

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 MATHEMATICS, SOUTH DAKOTA STATE UNIVERSITY, BOX 2220, BROOKINGS, SD 57007-1297.

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 \$25 for Regular Membership, \$35 for Sustain Membership, and \$65 for Institutional Membership; foreign rates, which are based on international mailing rates, are somewhat higher than domestic rates; please write for details. **THE FIBO-NACCI 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.

1986 by © The Fibonacci Association All rights reserved, including rights to this journal issue as a whole and, except where otherwise noted, rights to each individual contribution.

The Fibonacci Quarterly

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

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

EDITOR

GERALD E. BERGUM, South Dakota State University, Brookings, SD 57007

ASSISTANT EDITORS

MAXEY BROOKE, Sweeny, TX 77480 PAUL F. BYRD, San Jose State University, San Jose, CA 95192 LEONARD CARLITZ, Duke University, Durham, NC 27706 HENRY W. GOULD, West Virginia University, Morgantown, WV 26506 RODNEY HANSEN, Whitworth College, Spokane, WA 99251 A.P. HILLMAN, University of New Mexico, Albuquerque, NM 87131 A.F. HORADAM, University of New England, Armidale, N.S.W. 2351, Australia DAVID A. KLARNER, University of Nebraska, Lincoln, NE 68588 RICHARD MOLLIN, University of Calgary, Calgary T2N 1N4, Alberta, Canada JOHN RABUNG, Randolph-Macon College, Ashland, VA 23005 DONALD W. ROBINSON, Brigham Young University, Provo, UT 84602 LAWRENCE SOMER, George Washington University, Washington, DC 20052 M.N.S. SWAMY, Concordia University, Montreal H3C 1M8, Quebec, Canada D.E. THORO, San Jose State University, San Jose, CA 95192 THERESA VAUGHAN, University of North Carolina, Greensboro, NC 27412 CHARLES R. WALL, Trident Technical College, Charleston, SC 29411 WILLIAM WEBB, Washington State University, Pullman, WA 99163

BOARD OF DIRECTORS OF THE FIBONACCI ASSOCIATION

CALVIN LONG (President) Washington State University, Pullman, WA 99163 G.L. ALEXANDERSON University of Santa Clara, Santa Clara, CA 95053 HUGH EDGAR (Vice-President)

San Jose State University, San Jose, CA 95192

MARJORIE JOHNSON (Secretary-Treasurer) Santa Clara Unified School District, Santa Clara, CA 95051

JEFF LAGARIAS

Bell Laboratories, Murray Hill, NJ 07974

ACKNOWLEDGEMENTS

In addition to the members of the Board of Directors and our Assistant Editors, the following mathematicians, engineers, and physicists have assisted *The Fibonacci Quarterly* by refereeing papers during the past year. Their special efforts are sincerely appredicted. We apologize for any names that have inadvertently been overlooked.

George E. Andrews Pennsylvania State U.

Krassimir Atanassov Bulgarian Acad. of Sci.

Robert Backstrom GYMEA, N.S.W.

Anthony E. Barkauskas U. of Wisconsin/LaCrosse

Bruce C. Berndt U. of Illinois

George Berzsenyi Lamar U.

David Bressoud Pennsylvania State U.

Richard Brualdi U. of Wisconsin

John Burke Gonzaga U.

Dario Castellanos Valencia, Venezuela

M. J. DeLeon Florida Atlantic U.

Naisingh Deo Washington State U.

Underwood Dudley DePauw Un.

Ernest Eckert Aalborg U. Center

E. A. Enneking Portland State U.

John Ewell Northern Illinois U. James Flanigan Pacific Palisades, CA

Helaman Ferguson

Brigham Young U.

Joseph Gallian U. of Minnesota/Duluth

Peter Hagis Temple U.

F. T. Howard Wake Forest U.

Steven Kahan Queens College

Dan Kalman Rancho Palos Verdes, CA

J. R. Kerr National U. of Singapore

Clark Kimberling U. of Evansville

Clayton Knoshaug Bemidji State U.

Gunter Kohler U. of Wurzburg

Joseph Konhauser Macalester College

Steve Ligh U. of Southwestern LA

Pin-Yen Lin Republic of China

W. L. McDaniel U. of Missouri/St. Louis

Richard Mollin U. of Calgary R. M. Najar

U. of Wisconsin/Whitewater

Norman Richert U. of Houston

Ernst Selmer U. of Bergen

J. O. Shallit U. of Chicago

Tony Shannon U. of Wales

Donald Snow Brigham Young U.

Lawrence Somer Washington, D.C.

Peter St. John Rutgers U.

M. V. Subbarao U. of Alberta

Richard Taylor Princeton U.

Dmitri Thoro San Jose State U.

Stephen Turner Babson College

Marcellus Waddill Wake Forest U.

Albert Wilansky Lehigh U.

Kenneth Yocom South Dakota State U.

Hisashi Yokota South Dakota State U.

ON SOME POLYGONAL NUMBERS WHICH ARE, AT THE SAME TIME, THE SUMS, DIFFERENCES, AND PRODUCTS OF TWO OTHER POLYGONAL NUMBERS

SHOICHI HIROSE Mita High School, Tokyo 108 Japan (Submitted December 1981)

We denote the n^{th} g-gonal number by

 $P_{n,q} = n\{(g - 2)n - (g - 4)\}/2.$

For g = 3, 5, 6, and 8, we denote $P_{n,g}$ by T_n , the triangular numbers, P'_n , the pentagonal numbers, H_n , the hexagonal numbers, and O_n , the octagonal numbers, respectively. We denote $P_{n,g}$ by P_n whenever there is no danger of confusion. Sierpiński [18] has proved that "there exist an infinite number of trian-

Sierpiński [18] has proved that "there exist an infinite number of triangular numbers which are, at the same time, the sums, differences and products of two other triangular numbers >1." Ando [1] proved that "there exist an infinite number of g-gonal numbers that can be expressed as the sum and difference of two other g-gonal numbers at the same time." It was also shown in [6] that there are an infinite number of g-gonal numbers that can be expressed as the product of two other g-gonal numbers.

The present paper will show that there are infinitely many g-gonal numbers (g = 5, 6, and 8) which are at the same time the sums, differences, and products of two other g-gonal numbers.

1. THE EQUATION $P_{u+w} + P_{v+w} = P_{u+v+w}$

If $P_x + P_y = P_z$, by putting u = z - y, v = z - x, and w = x + y - z, we have x = u + w, y = v + w, and z = u + v + w. However, a little algebra shows that $P_{u+w} + P_{v+w} = P_{u+v+w}$ implies 2(g - 2)uv = (g - 2)w(w - 1) + 2w. Hence

Theorem 1: Any solution x, y, z of the equation $P_x + P_y = P_z$ can be expressed as x = u + w, y = v + w, z = u + v + w, where

$$w \equiv 0 \pmod{g-2}$$

and

$$uv = \{(g - 2)w^2 - (g - 4)w\}/2(g - 2).$$

Using this theorem, which is a generalization of the work of Fauquembergue [7] and of Shah [15] on triangular numbers, we can obtain the solutions of the equation $P_x + P_y = P_z$ in an efficient way. For example, we have the following table for g = 5.

ω	$(3w^2 - w)/6$	и	υ	x	y	z
3	4	2 1	2 4	5 4	5 7	7 8
6	17	1	17	7	23	24
9	39	3 1	13 39	12 10	22 48	25 49

Table 1. $P'_x + P'_y = P'_z$ ($w \le 9, u \le v$)

If we put v + w = w' in $P_{1+v+w} = P_{1+w} + P_{v+w}$ and $P_{1+w'} = P_{1+v'+w'} - P_{v'+w'}$, then we obtain g-gonal numbers that can be expressed as the sum and difference of two other g-gonal numbers at the same time.

Corollary: If $w \equiv 0 \pmod{(g-2)^2}$ and $v = \{(g-2)w^2 - (g-4)w\}/2(g-2)$, then we have

 $P_{v+w+1} = P_{w+1} + P_{v+w} = P_a - P_b, \text{ where}$ $a = \{(g-2)(v+w)^2 - (g-4)(v+w)\}/2(g-2) + v + w + 1$ $b = \{(g-2)(v+w)^2 - (g-4)(v+w)\}/2(g-2) + v + w.$

and

Putting w = x - 1 for g = 3, we obtain a result of Sierpiński [18]; putting w = 9n for g = 5, w = 16n for g = 6, w = 25k for g = 7, and w = 36n for g = 8, we obtain the results of Hansen [9], O'Donnell [13], Hindin [10], and O'Donnell [14], respectively.

2. THE EQUATION $P_{at-d} + P_{bt-e} = P_{ct-f}$

In this section we study somewhat more general second-degree sequences than P_n , and obtain necessary and sufficient conditions for certain infinite families of representations to exist. We then specialize to polygonal numbers. To this end, let $F(\alpha, \beta; n) = n(\alpha n - \beta)$, where α , β are integers with $(\alpha, \beta) = 1$ and $\alpha > 0$.

Theorem 2: Let a, b, c, d, e, and f be integers with a, b, and c positive and (a, b, c) = 1. A necessary and sufficient condition for the identity in t,

 $F(\alpha, \beta; at - d) + F(\alpha, \beta; bt - e) = F(\alpha, \beta; ct - f),$

to hold is that there exist integers p, q, r, and s that satisfy equations (0) and (I), or (0) and (II):

$$\begin{cases} a = (p + q)(p - q), \ b = 2pq, \ c = p^2 + q^2, \\ (p, q) = 1, \ p > q > 0, \ p + q \equiv 1 \pmod{2}, \end{cases}$$
(0)

[May

ON SOME POLYGONAL NUMBERS

$$\begin{cases} d = (p+q)r, \ e = \frac{q}{\alpha}s, \ f = (p-q)r + \frac{q}{\alpha}s, \\ q \equiv 0 \pmod{\alpha}, \ 2\alpha pr - (p-q)s = -\beta, \end{cases}$$
(1)

$$\begin{cases} d = \frac{p-q}{\alpha}r, \ e = ps, \ f = \frac{p-q}{\alpha}r + qs, \\ p \equiv q \pmod{\alpha}, \ 2qr - \alpha(p+q)s = \beta. \end{cases}$$
(II)

Proof: In order for the desired identity in t,

$$(at - d)(\alpha at - \alpha d - \beta) + (bt - e)(\alpha bt - \alpha e - \beta) = (ct - f)(\alpha ct - \alpha f - \beta),$$

to hold, it is necessary and sufficient that the equations

$$a^{2} + b^{2} = c^{2},$$
(1)
(2ad + \beta)a + (2ae + \beta)b = (2af + \beta)c,
(2)

$$(\alpha d + \beta)d + (\alpha e + \beta)e = (\alpha f + \beta)f$$
(3)

be valid.

From (2),

$$cf = ad + be + \frac{\beta(a+b-c)}{2\alpha}, \qquad (4)$$

and from (1), (3), and (4), we obtain

$$(a^{2} + b^{2})\{(\alpha d + \beta)d + (\alpha e + \beta)e\}$$

= $c^{2}(\alpha f + \beta)f$
= $\alpha(cf)^{2} + \beta c(cf)$
= $\alpha \left\{ad + be + \frac{\beta(a + b - c)}{2\alpha}\right\}^{2} + \beta c \left\{ad + be + \frac{\beta(a + b - c)}{2\alpha}\right\}.$

Expanding and transforming the above, we have

$$\alpha(bd - ae)^2 - \beta(a - b)(bd - ae) - \frac{\beta^2 ab}{2\alpha} = 0.$$

Hence,

$$\begin{cases} (a) \quad bd - ae = \frac{\beta(a - b - c)}{2\alpha}, \text{ or} \\ (b) \quad bd - ae = \frac{\beta(a - b + c)}{2\alpha}. \end{cases}$$
(5)

Now, for positive integers a, b, and c with (a, b, c) = 1 and b even, the solutions of (1) are given by

(0)
$$\begin{cases} a = (p+q)(p-q), \ b = 2pq, \ c = p^2 + q^2, \ \text{where} \\ p \text{ and } q \text{ are positive integral parameters with} \\ (p, q) = 1, \ p > q > 0, \ \text{and} \ p + q \equiv 1 \pmod{2}. \end{cases}$$

Equations (6) and (7) below are necessary for (4) and (5) to hold.

$$\beta(a + b - c) = 2\beta q(p - q) \equiv 0 \pmod{2\alpha}, \tag{6}$$

1986]

ON SOME POLYGONAL NUMBERS

$$\begin{cases} (a) & \beta(a - b - c) = -2\beta q(p + q) \equiv 0 \pmod{2\alpha}, \text{ or} \\ (b) & \beta(a - b + c) = 2\beta p(p - q) \equiv 0 \pmod{2\alpha}. \end{cases}$$
(7)

Since $(\alpha, \beta) = 1$ and (p, q) = 1, (6) and (7) hold only if

$$\begin{cases} (a) & q \equiv 0 \pmod{\alpha}, \text{ or} \\ (b) & p \equiv q \pmod{\alpha}. \end{cases}$$
(8)

(I) If $q \equiv 0 \pmod{\alpha}$, (5)(a) becomes

$$2pqd - (p + q)(p - q)e = -\beta \frac{q}{\alpha}(p + q),$$

so that we have

$$2\alpha pr - (p - q)s = -\beta$$
, where $d = (p + q)r$ and $e = \frac{q}{\alpha}s$.

Substituting this into (4), we have $f = (p - q)r + \frac{q}{\alpha}s$.

(II) If $p \equiv q \pmod{\alpha}$, (5)(b) becomes

$$2pqd - (p + q)(p - q)e = \beta p \cdot \frac{p - q}{\alpha},$$

so that we have

 $2qr - \alpha(p+q)s = \beta$, where $d = \frac{p-q}{\alpha}r$ and e = ps.

Substituting this into (4), we have $f = \frac{p-q}{\alpha}r + qs$. Thus, we have the equivalence relation

$$(1) \cdot (2) \cdot (3) \Leftrightarrow (0) \cdot (4) \cdot (5) \Leftrightarrow (0) \cdot (1) \text{ or } (0) \cdot (11),$$

which proves Theorem 2.

Corollary: Solutions of $P_x + P_y = P_z$ are obtained by x = at - d, y = bt - e, z = ct - f. We use Theorem 2 by putting

$$P_{n,g} = \frac{1}{2}F(g - 2, g - 4; n) \text{ for } g \text{ odd, and}$$

$$P_{n,g} = F\left(\frac{g - 2}{2}, \frac{g - 4}{2}; n\right) \text{ for } g (\neq 4) \text{ even.}$$

In the case g = 4, we obtain a, b, and c from Theorem 2 (0) by putting d = e = f = 0.

Example: If g = 5, then $\alpha = 3$, $\beta = 1$. Since $q \equiv 0 \pmod{3}$, or $p \equiv q \pmod{3}$, and (p, q) = 1, p > q > 0, $p + q \equiv 1 \pmod{2}$, we have

 $q = 1; p = 4, 10, 16, \dots,$ $q = 2; p = 5, 11, 17, \dots,$ $q = 3; p = 4, 8, 10, 14, 16, \dots$

[May

When p = 4, q = 1, $2qr - \alpha(p+q)s = \beta$ becomes 2r - 15s = 1, where one solution is r = 8, s = 1. Using these values in (0) \cdot (II), we obtain

a = 15, b = 8, c = 17, d = 8, e = 4, f = 9,

and

$$P_{15t-8}' + P_{8t-4}' = P_{17t-9}'$$

Changing t into 8t - 3 and 17t - 7, we have

$$P'_{136t-60} = P'_{120t-53} + P'_{64t-28} = P'_{289t-128} - P'_{255t-113}.$$

Table 2.
$$P'_{at-d} + P'_{bt-e} = P'_{ct-f}, P'_{at} + P'_{y} = P'_{z}$$
 ($z \le 30$)

	p	q	r	S	а	Ъ	С	d	е	f	t	x	у	z
(11)	4	.1	8	1	15	8	17	8	4	9	1 2	7 22	4 12	8 25
(I)	4	3	0	1	7	24	25	0	1	1	1	7	23	24
(II) (I)	5 8	2 3	16 3	3 29	21 55	20 48	29 73	16 33	15 29	22 44	1	5 22	5 19	7 29

Table 3. Correspondence of the Solutions of $P_x + P_y = P_z$ in [1] Ex. 1

g	Parity	Case	р	q	r	S	t
k:even		(1)	$\frac{(k-2)^2}{2}t+1$	$\frac{(k-2)^2}{2}t$	0	$\frac{k-4}{2}$	1
k:odd	t:even	(I)	$\frac{(k-2)^2}{2}t+1$	$\frac{(k-2)^2}{2}t$	0	k-4	1
	t:odd	(11)	$(k-2)^2t+1$	1	$\frac{(k-2)^{3}t+(3k-8)}{2}$	1	1

3. THE EQUATIONS $P_z = P_x + P_y = P_u - P_v = P_r P_s$

For $g \neq 4$, if $(g - 2)P_n - (g - 4) = 2P_m$, we conjecture that $P_{P_n} = P_n P_m$ can be expressed as the sum and difference of two other g-gonal numbers. But we cannot prove this. However, we have

Theorem 3: There exist an infinite number of hexagonal numbers that can be expressed as the sum-difference-product of two other hexagonal numbers.

Proof: If we assume $H_n = H_3 H_m$, then we have $(4n - 1)^2 - 15(4m - 1)^2 = -14$. By putting N = 4n - 1, M = 4m - 1, we get $N^2 - 15M^2 = -14$. Its complete solution is given by the formulas

ON SOME POLYGONAL NUMBERS

(i) $N_i + \sqrt{15}M_i = \pm (1 + \sqrt{15})(4 + \sqrt{15})^i$ and

(ii)
$$N_i + \sqrt{15}M_i = \pm(-1 + \sqrt{15})(4 + \sqrt{15})^i$$
,

where $i = 0, \pm 1, \pm 2, \pm 3, \dots$ In (i), if $N_i + \sqrt{15}M_i > 0$, i > 0, and $i \equiv 2 \pmod{4}$, then $N_i \equiv M_i \equiv -1 \pmod{4}$ 4). N_i satisfies a recurrence relation

$$N_{i+2} = 8N_{i+1} - N_i,$$

which leads to $N_{i+4} = 62N_{i+2} - N_i$. Also, by repetition, $N_{i+8} = 3842N_{i+4} - N_i$. From $4n_{i+8} - 1 = 3842(4n_{i+4} - 1) - (4n_i - 1)$, it follows that $n_{i+8} = 3842n_{i+4} - n_i - 960$. Changing 4i - 2 into i, it becomes

 $n_{i+2} = 3842n_{i+1} - n_i - 960,$

with initial values $n_1 = 38$, $n_2 = 145058$. Similarly, we get

$$m_{i+2} = 3842m_{i+1} - m_i - 960,$$

with initial values $m_1 = 10$, $m_2 = 37454$. For all i, we have

$$\begin{split} H_{n_i} &= H_3 H_{m_i} = 15m_i(2m_i - 1) \\ &= (4m_i - 1)(8m - 3) - (m_i - 1)(2m_i - 3) \\ &= H_{4m_i - 1} - H_{m_i - 1}. \end{split}$$

For $i \equiv 1 \pmod{7}$, we have $n_i \equiv -1 \pmod{13}$. On taking $t = (n_i + 1)/13$ in

$$H_{13t-1} = H_{5t} + H_{12t-1},$$

we get

$$H_{n_i} = H_{(5n_i+5)/13} + H_{(12n_i-1)/13}$$

Thus, for $i \equiv 1 \pmod{7}$, H_{n_i} is expressed as the sum-difference-product of two other hexagonal numbers. If we put i = 1, then we have

$$H_{38} = H_{15} + H_{35} = H_{39} - H_9 = H_3 H_{10}$$
.

In a similar way, we obtain

Theorem 4: For g = 5 and 8, there exist an infinite number of g-gonal numbers that can be expressed as the sum-difference-product of two other g-gonal numbers.

Proof: If we put

$$\begin{array}{l} n_1 = 4, \ n_2 = 600912, \ n_{i+2} = 155234n_{i+1} - n_i - 25872 \\ m_1 = 1, \ m_2 = 128115, \ m_{i+2} = 155234m_{i+1} - m_i - 25872 \end{array} \} \quad i = 1, 2, 3, \ldots,$$

then, for $i \equiv 9 \pmod{14}$, we have $n_i \equiv 7 \pmod{29}$ and $m_i \equiv 1 \pmod{2}$, so that

[May

$$P'_{n_i} = P'_{(21n_i - 2)/29} + P'_{(20n_i + 5)/29} = P'_{(23m_i - 7)/2} - P'_{(21m_i - 7)/2}$$
$$= P'_4 P'_{m_i}.$$

Also, if we put

 $\begin{array}{c} n_1 = 304, \ n_2 = 1345421055984, \\ n_{i+2} = 4430499842n_{i+1} - n_i - 1476833280 \\ m_1 = 38, \ m_2 = 166878943590, \\ m_{i+2} = 4430499842m_{i+1} - m_i - 1476833280 \end{array} \right\} \quad i = 1, 2, 3, \ldots,$

then, for $i \equiv 0, 1 \pmod{7}$, we have $n \equiv 14 \pmod{29}$, so that

$$O_{n_i} = O_{(21n_i - 4)/29} + O_{(20n_i + 10)/29} = O_{9m_i - 4} - O_{4m_i - 4} = O_5 O_{m_i}.$$

Here, if we put i = 1, then we have

$$O_{304} = O_{220} + O_{210} = O_{338} - O_{148} = O_5 O_{38}.$$

ACKNOWLEDGMENT

I am grateful to Professor Koichi Yamamoto of Tokyo Woman's Christian University for his valuable comments on this manuscript.

REFERENCES

- 1. S. Ando. "A Note on the Polygonal Numbers." The Fibonacci Quarterly 19 (1981):180-183.
- 2. J. Arkin. "Certain Arithmetical Properties of $\frac{1}{2}k(ak \pm 1)$." The Fibonacci Quarterly 8 (1970):531-537.
- 3. L. Bernstein. "Explicit Solutions of Pyramidal Diophantine Equations." Canadian Mathematical Bulletin 15 (1972):177-184.
- 4. P. Bundschuh. "Zwei Resultate über Trigonalzahlen." Elemente der Mathematik 26 (1971):12-14.
- 5. L. E. Dickson. History of the Theory of Numbers. II (Chelsea, 1971), 1-39.
- 6. L. C. Eggan, P. C. Eggan, & J. L. Selfridge. "Polygonal Products of Polygonal Numbers and the Pell Equation." The Fibonacci Quarterly 20 (1982): 24-28.
- 7. E. Fauquembergue et al. "Solution 1155: Triangulaire somme de deux autres triangulaires." L'Intermédiaires des Mathématiciens 5 (1898):69-71. 8. A. S. Fraenkel. "Diophantine Equations Involving Generalized Triangular
- and Tetrahedral Numbers." Computers in Number Theory. New York: Academic Press, 1971, pp. 99-114.
- 9. R. T. Hansen. "Arithmetic of Pentagonal Numbers." The Fibonacci Quarterly 8 (1970):83-87. 10. H. J. Hindin. "A Theorem Concerning Heptagonal Numbers." The Fibonacci
- Quarterly 18 (1980):258-259.
- 11. R. V. Iyer. "Triangular Numbers and Pythagorean Numbers." Scripta Mathematica 22 (1956):286-288.
- 12. M. N. Khatri. "Triangular Numbers and Pythagorean Triangles." Scripta
- Mathematica 21 (1955):94. 13. W. J. O'Donnell. "Two Theorems Concerning Hexagonal Numbers." The Fibonacci Quarterly 17 (1979):77-79.

ON SOME POLYGONAL NUMBERS

- 14. W. J. O'Donnell. "A Theorem Concerning Octagonal Numbers." Journal of Recreational Mathematics (1979-1980):271-272.
- 15. S. M. Shah. "On Triangular Numbers Which Are Sums of Two Triangular Numbers." Vidya 9 (1966):161-163.
- W. Sierpiński. "Sur les nombres triangulaires qui sont sommes de deux nombres triangulaires." Elemente der Mathematik 17 (1962):63-65.
- 17. W. Sierpiński. Elementary Theory of Numbers. Warzawa: Wroclawska Drukarnia Naukowa, 1964, pp. 84-87.
- W. Sierpiński. "Un théorème sur les nombres triangulaires." Elemente der Mathematik 23 (1968):31-32.
- A. Więckowski. "O Rozwiązanych Problemach Sierpińskiego Związanych z Liczbami Trójkątnymi." Matematyka 32 (1979):288-294.
- 20. A. Więckowski. "On Some Systems of Diophantine Equations Including the Algebraic Sum of Triangular Numbers." *The Fibonacci Quarterly 18* (1980): 165-170.
- 21. A. Więckowski. "O Związkach Równania $2t_x = t_y z$ Innymi Równaniami Diofantycznymi." Matematyka 34 (1981):113-123.

LETTER TO THE EDITOR

19 December 1985

Dear Editor:

Before the publication of my article, "Generators of Unitary Amicable Numbers," in the May 1985 issue of The Fibonacci Quarterly, Dr. H. J. J. te Riele and I exchanged letters concerning unitary amicable numbers. He pointed out that his report, NW 2/78, published by the Matematisch Centrum in Amsterdam (with which he is affiliated), contains many of the results in my paper, albeit from a slightly different point of view. Both references to these letters and to report NW 2/78 were inadvertently omitted from my article.

The Centrum's address: Stichting Matematisch Centrum Kruislaan 413 1098 SJ Amsterdam Postbus 4079 1009 AB Amsterdam The Netherlands

Sincerely yours,

0. William McClung

R. M. STERNHEIMER

Brookhaven National Laboratory, Upton, NY 11973 (Submitted December 1983; revised August 1984)

I. INTRODUCTION

In connection with the discussion in my earlier paper [1] entitled: "A Corollary to Iterated Exponentiation," in which I have presented a new conjecture concerning Fermat's Last Theorem, it occurred to me that it is of interest to make a systematic study of the sets of three integers x, y, z which satisfy the condition

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

Such a triplet of integers (x, y, z) is commonly referred to as a "Pythagorean triplet," for which we shall also use the abbreviation *P*-triplet.

The actual motivation of the present work is to explore as thoroughly as possible the two cases, n = 1 and n = 2, for which the Diophantine equation of Fermat has solutions, namely,

$$x^{n} + y^{n} = z^{n} \qquad (n = 1, 2).$$
⁽²⁾

This interest is, in turn, derived from my earlier conjecture [1] that because n = 1 and n = 2 are the only two positive integers that are smaller than e, (2) holds only for n = 1 and n = 2 when x, y, and z are restricted to being positive integers. Most of the discussion in the present paper will be devoted to the case in which n = 2.

II. PYTHAGOREAN DECOMPOSITIONS

By using a computer program devised by M. Creutz, we were able to determine all Pythagoeran triplets for which $z \leq 300$. At this point, a distinction must must be made between *P*-triplets for which x, y, and z have no common divisor [the so-called "primitive solutions" of (1)] and *P*-triplets which are related to the primitive solutions by multiplication by a common integer factor k. So, if x_i, y_i, z_i are relatively prime and obey (1), it is obvious that the derived triplet (kx_i, ky_i, kz_i) will also satisfy (1).

The original computer program was therefore modified to print out only the primitive solutions, and was extended up to $z \leq 3000$. To anticipate one of my results, the number of primitive solutions in any interval of 100 in z is approximately constant and equal to ≈ 16 . Thus there are 80 primitive solutions (PS) between z = 1 and 500, and 477 PS in the entire interval $1 \leq z \leq 3000$. We

1986]

The manuscript was authored under Contract No. DE-AC02-76CH00016 with the U.S. Department of Energy. Accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

will make the convention to denote by x the larger of the two numbers in the left-hand side of (1), i.e., x > y.

In Table 1, I have tabulated all primitive solutions for $1 \le z \le 500$. The triplets are presented in the order x_i , y_i , z_i . When a value of z_i is underlined, this indicates that it is not prime. The nonunderlined z_i values are primes which we will call "Pythagorean primes" or *P*-primes. In this work, and also for the region $501 \le z \le 2000$, the tables of primes and prime factors given in the Handbook of Chemistry and Physics [2] were essential.

When the z_i of the primitive solution is not a prime, I have underlined it, and the underlined number is usually followed by a subscript 1 or 2, which has the following significance. Already in the work for $z \leq 300$ (with all triplets listed), I have noticed the following rule: If $z_{p,i}$ and $z_{p,j}$ belong to two different primitive solutions, the product

$$z_{p,k} = z_{p,i} z_{p,j} \tag{3}$$

belongs to two new primitive solutions, namely,

$$(x_{1,k}, y_{1,k}, z_{p,k})$$
 and $(x_{2,k}, y_{2,k}, z_{p,k})$. (4)

These two new P decompositions are relatively prime and are also prime with respect to the expected decomposition obtained by taking the product of $z_{p,j}$ with the decomposition $(x_{p,i}, y_{p,i}, z_{p,i})$ and that obtained by taking the product of $z_{p,i}$ with the decomposition $(x_{p,j}, y_{p,j}, z_{p,j})$. Thus, there are four linearly independent P decompositions for the number $z_{p,k}$ of (3). To take an example, according to Table 1, the number 65 has the decompositions (56, 33, 65) and (63, 16, 65), and, in addition, (52, 39, 65) and (60, 25, 65) obtained from (4, 3, 5) and (12, 5, 13), respectively.

This rule is satisfied in all decompositions of products $z_{p,i} z_{p,j}$ provided that the prime factors of $z_{p,i}$ and $z_{p,j}$ are different. On the other hand, if $z_{p,i}$ and $z_{p,j}$ are merely powers of the same prime p_i , then there will be just one additional linearly independent Pythagorean decomposition for

$$z_{p,k} = p_i^{\alpha_i} p_i^{\alpha_{i'}} = p_i^{\alpha_i + \alpha_{i'}}.$$
 (5)

As an example, the number $25 = 5^2$ has one additional *P* decomposition, namely, (24, 7, 25) besides that derived from (4, 3, 5), namely, (20, 15, 25). Similarly, the number $125 = 5^3$ has one new *P* decomposition, namely, (117, 44, 125) in addition to the two decompositions derived from the *P* decompositions for 5 and 25, namely, (100, 75, 125) and (120, 35, 125), respectively.

We may notice that the square $5^2 = 25$ has two P decompositions and the cube $5^3 = 125$ has three P decompositions. Thus, in general, a power $p_i^{\alpha_i}$ will have α_i Pythagorean decompositions, where p_i is a Pythagorean prime (such as 5, 13, 17, etc.). In Table 1, I have indicated the factors $z_{p,i}$ and $z_{p,j}$ which give rise to the new double primitive solution, when $z_{p,k}$ is a product of two different $z_{p,i}$ and $z_{p,j}$ which are relatively prime to each other. When a single power $p_i^{\alpha_i}$ is involved, this has also been noted, e.g., $13^2 = 169$ has the new P decomposition (120, 119, 169), in addition to the one expected from (12, 5, 13), namely, (156, 65, 169).

The total number of primitive solutions in the successive intervals of 100 in Table 1 are: 16 from 1 to 100, 16 from 101 to 200, 15 from 201 to 300, 16 from 301 to 400, and 17 from 401 to 500, giving a total of

$$\Sigma n_p = 16 + 16 + 15 + 16 + 17 = 80.$$
(6)

108

Table 1. Listing of the Pythagorean primitive decompositions for the integers in the range $1 \le N \le 500$. The values of z which are not prime numbers are underlined, and the subscripts 1 and 2 indicate the two new primitive solutions associated with such numbers. An exception occurs when the number N_i is a power of a single *P*-prime number, $p_i^{\alpha_i}$, in which case only one new primitive solution arises. For the numbers which are underlined (non-primes), the prime decomposition is indicated.

vi	x_i, y_i, z_i	vi	x_i, y_i, z_i	vi	x_i , y_i , z_i	vi	x_i, y_i, z_i
. 1	4,3,5	21	105,88,137	41	$247,96,\underline{265}_1 = 5 \times 53$	61	352,135, <u>377</u> ₂ = 13 × 29
2	12,5,13	22	$143, 24, \underline{145}_1 = 5 \times 29$	42	264,23, <u>265</u> ₂ = 5 × 53	62	340,189,389
3	15,8,17	23	$144, 17, \underline{145}_2 = 5 \times 29$	43	260,69,269	63	325,228,397
4	24,7, <u>25</u> = 5 ²	24	140,51,149	44	252,115,277	64	399,40,401
5	21,20,29	25	132,85,157	45	231,160,281	65	391,120,409
6	35,12,37	26	$120, 119, \underline{169} = 13^2$	46	240,161, <u>289</u> = 17 ²	66	420,29,421
7	40,9,41	27	165,52,173	47	285,68,293	67	304,297, <u>425</u> = 5 × 85
8	45,28,53	28	180,19,181	48	$224,207,305_1 = 5 \times 61$	68	416,87, <u>425</u> ₂ = 5 × 85
9	60,11,61	29	$153,104, \underline{185}_1 = 5 \times 37$	49	$273, 136, 305_2 = 5 \times 61$	69	408,145,433
10	$56, 33, \underline{65}_1 = 5 \times 13$	30	176,57, <u>185</u> ₂ = 5 × 37	50	312,25,313	70	$396,203,\underline{445}_1 = 5 \times 89$
11	$63, 16, \underline{65}_2 = 5 \times 13$	31	168,95,193	51	308,75,317	71	437,84, <u>445</u> 2 = 5 × 89
12	55,48,73	32	195,28,197	52	253,204, <u>325</u> 1 = 5 × 65	72	351,280,449
13	$77, 36, \underline{85}_1 = 5 \times 17$	33	$156, 133, 205_1 = 5 \times 41$	53	323,36, <u>325₂</u> = 5 × 65	73	425,168,457
14	$84, 13, \underline{85}_2 = 5 \times 17$	34	187,84, <u>205</u> ₂ = 5 × 41	54	288,175,337	74	380,261,461
15	80,39,89	35	$171, 140, \underline{221}_1 = 13 \times 17$	55	299,180,349	75	$360,319,\underline{481}_1 = 13 \times 37$
16	72,65,97	36	$220, 21, \underline{221}_2 = 13 \times 17$	56	272,225,353	76	$480,31,\underline{481}_2 = 13 \times 37$
17	99,20,101	37	221,60,229	57	357,76, <u>365</u> 1 = 5 × 73	77	476,93, <u>485</u> 1 = 5 × 97
18	91,60,109	38	208,105,233	58	364,27, <u>365</u> ₂ = 5 × 73	78	483,44, <u>485</u> 2 = 5 × 97
19	112,15,113	39	209,120,241	59	275,252,373	79	$468,155,\underline{493}_1 = 17 \times 29$
20	$117,44,\underline{125}=5^3$	40	255,32,257	60	$345, 152, \underline{377}_1 = 13 \times 29$	80	$475, 132, \underline{493}_2 = 17 \times 29$
1	1	1		1		1	

In Table 1 the numbers z_i that are not underlined are the primes for which a Pythagorean decomposition is possible. We will call them Pythagorean primes or *P* primes. The other primes (which are not *P*-decomposable) will be called non-Pythagorean primes or *NP* primes, e.g., 2, 3, 7, 11, 19, 23, 31, 43, and 47 are the *NP* primes below N = 50.

As mentioned above, all of the primitive solutions up to N = 3000 have been obtained with the computer program. (The total running time on the CDC-7600 Computer was less than 30 seconds.) However, I have limited the main analysis to the numbers $N \leq 2000$.

In the discussion below, I will derive a general formula for the number n_d of Pythagorean decompositions for an arbitrary integer.

In connection with the results of (3) and (4), it was noted and proved by M. Creutz [3] that when the triplets (x_1, y_1, z_1) and (x_2, y_2, z_2) are multiplied by each other, the additional primitive solutions mentioned in (4) have the following form:

$$X_{1} = x_{1}y_{2} + y_{1}x_{2}, \qquad Y_{1} = |x_{1}x_{2} - y_{1}y_{2}|; \qquad (7)$$

$$X_{2} = |x_{1}y_{2} - y_{1}x_{2}|, \qquad Y_{2} = x_{1}x_{2} + y_{1}y_{2}.$$
(8)

Here we have omitted the subscript p for simplicity of notation. To prove the validity of (7) and (8), we note that

$$X_{1}^{2} + Y_{1}^{2} = x_{1}^{2}y_{2}^{2} + y_{1}^{2}x_{2}^{2} + 2x_{1}x_{2}y_{1}y_{2} + x_{1}^{2}x_{2}^{2} + y_{1}^{2}y_{2}^{2} - 2x_{1}x_{2}y_{1}y_{2}$$

= $(x_{1}^{2} + y_{1}^{2})(x_{2}^{2} + y_{2}^{2}) = z_{1}^{2}z_{2}^{2} = (z_{1}z_{2})^{2} = Z^{2},$ (9)

thus verifying that $Z \equiv z_1 z_2$ has the *P* decomposition (X_1, Y_1, Z) . A similar equation is obtained by calculating $X_2^2 + Y_2^2 = z_1^2 z_2^2 = Z^2$, thus confirming the new *P* triplet (X_2, Y_2, Z) .

As an example, for Z = 65, we have $x_1 = 4$, $y_1 = 3$, $z_1 = 5$ and $x_2 = 12$, $y_2 = 5$, $z_2 = 13$, which gives $X_1 = 56$, $Y_1 = 33$, leading to the triplet (56, 33, 65) listed in Table 1. Furthermore, equations (8) give $X_2 = 16$, $Y_2 = 63$, which is equivalent to the second triplet, (63, 16, 65), also listed in Table 1.

It is also obvious from (7) and (8) that if $x_1 = x_2$, $y_1 = y_2$, i.e., $z_{p,k} = z_{p,i}^2$ in the notation of (3), then

$$X_1 = 2x_1y_1, \qquad Y_1 = |x_1^2 - y_1^2|,$$

which gives rise to only one new *P* triplet, since for the other solution, $X_2 = 0$, $Y_2 = x_1^2 + y_1^2 = z_{p,i}^2 = z_{p,k}^2$. For the case $x_1 = x_2 = 4$, $y_1 = y_2 = 3$, we have

$$X_1 = 2x_1y_1 = 24,$$
 $Y_1 = 4^2 - 3^2 = 7,$

giving the one new triplet, (24, 7, 25).

In Table 2, all the Pythagorean primes from N = 1 to N = 2000 are listed. Successive intervals of 100 are separated by semicolons.

Table 2. List of all Pythagorean primes for $1 \le N \le 2000$, i.e., primes which satisfy (1) where x and y are positive integers. Those primes which are underlined belong to a set of twin primes, i.e., primes p_i and p_j such that $|p_i - p_j| = 2$. For each set of twin primes p_i , p_j , one and only one is a P-prime. The primes in successive intervals of 100 are separated by a semicolon.

<u>5</u>, <u>13</u>, <u>17</u>, <u>29</u>, 37, <u>41</u>, 53, <u>61</u>, <u>73</u>, 89, 97; <u>101</u>, <u>109</u>, <u>113</u>, <u>137</u>, <u>149</u>, 157, 173, <u>181</u>, <u>193</u>, <u>197</u>; <u>229</u>, 233, <u>241</u>, 257, <u>269</u>, 277, <u>281</u>, 293; <u>313</u>, 317, 337, <u>349</u>, 353, 373, 389, 397; 401, 409, <u>421</u>, <u>433</u>, 449, 457, <u>461</u>;

509, <u>521</u>, 541, 557, <u>569</u>, 577, 593; <u>601</u>, 613, <u>617</u>, <u>641</u>, 653, <u>661</u>, 673, 677; 701, 709, 733, 757, 761, 769, 773, 797; <u>809</u>, <u>821</u>, <u>829</u>, 853, <u>857</u>, 877, <u>881</u>; 929, 937, 941, 953, 977, 997;

1009, 1013, <u>1021</u>, <u>1033</u>, <u>1049</u>, <u>1061</u>, 1069, <u>1093</u>, 1097; 1109, 1117, 1129, <u>1153</u>, 1181, 1193; 1201, 1213, 1217, <u>1229</u>, 1237, 1249, <u>1277</u>, <u>1289</u>, 1297; <u>1301</u>, <u>1321</u>, 1361, 1373, 1381; 1409, <u>1429</u>, 1433, <u>1453</u>, <u>1481</u>, <u>1489</u>, 1493;

1549, 1553, 1597; 1601, <u>1609</u>, 1613, <u>1621</u>, 1637, 1657, <u>1669</u>, 1693, <u>1697</u>; 1709, <u>1721</u>, 1733, 1741, 1753, 1777, <u>1789</u>; 1801, 1861, <u>1873</u>, <u>1877</u>, 1889; 1901, 1913, <u>1933</u>, <u>1949</u>, 1973, 1993, <u>1997</u>.

III. CONNECTIONS WITH THE TWIN PRIMES

Note that many of the Pythagorean primes in Table 2 are underlined. These are the primes which belong to a set of twin primes, i.e., primes p_i and p_j , which are separated by 2, i.e., such that $|p_i - p_j| = 2$. As an example, 17 is part of the twin prime set (17, 19); similarly, 41 is part of the twin prime set (41, 43). By a survey of all twin primes $N_i < 2000$, it was found that in all cases, for each set of twin primes, one of them is a *P*-prime (*P*-decomposable), while the other is a non-*P*-prime. This result can be shown to follow naturally from a theorem due to Fermat, according to which all primes $p_i \equiv 1$ (mod 4) are *P*-primes, while all primes $q_j \equiv 3 \pmod{4}$ are non-*P*-primes. Actually, what Fermat proved is that all primes $p \equiv 1 \pmod{4}$ can be written in the form $p_i = a^2 + b^2$, and this is, according to an elementary theorem due to Diophantos, the necessary and sufficient condition for $p_i^2 = x_i^2 + y_i^2$ to be satisfied [4]. Here, $x_i = a^2 - b^2$ and $y_i = 2ab$, and the result follows naturally from the following equation:

$$p_i^2 \equiv (a^2 + b^2)^2 = (a^2 - b^2)^2 + (2ab)^2 = a^4 + b^4 - 2a^2b^2 + 4a^2b^2$$
. (10)

Obviously, $p_i \equiv 1 \pmod{4}$ means that p_i can be written as 4n + 1. Then, if p_j is either 2 units larger or smaller than p_i , it is given by 4n' + 3, and $p_j \equiv 3 \pmod{4}$.

Of the 147 *P*-primes listed in Table 2, 60 are twin primes. The remaining 87 = 147 - 60 *P*-primes are "isolated" primes, i.e., they do not belong to a twin set. If we consider successive intervals of 500, we find a total of 44 *P*-primes between 1 and 500; 36 *P*-primes between 501 and 1000; 36 *P*-primes between 1001 and 1500; and 31 *P*-primes between 1501 and 2000. Incidentally, there is a total of 302 prime numbers between 1 and 2000, so that the overall fraction of *P*-primes is $147/302 = 0.487 \approx 49\%$, close to 50\%, as would be expected from Fermat's Theorem concerning $p_i \equiv 1 \pmod{4}$.

The approximate equality of the number n_P of P-primes and n_{NP} of non-Pprimes indicates that the Pythagorean primes have an intimate connection with the entire system of positive integers and, in addition, this connection indicates that we may expect that very approximately on the order of one-half of all integers are P-decomposable in at least one way ($n_d \ge 1$), while the other half is not Pythagorean-decomposable. These integers will be called P-numbers and non-P or NP-numbers, respectively. Numerical results for the fractions of P-numbers in three different intervals for $N \le 2000$ will be given below. Obviously, for an integer N_i to be P-decomposable in at least one way, it is necessary and sufficient that N_i can be written as

$$N_i = p_i J, \tag{11}$$

where p_i is an arbitrary *P*-prime and *J* is a positive integer.

IV. THE DECOMPOSITION FORMULA FOR n_d

The most general integer can be written as

$$N_{k} = p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} p_{3}^{\alpha_{3}} \cdots q_{1}^{\beta_{1}} q_{2}^{\beta_{2}} q_{3}^{\beta_{3}} \cdots$$
$$= \prod_{i=1}^{n_{a}} p_{i}^{\alpha_{i}} \prod_{j=1}^{n_{b}} q_{j}^{\beta_{j}} \equiv A_{k} B_{k}, \qquad (12)$$

1986]

where the p_i and *P*-primes are the α_i are the corresponding powers, and similarly, the q_j are the non-*P*-primes and the β_j are the corresponding powers. In the second row of (12), n_a denotes the number of different *P*-primes in N_k and n_b denotes the number of different non-*P*-primes in the prime decomposition of N_k ; finally, A_k and B_k represent the two products involving $p_i^{\alpha_i}$ and $q_j^{\beta_j}$, respectively.

Theorem: The total number of Pythagorean decompositions n_d corresponding to N_k of (12) is given by:

$$n_{d} = \sum_{i=1}^{n_{a}} \alpha_{i} + 2 \sum_{i < j}^{n_{a}} \alpha_{i} \alpha_{j} + 4 \sum_{i < j < k}^{n_{a}} \alpha_{i} \alpha_{j} \alpha_{k} + 8 \sum_{i < j < k < l}^{n_{a}} \alpha_{i} \alpha_{j} \alpha_{k} \alpha_{k} + \cdots$$
$$+ 2^{n_{a} - 1} \alpha_{1} \alpha_{2} \alpha_{3} \cdots \alpha_{n_{a}}.$$
(13)

Here, the first sum extends over all α_i , the second sum extends over all possible products of pairs of α_i , the third sum extends over all possible products $\alpha_i \alpha_j \alpha_k$, where three α_i 's are involved, etc. As an example, for the number 65 of Table 1, we have $65 = 5^1 \times 13^1$, so that $\alpha_1 = \alpha_2 = 1$, and (13) gives

$$n_d = 1 + 1 + 2(1)(1) = 4.$$
⁽¹⁴⁾

Similarly, for $N_k = 325 = 5^2 \times 13$, with $\alpha_1 = 2$, $\alpha_2 = 1$, we find

$$n_d = 2 + 1 + 2(2)(1) = 7.$$
⁽¹⁵⁾

In order to illustrate equation (13), we consider the number $1625 = 5^3 \times 13$. First, we will count the number of ways in which 1625 can be written without mixing up the 5's and the 13 in the decomposition. We use the notation $(p_{\alpha_i}^{\alpha_i})$ with parentheses to indicate the decomposition of $p_{\alpha_i}^{\alpha_i}$. Now, there are clearly $\alpha_1 = 3$ decompositions pertaining to the powers of 5 alone; they are (5^3) , (5^2) , and (5), where (5^3) stands for (117, 44, 125) (see Table 1), (5^2) stands for (24, 7, 25), and (5) \equiv (4, 3, 5). Thus, three decompositions of 1625 can be written as $(5^3) \times 13$, $(5^2) \times 65$, and $(5) \times 325$, where the multiplication applies to the three integers x_i , y_i , and z_i listed above for each case. In addition, there is the decomposition $(13) \times 125$, where $(13) \equiv (12, 5, 13)$. These four decompositions correspond to $\alpha_1 + \alpha_2 = 3 + 1 = 4$. Next, we consider the cases in which a product of a power of 5 times 13 appears inside the parentheses. These cases are $(5^3 \times 13)$, $(5^2 \times 13) \times 5$, and $(5 \times 13) \times 25$. According to the rule of equations (3) and (4) for $z_{p,i}$ and $z_{p,j}$ having different prime factors, there are two new primitive solutions for each such case, e.g.,

$$(325) \times 5 = (253, 204, 325) \times 5$$
 and $(323, 36, 325) \times 5$,

where $325 = 5^2 \times 13$ (see Table 1). There are $\alpha_1 \alpha_2 = (3)(1) = 3$ such cases, and they contribute $2\alpha_1 \alpha_2 = 6$ decompositions. Thus, the total

 $n_d = 4 + 6 = 10 = \alpha_1 + \alpha_2 + 2\alpha_1\alpha_2$

as given by (13). This illustration can be generalized to give the various terms of (13) and to provide the proof by induction. In each case, the factor 2, 4, 8 in the second, third, and fourth terms, respectively, of (13) corresponds to the doubling of the primitive solutions described above, where more

[May

than one prime is involved. For another example of (13), consider the number

$$N = (5^2)(13)(17) = 5525.$$
(16)

It has 22 decompositions of the type

$$5525^2 = x^2 + y^2, \tag{17}$$

since $\alpha_1 = 2$, $\alpha_2 = \alpha_3 = 1$, and, from (13),

$$n_d = (2 + 1 + 1) + 2(2 + 2 + 1) + 4(2) = 4 + 10 + 8 = 22.$$
 (18)

Using (13), we have obtained the number of decompositions n_d for three sets of 51 integers, namely those extending from N = 50 to N = 100, those extending from N = 950 to 1000, and those extending from N = 1950 to 2000. The results are presented in Table 3, which lists n_p , the number of Pythagorean numbers (for which $n_d \ge 1$), n_{NP} , the number of non-*P*-prime numbers (for which $n_d = 0$), the total $\Sigma n_d/n_p$ and, finally, the ratio of n_p to the total number 51. It is seen that while $n_p/\text{all } N = 0.49$ for the first set (50-100), for the other two sets, $n_p/\text{all } N$ is constant at a value of ≈ 0.61 . However, the total number of decompositions, Σn_d , increases from 34 (for N = 50-100) to 58 (for N = 1950-2000), and the average $\Sigma n_d/n_p$ also increases from 1.36 to 1.87 per Pythagorean number. It thus appears that the fraction of all numbers that are *P*-decomposable reaches a plateau value of -0.61 for large N, at least in the range of N = 1000-2000.

Table 3. For three ranges of N: 50-100, 950-1000, 1950-2000, I have tabulated the total number of Pythagorean numbers n_P , the total number of non-*P*-numbers n_{NP} , the total number of *P*-decompositions Σn_d , and the ratios $\Sigma n_d/n_P$ and $n_P/51$, where 51 is the total number of integers in each range.

<i>N</i> range	n _P	n _{NP}	Σn_d	$\Sigma n / n_P$	n _P /51
50-100	25	26	34	1.36	0.490
950-1000	31	20	53	1.71	0.608
1950-2000	31	20	58	1.87	0.608

We note that for very large numbers N_k (say $N_k \sim 10^{20}$) which have many factors $p_i^{\alpha_i}$ [see (12)], the use of (13) for n_d becomes cumbersome. For this reason, I have derived a simpler formula for n_d which can be readily evaluated for large N_k . This formula is presented in Appendix A of this paper [see equation (A25)].

As a final remark regarding (12), we note that we may define a *Pythagorean* congruence (*P*-congruence) as follows: Referring to (12), it is seen that the product A_k determines completely the type and the number n_d of *P*-decompositions as given by (13). Therefore, we can write

$$N_k \equiv A_k(P) , \tag{19}$$

and all numbers $N_{k_{\perp}}$ with the same product A_k (but different values of B_k) will

1986]

have the same *P*-decompositions, except for a different cofactor B_{k_i} . The congruence (19) holds under the operation of multiplication, i.e., if we have two integers N_k and N_k , with different values of A_k and B_k , then the product $N_k N_k$, can be written as follows,

$$N_k N_{k'} = (A_k A_{k'}) B_k B_{k'}, \qquad (20)$$

and the *P*-decompositions of $N_k N_{k'}$ will be uniquely determined by the product $A_k A_{k'}$, except for the cofactor $B_k B_{k'}$, which multiplies all decompositions (x_i, y_i, z_i) . Therefore, $N_k N_{k'}$ is *P*-congruent to $A_k A_{k'}$:

$$N_k N_k \, = A_k A_k \, (P) \,. \tag{21}$$

As examples of Pythagorean congruence, we mention three cases: $84 \equiv 1(P)$, since 84 is not *P*-decomposable, and $84 = 2^2 \times 3 \times 7$ is a product of non-*P*-primes only; similarly, $6630 \equiv 1105(P) = 5 \times 13 \times 17(P)$, where 5, 13, and 17 are *P*-primes. Finally, $929 \equiv 929(P)$, since 929 is a *P*-prime.

V. CONCLUDING COMMENTS

Of particular interest among the *P*-triplets, are those for which x = z - 1 (see Table 1 for examples). In this case, it is easily seen that y must be an odd integer, which can therefore be written as

$$y = 2\nu + 1, \tag{22}$$

where v is an arbitrary positive integer. We can now write:

$$x^{2} + y^{2} = (z - 1)^{2} + (2v + 1)^{2}$$

= $z^{2} - 2z + 1 + 4v^{2} + 4v + 1 = z^{2}.$ (23)

Upon subtracting z^2 from the last two expressions in (23), and dividing by 2, we obtain

$$-z + 1 + 2v^2 + 2v = 0, \tag{24}$$

which gives

$$z = 2\nu(\nu + 1) + 1,$$
 (25)

and, therefore, x = z - 1 = 2v(v + 1), and a suitable (x, y, z) triplet exists for any choice of v (>0), i.e., for any odd integer except y = 1. [In the latter case, x = 0 and equation (1) is trivially satisfied.] Thus, the ensemble of numbers y includes all odd numbers ≥ 3 , and hence, obviously, all prime numbers except y = 1 and y = 2. An example of such a triplet (from Table 1) is (40,9,41), in which case v = 4, z = (2)(4)(5) + 1 = 41, x = z - 1 = 40. Thus, the set of y's for x = z - 1 contains all prime numbers larger than e. We see again the privileged position of the numbers y = 1 and y = 2 (cf. [1]) that are not included among the y_i 's in the P-triplets, in complete similarity to the exponents n = 1 and n = 2 for which Fermat's Last Theorem is satisfied [i.e., equation (2)]. I should also note that I can amplify the statement made in [1] concerning the Diophantine equation

$$F(x, y) \equiv x^{y} - y^{x} = 0.$$
⁽²⁶⁾

114

In [1], I stated that the only nontrivial solution of (26) for integer xand y is x = 2, y = 4. However, if we do not demand that y be an integer, but if we consider a limiting process for x and y, then another nontrivial solution exists for $x \rightarrow 1$, i.e., the limit of y as x approaches 1 from above ($x = 1 + \varepsilon$, $\varepsilon \rightarrow 0$) is $y = \infty$. Specifically, I have calculated the values of y determined by (26) for x = 1.1, x = 1.01, and x = 1.001, with the following results:

$$y(x = 1.1) = 43.56, \qquad x^y = y^x = 63.53;$$
 (27)

$$y(x = 1.01) = 658.81, \quad x^y = y^x = 703.0;$$
 (28)

$$y(x = 1.001) = 9133.4, \quad x^y = y^x = 9217.05.$$
 (29)

It is clear from these results that the limit of y as x approaches 1 from above is infinity, i.e.,

$$\lim_{x \to 1} y = \infty.$$
(30)

Thus, equation (26) is essentially satisfied for both x = 1 and x = 2, analogous to Fermat's Last Theorem, which is satisfied only for n = 1 and n = 2.

Parenthetically, I may note that for x = 0, (26) *cannot* be satisfied for any positive y, since

$$F(0, y) = 0^{y} - y^{0} = -1$$
(31)

for all y. Analogous to this result, Fermat's Last Theorem, equation (2), also has no solution for n = 0, since the left-hand side $x^0 + y^0 = 2$, whereas the right-hand side $z^0 = 1$.

In summary, I have shown that the Pythagorean decompositions of z according to (1) provide a new classification of the number system into: (a) *P*-numbers $N_{P,i}$ [see (11)] that are *P*-decomposable in at least one way $(n_d \ge 1)$; (b) non-*P*-numbers $N_{NP,i}$ that cannot be decomposed according to (11) and (12), i.e., for which all of the α_i exponents of (12) are zero. The system of integers is approximately evenly divided between *P*-numbers and non-*P*-numbers in the range $50 < N_i < 100$, although for large N_i in the range of ~ 900-2000, the *P*-numbers predominate slightly, to the extent of 60% of all integers.

The set of *P*-primes p_i and products or powers of the p_i , i.e., $p_i p_j$ or $p_i^{\alpha_i}$ give rise to the primitive solutions (x_i, y_i, z_i) for which (1) is satisfied. As described by equations (3) and (4), and (7)-(9), for each pair of primitive solutions $(x_{p,i}, y_{p,i}, z_{p,i})$ and $(x_{p,j}, y_{p,j}, z_{p,j})$, the product $z_{p,k} \equiv z_{p,i} z_{p,j}$ contributes two new primitive solutions (provided the prime factors of $z_{p,i}$ and $z_{p,j}$ are different).

The total number of Pythagorean decompositions for a given P-number $N_{p,i}$ increases rapidly with the number n_a of p_i primes [see equation (12)] and with the powers α_i associated with each p_i . I have obtained a general expression for n_d in terms of the α_i and n_a [see equation (13)]. Furthermore, (13) has been proven by induction in the discussion which follows (15). An equivalent formula for (13) will be derived in Appendix A. The results given in Appendix A provide the means for a rapid evaluation of n_d when the integer N_k [see (12)] is large, so that there is a large number n_a of P-primes p_i in the prime decomposition of N_k .

Concerning the primitive solutions, I have noticed empirically from the decomposition tables that the density of primitive solutions, i.e., their frequency, is almost constant in going from $N \sim 0-100$ to N = 3000. Thus, generally, for each additional interval of 100 in N, we obtain sixteen additional

primitive solutions. As an example, the total number of primitive solutions included in Table 1 for $1 \le N \le 500$ is exactly $80 = 5 \times 16$ [equation (6)]. For $1 \le N \le 1000$, the total number of primitive solutions is 158, and for the entire sample with $1 \le N \le 3000$, the total number of primitive solutions is 477, almost equal to the expected number $16 \times 30 = 480$. At present, I have no explanation for the remarkable constancy of the density (frequency) of primitive solutions as a function of N.

As a final comment, it is not clear at present to what extent the results reported in this paper for the case n = 2 will help in the ultimate proof of Fermat's Last Theorem. Nevertheless, my previous suggestion about the values of n > e [1] and its amplification as presented in this paper [equations (26)-(30)] may offer a guideline to a complete proof. In any case, the interesting discovery of the doubling of the primitive solutions [equations (3), (4)] and the derivation of the resulting decomposition formula [equation (13)] will perhaps shed new light on the nature of our integer number systme. Additional results on the evaluation of (13) and on the case n = 1 in (2) will be given in Appendix A and Appendix B, respectively.

APPENDIX A

EVALUATION OF EQUATION (13)

In connection with (13) for the number n_d of Pythagorean decompositions of an arbitrary integer N_k as given by (12), it seems of interest to tabulate typical values of n_d for integers with relatively low values of the exponents α_i . Table 4 shows a systematic listing of the numbers of decompositions n_d for all cases for which $\Sigma \alpha_i \leq 6$. Obviously, the table can be subdivided into subtables pertaining to those cases for which any given number of *P*-primes p_i are involved. Thus, the top part of the table pertains to $\alpha_1 > 0$, $\alpha_2 = \alpha_3 = \alpha_4 = \alpha_5 = \alpha_6 = 0$ (i.e., the case $n_a = 1$). The next panel of the table pertains to cases for which two Pythagorean primes occur ($n_a = 2$) in the decomposition of N_k [equation (12)], and these will be denoted α_1 and α_2 , i.e., α_3 , ..., $\alpha_6 = 0$. In this panel I have arbitrarily assumed that $\alpha_1 \ge \alpha_2$ and, of course, all cases are subject to the limitation that $\alpha_1 + \alpha_2 \le 6$. The third, fourth, fifth, and sixth panels of the table are similarly constructed.

The next-to-the-last column of the table lists the values of n_d , while the last column lists the values of N_{\min} , the smallest integer N_k for which the particular decomposition as given in the first six columns exists. In addition, the prime decomposition of N_{\min} is listed after the value of N_{\min} . Obviously, in order to obtain the lowest N_k value consistent with the set $\{\alpha_i\}$, we must assume that all of the β_j in (12) are zero, i.e., $B_k = 1$. Furthermore, it is necessary to choose for the *P*-prime with the largest α_i the value 5, then the value 13 for the *P*-prime with the next largest α_i , and so forth.

Several results are apparent from a study of Table 4 and of (13):

1. Consider equation (13) and a particular α_i , say $\alpha_{i,0}$. Because the particular $\alpha_{i,0}$ appears linearly in all of the terms of (13), n_d depends linearly on $\alpha_{i,0}$, and in particular, for equally spaced values of α_i , e.g.,

$$\alpha_{i,0}, \alpha_{i,0} + 1, \text{ and } \alpha_{i,0}, \alpha_{i,0} - 1,$$

we find

$$n_d(\alpha_{i,0} + 1) - n_d(\alpha_{i,0}) = n_d(\alpha_{i,0}) - n_d(\alpha_{i,0} - 1),$$
(A1)

[May

Table 4. Listing of special cases of (13) for the number of Pythagorean decompositions as a function of the α_i 's and n_a . I have tabulated all cases for which $\sum_{i=1}^{6} \alpha_i \leq 6$. The seventh column of the table gives the values of $n_d\{\alpha_i\}$ as obtained from (13). The last column gives the smallest number N_{\min} for which the listed exponents $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$, and α_6 are realized. The prime decomposition of N_{\min} is listed for each N_{\min} . The blank spaces in the columns for α_i correspond to values of $\alpha_i = 0$.

α	α2	α3	α4	α ₅	α ₆	$n_d\{\alpha_i\}$	N_{\min}
1 2 3 4 5 6						1 2 3 4 5 6	5 25 125 625 3125 15,625
1 2 3 3 3 4 4 5	1 1 2 1 2 3 1 2 1					4 7 12 10 17 24 13 22 16	$65 = 5 \times 13$ $325 = 25 \times 13$ $4225 = 25 \times 169$ $1625 = 125 \times 13$ $21,125 = 125 \times 169$ $274,625 = 125 \times 2197$ $8125 = 625 \times 13$ $105,625 = 625 \times 169$ $40,625 = 3125 \times 13$
1 2 2 3 3 4	1 1 2 2 1 2 1 2	1 1 2 1 1 1				13 22 37 62 31 52 40	$1105 = 5 \times 13 \times 17$ $5525 = 25 \times 13 \times 17$ $71,825 = 25 \times 169 \times 17$ $1,221,025 = 25 \times 169 \times 289$ $27,625 = 125 \times 13 \times 17$ $359,125 = 125 \times 169 \times 17$ $138,125 = 625 \times 13 \times 17$
1 2 2 3	1 1 2 1	1 1 1 1	1 1 1 1			40 67 112 94	$32,045 = 5 \times 13 \times 17 \times 29$ $160,225 = 25 \times 13 \times 17 \times 29$ $2,082,925 = 25 \times 169 \times 17 \times 29$ $801,125 = 125 \times 13 \times 17 \times 29$
1 2	1 1	1 1	1 1	1 1		121 202	$1,185,665 = 5 \times 13 \times 17 \times 29 \times 37$ 5,928,325 = 25 \times 13 \times 17 \times 29 \times 37
1	1	1	1	1	1	364	$48,612,265 = 5 \times 13 \times 17 \times 29 \times 37 \times 41$

and, indeed, for any two values of α_i which differ by 1, the differences

$$n_d(\alpha_i) - n_d(\alpha_i - 1)$$

will be the same. Of course, in applying (Al), one must keep all of the other 1986]

 α_j values constant. Equation (Al) can be used to check the correctness of the entries of Table 4. As an example,

$$n_d(2, 2) - n_d(2, 1) = 12 - 7 = n_d(2, 1) - n_d(2, 0)$$

= 7 - 2 = 5. (A2)

Similarly,

$$n_d(3, 1, 1, 1) - n_d(2, 1, 1, 1) = 94 - 67$$

= $n_d(2, 1, 1, 1) - n_d(1, 1, 1, 1)$
= $67 - 40 = 27.$ (A3)

Here I have used the notation $n_d(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and $n_d(\alpha_1, \alpha_2)$ for the corresponding entries in Table 4.

2. Next, we consider the cases where all of the α_i are 1, e.g.,

$$n_d(1, 1, 1) = 13, n_d(1, 1, 1, 1, 1) = 121,$$
 etc.

For simplicity, $n_d(1, 1, ..., 1)$ with ξ l's will be simply denoted by $n_d[1_{\xi}]$. We note that the $n_d[1_{\xi}]$ satisfy the recursion relations

$$n_d[1_{F+1}] = 3n_d[1_E] + 1.$$
(A4)

As an example, $n_d[1_6] = 364$; $n_d[1_5] = 121$, and we have

$$n_d[1_6] = 3n_d[1_5] + 1 = 364 = (3 \times 121) + 1.$$
 (A5)

Equation (A4) together with the additional condition $n_d[1_1] = 1$ can be used to derive all of the $n_d[1_{\xi}]$ values of Table 4, namely, 4 {= $n_d[1_2]$ }, 13, 40, 121, and 364.

I also note that the difference $n_d[1_{\xi} + 1] - n_c[1_{\xi}]$ obeys the equation

$$n_d[1_{F+1}] - n_d[1_F] = 3^{\xi}.$$
 (A6)

As an example: $n_d[1_6] - n_d[1_5] = 364 - 121 = 243 = 3^5$. Therefore, I find:

$$n_d[1_{\xi}] = \sum_{\eta=0}^{\xi-1} 3^{\eta}.$$
 (A7)

3. A similar relation is obtained when we calculate differences between values of $n_d(2, 1, \ldots, 1)$. For simplicity, we write $n_d(2, 1, \ldots, 1)$ with γ 1's as $n_d[2, 1_{\gamma}]$. We note that

$$n_d(2, 1, 1) - n_d(2, 1) = 22 - 7 = 15,$$
 (A8)

$$n_d(2, 1, 1, 1) - n_d(2, 1, 1) = 67 - 22 = 45,$$
 (A9)

and also

$$n_d(2, 1) - n_d(2) = 7 - 2 = 5.$$
 (A10)

These results suggest the relation:

118

$$n_d[2, 1_{\gamma}] - n_d[2, 1_{\gamma-1}] = 5 \times 3^{\gamma-1}.$$
 (A11)

In fact, for $\gamma = 4$, we find

$$n_d[2, 1_4] - n_d[2, 1_3] = 5 \times 3^3 = 135 = 202 - 67.$$
 (A12)

Moreover, I have found that

$$n_d[2, 1_{\gamma}] - n_d[1, 1_{\gamma}] = 3^{\gamma},$$
(A13)

and, therefore, in view of (A7), and generalizing to $n_d[k, 1_{\gamma}]$,

$$n_d[k, 1_{\gamma}] = \sum_{\eta=0}^{\gamma} 3^{\eta} + (k-1)3^{\gamma}, \qquad (A14)$$

where k is an arbitrary positive integer.

Finally, as a generalization of (A7), I have found that the $n_d[k_{\xi}]$ for an arbitrary number ξ of integers k, e.g., $n_d[2, 2, 2] = n_d[2_3]$, are given by the following expression:

$$n_d[k_{\xi}] = k \sum_{\eta=0}^{\xi-1} (2k+1)^{\eta}.$$
(A15)

As an example: $n_d[2, 2, 2] = n_d[2_3]$ is given by

$$n_d[2_3] = 2\sum_{\eta=0}^{2} (5)^{\eta} = 2(1+5+5^2) = 62,$$
 (A16)

in agreement with the corresponding entry in Table 4. The generalized recursion relation which pertains to (Al5) is

$$n_{d}[k_{\xi+1}] = (2k+1)n_{d}[k_{\xi}] + k.$$
(A17)

A more general formula which is based on (Al4) and (Al5) gives

$$n_{d}[k, k_{\gamma}'] = k' \sum_{n=0}^{\gamma-1} (2k'+1)^{n} + k(2k'+1)^{\gamma}.$$
(A18)

(A18) gives n_d for γ powers α_i equal to k' and a single power α_j equal to k. In an attempt to simplify the evaluation of (A15) and (A18), we note that the sum in (A18) can be written as follows:

$$\sum_{n=0}^{\gamma-1} (2k'+1)^n = (2k'+1)^{\gamma-1} \left[1 + \frac{1}{2k'+1} + \frac{1}{(2k'+1)^2} + \dots + \frac{1}{(2k'+1)^{\gamma-1}} \right].$$
(A19)

The expression in square brackets is the major part of the infinite series

$$\frac{1}{1 - 1/(2k'+1)} = 1 + \frac{1}{2k'+1} + \frac{1}{(2k'+1)^2} + \cdots$$
 (A20)

The left-hand side of (A20) can be rewritten as follows:

$$\frac{1}{1 - 1/(2k'+1)} = \frac{2k'+1}{2k'}.$$
 (A21)

.

Therefore, the sum of (A19) is approximately given by

$$\sum_{\eta=0}^{\gamma-1} (2k'+1)^{\eta} \cong (2k'+1)^{\gamma}/2k'.$$
 (A22)

The part of the expression (A20) which is not included in the sum of (A19) can be shown to result in a negative contribution to $n_d[k, k'_j]$, which is given by

$$\Delta n_d = -k' \left[\frac{1}{1 - 1/(2k' + 1)} - 1 \right] = -k' \left(\frac{2k' + 1}{2k'} - 1 \right) = -\frac{1}{2}.$$
 (A23)

Upon inserting these results in (A18), we obtain:

$$n_{d}[k, k_{\gamma}'] = k'(2k'+1)^{\gamma}/2k' - \frac{1}{2} + k(2k'+1)^{\gamma}$$
$$= \frac{1}{2}(2k'+1)^{\gamma}(2k+1) - \frac{1}{2}.$$
 (A24)

Equation (A24) suggests a natural generalization to an arbitrary number of different k_i 's, since each k_i gives rise to a power $(2k_i + 1)^{\gamma_i}$ in the expression for n_d . We therefore obtain:

$$n_d(\{\alpha_i\}) = \frac{1}{2} \prod_{i=1}^{i_{\max}} (2k + 1)^{\gamma_i} - \frac{1}{2}.$$
 (A25)

This equation permits a rapid evaluation of $n_d(\{\alpha_i\})$ and is completely equivalent to the much more complicated equation (13) from which it is ultimately derived. I may note that we have the additional relation

$$\sum_{i=1}^{i_{\max}} \gamma_i = n_a, \qquad (A26)$$

where n_a is the number of different *P*-primes, as used in (12). As an example, I consider the following number,

$$N[2, 1_{13}] \equiv 5^2 \times 13 \times 17 \times 29 \times 37 \times 41 \times 53 \times 61 \times 73 \times 89 \times 97 \times 101 \times 109 \times 113$$

= 6.1605 \times 10^{23}, (A27)

which is close to Avogadro's number

 $N_{\rm Av} = 6.02204 \times 10^{23}$.

The notation $N[2, 1_{13}]$ obviously means that the lowest *P*-prime, $p_1 = 5$, was squared and the next 13 *P*-primes (power $k_i = 1$) were multiplied in the order of increasing p_i (see Table 2).

According to (A25), the number of Pythagorean decompositions of $N[2, 1_{13}]$ is

$$n_d(\{\alpha_i\}) = \frac{1}{2}(5)(3^{13}) - \frac{1}{2} = 3,985,807.$$
 (A28)

In general, we may try to calculate numbers N_k which in a given range have the largest number of *P*-decompositions n_d . This is usually accomplished by multiplying an appropriate number γ_1 of *P*-primes, all taken linearly $(k_1 = 1)$, i.e., to the first power. This conclusion was derived from the results of Table 4 which show, for example, that $N[1, 1, 1, 1] = N[1_5] = 1,185,665$ has

[May

 $n_d = 121$ *P*-decompositions, whereas the slightly larger $N[2, 2, 2] = N[2_3] = 1,221,025$ has only $n_d = 62$ *P*-decompositions.

In view of this result, I have made a study of the numbers $N[1_{\gamma}]$, where $N[1_{\gamma}]$ denotes the product of the first γ primes in Table 2. As an example,

$$\mathbb{N}[1_{14}] = 5 \times 13 \times 17 \times 29 \times 37 \times 41 \times 53 \times 61 \times 73 \times 89 \times 97 \times 101 \times 109 \times 113$$

= 1.2321 × 10²³ (A29)

has $n_d[1_{14}]$ Pythagorean decompositions, where [from (A25)]:

$$n_d[1_{14}] = \frac{1}{2}(3^{14} - 1) = 2,391,484.$$
 (A30)

For several values of γ up to $\gamma = 25$, Table 5 gives the values of $N[1_{\gamma}]$, the corresponding $n_d[1_{\gamma}]$ [cf. (A30)], and the exponent $\sigma(\gamma)$, which will be defined presently. I noticed that $n_d[1_{\gamma}]$ is, in all cases, of the order of

 ${N[1_{\gamma}]}^{1/3}$ to ${N[1_{\gamma}]}^{1/4}$,

so that an accurate inverse power, denoted by $1/\sigma,$ can be defined for each $\gamma,$ such that

$$n_d[1_{\gamma}] = \{N[1_{\gamma}]\}^{1/\sigma} .$$
(A31)

 $\sigma(\gamma)$ is a slowly varying function of γ that increases from $\sigma = 2.732$ for $\gamma = 3$ to $\sigma = 4.145$ for $\gamma = 25$. Below $\gamma = 3$, $\sigma(\gamma)$ increases to $\sigma = 3.011$ for $\gamma = 2$ and to ∞ for $\gamma = 1$, since the first *P*-prime, $p_1 = 5$, has a single *P*-decomposition, and $5^0 = 1$. The resulting curve of $\sigma(\gamma)$ vs γ is shown in Figure 1.





			· · · · · · · · · · · · · · · · · · ·
γ	σ(γ)	N[1 _Y]	n _d [1 _Y]
1	∞	5	1
2	3.011	65	4
3	2.732	1105	13
4	2,813	32,045	40
5	2.916	1,185,665	121
6	3.001	48,612,265	364
8	3.184	1.572×10^{11}	3,280
10	3.358	1.021×10^{15}	29,524
12	3.503	1.004×10^{19}	265,720
14	3.620	1.232×10^{23}	2,391,484
17	3.789	3.949×10^{29}	64,570,081
20	3.936	2.286×10^{36}	1.743×10^{9}
22	4.024	1.076×10^{41}	1.569×10^{10}
25	4.145	1.553×10^{48}	4.236×10^{11}

Table 5. Values of $\sigma(\gamma)$, $N[1_{\gamma}]$, and $n_d[1_{\gamma}]$ for selected values of γ in the range $1 \leq \gamma \leq 25$ [see (A31)].

APPENDIX B

THE CASE n = 1 OF EQUATION (2) AND COMMENTS ABOUT GOLDBACH'S CONJECTURE

It is obvious that the case n = 1 of (2), namely

x + y = z

always has a solution with integers x, y, and z. We will assume, for definiteness, that $x \ge y$. Then (B1) has z/2 linearly independent solutions when z is even, and (z - 1)/2 linearly independent solutions when z is odd. As an example for z = 11, we have the following (11 - 1)/2 = 5 linear decompositions of

z: 10 + 1, 9 + 2, 8 + 3, 7 + 4, and 6 + 5. There is a well-known conjecture, namely Goldbach's Conjecture, that any even z can be written as the sum of two prime numbers x and y. To my knowledge, this conjecture has not yet been proven in the general case, i.e., for an arbitrary even z. In this Appendix I have made a systematic study of the linear decompositions [equation (B1)] of all the even numbers $z \leq 100$ in terms of sums of two primes x and y.

It can be shown that the total number of linearly independent decompositions of an even z into a sum of two odd numbers according to (B1) is z/4 for z = 4v (divisible by 4) and (z + 2)/4 for z = 4v + 2 (not divisible by 4). According to the above-mentioned program, I am led to consider all of the linear decompositions of z as a sum x + y, where x and y are restricted to being

[May

(B1)

prime numbers. It will be seen shortly that in this endeavor, the concepts of a Pythagorean prime (P-prime) and a non-P-prime are of great importance.

In Table 6, I have listed all of the prime decompositions for even z in the range from 2 to 100. The number z is also denoted by N. In the prime decompositions, I have underlined the value of x_i or y_i in those cases where x_i or y_i is a Pythagorean prime. The most striking result of this table (aside from the large number of prime decompositions as z = N increases) is that there are two types of cases, depending upon whether N is or is not divisible by 4: (a) If N is divisible by 4, i.e., $N = 4\nu$ ($\nu = \text{positive integer}$), then each decomposition occurs for 4 = 2 + 2, and this decomposition will be discussed further below.) (b) If N is not divisible by 4, i.e., for $N = 4\nu + 2$, the prime decompositions involve either the sum of two P-primes (both x and y underlined) or the sum of two non-P-primes (neither x nor y underlined). As an example, $N = 16 = \underline{13} + 3 = 11 + 5$. By contrast, N = 10 = 7 + 3 = 5 + 5.

These two rules can be derived from the theorem of Fermat [see the discussion preceding equation (10)] that all primes $p_i \equiv 1 \pmod{4}$ are Pythagorean primes, while all primes $q_i \equiv 3 \pmod{4}$ are non-*P*-primes. Thus, we can write:

$$p_{i} = 4v_{i} + 1,$$
 (B2)

$$q_i = 4v_j - 1, \tag{B3}$$

from which it follows that

$$p_i + q_j = 4(v_i + v_j) = 4v$$
 (B4)

for numbers N = 4v that are divisible by 4. On the other hand,

$$p_{i} + p_{i'} = 4v_{i} + 4v_{i'} + 2 = 4(v_{i} + v_{i'}) + 2 = 4v + 2,$$
(B5)

$$q_{j} + q_{j'} = 4v_{j} + 4v_{j'} - 2 = 4(v_{j} + v_{j'} - 1) + 2 = 4\overline{v} + 2,$$
 (B6)

for even numbers that are not divisible by 4, i.e., N = 4v + 2 or $4\overline{v} + 2$.

It may be noted that, in constructing Table 6, I have underlined the number 1, i.e., I have treated 1 as a Pythagorean prime (with the decomposition $1^2 = 1^2 + 0^2$). This is essentially a matter of definition, but it is mandated by the result that the decompositions which involve 1 obey the rules (a) and (b) described above, provided that 1 is regarded as a *P*-prime for the present purposes. I will also note that to regard 1 as a *P*-prime in cases where a direct addition is involved makes good sense, whereas in the arguments leading to the decomposition formula. (13), if I had introduced an arbitrary factor 1^{α_0} in the expression for N_k of (12), this would have invalidated (13) for the total number of decompositions n_d , unless $\alpha_0 = 0$.

The decomposition 4 = 2 + 2 is an apparent exception to rules (a) and (b) given above. It does not seem to conform to the rule that one of the pair (x, y) be a *P*-prime, whereas the other of the pair (x, y) should be a non-*P*-prime. One way to obviate this contradiction is to specify that rules (a) and (b) apply only when the prime numbers x and y are odd. Another way of looking at the situation with respect to both 1 and 2 is that, as was emphasized repeatedly in [1] and in this paper, both 1 and 2 are special integers to which some of the rules governing other primes (≥ 3) do not apply; see especially the last two paragraphs of [1] and the discussion following (26) above. This privileged position of 1 and 2 has been correlated with the special properties of the powers n = 1 and n = 2 in the original Fermat equation, (2). Finally, a third

and more speculative way to describe the status of the integer 2 in connection with 4 = 2 + 2 is that just as y = 1 had to be defined as a *P*-prime in connection with Table 6, but as a non-*P*-prime in connection with (13), so x = 2 or y = 2 behaves half of the time as a *P*-prime (with the decomposition $2^2 = 2^2 + 0^2$) and half of the time as a non-*P*-prime which has no decomposition $2^2 = x^2 + y^2$, where x, y > 0. According to this interpretation, we could write 4 = 3 + 1 = 2 + 2 in Table 6.

Table 6. Linear decompositions of all even numbers $2 \le N \le 100$. For each N = z, all of the linear decompositions into a sum of prime numbers z = x + y are listed. Values of x and y which correspond to Pythagorean primes are underlined; the nonunderlined values correspond to non-*P*-primes. Note that when N is divisible by 4, i.e., N = 4v (v = positive integer), one of the pair (x, y) is a *P*-prime whereas the other number in the sum is a non-*P*-prime. When N is divisible by 2, but not by 4, i.e., for N = 4v + 2, either both x and y are *P*-primes, or both x and y are non-*P*-primes. A possible exception occurs for the decomposition of 4 = 2 + 2 (see discussion in text). We assume that $x \ge y$.

N	$x_i + y_i$
2	<u>1+1</u>
4	$3+\underline{1}, 2+2$
6	5+1, 3+3
8	7+ <u>1</u> , <u>5</u> +3
10	7 + 3, <u>5</u> + <u>5</u>
12	11+ <u>1</u> , 7+ <u>5</u>
14	13+1, 11+3, 7+7
16	13+3, $11+5$
18	17 + 1, $13 + 5$, $11 + 7$
20	19 + 1, 17 + 3, 13 + 7
22	$19+3, \underline{17}+\underline{5}, 11+11$
24	$23+\underline{1}, 19+\underline{5}, \underline{17}+7, \underline{13}+11$
26	23+3, $19+7$, $13+13$
28	23+5, 17+11
30	$\underline{29}+\underline{1}$, 23+7, 19+11, $\underline{17}+\underline{13}$
32	31 + 1, 29 + 3, 19 + 13
34	$31+3, \underline{29}+\underline{5}, 23+11, \underline{17}+\underline{17}$
36	31+5, 29+7, 23+13, 19+17
38	37 + 1, 31 + 7, 19 + 19
40	$\frac{37}{37}+3$, $\frac{29}{29}+11$, $23+\frac{17}{17}$
42	41+1, 37+5, 31+11, 29+13, 23+19
44	43+1, 41+3, 37+7, 31+13

124

Table 6. continued

N	$x_i + y_i$
46	$43+3, \underline{41}+5, \underline{29}+17, 23+23$
48	47 + 1, $43 + 5$, $41 + 7$, $37 + 11$, $31 + 17$, $29 + 19$
50	47 + 3, 43 + 7, <u>37</u> + <u>13</u> , 31 + 19
52	47 + 5, 41 + 11, 29 + 23
54	53+1, 47+7, 43+11, $41+13$, $37+17$, 31+23
56	53+3, $43+13$, $37+19$
58	53+5, 47+11, $41+17$, $29+29$
60	$59+\underline{1}$, $\underline{53}+7$, $47+\underline{13}$, $43+\underline{17}$, $\underline{41}+19$, $\underline{37}+23$, $31+\underline{29}$
62	$\underline{61} + \underline{1}$, 59 + 3, 43 + 19, 31 + 31
64	$\underline{61}$ + 3, 59 + $\underline{5}$, $\underline{53}$ + 11, 47 + $\underline{17}$, $\underline{41}$ + 23
66	$\underline{61} + \underline{5}$, $59 + 7$, $\underline{53} + \underline{13}$, $47 + 19$, $43 + 23$, $\underline{37} + \underline{29}$
68	67 + 1, 61 + 7, 37 + 31
70	67 + 3, $59 + 11$, $53 + 17$, $47 + 23$, $41 + 29$
72	71 + 1, $67 + 5$, $61 + 11$, $59 + 13$, $53 + 19$, $43 + 29$, $41 + 31$
74	$\underline{73} + \underline{1}$, $71 + 3$, $67 + 7$, $\underline{61} + \underline{13}$, $43 + 31$, $\underline{37} + \underline{37}$
76	$\underline{73}+3$, $71+\underline{5}$, $59+\underline{17}$, $\underline{53}+23$, $47+\underline{29}$
78	$\underline{73} + \underline{5}$, $71 + 7$, $67 + 11$, $\underline{61} + \underline{17}$, $59 + 19$, $47 + 31$, $\underline{41} + \underline{37}$
80	79 + 1, $73 + 7$, $67 + 13$, $61 + 19$, $43 + 37$
82	79+3, $71+11$, $59+23$, $53+29$, $41+41$
84	$83+\underline{1}$, $79+\underline{5}$, $\underline{73}+11$, $71+\underline{13}$, $67+\underline{17}$, $\underline{61}+23$, $\underline{53}+31$, $47+\underline{37}$, $43+\underline{41}$
86	83+3, $79+7$, $73+13$, $67+19$, $43+43$
88	83 + 5, $71 + 17$, $59 + 29$, $47 + 41$
90	$\underline{89} + \underline{1}$, $83 + 7$, $79 + 11$, $\underline{73} + \underline{17}$, $71 + 19$, $67 + 23$, $\underline{61} + \underline{29}$, $59 + 31$, $\underline{53} + \underline{37}$,
	47 + 43
92	$\underline{89}+3$, $79+\underline{13}$, $\underline{73}+19$, $\underline{61}+31$
94	89+5, 83+11, 71+23, $53+41$, 47+47
96	89+7, $83+13$, $79+17$, $73+23$, $67+29$, $59+37$, $53+43$
98	97+1, 79+19, 67+31, $61+37$
100	97+3, $89+11$, $83+17$, $71+29$, $59+41$, $53+47$

1986]

The number of prime linear decompositions n_{kd} , (B1), varies somewhat sporadically in going from a specific N, N_i , to its neighbors $N_i + 2$, $N_i + 4$, etc. However, there is a definite trend of an increasing number of prime decompositions n_{kd} with increasing N, as would be expected because of the increasing number of integers x, y which are smaller than N, as N increases. We note, in particular, that $n_{kd} = 10$ for N = 90 (see Table 6). Since the total number of all linear decompositions of N = 90 into a sum of two odd numbers is

$$(N + 2)/4 = 23,$$

we see that the percentage of the linear decompositions which consist of sums of primes is 10/23 = 43%.

In Table 7 I have tabulated the total number of linear prime decompositions (*l*d) n_{ld} for all even numbers N in the range $2 \le N \le 100$. For the cases where N is not divisible by 4, I have also listed the partial n_{ld} 's for *two* P-primes (x, y), denoted by $n_{ld,2}$, and for *no* P-prime, denoted by $n_{ld,0}$. Obviously, when N is not divisible by 4, we have

$$n_{\rm kd} = n_{\rm kd, 2} + n_{\rm kd, 0} \,. \tag{B7}$$

At the bottom of the table, I have listed the total number of $\&d's \Sigma n_{\&d}$ in the range $2 \le N \le 50$ and $52 \le N \le 100$, and for the complete range $2 \le N \le 100$. It is seen that $\Sigma n_{\&d}$ increases from 78 for the first half of the table ($N \le 50$) to $\Sigma n_{\&d}$ = 135 for the second half of the table ($52 \le N \le 100$), showing the increase of the average $\Sigma n_{\&d}/25$ from 3.12 to 5.40.

Similar tabulations have been made for $\Sigma n_{kd,0}$ and $\Sigma n_{kd,2}$. It is seen that the total number of kd's with $n_{P-\text{primes}} = 0$ slightly predominates over the total number of kd's with $n_{P-\text{primes}} = 2$. The ratio for the complete sample of 108 decompositions (up to N = 100) is 60/48 = 1.25.

I have also written down the prime decompositions for eight even integers in the range $102 \le N \le 200$. The results are:

$$n_{ld}(N = 116) = 6$$
, $n_{ld}(130) = 7$, $n_{ld}(150) = 13$, $n_{ld}(164) = 6$,
 $n_{ld}(180) = 15$, $n_{ld}(182) = 7$, $n_{ld}(184) = 8$, and $n_{ld}(200) = 9$.

Finally, I wish to point out an important correlation which is as simple as the one derived by Fermat concerning $p_i = 4v + 1$ for a *P*-prime and $q_j = 4v + 3$ for a non-*P*-prime. It is well known that any prime number p_i can be written in the form

$$p_{i} = 6v_{i} + 1 \text{ or } 6v_{i} - 1,$$
 (B8)

where v_i is an arbitrary positive integer. (This equation does not, however, apply to the prime numbers 2 and 3, and for $p_i = 1$ we must use $v_i = 0$.) The argument for (B8) goes as follows: Consider a specific v_i . Then $6v_i + 1$ is divisible by neither 2 nor 3, and therefore may be a prime; $6v_i + 2$ is divisible by 2; $6v_i + 3$ is divisible by 3; $6v_i + 4$ is again divisible by 2; $6v_i + 5 = 6(v_i + 1) - 1$ is divisible by neither 2 nor 3, and therefore is a candidate for being a prime number.

Table 7. For all even integers \mathbb{N} in the range from 2 to 100, n_{kd} is the number of linear decompositions of \mathbb{N} into a sum of primes $\mathbb{N} = x_i + y_i$, as given in Eq. (B1). For the integers \mathbb{N} which are divisible by 2 but not by 4, i.e., for values $\mathbb{N} = 4\mathbb{V} + 2$, I have also listed the number of linear decompositions into a sum of two *P*-primes, denoted by $n_{kd,2}$, and the number of linear decompositions into a sum of two non-*P*-primes, denoted by $n_{kd,0}$. Obviously, for values of $\mathbb{N} = 4\mathbb{V} + 2$, we have $n_{kd} =$ $n_{kd,2} + n_{kd,0}$. The sum of all n_{kd} and $n_{kd,\alpha}$ ($\alpha = 0$ or 2) is listed at the end of the table for the intervals $2 \leq \mathbb{N} \leq 50$ and $52 \leq \mathbb{N} \leq 100$, and also for the total range $2 \leq \mathbb{N} \leq 100$.

N	n _{ld}	n _{ld,2}	n _{ld,0}	N	n_{ld}	n _{ld, 2}	n _{ld,0}
2	1	1	0	52	3		
4	2		Ũ	54	6	3	3
6	2	1	1	56	3	_	
8	2			58	4	3	1
10	2	1	1	60	7		
12	2			62	4	1	3
14	3	1	2	64	5		
16	2			66	6	3	3
18	3	2	1	68	3		
20	3			70	5	2	3
22	3	1	2	72	7		
24	4			74	6	3	3
26	3	1	2	76	5		
28	2			78	7	3	4
30	4	2	2	80	5		
32	3			82	-5	2	3
34	4	2	2	84	9		
36	4			86	5	1	4
38	3	1	2	88	4		
40	3			90	10	4	6
42	5	3	2	92	4		
44	4			94	5	2	3
46	4	2	2	96	7		
48	6			98	4	2	2
50	4	1	3	100	6		
	Σπ	$v_{ld} (2 \leq N)$	78	19	22		
	Σκ	$l_{\rm ld}$ (52 $\leq N$	135	29	38		
	Σr	$a_{\rm ld} (2 \leq N)$	213	48	60		

Now the correlation which can be derived from Fermat's p_i = 4v + 1 theorem is that all Pythagorean primes are of the form

 $p_i = 6v_i + 1$, if v_i is even, (B9)

 $p_i = 6v_i - 1, \quad \text{if } v_i \text{ is odd.} \tag{B10}$

1986]

and

Thus, 37 = (6)(6) + 1 is an example of (B9) (even $v_i = 6$); 89 = (6)(15) - 1 is an example of (B10).

In view of (B9) and (B10), the non-P-primes (except 2 and 3) are of the form

 $q_j = 6v_j - 1$, if v_j is even, $q_i = 6v_j + 1$, if v_j is odd.

It should perhaps be noted that not all v_i or v_j give rise to P- or non-Pprimes. The first few v_i values which do not give rise to a prime number are: $v_i = 20, 24, 31, 34, 36, 41$, etc. The preceding equations signify only that *if* a given number is a P-prime p_i or a non-P-prime q_j , then it can be expressed by (B9) or (B10), and (B11) or (B12), respectively.

Referring to the results of Table 7, I wish to note that the total number n_{kd} of prime decompositions has maxima when N is divisible by 6 (N = 6v), at least starting with N = 24. This trend is particularly noticeable when N lies in the range from 72 to 96. Thus, $n_{kd}(90) = 10$ is considerably larger than $n_{kd}(88) = 4$ and $n_{kd}(92) = 4$. Similarly, $n_{kd}(84) = 9$ characterizes a peak in the n_{kd} values as a function of N since, for the neighboring N = 82 and N = 86, we find $n_{kd}(82) = 5$ and $n_{kd}(86) = 5$. This property may be caused by the fact that, when N = 6v, we have two primes such that one of them is of the form $6v_1 + 1$ and the other prime can be written as $6v_2 - 1$, and in taking the sum, we obtain N = $6(v_1 + v_2) = 6v$. It is also interesting that in several cases, particularly for N = 6v, both members of each of two twin prime sets are involved, e.g.,

$$78 = 73 + 5 = 71 + 7 = 61 + 17 = 59 + 19$$
.

Note also that

and

 $90 = \underline{73} + \underline{17} = 71 + 19 = \underline{61} + \underline{29} = 59 + 31.$

84 = 73 + 11 = 71 + 13 = 41 + 43

ACKNOWLEDGMENTS

I would like to thank Dr. Michael Creutz for several helpful discussions, for a critical reading of the manuscript, and for devising the computer program designed to list the primitive solutions of equation (1). I am also indebted to Dr. Sidney Heller for a critical reading of the manuscript.

REFERENCES

- 1. R. M. Sternheimer. "A Corollary of Iterated Exponentiation." The Fibonacci Quarterly 23 (1985):146-148.
- 2. Handbook of Chemistry and Physics. 44th ed., pp. 244-251. Cleveland, Ohio: Chemical Rubber Publishing Co., 1963.
- 3. M. Creutz. Private communication.
- See also W. J. Le Veque. Elementary Theory of Numbers, p. 108. Reading, Mass: Addison-Wesley Publishing Co., 1962; and A. F. Horadam. "Fibonacci Number Triples." Amer. Math. Monthly 68 (1961):751-753.

128

[May

(B11)

ON THE MINIMUM OF A TERNARY CUBIC FORM

WERNER GEORG NOWAK Institut für Mathematik der Universität für Bodenkultur Gregor Mendel-Strasse 33, A-1180 Vienna, Austria (Submitted May 1984)

Let

$$f_a = f_a(x, y, z) = x^3 + y^3 + z^3 + 3axyz,$$

a an arbitrary real constant, and denote, for a lattice Λ in \mathbb{R}^3 , by $\mu_a(\Lambda)$ the infimum of $|f_a|$ if (x, y, z) runs through all lattice points of Λ except (0, 0, 0). It is the objective of the present paper to estimate, from the above, the supremum M_a of $\mu_a(\Lambda)$, taken over all lattices Λ with lattice constant 1. (Since any homogeneous ternary cubic polynomial can be transformed into the shape (1) by a suitable linear transformation, there is no loss of generality in starting from this canonical form.)

Classical work on this topic has been done by Mordell [6] (on the basis of his method of reducing the problem to a two-dimensional one) and by Davenport [1], [2]. Significant progress has been achieved in the special case a = 0. For arbitrary a however, the results obtained were not very sharp, as was noted by Golser [3], who improved upon Mordell's estimate for the general case, by a refined variant of his method. Later on, in [4], he observed that, for a certain range of the constant a, the bound can be improved further by the simple idea of inscribing a sphere into the star body $|f_a| \leq 1$.

The purpose of this short note is to establish a result that improves upon all known estimates for certain intervals of a (at least for $0.9 \le a \le 2.9$ and for $-6 \le a \le -1.2$; see the tables at the end) by the elementary procedure of inscribing an ellipsoid of the shape

$$E_t(r): x^2 + y^2 + z^2 + 2t(xy + xz + yz) \le r^2,$$
(2)

where t is a parameter with $-\frac{1}{2} < t < 1$, into the body $K_a: |f_a| \leq 1$. Our result reads

Theorem: For arbitrary real a and a parameter t with $-\frac{1}{2} \le t \le 1$, $t \ne 0$, we have

where

 M_{a}

$$\leq \sqrt{2}(1 - t)\sqrt{1 + 2t} m_a(t),$$

$$\begin{split} m_a(t) &:= \max\{ \left| 1 + a \right| (1 + 2t)^{-3/2} 3^{-1/2}, \phi_1(t), \phi_2(t) \}, \\ \phi_j(t) &:= (2 + 2t + 4tc_j + c_j^2)^{-3/2} \left| 2 + 3ac_j + c_j^3 \right| \quad (j = 1, 2), \\ c_j &:= (2t)^{-1} (b - 2t + (-1)^j (b^2 + 4t + 4bt^2)^{1/2}), b = a - 1. \end{split}$$

Proof: We first briefly recall some well-known facts from the *Geometry of Numbers*. The critical determinant $\Delta(K_{\alpha})$ of our body K_{α} is defined as the infimum of all lattice constants $d(\Lambda)$ of lattices Λ in \mathbb{R}^3 which have no point in the interior of K_{α} except the origin. For any such lattice Λ , we put

$$\Lambda_1 = d(\Lambda)^{-1/3}\Lambda,$$

1986]

129

(1)

[such that $d(\Lambda_1) = 1$] and $\Lambda' = \Lambda - \{(0, 0, 0)\}, \Lambda'_1 = \Lambda_1 - \{(0, 0, 0)\}$. Since f_a is homogeneous of degree 3, it follows that

$$\Delta(K_a) = \inf\{d(\Lambda) : \inf_{\Lambda'} | f_a| \ge 1\}$$

=
$$\inf_{d(\Lambda_1)=1} \inf_{\Lambda'_1} \{d \in \mathbb{R} : \inf_{\Lambda'_1} | f_a| \ge 1/d\}$$

=
$$(\sup_{d(\Lambda_1)=1} \inf_{\Lambda'_1} | f_a|)^{-1},$$

hence $M_a = \Delta(K_a)^{-1}$. We further note that the ellipsoid $E_t(r)$ can be transformed into the unit sphere by the linear transformation

$$x' = (x + ty + tz)r^{-1}, y' = (\sqrt{1 - t^2} y + \sqrt{t - t^2} z)r^{-1},$$
$$z' = \frac{\sqrt{(1 - t)(1 + 2t)}}{r\sqrt{1 + t}}z$$

which is of determinant $(1 - t)\sqrt{1 + 2t} r^{-3}$. Since the critical determinant of the unit sphere equals $1/\sqrt{2}$ (see Ollerenshaw [7] or [5], p. 259), we conclude that

$$\Delta(E_t(r)) = r^3 ((1 - t)\sqrt{1} + 2t\sqrt{2})^{-1}.$$
(3)

If we choose r maximal such that $E_t(r) \subset K_a$, then obviously $\Delta(K_a) \ge \Delta(E_t(r))$, hence

$$M_a = \Delta(K_a)^{-1} \le r^{-3}\sqrt{2}(1 - t)\sqrt{1 + 2t}$$

and, by homogeneity,

$$\max_{E_t(r)} |f_a| = 1 \iff \max_{E_t(1)} |f_a| = r^{-3}.$$

Therefore, it suffices to establish the following

Lemma: For arbitrary t with $-\frac{1}{2} \le t \le 1$, $t \ne 0$, the absolute maximum of $|f_a|$ on $E_t(1)$ equals $m_a(t)$.

Proof: Since the absolute maximum of $|f_a|$ can be found among the relative extrema of f_a on the boundary of $E_t(1)$, we determine the latter by Lagrange's rule. We obtain

$$3x^{2} + 3ayz + k(2x + 2t(y + z)) = 0, \qquad (4)$$

 $3y^{2} + 3axz + k(2y + 2t(x + z)) = 0,$ (5)

$$3z^{2} + 3axy + k(2z + 2t(x + y)) = 0,$$
(6)

$$x^{2} + y^{2} + z^{2} + 2t(xy + xz + yz) = 1.$$
⁽⁷⁾

This system does not have any solution with $x \neq y \neq z \neq x$, for otherwise we could infer from (4) and (5) (subtracting and dividing by x - y) that

$$3(x + y) - 3az + 2k - 2kt = 0$$

and similarly, from (5) and (6), that

[May
$$3(y + z) - 3ax + 2k - 2kt = 0.$$

Again subtracting, we would get the contradiction x = z (at least for $a \neq -1$; the case a = -1 then can be settled by an obvious continuity argument).

Furthermore, it is impossible that a solution of our system satisfies x = y = 0, because this would imply that ktz = 0 and z(3 + 2k) = 0, hence z = 0, which contradicts (7). There remain two possibilities (apart from cyclic permutations).

Case 1: $x = y = z \neq 0$. By (7), we have

$$x = y = z = \pm (1 + 2t)^{-1/2} 3^{-1/2}$$

and for these values of x, y, and z,

$$|f_a| = |1 + a|(1 + 2t)^{-3/2}3^{-1/2}.$$

Case 2: $0 \neq x = y \neq z$. Eliminating k from (4) and (6), we get

$$(2t - a - at)x^3 + (1 + at)x^2z + (a - 1 - t)xz^2 - tz^3 = 0.$$

This can be divided by x - z and yields

$$tz^{2} + (1 + 2t - a)xz + (2t - a - at)x^{2} = 0,$$

hence $z/x = c_j$ (j = 1, 2, as defined in our theorem). From (7) we deduce that

$$x = y = \pm (2 + 2t + 4tc_i + c_i^2)^{-1/2}, \quad z = c_i x,$$

and for these values of x, y, and z,

$$|f_a| = \phi_j(t) \quad (j = 1, 2).$$
 (9)

Combining (8) and (9), we complete the proof of the lemma and thereby that of our theorem.

Concluding Remarks: Letting $t \to 0$ in our result, we just obtain Golser's theorem 1 in [4]. However, this choice of t turns out not to be the optimal one. In principle, one could look for an "advantageous" choice of the parameter t (for a given value of the constant a) by computer calculations, but it can be justified by straightforward monotonicity considerations that it is optimal to choose t such that $\max\{\phi_1(t), \phi_2(t)\}$ equals the right-hand side of (8).

We conclude the paper with tables indicating the new upper bounds for M_a (for certain values of a) as well as the corresponding "favorable" values of t and the previously-known best results due to Golser [3], [4].

a	0.9	1	2	2.9
t	0.02799	0.040786	0.07973	0.07301
$M_a \leq$	1.428	1.4483	1.9442	2.5758
Golser: $M_a \leq$	1.454	1.5018	2.0597	2.5775

1986]

131

(8)

ON THE MINIMUM OF A TERNARY CUBIC FORM

а	-6	-5	-4	-3	-2	-1.2
t	-0.064204	-0.07892	-0.101987	-0.14273	-0.23042	-0.41324
$M_a \leq$	4.9848	4.1843	3.391	2.6116	1.8634	1.33
Golser: $M_a \leq$	5.03779	4.31314	3.58475	2.85169	2.1106	1.54372

REFERENCES

- 1. H. Davenport. "On the Minimum of a Ternary Cubic Form." J. London Math. Soc. 19 (1944):13-18.
- H. Davenport. "On the Minimum of $x^3 + y^3 + z^3$." J. London Math. Soc. 21 2. (1946):82-86.
- 3. G. Golser. "Schranken für Gitterkonstanten einiger Sternkörper." Ph.D. Dissertation, University of Vienna, 1973.
 G. Golser. "Über Gitterkonstanten spezieller Sternkörper." Sitz.-Ber. Os-
- terr. Akad. Wiss., Abt. II, math.-naturwiss. Kl. 184 (1975):227-238.
- 5. C. G. Lekkerkerker. Geometry of Numbers. Amsterdam-London: North Holland Publishing Co., 1969.
- 6. L. J. Mordell. "On the Minimum of a Ternary Cubic Form." J. London Math. Soc. 19 (1944):6-12.
- 7. K. Ollerenshaw. "The Critical Lattices of a Sphere." J. London Math. Soc. 23 (1948):297-299.

ON THE COEFFICIENTS OF A RECURSION RELATION FOR THE FIBONACCI PARTITION FUNCTION

TAD WHITE (Student) California Institute of Technology, Pasadena, CA 91126 (Submitted July 1984)

Let $F = \{1, 2, 3, 5, ...\}$ be the set of Fibonacci numbers, where $F_2 = 1$, $F_3 = 2$, and thereafter $F_n = F_{n-1} + F_{n-2}$. We shall examine the function $p_F(n)$, which we define to be the number of ways to additively partition the integer n into (not necessarily distinct) Fibonacci numbers.

We first consider the generating function for $p_F(n)$. By elementary partition theory, we have

$$\sum_{n \ge 0} p_F(n) x^n = \prod_{a \in F} \frac{1}{1 - x^a} = \prod_{m \ge 2} \frac{1}{1 - x^{F_m}}.$$
 (1)

Equivalently,

$$\left(\prod_{m \ge 2} (1 - x^{F_m})\right) \sum_{n \ge 0} p_F(n) x^n = 1.$$
 (2)

We may expand the infinite product as a power series

$$\prod_{m \ge 2} (1 - x^{F_m}) = \sum_{m \ge 0} a_m x^m,$$
(3)

where a_m counts the number of partitions of m into an even number of distinct Fibonacci numbers, minus the number of partitions of m into an odd number of distinct Fibonacci numbers; we may write this as

$$a_{m} = p_{p}^{e}(m) - p_{p}^{o}(m).$$
⁽⁴⁾

We shall see later that knowledge of the terms a_m will lead us to a recursion relation for $p_p(n)$. With this objective in mind, we prove the following.

Theorem: Let

$$P_k = \prod_{m=2}^k (1 - x^{F_m}) \quad \text{when } k \ge 2,$$

and set $P_1 = 1$. Let $L_n = F_{n+1} + F_{n-1}$ be the n^{th} Lucas number. Then

$$P_{\infty} = \prod_{m \ge 2} (1 - x^{F_m}) = 1 - x - x^2 + \sum_{k \ge 3} x^{L_k} P_{k-2}.$$

First proof: This proof is combinatorial in nature. First consider the partial products P_k . When expanded as a power series of the form

$$P_k = \sum_{m=0}^k \alpha_m^{(k)} x^m,$$

1986]

the coefficients $a_m^{(k)}$ represent the same thing as the a_m , except that the partitions are now restricted to Fibonacci numbers not exceeding F_k . It is evident that $a_m^{(k)} = a_m$ for all m such that $0 \le m < F_{k+1}$, by inspection of (4). We shall use this fact later.

We may partition an integer n into distinct Fibonacci numbers in one particular way by first writing down the largest Fibonacci number not greater than n, subtracting, and iterating this process on the difference. For example,

$$27 = 21 + 5 + 1$$
.

See the references listed at the end of this paper for a more detailed discussion of these points.

For simplicity of notation, we will represent a partition of a number into distinct Fibonacci numbers as a string of 1's and 0's, with the rightmost place corresponding to $F_2 = 1$, and each succeeding place corresponding to the next Fibonacci number. In the above example,

$$27 = 1 \cdot 21 + 0 \cdot 13 + 0 \cdot 8 + 1 \cdot 5 + 0 \cdot 3 + 0 \cdot 2 + 1 \cdot 1$$

which we may write more compactly as

27:⁽⁸⁾ 27:1001001,

where the (8) signifies that the 1 below it is the coefficient of $F_{a} = 21$.

The first few terms a_m for m = 0, 1, 2, and 3 can be obtained by direct calculation of the first few P_k ; they are seen to be 1, -1, -1, and 0, respectively. Now let $n \ge 3$; our objective will be to characterize the terms a_m in the range $L_n \le m < L_{n+1}$. As $L_3 = 4$, this will give us a_m for every nonnegative m. Since $n \ge 3$, we have a partition of L_{n+1} obtained in the above manner (from here on, all partitions are into distinct Fibonacci numbers, unless otherwise stated):

$$L_{n+1}: 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ \cdots \ 0$$

Thus, we have the following nine possibilities for partitions of *m*, where $L_n \leq m < L_{n+1}$:

(<i>n</i>)	(n)	(<i>n</i>)
(a) $1 \ 0 \ 0 \ 1 \ x \ \cdots \ x$	(d) $0 1 1 0 x \cdots x$	(g) 0 0 1 1 $x \cdots x$
(b) $1 \ 0 \ 0 \ x \ \cdots \ x$	(e) $0 \ 1 \ 0 \ 1 \ x \ \cdots \ x$	(h) $0 \ 0 \ 1 \ 0 \ x \ \cdots \ x$
(c) $0 1 1 1 x \cdots x$	(f) $0 \ 1 \ 0 \ 0 \ x \ \cdots \ x$	(i) $0 \ 0 \ 0 \ x \ x \ \cdots \ x$

The x's indicate "we don't care which digits go here."

In the above list, we may find a one-to-one correspondence between the partitions in (a) and the partitions in (c). Given a partition beginning with 100, we may replace these three digits with 011. Both strings will have equal value because $F_{n+2} = F_{n+1} + F_n$. However, out of each of these pairs of partitions, one is a partition of even cardinality, whereas the other is odd, since they are different only in their first three places. Hence, these partitions will cancel each other out when we compute a_m using equation (4). Similarly, there is a one-to-one correspondence between partitions of type (b) and of type (d), and they cancel out for the same reason. Partitions of the forms (f) and (g) differ only in the positions corresponding to F_{n+1} , F_n , and F_{n-1} ; they cancel each other out in the same way. Partitions of the forms (h) and (i) are excluded from possibility. To see this, recall that

[May

$$F_1 + F_2 + \cdots + F_k = F_{k+2} - 1.$$

Thus, the largest number expressible in the form (h) is

$$F_n + F_n - 2 < 2F_n.$$

But $L_n = F_{n+1} + F_{n-1}$, so

$$L_n = F_n + 2F_{n-1} > F_n + F_{n-1} + F_{n-2} = 2F_n.$$

Thus, if *m* is expressible in the form (h), then $m < L_n$, contrary to assumption. Similarly, if *m* is expressible in the form (i), then $m \le F_{n+1} - 2$, which is less than F_{n+1} , which in turn is less than L_n , again a contradiction.

Therefore, the only class of partitions of m which will contribute to the right-hand side of (4) are those of the form (e). But the leftmost four places in (e) form our partition of L_n ; therefore, the $x \cdots x$ in (e) must represent a partition of $m - L_n$ into distinct Fibonacci numbers of size less than or equal to n - 2. Conversely, given any such partition of $m - L_n$, we can construct a partition of m of the form (e). Since both partitions in this correspondence are of the same parity, i.e., either both are partitions into odd numbers of Fibonacci numbers or both are partitions into even numbers of Fibonacci numbers, we deduce from (4) that

$$a_{L_{n+m}} = a_{m}^{(n-2)}, \text{ whenever } 0 \le m < L_{n-1}.$$
 (6)

We have thus proved the theorem.

Second proof: This proof is analytical. We require the following two results: Let $A = a_1, a_2, \ldots$ be an arbitrary set of positive integers. If |q| < 1, then

$$\prod_{a \in A} \frac{1}{(1 - zq^{a})} = 1 + \sum_{i \ge 1} \frac{zq^{a_i}}{(1 - zq^{a_1})(1 - zq^{a_2}) \cdots (1 - zq^{a_i})},$$
(7)

and

$$\prod_{a \in A} (1 + zq^{a}) = 1 + \sum_{i \ge 1} (1 + zq^{a_{1}}) \cdots (1 + zq^{a_{i-1}})zq^{a_{i}}.$$
(8)

Proof of (7): We consider the partial products. Clearly,

$$\frac{1}{(1-zq^{a_1})}=1+\frac{zq^{a_1}}{(1-zq^{a_1})}.$$

Now suppose that

-

$$\prod_{i=1}^{n} \frac{1}{(1 - zq^{a_1})} = 1 + \sum_{i=1}^{n} \frac{zq^{a_i}}{(1 - zq^{a_1})(1 - zq^{a_2})} \cdots (1 - zq^{a_i})$$

Then

$$\prod_{i=1}^{n+1} \frac{1}{(1-zq^{a_i})} = \left(\prod_{i=1}^{n} \frac{1}{(1-zq^{a_i})}\right) \left(1 + \frac{zq^{a_{n+1}}}{(1-zq^{a_{n+1}})}\right)$$
$$= 1 + \sum_{i=1}^{n} \frac{zq^{a_i}}{(1-zq^{a_1})\cdots(1-zq^{a_i})} + \frac{zq^{a_{n+1}}}{(1-zq^{a_{n+1}})}\prod_{i=1}^{n} \frac{1}{(1-zq^{a_i})}$$

1986]

(5)

$$= 1 + \sum_{i=1}^{n+1} \frac{zq^{a_i}}{(1 - zq^{a_1}) \cdots (1 - zq^{a_i})}.$$

By induction on *n*, the partial products on the left-hand side of (7) are equal to the partial sums on the right-hand side. As $|q| \leq 1$, the sum converges. This proves (7).

Proof of (8): The first partial product is clearly the first partial sum. So suppose that

$$\prod_{i=1}^{n} (1 + zq^{a_i}) = 1 + \sum_{i=1}^{n} (1 + zq^{a_1}) \cdots (1 + zq^{a_{i-1}})zq^{a_i}.$$

Then

$$\prod_{i=1}^{n+1} (1 + zq^{a_i}) = \left(\prod_{i=1}^n (1 + zq^{a_i})\right) (1 + zq^{a_{n+1}})$$

= $1 + \sum_{i=1}^n (1 + zq^{a_1}) \cdots (1 + zq^{a_{i-1}}) zq^{a_i} + zq^{a_{n+1}} \prod_{i=1}^n (1 + zq^{a_i})$
= $1 + \sum_{i=1}^{n+1} (1 + zq^{a_1}) \cdots (1 + zq^{a_{i-1}}) zq^{a_i}.$

By induction on n, this proves (8).

The following argument is due to the referee.

In (8) we set z = -1, q = x, and A = F:

$$\prod_{m \ge 2} (1 - x^{F_m}) = 1 - x - x^2 + x^3 - \sum_{m \ge 3} (1 - x^{F_2}) \cdots (1 - x^{F_m}) x^{F_{m+1}}$$

$$= 1 - x - x^2 + x^3 - \sum_{m \ge 3} (1 - x^{F_2}) \cdots (1 - x^{F_{m-1}}) x^{F_{m+1}}$$

$$+ \sum_{m \ge 3} (1 - x^{F_2}) \cdots (1 - x^{F_{m-1}}) x^{F_{m+2}}$$

$$= 1 - x - x^2 + x^3 - \sum_{m \ge 3} (1 - x^{F_2}) \cdots (1 - x^{F_{m-2}}) x^{F_{m+1}}$$

$$+ \sum_{m \ge 3} (1 - x^{F_2}) \cdots (1 - x^{F_{m-2}}) x^{L_m}$$

$$+ \sum_{m \ge 3} (1 - x^{F_2}) \cdots (1 - x^{F_{m-1}}) x^{F_{m+2}}$$

$$= 1 - x - x^2 + \sum_{m \ge 3} (1 - x^{F_2}) \cdots (1 - x^{F_{m-2}}) x^{L_m}.$$

This proves the theorem.

Corollary: For all $m \ge 0$, a_m is either 1, -1, or 0.

Proof: We have already seen that this is true for $m \leq 3$. Now the degree of P_{k-2} is $1 + 2 + 3 + \cdots + F_{k-2}$, or $F_k - 2$, which is clearly less than $L_{k+1} - L_k$, which equals L_{k-1} . What this tells us is that the polynomials on the right-hand side of the theorem add together without overlapping. Thus, we only need to show that each P_k has coefficients $a_m^{(k)} = 0$, 1, or -1 for all m.

[May

We do this by induction on k. Clearly, it is true for k = 1, as $P_1 = 1$. Suppose, then, that $a_m^{(k)} = 1$, -1, or 0 for all m and all k < n. By the definition of P_n , it is clear that the first F_{n+1} coefficients of P_n are identical to those of P_{∞} ; in other words,

 $a_m = a_m^{(n)}$ for all *m* such that $0 \le m \le F_{n+1}$.

Hence, by the theorem, the first n + 1 terms $a_m^{(n)}$ are the coefficients of the partial products P_k with k such that $L_k < F_{n+1}$; this includes all k less than n - 2 because $L_{n-3} < F_{n+1} < L_{n-2}$. By the induction hypothesis, the first F_{n+1} coefficients are either 1, -1, or 0.

Now recall that P_n is a finite product of "antipalindromic" polynomials of the form $(1 - x^{F_k})$. Thus, we have

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

whenever both subscripts are positive, since the degree of P_n is $F_{n+2} - 2$. But $F_{n+1} > \frac{1}{2}(F_{n+2} - 2)$, so the first half of the coefficients in P_n are 1, -1, or 0. By (9), so are the last half. By induction, all P_k 's have coefficients 1, -1, or 0. By the theorem, all terms a_m are 1, -1, or 0. This proves the corollary.

By equating like terms on both sides of (2), where we have evaluated the product P as the power series (3), we obtain, for all $n \ge 0$:

$$a_0 p_F(n) + a_1 p_F(n-1) + \cdots + a_{n-1} p_F(1) + a_n p_F(0) = 0,$$

where $p_p(0) = 1$ in accordance with the power series (1). This yields a recursion for $p_p(n)$ with all coefficients a_k equal to 1, -1, or 0.

REFERENCES

- Br. U. Alfred. "Exploring the Fibonacci Representations of Integers." The Fibonacci Quarterly 1(1963):72.
- J. L. Brown, Jr. "A New Characterization of the Fibonacci Numbers." The Fibonacci Quarterly 3 (1965):1-8.
- D. E. Daykin. "Representations of Natural Numbers as Sums of Generalized Fibonacci Numbers." J. London Math. Soc. 35 (1960):143-160.
- H. H. Ferns. "On the Representations of Integers as Sums of Distinct Fibonacci Numbers." The Fibonacci Quarterly 3 (1965):21-29.

1986]

HIGHER-ORDER FIBONACCI SEQUENCES MODULO M

DEREK K. CHANG

California State University, Los Angeles, CA 90032 (Submitted July 1984)

Let $\{U_n, n \ge 0\}$ be the ordinary Fibonacci sequence defined by

 $U_0 = 0$, $U_1 = 1$, $U_n = U_{n-1} + U_{n-2}$, for $n \ge 2$.

For any integer $k \ge 2$, let $\{V_k(n), n \ge -k + 2\}$ be the k^{th} -order Fibonacci sequence defined by

$$V_k(j) = 0, \text{ for } -k + 2 \le j \le 0, \quad V_k(1) = 1,$$

and
$$V_k(n) = V_k(n-1) + V_k(n-2) + \dots + V_k(n-k), \text{ for } n \ge 2.$$

It is well known that, for any integer $m \ge 2$, the sequence U_n $[=V_2(n)] \mod m$ is periodic, and it is easy to see that this also holds for any sequence $V_k(n) \mod m$ with $k \ge 3$. For any $m \ge 2$, let p(k, m) denote the length of the period of the sequence $V_k(n) \mod m$. The proof of the next result is almost identical to that in [3] for the ordinary Fibonacci sequence $V_2(n)$, thus is omitted here.

Theorem 1: The sequence $V_k(n) \mod m$ is simply periodic, i.e., it is periodic and it repeats by returning to its starting values. If *m* has the prime factorization $m = \pi q_i^{s_i}$, then $p(k, m) = \text{lcm} [p(k, q_i^{s_i})]$, the least common multiple of the $p(k, q_i^{s_i})$.

In order to prove Theorem 2, we first state Lemma 1, the proof of which is quite simple and, therefore, will be omitted here.

Lemma 1: Let $\{W_i(n), n \ge 0\}$, i = 1, 2, 3, be three sequences such that for each i, $W_i(n) = W_i(n-1) + \cdots + W_i(n-k)$ for all $n \ge k$. If the equality $W_3(n) = W_1(n) + W_2(n)$ holds for $0 \le n \le k - 1$, it also holds for all $n \ge k$.

The following result extends the corresponding result [3] for the sequence $V_2(n)$ to any sequence $V_k(n)$ with $k \ge 2$. Our proof is quite different from that in [3], and we do not have a general formula for $V_k(n)$.

Theorem 2: Let q be any prime number. If $p(k, q^2) \neq p(k, q)$, then

 $p(k, q^e) = q^{e-1}p(k, q)$

(1)

for any integer $e \ge 2$.

Proof: Let r = p(k, q). For the sake of simpler notation, we shall prove (1) only for e = 2. The same proof stands, with obvious modifications, for e > 2. Define the k-tuple

$$T_0 = (V_k(-k+2), \ldots, V_k(1)) = (0, \ldots, 0, 1),$$

and

[May

$$T_{1} = (V_{k}(-k+2+r), \dots, V_{k}(1+r)) = (0, \dots, 0, 1) \mod q$$
$$= (qs_{1}, \dots, qs_{k-1}, qs_{k}+1) \mod q^{2},$$

where $0 \leq s_j \leq q$ for $1 \leq j \leq k$, and $s_1 + \cdots + s_k \geq 1$. The k-tuple T_1 is obtained by moving T_0 r units to the right.

 $\ensuremath{\mathcal{T}_{\text{l}}}$ can be decomposed as follows:

$$T_{1} = qs_{1}(1, 1, 2, ..., 2^{k-2}) + q(s_{2} - s_{1})(0, 1, 1, ..., 2^{k-3}) + q(s_{3} - s_{2} - s_{1})(0, 0, 1, ..., 2^{k-4}) + \cdots + [q(s_{k} - s_{k-1} - \cdots - s_{1}) + 1](0, 0, ..., 0, 1) \mod q^{2}.$$

Applying Lemma 1, one can obtain the k-tuple T_2 by moving $T_1 r$ units to the right.

$$\begin{split} T_2 &= [q(s_k - s_{k-1} - \dots - s_1) + 1](qs_1, qs_2, qs_3, \dots, qs_{k-1}, qs_k + 1) + \dots \\ &+ q(s_2 - s_1)(qs_{k-1}, qs_k + 1, q(s_k + s_{k-1} + s_{k-2}) + 1, \dots, q(\dots) + 2^{k-3}) \\ &+ qs_1(qs_k + 1, q(s_k + s_{k-1} + s_{k-2}) + 1, \dots, q(\dots) + 2^{k-2}) \mod q^2 \\ &= (2qs_1, 2qs_2, \dots, 2qs_{k-1}, 2qs_k + 1) \mod q^2. \end{split}$$

Similarly, one has

$$T_j = (jqs_1, jqs_2, ..., jqs_{k-1}, jqs_k + 1) \mod q^2$$

for $2 \le j \le q$. Since q is a prime number, $T_j \ne T_0$ for $1 \le j \le q - 1$, and since $T_q = T_0 \mod q^2$, we have $p(k, q^2) = qr = qp(k, q)$. This completes the proof.

As a final remark, we note that some simple facts about higher-order Fibonacci sequences can be easily observed. For example, many moduli *m* have the property that the sequence $V_k(n) \mod m$ contains a complete system of residue modulo m, while m = 8 and m = 9 are the smallest moduli which do not have this property in the case k = 3, and they are said to be defective [2]. For m = 2and m = 11, the sequence $V_3(n) \mod m$ is uniformly distributed. (See [1] for a definition.) It is interesting to extend the results for ordinary Fibonacci sequences to those of higher order.

REFERENCES

- L. Kuipers & J. S. Shiue. "A Distribution Property of the Sequence of Fibonacci Numbers." The Fibonacci Quarterly 10 (1972):375-376, 392.
 A. P. Shah. "Fibonacci Sequence Modulo m." The Fibonacci Quarterly 6
- (1968): 139 141.
- 3. D. D. Wall. "Fibonacci Series Modulo m." Amer. Math. Monthly 67 (1960): 525-532.

A NOTE ON PASCAL-T TRIANGLES, MULTINOMIAL COEFFICIENTS, AND PASCAL PYRAMIDS

RICHARD C. BOLLINGER Behrend College, Pennsylvania State University, Erie, PA 16563 (Submitted August 1984)

1. INTRODUCTION

In what follows we give a formula for the entries in the Pascal-T triangle T_m in terms of the multinomial coefficients; this is the counterpart for these arrays of the result of Philippou [1] on the elements of the Fibonacci k-sequences in terms of the multinomial coefficients. The proof is direct, and the method also leads to a recurrence relation which gives the elements of a given triangle T_m as a combination of certain elements of the "preceeding" triangle T_{m-1} , the coefficients in the combination being binomial coefficients. Finally, because the multinomial coefficients provide the connection here, we offer some remarks on those arrays of multinomial coefficients referred to in the literature as "Pascal pyramids."

It will be convenient to recall the definition of the triangle T_m .

Definition 1.1: For any $m \ge 0$, T_m is the array whose rows are indexed by n = 0, 1, 2, ..., and columns by k = 0, 1, 2, ..., and whose entries are obtained as follows:

- a) T_0 is the all-zero array;
- b) T_1 is the array all of whose rows consist of a one followed by zeros;
- c) T_m , $m \ge 2$, is the array whose n = 0 row is a one followed by zeros, whose n = 1 row is *m* ones followed by zeros, and any of whose entries in subsequent rows is the sum of the *m* entries just above and to the left in the preceeding row.

The entry in row n and column k is denoted by $C_m(n, k)$, although we note that

 $C_2(n, k) = \binom{n}{k},$

since T_2 is *the* Pascal Triangle. There will be n(m - 1) + 1 nonzero entries in row n, and the principal property we need is that these are the coefficients (see, e.g., [2], p. 66) in the expansion

$$(1 + t + t2 + \dots + tm-1)n = \sum_{k=0}^{n(m-1)} C_m(n, k) t^k.$$
(1.1)

Although it is easy to use property (c) to build the array T_m by means of the relation

$$C_m(n, k) = \sum_{j=0}^{m-1} C_m(n-1, k-j), \qquad (1.2)$$

the main result presented here evaluates $C_m(n, k)$ directly as a sum of certain multinomial coefficients.

[May

2. FORMULAS FOR $C_m(n, k)$

Theorem 2.1: If $C_m(n, k)$ is the (n, k)-entry in $T_m, m \ge 3$, then for any $n \ge 0$ and $0 \le k \le n(m - 1)$,

$$C_{m}(n, k) = \sum_{n_{1}, n_{2}, \dots, n_{m}} \binom{n}{n_{1}, n_{2}, \dots, n_{m}},$$
(2.1)

where the summation is over all *m*-part compositions n_1 , n_2 , ..., n_m of *n* such that (1) $n_1 + n_2 + \cdots + n_m = n$, and (2) $0n_1 + 1n_2 + \cdots + (m-1)n_m = k$.

Proof: The proof follows directly from the multinomial theorem, for if in

$$(x_1 + x_2 + \dots + x_m)^n = \sum \binom{n}{n_1, \dots, n_m} x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}, \qquad (2.2)$$

where the summation is over all *m*-part compositions of *n*, we put $x_i = t^{i-1}$, $1 \le i \le m$, we have

$$(1 + t + \dots + t^{m-1})^n = \sum {\binom{n}{n_1, \dots, n_m}} t^{\frac{n_2 + 2n_3 + \dots + (m-1)n_m}{m}}, \qquad (2.3)$$

and when the coefficients of t^k on the right-hand sides of (1.1) and (2.3) are equated, (2.1) follows from conditions (1) and (2).

Example: $C_4(4, 4) = \begin{pmatrix} 4 \\ 0, 4, 0, 0 \end{pmatrix} + \begin{pmatrix} 4 \\ 1, 2, 1, 0 \end{pmatrix} + \begin{pmatrix} 4 \\ 2, 0, 2, 0 \end{pmatrix} + \begin{pmatrix} 4 \\ 2, 1, 0, 1 \end{pmatrix}$ = 1 + 12 + 6 + 12 = 31

Another application of the multinomial expansion, used partly as a binomial expansion, gives the following theorem.

Theorem 2.2:

$$C_m(n, k) = \sum_{j=0}^n \binom{n}{j} C_{m-1}(j, k-j).$$
(2.4)

Proof: If the left side of (2.2) is grouped as $[x_1 + (x_2 + \dots + x_m)]^n$, expanded as a binomial, and again t^{i-1} is substituted for x_i , the result is

$$\sum_{k=0}^{n(m-1)} C_m(n, k) t^k = \sum_{j=0}^n {n \choose j} t^j (1 + t + \dots + t^{m-2})^j.$$
(2.5)

But then the factors $(1 + t + \dots + t^{m-2})^j$ may be expressed in terms of C_{m-1} 's, using (1.1). When the coefficients of a given power of t on the right of (2.5) are collected and equated to the corresponding coefficient on the left, then (2.4) follows.

Example:
$$C_4(4, 4) = \binom{4}{0}C_3(0, 4) + \binom{4}{1}C_3(1, 3) + \binom{4}{2}C_3(2, 2)$$

+ $\binom{4}{3}C_3(3, 1) + \binom{4}{4}C_3(4, 0)$
= $1 \cdot 0 + 4 \cdot 0 + 6 \cdot 3 + 4 \cdot 3 + 1 \cdot 1 = 31$

1986]

A NOTE ON PASCAL-T TRIANGLES, MULTINOMIAL COEFFICIENTS, AND PASCAL PYRAMIDS

3. THE PASCAL PYRAMID

The device used in the previous theorem of bracketing off one term of a multinomial in order to expand the result as a binomial can, of course, be repeated with the remaining multinomial parts, eventually running the unexpanded part down to a binomial itself; this offers the possibility of obtaining the multinomials entirely as products of binomial coefficients. In fact, this has been done in [3] and [4] for a trinomial expansion, with the multinomial coefficients appearing in the successive powers of $(x_1 + x_2 + x_3)$ being associated with points in triangular arrays, which form successive levels of a pyramidal structure-the so-called Pascal pyramid. For example, Figure 1 shows the first four levels, with each point labelled with both a multinomial coefficient and the composition which gives rise to it (the compositions can be obtained by designating the sides as first, second, third in some fashion, and letting n_1 , n_2 , n_3 in the composition measure units of perpendicular distances from the first, second, third sides, respectively). The law of formation for this trinomial case is clear (and also correct, as is easily verified by doing the reduction described earlier): just generate the ordinary Pascal triangle down to level n, and then multiply the rows successively upward by the numbers found in the last line. For n = 3, e.g.,





Figure 1. Levels of the Pascal Pyramid for the Case $(x_1 + x_2 + x_3)$

[May

This works nicely, the idea is not restricted to trinomials (the generalization is not just a bigger triangle, but it is similarly simple), and there have been several comments to the effect that it is surprising that the Pascal pyramids (or hyperpyramids) are not more widely known or used.

Why should this be? An answer would seem to be that as soon as one gets past the trinomials, the method, while still elegant, becomes computationally unwieldy. That is, in the usual expansion of a multinomial $(x_1 + \cdots + x_m)^n$ there are $\binom{n+m-1}{n}$ terms corresponding to the *m*-part compositions of *n*. To see what is required to deal with these in terms of products of binomials, we look at what might be called the Pascal square, in which we tabulate for m = 0, 1, 2, ... and n = 0, 1, 2, ... the number of *m*-part compositions of *n* (taking the entry for m = n = 0 to be one). The first several lines are shown below:

	n					
No. Parts <i>m</i>	0	1	2	3	4	5
0	1	0	0	0	0	0
1	1	1	1	1	1	1
2	1	2	3	4	5	6
3	1	3	6	10	15	21
4	1	4	10	20	35	56
5	1	5	15	35	70	126
-		-				

Pascal Square

Here, the law of formation is that each entry is the sum of all those entries above and to the left of it in the preceeding row, and we recognize the m = 3row as the triangular numbers, the m = 4 as the pyramidal numbers, and so on. The point here is that the square shows that the trinomials (m = 3) are simple sequences of products of binomials; as in the example, the ten trinomials in $(x_1 + x_2 + x_3)^3$ reduce to 4 + 3 + 2 + 1 products of binomials. But for m > 3, we find not sequences, but sequences of sequences. The thirty-five terms in $(x_1 + x_2 + x_3 + x_4)^4$ [the (4, 4) entry], e.g., have to be obtained using the sequence

> 15 = 5 + 4 + 3 + 2 + 1, 10 = 4 + 3 + 2 + 1, 6 = 3 + 2 + 1, 3 = 2 + 1,1 = 1,

of sequences of products of binomials. It would seem that in spite of the appeal of an array for multinomial coefficients similar to the triangle for binomials, one is better off for most purposes using a convenient algorithm (e.g., [5], pp. 46-51) to generate the *m*-part compositions of *n*, from which the exponents on the x_i and the multinomial associated with a given term are immediately available.

1986]

A NOTE ON PASCAL-T TRIANGLES, MULTINOMIAL COEFFICIENTS, AND PASCAL PYRAMIDS

REFERENCES

- 1. A. N. Philippou. "A Note on the Fibonacci Sequence of Order k and the Multinomial Coefficients." The Fibonacci Quarterly 21 (1983):82-86.
- 2. G. Chrystal. Textbook of Algebra, Part One. 5th edition. New York: Dover, 1961.
- 3. H. Staib & L. Staib. "The Pascal Pyramid." The Mathematics Teacher 71 (1978):505-510.
- 4. H. F. Lucas. "Paths and Pascal Numbers." College Mathematics Journal 14 (1983):329-341.
- 5. A. Nijenhuis & H. S. Wilf. *Combinatorial Algorithms*. 2nd edition. New York: Academic Press, 1978.

ANNOUNCEMENT

SECOND INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS

August 13–16, 1986 San Jose State University San Jose, California 95192

LOCAL COMMITTEE Bergum, Gerald, *Chairman* Edgar, Hugh, *Cochairman*

> Thoro, Dmitri Johnson, Marjorie Lange, Lester



INTERNATIONAL COMMITTEE Philippou, A. (Greece) Chairman Horadam, A.F. (Australia), Cochairman Bergum, G. (U.S.A.) Kiss, P. (Hungary) Long, C. (U.S.A.) Ando, S. (Japan)

CALL FOR PAPERS

The SECOND INTERNATIONAL CONFERENCE ON FIBONACCI NUMBERS AND THEIR APPLICATIONS will take place at San Jose State University, San Jose, CA, Aug. 13-16, 1986. This conference is sponsored jointly by The Fibonacci Association and San Jose State University.

Papers on all branches of mathematics and science related to the Fibonacci numbers and their generalizations are welcome. Manuscripts are requested by June 15, 1986. Abstracts and manuscripts should be send to the chairman of the local committee. 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, 1986. All talks should be limited to one hour.

For further information concerning the conference, please contact either of the following:

Professor G.E. Bergum, Editor The Fibonacci Quarterly Department of Mathematics South Dakota State University P.O. Box 2220 Brookings, S.D. 57007–1297 Professor Calvin Long Department of Mathematics Washington State University Pullman, Wash. 99163

[May

AN ENTIRE FUNCTION THAT GIVES THE FIBONACCI NUMBERS AT THE INTEGERS

A. W. GOODMAN University of South Florida, Tampa FL 33620 (Submitted August 1984)

1. INTRODUCTION

It is well known that $\Gamma(z)$ is an analytic function of z that gives n! when z = n + 1. It is reasonable to look for a similar function for the Fibonacci numbers F_n . Several such functions are known (see Bunder [2] where further references are given), but the formula we will derive is more general than any of those obtained earlier.

To be specific, we are looking for an F(z) with the following properties:

- (a) F(z) is an analytic function (perhaps entire),
- (b) F(z) is real valued for all real z,
- (c) $F(n) = F_n$, the n^{th} Fibonacci number for all integers n,
- (d) For z in the domain of analyticity we have

$$F(z + 2) = F(z + 1) + F(z).$$
(1)

It is clear that if $F(0) = F_0 = 0$ and $F(1) = F_1 = 1$, then equation (1) implies that $F(n) = F_n$ for every positive integer n. This follows immediately from the defining equations $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$. In fact, this latter relation can be used to define the Fibonacci numbers for negative integers.

If F(z) satisfies the functional equation (1), then so does each derivative $F^{(m)}(z)$, $m = 1, 2, \ldots$. This suggests that we try e^{Rz} as a solution, for some number R. When e^{Rz} is used in (1), we find that it is a solution if and only if e^R is a root of

 $x^2 = x + 1.$ (2)

Using the standard notation for the roots of (2), we have

$$\alpha = \frac{1 + \sqrt{5}}{2}, \qquad \beta = \frac{1 - \sqrt{5}}{2}, \qquad (3)$$

and hence

 $R = \ln \alpha \text{ or } R = \ln \beta = \ln |\beta| + (2q + 1)\pi i, q = 0, \pm 1, \pm 2, \dots$

Using the linearity of (1) (see Spickerman [4]), it is clear that if p and q are integers, and C_1 and C_2 are arbitrary real numbers, then

$$f(z) = C_1 e^{z(\ln \alpha + 2p\pi i)} + C_2 e^{z(\ln |\beta| + (2q+1)\pi i)}$$
(4)

satisfies the functional equation (1). Now f(z) is an entire function but it is not real valued for every real z_i . To remedy this defect, we consider

1986]

 $[f(z) + \overline{f(z)}]/2.$

This function is not an analytic function, but if we replace z by x we obtain the real function

$$F(x) = C_1 e^{x \ln \alpha} \cos 2p \pi x + C_2 e^{x \ln |\beta|} \cos(2q + 1) \pi x.$$
 (5)

If we now replace x by z in (5), we have a function that satisfies the conditions (a), (b), and (d). The initial conditions F(0) = 0 and F(1) = 1 force the selection $C_1 = 1/\sqrt{5}$ and $C_2 = -1/\sqrt{5}$. Then, finally, the function

$$F(z) = \frac{1}{\sqrt{5}} \left[e^{z \ln \alpha} \cos 2p\pi z - e^{z \ln |\beta|} \cos(2q+1)\pi z \right]$$
(6)

has all of the properties (a), (b), (c), and (d) that we wish.

Equation (6) was given earlier by Spickerman [4] and is an entire function that gives the Fibonacci numbers for integral values of z.

2. THE MAIN THEOREM

Equation (6) gives a countable infinity of functions that satisfy the conditions (a), (b), (c), and (d), and we may ask if we now have all such functions. In fact, we shall soon see that (6) gives only a tiny portion of the functions that satisfy (a), (b), (c), and (d). We first observe that if α and β are the roots of (2) and *m* is an integer, then

$$G(z) = e^{z \ln \alpha} \sin 2m\pi z + e^{z \ln |\beta|} \sin(2m+1)\pi z$$
(7)

satisfies the three conditions (a), (b), and (d). Further, G(n) = 0 for every integer n.

We now take linear combinations of the functions F(z) and G(z) defined by (6) and (7). To simplify the presentation, we impose a condition on the coefficients to ensure that we obtain entire functions.

Definition: We say that the real sequences $\{A_m\}$, $\{B_m\}$, $\{C_m\}$, and $\{D_m\}$ satisfy condition E if

$$\sum_{m=0}^{\infty} C_m = 1, \qquad \sum_{m=0}^{\infty} D_m = 1$$
 (8)

and

$$\sum_{m=0}^{\infty} A_m e^{mz}, \qquad \sum_{m=0}^{\infty} B_m e^{mz}, \qquad \sum_{m=0}^{\infty} C_m e^{mz}, \qquad \sum_{m=0}^{\infty} D_m e^{mz}$$
(9)

are all entire functions.

These are very weak restrictions. For example, (9) is trivially satisfied if all but a finite number of terms in each sequence are zero. The linearity of equation (1), and our earlier work, immediately give

Theorem 1: Let $\{A_m\}$, $\{B_m\}$, $\{C_m\}$, $\{D_m\}$ satisfy condition *E*, and let α and β be defined by (3). Then each one of the functions

$$F(z) = \frac{1}{\sqrt{5}} \sum_{m=0}^{\infty} C_m e^{z \ln \alpha} \cos 2m\pi z - \frac{1}{\sqrt{5}} \sum_{m=0}^{\infty} D_m e^{z \ln |\beta|} \cos(2m+1)\pi z +$$
(10) (continued)

[May

AN ENTIRE FUNCTION THAT GIVES THE FIBONACCI NUMBERS AT THE INTEGERS

$$+\sum_{m=0}^{\infty} A_m e^{z \ln \alpha} \sin 2m\pi z + \sum_{m=0}^{\infty} B_m e^{z \ln |\beta|} \sin(2m+1)\pi z$$

satisfies the conditions (a), (b), (c), and (d).

It is clear that (1) gives an uncountable infinity of suitable functions. We still have an uncountable infinity if we set all coefficients equal to zero except C_0 , $C_1 = 1 - C_0$, D_0 , and $D_1 = 1 - D_0$. Do we have all such function? In other words, given a function with prop-

Do we have all such function? In other words, given a function with properties (a), (b), (c), and (d), is it one of the functions described in Theorem 1? This is an open problem.

The Fibonacci numbers satisfy many interesting relations, see, for example, Bachman [1, II:55-96], Vorob'ev [5], or Wall [6]. Many of these generalize, and we cite only a few here.

If F(z) is any one of the uncountably many functions given in Theorem 1, then, for all z,

$$\sum_{k=0}^{N} F(z+k) = F(z+N+2) - F(z+1), \qquad (11)$$

$$\sum_{k=1}^{N} F(z + 2k - 1) = F(z + 2N) - F(z), \qquad (12)$$

and

k

$$\sum_{k=0}^{2N} (-1)^k F(z+k) = F(z+2N-1) - F(z-2).$$
(13)

3. A GENERALIZATION

One natural generalization arises when we replace $F_{n+2} = F_{n+1} + F_n$ by

 $F_{n+2} = rF_{n+1} + sF_n$

and impose the initial conditions $F_0 = a$ and $F_1 = b$. To extend the work of §1 and §2, we look for entire functions that are real on the real axis, give the generalized Fibonacci numbers at the positive integers, and satisfy the functional equation

$$F(z + 2) = rF(z + 1) + sF(z)$$
(14)

for all z. Here we restrict r, s, a, and b to be real. We preserve the basic notation of §2 and set

$$\alpha = \frac{r + \sqrt{r^2 + 4s}}{2}, \qquad \beta = \frac{r - \sqrt{r^2 + 4s}}{2}, \qquad (15)$$

the two roots of

 $x^2 = rx + s. \tag{16}$

[Compare this equation with equation (2).]

For simplicity, we assume that α and β are distinct real roots, and this implies that $r^2 + 4s > 0$. We also assume that $s \neq 0$ because, if s = 0, equation (14) reduces to F(z + 1) = rF(z) for all z, and the generalized Fibonacci sequence is then a geometric sequence. If r and s are positive, then $\alpha > 0 > \beta$. We consider this case first.

1986]

Theorem 2: Suppose that $\alpha > 0 > \beta$, where α and β are given by (15), r and s are real numbers, and the sequences $\{A_m\}$, $\{B_m\}$, $\{C_m\}$, and $\{D_m\}$ satisfy condition E. Set

$$F(z) = \sum_{m=0}^{\infty} \frac{-\alpha\beta + b}{\alpha - \beta} C_m e^{z \ln \alpha} \cos 2m\pi z + \sum_{m=0}^{\infty} \frac{\alpha\alpha - b}{\alpha - \beta} D_m e^{z \ln |\beta|} \cos(2m + 1)\pi z + \sum_{m=0}^{\infty} (A_m e^{z \ln \alpha} \sin 2m\pi z + B_m e^{z \ln |\beta|} \sin(2m + 1)\pi z).$$
(17)

Then:

- (a) F(z) is an entire function;
- (b) F(z) is real on the real axis;
- (c) F(z) satisfies the functional equation (14);
- (d) for all positive integers $F(n) = F_n$, the n^{th} generalized Fibonacci number defined by $F_0 = \alpha$, $F_1 = b$, $F_{n+2} = rF_{n+1} + sF_n$, $n = 0, 1, 2, \ldots$.

We omit the proof because it follows the pattern set forth in §2. First, one shows that each individual term satisfies (14), and then one applies the linearity property. A simple computation shows that $F(0) = \alpha$ and F(1) = b. Parker [3] obtained a simplified version of (17) in which only two of the coefficients are different from zero.

If r > 0 and s < 0, then $\alpha > \beta > 0$. In this case, we have

Theorem 3: Suppose that $\alpha > \beta > 0$ and the sequences $\{A_m\}$, $\{B_m\}$, $\{C_m\}$, and $\{D_m\}$ satisfy condition *E*. Set

$$F(z) = \sum_{m=0}^{\infty} \frac{-\alpha\beta + b}{\alpha - \beta} C_m e^{z \ln \alpha} \cos 2m\pi z + \sum_{m=0}^{\infty} \frac{\alpha\alpha - b}{\alpha - \beta} D_m e^{z \ln \beta} \cos 2m\pi z + \sum_{m=0}^{\infty} (A_m e^{z \ln \alpha} \sin 2m\pi z + B_m e^{z \ln \beta} \sin 2m\pi z).$$
(18)

Then F(z) satisfies conditions (a), (b), (c), and (d) of Theorem 2.

The proof is similar to that of Theorem 2; thus, it is omitted here.

If r < 0 and s < 0, then $0 > \alpha > \beta$. In this case, we replace α and β by $|\alpha|$ and $|\beta|$, respectively, in (18). Further, cos $2m\pi z$ is replaced by $\cos(2m + 1)\pi z$ and $\sin 2m\pi z$ is replaced by $\sin(2m + 1)\pi z$. The details are left to the reader.

In each of the three cases, there is an uncountable infinity of functions, each satisfying the conditions (a), (b), (c), and (d).

4. CONCLUDING REMARKS

We return to the original Fibonacci sequence 0, 1, 1, 2, 3, 5, ... treated in §§1 and 2. If α and β are given by (3), then, as is well known,

$$F_n = \frac{1}{\sqrt{5}} (\alpha^n - \beta^n) \,. \tag{19}$$

[May

AN ENTIRE FUNCTION THAT GIVES THE FIBONACCI NUMBERS AT THE INTEGERS

This formula for F_n is called Binet's formula. If we replace the minus sign by a plus sign in (19), we obtain

$$L_n = \alpha^n + \beta^n. \tag{20}$$

These numbers L_n , n = 0, 1, 2, ..., are often called the Lucas numbers [5, 6]. Now $L_0 = 2$, $L_1 = 1$, and $L_{n+2} = L_{n+1} + L_n$ for n = 0, 1, 2, Consequently, Theorem 2 gives a set of uncountably many entire functions for the Lucas numbers. Indeed, set a = 2 and b = 1 in (17) to obtain

$$\frac{-\alpha\beta+b}{\alpha-\beta} = 1 \quad \text{and} \quad \frac{\alpha\alpha-b}{\alpha-\beta} = 1. \tag{21}$$

Then $F(n) = L_n$ for all n.

Finally, we note that Binet's formula can be extended to cover the generalized Fibonacci numbers treated in §3. Let r, s, a, b, α , and β be real numbers, where α and β are given by (15). If $F_0 = a$, $F_1 = b$, $F_{n+2} = rF_{n+1} + sF_n$, for $n = 0, 1, 2, \ldots$, then

$$F_n = \frac{-\alpha\beta + b}{\alpha - \beta} \alpha^n + \frac{\alpha\alpha - b}{\alpha - \beta} \beta^n, \text{ for } n = 0, 1, 2, \dots$$
 (22)

Here, of course, we assume that $r^2 + 4s > 0$ so $\alpha \neq \beta$ and both α and β are real numbers. For brevity, we omit the discussion of the special cases (a) $\alpha = \beta$, (b) $\alpha = 0 > \beta$, and (c) $\alpha > \beta = 0$. In these last two cases, equation (16) gives s = 0. Hence, $F_{n+1} = rF_n$ and the sequence $\{F_n\}$ is a geometric sequence.

REFERENCES

- 1. Paul Bachman. Niedere Zahlentheorie. New York: Chelsea, 1968.
- 2. M. W. Bunder. "More Fibonacci Functions." The Fibonacci Quarterly 16 (1978):97-98.
- 3. Francis D. Parker. "A Fibonacci Function." The Fibonacci Quarterly 6 (1968):1-2.
- 4. W. R. Spickerman. "A Note on Fibonacci Functions." The Fibonacci Quarterly 8 (1970):397-401.
- 5. N. N. Vorob'ev. Fibonacci Numbers. New York: Blaisdell, 1961.
- 6. Charles R. Wall. Selected Topics in Elementary Number Theory. Columbia: University of South Carolina Press, 1971.

1986]

ON THE ENUMERATOR FOR SUMS OF THREE SQUARES

JOHN A. EWELL

Northern Illinois University, DeKalb, IL 60115 (Submitted September 1984)

1. INTRODUCTION

For each nonnegative integer n, $r_3(n)$ denotes the cardinal number of the set:

$$\{(x_1, x_2, x_3) \in \mathbb{Z}^3 | n = x_1^2 + x_2^2 + x_3^2\}.$$

We here propose to express r_3 in terms of simple divisor functions, defined as follows.

Definition: For each pair of positive integers i, n, with $i \leq 2$, $\delta_i(n)$ is defined by

$$\delta_i(n) = \sum_{\substack{d \mid n \\ d \equiv i \pmod{3}}} (-1)^{(n/d) - 1}.$$

Theorem 1: Let *n* denote an arbitrary positive integer.

(i) If $n = 3m^2$, for some positive integer *m*, then

$$\begin{aligned} r_{3}(n) &= 2 + 6(-1)^{n} [\delta_{2}(n) - \delta_{1}(n)] \\ &+ 12(-1)^{n} \sum_{i=1}^{n} (-1)^{n} [\delta_{2}(n - 3i^{2}) - \delta_{1}(n - 3i^{2})]. \end{aligned}$$

(ii) If *n* is not of the form $3m^2$, then

$$\begin{split} r_3(n) &= 6(-1)^n [\delta_2(n) - \delta_1(n)] \\ &+ 12(-1)^n \sum_{i=1}^n (-1)^n [\delta_2(n-3i^2) - \delta_1(n-3i^2)]. \end{split}$$

In both statements (i) and (ii), summation for the sums indexed by i extends over all values of i for which the arguments of δ_1 and δ_2 are positive.

In §2, we prove this theorem. Our concluding remarks are concerned with comparison of the present representation of r_3 with the classical representation due to Dirichlet.

2. PROOF OF THEOREM 1

Our proof is predicated on the quintuple-product identity

$$\prod_{1}^{\infty} (1 - x^{n})(1 - ax^{n})(1 - a^{-1}x^{n-1})(1 - a^{2}x^{2n-1})(1 - a^{-2}x^{2n-1}) = \sum_{-\infty}^{\infty} x^{n(3n+1)/2}(a^{3n} - a^{-3n-1}), \qquad (1)$$

which (as observed by Carlitz and Subbarao [1]) is derivable from the classical

150

[May

ON THE ENUMERATOR FOR SUMS OF THREE SQUARES

triple-product identity

æ

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

Both identities are valid for each pair of complex numbers a, x such that $a \neq 0$ and |x| < 1. We shall also require the following classical identities associated with the names of Euler, Gauss, and Jacobi.

$$\prod_{1}^{n} (1 - x^{2n-1})(1 + x^n) = 1,$$
(3)

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

Identity (4) is an easy special case of (2) (simply set a = 1), but we list it separately to observe that the cube of its right side generates r_3 .

In (1), let $a \rightarrow a^2$ and multiply the resulting identity by a to get:

$$(a - a^{-1}) \prod_{1}^{\infty} (1 - x^{n}) (1 - a^{2}x^{n}) (1 - a^{-2}x^{n}) (1 - a^{4}x^{2n-1}) (1 - a^{-4}x^{2n-1})$$

$$= a \sum_{-\infty}^{\infty} x^{n(3n+1)/2} a^{6n} - a^{-1} \sum_{-\infty}^{\infty} x^{n(3n+1)/2} a^{-6n}$$

$$= a \prod_{1}^{\infty} (1 - x^{3n}) (1 + a^{6}x^{3n-1}) (1 + a^{-6}x^{3n-2})$$

$$- a^{-1} \prod_{1}^{\infty} (1 - x^{3n}) (1 + a^{-6}x^{3n-1}) (1 + a^{6}x^{3n-2}).$$
(5)

Here we have used (2) to express the infinite series as infinite products. For the sake of brevity, put

$$F(a) = F(a, x) = \prod_{1}^{\infty} (1 - a^2 x^n) (1 - a^{-2} x^n) (1 - a^4 x^{2n-1}) (1 - a^{-4} x^{2n-1}),$$

$$G(a) = G(a, x) = \prod_{1}^{\infty} (1 + a^6 x^{3n-1}) (1 + a^{-6} x^{3n-2}),$$

and

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

Hence, (5) becomes

$$\prod_{1}^{\infty} (1 - x^{n})(a - a^{-1})F(a) = \prod_{1}^{\infty} (1 - x^{3n})\{aG(a) - a^{-1}H(a)\}.$$

We now differentiate the foregoing identity with respect to a to get:

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

=
$$\prod_{1}^{\infty} (1 - x^{3n}) \{ G(a) + a^{-2}H(a) + aG'(a) - a^{-1}H'(a) \}.$$
 (6)

Sequentially, we use the technique of logarithmic differentiation to evaluate G'(a) and H'(a), substitute these evaluations into (6), let $a \rightarrow 1$ in the resulting identity, and finally cancel a factor of 2 to get:

1986]

ON THE ENUMERATOR FOR SUMS OF THREE SQUARES

$$\begin{split} &\prod_{1}^{\infty} (1-x^{n})^{3} (1-x^{2n-1})^{2} \\ &= \prod_{1}^{\infty} (1-x^{3n}) (1+x^{3n-1}) (1+x^{3n-2}) \left\{ 1+6 \left(\sum_{1}^{\infty} \frac{x^{3n-1}}{1+x^{3n-1}} - \sum_{1}^{\infty} \frac{x^{3n-2}}{1+x^{3n-2}} \right) \right\} \\ &= \prod_{1}^{\infty} (1-x^{3n}) (1+x^{3n-1}) (1+x^{3n-2}) \left\{ 1+6 \sum_{1}^{\infty} \left[\delta_{2}(n) - \delta_{1}(n) \right] x^{n} \right\}. \\ &\prod_{1}^{\infty} \frac{(1-x^{n})^{3} (1-x^{2n-1})^{2}}{(1-x^{3n}) (1+x^{3n-1}) (1+x^{3n-2})} \\ &= \prod_{1}^{\infty} (1-x^{n})^{3} (1-x^{2n-1})^{3} \cdot \frac{(1+x^{3n}) (1+x^{3n-1}) (1+x^{3n-2})}{(1-x^{3n}) (1+x^{3n-1}) (1+x^{3n-2})} \\ &= \lim_{1}^{\infty} (1-x^{n})^{3} (1-x^{2n-1})^{3} \cdot \frac{(1+x^{3n}) (1+x^{3n-1}) (1+x^{3n-2})}{(1-x^{3n}) (1+x^{3n-1}) (1+x^{3n-2})} \\ &= \lim_{1}^{\infty} (1-x^{n})^{3} (1-x^{2n-1})^{3} \cdot \frac{(1+x^{3n}) (1+x^{3n-1}) (1+x^{3n-2})}{(1-x^{3n}) (1+x^{3n-1}) (1+x^{3n-2})} \\ &= \lim_{1}^{\infty} (1-x^{n})^{3} (1-x^{2n-1})^{3} \cdot \frac{(1+x^{3n}) (1+x^{3n-1}) (1+x^{3n-2})}{(1-x^{3n}) (1+x^{3n-1}) (1+x^{3n-2})} \\ &= \lim_{1}^{\infty} (1-x^{n})^{3} (1-x^{2n-1})^{3} \cdot \frac{(1+x^{3n}) (1+x^{3n-1}) (1+x^{3n-2})}{(1-x^{3n}) (1+x^{3n-1}) (1+x^{3n-2})} \\ &= \lim_{1}^{\infty} (1-x^{n})^{3} (1-x^{2n-1})^{3} \cdot \frac{(1+x^{3n}) (1+x^{3n-1}) (1+x^{3n-2})}{(1-x^{3n}) (1+x^{3n-1}) (1+x^{3n-2})} \\ &= \lim_{1}^{\infty} (1-x^{n})^{3} (1-x^{2n-1})^{3} \cdot \frac{(1+x^{2n-1}) (1+x^{2n-1}) (1+x^{2n-2})}{(1-x^{2n-1}) (1+x^{2n-1}) (1+x^{2n-2})} \\ &= \lim_{1}^{\infty} (1-x^{2n-1})^{3} (1-x^{2n-1})^{3} \cdot \frac{(1+x^{2n-1}) (1+x^{2n-1}) (1+x^{2n-2})}{(1-x^{2n-1}) (1+x^{2n-2})} \\ &= \lim_{1}^{\infty} (1-x^{2n-1})^{3} (1-x^{2n-1})^{3} \cdot \frac{(1+x^{2n-1}) (1+x^{2n-1}) (1+x^{2n-2})}{(1-x^{2n-1}) (1+x^{2n-2})} \\ &= \lim_{1}^{\infty} (1-x^{2n-1})^{3} (1-x^{2n-1})^{3} \cdot \frac{(1+x^{2n-1}) (1+x^{2n-2})}{(1-x^{2n-1}) (1+x^{2n-2})} \\ &= \lim_{1}^{\infty} (1-x^{2n-1})^{3} (1-x^{2n-1})^{3} \cdot \frac{(1+x^{2n-1}) (1+x^{2n-2})}{(1-x^{2n-1}) (1+x^{2n-2})} \\ &= \lim_{1}^{\infty} (1-x^{2n-1})^{3} \cdot \frac{(1-x^{2n-1}) (1+x^{2n-2})}$$

Now,

$$= \left\{ \sum_{0}^{\infty} r_{3}(n) (-x)^{n} \right\} \cdot \prod_{1}^{\infty} \frac{1+x^{3n}}{1-x^{3n}}.$$

Hence,

$$\begin{split} \sum_{0}^{\infty} r_{3}(n) (-x)^{n} &= \prod_{1}^{\infty} \frac{1 - x^{3n}}{1 + x^{3n}} \Big\{ 1 + 6 \sum_{1}^{\infty} [\delta_{2}(n) - \delta_{1}(n)] x^{n} \Big\} \\ &= \Big\{ 1 + 2 \sum_{1}^{\infty} (-x^{3})^{n^{2}} \Big\} \Big\{ 1 + 6 \sum_{1}^{\infty} [\delta_{2}(n) - \delta_{1}(n)] x^{n} \Big\}. \end{split}$$

Now, letting $x \rightarrow -x$, we have

$$\sum_{0}^{\infty} r_{3}(n)x^{n} = 1 + 2\sum_{m=1}^{\infty} x^{3m^{2}} + 6\sum_{n=1}^{\infty} (-1)^{n} [\delta_{2}(n) - \delta_{1}(n)]x^{n}$$
$$+ 12\sum_{n=1}^{\infty} (-1)^{n} x^{n} \sum_{i=1}^{n} (-1)^{i} [\delta_{2}(n - 3i^{2}) - \delta_{1}(n - 3i^{2})]$$

[Here we adopt the convention that $\delta_i(k) = 0$ whenever k < 0, i = 1, 2.] Equating coefficients of like powers of x, we thus prove our theorem. [Note that $r_3(0) = 1$.]

CONCLUDING REMARKS

There is a somewhat complicated formula for $r_3(n)$ $[n \in \mathbb{Z}^+]$ due to Dirichlet. This is:

$$r_{3}(n) = \frac{16}{\pi} n^{1/2} \chi_{2}(n) K(-4n) \cdot \prod_{p^{2} \mid n} \left(1 + \frac{1}{p} + \dots + \frac{1}{p^{\tau-1}} + \frac{1}{p^{\tau}} \left(1 - \left(\frac{p^{-2\tau} n}{p} \right) \frac{1}{p} \right)^{-1} \right),$$

where the definition of τ is $p^{2\tau} | n$, but $p^{2(\tau+1)} | n$,

$$K(-4n) = \sum_{m=1}^{\infty} \left(\frac{-4n}{m}\right) \frac{1}{m},$$

Here, and above, $\left(\frac{-4n}{m}\right)$ is a Jacobi symbol. And

[May

 $\chi_{2}(n) = \begin{cases} 0 & \text{if } 4^{-a}n \equiv 7 \pmod{8}, \\ 2^{-a}, & \text{if } 4^{-a}n \equiv 3 \pmod{8}, \\ 3 \cdot 2^{-1-a}, & \text{if } 4^{-a}n \equiv 1, 2, 5, 6 \pmod{8}, \end{cases}$

and here the definition of a is $4^{a} | n$, but $4^{a+1} \nmid n$. This formula (among others) is given by Hua [2, pp. 215-216]. First of all, it is far from obvious that this expression for $r_{3}(n)$ is an integer, whereas our expressions of Theorem 1 are clearly integral. However, Dirichlet's formula permits an easy proof of the fact: $r_{3}(n) > 0$, if and only if, n is not of the form $4^{a}(8m + 7)$. At the moment, the author has not seen a way of deducing this fact from Theorem 1.

REFERENCES

- 1. L. Carlitz & M. V. Subbarao. "A Simple Proof of the Quintuple-Product Identity." Proc. Amer. Math. Soc. 32 (1972):42-44.
- 2. Loo-Keng Hua. Introduction to Number Theory. New York: Springer-Verlag, 1982.

BERNOULLI NUMBERS AND KUMMER'S CRITERION

HARLAN R. STEVENS*

The Pennsylvania State University, University Park, PA 16802 (Submitted April 1984)

1. INTRODUCTION

There is a large literature concerning various properties of the Bernoulli numbers; see, for example, [1, 12, 16, 23] and their references. According to H. S. Vandiver [23], by 1960 over 1500 papers had been written on the subject. The main thrust of the present paper is to consider several congruence properties of the Bernoulli numbers that extend various results of Vandiver, Nielson, Carlitz, and Stevens; see [2, 16, 19, 22]. The Bernoulli numbers B_n $(n \ge 0)$ are defined by the expansion

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!} ,$$

which is equivalent to

$$\sum_{r=0}^{n} \binom{n}{r} B_r = B_n \qquad (n > 1)$$
(1.1)

together with $B_0 = 1$. It is sometimes convenient to write (1.1) in the form

$$(B+1)^n = B^n \qquad (n > 1) \tag{1.2}$$

where it is understood that, after expansion of the left-hand side, we replace B^{k} by B_{k} . It is easy to check that for the first few values of n we have

$$B_1 = -1/2$$
, $B_2 = 1/6$, $B_{\mu} = -1/30$,

and that in general $B_{2k+1} = 0$ if $k \ge 1$.

Bernoulli numbers have numerous interesting properties. For example, if $S_n(k) = 1^n + \cdots + k^n$, then $S_n(k) = (B_{n+1}(k+1) - B_{n+1})/(n+1)$, where $B_n(x) = (B+x)^n$. The Bernoulli numbers are related to class numbers and to Fermat's Last Theorem. Moreover, they satisfy numerous recurrences and congruences. For further details regarding various properties of the Bernoulli numbers, the reader should consult the papers [1, 12, 16, 23] and their references.

2. CONGRUENCE PROPERTIES

If p is a prime, we now consider several congruence properties of sequences of rational numbers where we say that a/b is integral modulo p if (b, p) = 1.

[May

^{*}Professor Stevens passed away on December 3, 1983. Many of the results in this paper were presented by him to the departmental number theory seminar held on December 1, 1983. The paper, based on results obtained by Professor Stevens, has been written by several departmental colleagues.

Moreover, if a/b and c/d are integral modulo p, then

$$\frac{a}{b} \equiv \frac{c}{d} \pmod{p} \text{ if } ad \equiv bc \pmod{p}.$$

We assume throughout this paper that p is an odd prime even though similar results could be obtained for the case in which p = 2.

In [15] Kummer proved that

$$\frac{B_{n+1-p}}{n+p-1} \equiv \frac{B_n}{n} \pmod{p}$$

for all n > 1, where $(p - 1) \nmid n$. More generally, one can consider congruences of the form

$$\sum_{s=0}^{r} (-1)^{s} {r \choose s} \frac{B_{n+s(p-1)}}{n+s(p-1)} \equiv 0 \pmod{p^{r}}$$
(2.1)

for n > r, where $(p - 1) \nmid n$. In [15] Kummer studied congruences similar to the above but in a more general setting in which he proved the following theorem.

Theorem 1 (Kummer): Let a_n be integral modulo p and suppose

$$\sum_{n=0}^{\infty} a_n \frac{x^n}{n!} = \sum_{n=0}^{\infty} A_n (e^x - 1)^n.$$
(2.2)

If the A_n are integral modulo p, then

$$\sum_{s=0}^{r} (-1)^{s} {r \choose s} a_{n+s(p-1)} \equiv 0 \pmod{p^{r}}, \text{ for } n \ge r \ge 1.$$
(2.3)

Nielson showed in [16] that if $a_n = B_n$, the n^{th} Bernoulli number, then the Bernoulli numbers themselves satisfy (2.3) if $(p-1) \nmid n$, where the modulus is replaced by p^{r-1} . In attempting to remove the restriction $(p-1) \nmid n$, Vandiver [22] showed that if n = a(p-1) and $a_n = B_n$ then (2.3) holds modulo p^{r-1} provided that $r + a . This latter restriction is, however, a rather severe one. In [2] Carlitz showed that the congruence (2.3) holds if <math>r and that some much weaker congruences hold if <math>r \ge p - 1$.

Congruences similar to (2.3) were later studied in a series of papers by Carlitz and Stevens [5-9, 18-21]. Recently, a number of authors have taken renewed interest in the topic of congruences for various sequences of numbers. For example, Rota and Sagan [17], Gessel [13], J. Cowles [10], and J. Cowles, S. Chowla, and M. J. Cowles [11] have used various general combinatorial techniques, such as group actions on sets, to obtain various congruence properties for several sequences of numbers.

If one looks at Kummer's Criterion (2.2) and (2.3), it is easy to see that the condition is sufficient but not necessary. We will make use of the following theorem due to Carlitz [5].

Theorem 2 (Carlitz): Let a_n be integral modulo p and suppose

$$\sum_{n=0}^{\infty} a_n \frac{x^n}{n!} = \sum_{k=0}^{\infty} A_k \frac{(e^x - 1)^k}{k!}.$$

Then $A_k \equiv 0 \pmod{p^{\lfloor k/p \rfloor}}$ for all $k \ge 0$ if and only if

1986]

$$\sum_{s=0}^{r} (-1)^{s} \binom{r}{s} a_{n+s(p-1)} \equiv 0 \pmod{p^{r}}, \text{ for all } n \ge r \ge 1.$$

3. APPLICATIONS

In this section we apply Theorem 2 to the Bernoulli numbers to obtain several congruences that extend various results of Vandiver, Nielson, Carlitz, and Stevens, see [1, 16, 19, 22]. Finally, we use the theorem to obtain an elementary proof of the Staudt-Clausen theorem. Let us put

$$\frac{x}{e^{x}-1} = \sum_{n=0}^{\infty} B_{n} \frac{x^{n}}{n!} = \frac{\log(1+(e^{x}-1))}{e^{x}-1} = \sum_{n=0}^{\infty} (-1)^{n} \frac{n!}{n+1} \frac{(e^{x}-1)^{n}}{n!},$$

so that

$$A_n = \frac{\left(-1\right)^n n!}{n+1} \,.$$

Now however, the A_n 's do not satisfy the condition of the theorem. If we multiply by p, each coefficient in the new series does satisfy the condition, except for the coefficient of

$$\frac{(e^x - 1)^{p^2 - 1}}{(p^2 - 1)!}.$$

Thus, we have

$$\sum_{n=0}^{\infty} pB_n \frac{x^n}{n!} = \frac{(-1)^{p^2-1}}{p} (e^x - 1)^{p^2-1} + C(x),$$

where C(x) satisfies the condition of the theorem. Hence, if D is the derivative operator, then

$$(D^{p} - D)^{r} \sum_{n=0}^{\infty} pB_{n} \frac{x^{n}}{n!} \equiv (D^{p} - D)^{r} \frac{(-1)^{p^{2}-1}}{p} (e^{x} - 1)^{p^{2}-1} \pmod{p^{r}},$$

where we say that

$$\sum_{n=0}^{\infty} a_n \frac{x^n}{n!} \equiv \sum_{n=0}^{\infty} b_n \frac{x^n}{n!} \pmod{m}$$

if $a_n \equiv b_n \pmod{m}$ for each $n \ge 0$. We now consider $(D^p - D)^r (e^x - 1)^{p^2 - 1} \pmod{p^{r+1}}$. Since

$$(e^{x} - 1)^{p^{2}-1} = \sum_{j=0}^{p^{2}-1} (-1)^{p^{2}-1-j} {p^{2}-1 \choose j} e^{jx},$$

if we apply the operator $(D^{p} - D)^{r}$, we get after some simplification that, for each $n \ge 0$, the coefficient of $x^n/n!$ is

$$\sum_{j=0}^{p^2-1} (-1)^{p^2-1-j} {p^2-1 \choose j} (j^{p-1}-1)^r j^{n+r}.$$
(3.1)

[May

We now break the sum (3.1) into two sums Σ' and Σ'' , where in Σ' we sum over those j for which $p \nmid j$, while in Σ'' we sum over those j for which $p \mid j$. To compute Σ' , suppose that $j^{p-1} - 1 = pk(j)$, so that

$$\sum' = p^{r} \sum_{j=0}^{p^{r-1}} (-1)^{p^{2}-1-j} {p^{2}-1 \choose j} k(j)^{r} j^{n+r}.$$

We know that

$$\binom{p^2-1}{j} \equiv (-1)^j \pmod{p}.$$

If $j' \equiv j \pmod{p}$ so that j' = j + Qp, then $k(j') \equiv k(j) - j^{p-2}Q \pmod{p}$, and hence $r^2 - 1$

$$(*) \qquad \sum_{j=0}^{p^{r-1}} (-1)^{p^{2}-1} - j \binom{p^{2}-1}{j} (k(j))^{r} j^{n+r} \\ \equiv (-1)^{p^{2}-1} \sum_{j=1}^{p-1} \left[\sum_{Q=0}^{p-1} (k(j) - j^{p-2}Q)^{r} \right] j^{n+r} \pmod{p} \\ \equiv (-1)^{p^{2}-1} \sum_{j=1}^{p-1} j^{n+r} \sum_{Q=0}^{p-1} Q^{r} \pmod{p},$$

since the terms in the brackets run through a complete residue system modulo p. If $(p-1) \not\mid r$, then the inner sum is zero modulo p, while if $(p-1) \not\mid (n+r)$, then the outer sum is zero modulo p. If $(p-1) \mid r$ and $(p-1) \mid (n+r)$, then the left-hand side of (*) is congruent to $(-1)^{p^2-1}$ modulo p. Hence,

$$\Sigma' \equiv \begin{cases} 0 \pmod{p^{r+1}} & \text{if } (p-1) \not\mid r \\ 0 \pmod{p^{r+1}} & \text{if } (p-1) \not\mid (n+r) \\ (-1)^{p^2-1} \pmod{p^{r+1}} & \text{if } (p-1) \mid r \text{ and } (p-1) \mid (n+r). \end{cases}$$

Along similar lines, we may compute the sum Σ'' to obtain

$$\Sigma'' \equiv \begin{cases} 0 \pmod{p^{r+1}} & \text{if } (p-1) \nmid (n+r) \\ (-1)^{p^2+r} p^{n+r} \pmod{p^{r+1}} & \text{if } (p-1) \mid (n+r) \end{cases}$$

Therefore, combining the congruences obtained for Σ' and Σ'' , we see that pB_n is integral modulo p. Thus, we may apply Theorem 2 to the sequence $a_n = pB_n$ to obtain

Theorem 3: Let $N = \sum_{s=0}^{r} (-1)^{r-s} {r \choose s} B_{n+s(p-1)}$

(A) If $(p-1) \not\mid n$ where $n \ge r \ge 1$, then $N \equiv 0 \pmod{p^{r-1}}$.

(B) If (p-1)|n and (p-1)/r where $n > r \ge 1$, then $N \equiv 0 \pmod{p^{r-1}}$.

(C) If
$$(p-1)|n$$
 and $(p-1)|r$ where $n > r \ge 1$, then $N \equiv p^{r-2} \pmod{p^{r-1}}$.

(D) If
$$n = r$$
 and $(p - 1) | n$, then $N \equiv 0 \pmod{p^{r+1}}$.

We note that (A) is a result of Nielson [16], while the result in (B) improves upon results of Vandiver [22] and Carlitz [2].

1986]

BERNOULLI NUMBERS AND KUMMER'S CRITERION

We now obtain a generalization of these congruences. Since

$$\begin{aligned} x^{p^e} - y^{p^e} &= (x^{p^{e^{-1}}} - y^{p^{e^{-1}}}) (x^{(p-1)p^{e^{-1}}} + x^{(p-2)p^{e^{-1}}}y^{p^{e^{-1}}} \\ &+ x^{(p-3)p^{e^{-1}}}y^{2p^{e^{-1}}} + \cdots + y^{(p-1)p^{e^{-1}}}), \end{aligned}$$

by induction on *e* one can prove the following identity:

$$x^{p^{e^{-1}}} - y^{p^{e^{-1}}} = \sum_{i=0}^{e^{-1}} p^{i} (x - y)^{p^{e^{-1}-i}} f_{i}(x, y) \qquad (e \ge 1)$$
(3.2)

where each $f_i(x, y)$ is a polynomial in x and y. Let E be the difference operator, and suppose $b \ge 1$. Let $x = E^{b(p-1)}$ and y = 1 in (3.2) and then take the r^{th} power of both sides. We obtain

$$\sum_{s=0}^{r} (-1)^{r-s} {r \choose s} B_{n+sbp^{s-1}(p-1)} \equiv 0 \pmod{p^{A}}$$
(3.3)

where A is the minimum of

$$-1 + \sum_{i=1}^{e^{-1}} i\alpha + \sum_{i=0}^{e^{-1}} p^{e^{-1-i}}\alpha_i \text{ and } \alpha_0 + \cdots + \alpha_{e^{-1}} = r.$$

This minimum occurs when

 $\alpha_0 = \cdots = \alpha_{e-2} = 0$ and $\alpha_{e-1} = r$.

Hence, if $n \ge er$, then A = er - 1. We may now state

Theorem 4: Let $b \ge 1$, $e \ge 1$, and $M = \sum_{s=0}^{r} (-1)^{r-s} {r \choose s} B_{n+sbp^{e-1}(p-1)}$. (A) If $r \ge 1$, $n \ge er$, and either $(p-1) \nmid n$ or $(p-1) \nmid r$, then $M \equiv 0 \pmod{p^{er-1}}$.

(B) If n > er, (p - 1) | n, and (p - 1) | r, then $M \equiv 0 \pmod{p^{er-2}}$.

These results should be compared with Theorem 8 of Stevens [19].

We now apply Theorem 2 to obtain an elementary proof of

Theorem 5 (Staudt-Clausen): If $n \ge 1$, then

$$B_{2n} = G_{2n} - \sum_{(p-1)|2n} \frac{1}{p}$$

where G_{2n} is an integer.

Proof: It suffices to show that $pB_n \equiv -1 \pmod{p}$ if and only if (p-1)|n. We have

$$\sum_{k=0}^{\infty} pB_k \frac{x^k}{k!} = \sum_{k=0}^{\infty} (-1)^k \frac{p}{k+1} (e^x - 1)^k.$$

By induction on *n* in (1.1), it is easy to show that $pB_n \equiv 0 \pmod{p}$ if $0 \le n \le p - 2$, and hence from (1.1) we have that $pB_{p-1} \equiv -1 \pmod{p}$. If n = a(p - 1),

[May

then for r = 1 we have $pB_{a(p-1)} \equiv pB_{p-1} \pmod{p}$ so that $B_{a(p-1)} \equiv -1/p + Q$ where Q is integral modulo p. Similarly, $pB_n \equiv 0 \pmod{p}$ if $(p-1) \nmid n$. Thus p divides the denominator of B_n if and only if (p-1)|n.

REFERENCES

- "Bernoulli Numbers." The Fibonacci Quarterly 6 (1968):71-85. l. L. Carlitz.
- "Some Congruences for the Bernoulli Numbers." Amer. J. Math. 2. L. Carlitz. 75 (1953):163-172.
- 3. L. Carlitz. "Recurrences for the Bernoulli and Euler Numbers." J. Reine Ang. Math. 215 (1964):184-191.
- 4. L. Carlitz. "Recurrences for the Bernoulli and Euler Numbers." Math. Nach. 29 (1965):151-160.
- 5. L. Carlitz. "Criteria for Kummer's Congruences." Acta Arith. 6 (1961): 375-391.
- "A Note on Kummer's Congruences." Archiv der Math. 7 (1957): 6. L. Carlitz. 441-445.
- 7. L. Carlitz. "Kummer's Congruences (mod 2^r)." Monat. für Math. 63 (1959): 394-400.
- 8. L. Carlitz. "Composition of Sequences Satisfying Kummer's Criterion." Collectanea Math. 11 (1959):137-152.
- L. Carlitz & H. Stevens. "Criteria for Generalized Kummer's Congruences." J. Reine Ang. Math. 207 (1961):203-220.
- J. Cowles. "Some Congruence Properties of Three Well Known Sequences: Two Notes." J. Number Theory 12 (1980):84-86.
- J. Cowles, S. Chowla, & M. J. Cowles. "Congruence Properties for Apéry Numbers." J. Number Theory 12 (1980):188-190.
- 12. L. E. Dickson. History of the Theory of Numbers. II. New York: Chelsea, 1952.
- 13. I. M. Gessel. "Congruences for Bell and Tangent Numbers." The Fibonacci Quarterly 19 (1981):137-144.
- 14. A. Hurwitz. "Über die Entiwickelungscoefficienten der lemniscatischen Funktionen." Mathematische Werke 2 (1933):342-373.
- 15. E. E. Kummer. "Über eine allegemeine Eigenschaft der rational Entiwickelungscoefficienten einer bestimmten Gattung analytischer Funktionen." J. Reine Ang. Math. 41 (1851):368-372.
- 16. N. Nielson. Traite elementaire des nombres de Bernoulli. Paris, 1923.
- 17. G. C. Rota & B. Sagan. "Congruences Derived from Group Actions." Europ. J. Comb. 1 (1980):67-76.
- 18. H. Stevens. "Generalized Kummer Congruences for Products of Sequences." Duke Math. J. 28 (1961):25-38.
- 19. H. Stevens. "Generalized Kummer Congruences for Products of Sequences: Applications." Duke Math. J. 28 (1961):261-276. 20. H. Stevens. "Kummer Congruences for Products of Numbers." Math. Nach. 24
- (1962):219-227.
- 21. H. Stevens. "Kummer's Congruences of a Second Kind." Math. Zeitschr. 79 (1962):180-192.
- 22. H. S. Vandiver. "Certain Congruences Involving the Bernoulli Numbers." Duke Math. J. 5 (1939):548-551.
- 23. H. S. Vandiver. "On Developments in an Arithmetic Theory of Bernoulli and Allied Numbers." Scripta Math. 25 (1960):273-303.
- 24. H. S. Vandiver. "Fermat's Last Theorem." Amer. Math. Monthly 53 (1946): 555-578.

1986]

CALVIN T. LONG

Washington State University, Pullman, WA 99164 (Submitted November 1984)

1. INTRODUCTION

One of the more appealing aspects of the Fibonacci sequence, and certainly the most appealing to the uninitiated, is the very large number of remarkable identities that can be found. Discussing identities with Vern Hoggatt several years ago, I pointed out that it was easy to discover new identities simply by varying the pattern of known identities and using inductive reasoning to guess new results. With characteristic enthusiasm, Vern immediately picked up on the idea and suggested that an appropriate paper be written. Shortly after returning home, I received a letter from Vern which began: "There are a surprising number of good ways of expanding the list of identities. Consider" And the last sentence read: "At least some of this is sparkling new, and we are only using observation."

What follows is an account of some of the ideas we were sharing. They are not deep but, like Vern, I find them interesting. Of course, the ideas can be extended to more general recurrent sequences in obvious ways, but we restrict our attention here to the familiar Fibonacci and Lucas sequences defined by

$$F_i = \frac{\alpha^i - \beta^i}{\sqrt{5}} \quad \text{and} \quad L_i = \alpha^i + \beta^i, \tag{1}$$

where $\alpha = (1 + \sqrt{5})/2$, $\beta = (1 - \sqrt{5})/2$, and *i* is an integer.

2. THE GENERAL IDEA

The identities

$$\sum_{i=1}^{n} F_{i}^{2} = F_{n}F_{n+1}$$
(2)
$$\sum_{i=1}^{n} L_{i}^{2} = L_{n}L_{n+1} - 2$$
(3)

and

160

$$\sum_{i=1}^{n} L^{2} = \begin{cases} 5F_{n}F_{n+1} & n \text{ even,} \\ 5F_{n}F_{n+1} & -4 & n \text{ odd.} \end{cases}$$
(3')

How might these be generalized? Well, sums of squares might be viewed as sums of terms of the *second degree* in Fibonacci and Lucas numbers. Thus, one might consider other such sums like, for example,

 $\sum_{i=1}^{n} F_{i}F_{i+1}, \sum_{i=1}^{n} F_{i}F_{i+2}, \dots, \sum_{i=1}^{n} F_{i}F_{i+d}$

[May

and their Lucas counterparts or the mixed sums

 $\sum_{i=1}^{n} F_{i} L_{i+1}, \sum_{i=1}^{n} F_{i} L_{i+2}, \dots, \sum_{i=1}^{n} F_{i} L_{i+d}.$

One can now proceed formally, or with a little guessing, to obtain, for $d\ {\rm any}$ positive integer,

$$\sum_{i=1}^{n} F_{i}F_{i+d} = \begin{cases} F_{n}F_{n+d+1} & n \text{ even,} \\ F_{n}F_{n+d+1} - F_{d} & n \text{ odd,} \end{cases}$$
(4)

$$\sum_{i=1}^{n} L_{i}L_{i+d} = \begin{cases} 5F_{n}F_{n+d+1} & n \text{ even,} \\ \\ 5F_{n}F_{n+d+1} - L_{d+3} & n \text{ odd,} \end{cases}$$
(5)

$$\sum_{i=1}^{n} F_{i} L_{i+d} = \begin{cases} F_{n} L_{n+d+1} & n \text{ even,} \\ F_{n} F_{n+d+1} - L_{d} & n \text{ odd,} \end{cases}$$
(6)

$$\sum_{i=1}^{n} L_{i}F_{i+d} = \begin{cases} F_{n}L_{n+d+1} & n \text{ even,} \\ F_{n}L_{n+d+1} - F_{d+3} & n \text{ odd,} \end{cases}$$
(7)

which, as one would expect, exhibit a pleasing symmetry.

The proofs are straightforward utilizing Binet's formulas (1) and the known identities (see [1] and [10])

$$F_{r+2s} - F_r = \begin{cases} F_s L_{r+s} & s \text{ even,} \\ L_s F_{r+s} & s \text{ odd,} \end{cases}$$

$$\tag{8}$$

$$L_{r+2s} - L_r = \begin{cases} 5F_s F_{r+s} & s \text{ even,} \\ L_s L_{r+s} & s \text{ odd,} \end{cases}$$

$$\tag{9}$$

$$F_{r+2s} + F_r = \begin{cases} L_s F_{r+s} & s \text{ even,} \\ F_s L_{r+s} & s \text{ odd,} \end{cases}$$

$$(10)$$

$$L_{r+2s} + L_r = \begin{cases} L_s L_{r+s} & s \text{ even} \\ 5F_s F_{r+s} & s \text{ odd.} \end{cases}$$
(11)

As an example of the proofs of (4)-(7), we prove (4). Since $\alpha\beta = -1$, $1 - \alpha^2 = -\alpha$, and $1 - \beta^2 = -\beta$, we have

$$\sum_{i=1}^{n} F_{i}F_{i+d} = \sum_{i=1}^{n} \left(\frac{\alpha^{i} - \beta^{i}}{\sqrt{5}}\right) \left(\frac{\alpha^{i+d} - \beta^{i+d}}{\sqrt{5}}\right)$$

(continued)

1986]

$$= \frac{\alpha d (\alpha^2 - \alpha^{2n+2})}{5(1 - \alpha^2)} + \frac{\beta^d (\beta^2 - \beta^{2n+2})}{5(1 - \beta^2)} - \left(\frac{\alpha d + \beta d}{5}\right) \cdot \sum_{i=1}^n (-1)^i$$

= $\frac{1}{5} \left\{ \alpha d (\alpha^{2n+1} - \alpha) + \beta^d (\beta^{2n+1} - \beta) - L_d \cdot \sum_{i=1}^n (-1)^i \right\}$
= $\frac{1}{5} \left\{ \alpha^{2n+d+1} + \beta^{2n+d+1} - (\alpha^{d+1} + \beta^{d+1}) - L_d \cdot \sum_{i=1}^n (-1)^n \right\}.$

Therefore, for *n* even,

$$\sum_{i=1}^{n} F_{i}F_{i+d} = \frac{1}{5}(L_{2n+d+1} - L_{d+1}) = F_{n}F_{n+d+1}$$

by (9). For n odd, we have

$$\sum_{i=1}^{n} F_{i}F_{i+d} = \frac{1}{5}(L_{2n+d+1} - L_{d+1} + L_{d}) = \frac{1}{5}(L_{2n+d+1} - L_{d-1})$$
$$= \frac{1}{5}(L_{2n+d+1} + L_{d+1} - 5F_{d}) = F_{n}F_{n+d+1} - F_{d}$$

by (11), since $L_{d+1} = L_d + L_{d-1}$ and $L_{d-1} + L_{d+1} = 5F_d$ for all d. The other results are proved similarly.

3. THE IDENTITY
$$L_n^2 - 5F_n^2 = 4(-1)^n$$

As a second example, we consider the identity

$$L_n^2 - 5F_n^2 = 4(-1)^n$$
.

Again the terms on the left are of the second degree and we are led to consider expressions like

$$L_n^2 - 5F_{n+d}^2$$
, $L_nL_{n+d} - 5F_nF_{n+d}$, $L_nF_{n+d} - F_nL_{n+d}$, $L_nL_m - 5F_{n+d}F_{m+d}$,

and so on. As before, one can proceed either inductively or formally, or with a combination of both approaches, and it is a meta-theorem that we will not be disappointed. In fact, the following results can be exhibited. Let m, n, and d be integers. Then

$$L_{n}L_{m} - 5F_{n+d}F_{m+d} = \begin{cases} 5F_{-d}F_{m+n+d} + 2(-1)^{n}L_{m-n} & d \text{ even,} \\ L_{-d}L_{m+n+d} & d \text{ odd,} \end{cases}$$
(13)

$$L_{n}L_{m} - L_{n+d}L_{m+d} = \begin{cases} 5F_{-d} F_{m+n+d} & d \text{ even,} \\ \\ L_{-d} L_{m+n+d} + 2(-1)^{n}L_{m-n} & d \text{ odd,} \end{cases}$$
(14)

$$F_{n}F_{m} - F_{n+d}F_{m+d} = \begin{cases} F_{-d}F_{m+n+d} & d \text{ even,} \\ \frac{1}{5}(L_{-d}L_{m+n+d} - 2(-1)^{n}L_{m-n}) & d \text{ odd,} \end{cases}$$
(15)

[May

(12)

$$L_{n}F_{m} - L_{n+d}F_{m+d} = \begin{cases} F_{-d}L_{m+n+d} & d \text{ even,} \\ L_{-d}F_{m+n+d} - 2(-1)^{n}F_{m-n} & d \text{ odd,} \end{cases}$$
(16)

$$L_{n}F_{m} - L_{m+d}F_{n+d} = \begin{cases} F_{-d}L_{m+n+d} + 2(-1)^{n}F_{m-n} & d \text{ even,} \\ \\ L_{-d}F_{m+n+d} & d \text{ odd,} \end{cases}$$
(17)

$$L_n L_{m+d} - 5F_n F_{m+d} = 2(-1)^n L_{m-n+d}, \qquad (18)$$

$$L_n F_{m+d} - L_{m+d} F_n = 2(-1)^n F_{m-n+d}, \qquad (19)$$

$$L_n L_m - 5F_{n-d}F_{m+d} = (-1)^n L_{-d}L_{m-n+d}, \qquad (20)$$

$$L_n L_m - L_{n-d} L_{m+d} = 5(-1)^{n+1} F_{-d} F_{m-n+d},$$
⁽²¹⁾

$$F_n F_m - F_{n-d} F_{m+d} = (-1)^{n+1} F_{-d} F_{m-n+d}, \qquad (22)$$

$$L_n F_m - L_{n-d} F_{m+d} = (-1)^n F_{-d} L_{m-n+d},$$
(23)

$$F_n L_m - L_{n-d} F_{m+d} = (-1)^{n+1} L_{-d} F_{m-n+d}.$$
(24)

Moreover, these identities, or the known identities,

$$F_{m+n+1} = F_m F_n + F_{m+1} F_{n+1},$$
(25)

$$L_{m+n+1} = L_m F_n + L_{m+1} F_{n+1}, \tag{26}$$

and

$$5F_{m+n+1} = L_m L_n + L_{m+1} L_{n+1}, \tag{27}$$

suggest that we seek identities like (13)-(24) but with a plus sign on the left in place of the minus sign. Identities indeed exist and, somewhat surprisingly, are exactly the same as before but with the even and odd cases reversed. Thus, for example

$$F_{n}F_{m} + F_{n+d}F_{m+d} = \begin{cases} \frac{1}{5}(L_{-d}L_{n+m+d} - 2(-1)^{n}L_{m-n}) & d \text{ even,} \\ F_{-d}F_{n+m+d} & d \text{ odd.} \end{cases}$$
(28)

This should be compared with (15) above. Since this is the only change required, we refrain from listing the remaining counterparts to (13)-(24).

The proofs of (13)-(24) and their counterparts with the plus sign on the left-hand side all depend on Binet's formulas, identities (7)-(9) and equivalent identities obtained by replacing d by -d, and on the identities

$$F_{-n} = (-1)^{n-1} F_n \tag{29}$$

and

$$L_{-n} = (-1)^n L_n \tag{30}$$

for all n. As an example, we prove (14). We have

$$L_n L_m - L_{n+d} L_{m+d} = (\alpha^n + \beta^n) (\alpha^m + \beta^m) - (\alpha^{n+d} + \beta^{n+d}) (\alpha^{m+d} + \beta^{m+d})$$

(continued)

1986]

$$= \alpha^{m+n} + \beta^{m+n} + (\alpha\beta)^{n} (\alpha^{m-n} + \beta^{m-n})$$

- $\alpha^{m+n+2d} - \beta^{m+n+2d} - (\alpha\beta)^{n+d} (\alpha^{m-n} + \beta^{m-n})$
= $-(L_{m+n+2d} - L_{m+n}) + (-1)^{n} [1 - (-1)^{d}] L_{m-n}.$

Thus, using (9), (29), and (30), we have, for d even,

$$L_n L_m - L_{n+d} L_{m+d} = -5F_d F_{m+n+d} = 5F_{-d} F_{m+n+d}$$

and, for d odd,

$$L_n L_m - L_{n+d} L_{m+d} = -L_d L_{m+n+d} + 2(-1)^n L_{m-n} = L_{-d} L_{m+n+d} + 2(-1)^n L_{m-n}$$

as claimed.

and

4. HIGHER-ORDER IDENTITIES

Casting about for other identities to treat in the same way,

$$F_{n+3}^2 - 2F_{n+2}^2 - 2F_{n+1}^2 + F_n^2 = 0$$
(31)

$$F_{n+3}F_{n+4} - 2F_{n+2}F_{n+3} - 2F_{n+1-n+2} + F_nF_{n+1} = 0$$
(32)

were found in a paper by Hoggatt and Bicknell [6]. Note that (32) is already related to (31) in the manner of this paper, and one would expect such results as

$$L_{n+3}^{2} - 2L_{n+2}^{2} - 2L_{n+1}^{2} + L_{n}^{2} = 0,$$
(33)

$$F_{n+3}L_{n+3} - 2F_{n+2}L_{n+2} - 2F_{n+1}L_{n+1} + F_nL_n = 0,$$
(34)

$$F_{n+3}L_{m+3} - 2F_{n+2}L_{m+2} - 2F_{n+1}L_{m+1} + F_nL_m = 0,$$
(35)

and so on. Checking a bit further, I found that these and a good deal more are already known to hold. In [2], T. Brennan shows that

$$\sum_{r=0}^{n+1} (-1)^{r(r+1)/2} {n+1 \choose r} x^{n+1-r} = 0$$
(36)

where

$$\begin{bmatrix} n \\ r \end{bmatrix} = \frac{F_n F_{n-1} \cdots F_{n-r+1}}{F_r F_{r-1} \cdots F_1}, \quad \begin{bmatrix} n \\ 0 \end{bmatrix} = 1, \quad (37)$$

is the auxiliary equation for q_n , where q_n is the product of any n sequences satisfying the recurrence $\mu_{n+2} = \mu_{n+1} + \mu_n$.

For n = 2, (36) becomes

$$x^3 - 2x^2 - 2x + 1 = 0, (38)$$

which implies the truth of (33)-(35) and all other such generalizations. For n = 3, (36) becomes

$$x^4 - 3x^3 - 6x^2 + 3x + 1 = 0, (39)$$

164

[May

which implies such identities as

$$F_{n+4}^{3} - 3F_{n+3}^{3} - 6F_{n+2}^{3} + 3F_{n+1}^{3} + F_{n}^{3} = 0,$$

$$F_{n+4}F_{m+4}F_{p+4} - 3F_{n+3}F_{m+3}L_{p+3} - 6F_{n+2}F_{m+2}L_{p+2}$$
(40)

$$+ 3F_{n+1}F_{m+1}L_{p+1} + F_nF_mL_p = 0, (41)$$

and so on. Those interested in these and similar matters should also see [3], [5], [7], [8], [9], and [11].

As a final example, we consider the well-known and elegant identity

$$F_{3n} = F_{n+1}^3 + F_n^3 - F_{n-1}^3$$
(42)

(see [12], p. 11). In the spirit of this paper, there are three immediate generalizations, and one has only to consider a few examples to guess the following:

$$L_{3n} = L_{n+1}F_{n+1}^2 + L_nF_n^2 - L_{n-1}F_{n-1}^2,$$
(43)

$$5F_{3n} = F_{n+1}L_{n+1}^2 + F_nL_n^2 - F_{n-1}L_{n-1}^2,$$
(44)

and

$$5L_{3n} = L_{n+1}^3 + L_n^3 - L_{n-1}^3.$$
(45)

For completeness, we prove each of (42)-(45). They are not difficult, but are a bit subtle, and it is easy to take a wrong turn. We make repeated use of (25), (26), and (27), above.

To prove (42), we use (25), and write

$$\begin{aligned} &= F_{n-1+2n+1} \\ &= F_{n-1}F_{2n} + F_nF_{2n+1} \\ &= F_{n-1}F_{n-1+n+1} + F_nF_{n+n+1} \\ &= F_{n-1}(F_{n-1}F_n + F_nF_{n+1}) + F_n(F_n^2 + F_{n+1}^2) \\ &= F_{n-1}F_n(F_{n-1} + F_{n+1}) + F_n^3 + F_nF_{n+1}^2 \\ &= F_{n-1}(F_{n+1} - F_{n-1})(F_{n+1} + F_{n-1}) + F_n^3 + F_nF_{n+1}^2 \\ &= F_{n-1}F_{n+1}^2 - F_{n-1}^3 + F_n^3 + F_nF_{n+1}^2 \\ &= F_{n+1}^2(F_{n-1} + F_n) + F_n^3 - F_{n-1}^3 \end{aligned}$$

as claimed.

F

For (43), we use (26) and the formulas

$$F_{2n} = F_{n+1}^2 - F_{n-1}^2$$
 and $F_{2n+1} = F_n^2 + F_{n+1}^2$

from the proof of (42) to write

$$L_{3n} = L_{n-1+2n+1}$$

= $L_{n-1}F_{2n} + L_nF_{2n+1}$
= $L_{n-1}(F_{n+1}^2 - F_{n-1}^2) + L_n(F_n^2 + F_{n+1}^2)$
= $L_{n-1}F_{n+1}^2 - L_{n-1}F_{n-1}^2 + (L_nF_n^2 + L_nF_{n+1}^2)$

(continued)

1986]

$$= F_{n+1}^{2} (L_{n-1} + L_{n}) + L_{n}F_{n}^{2} - L_{n-1}F_{n-1}^{2}$$

= $L_{n+1}F_{n+1}^{2} + L_{n}F_{n}^{2} - L_{n-1}F_{n-1}^{2}$.

For (44), we use (27) and (26) to write

$$\begin{split} 5F_{3n} &= 5F_{n-1+2n+1} \\ &= L_{n-1}L_{2n} + L_nL_{2n+1} \\ &= L_{n-1}L_{n-1+n+1} + L_nL_{n+n+1} \\ &= L_{n-1}(L_{n-1}F_n + L_nF_{n+1}) + L_n(L_nF_n + L_{n+1}F_{n+1}) \\ &= L_{n-1}^2(F_n + L_{n-1}L_nF_{n+1} + L_n^2F_n + L_nL_{n+1}F_{n+1}) \\ &= L_{n-1}^2(F_{n+1} - F_{n-1}) + L_{n-1}L_nF_{n+1} + L_n^2F_n + L_n(L_{n-1} + L_n)F_{n+1} \\ &= F_{n+1}(L_{n-1}^2 + 2L_{n-1}L_n + L_n^2) + L_n^2F_n - L_{n-1}^2F_{n-1} \\ &= F_{n+1}(L_{n-1}^2 + F_nL_n^2 - F_{n-1}L_{n-1}^2). \end{split}$$

Finally, to obtain (45), we use (26) and (27) to write

 $5L_{3n} = 5L_{n-1+2n+1}$ $= 5(L_{n-1}F_{2n} + L_nF_{2n+1})$ = $L_{n-1} \cdot 5F_{n-1+n+1} + L_n \cdot 5F_{n+n+1}$ $= L_{n-1}(L_{n-1}L_n + L_nL_{n+1}) + L_n(L_n^2 + L_{n+1}^2)$ $= L_{n-1}^{2} (L_{n+1} - L_{n-1}) + L_{n-1} L_{n} L_{n+1} + L_{n}^{3} + L_{n} L_{n+1}^{2}$ $= L_{n-1}^{2}L_{n+1} - L_{n-1}^{3} + L_{n-1}L_{n}L_{n+1} + L_{n}^{3} + (L_{n+1} - L_{n-1})L_{n+1}^{2}$ $= L_{n+1}^{3} + L_{n}^{3} - L_{n-1}^{3} + L_{n-1}L_{n+1}(L_{n-1} + L_{n} - L_{n+1})$ $= L_{n+1}^{3} + L_{n}^{3} - L_{n-1}^{3}$

as claimed.

REFERENCES

- 1. G.E. Bergum & V.E. Hoggatt, Jr. "Sums and Products of Recurring Sequences." The Fibonacci Quarterly 13 (1975):115-120.
- T. A. Brennan. "Fibonacci Powers and Pascal's Triangle in a Matrix." The 2. Fibonacci Quarterly 2 (1964):93-103, 177-184.
- 3. L. Carlitz. "The Characteristic Polynomial of a Certain Matrix of Binomial Coefficients." The Fibonacci Quarterly 3 (1965):81-94.
- V. E. Hoggatt, Jr. Fibonacci and Lucas Numbers. Boston: Houghton-Mifflin, 1969; rpt. The Fibonacci Association, 1980.
- 5. V. E. Hoggatt, Jr. "Fibonacci Numbers and Generalized Binomial Coefficients." The Fibonacci Quarterly 5 (1967):383-400.
- 6. V. E. Hoggatt, Jr., & M. Bicknell. "Some New Fibonacci Identities." The Fibonacci Quarterly 2 (1964):29-32.
- V. E. Hoggatt, Jr., & M. Bicknell. "Fourth Power Fibonacci Identities from Pascal's Triangle." *The Fibonacci Quarterly* 2 (1964):261-266.
 V. E. Hoggatt, Jr., & A. P. Hillman. "The Characteristic Polynomial of the
- Generalized Shift Matrix." The Fibonacci Quarterly 3 (1965):91-94.

[May
DISCOVERING FIBONACCI IDENTITIES

- 9. D. Jarden. Recurring Sequences. 2nd ed. Jerusalem, Israel: Riveon Lematika, 1966, pp. 30-33. 10. C. T. Long. "On a Fibonacci Arithmetic Trick." The Fibonacci Quarterly 23
- (1985):221-231.
- 11. R. F. Torretto & J. A. Fuchs. "Generalized Binomial Coefficients." The Fibonacci Quarterly 2 (1964):296-302.
- 12. N. N. Vorob'ev. Fibonacci Numbers. New York: Blaisdell, 1961.

The book FIBONACCI NUMBERS AND THEIR APPLICATIONS containing the papers presented at the First international Conference on Applications of The Fibonacci Numbers held in Patras, Greece, can be purchased for \$44.50 (a 25% discount).

All orders should be prepaid by Cheque, credit card, or international money order. Order from:

> KLUWER ACADEMIC PUBLISHERS 190 OLD DERBY STREET HINGHAM, MA 02043 U.S.A.

if you reside in North America or Canada. Residents of all other countries should order from:

> KLUWER ACADEMIC PUBLISHERS GROUP DISTRIBUTION CENTRE P.O. BOX 322 3300 AH DORDRECHT THE NETHERLANDS

+topological interaction in

EXPLICIT FORMULAS FOR NUMBERS OF RAMANUJAN

F. T. HOWARD

Wake Forest University, Winston-Salem, NC 27109 (Submitted August 1984)

1. INTRODUCTION

In Chapter 3 of his second notebook [1, p. 165], Ramanujan defined numbers a(n, k) such that a(2, 0) = 1 and for $n \ge 2$,

$$a(n + 1, k) = (n - 1)a(n, k - 1) + (2n - 1 - k)a(n, k).$$
(1.1)

He defined a(n, k) = 0 when k < 0 or k > n - 2. The numbers were used in the following way: Fix a > 1/e and for real h define x > 0 by the relation

 $x^x = a^a e^h$.

Then it can be shown [1, pp. 164-165] that

$$\frac{x-a}{a}=\sum_{n=1}^{\infty}\left(-1\right)^{n-1}\frac{A_n}{n!}\left(\frac{h}{a}\right)^n,$$

where |h| is sufficiently small, $A_1 = (1 + \log \alpha)^{-1}$,

$$A_n = \sum_{k=0}^{n-2} a(n, k) (1 + \log a)^{1+k-2n}, \quad n \ge 2.$$

The values of a(n, k) for $2 \le n \le 7$ are given in the following table.

n k	0	1	2	3	4	5
2 3	1 3	1				
4	15	10	2			
5	105	105	40	6		
6	945	1260	700	196	24	
7	10395	17325	12600	5068	1148	120

Table 1

The purpose of this paper is to show how $\alpha(n, k)$ can be expressed in terms of Stirling numbers of the first kind and associated Stirling numbers of the second kind. We prove in §2 that

$$a(n, n-2) = (n-2)! = (-1)^n s(n-1, 1),$$

$$a(n, n-3) = (-1)^n (n-2) s(n-1, 1) + (-1)^{n-1} 2 s(n-1, 2),$$

and in general, for $k \ge 2$,

[May

EXPLICIT FORMULAS FOR NUMBERS OF RAMANUJAN

$$a(n, n - k) = \sum_{t=1}^{k-1} (-1)^{n-1-t} P_{k,t}(n) s(n - 1, t),$$

where $P_{k,t}(n)$ is a polynomial in n of degree k - 1 - t and s(n - 1, t) is the Stirling number of the first kind. A recurrence formula for the coefficients of $P_{k,t}(n)$ is derived and the values of $P_{k,t}(n)$ for $2 \le k \le 6$ are computed (see Table 2). In §3 we show that

$$a(n, 0) = b(2n - 2, n - 1), a(n, 1) = b(2n - 3, n - 2),$$

and, for k > 1,

$$a(n, k) = \sum_{r=3}^{n-k+1} Q_k(n, r) \frac{(2n-k-3)!!}{(2r-3)!!} (r-1)b(2r-3, r-2),$$

where the $Q_k(n, r)$ are rational numbers,

$$n!! = \begin{cases} 1.3 \cdots n & \text{if } n \text{ is odd,} \\ 2.4 \cdots n & \text{if } n \text{ is even,} \end{cases}$$
(1.2)

and b(n, k) is the associated Stirling number of the second kind. A recurrence formula for $Q_k(n, r)$ is worked out and the values of $Q_k(n, r)$ for k = 2 and k = 3 are given. In §4 we prove an identity for the Stirling numbers of the first kind. This identity, interesting in its own right, is used in the proof of Theorem 2.1.

2. STIRLING NUMBERS OF THE FIRST KIND

Throughout the paper we use the notation

$$(x)_n = x(x - 1) \cdots (x - n + 1).$$

The Stirling number of the first kind, s(n, k), can be defined by means of

$$(x)_{n} = \sum_{k=0}^{n} s(n, k) x^{k}.$$
 (2.1)

These numbers are well known and have been extensively studied; a table of values for $1 \le n \le 15$ can be found in [2, p. 310]. In particular,

$$s(n, 1) = (-1)^{n-1}(n-1)!.$$

By (1.1) and the fact that $\alpha(n, k) = 0$ for k > n - 2, we have

$$a(n, n-2) = (n-2)a(n-1, n-3) = (n-2)!a(2, 0) = (n-2)!,$$

and therefore

$$a(n, n-2) = (-1)^n s(n-1, 1).$$

Theorem 2.1: For $k \ge 2$,

$$\alpha(n, n - k) = \sum_{t=1}^{k-1} P_{k, t}(n) (-1)^{n-1-t} s(n - 1, t),$$

1986]

where $P_{k,t}(n)$ is a polynomial in n of degree k - 1 - t. The coefficient of n^{k-1-t} is t!/(k - t - 1)!. If we write

$$P_{k,t}(n) = \sum_{j=0}^{k-1-t} c_k(t, j) (n-1)_j = \sum_{j=0}^{k-1-t} d_k(t, j) (n-2)_j,$$

then, for k > 2, $d_k(1, 0) = 0$, $d_k(t, 0) = (k - 1)c_{k-1}(t - 1, 0)$ for t > 1, and

$$d_{k}(t, j) = \sum_{m=t}^{k-1-j} (-1)^{m-t} \left(\frac{1}{j}\right)^{m-t+1} (d_{k-1}(m, j-1) + (k-1)c_{k-1}(m, j))$$

for $t \ge 1$, j > 0.

Proof: We showed above that the theorem is true for a(n, n - 2); assume it is true for a(n, n - (k - 1)), so we can write

$$a(n, n - (k - 1)) = \sum_{m=1}^{k-2} P_{k-1,m}(n) (-1)^{n-1-m} s(n - 1, m), \qquad (2.2)$$

$$P_{k-1,m}(n) = \sum_{j=0}^{k-2-m} c_{k-1}(m, j) (n-1)_j = \sum_{j=0}^{k-2-m} d_{k-1}(m, j) (n-2)_j. \quad (2.3)$$

By (1.1), we have the recurrence

$$a(n, n-k) = (n-2)a(n-1, n-1-k) + (n-3+k)a(n-1, n-k).$$
(2.4)

We define the formal power series

$$A_{k}(x) = \sum_{n=k}^{\infty} a(n, n-k) \frac{x^{n-1}}{(n-2)!}$$

and sum on both sides of (2.4), after multiplying by $\frac{x^{n-1}}{(n-2)!}$, to obtain

$$A_k(x) = xA_k(x) + \sum_{n=k}^{\infty} (n-3+k)a(n-1, n-k)\frac{x^{n-1}}{(n-2)!}.$$

Therefore,

$$A_k(x) = \frac{1}{1-x} \sum_{n=k-1}^{\infty} (n-2+k)a(n, n-(k-1)) \frac{x^n}{(n-1)!}.$$
 (2.5)

Comparing coefficients of x^{n-1} in (2.5), we have

$$a(n, n-k) = \sum_{r=k-1}^{n-1} \frac{(n-2)!}{(r-2)!} a(r, r-(k-1)) + (k-1) \sum_{r=k-1}^{n-1} \frac{(n-2)!}{(r-1)!} a(r, r-(k-1)).$$
(2.6)

We now substitute into (2.6) the formula for $\alpha(r, r - (k - 1))$ given by (2.2) and (2.3). Then (2.6) becomes, after some manipulation,

[May

EXPLICIT FORMULAS FOR NUMBERS OF RAMANUJAN

$$a(n, n-k) = \sum_{m=1}^{k-2} \sum_{j=0}^{k-2-m} (-1)^{m-n} d_{k-1}(m, j) \sum_{r=j+1}^{n-2} \frac{(n-2)!(-1)^{n-r}}{(r-j-1)!} s(r, m) + (k-1) \sum_{m=1}^{k-2} \sum_{j=0}^{k-2-m} (-1)^{m-n} c_{k-1}(m, j) \sum_{r=j}^{n-2} \frac{(n-2)!(-1)^{n-r}}{(r-j)!} s(r, m).$$
(2.7)

At this point we need the following lemma, which we prove in §4.

Lemma 2.1: We have

$$\sum_{r=j}^{n} \frac{n! (-1)^{n-r}}{(r-j)!} s(r, m) = \begin{cases} -(n)_{j} \sum_{t=1}^{m} s(n+1, t) \left(\frac{1}{j}\right)^{m-t+1} & \text{if } j > 0, \\ s(n+1, m+1) & \text{if } j = 0. \end{cases}$$

We now substitute the formulas of Lemma 2.1 (with n replaced by n-2 and j replaced by j+1) into (2.7) and change the order of the m, t summations. We have

$$a(n, n - k) = \sum_{t=1}^{k-2} \sum_{j=0}^{k-1-t} d_k(t, j) (n - 2)_j (-1)^{n-1-t} s(n - 1, t) + d_k(k - 1, 0) (-1)^{n-k} s(n - 1, k - 1) = \sum_{t=1}^{k-1} P_{k, t}(n) (-1)^{n-1-t} s(n - 1, t)$$

where $d_k(1, 0) = 0$, $d_k(t, 0) = (k - 1)c_{k-1}(t - 1, 0)$ for t > 1 and

$$d_{k}(t, j) = \sum_{m=t}^{k-1-j} (-1)^{m-t} \left(\frac{1}{j}\right)^{m-t+1} (d_{k-1}(m, j-1) + (k-1)c_{k-1}(m, j))$$

for $t \ge 1, \ j > 0$. It follows that $P_{k, \ t}(n)$ has degree k - 1 - t and the coefficient of n^{k-1-t} is

$$d_{k}(t, k - 1 - t) = \frac{1}{k - 1 - t} d_{k - 1}(t, k - 2 - t)$$
$$= \frac{1}{(k - 1 - t)!} d_{t + 1}(t, 0).$$

Since

$$\begin{split} P_{k,\,k-1}(n) &= d_k(k-1,\,0) = (k-1)c_{k-1}(k-2,\,0) \\ &= (k-1)d_{k-1}(k-2,\,0) = (k-1)!, \end{split}$$

the coefficient of n^{k-1-t} in $P_{k,t}(n)$ is $\frac{t!}{(k-1-t)!}$. This completes the proof of Theorem 2.1.

From Theorem 2.1, we have the following special cases:

$$c_{k}(t, j) = 0 = d_{k}(t, j) \text{ if } j > k - 1 - t,$$

$$c_{k}(k - 2, 1) = d_{k}(k - 2, 1) = (k - 2)!$$

$$c_{k}(k - 2, 0) = (k - 1)! + (-1)^{k - 1}s(k, 2),$$

$$d_{k}(k - 2, 0) = k(k - 2)! + (-1)^{k - 1}s(k, 2),$$

1986]

EXPLICIT FORMULAS FOR NUMBERS OF RAMANUJAN

$$c_k(t, k - 2 - t) = [t!(k - 2) + (-1)^t(t + 1)s(t + 1, 2)]/(k - 2 - t)!,$$

$$d_k(t, k - 2 - t) = [t!(k - 1) + (-1)^t(t + 1)s(t + 1, 2)]/(k - 2 - t)!.$$

It follows that

$$P_{k,k-2}(n) = (k-2)!n + (k-2)(k-2)! + (-1)^{k-1}s(k, 2).$$
(2.8)

We have already pointed out that

$$P_{k, k-1}(n) = (k-1)!.$$
(2.9)

The evidence seems to indicate that

$$P_{k,1}(n) = \binom{n+k-5}{k-2},$$

.

but this has not been proved. Since $(n - 1)_j = (n - 2)_j + j(n - 2)_{j-1}$, we have the relationship:

$$d_k(t, j) = c_k(t, j) + (j + 1)c_k(t, j + 1).$$
(2.10)

Since

$$(n-2)_{j} = \sum_{r=0}^{j} (-1)^{j-r} j! (n-1)_{r} / r!,$$

we have

$$c_k(t, j) = (-1)^j \sum_{r=j}^{k-1-t} (-1)^r r! d_k(t, r) / j!.$$

Using (2.10) and (2.11), we can obviously write the recurrence for the coefficients $P_{k,t}(n)$ in several different ways.

The following values of $P_{k,t}(n)$ have been worked out using Theorem 2.1.

k^{t}	1	2	3	4	5
2	1				
3	n – 2	2			
4	$\binom{n-1}{2}$	2n - 7	6		
5	$\binom{n}{3}$	(n - 2)(n - 4)	6n - 32	24	
6	$\binom{n+1}{4}$	$2\binom{n-1}{3} - \binom{n-1}{2}$	$3n^2 - 29n + 61$	24n - 178	120

Table 2

3. ASSOCIATED STIRLING NUMBERS

The associated Stirling number of the second kind, b(n, k), can be defined by means of

$$(e^{x} - x - 1)^{k} = k! \sum_{n=2k}^{\infty} b(n, k) \frac{x^{n}}{n!}.$$

[May

(2.11)

We are using the notation of Riordan [3, pp. 74-78] for these numbers. They are also discussed in [2, pp. 221-222], where the notation $S_2(n, k)$ is used. A recurrence formula is

$$b(n + 1, k) = kb(n, k) + nb(n - 1, k - 1)$$
(3.1)

with b(0, 0) = 1 and b(n, k) = 0 if n < 2k. A table of values for b(n, k), $1 \le n \le 18$, is given in [2, p. 222]. It follows from (3.1) that

 $b(2n, n) = 1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n - 1) = (2n - 1)!!,$

with the notation of (1.2).

Also,

Since a(n, 0) = (2n - 3)a(n - 1, 0) = (2n - 3)!!, we have

$$a(n, 0) = b(2n - 2, n - 1), \quad n \ge 2. \tag{3.2}$$

$$b(2n-1, n-1) = (n-1)b(2n-2, n-1) + (2n-2)b(2n-3, n-2)$$

= (n-1)a(n, 0) + (2n-2)b(2n-3, n-2), (3.3)

with b(3, 1) = 1. Comparing (3.3) with (1.1), we have

$$a(n, 1) = b(2n - 3, n - 2), n \ge 3.$$
 (3.4)

Let $F_k(x)$ be the formal power series

$$\sum_{n=0}^{\infty} \frac{a(n+1, k)}{(2n-k-1)!!} x^{n}.$$

Then from (1.1) we have

$$F_k(x) = \frac{1}{1-x} \sum_{n=0}^{\infty} \frac{(n-1)a(n, k-1)}{(2n-k-1)!!} x^n.$$
(3.5)

Comparing coefficients of x^{n-1} in (3.5), we have

$$a(n, k) = \sum_{j=k+1}^{n-1} \frac{(2n-k-3)!!}{(2j-k-1)!!} (j-1)a(j, k-1).$$
(3.6)

It follows from (3.4) and (3.6) that

$$a(n, 2) = \sum_{r=3}^{n-1} \frac{(2n-5)!!}{(2r-3)!!} (r-1)b(2r-3, r-2).$$
(3.7)

Theorem 3.1: For $k \ge 2$,

$$\alpha(n, k) = \sum_{r=3}^{n-k+1} Q_k(n, r) \frac{(2n-k-3)!!}{(2r-3)!!} (r-1)b(2r-3, r-2),$$

where the $Q_k(n, r)$ are rational numbers such that $Q_2(n, r) = 1$ and

$$Q_{k}(n, r) = \sum_{m=r+k-2}^{n-1} \frac{(2m-k-2)!!}{(2m-k-1)!!} (m-1)Q_{k-1}(m, r)$$

for $3 \leq r \leq n - 1$ and $n \geq 4$.

173

1986]

Proof: According to (3.7), the Theorem is true for a(n, 2); assume it is true for a(n, k - 1). The proof for a(n, k) follows immediately when we substitute

$$a(j, k-1) = \sum_{r=3}^{j-k+2} Q_{k-1}(j, r) \frac{(2j-k-2)!!}{(2r-3)!!} (r-1)b(2r-3, r-2)$$

into (3.6) and change the order of the summations. This completes the proof.

It is not difficult to evaluate

$$Q_{3}(n, r) = \sum_{m=r+1}^{n-1} \frac{(2m-5)!!}{(2m-4)!!} (m-1)$$
$$= \frac{n(2n-5)}{3 \cdot 4^{n-3}} {2n-6 \choose n-3} - \frac{(r+1)(2r-3)}{3 \cdot 4^{r-2}} {2r-4 \choose r-2},$$

but apparently the formulas for $Q_k(n, r)$ for $k \ge 3$ are complicated.

4. PROOF OF LEMMA 2.1

The second equality in Lemma 2.1 is proved in [2, p. 215]. To the writer's knowledge, the first equality is new and is of interest in its own right. We shall make use of the generating function

$$(1 + t)^{u} = \sum_{n=0}^{\infty} \sum_{k=1}^{n} s(n, k) u^{k} \frac{t^{n}}{n!}, \qquad (4.1)$$

which follows from (2.1) and the MacLaurin series for $(1 + t)^{u}$. We have

$$t^{j}(u)_{j}(1+t)^{u-j} = \sum_{n=j}^{\infty} \sum_{k=1}^{n} s(n, k) u^{k} \frac{t^{n}}{(n-j)!}, \qquad (4.2)$$

 \mathbf{so}

$$t^{j}(u)_{j}\left(1+t\right)^{u-j-1} = \sum_{n=j}^{\infty} \sum_{r=j}^{n} \left(\sum_{k=1}^{r} \frac{(-1)^{n-r} s(r,k)u^{k}}{(r-j)!}\right) \frac{t^{n}}{n!}.$$
(4.3)

From (4.1) and the binomial theorem,

$$(1+t)^{u-j-1} = 1 + \sum_{n=1}^{\infty} \sum_{k=1}^{n} s(n, k) \sum_{r=0}^{k} {k \choose r} (-j-1)^{k-r} u^{r} \frac{t^{n}}{n!},$$

so

$$t^{j}(u)_{j}(1+t)^{u-j-1} = t^{j}(u)_{j} + \sum_{n=1}^{\infty} \sum_{k=1}^{n} s(n, k) \sum_{r=0}^{k} {k \choose r} (-j-1)^{k-r} \left(\sum_{m=1}^{j} s(j, m) u^{r+m} \right) \frac{t^{n+j}}{n!}.$$
 (4.4)

Comparing coefficients of $u^k t^n/n!$ in (4.3) and (4.4), we have

$$\sum_{r=j}^{n} \frac{(-1)^{n-r} s(r, k) n!}{(r-j)!} = (n)_{j} \sum_{m=1}^{j} s(j, m) \sum_{i=k-m}^{n-j} {i \choose k-m} (-j-1)^{i-k+m} s(n-j, i).$$
(4.5)

We now obtain the right-hand side of (4.5) in another way. We know

[May

EXPLICIT FORMULAS FOR NUMBERS OF RAMANUJAN

$$(n)_{j}(x)_{n+1} / (x - j)$$

$$= (n)_{j}(x)_{j}(x - j - 1)_{n-j}$$

$$= (n)_{j} \sum_{m=0}^{j} s(j, m) x^{m} \sum_{i=0}^{n-j} s(n - j, i) (x - j - 1)^{i}$$

$$= (n)_{j} \sum_{m=1}^{j} s(j, m) \sum_{i=0}^{n-j} s(n - j, i) \left(\sum_{w=0}^{i} {i \choose w} (-j - 1)^{i-w} \right) x^{w+m}.$$
(4.6)

The coefficient of x^k on the right side of (4.6) is

$$(n)_{j}\sum_{m=1}^{j} s(j, m) \sum_{i=k-m}^{n-j} {i \choose k-m} (-j-1)^{i-k+m} s(n-j, i),$$

which can be compared to the right side of (4.5). The left side of (4.6) can be written -(n)

$$(n)_{j}(x)_{n+1}/(x-j) = \frac{-(n)_{j}}{j} \frac{1}{1-\left(\frac{x}{j}\right)} \sum_{m=0}^{\infty} s(n+1, m)x^{m},$$

so the coefficient of x^k is

$$-(n)_{j}\sum_{m=1}^{k}s(n+1, m)\left(\frac{1}{j}\right)^{k-m+1}.$$
(4.7)

Comparing (4.7) and the left side of (4.5), we have the first equality of Lemma 2.1. This completes the proof.

REFERENCES

- 1. Bruce C. Berndt, Ronald J. Evans, & B. M. Wilson. "Chapter 3 of Ramanujan's Second Notebook." Advances in Mathematics 49 (1983):123-169.
- 2. L. Comtet. Advanced Combinatorics. Dordrecht: D. Reidel, 1974.
- 3. J. Riordan. An Introduction to Combinatorial Analysis. New York: Wiley, 1958.

1986]

SKEW CIRCULANTS AND THE THEORY OF NUMBERS: AN ADDENDUM

I. J. GOOD

Virginia Polytechnic Institute and State University, Blacksburg, VA 24061 (February 3, 1986)

While correcting the proofs of my article "Skew Circulants and the Theory of Numbers," my interest in the topic was revived, and I have now tracked down some relevant work by the great Jacobi. On pages 277 and 278 of his paper "Uber die complexen Primzahlen, welche in der Theorie der Reste 5^{ten}, 8^{ten} und 12^{ten} Potenzen zu Betrachten sind" (1839), which is in Volume VI of his collected papers, he shows that any prime of the form 8n + 1 can be factorized as $\phi(\alpha)\phi(\alpha^3)\phi(\alpha^5)\phi(\alpha^7)$, where $\alpha = \exp(2\pi i/8)$ and $\phi(\alpha)$ is of the form $y' + y''\alpha^2 + y''\alpha^2$ $z'\alpha + z''\alpha^3$, and this is equivalent to my first conjecture although Jacobi does not mention skew circulants. His proof depends on Gauss's theory of "biquadratic residues" and on work by Lagrange (presumably Lagrange's Oeuvres III, pp. 693-795). Jacobi's proof is too succinct for me to understand, and I think he may have been slightly careless. For example, he says (in free translation): "One can prove that any number a + ib that divides a number of the form $y^2 - iz^2$ is again of this form itself, and the proof is exactly like that of the analogous fact that any whole number that divides a number of the form $y^2 + z^2$ is itself a sum of two squares. (Without some gloss, this last statement is false; for example, 7 divides $49^2 + 196^2$. No doubt y and z are supposed to be mutually prime.) If his paper had been written by a much less eminent mathematician, I might have suspected that his claims were based in part on numerical evidence and not on complete proofs.

The basic idea in Jacobi's proof is to note that much of ordinary number theory can be generalized to the Gaussian integers a + ib.

Jacobi states that a similar method can be used to prove that every prime of the form 12n + 1 can be expressed as a product of four factors each related to a twelfth root of unity. (Also in the forms $a^2 + b^2$, $c^2 + 3d^2$, and $e^2 - 3f^2$.) This result cannot lead to an expression of 12n+1 as a skew circulant of order other than 2 because, for example, 13 and 37 are primes of the form 12n+1 but not of the form 8m+1. Jacobi mentions further that a prime of the form 5n+1can always be written in the form $a^2 - 5b^2$. The smallest prime that is of all three forms $5\ell+1$, 8m+1, and 12n+1 is 241 and is, therefore, presumably the smallest number that can be expressed in all six of the ways:

$$a^{2} + b^{2}$$
, $c^{2} + 2d^{2}$, $e^{2} + 3f^{2}$, $g^{2} - 2h^{2}$, $k^{2} - 3k^{2}$, and $p^{2} - 5q^{2}$

Indeed,

 $241 = 4^{2} + 15^{2}$ = $13^{2} + 2 \times 6^{2}$ = $7^{2} + 3 \times 8^{2}$ = $21^{2} - 2 \times 10^{2}$ = $17^{2} - 3 \times 4^{2}$ = $31^{2} - 5 \times 12^{2}$.

[May

SKEW CIRCULANTS AND THE THEORY OF NUMBERS: AN ADDENDUM

Any prime of the form 120n + 1 will, of course, have the six representations. Presumably (i) the expressions with positive signs are unique, and (ii) those with negative signs have an infinity of representations.

The main point of this addendum is, of course, that the first conjecture in my paper is equivalent to a result seemingly proved by Jacobi in 1839, although he did not express the result in terms of skew circulants.

I expect that anyone familiar with both Gauss's and Lagrange's work would be able to prove my second conjecture which specified all the integers expressible as skew circulants of order 4. Unfortunately, during the next several months, my other commitments will prevent me from achieving the requisite familiarity, fascinating though this study would undoubtedly be.

\$\$\$\$

ON FIBONACCI BINARY SEQUENCES

DEREK K. CHANG

California State University, Los Angeles, CA 90032 (Submitted July 1984)

A Fibonacci binary sequence of degree k is defined as a $\{0, 1\}$ -sequence such that no k + 1 1's are consecutive. For k = 1, we have ordinary Fibonacci sequences [2]. Let G(k, n) denote the number of Fibonacci binary sequences of degree k and length n. As was given in [2], it can be easily verified that for k = 1, we have $G(1, 1) = 2 = F_2$, $G(1, 2) = 3 = F_3$, and G(1, n) = G(1, n - 1) + $G(1, n - 2) = F_{n+1}$ for $n \ge 3$, where F_n is the nth Fibonacci number. In general, we have

$$G(k, n) = 2^n \qquad \text{for } 1 \le n \le k, \qquad (1a)$$

$$G(k, n) = \sum_{j=1}^{k+1} G(k, n-j) \quad \text{for } n \ge k+1.$$
 (1b)

Thus, for any $k \ge 1$, the sequence $\{F_{k,n} = G(k, n-1), n \ge 0\}$ is the k^{th} -order Fibonacci sequence, where we set G(k, -1) = G(k, 0) = 1 for convenience.

Let W(k, n) denote the total number of 1's in all binary sequences of degree k and length n. Then,

$$W(k, n) = n2^{n-1}$$
 for $0 \le n \le k$, (2a)

$$W(k, n) = \sum_{j=0}^{k} [W(k, n - j - 1) + jG(k, n - j - 1)] \text{ for } n \ge k + 1. \quad (2b)$$

The ratio q(k, n) = W(k, n)/nG(k, n) gives the proportion of 1's in all the binary sequences of degree k and length n. It was proved in [2] that the limit

$$q(k) = \lim_{n \to \infty} q(k, n),$$

which is the asymptotic proportion of 1's in Fibonacci binary sequences of degree k, exists for k = 1, and actually the limit is $q(1) = (5 - \sqrt{5})/10$. It is interesting to extend this result and solve the problem for all integers $k \ge 1$.

Let $\{A(n), n \ge -(k + 1)\}$ be a sequence of numbers with A(j) = 0 for $-(k + 1) \le j \le -1$. If we define a sequence

$$B(n) = A(n) - A(n-1) - \cdots - A(n-k-1) \text{ for } n \ge 0,$$

similar to the result in the case k = 1, we have the inverse relation

$$A(n) = \sum_{j=0}^{k} G(k, j-1)B(n-j) \text{ for } n \ge 0,$$
(3)

where the sequence $\{G(k, n), n \ge -1\}$ is defined above. From (2), we obtain

$$\sum_{m=0}^{k} mG(k, n-m-1) = W(k, n) - \sum_{j=0}^{k} W(k, n-j-1) \quad \text{for } n \ge k+1.$$

The inverse relation (3) then implies that

$$W(k, n) = \sum_{j=0}^{n} \left(G(k, j-1) \left[\sum_{m=0}^{k} mG(k, n-j-m-1) \right] \right) \text{ for } n \ge k+1, \quad (4)$$

178

[May

where we set G(k, n) = 0 for $n \leq -2$ for convenience.

The characteristic equation for the recursion (1) is

$$h(x) = x^{k+1} - x^k - \cdots - x - 1 = 0.$$
⁽⁵⁾

Let r_1, \ldots, r_{k+1} be its solution. We have the expression

$$G(k, n) = \sum_{j=1}^{k+1} c_j r_j^n, \text{ for } n \ge 0,$$
(6)

where c_j are constants [1]. It is known that (5) has exactly one solution, say r_1 , whose norm is not less than 1 [3]. Using Cramer's rule, we obtain an explicit form for c_1 from (6):

$$c_{1} = \frac{(2 - r_{2})(2 - r_{3}) \dots (2 - r_{k+1})(r_{2} - r_{3}) \dots (r_{k} - r_{k+1})}{(r_{1} - r_{2})(r_{1} - r_{3}) \dots (r_{1} - r_{k+1})(r_{2} - r_{3}) \dots (r_{k} - r_{k+1})}$$
$$= \frac{(2 - r_{2}) \dots (2 - r_{k+1})}{(r_{1} - r_{2}) \dots (r_{1} - r_{k+1})} = \frac{1}{(2 - r_{1})h'(r_{1})}.$$

From the equality (4), we get

$$W(k, n) = \sum_{j=0}^{n} \left[\left(\sum_{k=1}^{k+1} c_{k} r_{k}^{j-1} \right) \left(\sum_{m=1}^{k} m \left(\sum_{p=1}^{k+1} c_{p} r_{p}^{n-j-m-1} \right) \right) \right].$$

Since $|r_{\ell}| < 1$ for $2 \leq \ell \leq n+1$ and $G(k, n) = O(r_1')$, we have $\sum_{j=0}^{n} c_{\ell} r_{\ell}^{j-1} m c_p r_p^{n-j-m-1}$

$$= \begin{cases} mc_{\ell}c_{p}r_{\ell}^{-1}r_{p}^{m-1}(r_{p}^{n+1} - r_{\ell}^{n+1})(r_{p} - r_{\ell})^{-1} = o(nG(k, n)) \text{ for } r_{p} \neq r_{\ell} \\ nmc_{\ell}c_{p}r_{\ell}^{n-m-2} = o(nG(k, n)) \text{ for } r_{\ell} = r_{p} \neq r_{1}. \end{cases}$$

Thus,

$$q(k) = \lim_{n \to \infty} \frac{W(k, n)}{nG(k, n)} = \lim_{n \to \infty} \sum_{j=0}^{n} c_1 r_1^{j-1} \left(\sum_{m=1}^{k} m c_1 r_1^{n-j-m-1} \right) / n c_1 r_1^n$$
$$= c_1 \sum_{m=1}^{k} m r_1^{-m-2}.$$

We have established the rollowing result.

Theorem: Let r be the solution of (5) in the interval (1, 2). Then

$$q(k) = \left(\sum_{j=1}^{k} jr^{-j-2}\right) / \left[(2 - r) \left((k+1)r^{k} - \sum_{j=1}^{k} jr^{j-1} \right) \right].$$

Finally, three numerical examples are presented below.

For k = 2, r = 1.83929, q(2) = 0.38158. For k = 3, r = 1.92756, q(3) = 0.43366. For k = 4, r = 1.96595, q(4) = 0.46207.

REFERENCES

- 1. R. A. Brualdi. *Introductory Combinatorics*. New York: North-Holland, 1977. 2. P. H. St. John. "On the Asymptotic Proportions of Zeros and Ones in Fibo-
- nacci Sequences." The Fibonacci Quarterly 22 (1984):144-145.
 3. E. P. Miles, Jr. "Generalized Fibonacci Numbers and Associated Matrices."
- 3. E. P. Miles, Jr. "Generalized Fibonacci Numbers and Associated Matrices." Amer. Math. Monthly 67 (1960):745-752.

179

1986]

ELEMENTARY PROBLEMS AND SOLUTIONS

Edited by A. P. HILLMAN

Assistant Editors GLORIA C. PADILLA and CHARLES R. WALL

Please send all communications regarding ELEMENTARY PROBLEMS AND SOLUTIONS to 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

and

 $F_{n+2} = F_{n+1} + F_n, F_0 = 0, F_1 = 1$ $L_{n+2} = L_{n+1} + L_n, L_0 = 2, L_1 = 1.$

PROBLEMS PROPOSED IN THIS ISSUE

B-568 Proposed by Wray G. Brady, Slippery Rock University, Slippery Rock, PA

Find a simple curve passing through all of the points

 $(F_1, L_1), (F_3, L_3), \ldots, (F_{2n+1}, L_{2n+1}), \ldots$

8-569 Proposed by Wray G. Brady, Slippery Rock University, Slippery Rock, PA

Find a simple curve passing through all of the points

$$(F_0, L_0), (F_2, L_2), \ldots, (F_{2n}, L_{2n}), \ldots$$

8-570 Proposed by Herta T. Freitag, Roanoke, VA

Let a, b, and c be the positive square roots of F_{2n-1} , F_{2n+1} , and F_{2n+3} , respectively. For $n = 1, 2, \ldots$, show that

(a + b + c)(-a + b + c)(a - b + c)(a + b - c) = 4.

B-571 Proposed by Heinz-Jürgen Seiffert, Student, Berlin, Germany

Conjecture and prove a simple expression for

$$\sum_{r=0}^{\left[n/2\right]} \frac{n}{n-r} \binom{n-r}{r}$$

where [n/2] is the largest integer m with $2m \leq n$.

[May

<u>B-572</u> Proposed by Ambati Jaya Krishna, Student, Johns Hopkins University, Baltimore, MD, and Gomathi S. Rao, Orangeburg, SC

Evaluate the continued fraction:

$$1 + \frac{2}{3 + \frac{4}{5 + \frac{6}{7 + \cdots}}}$$

B-573 Proposed by Charles R. Wall, Trident Technical College, Charleston, SC

For all nonnegative integers n, prove that

$$\sum_{k=0}^{n} \binom{n}{k} L_{k} L_{n-k} = 4 + 5 \sum_{k=0}^{n} \binom{n}{k} F_{k} F_{n-k}.$$

SOLUTIONS

Congruence Modulo 12

B-544 Proposed by Herta T. Freitag, Roanoke, VA

Show that $F_{2n+1}^2 \equiv L_{2n+1}^2 \pmod{12}$ for all integers *n*.

Solution by Piero Filipponi, Fdn. U. Bordoni, Rome, Italy

First we rewrite the statement as

$$L_{2n+1}^2 - F_{2n+1}^2 \equiv 0 \pmod{12}, \qquad (1)$$

then using Hoggatt's I_{18} and I_{17} , we obtain

$$L_{2n+1}^2 - F_{2n+1}^2 = 4(F_{2n+1}^2 - 1) = 4(F_{2n+1} + 1)(F_{2n+1} - 1).$$

Since $F_{2n+1} \equiv \pm 1 \pmod{3}$, it is apparent that congruence (1) is satisfied for all integers n.

Also solved by Wray G. Brady, Paul S. Bruckman, L. A. G. Dresel, A. F. Horadam, L. Kuipers, Bob Prielipp, M. Robert Schumann, Heinz-Jürgen Seiffert, A. G. Shannon, Sahib Singh, Lawrence Somer, J. Suck, and the proposer.

Congruences Modulo 5

8-545 Proposed by Herta T. Freitag, Roanoke, VA

Show that there exist integers a, b, and c such that

 $F_{4n} \equiv an \pmod{5}$ and $F_{4n+2} \equiv bn + c \pmod{5}$

for all integers n.

Solution by Hans Kappus, Rodersdorf, Switzerland

We prove by induction that for n = 0, 1, 2, ...

1986]

ELEMENTARY PROBLEMS AND SOLUTIONS

$$F_{4n} \equiv 3n \pmod{5},$$

$$F_{4n+2} \equiv 2n + 1 \pmod{5}$$
.

This is obviously true for n = 0, 1, 2. Assume (1) and (2) hold for some $n \ge 2$. Then for this n,

$$F_{4n+1} \equiv F_{4n+2} - F_{4n} \equiv 4n + 1 \pmod{5},$$

 $F_{4n+3} \equiv 2F_{4n+2} - F_{4n} \equiv n+2 \pmod{5}$,

therefore 4n+3

$$F_{4(n+1)} \equiv 3F_{4n+2} - F_{4n} \equiv 3(n+1) \pmod{5},$$

hence (1) is true for all n. Furthermore,

$$F_{4(n+1)+2} \equiv 2F_{4(n+1)} + F_{4n+3} \equiv 2(n+1) + 1 \pmod{5}.$$

The proof is now finished.

Also solved by Wray G. Brady, Paul S. Bruckman, L.A.G. Dresel, A. F. Horadam, L. Kuipers, Bob Prielipp, Heinz-Jürgen Seiffert, A. G. Shannon, Sahib Singh, J. Suck, and the proposer.

Fibonacci Combinatorial Problem

<u>B-546</u> Proposed by Stuart Anderson, East Texas State University, Commerce, TX and John Corvin, Amoco Research, Tulsa, OK

For positive integers a, let S_a be the finite sequence a_1, a_2, \ldots, a_n defined by

 $a_1 = a$,

 $a_{i+1} = a_i/2$ if a_i is even, $a_{i+1} = 1 + a_i$ if a_i is odd,

the sequence terminates with the earliest term that equals 1.

For example, S_5 is the sequence 5, 6, 3, 4, 2, 1, of six terms. Let K_n be the number of positive integers a for which S_a consists of n terms. Does K_n equal something familiar?

Solution by Piero Filipponi, Fdn. U. Bordoni, Rome, Italy

It is evident that the only sequence of length 1 is S_1 , the only sequence of length 2 is S_2 , and the only sequence of length 3 is S_4 . That is, we have

$$k_1 = k_2 = k_2 = 1. (1)$$

Let us read the sequences in reverse order so that a is the n^{th} term of S_a . By definition, a sequence S_a^n (of length n) can generate exactly one(two) sequence(s) S_a^{n+1} of length n + 1, if a is odd(even). Denoting by $e(S_a^n)$ and $o(S_a^n)$ the number of sequences of length n ending with an even term and with an odd term, respectively, we can write

$$e(S_a^{n+1}) = k_n$$

 $o(S_a^{n+1}) = e(S_a^n) = k_{n-1},$

[May

182

(1)

from which we obtain

$$k_{n+1} = e(S_a^{n+1}) + o(S_a^{n+1}) = k_n + k_{n-1}.$$

From (1) and (2), it is readily seen that

 $k_n = F_{n-1}$, for n > 1.

Also solved by Paul S. Bruckman, L.A.G. Dresel, Ben Freed & Sahib Singh, Hans Kappus, L. Kuipers, Graham Lord, J. Suck, and the proposer.

Return Engagement

B-547 Proposed by Philip L. Mana, Albuquerque, NM

For positive integers p and n with p prime, prove that

 $L_{np} \equiv L_n L_p \pmod{p}$.

Solution by Sahib Singh, Clarion University of Pennsylvania, Clarion, PA

This result has been proved in B-182 (The Fibonacci Quarterly, 1970).

Also solved by Paul S. Bruckman, Odoardo Brugia & Piero Filipponi, L. A. G. Dresel, L. Kuipers, Bob Prielipp, Lawrence Somer, J. Suck, and the propower.

Number of Squares Needed

8-548 Proposed by Valentina Bakinova, Rondout Valley, NY

Let D(n) be defined inductively for nonnegative integers n by D(0) = 0 and $D(n) = 1 + D(n - [\sqrt{n}]^2)$, where [x] is the greatest integer in x. Let n_k be the smallest n with D(n) = k. Then

$$n_0 = 0$$
, $n_1 = 1$, $n_2 = 2$, $n_3 = 3$, and $n_4 = 7$.

Describe a recursive algorithm for obtaining n_k for $k \ge 3$.

Solution by L. A. G. Dresel, University of Reading, England

Let $[\sqrt{n}] = q$, so that $q^2 \le n \le (q+1)^2 - 1$, and let $R(n) = n - q^2$, so that we have $0 \le R(n) \le 2q$. Suppose now that n is the smallest integer for which R(n) = r, and consider the case where r is odd. Then we have r = 2q - 1 and

$$n = (q + 1)^{2} - 2 = \frac{1}{4}(r + 3)^{2} - 2.$$

By definition, we have

 $D(n_{k+1}) = k + 1$

 $D(n_{k+1}) = 1 + D(R(n_{k+1})),$

therefore

$$D(R(n_{k+1})) = k.$$

1986]

and

183

(2)

Since n_k is the smallest n for which D(n) = k, it follows that

 n_{k+1} is the smallest *n* for which $R(n) = n_k$.

Now taking the case where $n \equiv 3 \pmod{4}$, this leads to

$$n_{k+1} \equiv \frac{1}{4}(n_k + 3)^2 - 2$$

and we have also $n_{k+1} \equiv 3 \pmod{4}$. Hence, starting with $n_3 = 3$, we can use the above recursive algorithm for $k \ge 3$.

Also solved by Paul S. Bruckman, Hans Kappus, L. Kuipers, Jerry M. Metzger, Sahib Singh, and the proposer.

Generalized Fibonacci Numbers

B-549 Proposed by George N. Philippou, Nicosia, Cyprus

Let H_0 , H_1 , ... be defined by $H_0 = q - p$, $H_1 = p$, and $H_{n+2} = H_{n+1} + H_n$ for $n = 0, 1, \ldots$. Prove that, for $n \ge m \ge 0$,

$$H_{n+1}H_m - H_{m+1}H_n = (-1)^{m+1} [pH_{n-m+2} - qH_{n-m+1}].$$

Solution by L. A. G. Dresel, University of Reading, England

Define $D(n, m) = H_{n+1}H_m - H_{m+1}H_n$. Then

 $D(n, m) = H_m(H_n + H_{n-1}) - H_n(H_m + H_{m-1})$ = $H_m H_{n-1} - H_n H_{m-1} = -D(n - 1, m - 1).$

Repeating this reduction step a further m - 2 times, we obtain

$$D(n, m) = (-1)^{m-1}D(n - m + 1, 1)$$

= $(-1)^{m+1}(H_{n-m+2}H_1 - H_2H_{n-m+1})$
= $(-1)^{m+1}(pH_{n-m+2} - qH_{n-m+1}).$

Also solved by Paul S. Bruckman, Piero Filipponi, Herta T. Freitag, A. F. Horadam, L. Kuipers, Bob Prielipp, A. G. Shannon, P. D. Siafarikas, Sahib Singh, J. Suck, and the proposer.

ADVANCED PROBLEMS AND SOLUTIONS

Edited by RAYMOND E. WHITNEY

Please send all communications concerning ADVANCED PROBLEMS AND SOLUTIONS to RAYMOND E. WHITNEY, MATHEMATICS DEPARTMENT, LOCK HAVEN UNIVERSITY, LOCK HAVEN, PA 17745. This department especially welcomes problems believed to be new or extending old results. Proposers should submit solutions or other information that will assist the editor. To facilitate their consideration, all solutions should be submitted on separate signed sheets within two months after publication of the problems.

PROBLEMS PROPOSED IN THIS ISSUE

H-397 Proposed by Paul S. Bruckman, Fair Oaks, CA

For any positive integer n, define the function F_n on **C** as follows:

$$F_n(x) \equiv (g^n - 1)(x),$$
 (1)

where g is the operator

$$g(x) \equiv x^2 - 2. \tag{2}$$

(Thus, $F_3(x) = \{(x^2 - 2)\}^2 - 2\}^2 - 2 - x = x^8 - 8x^6 + 20x^4 - 16x^2 - x + 2\}$. Find all 2^n zeros of F_n .

H-398 Proposed by Ambati Jaya Krishna, Freshman, Johns Hopkins University

Let

$$a + b + c + d + e = \left(\sum_{1}^{\infty} \left(\frac{(-1)^{n+1}}{2n-1} \frac{2}{3} \cdot 9^{1-n} + 7^{1-2n}\right)\right)^2$$
$$a^2 + b^2 + c^2 + d^2 + e^2 = \frac{45}{512} \sum_{1}^{\infty} n^{-4},$$

and

a, b, c, d, $e \in \mathbb{R}$. What are the values of a, b, c, d, and e if e is to attain its maximum value?

H-399 Proposed by M. Wachtel, Zürich, Switzerland

The twin sequences:
$$\frac{L_{1+6n} - 1}{2} = 0$$
, 14, 260, 4674, 83880, ...

and

are representable by infinitely many identities, partitioned into several groups of similar structure:

 $\frac{L_{5+6n}-1}{2} = 5, 99, 1785, 32039, \dots$

1986]

ADVANCED PROBLEMS AND SOLUTIONS

	$\frac{L_{1+6n}-1}{2} = \text{identical to:}$	$\frac{L_{5+6n}-1}{2} = \text{identical to:}$
	Group I	
S_1	$3L_{-3+6n} + \frac{5F_{-5+6n} - 1}{2}$	$3L_{1+6n} + \frac{5F_{-1+6n} - 1}{2}$
S ₂	$61L_{-9+6n} + \frac{11L_{-14+6n} - 1}{2}$	$61L_{-5+6n} + \frac{11L_{-10+6n} - 1}{2}$
S ₃	$1103L_{-15+6n} + \frac{105F_{-23+6n} - 1}{2}$	$1103L_{-11+6n} + \frac{105F_{-19+6n} - 1}{2}$
S ₄	$19801L_{-21+6n} + \frac{199L_{-32+6n} - 1}{2}$	$19801L_{-17+6n} + \frac{199L_{-28+6n} - 1}{2}$
S_n	•••	

Groups II and III (in addition, there are more groups):

11.	S_1	$L_{-1+6n} + \frac{L_{-2+6n} - 1}{2}$	$L_{3+6n} + \frac{L_{2+6n} - 1}{2}$
	S ₂	$23L_{-7+6n} + \frac{15F_{-11+6n} - 1}{2}$	$23L_{-3+6n} + \frac{15F_{-7+6n} - 1}{2}$
	Sn		••••
		5 <i>v</i> + 1	57 + 1
111.	S_1	$2L_{-1+6n} - \frac{J_{-2+6n} + 1}{2}$	$2L_{3+6n} - \frac{5L_{2+6n} + 1}{2}$
111.	S ₁ S ₂	$2L_{-1+6n} - \frac{5L_{-2+6n} + 1}{2}$ $24L_{-7+6n} - \frac{7L_{-11+6n} + 1}{2}$	$2L_{3+6n} - \frac{5L_{2+6n} + 1}{2}$ $24L_{-3+6n} - \frac{7L_{-7+6n} + 1}{2}$

Find the construction rules for S_n for each group.

[May

;

SOLUTIONS

Sum Formula!

<u>H-373</u> Proposed by Andreas N. Philippou, University of Patras, Greece (Vol. 22, no. 3, August 1984)

For any fixed integers $k \ge 0$ and $r \ge 2$, set

$$f_{n+1,r}^{(k)} = \sum_{\substack{n_1, \dots, n_k \ni \\ n_1 + 2n_2 + \dots + n_k = n}} {n_1 + \dots + n_k + r - 1 \choose n_1 + \dots + n_k + r - 1}, \ n \ge 0.$$

Show that

$$f_{n+1,r}^{(k)} = \sum_{\ell=0}^{n} f_{\ell+1,1}^{(k)} f_{n+1-\ell,r-1}^{(k)}, \ n \ge 0.$$

Solution by C. Georghiou, University of Patras, Greece

Note that the definition of $f_{n+l,r}^{(k)}$ can be extended to include every positive real number r. Define also

$$f_{n+1}^{(k)} = \delta_{n,0}, \quad n \ge 0,$$

where $\delta_{n,m}$ is the Kronecker symbol. Then we show that

$$f_{n+1,r}^{(k)} = \sum_{\ell=0}^{n} f_{\ell+1,s}^{(k)} f_{n+\ell-1,r-s}^{(k)}, \quad n \ge 0, \qquad (*)$$

for any fixed positive integer k and any fixed nonnegative real number r.

We use generating functions. For fixed k and r, let $F_{k,r}(x)$ be the generating function of the sequence $\{f_{n+1,r}^{(k)}\}_{n=0}^{\infty}$. Then

$$F_{k,r}(x) = (1 - x - x^2 - \cdots - x^k)^{-r}.$$

Indeed, for some neighborhood of x = 0, we have

$$(1 - x - x^{2} - \dots - x^{k})^{-r} = \sum_{n=0}^{\infty} {\binom{-r}{n}} (-1)^{n} (x + x^{2} + \dots + x^{k})^{n}$$

$$= \sum_{n=0}^{\infty} {\binom{r+n-1}{n}} \sum_{n_{1}+n_{2}+\dots+n_{k}=n} {\binom{n_{1}+n_{2}+\dots+n_{k}}{n_{1}, n_{2}, \dots, n_{k}}} x^{n_{1}+2n_{2}+\dots+kn_{k}}$$

$$= \sum_{n=0}^{\infty} \sum_{n_{1}+n_{2}+\dots+n_{k}=n} {\binom{n_{1}+n_{2}+\dots+n_{k}+r-1}{n_{1}+n_{2}+\dots+n_{k}}} x^{n_{1}+2n_{2}+\dots+kn_{k}}$$

$$= \sum_{n=0}^{\infty} x^{n} \sum_{n_{1}+2n_{2}+\dots+kn_{k}=n} {\binom{n_{1}+n_{2}+\dots+n_{k}+r-1}{n_{1}, n_{2}, \dots, n_{k}}} x^{n_{1}+2n_{2}+\dots+kn_{k}}$$

(

1986]

ADVANCED PROBLEMS AND SOLUTIONS

Equation (*) follows from

$$F_{k,r}(x) = F_{k,s}(x)F_{k,r-s}(x).$$

Note also that the restriction for $r \ge 0$ can be relaxed to r any real number.

Also solved by P. Bruckman.

Bounds of Joy

H-374 Proposed by Charles R. Wall, Trident Technical College, Charleston, SC (Vol. 22, no. 3, August 1984)

If $\sigma^*(n)$ is the sum of the unitary divisors of n, then

$$\sigma^{*}(n) = \prod_{p^{e} \parallel n} (1 + p^{e}),$$

where p^e is the highest power of the prime p that divides n. The ratio $\sigma^*(n)/n$ increases as new primes are introduced as factors of n, but decreases as old prime factors appear more often. As N increases, is $\sigma^*(N!)/N!$ bounded or unbounded?

Solution by the proposer.

The primes between N/2 and N divide N! exactly once, and those not exceeding N/2 divide N! more than once. By considering special cases for $N \pmod{4}$, it is easy to show by telescoping products that

$$\prod_{N/2$$

if $N \ge 6$. Also

$$\prod_{\substack{p \in \|n\\ p \leq N/2}} (1 + p^{-e}) < \prod_{\substack{p \text{ prime}}} (1 + p^{-2}) = \prod_{\substack{p \ p \ p = 1}} (1 - p^{-4})/(1 - p^{-2}) = \zeta(2)/\zeta(4) = 15/\pi^2 < 1.52.$$

Therefore,

 $\sigma^*(N!)/N! < (1.52)(1.5) = 2.28$

if $N \ge 6$. The cases $1 \le N \le 5$ are easily checked, so $\sigma^*(N!)/N! < 2.28$ for all N. (Actually, the best bound is 2, achieved for N = 3.)

Also solved by P. Bruckman who remarked that $\sigma(N!)/N!$ is unbounded.

Conjectures No More

<u>H-375</u> Proposed by Piero Filipponi, Rome, Italy (Vol. 22, no. 3, August 1984)

Conjecture 1

If $F_k \equiv 0 \pmod{k}$ and $k \neq 5^n$, then $k \equiv 0 \pmod{12}$.

Conjecture 2

Let m > 1 be odd. Then, $F_{12m} \equiv 0 \pmod{12m}$ implies either 3 divides m or 5 divides m.

188

[May

Conjecture 3

Let p > 5 be a prime such that $p \nmid F_{2\mu}$, then $F_{1,2m} \notin 0 \pmod{12m}$.

Conjecture 4

If $L_k \equiv 0 \pmod{k}$, then $k \equiv 0 \pmod{6}$ for k > 1.

Solution by Lawrence Somer, Washington, D.C.

In answering the conjectures, we will make use of several definitions and known results. The rank of apparition of k in $\{F_n\}$, denoted by $\alpha(k)$, is the least positive integer m such that $k | F_m$. The prime p is a primitive divisor of F_n if $p | F_n$, but $p \nmid F_m$ for $1 \le m < n$. The following theorem will be the main result we will use and is given by D. Jarden as Theorem A in his paper "Divisibility of Fibonacci and Lucas Numbers by Their Subscripts" [2, pp. 68-75].

Theorem 1: Let $p_1,\,p_2,\,\ldots,\,p_n$ be the distinct primes dividing k, where k>1. Then $k\big|F_k$ if and only if

 $[a(p_1), a(p_2), \ldots, a(p_n)]|k,$

where $[a, b, \ldots]$ denotes the least common multiple of a, b, \ldots .

We will also need the following propositions.

Proposition 1: Let $m \ge 3$. Then $F_m | F_n$ if and only if m | n.

Proposition 2: Let

$$k = \prod_{i=1}^{m} p_i^{n_i}$$

be the canonical factorization of k into prime powers. Let r_i be the highest power of p_i dividing $F_{a(p_i)}$ for $1 \le i \le m$. Then

$$\alpha(k) = \operatorname{LCM}_{1 \leq i \leq m} \left\{ \alpha(p_i) p_i^{\max(0, n_i - r_i)} \right\}.$$

Proposition 3: If p is a prime and $p \neq 2$ or 5, then the prime factors of a(p) are less than p.

Proposition 4: If $n \neq 1$, 2, 6, or 12, then F_n has a primitive prime divisor.

Proposition 1 is well known. Propositions 2 and 3 are given by Jarden in [2, p. 68]. Proposition 4 is proved by Carmichael [1, p. 61].

Conjecture 1: FALSE. There is an infinite number of counterexamples. By Theorem F in Jarden's paper [2, p. 72], if $k|F_k$, then 12|k or 5|k. Thus, in any counterexample to Conjecture 1, 5 must divide k. Let $n \ge 2$. Let the divisors of 5^n that are unequal to 5 be denoted by p_1, p_2, \ldots, p_m . Since $F_5 = 5$, such prime divisors exist by Proposition 4. Let

$$k = 5^{r_n} \sum_{i=1}^{m} p_i^{t_i},$$
 (1)

1986]

where $r_n \ge n$ and at least one of the t_i 's ≥ 1 . It follows from Theorem 1 and Propositions 1, 2, and 4 that k is a counterexample to Conjecture 1. Clearly, there is an infinite number of such counterexamples. In particular, by a table of the factorizations of Fibonacci numbers given by Jarden [2, pp. 36-59], the only primitive prime divisor of F_{25} is 3001 and the only primitive prime divisor of F_{125} is 158414167964045700001. Then, by (1),

and

 $k_1 = 5^{r_1} 3001^{s_1}$

(2) (3)

(6)

 $k_2 = 5^{r_2} 3001^{s_2} 158414167964045700001^{t_2}$

are each counterexamples to Conjecture 1, where

$$r_1 \ge 2$$
, $s_1 \ge 1$, $r_2 \ge 3$, $s_2 \ge 0$, and $t_2 \ge 1$.

We now provide another infinite class of counterexamples to Conjecture 1. Suppose that k is a counterexample to Conjecture 1. Let q_1, q_2, \ldots, q_d be distinct primes such that $q_i \nmid k$ and q_i is a primitive divisor of F_{k_i} , where $1 \leq i \leq d$ and $k_i \mid k$. By Proposition 4, such q_i 's exist. Then, by Theorem 1,

$$k' = k \prod_{i=1}^{d} q_{i}^{n_{i}}$$
(4)

is also a counterexample to Conjecture 1, where at least one of the n_i 's ≥ 1 . One can show that all counterexamples to Conjecture 1 are of the forms given in (1) or (4). Since $k|F_k$, it follows by (4) and Propositions 1 and 4 that F_k is also a counterexample to Conjecture 1. Let F(n) denote F_n , $F(F(n)) = F^{(2)}(n)$ denote F_{F_n} and so on. Then by (2), (3), and Proposition 4,

$$F^{(r)}(5^{r_1}3001^{s_1}) \tag{5}$$

and

 $F^{(s)}(5^{r_2}3001^{s_2}158414167964045700001^{t_2})$

are each explicit counterexamples to Conjecture 1, where

$$r_1 \ge 2$$
, $r_2 \ge 2$, $s \ge 1$, $s_2 \ge 0$, $t_2 \ge 1$,

and either it is the case that $r \ge 2$ and $s_1 \ge 0$ or it is the case that $s_1 \ge 1$ and $r \ge 1$.

Conjecture 2: TRUE. Suppose that Conjecture 2 were false. Then m > 1 and all the prime factors of *m* are greater than 5. Let *p* be the smallest prime factor of *m*. By Theorem 1, a(p) | 12m. By Proposition 3, each prime factor of a(p) is less than *p*. It thus follows that a(p) is relatively prime to *m* and hence, a(p) | 12. However, $F_1 = F_2 = 1$ and the only prime divisors of F_3 , F_4 , F_6 , or F_{12} are 2 or 3. We thus have a contradiction and the result follows.

Conjecture 3: This does not make sense as stated.

Conjecture 4: TRUE, by Theorem F in Jarden's paper [2, p. 72]. Theorem F further states that if $L_k \equiv 0 \pmod{k}$, then $4 \nmid k$.

[May

References

- 1. R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$." Ann. Math. Second Series 15 (1913):30-70.
- D. Jarden. Recurring Sequences. 3rd ed. Jerusalem: Riveon Lematematika, 1973

Also solved by P. Bruckman and L. Dresel.

New Construction

H-376 Proposed by H. Klauser, Zürich, Switzerland (Vol. 22, no. 4, November 1984)

Let (a, b, c, d) be a quadruple of integers with the property that

 $(a^3 + b^3 + c^3 + d^3) = 0.$

Clearly, at least one integer must be negative.

Examples: (3, 4, 5, 6), (9, 10, -1, -12)

Find a construction rule so that:

out of two given quadruples a new quadruple arises;
 out of the given quadruple a new quadruple arises.

Solution by Paul Bruckman, Fair Oaks, CA

 $(a'')^3 + (b'')^3 + (c'')^3 + (d'')^3$

We let S denote the set of all quadruples $(a, b, c, d) \in \mathbb{Z}^4$ such that

$$a^3 + b^3 + c^3 + d^3 = 0. (1)$$

Lemma 1: Given $(a, b, c, d) \in S$, $(a', b', c', d') \in S$, let

$$p = a(a')^{2} + b(b')^{2} + c(c')^{2} + d(d')^{2},$$

$$q = a^{2}a' + b^{2}b' + c^{2}c' + d^{2}d'.$$
(2)

Also, let

$$a'' = pa - qa', b'' = pb - qb', c'' = pc - qc', d'' = pd - qd'.$$
 (3)

Then

$$(a'', b'', c'', d'') \in S.$$
 (4)

$$= p^{3}(a^{3} + b^{3} + c^{3} + d^{3}) - q^{3}\{(a')^{3} + (b')^{3} + (c')^{3} + (d')^{3}\}$$

$$- 3p^{2}q(a^{2}a' + b^{2}b' + c^{2}c' + d^{2}d')$$

$$+ 3pq^{2}\{a(a')^{2} + b(b')^{2} + c(c')^{2} + d(d')^{2}\}$$

$$= p^{3} \cdot 0 - q^{3} \cdot 0 - 3p^{2}q \cdot q + 3pq^{2} \cdot p = 0.$$

This shows that $(a'', b'', c'', d'') \in S$ given by (2) and (3) may be constructed from the given quadruples $(a, b, c, d) \in S$ and $(a', b', c', d') \in S$, solving

1986]

Part 1 of the problem.

Example: If (a, b, c, d) = (3, 4, 5, -6), (a', b', c', d') = (-1, 9, 10, -12), then p = -37, q = -47, (a'', b'', c'', d'') = (-158, 275, 285, -342).

Lemma 2: Given $(a, b, c, d) \in S$, let

$$r = ab^{2} + bc^{2} + cd^{2} + da^{2}, \ s = a^{2}b + b^{2}c + c^{2}d + d^{2}a.$$
 (5)

Also, let

A = rb - sc, B = rc - sd, C = rd - sa, D = ra - sb. (6) Then

$$(A, B, C, D) \in S. \tag{7}$$

Proof: $A^3 + B^3 + C^3 + D^3 = (r^3 - s^3)(a^3 + b^3 + c^3 + d^3)$

$$- 3r^{2}s(b^{2}c + c^{2}d + d^{2}a + a^{2}b) + 3rs^{2}(bc^{2} + cd^{2} + da^{2} + ab^{2}) = (r^{3} - s^{3}) \cdot 0 - 3r^{2}s \cdot s + 3rs^{2} \cdot r = 0.$$

Thus, $(A, B, C, D) \in S$ given by (5) and (6) may be constructed from the given quadruple $(a, b, c, d) \in S$, solving Part 2 of the problem.

Example: If (a, b, c, d) = (3, 4, 5, -6), then r = 274, s = 74, (A, B, C, D) = (726, 1814, -1866, 526).

Also solved by the proposer.

SUSTAINING MEMBERS

*A.L. Alder S. Ando *J. Arkin L. Bankoff F. Bell M. Berg J.G. Bergart G. Bergum G. Berzsenyi *M. Bicknell-Johnson C. Bridger *Br. A. Brousseau P.S. Bruckman M.F. Bryn P.F. Byrd G.D. Chakerian J.W. Creely M.J. DeLeon J. Desmond

H. Diehl T.H. Engel J.L. Ercolano D.R. Farmer F.F. Frey, Jr. C.L. Gardner AA. Gioia R.M. Giuli I.J. Good *H.W. Gould H.E. Heatherly A.P. Hillman *A.F. Horadam F.T. Howard R.J. Howell R.P. Kelisky C.H. Kimberling J.C. Lagarias J. Lahr *J. Maxwell

L. Miller M.G. Monzingo S.D. Moore, Jr. K. Nagasaka F.G. Ossiander A. Prince E.D. Robinson S.E. Schloth J.A. Schumaker J. Sjoberg L. Somer M.N.S. Swamy *D. Thoro R. Vogel M. Waddill *L.A. Walker J.E. Walton G. Weekly R.E. Whitney **B.E.** Williams

*Charter Members

INSTITUTIONAL MEMBERS

THE BAKER STORE EQUIPMENT COMPANY *Cleveland, Ohio*

BOSTON COLLEGE Chestnut Hill, Massachusetts BUCKNELL UNIVERSITY Lewisburg, Pennsylvania

CALIFORNIA STATE UNIVERSITY, SACRAMENTO Sacramento, California

FERNUNIVERSITAET HAGEN Hagen, West Germany

GENERAL BOOK BINDING COMPANY Chesterland, Ohio

NEW YORK PUBLIC LIBRARY GRAND CENTRAL STATION New York, New York PRINCETON UNIVERSITY Princeton, New Jersey SAN JOSE STATE UNIVERSITY San Jose, California SANTA CLARA UNIVERSITY Santa Clara, California SCIENTIFIC ENGINEERING INSTRUMENTS, INC. Sparks, Nevada TRI STATE UNIVERSITY Angola, Indiana UNIVERSITY OF CALIFORNIA, SANTA CRUZ Santa Cruz, California UNIVERSITY OF GEORGIA Athens, Georgia 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.

Recurring Sequences by Dov Jarden. Third and enlarged edition. Riveon Lematematika, Israel, 1973.

Tables of Fibonacci Entry Points, Part One. Edited and annotated by Brother Alfred Brousseau. FA, 1965.

Tables of Fibonacci Entry Points, Part Two. Edited and annotated by Brother Alfred Brousseau. FA, 1965.

A Collection of Manuscripts Related to the Fibonacci Sequence—18th Anniversary Volume. Edited by Verner E. Hoggatt, Jr. and Marjorie Bicknell-Johnson. FA, 1980.

Please write to the Fibonacci Association, Santa Clara University, Santa Clara, CA 95033, U.S.A., for current prices.