]. Inverses and products are not listed. The pairs listed by Wall [8] were not examined for the generators arising there. A description of another method of forming generators can be found in [3] and

[5]. No effort was made to produce generators for the list given here. This list is intended to be typical, not inclusive.

Table of Primitive Generators

1.	$(2 \cdot 3^2, 2^2)$	15.	$(2^3 \cdot 3 \cdot 17, 2)$
2.	$(2 \cdot 5, 2)$	16.	$(2^4 \cdot 11 \cdot 43, 2^3)$
3.	$(2 \cdot 17, 2^3)$	17.	$(2 \cdot 3 \cdot 5 \cdot 41, 2 \cdot 3^3)$
4.	$(2 \cdot 257, 2^7)$	18.	$(2^6 \cdot 3 \cdot 11 \cdot 43, 2)$
5.	$(2 \cdot 65537, 2^{15})$	19.	$\left(\frac{2 \cdot 11}{17}, 2^4 \cdot 17\right)$
6.	$(2^2 \cdot 3, 2)$	20.	$\left(\frac{2 \cdot 5 \cdot 13}{3^2}, 2 \cdot 3^3 \cdot 5\right)$
7.	$(2^2 \cdot 11, 2^3)$	21.	$\left(\frac{2^3 \cdot 11 \cdot 43}{17}, 2^4 \cdot 17\right)$
8.	$(2^2 \cdot 43, 2^5)$	22.	$\left(\frac{2^3 \cdot 3 \cdot 5 \cdot 11 \cdot 43}{17}, 2^4 \cdot 3 \cdot 17\right)$
9.	$(2^2 \cdot 683, 2^9)$	23.	$\left(\frac{2^3 \cdot 2^3 \cdot 11 \cdot 41 \cdot 43}{17}, 2^4 \cdot 3^3 \cdot 17\right)$
10.	$(2^2 \cdot 2731, 2^{11})$	24.	$(3 \cdot 5, 3)$
11.	$(2^2 \cdot 43691, 2^{15})$	25.	$(3 \cdot 41, 3^3)$
12.	$(2^2 \cdot 173763, 2^{17})$	26.	$(3 \cdot 21523361, 3^{15})$
13.	$(2^2 \cdot 2796203, 2^{21})$	27.	$\left(\frac{3}{2}, 2^2 \cdot 3\right)$
14.	$(2^2 \cdot 3^2 \cdot 17, 2^2)$	28.	$\left(\frac{5 \cdot 13}{3}, 3^3 \cdot 5\right)$

3. Unitary Sociable Numbers

Lal, Tiller, and Summers [2] defined unitary sociable numbers as sets of numbers m_i, $i = 1, 2, \ldots, n$, so that

$$\sigma^*(m_i) - m_i = m_{i+1}, \text{ for } i = 1, 2, \ldots, n - 1,$$

and

$$\sigma^*(m_n) - m_n = m_1.$$

Use the convention that m_1 is the smallest number in the set.

Unitary sociable sets are extensions of unitary amicable pairs. The notation for amicable pairs can also be extended. Given a unitary sociable set, let

$$T = \text{gucd}(m_1, m_2, \ldots, m_n)$$

and set $m_i = TM_i$, $i = 1, 2, \ldots, n$. Then, one can denote a unitary sociable set by the notation

$$S = (T; M_1, \ldots, M_n).$$

All the results of Section 2 are valid with U's replaced by S's.

The T values were calculated for all sets in [2]. No matches were found between these values and the generators given in the table. The production of new unitary sociable sets by the methods of this paper must await more extensive lists of generators.

References

1. P. Hagis, Jr. "Unitary Amicable Numbers." *Math. Comp.* *25* (1971):915-918.
2. M. Lal, G. Tiller, & R. Summers. "Unitary Sociable Numbers." *Proc. 2nd Manitoba Conf. Numer. Math., Cong. Number.* VII:211-216. University of Manitoba Press, 1972.
3. O. W. McClung. "Generators of Unitary Amicable Numbers." *Fibonacci Quarterly 23* (1985):158-165.
4. O. W. McClung. "Letter to the Editor." *Fibonacci Quarterly 24* (1986):106.
5. H. J. J. te Riele. *Further Results on Unitary Aliquot Sequences.* Report NW 2/78, Mathematical Center, Amsterdam. 2nd ed., January 1978 (1st ed., March 1973).
6. H. J. J. te Riele. "On Generating New Amicable Pairs from Given Amicable Pairs." *Math. Comp.* *42* (1984):219-223.
7. H. J. J. et Riele. Private Correspondence.
8. C. R. Wall. "Topics Related to the Sum of Unitary Divisors of an Integer." Ph.D. Dissertation, The University of Tennessee, 1970.

*****

RECURRENCE RELATIONS FOR A POWER SERIES

László Cseh and Imre Merényi
Students, Babes-Bolyai University, 3400 Cluj, Romania
(Submitted April 1987)

For integers $n \geq 2$, $r \geq 0$, let

$$S_n(r) = \sum_{k=1}^{\infty} k^r n^{-k}.$$

It was proved in [1] that, for all $r \geq 1$,

$$S_n(r) = \frac{n}{n-1}\left[\binom{r}{1}S_n(r-1) - \binom{r}{2}S_n(r-2) + \cdots + (-1)^{r+1}\binom{r}{r}S_n(0)\right].$$

The purpose of this paper is to extend this result for arithmetic progressions and also to obtain a related formula with no alternate signs.

Let a and q be real numbers, and let $(a_k)_{k \geq 0}$ be the arithmetic progression

$$(a + kq)_{k \geq 0}.$$

If $|x| < 1$ and $r \in \{0, 1, \ldots\}$, we define

$$S_r(x) = \sum_{k=1}^{\infty} a_k^r x^k. \tag{1}$$

In this note we establish two recurrence relations for the series (1). Namely:

$$S_r(x) = \frac{x}{1-x}\left[(a+q)^r + \binom{r}{1}qS_{r-1}(x) + \binom{r}{2}q^2S_{r-2}(x) + \cdots + q^rS_0(x)\right] \tag{2}$$

and

$$S_r(x) = \frac{1}{1-x}\left[a^rx + \binom{r}{1}qS_{r-1}(x) - \binom{r}{2}q^2S_{r-2}(x) + \cdots + (-1)^{r+1}q^rS_0(x)\right]. \tag{3}$$

Let us denote by $S_r(x, m)$ the m-adic partial sum, i.e.,

$$S_r(x, m) = \sum_{k=1}^{m} a_k^r x^k.$$

Proof of (2): We first deduce a functional equation for $S_r(x, m)$.

$$\begin{aligned}
S_r(x, m+p) &= \sum_{k=1}^{m+p} a_k^r x^k = \sum_{k=1}^{m} a_k^r x^k + \sum_{k=m+1}^{m+p} a_k^r x^k \\
&= S_r(x, m) + x^m \sum_{i=1}^{p} a_{m+i}^r x^i \\
&= S_r(x, m) + x^m \sum_{i=1}^{p} (mq + a_i)^r x^i \\
&= S_r(x, m) + x^m \sum_{i=1}^{p} \sum_{j=0}^{r} \binom{r}{j}(mq)^j a_i^{r-j} x^i \\
&= S_r(x, m) + x^m \sum_{j=0}^{r} \binom{r}{j}(mq)^j \sum_{i=1}^{p} a_i^{r-j} x^i
\end{aligned}$$

$$= S_r(x,\ m) + x^m \sum_{j=0}^{r} \binom{r}{j}(mq)^j S_{r-j}(x,\ p).$$

For $m = 1$, we obtain

$$S_r(x,\ p+1) = (a+q)^r x + x\sum_{j=0}^{r}\binom{r}{j} q^j S_{r-j}(x,\ p)$$

$$= (a+q)^r x + xS_r(x,\ p) + x\sum_{j=1}^{r}\binom{r}{j} q^j S_{r-j}(x,\ p).$$

Now, if $p \to \infty$, we have

$$S_r(x) = (a+q)^r x + xS_r(x) + x\sum_{j=1}^{r}\binom{r}{j} q^j S_{r-j}(x),$$

or

$$S_r(x) = \frac{x}{1-x}\left[(a+q)^r + \binom{r}{1} qS_{r-1}(x) + \binom{r}{2} q^2 S_{r-2}(x) + \cdots + q^r S_0(x)\right],$$

which was to be proved.

Proof of (3): We proceed as follows:

$$S_r(x,\ m) = \sum_{k=1}^{m} a_k^r x^k = \sum_{k=1}^{m} x^k \sum_{i=1}^{k} (a_i^r - a_{i-1}^r) + \sum_{k=1}^{m} a^r x^k$$

$$= \sum_{k=1}^{m} x^k \sum_{i=1}^{k} [a_i^r - (a_i - q)^r] + \sum_{k=1}^{m} a^r x^k$$

$$= \sum_{k=1}^{m} x^k \sum_{i=1}^{k} \sum_{j=1}^{r} (-1)^{j+1}\binom{r}{j} a_i^{r-j} q^j + a^r \sum_{k=1}^{m} x^k$$

$$= \sum_{k=1}^{m} \sum_{i=1}^{k} \sum_{j=1}^{r} (-1)^{j+1}\binom{r}{j} a_i^{r-j} q^j x^k + a^r \sum_{k=1}^{m} x^k$$

$$= \sum_{j=1}^{r} (-1)^{j+1}\binom{r}{j} q^j \sum_{i=1}^{m} \sum_{k=1}^{m} a_i^{r-j} x^k + a^r \sum_{k=1}^{m} x^k$$

$$= \sum_{j=1}^{r} (-1)^{j+1}\binom{r}{j} q^j \sum_{i=1}^{m} a_i^{r-j} \sum_{k=1}^{m} x^k + a^r \sum_{k=1}^{m} x^k$$

$$= \sum_{j=1}^{r} (-1)^{j+1}\binom{r}{j} q^j \sum_{i=1}^{m} \frac{1}{1-x}(a_i^{r-j} x^i - a_i^{r-j} x^{m+1}) + a^r \sum_{k=1}^{m} x^k$$

$$= \frac{1}{1-x} \sum_{j=1}^{r} (-1)^{j+1}\binom{r}{j} q^j [S_{r-j}(x,\ m) - x^{m+1} s_{r-j}(m)] + a^r \sum_{k=1}^{m} x^k,$$

where

$$s_{r-j}(m) = \sum_{i=1}^{m} a_i^{r-j}.$$

So $S_r(x,\ m)$ can be written as

$$S_r(x,\ m) = \frac{1}{1-x} \sum_{j=1}^{r} (-1)^{j+1}\binom{r}{j} q^j S_{r-j}(x,\ m) - T(x,\ m) + a^r \sum_{k=1}^{m} x^k, \tag{4}$$

with

with

$$T(x,\ m) = \frac{x^{m+1}}{1-x}\sum_{j=1}^{r}(-1)^{j+1}\binom{r}{j}q^j s_{r-j}(m).$$

We will show that

$$T(x,\ m) \to 0 \text{ as } m \to \infty. \tag{5}$$

We have

$$a^r = (a_1 - q)^r = a_1^r - \binom{r}{1}a_1^{r-1}q + \cdots + (-1)^r q^r$$

$$a_1^r = (a_2 - q)^r = a_2^r - \binom{r}{1}a_2^{r-1}q + \cdots + (-1)^r q^r$$

....

$$a_{m-1}^r = (a_m - q)^r = a_m^r - \binom{r}{1}a_m^{r-1}q + \cdots + (-1)^r q^r.$$

So that

$$a^r = a_m^r - \binom{r}{1}qs_{r-1}(m) + \cdots + (-1)^r q^r s_0(m)$$

or

$$\sum_{j=1}^{r}(-1)^{j+1}\binom{r}{j}q^j s_{r-j}(m) = a_m^r - a^r$$

and (5) is now clear.

Let $m \to \infty$ in (4). It then follows that

$$S_r(x) = \frac{1}{1-x}\left[a^r x + \binom{r}{1}qS_{r-1}(x) - \binom{r}{2}q^2 S_{r-2}(x) + \cdots + (-1)^{r+1}q^r S_0(x)\right],$$

is exactly (3).

Remark: Of course, one can consider

$$\overline{S}_r(x) = \sum_{k=0}^{\infty} a_k^r x^k \quad (|x| < 1,\ r \geq 0),$$

and obtain

$$\overline{S}_r(x) = \frac{x}{1-x}\left[a^r + \binom{r}{1}q\overline{S}_{r-1}(x) + \binom{r}{2}q^2\overline{S}_{r-2}(x) + \cdots + q^r\overline{S}_0(x)\right] + a^r, \tag{2'}$$

and

$$\overline{S}_r(x) = \frac{1}{1-x}\left[(a-q)^r + \binom{r}{1}q\overline{S}_{r-1}(x) - \binom{r}{2}q^2\overline{S}_{r-2}(x) + \cdots + (-1)^{r+1}q^r\overline{S}_0(x)\right], \tag{3'}$$

respectively.

Reference

1. L. Cseh & I. Merényi. Problem E 3153. *Amer. Math. Monthly* 93 (1986).

*****

ON SOME SECOND-ORDER LINEAR RECURRENCES

C. Georghiou
University of Patras, Patras, Greece
(Submitted April 1987)

1. Introduction

Many problems lead to constant coefficient linear recurrences, mostly of the second order, for which explicit solutions are readily available. In some cases, however, one is faced with the problem of solving nonconstant coefficient linear recurrences. Second- and higher-order linear recurrences with variable coefficients cannot always be solved in closed form. The methods available to deal with such cases are very limited. On the other hand, the theory of differential equations is richer in special formulas and techniques than the theory of difference equations. The lack of a simple "change of variable rule," that is, a formula analogous to the differential formula

$$\frac{dy}{dx} = \frac{dy}{dt}\frac{dt}{dx},$$

in the calculus of finite differences, precludes most of these techniques to carry over when we attempt to solve a difference equation.

Of course, in such cases, a step-by-step procedure, starting with the initial values, is always possible. And in many cases it may be the best approach, especially if one needs the value of the independent variable not far from its initial points. However, we frequently ask the question whether the solution may be written in closed form.

When a certain class of second-order linear recurrences was studied, we arrived at a theorem not found anywhere in the literature and which is stated, after some preliminaries, in the next section. In Section 3 we give a proof of the theorem, and its consequences are examined. It is found that a whole class of second-order linear recurrences can be solved in closed form. Finally, an example is given where the theorem is applied.

2. Preliminaries and a Theorem

Let $I = \{\ldots, -1, 0, 1, \ldots\}$ be the set of all integers. The domain of the (complex-valued) functions defined in this paper will be subsets of I of the form $I_N = \{N, N+1, N+2, \ldots\}$ where $N \in I$ (usually $N = 0$ or 1). We are going to consider linear recurrences written in operator form as

$$E^2y + aEy + by = 0 \tag{1}$$

where E is the shift operator, i.e., $Ey = y(n+1)$, a, b, and y are functions on I_N and where $b(n) \neq 0$ for $n \in I_N$. We will also use the notation

$$y'' + ay' + by = 0 \tag{2}$$

where $y' \equiv Ey$, $y'' \equiv E^2y$, and so on, in order to stress the analogy between recurrences and differential equations.

First, we examine the constant coefficient second-order linear recurrences

$$E^2y + \mu Ey + \nu y = 0 \tag{3}$$

where Greek letters will always stand for scalar quantities.

In the elementary exposition of the theory [1] we try solutions of the form $y(n) = \lambda^n$ for some as yet undetermined scalar λ, and we are thus led to the notion of the characteristic polynomial associated with the given equation. In general, we are able to find two linearly independent solutions and hence the general solution. The question arises, however, as to why we try solutions of that particular form. In the more advanced exposition of the theory [3], linear recurrences are treated as a special case of first-order linear systems where the trial solutions $y(n) = \lambda^n$ appear naturally when we attempt to calculate A^n where A is the matrix coefficient of the system.

For the moment, we make the observation that when (3) is premultiplied by E we get

$$E^2(Ey) + \mu E(Ey) + \nu(Ey) = 0, \tag{4}$$

i.e., whenever y is a solution, Ey is also a solution of (3) and, furthermore, the assumption for the existence of solutions of the form $y(n) = \lambda^n$ is equivalent to the statement $Ey = \lambda y$ for some λ.

Next, take the less trivial case of the recurrence

$$aE(aEy) + \mu aEy + \nu y = 0 \tag{5}$$

where $a(n) \neq 0$ for $n \in I_N$. We try to solve (5) as a first-order recurrence (of the Riccati-type) in a. The substitution $a = Eu/u$ leads to the constant coefficient linear recurrence

$$E^2(uy) + \mu E(uy) + \nu(uy) = 0, \tag{6}$$

which has solutions of the form $u(n)y(n) = \lambda^n$ or

$$\frac{u(n+1)y(n+1)}{u(n)y(n)} = \lambda,$$

i.e., $aEy = \lambda y$ for some λ. Note also that if (5) is premultiplied by E and then by a we get

$$aE(aE(aEy)) + \mu aE(aEy) + \nu aEy = 0, \tag{7}$$

i.e., whenever y is a solution, aEy is also a solution of (5).

The above discussion suggests the following.

Theorem: Let L and M be two linear (difference) operators and suppose that $LMy = 0$ whenever $Ly = 0$. Then there exists (at least) a solution y of $Ly = 0$ such that $My = \lambda y$ for some λ.

3. Proof of the Theorem

Let $\{y_1, y_2, \ldots, y_m\}$ be a basis for the null space of L. Then My_i is also in the null space, $i = 1, 2, \ldots, m$ and can be written as a linear combination of the basis, i.e.,

$$My_i = \sum_{k=1}^{m} c_{ik} y_k, \quad i = 1, 2, \ldots, m. \tag{8}$$

Form the matrix $C = [c_{ik}]$ associated with the operator M and let μ be an eigenvector of C^T with associated eigenvalue λ, i.e., $C^T\mu = \lambda\mu$. Now, let

$$y = \sum_{i=1}^{m} \mu_i y_i.$$

Then

$$My = M\left(\sum_{i=1}^{m} \mu_i y_i\right) = \sum_{i=1}^{m} \mu_i My_i = \sum_{i=1}^{m} \mu_i \sum_{k=1}^{m} c_{ik} y_k$$

$$= \sum_{k=1}^{m}\left(\sum_{i=1}^{m}\mu_i c_{ik}\right)y_k = \lambda y. \tag{9}$$

Now let

$$L \equiv E^2 + aE + bI, \tag{10}$$

and

$$M \equiv pE + qI \tag{11}$$

where $b(n)p(n)q(n) \neq 0$ for $n \in I_N$ and I is the identity operator. Since $My = \lambda y$ can always be solved in closed form, the following problem arises:

> "Given a second-order linear operator L (10), find a first-order operator M (11) such that $LMy = 0$ whenever $Ly = 0$."

Although it is not always possible to find such an M, we proceed to deal with the problem and find out what can be said about it.

It is easy to see that

$$LM = p''E^3 + (q'' + ap')E^2 + (aq' + bp)E + bqI$$

and

$$ML = pE^3 + (a'p + q)E^2 + (b'p + aq)E + bqI. \tag{12}$$

Then

$$pLM - p''ML = rL, \tag{13}$$

provided that

$$r = qp - qp'' \tag{14}$$

and

$$a'p'' - ap' - q'' + q = 0; \tag{15}$$

$$b'p'' - bp - aq' + aq = 0. \tag{16}$$

Thus, p and q must satisfy the second-order linear system (15) and (16). Note, however, that (15) can be "summed," since it can be written as

$$\Delta(ap') = \Delta(\Delta + 2I)q \tag{17}$$

where $\Delta = E - I$ is the difference operator. When (17) is premultiplied by Δ^{-1} gives

$$ap' = q' + q + c \tag{18}$$

where c is a constant. Elimination now of q from (16) and (18) gives

$$ab''p''' - a'(aa' - b')p'' + a(aa' - b')p' - a'bp = 0, \tag{19}$$

which is a third-order linear recurrence in p. Solving (19) is a more difficult problem than the original one (10). Note, however, that if $aa' = b'$, (19) is only a two-term recurrence, which means that the recurrence

$$y'' + a'y' + aa'y = 0 \tag{20}$$

can be solved in closed form for any a. We can say something more. From (18) we have

$$a = (q' + q + c)/p', \tag{21}$$

and when the above expression is substituted in (16) we obtain

$$b = (q^2 + cq + d)/pp' \tag{22}$$

where d is a constant. We are, thus, led to the conclusion that the second-order linear recurrences of the form

$$pp'y'' + p(q' + q + \mu)y' + (q^2 + \mu q + \nu)y = 0, \tag{23}$$

where μ, ν are scalar quantities and p, q are arbitrary functions, can be solved in closed form. Finally, note that (20) is a special case of (23), and when q is constant and $p(n) = n$ in (23) we have the Euler-type difference equation [2].

As an application of the above discussion consider the recurrence

$$y(n+2) - 2(n+1)y(n+1) + \left(n + \frac{1}{2}\right)^2 y(n) = 0. \tag{24}$$

Then

$$L \equiv E^2 - 2(n+1)E + \left(n + \frac{1}{2}\right)^2 I.$$

It is easy to see that

$$L(E - nI)y - (E - nI)Ly = 0.$$

Therefore, the theorem applies for (24) and, consequently, there is (at least) one solution of (24) among the solutions of

$$(E - nI)y = \lambda y,$$

which are

$$y(n) = \lambda(\lambda + 1)(\lambda + 2) \ldots (\lambda + n - 1).$$

Substitution of $y(n)$ into (24) gives

$$\lambda^2 - \lambda + \frac{1}{4} = 0 \quad \text{or} \quad \lambda = \frac{1}{2}.$$

Therefore, one solution of (24) is

$$y_1(n) = \frac{1}{2}\left(\frac{1}{2} + 1\right)\left(\frac{1}{2} + 2\right) \ldots \left(\frac{1}{2} + n - 1\right) \quad \text{or} \quad y\ (n) = \Gamma\left(\frac{1}{2} + n\right),$$

where $\Gamma(\cdot)$ is the Gamma function. The other, linearly independent, solution $y_2(n)$ can be found by the method of the reduction of order.

References

1. S. Goldberg. *Difference Equations*. New York: Wiley & Sons, 1958.
2. C. Jordan. *Calculus of Finite Differences*. New York: Chelsea, 1965.
3. K. S. Miller. *Linear Difference Equations*. New York: W. A. Benjamin, 1968.

*****

ON A CONJECTURE BY HOGGATT WITH EXTENSIONS TO HOGGATT SUMS AND HOGGATT TRIANGLES

Daniel C. Fielder and Cecil O. Alford
Georgia Institute of Technology, Atlanta, Georgia 30332-0250
(Submitted April 1987)

1. Introduction

In letters [1] to one of us (Fielder) in mid-1977, the late Verner Hoggatt conjectured that the third diagonal of Pascal's triangle could be used in a simple algorithm to generate rows of integers whose row sums equaled correspondingly indexed Baxter permutation values (see [3], [4]). Later, in 1978, Chung, Graham, Hoggatt, and Kleiman produced a remarkable paper [2] in which they derived a general solution for Baxter permutation values.

In planning an extension of Hoggatt's work, we searched for, but never found, a proof of Hoggatt's conjecture or even a documented statement of the conjecture. Reference [2] did, however, state that Hoggatt had found a simple way of finding the first ten Baxter permutation values but, again, without giving the conjecture. In this note, we formalize Hoggatt's conjecture, derive formulas for the values predicted by the conjecture, and then prove the conjecture. As new material, we extend Hoggatt's conjecture to *all* Pascal diagonals. In so doing, we will introduce structures called *Hoggatt triangles* and integers called *Hoggatt sums*. These names were the explicit choice of one of us (Fielder) as a tribute to Verner Hoggatt for his work with Pascal triangles and, in some small way, to express gratitude for Vern's guidance, help, and friendship through the years. Finally, we report briefly on a computer-aided experiment to obtain recursion formulas for selected Hoggatt sums.

2. Hoggatt's Conjecture

Whereas Hoggatt chose a column representation to demonstrate his algorithm, we use a diagonal format. There is, of course, no conceptual or computational difference.

Hoggatt's conjecture may be phrased as follows: "Select the zeroth[1] and third right diagonal of Pascal's triangle and let them become, respectively, the zeroth and first right diagonal of a new triangle with as yet undetermined values for the entries of the other diagonals. For $m = 2, 3, 4, \ldots$, in succession, compute the m^{th} row sum and m^{th} row entries for the new triangle as

$$\text{Row}_m\,\text{sum} = 1 + \binom{m+2}{3}\left[\frac{(R_{m-1})_0}{D_0} + \frac{(R_{m-1})_1}{D_1} + \cdots + \frac{(R_{m-1})_{m-1}}{D_{m-1}}\right] \tag{1}$$

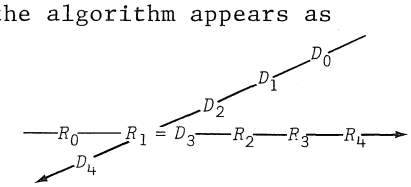
where the (R_{m-1}) 's are the $(m-1)^{\text{th}}$ row integers starting with $q = 0$ at the left and the D 's are the first diagonal integers starting with $q = 0$ at the top right. Then the m^{th} row sum as given by (1) is identically the m^{th} Baxter permutation value S_m."

[1] Unless stated otherwise, the counting of indices, rows, columns, diagonals, etc. in this note starts with zero as the first encountered.

In order to visualize the algorithm of (1), assume that integers of the rows through the four have been found through successive application of the right side of (1). The diagrams below illustrate how the fifth row is constructed. (Note that the first two integers of any row are always known.)

$$\begin{array}{ccccccccccc} &&&&&1&&&&& \\ &&&&1&&1&&&& \\ &&&1&&4&&1&&& \\ &&1&&10&&10&&1&& \\ &1&&20&&50&&20&&1& \\ 1&&35&&X&&X&&X&&X \end{array} \tag{2}$$

By using R_s for the fourth row entries and D_s for the first diagonal entries, a graphic preparation for the algorithm appears as



(3)

When generated by (1), the fifth row becomes

$$R_0,\ D_4 \times \frac{R_0}{D_0},\ D_4 \times \frac{R_1}{D_1},\ D_4 \times \frac{R_2}{D_2},\ D_4 \times \frac{R_3}{D_3},\ D_4 \times \frac{R_4}{D_4}, \tag{4}$$

with calculated values, 1, 35, 175, 175, 35, 1. The row sum is 422, which equals Baxter permutation S_5. The rows completed prior to row five have sums equal to S_0, S_1, S_2, S_3, S_4, respectively. In anticipation of later work, the new triangle will be called a *Hoggatt triangle of order three*.

3. Formulas for Row Sums, Row Integers, and Proof of the Conjecture

The development of formulas for the row sums is presented by using the third right diagonal of Pascal's triangle. (If the entries are in the binomial coefficient form, the procedure is easy to follow.) This, in turn, is used as the first diagonal of a third-order Hoggatt triangle. Apply (1) as before, but retain the accumulated binomial coefficients in the row construction. The construction of rows one and two is shown.

$$S_1 = 1 + \binom{3}{3}\left[\frac{1}{\binom{3}{3}}\right] = 1 + \frac{\binom{3}{3}}{\binom{3}{3}}, \tag{5}$$

$$S_2 = 1 + \binom{4}{3}\left[\frac{1}{\binom{3}{3}} + \frac{\frac{\binom{3}{3}}{\binom{3}{3}}}{\binom{4}{3}}\right] = 1 + \frac{\binom{4}{3}}{\binom{3}{3}} + \frac{\binom{4}{3}\binom{3}{3}}{\binom{3}{3}\binom{4}{3}}, \tag{6}$$

The obvious pattern of the development can be generalized by summations in which the total is the general m^{th} row sum and the individual terms of a summation are the m^{th} row values of a third-order Hoggatt triangle.

$$S = 1 + \sum_{h=0}^{m-1} \prod_{k=0}^{h} \frac{\binom{m+2-k}{3}}{\binom{3+k}{3}} = 1 + \sum_{h=0}^{m-1} \prod_{k=0}^{h} \frac{(m+2-k)^{(3)}}{(3+k)^{(3)}}. \tag{7}$$

The general t^{th} term, $0 \le t \le m$ of our development for S_m in (7) can be shown as:[2]

$$\frac{(m+2)^{(3)}(m+1)^{(3)}(m)^{(3)}(m-1)^{(3)} \ldots (m-t+3)^{(3)}}{(3)^{(3)}(4)^{(3)}(5)^{(3)}(6)^{(3)} \ldots (t+2)^{(3)}}$$

$$= \frac{(m+2)^{(t)}(m+1)^{(t)}(m)^{(t)}}{(t+2)^{(t)}(t+1)^{(t)}(t)^{(t)}}. \tag{8}$$

In reference [2], the successful derivation of a compact expression for Baxter permutation values appears as $B(n)$ in equation (1) of [2] and also on page 392 of [2]. In [2], index n starts at one, while our index starts at zero (as does Hoggatt's original index). For compatibility with our index, $B(n)$ of [2] becomes

$$B(m+1) = \binom{m+2}{1}^{-1}\binom{m+2}{2}^{-1}\sum_{k=1}^{m+1}\binom{m+2}{k-1}\binom{m+2}{k}\binom{m+2}{k+1}. \tag{9}$$

The general t^{th} term, $0 \le t \le m$, from (9) is

$$\frac{2\binom{m+2}{t}\binom{m+2}{t+1}\binom{m+2}{t+2}}{(m+2)^2(m+1)} = \frac{2(m+2)^{(t)}(m+2)^{(t+1)}(m+2)^{(t+2)}}{(m+2)^2(m+1)(t+2)!(t+1)!(t)!}. \tag{10}$$

To prove Hoggatt's conjecture, all we need do is show that $B(m+1)$ in (9) and our S_m in (7) have identical t^{th} terms. By restructuring the right side of (10) and canceling like numerator-denominator terms as shown below

$$\frac{\cancel{2}(m+2)^{(t)}\cancel{(m+2)}(m+1)^{(t)}\cancel{(m+2)}\cancel{(m+1)}(m)^{(t)}}{\cancel{(m+2)^2}\cancel{(m+1)}(t+2)^{(t)}\cdot\cancel{2}\cdot 1(t+1)^{(t)}\cdot 1(t)^{(t)}}, \tag{11}$$

we have identically the right side of (8).

If $(m-t)$ is substituted for t in the left side of (10), the same binomial coefficient product is obtained except for reverse order. This indicates equality between the $(m-t)^{\text{th}}$ and t^{th} terms of the sum and establishes symmetry of third-order Hoggatt triangles about a central vertical axis.

Thus, thanks in large measure to work [2] in which Hoggatt participated, a solid conjecture proof exists. We would like to think that Vern would be pleased to know that there are no longer any loose ends.

4. Hoggatt Sums and Hoggatt Triangles

A natural extension of Hoggatt's conjecture is to apply it to all right diagonals of Pascal's triangle. In this paper, the resultant row sums are called Hoggatt sums and the triangles formed by the successive row elements are called Hoggatt triangles. A particular row sum is identified by its index (0, 1, 2, ...) and its order. Order is equal to the index of the particular Pascal diagonal. Order of a Hoggatt triangle is similarly specified. The physical

[2] The terminology $(s)^{(p)} = p!\binom{s}{p}$ is a "partial" factorial, where

$$(s)^{(p)} = (s)(s-1)\ldots(s-p+1).$$

Because $0! = 1$, $(s)^{(0)} = (0)^{(0)} = 1$.

layout of a Hoggatt triangle is similar to that of Pascal's triangle in that each has the same number of row members. The k^{th} row of a Pascal triangle can be computed from the $(k - 1)^{\text{st}}$ row. Hoggatt triangles share this attribute but additionally require data from the first diagonal to complete a new row.

The general Hoggatt development, including the proof of symmetry, is similar to that used earlier for the special case of $d = 3$. The row sum, $(S_d)_m$, becomes

$$(S_d)_m = (R_m)_0 + \sum_{i=0}^{m} (R_m)_{i+1}, \tag{12}$$

where

$$(R_m)_0 = 1, \; (R_m)_{i+1} = \frac{\binom{m+d-1}{d}(R_{m-1})_i}{\binom{d+i}{d}} \tag{13}$$

and $\binom{d+i}{d}$ is the i^{th} element of the d^{th} Pascal diagonal.

In our terminology, d is the order and m is the index of the row sum. With the nucleus diagonals in place, operations similar to (5) and (6) lead to the summation forms

$$(S_d)_m = 1 + \sum_{h=0}^{m-1} \prod_{k=0}^{h} \frac{\binom{m+d-1-k}{d}}{\binom{d+k}{d}} = \sum_{k=1}^{m+1} \prod_{h=1}^{d} \frac{\binom{m+d-1}{k-2+h}}{\binom{m+d-1}{h-1}}. \tag{14}$$

The right expression in (14) is the reference [2] "analog" of the left expression in that, for $d = 3$, it reduces to (9).

Examples of Hoggatt triangles appear in Appendix A; Hoggatt sums in Appendix B. Although the extension of Hoggatt's conjecture is new, it is interesting to note that several of the resulting triangles or sums of orders zero through three are already well known. This actually enhances Hoggatt's work, since his conjecture and extensions introduce new ways of calculating the triangles and/or sums. For example, Hoggatt and Bicknell [5] point out that the array we designate as the Hoggatt triangle of order zero provides triangular numbers in base nine. Development of the Hoggatt triangle of order one introduces a new way of generating the time-honored Pascal triangle. Reference [5] anticipates the Hoggatt triangle of order two as an array of generalized binomial coefficients for the triangular numbers. Further, [5] demonstrates that Hoggatt sums of order two are identically the Catalan numbers, C_{n+1}. The equivalence of Hoggatt sums of order three and Baxter permutation values needs no further discussion.

5. A Computational Experiment

If a sequence of integers follows a linear index-invariant recursion, it is very easy to find the recursion formula. However, when the recursion is index-variant, the analytic difficulty increases dramatically. Reference [2] credits Paul S. Bruckman for equation (21) of [2], the linear, third-order, index-variant recursion formula for Baxter permutation values (Hoggatt sums of order three). When recast in our index m, Bruckman's formula is identically that which Hoggatt stated in [1]. Unfortunately, we have no way of knowing how Vern obtained this formula.

After a brief struggle with z-transform methods (see Jury's comments in [6], p. 59), we decided to attempt a nonanalytical determination of recursion formulas for second- and third-order Hoggatt sums as an experiment in digital computation. Because of the large, exact integers involved and the need for mixed symbolic and numeric operations, we chose to compute, in muMath, one of the currently available computer algebra systems (see [7], [8]). The experiment consisted essentially of a brute-force calculation of the coefficients of a recursion formula using simultaneous linear equations. After each run through the experiment, any false, inconsistent, or arbitrary values were either deleted or reassigned and the run repeated with fewer equations.

Surprisingly, we could never duplicate the coefficients of Bruckman's formula. A significant result, however, was that we could obtain an infinite number of sets of coefficients for formulas which were correct for all m values except one. For Hoggatt sums of order three (or Baxter permutation values), S_7 was always indeterminate. While the presence of arbitrary coefficients was responsible for the infinite number of sets of valid coefficients, the indeterminancy of S_7 was independent of the arbitrary coefficients. The results for the second-order Hoggatt sums were similar except that the sole indeterminant value occurred for $m = 2$, i.e., S_2 was indeterminant.

From the experiment we can ask, "Is Bruckman's analytical solution the only solution with no indeterminant S_m's? Also, does the above behavior hold for $d = 4, 5, 6, \ldots$?"

For a more detailed account of the experiment as well as more complete derivations from within the main body of the paper, the reader is encouraged to contact the authors.

6. Summary

We have proved Hoggatt's conjecture and have extended it to all Pascal diagonals. Formulas for obtaining Hoggatt triangles and sums have been developed. We have shown that lower-order triangles and sums provide new ways to view previously known structures. A computational experiment produced an infinite number of restricted recursion formulas for several lower-order Hoggatt sums.

7. Acknowledgments

We are indebted to Marjorie Bicknell-Johnson and Paul S. Bruckman for sharing their recollections, calculations, and correspondence relative to the time when Vern Hoggatt conceived his conjecture. Specifically, Bicknell-Johnson alerted us to the Catalan connection, while Bruckman provided an outline of his analytic derivation of the recursion formula for Baxter permutation values.

We also wish to thank the referees for excellent suggestions which improved the content and readability of the paper. The first referee provided the right expression of (8), which simplified our calculations greatly. The second referee contributed a neat, condensed version of (12) and (13) and also found the errors from two embarrassing typos by the senior author.

APPENDICES

Appendix A: Hoggatt Triangles

1
1 1
1 3 1
1 6 6 1
1 10 20 10 1
1 15 50 50 15 1
1 21 105 175 105 21 1

ORDER TWO

1
1 1
1 4 1
1 10 10 1
1 20 50 20 1
1 35 175 175 35 1
1 56 490 980 490 56 1

ORDER THREE

1
1 1
1 5 1
1 15 15 1
1 35 105 35 1
1 70 490 490 70 1
1 126 1764 4116 1764 126 1

ORDER FOUR

1
1 1
1 6 1
1 21 21 1
1 56 196 56 1
1 126 1176 1176 126 1
1 252 5292 14112 5292 252 1

ORDER FIVE

Appendix B: Hoggatt Sums

SUMS	VALUE
s0	1
s1	2
s2	5
s3	14
s4	42
s5	132
s6	429
s7	1430
s8	4862
s9	16796
s10	58786
s11	208012
s12	742900
s13	2674440
s14	9694845
s15	35357670
s16	129644790
s17	477638700
s18	1767263190
s19	6564120420
s20	24466267020
s21	91482563640
s22	343059613650
s23	1289904147324
s24	4861946401452
s25	18367353072152
s26	69533550916004
s27	263747951750360
s28	1002242216651368
s29	3814986502092304
s30	14544636039226909
s31	55534064877048198
s32	212336130412243110
s33	812944042149730764
s34	3116285494907301262
s35	11959798385860453492
s36	45950804324621742364
s37	176733862787006701400
s38	680425371729975800390
s39	2622127042276492108820
s40	10113918591637898134020
s41	39044429911904443959240
s42	150853479205085351660700
s43	583300119592996693088040
s44	2257117854077248073253720
s45	8740328711533173390046320
s46	33868773757191046886429490
s47	131327898242169365477991900
s48	509552245179617138054608572
s49	1978261657756160653623774456
s50	7684785670514316385230816156
s51	29869166945772625950142417512
s52	116157871455782434250553845880
s53	451959718027953471447609509424
s54	1759414616608818870992479875972
s55	6852456927844873497549658464312
s56	26700952856774851904245220912664
s57	104088460289122304033498318812080
s58	405944995127576985730643443367112
s59	1583850964596120042686772779038896

ORDER TWO

SUMS	VALUE
s0	1
s1	2
s2	6
s3	22
s4	92
s5	422
s6	2074
s7	10754
s8	58202
s9	326240
s10	1882960
s11	11140560
s12	67329992
s13	414499438
s14	2593341586
s15	16458756586
s16	105791986682
s17	687782586844
s18	4517543071924
s19	29949238543316
s20	200234184620736
s21	1349097425104912
s22	9154276618636016
s23	62522506583844272
s24	429600060173571952
s25	2968354097506204352
s26	20616682170931488704
s27	143886306136373723072
s28	1008739441056488779984
s29	7101857696077190042814
s30	50197792010624790718274
s31	356134037157421426324858
s32	2535503283457453475113498
s33	18111330098002679241995204
s34	129775523667497672794119820
s35	932649996060323085135343660
s36	6721418743462792115061865000
s37	48568825344643221105258466964
s38	351844920522232388929981300716
s39	2554987813422078288794169298972
s40	18596055885560437500207978342572
s41	135644235608879594521014316895264
s42	991488035658098636545959755543168
s43	7261715593999548236305978326928768
s44	53286745759568455589698874494878272
s45	391734954014771562094562102701976912
s46	2884866707621100648995326107469142704
s47	21280832747254136400685727258623694064
s48	157235970697232109921578618634420133232
s49	1163558691573487855005674103586862832160
s50	8623270949913637637693313639417883473760
s51	63999829606711522650915748086714806055520
s52	475648020504874336968975846703558704767360
s53	3539736620746899551478214384426524560969920
s54	26376309482014901194800065543131184691392320
s55	196786571758072254774209654628466146096941120
s56	1469930377434643825117255656238830229231391040
s57	10992599534625333878995280114433052775213597440
s58	82298082996123210666432106893608345734255512320
s59	616806373541881093477734895753501754683667475200

ORDER THREE

Appendix B (continued)

SUMS	VALUE
S0	1
S1	2
S2	7
S3	32
S4	177
S5	1122
S6	7898
S7	60398
S8	494078
S9	4274228
S10	38763298
S11	366039104
S12	3579512809
S13	36091415154
S14	373853631974
S15	3966563630394
S16	42997859838010
S17	475191259977060
S18	5344193918791710
S19	61066078557804360
S20	707984385321707910
S21	8318207051955884772
S22	98936727936728464152
S23	1190144254132426538652
S24	14467503754920598547852
S25	177588968969030657062952
S26	2199766555762125604480244
S27	27479841323744789830066304
S28	346013356369921918769855929
S29	4389333539509515126591248594
S30	56070810203828991362664847534
S31	720991537747532706012643525026
S32	9328596513998279672146714203426
S33	121407761182708178024779745555236
S34	1588853327416452312225693971901886
S35	20902698473348916294574193083438576
S36	276366709279158375016777229713551178
S37	3671353895684626011348096048652533188
S38	48991879229954382412465500058360070428
S39	656578339509065473624710057081932405468
S40	8835422665626508141712557966494394806108
S41	119361980337149820156413158335452884741480
S42	1618555251833277417723413502651871963117380
S43	22026306046942304682421202107440636378252080
S44	300775665856985037635815504148162320960569030
S45	4120680721821174437200697187060554338727113380
S46	56632089950769630959003010091719578219572701768
S47	780672963674065363024657714942613611640651191668
S48	10792880714535509030956272898321515183823343600148
S49	149630114772321753565389670918869975981300480583368
S50	2080024562297436725383387627342232184290452724623868
S51	28989631221925585334377822573493132380111499239694256
S52	405042859452333599815966969539580644980304039216295996
S53	5672895639230230744501228216933481231786496342059764296
S54	79637499355923524957310381320358435277891452641832058656
S55	1120481796741420900139026353148731893246859107399301109816
S56	15799141364786589904575760510447056727208857922105968342104
S57	223240203381865382931261283307541517610831772674383845140304
S58	3160762512031293096204497160156094620737550686304124391199144
S59	44839790319506826307665601833880717528407912782175379485606144

ORDER FOUR

SUMS	VALUE
S0	1
S1	2
S2	8
S3	44
S4	310
S5	2606
S6	25202
S7	272582
S8	3233738
S9	41454272
S10	567709144
S11	8230728508
S12	125413517530
S13	1996446632130
S14	33039704641922
S15	566087847780250
S16	10006446665899330
S17	181938461947322284
S18	3393890553702212368
S19	64807885247524512668
S20	1264344439859632559216
S21	25157307567003414461132
S22	509758613701956725065312
S23	10504632497377410035604512
S24	219882344614457972071894112
S25	4670084185135656513206765312
S26	100545485811075166151802795824
S27	2192418844178243335833955155336
S28	48379667285208331243156909951858
S29	1079611110993258648130498445227930
S30	24347329288405445022766602579123442
S31	554566629846326336323633836780509714
S32	12750735363523736895224533482780247714
S33	295784841468452675270005420750848137236
S34	6919476264486250695584491663120163937904
S35	163169952940281696912145006005492340179568
S36	3877071820176178830433674797637159283033876
S37	92790578667967629170910388674462669088090860
S38	2236101047387592560288927021551097525450121020
S39	54241035539604690484028904444539438691470414804
S40	1323989240924397287678504113074504691152647841900
S41	32511753934173216440442934840169645923808825880160
S42	802940141706099352768612717751656935735641885154128
S43	19939180912572384650238245526841891336089453041203076
S44	497753077340750439345361117379228609393516565922287616
S45	12488499358131177277361272166359232020651763382248580116
S46	314835804201793426134718207824493669241936791219996967272
S47	7974948166936771934625468937473862232444337311576280767968
S48	202903531153561613979904796282755350111618310117591503533536
S49	5184669810730751738195690096846261341819375230915901136000064
S50	133031155163064817158937067974769173342349063013900835309293824
S51	3427055486216516092233309733621545807996225269108441463298272448
S52	88626309532650460632389871849045042148680549782040988260727829632
S53	2300485147484122546569992300460137733495781737369600781780516134976
S54	59928849983050369859897945129004440086248293188817578582162240727680
S55	1566605017513482961732955658845929295951027100154584705176100343447424
S56	41090373302605147887752883307921674253835971440718737659073287348513408
S57	1081259820998848048353209424742475697589922619283381601497939222715737088
S58	28541983181144917576594561989169677540337165840094612722197240073620315232
S59	755716976463771668194168330657640641261070871073397885785459539567999933788

ORDER FIVE

References

1. Personal letters from Verner E. Hoggatt, Jr., to Daniel C. Fielder, dated June 15, 1977, August 19, 1977, and October 28, 1977.
2. F. R. K. Chung, R. L. Graham, V. E. Hoggatt, Jr., & M. Kleiman. "The Number of Baxter Permutations." *Journal of Combinatorial Theory 24.3* (1978):382-394.
3. G. Baxter & J. T. Joichi. "On Permutations Induced by Commuting Functions, and an Imbedding Question." *Math. Scand. 13* (1963):140-150.
4. W. M. Boyce. "Generation of a Class of Permutations Associated with Commuting Functions." *Math. Algorithms 2* (1967):14-26.
5. V. E. Hoggatt, Jr., & M. Bicknell. "Triangular Numbers." *Fibonacci Quarterly 12.3* (1974):221-230.
6. E. I. Jury. *Theory and Application of the z-Transform Method.* New York: Wiley & Sons, 1964.
7. D. Small, J. Hosack, & K. Lane. "Computer Algebra Systems in Undergraduate Instruction." *The College Mathematics Journal 17.5* (1987):423-433.
8. D. D. Shochat. "A Symbolic Mathematics System." *Creative Computing 8.10* (1982):26-33.

*****

PROPERTIES OF A RECURRING SEQUENCE

A. K. Agarwal
The Pennsylvania State University, Mont Alto, PA 17237
(Submitted June 1986)

1. Introduction

Recurring sequences such as the Fibonacci sequence defined by

$$F_0 = 0,\ F_1 = 1;\ F_n = F_{n-1} + F_{n-2},\ n \geq 2 \tag{1.1}$$

and the Lucas sequence given by

$$L_0 = 2,\ L_1 = 1;\ L_n = L_{n-1} + L_{n-2},\ n \geq 2, \tag{1.2}$$

have been extensively studied because they have many interesting combinatorial properties.

In the present paper, we study the sequence

$$\{L_{2n+1}\}_{n=0}^{\infty},$$

which obviously satisfies the recurrence relation

$$L_1 = 1,\ L_3 = 4,\ 3L_{2n+1} - L_{2n-1} = L_{2n+3}, \tag{1.3}$$

and is generated by [9, p. 125]

$$\sum_{k=0}^{n} L_{2n+1}t^n = (1 + t)(1 - 3t + t^2)^{-1},\ |t| < 1. \tag{1.4}$$

It can be shown that these numbers possess the following interesting property,

$$\sum_{n=0}^{\infty} (-1)^{n+k}\binom{2n+1}{n-k} L_{2k+1} = 1, \tag{1.5}$$

for every nonnegative integral value of n, which can be rewritten as

$$\sum_{k=0}^{n} \frac{(-1)^k L_{2k+1}}{(n-k)!\,(n+k+1)!} = \frac{(-1)^n}{(2n+1)!}. \tag{1.6}$$

In sections 2 and 3, we study two different q-analogues of L_{2n+1}. In the last section we pose some open problems and make some conjectures. As usual, we shall denote the rising q-factorial by

$$(a;\ q)_n = \prod_{i=0}^{\infty} \frac{(1 - aq^i)}{(1 - aq^{n+i})}. \tag{1.7}$$

Note that, if n is a positive integer, then

$$(a;\ q)_n = (1 - a)(1 - aq)\ \dots\ (1 - aq^{n-1}), \tag{1.8}$$

and

$$\lim_{n\to\infty}(a;\ q)_n = (a;\ q)_\infty = (1 - a)(1 - aq)(1 - aq^2)\dots\ . \tag{1.9}$$

The Gaussian polynomial $\begin{bmatrix} n \\ m \end{bmatrix}$ is defined by [4, p. 35]

$$\begin{bmatrix} n \\ m \end{bmatrix} = \begin{cases} (q;\ q)_n/(q;\ q)_m(q;\ q)_{n-m} & \text{if } 0 \le m \le n, \\ 0 & \text{otherwise.} \end{cases} \tag{1.10}$$

2. First q-Analogue of L_{2n+1}

To obtain our first q-analogue of L_{2n+1}, we use the following lemma, due to Andrews [5, Lemma 3, p. 8].

Lemma 2.1: If, for $n \ge 0$,

$$\beta_n = \sum_{k=0}^{n} \frac{\alpha_k}{(q;\ q)_{n-k}(aq;\ q)_{n+k}}, \tag{2.1}$$

then

$$\alpha_n = (1 - aq^{2n}) \sum_{k=0}^{n} \frac{(aq;\ q)_{n+k-1}(-1)^{n-k} q^{\binom{n-k}{2}} \beta_k}{(q;\ q)_{n-k}}. \tag{2.2}$$

Multiplying both sides of (2.1) by $(1 - q)^{-1}$, with $a = q$ and

$$\beta_n = \frac{(-1)^n}{(q^2;\ q)_{2n}},$$

and using (1.8), we obtain

$$\frac{(-1)^n}{(q;\ q)_{2n+1}} = \sum_{k=0}^{n} \frac{\alpha_k}{(q;\ q)_{n-k}(q;\ q)_{n+k+1}},\ n \ge 0, \tag{2.3}$$

which, when compared with (1.6), will give us our first q-analogue of L_{2n+1} if we let α_k play the role of $(-1)^k L_{2k+1}$. Observe that (2.3), by using (1.10), is equivalent to

$$\sum_{k=0}^{n} (-1)^n \alpha_k \begin{bmatrix} 2n + 1 \\ n - k \end{bmatrix} = 1,\ n \ge 0. \tag{2.4}$$

Letting $\alpha_k = C_k(q)(-1)^k$ in (2.4) and (2.3), we have

$$\sum_{k=0}^{n} (-1)^{n-k} \begin{bmatrix} 2n + 1 \\ n - k \end{bmatrix} C_k(q) = 1,\ n \ge 0, \tag{2.5}$$

and, by applying Lemma 2.1 to (2.3),

$$C_n(q) = \sum_{k=0}^{n} \begin{bmatrix} n + k \\ n - k \end{bmatrix} \frac{(1 - q^{2n+1}) q^{\binom{n-k}{2}}}{(1 - q^{2k+1})},\ n \ge 0. \tag{2.6}$$

Now we prove the following:

Theorem 2.1: For all $n \ge 0$, $C_n(q)$ is a polynomial.

Proof: Let

$$D_{n,j}(q) = \begin{bmatrix} n + j \\ n - j \end{bmatrix} \frac{1 - q^{2n+1}}{1 - q^{2j+1}} q^{\binom{n-j}{2}}. \tag{2.7}$$

Since

$$C_n(q) = \sum_{j=0}^{n} D_{n,j}(q),$$

it suffices to prove that $D_{n,j}(q)$ is a polynomial. Now

$$\begin{aligned}
D_{n,j}(q) &= \begin{bmatrix} n+j \\ n-j \end{bmatrix} \frac{(1 - q^{2j+1} + q^{2j+1} - q^{2n+1})}{(1 - q^{2j+1})} q^{\binom{n-j}{2}} \\
&= \begin{bmatrix} n+j \\ n-j \end{bmatrix} \left(1 + \frac{q^{2j+1}(1 - q^{2n-2j})}{1 - q^{2j+1}}\right) q^{\binom{n-j}{2}} \\
&= \begin{bmatrix} n+j \\ n-j \end{bmatrix} q^{\binom{n-j}{2}} + \frac{(q;\, q)_{n+j} q^{2j+1+\binom{n-j}{2}} (1 - q^{n-j})(1 + q^{n-j})}{(q;\, q)_{n-j} (q;\, q)_{2j} (1 - q^{2j+1})} \\
&= \begin{bmatrix} n+j \\ n-j \end{bmatrix} q^{\binom{n-j}{2}} + \begin{bmatrix} n+j \\ n-j-1 \end{bmatrix} q^{2j+1+\binom{n-j}{2}} (1 + q^{n-j}),
\end{aligned}$$

which is obviously a polynomial.

Theorem 2.2: The coefficient of q^n in $C_\infty(q)$ equals twice the number of partitions of n into distinct parts.

Proof: $$C_\infty(q) = \lim_{n\to\infty} C_n(q) = \lim_{n\to\infty} \sum_{j=0}^{n} \begin{bmatrix} 2n-j \\ j \end{bmatrix} \frac{(1 - q^{2n+1})}{(1 - q^{2n-2j+1})} q^{\binom{j}{2}}$$

$$= \sum_{j=0}^{\infty} \frac{1}{(q;\, q)_j} q^{\binom{j}{2}},$$ since it can be shown that

$$\lim_{n\to\infty} \begin{bmatrix} 2n+a \\ n+b \end{bmatrix} = \prod_{n=1}^{\infty} \frac{1}{1 - q^n}. \tag{2.8}$$

Using the identity [4, Eq. (2.2.6), p. 19], we have

$$\sum_{j=0}^{\infty} \frac{q^{\binom{j}{2}}}{(q;\, q)_j} = \prod_{n=0}^{\infty} (1 + q^n) = 2 \prod_{n=1}^{\infty} (1 + q^n). \tag{2.9}$$

Noting that $\prod_{n=1}^{\infty} (1 + q^n)$ generates partitions into distinct parts, we are done.

We now note that the numbers

$$D_{n,n-j}(1) = d_{n,j}$$

have a combinatorial meaning. However, we first recall the definitions of lattice points and lattice paths.

Definition 2.1: A point whose coordinates are integers is called a lattice point. (Unless otherwise stated, we take these integers to be nonnegative.)

Definition 2.2: By a lattice path (or simply a path), we mean a minimal path via lattice points taking unit horizontal and unit vertical steps.

In Church [2], it is shown that $d_{n,k}$ $(0 \le k \le n)$ is the number of lattice paths from $(0, 0)$ to $(2n + 1 - k, k)$ under the following two conditions:

(1) The paths do not cross $y = x + 1$ (or, equivalently, do not have two vertical steps in succession).

(2) The first and last steps cannot both be vertical.

Example: For $n = 3$, we have $d_{3,0} = 1$, $d_{3,1} = 7$, $d_{3,2} = 14$, and $d_{3,3} = 7$.

The values $d_{n,k}$ also appear along the rising diagonals (see [8, p. 486]).

3. Second q-Analogue of L_{2n+1}

The second q-analogue of the numbers L_{2n+1} is suggested by the q-extension of Fibonacci numbers found in the literature (cf. [3, p. 302; 1, p. 7]).

Equation (1.4) can be written as

$$\sum_{n=0}^{\infty} L_{2n+1}\, t^n = (1 + t) \sum_{n=0}^{\infty} \frac{t^n}{(1 - t)^{2n+2}}, \tag{3.1}$$

provided $|t/(1 - t)^2| < 1$.

Letting

$$\sum_{n=0}^{\infty} \overline{C}_n(q) t^n = (1 + t) \sum_{n=0}^{\infty} \frac{q^{n^2} t^n}{(t;\, q)_{2n+2}}, \tag{3.2}$$

we have

$$\sum_{n=0}^{\infty} \overline{C}_n(q) t^n = (1 + t) \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \begin{bmatrix} 2n + 1 + m \\ m \end{bmatrix} q^{n^2} t^{n+m}, \tag{3.3}$$

by using [4, Eq. (3.3.7), p. 36], which is

$$(z;\, q)_N^{-1} = \sum_{j=0}^{\infty} \begin{bmatrix} N + j - 1 \\ j \end{bmatrix} z^j. \tag{3.4}$$

Equating the coefficients of t^n in (3.3), we get

$$\overline{C}_n(q) = \sum_{m=0}^{n} B_{n,m}(q) + \sum_{m=0}^{n-1} B_{n-1,m}(q), \tag{3.5}$$

where

$$B_{n,m}(q) = q^{(n-m)^2} \begin{bmatrix} 2n - m + 1 \\ m \end{bmatrix}. \tag{3.6}$$

Since each $B_{n,m}(q)$ is a polynomial, $\overline{C}_n(q)$ is also a polynomial for all $n \geq 0$.

Theorem 3.1: Let

$$\overline{C}_\infty(q) = \lim_{t \to 1}(1 - t) \sum_{n=0}^{\infty} \overline{C}_n(q) t^n. \tag{3.7}$$

Then

$$\overline{C}_\infty(q) = 2(P_1(q) + qP_2(q)), \tag{3.8}$$

where $P_1(q)$ is an enumerative generating function which generates partitions into parts which are either odd or congruent to 16 or 4 (mod 20), and $P_2(q)$ is another enumerative generating function which generates partitions into parts which are either odd or congruent to 12 or 8 (mod 20).

Proof: Starting with the left-hand side of (3.7), we have

$$\begin{aligned}\overline{C}_\infty(q) &= \lim_{t\to 1}(1 - t)\sum_{n=0}^{\infty}\frac{(1 + t)q^{n^2}t^n}{(t;\, q)_{2n+2}} = 2\sum_{n=0}^{\infty}\frac{q^{n^2}}{(q;\, q)_{2n+1}}\\ &= 2\sum_{n=0}^{\infty}\frac{q^{n^2}}{(q;\, q)_{2n}}\left(1 + \frac{q^{2n+1}}{1 - q^{2n+1}}\right)\\ &= 2\sum_{n=0}^{\infty}\frac{q^{n^2}}{(q;\, q)_{2n}} + 2q\sum_{n=0}^{\infty}\frac{q^{n(n+2)}}{(q;\, q)_{2n+1}}.\end{aligned}$$

Now, an appeal to the following two identities found in Slater's compendium [6, I-(74), p. 160; I-(96), p. 162], i.e.,

$$\prod_{n=1}^{\infty}(1 - q^{20n-8})(1 - q^{20n-12})(1 - q^{20n})$$

$$= \prod_{n=1}^{\infty}\frac{(1 - q^{2n})}{(1 + q^{2n-1})}\sum_{n=0}^{\infty}\frac{q^{n^2}}{(q;\, q)_{2n}}, \tag{3.9}$$

and

$$\prod_{n=1}^{\infty}(1 - q^{10n-4})(1 - q^{10n-6})(1 - q^{20n-18})(1 - q^{20n-2})(1 - q^{10n})$$

$$= \prod_{n=1}^{\infty}(1 - q^n)\sum_{n=0}^{\infty}\frac{q^{n(n+2)}}{(q;\, q)_{2n+1}}, \tag{3.10}$$

proves the theorem.

Next, we define the polynomials $E_{n,m}(q)$ by

$$E_{n,m}(q) = \begin{cases} B_{n,m}(q) + B_{n-1,m}(q) & \text{if } 0 \le m \le n - 1,\\ \begin{bmatrix} n + 1\\ n\end{bmatrix} & \text{if } m = n,\\ 0 & \text{otherwise.}\end{cases} \tag{3.11}$$

To give a combinatorial interpretation of the polynomials $B_{n,m}(q)$ and $E_{n,m}(q)$, we consider an integer triangle whose entries $e_{n,k}$ ($n = 0, 1, 2, \ldots;\ 0 \le k \le n$) are given by

$$e_{n,k} = b_{n,k} + b_{n-1,k}, \tag{3.12}$$

where $b_{n,k}$ is the $(k + 1)^{\text{th}}$ coefficient in the expansion of $(x + y)^{2n+1-k}$ when $0 \le k \le n$, and $b_{n,k} = 0$ for $k > n$.

It can be shown that

$$\sum_{k=0}^{n} b_{n,k} = F_{2n+2} \quad\text{and}\quad \sum_{k=0}^{n} e_{n,k} = L_{2n+1}.$$

Note that $E_{n,m}(q)$ and $B_{n,m}(q)$ are q-extensions of the numbers $e_{n,m}$ and $b_{n,m}$ respectively. Moreover, $B_{n,m}(1) = b_{n,m}$ is the number of lattice paths from (1, 0) to $(2n + 1 - m, m)$ with no two successive vertical steps. Defining $E_n(q)$ by

$$E_n(q) = \sum_{k=0}^{n}\begin{bmatrix} 2n + 1\\ n - k\end{bmatrix}\overline{C}_k(q)(-1)^{n-k}, \tag{3.13}$$

it is easy to show that $E_n(q)$ is a polynomial in q where the sum of the coefficients is equal to unity.

Note also that (2.7) and (3.13) are q-analogues of (1.5).

Finally, we set

$$D_n(q) = \sum_{m=0}^{n} B_{n,m}(q), \tag{3.14}$$

and observe that $D_n(q)$ is a q-analogue of W_{n+1}, where W_n is the weighted composition function with weights 1, 2, ..., n [7, p. 39]; hence, (3.5) leads to the formula

$$L_{2n+1} = W_{n+1} + W_n,\ n \geq 1. \tag{3.15}$$

Note that the sum of the coefficients of $D_n(q)$ is the Fibonacci number F_{2n+2}.

We close this section with the following theorem, which is easy to prove.

Theorem 3.2: Let $\overline{C}_\infty(q)$ be defined by (3.7) and $D_\infty(q) = \lim_{n\to\infty} D_n(q)$, then

$$D_\infty(q) = \frac{1}{2}\overline{C}_\infty(q). \tag{3.16}$$

4. Conclusion

We have given several combinatorial interpretations of the polynomials

$$C_n(q),\ D_{n,m}(q),\ \overline{C}_n(q),\ B_{n,m}(q), \text{ and } E_{n,m}(q) \text{ at } q = 1,$$

the most obvious question that arises is: Is it possible to interpret these polynomials as generating functions? We make the following conjectures:

Conjecture 1: In the expansion of $C_n(q)$, the coefficient of q^k ($k \leq 2n - 2$) equals twice the number of partitions of k into distinct parts.

Conjecture 2: For $1 \leq k \leq n$, let

$A(k, n)$ = the number of partitions of k into parts $\not\equiv 0, \pm 2, \pm 6, \pm 8, 10 \pmod{20}$ + the number of partitions of $k - 1$ into parts $\not\equiv 0, \pm 2, \pm 4, \pm 6, 10 \pmod{20}$.

then the coefficient of q^k in the expansion of $D_n(q)$ equals $A(k, n)$.

Conjecture 3: In the expansion of $\overline{C}_n(q)$, the coefficient of q^k ($k \leq n - 1$) equals $2A(k, n - 1)$.

Remark: Theorems 2.2, 3.1, and 3.2 are the limiting cases $n \to \infty$ of Conjectures 1, 3, and 2 respectively.

We hope that some interested readers can prove Conjectures 1, 2, and 3.

Acknowledgment

I wish to thank the referee for his many helpful suggestions.

References

1. A. K. Agarwal & G. E. Andrews. "Hook Differences and Lattice Paths." *J. Statist. Plann. Inference* 14 (1986):5-14.

2. C. A. Church, Jr. "Lattice Paths and Fibonacci and Lucas Numbers." *Fibonacci Quarterly 12.4* (1974):336-338.
3. G. E. Andrews. "A Polynomial Identity which Implies the Rogers-Ramanujan Identities." *Scripta Math. 28* (1970):297-305.
4. G. E. Andrews. *The Theory of Partitions, Encyclopedia of Mathematics and Its Applications*. New York: Addison-Wesley, 1976.
5. G. E. Andrews. "Connection Coefficient Problems and Partitions, Relations between Combinatorics and Other Parts of Mathematics." D. K. Ray Chaudhuri, ed. *Proc. Symp. Pure Math. 34* (1979):1-24.
6. L. J. Slater. "Further Identities of the Rogers-Ramanujan Type. *Proc. London Math. Soc. 54.2* (1952):147-167.
7. L. Moser & E. L. Whitney. "Weighted Compositions." *Canadian Math. Bull. 4* (1961):39-43.
8. Mark Feinberg. "Lucas Triangle." *Fibonacci Quarterly 5* (1967):486-490.
9. V. E. Hoggatt, Jr. "Some Special Fibonacci and Lucas Generating Functions." *Fibonacci Quarterly 9.2* (1971):121-133.

*****

AN ASYMPTOTIC FORMULA CONCERNING A GENERALIZED EULER FUNCTION

L. Tóth and J. Sándor
N. Golescu Nr. 5, 3900 Satu-Mare and 4136 Forteni 79, Jud. Harghita, Romania
(Submitted April 1987)

1. Introduction

Harlan Stevens [8] introduced the following generalization of the Euler φ-function. Let $F = \{f_1(x), \ldots, f_k(x)\}$, $k \geq 1$, be a set of polynomials with integral coefficients and let A represent the set of all ordered k-tuples of integers $(a_1, \ldots, a_k)$ such that $0 \leq a_1, \ldots, a_k \leq n$. Then $\varphi_F(n)$ is the number of elements in A such that the g.c.d. $(f_1(a_1), \ldots, f_k(a_k)) = 1$. We have, for $n = \Pi_{j=1}^{r} p_j^{e_j}$,

$$\varphi_F(n) = n^k \cdot \prod_{j=1}^{r}\left(1 - \frac{N_{1j} \ldots N_{kj}}{p_j^k}\right)$$

where N_{ij} is the number of incongruent solutions of $f_i(x) \equiv 0 \pmod{p_j}$, see [8, Theorem 1].

This totient function is multiplicative and it is very general. As special cases, we obtain Jordan's well-known totient $J_k(n)$ [3, p. 147] for $f_1(x) = \cdots = f_k(x) = x$; the Euler totient function $\varphi(n) \equiv J_1(n)$; Schemmel's function $\phi_t(n)$ [7] for $k = 1$ and $f_1(x) = x(x+1) \ldots (x+t-1)$, $t \geq 1$; also the totients investigated by Nagell [5], Alder [1], and others (cf. [8]).

The aim of this paper is to establish an asymptotic formula for the summatory function of $\varphi_F(n)$ using elementary arguments and preserving the generality. We shall assume that each polynomial $f_i(x)$ has relatively prime coefficients, that is, for each

$$f_i(x) = a_{ir_i}x^{r_i} + a_{ir_i-1}x^{r_i-1} + \cdots + a_{i0}$$

the g.c.d. $(a_{ir_i}, a_{ir_i-1}, \ldots, a_{i0}) = 1$.

2. Prerequisites

We need the following result stated by Stevens [8].

Lemma 1:

$$\varphi_F(n) = \sum_{d|n} \mu(d)\Omega_F(d)\left(\frac{n}{d}\right)^k, \tag{1}$$

where μ is the Möbius function and $\Omega_F(n)$ is a completely multiplicative function defined as follows: $\Omega_F(1) = 1$ and, for $1 < n = \Pi_{j=1}^{r} p_j^{e_j}$,

$$\Omega_F(n) = \prod_{j=1}^{r}(N_{1j} \ldots N_{kj})^{e_j}.$$

Under the assumption mentioned in the Introduction, we now prove

Lemma 2:

$$|\mu(n)\Omega_F(n)| = O(n^\varepsilon) \text{ for all positive } \varepsilon. \tag{2}$$

Proof: Suppose the congruence

$$f_i(x) = a_{ir_i}x^{r_i} + a_{ir_i-1}x^{r_i-1} + \cdots + a_{i0} \equiv 0 \pmod{p_j}$$

is of degree s_{ij}, $0 \le s_{ij} \le r_i$, where

$$a_{is_{ij}} \not\equiv 0 \pmod{p_j}.$$

Then, as is well known (by Lagrange's theorem), the congruence

$$f_i(x) \equiv 0 \pmod{p_j}$$

has at most s_{ij} incongruent roots, where $s_{ij} \le r_i$ for all primes p_j; therefore, $N_{ij} \le r_i$ for all primes p_j and $N_{ij} \le 2 + \max_{1\le i\le k} r_i = M$, $M > 1$, for all i and j.

Now, for $n = \Pi_{j=1}^{r} p_j^{e_j}$, $|\mu(n)\Omega_F(n)| = 0$ if j exists such that $e_j \ge 2$; otherwise,

$$|\mu(n)\Omega_F(n)| = \left|(-1)^r \cdot \prod_{j=1}^{r}(N_{1j} \ \ldots \ N_{kj})\right| \le (M^k)^r.$$

Hence, $|\mu(n)\Omega_F(n)| \le A^{\omega(n)}$ for all n, where $A = M^k > 1$.

On the other hand, one has

$$2^{\omega(n)} = 2^r \le \prod_{j=1}^{r}(e_j + 1) = d(n),$$

so $\omega(n) \le \log_2 A$, which implies

$$|\mu(n)\Omega_F(n)| \le A^{\log_2 d(n)}.$$

Further, it is known that $d(n) = O(n^{\alpha})$ for all $\alpha > 0$ (see [4, Theorem 315]). By choosing $\alpha = \varepsilon/\log_2 A > 0$, we obtain $|\mu(n)\Omega_F(n)| = O(n^{\varepsilon})$, as desired.

Lemma 3: The series

$$\sum_{n=1}^{\infty}\frac{\mu(n)\,\Omega_F(n)}{n^{s+1}}$$

is absolutely convergent for $s > 0$, and its sum is given by

$$\lambda_F(s) = \prod_p\left(1 - \frac{N_1 \cdots N_k}{p^{s+1}}\right), \tag{3}$$

where N_i denotes the number of incongruent solutions of $f_i(x) \equiv 0 \pmod{p}$.

Proof: The absolute convergence follows by Lemma 2:

$$|\mu(n)\Omega_F(n)/n^{s+1}| \le K \cdot 1/n^{s+1-\varepsilon},$$

where $K > 0$ is a constant and $\varepsilon > 0$ is such that $s - \varepsilon > 0$. Note that the general term is multiplicative in n, so the series can be expanded into an infinite Euler-type product [3, 17.4]:

$$\sum_{n=1}^{\infty}\frac{\mu(n)\Omega_F(n)}{n^s} = \prod_p\left(\sum_{\ell=0}^{\infty}\frac{\mu(p^{\ell})\Omega_F(p^{\ell})}{p^{\ell s}}\right) = \prod_p\left(1 - \frac{\Omega_F(p)}{p^s}\right) = \lambda_F.$$

From here on, we shall use the following well-known estimates.

Lemma 4:

$$\sum_{n\le x} n^s = \frac{x^{s+1}}{s+1} + O(x^s), \quad s > 1; \tag{4}$$

$$\sum_{n \le x} \frac{1}{n^s} = O(x^{1-s}), \quad 0 < s < 1; \tag{5}$$

$$\sum_{n > x} \frac{1}{n^s} = O\left(\frac{1}{x^{s-1}}\right), \quad s > 1. \tag{6}$$

3. Main Results

Theorem 1:

$$\sum_{n \le x} \varphi_F(n) = \frac{\lambda_F(k)x^{k+1}}{k+1} + O(R_k(x)), \tag{7}$$

where $R_k(x) = x^k$ or $x^{1+\varepsilon}$ (for all $\varepsilon > 0$) according as $k \ge 2$ or $k = 1$.

Proof: Using (1) and (4), one has

$$\begin{aligned}\sum_{n \le x} \varphi_F(n) &= \sum_{d\delta = n \le x} \mu(d)\Omega_F(d)\delta^k = \sum_{d \le x} \mu(d)\Omega_F(d) \sum_{\delta \le x/d} \delta^k \\ &= \sum_{d \le x} \Omega_F(d)\mu(d)\left\{\frac{1}{k+1} \cdot (x/d)^{k+1} + O((x/d)^k)\right\} \\ &= \frac{x^{k+1}}{k+1} \cdot \sum_{d=1}^{\infty} \frac{\mu(d)\Omega_F(d)}{d^{k+1}} + O\left(x^{k+1} \cdot \sum_{d > x} \frac{|\mu(d)\Omega_F(d)|}{d^{k+1}}\right) \\ &\quad + O\left(x^k \cdot \sum_{d \le x} \frac{|\mu(d)\Omega_F(d)|}{d^k}\right).\end{aligned}$$

Here the main term is

$$\frac{\lambda_F(k)x^{k+1}}{k+1}$$

by (3); then, in view of (2) and (6), the first remainder term becomes

$$O\left(x^{k+1} \cdot \sum_{d > x} \frac{d^\varepsilon}{d^{k+1}}\right) = O\left(x^{k+1} \cdot \sum_{d > x} \frac{1}{d^{k+1-\varepsilon}}\right) = O(x^{1+\varepsilon}) \quad \text{(choosing } 0 < \varepsilon < 1\text{)}.$$

For the second remainder term, (2) implies

$$O\left(x^k \cdot \sum_{d \le x} \frac{d^\varepsilon}{d^k}\right) = O\left(x^k \cdot \sum_{d \le x} \frac{1}{d^{k-\varepsilon}}\right),$$

which is

$$O(x^k) \text{ for } k \ge 2, \text{ and } O(x \cdot x^{1-1+\varepsilon}) = O(x^{1+\varepsilon}) \text{ for } k = 1 \text{ [by (5)]}.$$

This completes the proof of the theorem.

For $f_1(x) = \cdots = f_k(x) = x$, we have $N_{ij} = 1$ for all i and j; thus, $\varphi_F(n) = J_k(n)$ - the Jordan totient function. This yields

Corollary 1 (cf. [2, (3.7) and (3.8)]):

$$\sum_{n \le x} J_k(n) = \frac{x^{k+1}}{(k+1)\zeta(k+1)} + O(x^k), \quad k \ge 2; \tag{8}$$

$$\sum_{n \le x} \varphi(n) = \frac{x^2}{2\zeta(2)} + O(x^{1+\varepsilon}), \quad k = 1, \text{ for all } \varepsilon > 0, \tag{9}$$

where $\zeta(s)$ is the Riemann zeta function.

Remark: The O-term of (9) can easily be improved into $O(x \log x)$, see Mertens' formula [4, Theorem 330].

By selecting $k = 1$ and $f_1(x) = x(x + 1) \ldots (x + t - 1)$, $t \geq 1$, we get

$$\varphi_F(n) = \phi_t(n) \text{ - Schemmel's totient function [7],}$$

for which $N_1 = p$ if $p < t$, and $N_1 = t$ if $p \geq t$. Using Theorem 1, we conclude

Corollary 2:

$$\sum_{n \leq x} \phi_t(n) = \frac{x^2}{2} \prod_{p < t}\left(1 - \frac{1}{p}\right) \cdot \prod_{p \geq t}\left(1 - \frac{t}{p^2}\right) + O(x^{1+\varepsilon}) \text{ for all } \varepsilon > 0. \tag{10}$$

For $t = 2$, $\phi_2(n) \equiv \varphi'(n)$, see [6, p. 37, Ex. 20], and we have

Corollary 3:

$$\sum_{n \leq x} \varphi'(n) = \frac{x^2}{2} \cdot \prod_{p}\left(1 - \frac{2}{p^2}\right) + O(x^{1+\varepsilon}) \text{ for all } \varepsilon > 0. \tag{11}$$

Choosing $k = 1$ and $f_1(x) = x(\lambda - x)$, we obtain

$$\varphi_F(n) \equiv \theta(\lambda, n) \text{ - Nagell's totient function [5],}$$

where $N_1 = 1$ or 2, according as $p \mid \lambda$ or $p \nmid \lambda$, and we have

Corollary 4:

$$\sum_{n \leq x} \theta(\lambda, n) = \frac{x^2}{2} \cdot \prod_{p \mid \lambda}\left(1 - \frac{1}{p^2}\right) \cdot \prod_{p \nmid \lambda}\left(1 - \frac{2}{p^2}\right) + O(x^{1+\varepsilon}) \text{ for all } \varepsilon > 0. \tag{12}$$

Now, let $f_1(x) = \cdots = f_k(x) = x^2 + 1$, $N_i = 1$, 2, or 0, according as $p = 2$, $p \equiv 1 \pmod 4$, or $p \equiv 3 \pmod 4$, see [8, Ex. 4]. In this case, we have

Corollary 5:

$$\sum_{n \leq x} \varphi_F(n) = \frac{x^{k+1}}{k + 1}\left(1 - \frac{1}{2^{k+1}}\right) \cdot \prod_{p \equiv 1 \pmod 4}\left(1 - \frac{2^k}{p^{k+1}}\right) \tag{13}$$

$$+ O(R_k(x)), \text{ with } R_k(x) \text{ as given in Theorem 1.}$$

Theorem 2: Let $f(x)$ be a polynomial with integral coefficients. The probability that for two positive integers a, b, $a \leq b$, we have $(f(a), b) = 1$ is

$$\prod_{p}\left(1 - \frac{N(p)}{p^2}\right),$$

where $N(p)$ denotes the number of incongruent solutions of $f(x) \equiv 0 \pmod p$.

Proof: Let n be a fixed positive integer and consider all the pairs of integers (a, b) satisfying $1 \leq a \leq b \leq n$:

$$\begin{array}{ccccc}
(1, 1) & (1, 2) & (1, 3) & \ldots & (1, n) \\
 & (2, 2) & (2, 3) & \ldots & (2, n) \\
 & & (3, 3) & \ldots & (3, n) \\
 & & & \ddots & \vdots \\
 & & & & (n, n)
\end{array}$$

There are

$$A(n) = \frac{n(n+1)}{2} \sim \frac{n^2}{2}$$

such pairs and the property $(f(a), b) = 1$ is true for $B(n)$ pairs of them, where

$$B(n) = \varphi_F(1) + \varphi_F(2) + \cdots + \varphi_F(n) \sim \frac{n^2}{2} \cdot \prod_p \left(1 - \frac{N(p)}{p^2}\right) \text{ by Theorem 1.}$$

Hence, the considered probability is

$$\lim_{n \to \infty} \frac{B(n)}{A(n)} = \prod_p \left(1 - \frac{N(p)}{p^2}\right).$$

As immediate consequences, we obtain, for example:

Corollary 6 [4, Theorem 332]: The probability of two positive integers being prime to one another is

$$1/\zeta(2) = 6/\pi^2.$$

Corollary 7 $(\Omega_F(n) = \phi_2(n))$: The probability that, for two positive integers a and b, $a \le b$, we have $(a(a+1), b) = 1$, is

$$\prod_p \left(1 - \frac{2}{p^2}\right).$$

Acknowledgment

The authors wish to thank the referee for helpful suggestions.

References

1. H. L. Alder. "A Generalization of the Euler φ-Function." *Amer. Math. Monthly* *65* (1958):690-692.
2. E. Cohen. "An Elementary Method in the Theory of Numbers." *Duke Math. J.* *28* (1961):183-192.
3. L. E. Dickson. *History of the Theory of Numbers*. Vol. I. New York: Chelsea, 1952.
4. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford: Clarendon Press, 1960.
5. T. Nagell. "Verallgemeinerung eines Satzes von Schemmel." *Skr. Norske Vid. Akad. Oslo I. Math.-Naturv. Klasse* *13* (1923):23-25.
6. I. Niven & H. S. Zuckerman. *An Introduction to the Theory of Numbers*. New York: Wiley & Sons, 1960.
7. V. Schemmel. "Uber relative Primzahlen." *J. Reine Angew. Math.* *70* (1869): 191-192.
8. H. Stevens. "Generalizations of the Euler φ-Function." *Duke Math. J.* *38* (1971):181-186.
9. Problem E.2330. *Amer. Math. Monthly* *78* (1971):1138.

*****

ELEMENTARY PROBLEMS AND SOLUTIONS

Edited by

A. P. Hillman

Please send all communications regarding ELEMENTARY PROBLEMS AND SOLUTIONS to Dr. A. P. HILLMAN; 709 SOLANO DR., S.E.; ALBUQUERQUE, NM 87108. Each solution or problem should be on a separate sheet (or sheets). Preference will be given to those typed with double spacing in the format used below. Solutions should be received within four months of the publication date.

DEFINITIONS

The Fibonacci numbers F_n and the Lucas numbers L_n satisfy

$$F_{n+2} = F_{n+1} + F_n,\ F_0 = 0,\ F_1 = 1$$

and

$$L_{n+2} = L_{n+1} + L_n,\ L_0 = 2,\ L_1 = 1.$$

PROBLEMS PROPOSED IN THIS ISSUE

<u>B-640</u> *Proposed by Russell Euler, Northwest Missouri State U., Marysville, MO*

Find the determinant of the $n \times n$ matrix (x_{ij}) with $x_{ij} = 1$ for $j = i$ and for $j = i - 1$, $x_{ij} = -1$ for $j = i + 1$, and $x_{ij} = 0$, otherwise.

<u>B-641</u> *Proposed by Dario Castellanos, U. de Carabobo, Valencia, Venezuela*

Prove that

$$F_{mn} = \frac{1}{\sqrt{5}}\left[\left(\frac{L_m + \sqrt{5}F_m}{2}\right)^n - \left(\frac{L_m - \sqrt{5}F_m}{2}\right)^n\right],$$

$$L_{mn} = \left(\frac{L_m + \sqrt{5}F_m}{2}\right)^n + \left(\frac{L_m - \sqrt{5}F_m}{2}\right)^n.$$

<u>B-642</u> *Proposed by Piero Filipponi, Fond. U. Bordoni, Rome, Italy*

It is known that

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

and it can readily be proven that

$$L_{3(2n+1)} = L_{2n+1}^3 + 3L_{2n+1}.$$

Generalize these identities by expressing $L_{k(2n+1)}$, for integers $k \geq 2$, as a polynomial in L_{2n+1}.

<u>B-643</u> *Proposed by T. V. Padnakumar, Trivandrum, South India*

For positive integers a, n, and p, with p prime, prove that

$$\binom{n + ap}{p} - \binom{n}{p} \equiv a \pmod{p}.$$

B-644 *Proposed by H. W. Corley, U. of Texas at Arlington*

Consider three children playing catch as follows. They stand at the vertices of an equilateral triangle, each facing its center. When any child has the ball, it is thrown to the child on her or his left with probability 1/3 and to the child on the right with probability 2/3. Show that the probability that the initial holder has the ball after n tosses is

$$\frac{2}{3}\left(\frac{\sqrt{3}}{3}\right)^n \cos\left(\frac{5n\pi}{6}\right) + \frac{1}{3} \text{ for } n = 0, 1, 2, \ldots .$$

B-645 *Proposed by R. Tošić, U. of Novi Sad, Yugoslavia*

Let

$$G_{2m} = \binom{2m-1}{m} - 2\binom{2m-1}{m-3} + \binom{2m}{m-5} \text{ for } m = 1, 2, 3, \ldots,$$

$$G_{2m+1} = \binom{2m}{m} - \binom{2m+1}{m-2} + 2\binom{2m}{m-5} \quad \text{for } m = 0, 1, 2, \ldots,$$

where $\binom{n}{k} = 0$ for $k < 0$. Prove or disprove that $G_n = F_n$ for $n = 0, 1, 2, \ldots$.

SOLUTIONS

Cyclic Permutations Modulo 6 and Modulo 5

B-616 *Proposed by Stanley Rabinowitz, Alliant Computer Systems Corp., Littleton, MA*

(a) Find the smallest positive integer a such that

$$L_n \equiv F_{n+a} \pmod 6 \text{ for } n = 0, 1, \ldots .$$

(b) Find the smallest positive integer b such that

$$L_n \equiv F_{5n+b} \pmod 5 \text{ for } n = 0, 1, \ldots .$$

Solution by Piero Filipponi, Fond. U. Bordoni, Rome, Italy

By inspection of the sequences $\{L_n\}$ and $\{F_n\}$ reduced modulo 6 (both with repetition period equal to 24), it is readily seen that $a = 6$.

By inspection of the above sequences reduced modulo 5 (repetition period equals 8 for $\{L_n\}$ and 20 for $\{F_n\}$), it is readily seen that $b = 3$.

Also solved by Paul S. Bruckman, Herta T. Freitag, L. Kuipers, Bob Prielipp, H.-J. Seiffert, Sahib Singh, Lawrence Somer, and the proposer.

Fibonacci Parallelograms

B-617 *Proposed by Stanley Rabinowitz, Littleton, MA*

Let R be a rectangle each of whose vertices has Fibonacci numbers as its coordinates x and y. Prove that the sides of R must be parallel to the coordinate axes.

Solution taken from those by Paul S. Bruckman, Fair Oaks, CA and Philip L. Mana, Albuquerque, NM

It will be shown that the rectangle either has its sides parallel to the axes or it is a square whose sides have inclinations 45° and -45°.

Let (F_a, F_h), (F_b, F_i), (F_c, F_j), (F_d, F_k) be the vertices of a parellelogram in counterclockwise order. If its sides are not parallel to the axes, we may assume that

$$F_a < F_b < F_c \quad \text{and} \quad F_a < F_d < F_c. \tag{1}$$

Since the diagonals bisect each other,

$$F_a + F_c = F_b + F_d. \tag{2}$$

By (1), $c - a \geq 2$, so $F_a + F_c$ is a unique Zeckendorf representation. This, with (1) and (2), implies that $b = d$ and that $b = a + 2$ and $c = a + 3$.

Similarly, one has

$$F_i < F_h < F_j \quad \text{and} \quad F_i < F_j < F_k$$

and can show that $j = h = i + 2$ and $k = i + 3$. Now the slope of two sides is

$$\frac{F_i - F_h}{F_b - F_a} = \frac{F_i - F_{i+2}}{F_{a+2} - F_a} = -\frac{F_{i+1}}{F_{a+1}}$$

and the slope of the other sides is F_{i+1}/F_{a+1}. Thus, the parallelogram is a rectangle if and only if $F_{i+1}^2 = F_{a+1}^2$. This happens (for nonnegative subscripts) if and only if $F_{i+1} = F_{a+1}$. This, in turn, is true if and only if $i = a$ or $\{i, a\} = \{0, 1\}$. These cases give the rectangles with vertices

(F_a, F_{a+2}),	(F_{a+2}, F_a),	(F_{a+3}, F_{a+2}),	(F_{a+2}, F_{a+3});
(0, 2),	(1, 1),	(2, 2),	(1, 3);
(2, 0),	(1, 1),	(2, 2),	(3, 1).

Each of these is a square whose sides have inclinations 45° and -45°.

Counterexamples (that is, squares with sides not parallel to the axes) given by Piero Filipponi and Herta Freitag.

Multiples of 40

B-618 *Proposed by Herta T. Freitag, Roanoke, VA*

Let $S(n) = L_{2n+1} + L_{2n+3} + L_{2n+5} + \cdots + L_{4n-1}$. Prove that $S(n)$ is an integral multiple of 10 for all even positive integers.

Solution by Sahib Singh, Clarion U. of Pennsylvania, Clarion, PA

We prove a more general result, namely:

$$S(n) \equiv 0 \pmod{40} \text{ for all even positive integers } n.$$

Using Binet form for Lucas numbers with $L_m = \alpha^m + \beta^m$, we have:

$$S(n) = \alpha^{2n+1}\sum_{i=0}^{n-1}\alpha^{2i} + \beta^{2n+1}\sum_{i=0}^{n-1}\beta^{2i}$$

$$= \alpha^{4n} - \alpha^{2n} + \beta^{4n} - \beta^{2n} = L_{4n} - L_{2n}.$$

Let $n = 2k$, then

$$S(2k) = L_{8k} - L_{4k} = 5F_{6k}F_{2k}, \text{ where } k \geq 1,$$

by using I_{16} and I_{25} in Hoggatt's *Fibonacci and Lucas Numbers*.

Since F_6 divides F_{6k}; we conclude that:

$$S(2k) \equiv 0 \pmod{40}.$$

Also solved by Paul S. Bruckman, David M. Burton, Piero Filipponi, L. Kuipers, Bob Prielipp, H.-J. Seiffert, Lawrence Somer, and the proposer.

More Multiples of 10

B-619 *Proposed by Herta T. Freitag, Roanoke, VA*

Let $T(n) = F_{2n+1} + F_{2n+3} + F_{2n+5} + \cdots + F_{4n-1}$. For which positive integers n is $T(n)$ an integral multiple of 10?

Solution by David M. Burton, U. of New Hampshire, Durham, NH

$T(n)$ is an integral multiple of 10 provided n is a multiple of 5. First, note that the identity

$$F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$$

gives us $T(n) = F_{4n} - F_{2n}$.

Now

$$F_{4n} - F_{2n} \equiv 2n \text{ or } 4n \pmod 5,$$

according as n is odd or even; thus, $T(n) \equiv 0 \pmod{10}$ if and only if 5 divides n.

To see that $F_{4n} - F_{2n} \equiv 2n$ or $4n \pmod 5$, simply use the congruence

$$F_{2n} \equiv n(-1)^{n+1} \pmod 5.$$

[see the solution to Problem B-379 in the April 1979 issue], which yields

$$F_{4n} - F_{2n} \equiv 4n[2 - (-1)^n] \pmod 5.$$

This could equally well be derived from the congruence

$$F_{2n} = nL_n \pmod 5$$

[see the solution to Problem B-368 in the December 1978 issue], together with the two relations

$$L_{2n} = 5F_n^2 + 2(-1)^n \equiv 2 \text{ or } 3 \pmod 5,$$

$$L_{4n} = 5F_{2n}^2 + 2 \equiv 2 \pmod 5.$$

Also solved by Paul S. Bruckman, Piero Filipponi, L. Kuipers, Bob Prielipp, H.-J. Seiffert, Sahib Singh, Lawrence Somer, and the proposer.

Congruence Modulo 9

B-620 *Proposed by Philip L. Mana, Albuquerque, NM*

Prove that $F^n_{24k+3} + F^n_{24k+5} \equiv 2F^n_{24k+6} \pmod 9$ for all n and k in $N = \{0, 1, 2, \ldots\}$.

Solution by Paul S. Bruckman, Fair Oaks, CA

The sequence $(F_n \pmod 9))_{n=0}^{\infty}$ is periodic with period 24, and the period is as follows:

$$(0,1,1,2,3,5,8,4,3,7,1,8,0,8,8,7,6,4,1,5,6,2,8,1).$$

Inspection of this period shows that:

$$F_{24k+3} \equiv 2,\ F_{24k+5} \equiv 5, \text{ and } F_{24k+6} \equiv 8 \pmod 9.$$

The problem is therefore equivalent to proving the congruence

$$2^n + 5^n \equiv 2 \cdot 8^n \pmod 9, \text{ for all } n. \tag{1}$$

We form the sequences

$$(2^n \pmod 9))_{n=0}^{\infty},\ (5^n \pmod 9))_{n=0}^{\infty}, \text{ and } (2 \cdot 8^n \pmod 9))_{n=0}^{\infty},$$

and find that these are all periodic of period 6; these periods are,

$$(1,2,4,8,7,5),\ (1,5,7,8,4,2), \text{ and } (2,7,2,7,2,7),$$

respectively (actually, the last sequence is periodic with only period 2, but we have triplicated the terms in order to make them compatible with those of the other two sequences). Therefore, we see that in all cases, the congruence in (1) is satisfied, proving the original problem.

Also solved by Odoardo Brugia & Piero Filipponi, Herta T. Freitag, L. Kuipers, Bob Prielipp, Sahib Singh, Lawrence Somer, and the proposer.

Powers of F_{2h} modulo F_{2h-1}

B-621 *Proposed by Piero Filipponi, Fond. U. Bordoni, Rome, Italy*

Let $n = 2h - 1$ with h a positive integer. Also, let $K(n) = F_hL_{h-1}$. Find sufficient conditions on F_n to establish the congruence

$$F_{n+1}^{K(n)} \equiv 1 \pmod{F_n}.$$

Solution by Sahib Singh, Clarion U. of Pennsylvania, Clarion, PA

As $n + 1$ is even, therefore using I_{13} of Hoggatt's *Fibonacci and Lucas Numbers*, we have

$$F_nF_{n+2} = F_{n+1}^2 + 1 \Rightarrow F_{n+1}^2 \equiv -1 \pmod{F_n}.$$

Thus, the order of F_{n+1} modulo F_n is 4.

From the property of order, it follows that:

$$F_{n+1}^{F_hL_{h-1}} \equiv 1 \pmod{F_n} \text{ is true only when 4 divides } F_hL_{h-1}.$$

This is possible when 4 divides F_h or 4 divides L_{h-1}. (Since 2 is not a factor of F_h and also a factor of F_{h-1} for any h.)t possible for any h.)

$$4 \text{ divides } F_h \Rightarrow h = 6t \text{ or } n = 12t - 1.$$

$$4 \text{ divides } L_{h-1} \Rightarrow h - 1 = (2t - 1)3 \Rightarrow h = 6t - 2 \Rightarrow n = 12t - 5.$$

Thus, the required values of n are 1 and 3, together with those positive integers n which satisfy

$$n \equiv 7 \pmod{12} \quad \text{or} \quad n \equiv 11 \pmod{12}.$$

Also solved by Paul S. Bruckman, L. Kuipers, Bob Prielipp, Lawrence Somer, and the proposer.

*****

LETTER TO THE EDITOR

February 3, 1989

Dear Dr. Bergum,

I'd like to point out that some results which appeared in Michael Mays's recent article, "Iterating the Division Algorithm" [*Fib. Quart.* 25 (1987):204-213] were already known.

In particular, his Algorithm 6, which on input (b, a) sets $a = a$ and $a_1 = b \bmod a$, appeared in my paper, "Metric Theory of Pierce Expansions," [*Fib. Quart.* 24 (1986):22-40]. His Theorem 4, proving that $L(b, a) \leq 2\sqrt{b} + 2$ [where $L(b, a)$ is the least n such that $a = 0$), appears in my paper as Theorem 19.

Let Ω, Ω' be defined as follows: we write $f(n) = \Omega(g(n))$ if there exist c, N such that $f(n) \geq cg(n)$ for all $n \geq N$. We write $f(n) = \Omega'(g(n))$ if there exists c such that $f(n) \geq cg(n)$ infinitely often. Since my paper appeared, I have proved

$$\max_{1 \leq a \leq n} L(n, a) = \Omega'(\log n)$$

and

$$\sum_{1 \leq a \leq n} L(n, a) = \Omega(n \log \log n).$$

The details are available to those interested.

Recently, I also stumbled across what may be the first reference to this type of algorithm. It is J. Binet, "Recherches sur la théorie des nombres entiers et sur la résolution de l'équation indéterminee du premier degré qui n'admet que des solutions entières," *J. Math. Pures Appl.* 6 (1841):449-494. Binet's algorithm, however, takes the *absolutely least residue* at each step, rather than the positive residue, and it is therefore easier to prove there are no long expansions.

Sincerely yours,

Jeffrey Shallit

ADVANCED PROBLEMS AND SOLUTIONS

Edited by

Raymond E. Whitney

Please send all communications concerning ADVANCED PROBLEMS AND SOLUTIONS to RAYMOND E. WHITNEY, MATHEMATICS DEPARTMENT, LOCK HAVEN UNIVERSITY, LOCK HAVEN, PA 17745. This department especially welcomes problems believed to be new or extending old results. Proposers should submit solutions or other information that will assist the editor. To facilitate their consideration, all solutions should be submitted on separate signed sheets within two months after publication of the problems.

PROBLEMS PROPOSED IN THIS ISSUE

H-430 *Proposed by Larry Taylor, Rego Park, NY*

Find integers j, $-2 < k < +2$, m_i and n_i such that:

(A) $5F_{m_i}F_{n_i} = L_k + L_{j+i}$, for $i = 1, 5, 9, 13, 17, 21$;

(B) $5F_{m_i}F_{n_i} = L_k - L_{j+i}$, for $i = 3, 7, 11, 15, 19, 23$;

(C) $F_{m_i}L_{n_i} = F_k + F_{j+i}$, for $i = 1, 2, \ldots, 22, 23$;

(D) $L_{m_i}F_{n_i} = F_k - F_{j+i}$, for $i = 1, 3, \ldots, 21, 23$;

(E) $L_{m_i}L_{n_i} = L_k - L_{j+i}$, for $i = 1, 5, 9, 13, 17, 21$;

(F) $L_{m_i}L_{n_i} = L_{-k} + L_{j+i}$, for $i = 2, 4, 6, 8$;

(G) $L_{m_i}L_{n_i} = L_k + L_{j+i}$, for $i = 3, 7, 11, 15, 16, 18, 19, 20, 22, 23$;

(H) $L_{m_i}L_{n_i} = L_k + F_{j+i}$, for $i = 10$;

(I) $L_{m_i}F_{n_i} = L_k + F_{j+i}$, for $i = 12$;

(J) $5F_{m_i}F_{n_i} = L_k + F_{j+i}$, for $i = 14$.

H-431 *Proposed by Piero Filipponi, Rome, Italy*

LA CATENA DI S. ANTONIO (St. Anthony's chain)

Let us consider a town having n (≥ 1) residents.

Step 1: One of them first draws out at random k ($1 \leq k \leq n$) distinct names from a directory containing the names of all town-dwellers (possibly, he/she may draw out also his/her own name), then he/she sends each of them an envelope containing one dollar.

Step 2: Every receiver (possibly, the sender himself/herself) acts as the sender.

Steps 3, 4, ...: As Step 2.

Find the probability $P_m(s, k, n)$ that, after s (≥ 1) steps, every town-dweller has received at least m (≥ 1) dollars.

Remark: It can readily be seen that

$$P_m(s,\ n,\ n) = 1 \text{ for } s = m,\ \lim_{s\to\infty} P_m(s,\ k,\ n) = 1, \text{ and}$$

$$P_1(s,\ k,\ n) = 0 \text{ if } s \le \begin{cases} n - 1 & (\text{for } k = 1) \\ \log_k(n(k-1)+1) - 1 & (\text{for } 1 < k < n). \end{cases}$$

<u>H-432</u> *Proposed by Piero Filipponi, Rome, Italy*

For k and n nonnegative integers and m a positive integer, let $M(k,\ n,\ m)$ denote the arithmetic mean taken over the k^{th} powers of m consecutive Lucas numbers of which the smallest is L_n.

$$M(k,\ n,\ m) = \frac{1}{m}\sum_{j=n}^{n+m-1} L_j^k.$$

For $k = 2^h$ ($h = 0, 1, 2, 3$), find the smallest nontrivial value m_h ($m_h > 1$) of m for which $M(k,\ n,\ m)$ is integral for every n.

SOLUTIONS

<u>Old Timer</u>

<u>H-365</u> *Proposed by Larry Taylor, Rego Park, NY*
(Vol. 22.1, February 1984)

Call a Fibonacci-Lucas identity divisible by 5 if every term of the identity is divisible by 5. Prove that, for every Fibonacci-Lucas identity not divisible by 5, there exists another Fibonacci-Lucas identity not divisible by 5 that can be derived from the original identity in the following way:

1) If necessary, restate the original identity in such a way that a derivation is possible.

2) Change one factor in every term of the original identity from F_n to L_n or from L_n to $5F_n$ in such a way that the result is also an identity. If the resulting identity is not divisible by 5, it is the derived identity.

3) If the resulting identity is divisible by 5, change one factor in every term of the original identity from L_n to F_n or from $5F_n$ to L_n in such a way that the result is also an identity. This is equivalent to dividing every term of the first resulting identity by 5. Then, the second resulting identity is the derived identity.

For example, $F_nL_n = F_{2n}$ can be restated as

$$F_nL_n = F_{2n} \pm F_0(-1)^n.$$

This is actually two distinct identities, of which the derived identities are

$$L_n^2 = L_{2n} + L_0(-1)^n$$

and

$$5F_n^2 = L_{2n} - L_0(-1)^n.$$

Partial solution by the proposer

<u>1. Fibonacci-Lucas Equations</u>

We define a Fibonacci-Lucas equation as an equation in one unknown in which one of the roots is equal to $(1+\sqrt{5})/2$. Let $x = \sqrt{5}$ and $\alpha = (1+x)/2$. Let j

and k be integers, and let

$$A = F_jF_k, \quad B = F_jL_k, \quad C = L_jF_k, \quad D = L_jL_k, \quad E = F_{k+j},$$
$$F = F_{k-j}, \quad G = L_{k+j}, \quad H = L_{k-j}, \quad i = (-1)^j.$$

(Notice that F is not a Fibonacci number because it does not have a subscript.) Then, the following results are known:

$$5A = G - Hi,$$
$$B = E - Fi,$$
$$C = E + Fi,$$
$$D = G + Hi.$$

Let n be an integer. From

$$a^n = \frac{L_n + F_nx}{2}$$

and

$$xa^n = \frac{5F_n + L_nx}{2},$$

the following results can be obtained:

$$F_ja^k = (B + Ax)/2 \tag{1}$$
$$F_jxa^k = (5A + Bx)/2 \tag{2}$$
$$L_ja^k = (D + Cx)/2 \tag{3}$$
$$L_jxa^k = (5C + Dx)/2 \tag{4}$$
$$F_ka^j = (C + Ax)/2 \tag{5}$$
$$L_ka^j = (D + Bx)/2 \tag{6}$$
$$F_kxa^j = (5A + Cx)/2 \tag{7}$$
$$L_kxa^j = (5B + Dx)/2 \tag{8}$$

Subtracting (5) from (1), (6) from (2), (7) from (3), (8) from (4) gives:

$$(B - C)/2 = -Fi$$
$$(5A - D)/2 = -Hi$$
$$(D - 5A)/2 = Hi$$
$$(5C - 5B)/2 = 5Fi$$

After (4) minus (8) has been divided by x, this gives the following set of four Fibonacci-Lucas equations;

(E_1) $\quad F_ja^k - F_ka^j + F_{k-j}(-1)^j = 0$

(E_2) $\quad F_jxa^k - L_ka^j + L_{k-j}(-1)^j = 0$

(E_3) $\quad L_ja^k - F_kxa^j - L_{k-j}(-1)^j = 0$

(E_4) $\quad L_ja^k = L_ka^j - F_{k-j}x(-1)^j = 0$

2. Fibonacci-Lucas Identities

As yet, there is no rigorous definition of a Fibonacci-Lucas identity. Until such a definition is formulated, there will not be a complete solution of this problem. However, the following tentative definition can serve as the basis of a partial solution: Define a Fibonacci-Lucas identity as a rational form that can be derived from a Fibonacci-Lucas equation.

Let the letters A through L be redefined as follows:

$$A = F_jF_{n+k},\quad B = F_jL_{n+k},\quad C = L_jF_{n+k},\quad D = L_jL_{n+k},$$

$$E = F_kF_{n+j},\quad F = F_kL_{n+j},\quad G = L_kF_{n+j},\quad H = L_kL_{n+j},$$

$$I = F_{k-j}F_n,\quad J = F_{k-j}L_n,\quad K = L_{k-j}F_n,\quad L = L_{k-j}L_n.$$

After equations (E_1) through (E_4) have been multiplied by a^n, they can be restated as follows:

$$(B + Ax)/2 - (F + Ex)/2 + (J + Ix)/2i = 0$$

$$(5A + Bx)/2 - (H + Gx)/2 + (L + Kx)/2i = 0$$

$$(D + Cx)/2 - (5E + Fx)/2 - (L + Kx)/2i = 0$$

$$(D + Cx)/2 - (H + Gx)/2 - (5I + Jx)/2i = 0$$

Let

$$P_1 = A - E + Ii,\quad Q_1 = B - F + Ji,$$

$$P_2 = B - G + Ki,\quad Q_2 = 5A - H + Li,$$

$$P_3 = C - F - Ki,\quad Q_3 = D - 5E - Li,$$

$$P_4 = C - G - Ji,\quad Q_4 = D - H - 5Ii.$$

Then $(Q_t + P_t x)/2 = 0$ for $t = 1, 2, 3, 4$. But Q_t is a rational number. If $P_t \neq 0$, then $P\,x$ is an irrational number. The sum of a rational number and an irrational number cannot be equal to zero. Therefore, $P_t = 0$ and $Q_t = 0$.

It is clear that $P_t = 0$ and $Q_t = 0$ are rational forms that can be derived from a Fibonacci-Lucas equation. In the following set of eight Fibonacci-Lucas identities,

$P_1 = 0$ is equivalent to Identity (I_1);
$Q_1 = 0$ is equivalent to Identity (I_2);
$P_2 = 0$ is equivalent to Identity (I_3);
$Q_2 = 0$ is equivalent to Identity (I_4);
$P_3 = 0$ is equivalent to Identity (I_6);
$Q_3 = 0$ is equivalent to Identity (I_5);
$P_4 = 0$ is equivalent to Identity (I_7);
$Q_4 = 0$ is equivalent to Identity (I_8):

(I_1) $\quad F_jF_{n+k} = F_kF_{n+j} - F_{k-j}F_n(-1)^j$

(I_2) $\quad F_jL_{n+k} = F_kL_{n+j} - F_{k-j}L_n(-1)^j$

(I_3) $\quad F_jL_{n+k} = L_kF_{n+j} - L_{k-j}F_n(-1)^j$

(I_4) $\quad 5F_jF_{n+k} = L_kL_{n+j} - L_{k-j}L_n(-1)^j$

(I_5) $\quad L_jL_{n+k} = 5F_kF_{n+j} + L_{k-j}L_n(-1)^j$

(I_6) $\quad L_jF_{n+k} = F_kL_{n+j} + L_{k-j}F_n(-1)^j$

(I_7) $\quad L_jF_{n+k} = L_kF_{n+j} + F_{k-j}L_n(-1)^j$

(I_8) $\quad L_jL_{n+k} = L_kL_{n+j} + 5F_{k-j}F_n(-1)^j$

It can be observed that Identities (I_1) through (I_8) are not divisible by 5. Also note that (I_1) and (I_2) can be derived from each other by the method described in this problem, (I_3) and (I_4) can be derived from each other, (I_6) and (I_5) can be derived from each other, and (I_7) and (I_8) can be derived from each other.

A Prime Example

H-408 *Proposed by Robert Shafer, Berkeley, CA*
(Vol. 25.1, February 1987)

(a) Define $u_0 = 3$, $u_1 = 0$, $u_2 = 2$, and $u_{n+1} = u_{n-1} + u_{n-2}$ for all integers n.

(b) In addition, let $w_0 = 3$, $w_1 = 0$, $w_2 = -2$, and $w_{n+1} = -w_{n-1} + w_{n-2}$ for all integers n.

Prove:

$$u_p \equiv w_p \equiv 0 \pmod{p} \quad \text{and} \quad u_{-p} \equiv -w_{-p} \equiv -1 \pmod{p},$$

where p is a prime number.

Solution by C. Georghiou, Patras, Greece

We need the following lemma.

Lemma: Let

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$$

be a monic polynomial with integer coefficients and denote its roots by r_1, r_2, ..., r_n. Then, for any prime p,

$$r_1^p + r_2^p + \cdots + r_n^p \equiv (r_1 + r_2 + \cdots + r_n)^p \pmod{p}.$$

Proof: First, it is easy to see that if p is prime, then the multinomial coefficient

$$\frac{p!}{k_1!k_2! \ldots k_n!}$$

is divisible by p when $0 \le k_i < p$, $i = 1, 2, \ldots, n$, and $k_1 + k_2 + \cdots + k_n = p$. Second, by the multinomial theorem, we have

$$\begin{aligned}(r_1 + r_2 + \cdots + r_n)^p &= \sum_{k_1+k_2+\cdots+k_n=p} \binom{p}{k_1, k_2, \ldots, k_n} r_1^{k_1} r_2^{k_2} \cdots r_n^{k_n} \\ &= r_1^p + r_2^p + \cdots + r_n^p + \sum_{\substack{0 \le k_1 \le k_2 \le \cdots \le k_n < p \\ k_1+k_2+\cdots+k_n=p}} \binom{p}{k_1, k_2, \ldots, k_n} \\ &\quad \times g_k(r_1, r_2, \ldots, r_n),\end{aligned}$$

where

$$g_k \equiv g_{k_1 k_2 \ldots k_n}$$

is a symmetric polynomial with integer coefficients. Then, by the Fundamental Theorem on Symmetric FUnctions (see, e.g., C. R. Hadlock: *Field Theory and Its Classical Problems*, MAA Publ., 1978, p. 42), each $g_k(r_1, r_2, \ldots, r_n)$ can be written as a polynomial h_k in the elementary symmetric functions with integer coefficients. Since $g_k(r_1, r_2, \ldots, r_n)$ takes integer values, the lemma is established.

(a) From the initial conditions we find that, for $-\infty < n < +\infty$,

$$u_n = r_1^n + r_2^n + r_3^n$$

where r_1, r_2, r_3 are the roots of the (irreducible) polynomial

$$f(x) = x^3 - x - 1.$$

Therefore, for any prime p,

$$u_p = r_1^p + r_2^p + r_3^p \equiv (r_1 + r_2 + r_3)^p = 0 \pmod{p};$$

$$u_{-p} = \left(\frac{1}{r_1}\right)^p + \left(\frac{1}{r_2}\right)^p + \left(\frac{1}{r_3}\right)^p \equiv \left(\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3}\right)^p = (-1)^p = -1 \pmod{p}.$$

(b) Same as above, with r_1, r_2, r_3 the roots of the (irreducible) polynomial

$$f(x) = x^3 + x - 1,$$

and we find that

$$w_p = r_1^p + r_2^p + r_3^p \equiv (r_1 + r_2 + r_3)^p = 0 \pmod{p};$$

$$w_{-p} = r_1^{-p} + r_2^{-p} + r_3^{-p} \equiv \left(\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3}\right)^p = 1^p = 1 \pmod{p}.$$

Also solved by P. Bruckman and the proposer.

*****

SUSTAINING MEMBERS

*Charter Members

A.F. Alameddine
*A.L. Alder
G.L. Alexanderson
S. Ando
R. Andre-Jeannin
*J. Arkin
M.K. Azarian
L. Bankoff
F. Bell
M. Berg
J.G. Bergart
G. Bergum
G. Berzsenyi
*M. Bicknell-Johnson
M.F. Bryn
P.F. Byrd
G.D. Chakerian
J.W. Creely
P.A. DeCaux
M.J. DeLeon
J. Desmond
H. Diehl
T.H. Engel
D.R. Farmer
P. Flanagan
F.F. Frey, Jr.
Emerson Frost
Anthony Gioia
R.M. Giuli
I.J. Good
*H.W. Gould
M. Guild
H. Harborth
H.E. Heatherly
A.P. Hollman
*A.F. Horadam
F.T. Howard
R.J. Howell
H. Ibstedt
R.P. Kelisky
C.H. Kimberling
J. Lahr
J. C. Lagarias
N. Levine
C.T. Long
Br. J. M. Mahon
*J. Maxwell
F.U. Mendizabal
L. Miller
M.G. Monzingo
S.D. Moore, Jr.
J.F. Morrison
K. Nagasaka
F.G. Ossiander
A. Prince
S. Rabinowitz
E.D. Robinson
S.E. Schloth
J. A. Schumaker
A.G. Shannon
D. Singmaster
J. Sjoberg
B. Sohmer
L. Somer
M.N.S. Swamy
*D. Thoro
J.C. Turner
R. Vogel
J.N. Vitale
M. Waddill
J.E. Walton
G. Weekly
R.E. Whitney
B.E. Williams
A.C. Yanoviak

INSTITUTIONAL MEMBERS

THE BAKER STORE EQUIPMENT COMPANY
Cleveland, Ohio

BOSTON COLLEGE
Chestnut Hill, Massachusetts

BUCKNELL UNIVERSITY
Lewisburg, Pennsylvania

CALIFORNIA STATE UNIVERSITY SACRAMENTO
Sacramento, California

THE COLLEGE OF IDAHO
Caldwell, Idaho

EMERGING TECHNOLOGIES GROUP, INC.
Dix Hills, New York

ETH-BIBLIOTHEK
Zurich, Switzerland

FERNUNIVERSITAET HAGEN
Hagen, West Germany

HOWELL ENGINEERING COMPANY
Bryn Mawr, California

NEW YORK PUBLIC LIBRARY GRAND CENTRAL STATION
New York, New York

NORTHWESTERN UNIVERSITY
Evanston, Illinois

PRINCETON UNIVERSITY
Princeton, New Jersey

SAN JOSE STATE UNIVERSITY
San Jose, California

SANTA CLARA UNIVERSITY
Santa Clara, California

KLEPKO, INC.
Sparks, Nevada

TECHNOLOGICAL EDUCATION INSTITUTE
Larissa, Greece

UNIVERSITY OF SALERNO
Salerno, Italy

UNIVERSITY OF CALIFORNIA, SANTA CRUZ
Santa Cruz, California

UNIVERSITY OF GEORGIA
Athens, Georgia

UNIVERSITY OF NEW ENGLAND
Armidale, N.S.W. Australia

WAKE FOREST UNIVERSITY
Winston-Salem, North Carolina

WASHINGTON STATE UNIVERSITY
Pullman, Washington

JOVE STATISTICAL TYPING SERVICE
2088 Orestes Way
Campbell, California 95008

BOOKS AVAILABLE THROUGH THE FIBONACCI ASSOCIATION

Introduction to Fibonacci Discovery by Brother Alfred Brousseau. Fibonacci Association (FA), 1965.

Fibonacci and Lucas Numbers by Verner E. Hoggatt, Jr. FA, 1972.

A Primer for the Fibonacci Numbers. Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1972.

Fibonacci's Problem Book. Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1974.

The Theory of Simply Periodic Numerical Functions by Edouard Lucas. Translated from the French by Sidney Kravitz. Edited by Douglas Lind. FA, 1969.

Linear Recursion and Fibonacci Sequences by Brother Alfred Brousseau. FA, 1971.

Fibonacci and Related Number Theoretic Tables. Edited by Brother Alfred Brousseau. FA, 1972.

Number Theory Tables. Edited by Brother Alfred Brousseau. FA, 1973.

Tables of Fibonacci Entry Points, Part One. Edited and annotated by Brother Alfred Brousseau. FA, 1965.

Tables of Fibonacci Entry Points, Part Two. Edited and annotated by Brother Alfred Brousseau. FA, 1965.

A Collection of Manuscripts Related to the Fibonacci Sequence—18th Anniversary Volume. Edited by Verner E. Hoggatt, Jr. and Marjorie Bicknell-Johnson. FA, 1980.

Fibonacci Numbers and Their Applications. Edited by A.N. Philippou, G.E. Bergum and A.F. Horadam.

Please write to the Fibonacci Association, Santa Clara University, Santa Clara, CA 95053, U.S.A., for current prices.