

# The Fibonacci Quarterly

THE OFFICIAL JOURNAL OF THE FIBONACCI ASSOCIATION

## TABLE OF CONTENTS

On the Uniqueness of Reduced Phi-Partitions .....	Corey Powell	194
Book Announcement: Fibonacci Entry Points and Periods for Primes 100,003 through 415,993 ..... A Monograph by Daniel C. Fielder and Paul S. Bruckman		199
On the Structure of Quadratic Irrationals Associated with Generalized Fibonacci and Lucas Numbers ... Edward B. Burger and Christopher S. Kollett		200
An Extension of Stirling Numbers .....	David Branson	213
Sixth International Conference Proceedings .....		223
The Asymptotic Behavior of the Golden Numbers .....	Helmut Prodinger	224
Digraphs from Powers Modulo $p$ .... Caroline Lucheta, Eli Miller and Clifford Reiter		226
Author and Title Index for Sale .....		239
Construction of Small Consecutive Niven Numbers .....	Brad Wilson	240
Sums of Powers of Integers via Generating Functions .....	F.T. Howard	244
A Fibonacci Model of Infectious Disease .....	F. Dubeau and A.G. Shannon	257
On the Fibonacci Numbers Whose Subscript Is a Power .....	Piero Filipponi	271
On the Diophantine Equation $(\frac{x(x-1)}{2})^2 = (\frac{y(y-1)}{2})$ .....	Ming Luo	277
Generalized Hockey Stick Identities and $N$ -Dimensional Blockwalking .....	Charles H. Jones	280

VOLUME 34

JUNE-JULY 1996

NUMBER 3

## PURPOSE

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

## EDITORIAL POLICY

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

## SUBMITTING AN ARTICLE

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

<http://www.sdstate.edu/~wcsc/http/fibhome.html>

Two copies of the manuscript should be submitted to: **GERALD E. BERGUM, EDITOR, THE FIBONACCI QUARTERLY, DEPARTMENT OF COMPUTER SCIENCE, SOUTH DAKOTA STATE UNIVERSITY, BOX 2201, BROOKINGS, SD 57007-1596.**

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

## SUBSCRIPTIONS, ADDRESS CHANGE, AND REPRINT INFORMATION

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

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

Annual domestic Fibonacci Association membership dues, which include a subscription to **THE FIBONACCI QUARTERLY**, are \$37 for Regular Membership, \$42 for Library, \$47 for Sustaining Membership, and \$74 for Institutional Membership; foreign rates, which are based on international mailing rates, are somewhat higher than domestic rates; please write for details. **THE FIBONACCI QUARTERLY** is published each February, May, August and November.

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

©1996 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)  
and Br. Alfred Brousseau (1907-1988)*

*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 57007-1596  
e-mail: Bergumg@mg.sdstate.edu

## **EDITORIAL BOARD**

DAVID M. BRESSOUD, Macalester College, St. Paul, MN 55105-1899  
JOHN BURKE, Gonzaga University, Spokane, WA 99258-0001  
LEONARD CARLITZ, Emeritus Editor, Duke University, Durham, NC 27708-0251  
BART GODDARD, East Texas State University, Commerce, TX 75429-3011  
HENRY W. GOULD, West Virginia University, Morgantown, WV 26506-0001  
HEIKO HARBORTH, Tech. Univ. Carolo Wilhelmina, Braunschweig, Germany  
A.F. HORADAM, University of New England, Armidale, N.S.W. 2351, Australia  
CLARK KIMBERLING, University of Evansville, Evansville, IN 47722-0001  
STEVE LIGH, Southeastern Louisiana University, Hammond, LA 70402  
RICHARD MOLLIN, University of Calgary, Calgary T2N 1N4, Alberta, Canada  
GARY L. MULLEN, The Pennsylvania State University, University Park, PA 16802-6401  
HAROLD G. NIEDERREITER, Institute for Info. Proc., A-1010, Vienna, Austria  
SAMIH OBAID, San Jose State University, San Jose, CA 95192-0103  
NEVILLE ROBBINS, San Francisco State University, San Francisco, CA 94132-1722  
DONALD W. ROBINSON, Brigham Young University, Provo, UT 84602-6539  
LAWRENCE SOMER, Catholic University of America, Washington, D.C. 20064-0001  
M.N.S. SWAMY, Concordia University, Montreal H3G 1M8, Quebec, Canada  
ROBERT F. TICHY, Technical University, Graz, Austria  
WILLIAM WEBB, Washington State University, Pullman, WA 99164-3113  
ANNE LUDINGTON YOUNG, Loyola College in Maryland, Baltimore, MD 21210-2699

## **BOARD OF DIRECTORS THE FIBONACCI ASSOCIATION**

CALVIN LONG (President)  
Northern Arizona University, Flagstaff, AZ 86011-5717  
G.L. ALEXANDERSON  
Santa Clara University, Santa Clara, CA 95053-0001  
ANDREW GRANVILLE  
University of Georgia, Athens, GA 30601-3024  
PETER HAGIS, JR.  
880 Edison Avenue, Philadelphia, PA 19116  
FRED T. HOWARD  
Wake Forest University, Winston-Salem, NC 27106-5239  
MARJORIE JOHNSON (Secretary-Treasurer)  
665 Fairlane Avenue, Santa Clara, CA 95051  
LESTER LANGE  
Moss Landing Marine Labs, Moss Landing, CA 95039-0450  
JEFF LAGARIAS  
Bell Laboratories, Murray Hill, NJ 07974-0636  
THERESA VAUGHAN  
University of North Carolina, Greensboro, NC 27410-5608

# ON THE UNIQUENESS OF REDUCED PHI-PARTITIONS

Corey Powell

Department of Mathematics, University of California at Berkeley, Berkeley, CA 94720

(Submitted July 1994)

## 1. PRELIMINARIES

For any positive integer  $k$ , let  $P_k = k^{\text{th}}$  prime and define  $s_k = \prod_{j=1}^{k-1} P_j$ . A positive integer  $n$  is *simple* if  $n = s_k$  for some positive integer  $k$ .

A  $\phi$ -partition of  $n$  is a partition  $n = d_1 + \cdots + d_i$ , where  $i$  and  $d_1, \dots, d_i$  are positive integers, that satisfies the condition  $\phi(n) = \phi(d_1) + \cdots + \phi(d_i)$ , where  $\phi$  is the Euler phi-function. In [1], Jones shows that the simple integers  $s_k$  have only the trivial  $\phi$ -partition  $s_k = s_k$ , and so define a  $\phi$ -partition of a positive integer  $n$  to be *reduced* if all the summands are simple.

Writing a partition as  $\sum_{j=1}^i b_j * d_1 + \cdots + b_i * d_i$ , means that  $d_j$  occurs  $b_j$  times in the partition for  $j = 1, \dots, i$ .

Every positive integer  $n$  has a unique partition  $\sum_{j=1}^i c_j * s_j$  satisfying the condition that  $0 \leq c_j < P_j$  for  $j \geq 1$ . This partition is a special type of *Cantor base representation* of  $n$ , which is a direct extension of the standard base 10 representation of  $n$ .

Throughout the paper,  $n$  will denote a positive integer. Let  $p_1 < p_2 < \cdots < p_\ell$  be the primes dividing  $n$  and let  $q_1 < q_2 < \cdots$  be the primes not dividing  $n$ .

## 2. THE ALGORITHM

Jones gives the following recursive algorithm for finding a reduced  $\phi$ -partition for  $n$ :

1. If  $n$  is simple, then  $n = 1 * n$  is a reduced  $\phi$ -partition.
2. If  $p^2 | n$  for some prime  $p$ , then  $p * (n/p)$  is a  $\phi$ -partition of  $n$ . Apply the algorithm to  $n/p$  to give a reduced  $\phi$ -partition  $\sum_{j=1}^i a_j * s_j$  for  $n/p$ ; the desired reduced  $\phi$ -partition for  $n$  is  $\sum_{j=1}^i (a_j p) * s_j$ .
3. If  $n$  is square-free and not simple, then let  $p$  be a prime divisor of  $n$  and let  $q$  be a prime such that  $q < p$  and  $q \nmid n$ . Such  $p$  and  $q$  exist since  $n$  is not simple;  $p$  could be chosen to be the largest prime dividing  $n$ , and  $q$  could be chosen to be the smallest prime not dividing  $n$ . Then  $(p-q) * (n/p) + 1 * (qn/p)$  is a  $\phi$ -partition for  $n$ . Apply the algorithm to  $n/p$  and  $qn/p$  to give reduced  $\phi$ -partitions  $\sum_{j=1}^i a_j * s_j$  and  $\sum_{j=1}^i a'_j * s_j$ , respectively. The desired reduced  $\phi$ -partition for  $n$  is  $\sum_{j=1}^i [(p-q)a_j + a'_j] * s_j$ .

At each step of the algorithm, it will be generally true that more than one prime or pair of primes can be chosen. The next section shows that the result of the algorithm is independent of these choices.

## 3. THE ALGORITHM GIVES A UNIQUE REDUCED $\phi$ -PARTITION

For any integer  $w$ , let  $\phi_w(n) = n \prod_{p|n} (1 - w/p)$ , so that  $\phi_0(n) = n$  and  $\phi_1(n) = \phi(n)$ . Define a  $\phi_w$ -partition and a reduced  $\phi_w$ -partition analogously to a  $\phi$ -partition and a reduced  $\phi$ -partition, respectively.



If  $p$  is prime and  $p^2 | n$ , then  $\phi_w(n) = p\phi_w(n/p)$ , and so  $p * (n/p)$  is a  $\phi_w$ -partition of  $n$ . If  $p$  and  $q$  are primes,  $p | n$ ,  $p^2 \nmid n$ ,  $q \nmid n$  and  $p > q$ , then

$$\begin{aligned}\phi_w(n) &= (p-w)\phi_w(n/p) \\ &= (p-q)\phi_w(n/p) + (q-w)\phi_w(n/p) \\ &= (p-q)\phi_w(n/p) + \phi_w(qn/p),\end{aligned}$$

so that  $(p-q) * (n/p) + 1 * (qn/p)$  is a  $\phi_w$ -partition of  $n$ . These facts together with an induction argument show that any reduced  $\phi$ -partition given by the algorithm is also a reduced  $\phi_w$ -partition for every integer  $w$ .

For the rest of the paper, let  $i$  be the unique positive integer such that  $s_i \leq n < s_{i+1}$ ; any reduced  $\phi$ -partition of  $n$  can be written in the form  $\sum_{j=1}^i b_j * s_j$ .

**Theorem 1:** The reduced  $\phi$ -partition for  $n$  given by the algorithm above is independent of the primes chosen at each step of the algorithm.

**Proof:** Suppose that  $\sum_{j=1}^i a_j * s_j$  is a reduced  $\phi$ -partition of  $n$  given by the algorithm. By replacing  $w$  with  $P_1$ , with  $P_2$ , ..., and finally with  $P_i$ , the following system of  $i$  equations and  $i$  unknowns is obtained:

$$\begin{aligned}a_1\phi_{P_1}(s_1) + a_2\phi_{P_1}(s_2) + \cdots + a_i\phi_{P_1}(s_i) &= \phi_{P_1}(n), \\ a_1\phi_{P_2}(s_1) + a_2\phi_{P_2}(s_2) + \cdots + a_i\phi_{P_2}(s_i) &= \phi_{P_2}(n), \\ &\vdots \\ a_1\phi_{P_i}(s_1) + a_2\phi_{P_i}(s_2) + \cdots + a_i\phi_{P_i}(s_i) &= \phi_{P_i}(n).\end{aligned}$$

This system of equations can be rewritten in the form  $N\vec{a} = \vec{b}$ , where the matrix  $N$  has entries

$$N_{\ell k} = \phi_{P_\ell}(s_k) = \prod_{j=1}^{k-1} (P_j - P_\ell).$$

If  $\ell < k$ , then  $N_{\ell k} = 0$ , so that  $N$  is lower-triangular, and if  $\ell = k$ , then  $N_{\ell k} \neq 0$ , so that  $N$  is invertible. It follows that the solution to this linear system uniquely determines the coefficients  $a_j$  in the reduced  $\phi$ -partition given by the algorithm.  $\square$

The algorithm gives a unique reduced  $\phi$ -partition for  $n$ , but frequently this is not the only reduced  $\phi$ -partition that  $n$  has. The integer 8, for example, has 2 reduced  $\phi$ -partitions:  $4 * 2$  and  $2 * 1 + 6$ . Certain characteristics of the reduced  $\phi$ -partition given by the algorithm are critical, however, in determining whether  $n$  has a unique reduced  $\phi$ -partition. The following two theorems summarize these characteristics. Let  $M(n) = n / (\prod_{p \mid n, p \text{ prime}} p)$ .

**Theorem 2:** Let  $k$  be the largest integer such that  $s_k | n$  and let  $\ell$  be the number of distinct prime factors of  $n$ . The algorithm above gives a reduced  $\phi$ -partition for  $n$  of the form  $\sum_{j=k}^{\ell+1} a_j * s_j$ , where  $a_{\ell+1} = M(n)$  and  $a_k \geq a_{k+1} \geq \cdots \geq a_{\ell+1}$ .

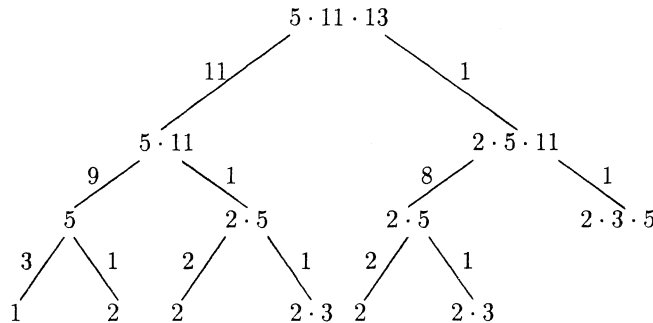
**Proof:** It follows that  $a_j = 0$  for  $1 \leq j < k$  from examining the first  $k-1$  equations of the linear system above and noting that  $b_j = \phi_{P_j}(n) = 0$  for  $1 \leq j < k$ . It is clear that  $a_{\ell+1} = M(n)$  and

$a_j = 0$  for  $\ell + 1 < j$  from the three cases presented in the algorithm together with an induction argument on  $n$ .

The claim that  $a_k \geq a_{k+1} \geq \dots \geq a_{\ell+1}$  will also be proven by induction on  $n$ . If  $n = 1$ , then  $1 = 1 * 1$  is the reduced  $\phi$ -partition. If  $n > 1$  and  $p^2 | n$  for some prime  $p$ , then establish the claim by using the  $\phi$ -partition  $n = p * (n/p)$  and applying the induction hypothesis to  $n/p$ .

If  $n$  is square-free, then the proof is divided into two cases. In the first case,  $p_\ell < q_1$ , so that  $n = s_k$ . If  $p_\ell > q_1$  and there is a prime  $t$  such that  $t \nmid n$  and  $q_1 < t < p_\ell$ , then the claim follows from using the  $\phi$ -partition  $n = (p_\ell - t) * (n/p_\ell) + 1 * (tn/p_\ell)$  and applying the induction hypothesis to  $n/p_\ell$  and  $tn/p_\ell$ . If  $p_\ell > q_1$ , but there is no prime  $t$  as described above, then  $q_1 n/p_\ell = s_{\ell+1}$ , since  $q_1 n/p_\ell$  is simple and has the same number of prime factors as  $n$ . Prove the claim by using the  $\phi$ -partition  $n = (p_\ell - q_1) * (n/p_\ell) + 1 * s_{\ell+1}$  and applying the induction hypothesis to  $n/p_\ell$ .  $\square$

By Theorem 1, the reduced  $\phi$ -partition  $n = \sum_{j=1}^l a_j * s_j$  given by the algorithm can be represented by a weighted binary tree as follows. As noted in part 3 of the algorithm, it is possible to choose  $p$  as the largest prime dividing  $n$  and choose  $q$  as the smallest prime dividing  $n$ . Assume without loss of generality that  $n$  is square-free; the algorithm will find a reduced  $\phi$ -partition for  $\prod_{p \mid n} p$  and incorporate this reduced  $\phi$ -partition into the  $\phi$ -partition  $n = M(n) * \prod_{p \mid n} p$ . If  $n$  is not simple, then the left branch has weight  $p_\ell - q_1$  and the left child is  $n/p_\ell$ , while the right branch has weight 1 and the right child is  $q_1 n/p_\ell$ . Apply this process recursively to  $n/p_\ell$  and  $q_1 n/p_\ell$ , terminating only when all the leaves of the tree are simple integers. The example below gives the tree for  $5 \cdot 11 \cdot 13$ .



It is possible to determine  $a_j$  from the tree representation by taking the sum over all paths from  $n$  to  $s_j$  of the product of the weights along each path. The coefficient  $a_2$  for  $5 \cdot 11 \cdot 13$ , for example, is  $11 \cdot 9 \cdot 1 + 11 \cdot 1 \cdot 2 + 1 \cdot 8 \cdot 2$ .

Let  $n = p_1 \dots p_\ell$ , and suppose that  $m$  is a vertex at level  $u = u(m)$  of the tree described above, where level 0 denotes the top of the tree. Let  $L = L(m)$  and  $R = R(m) = u = L(m)$  be the number of left and right branches, respectively, in the path from  $n$  to  $m$ , and define  $t_0 < t_1 < \dots < t_{L-1}$  to be the levels where the path branches to the left. An induction argument on the level  $u$  proves the following lemma.

**Lemma 3:** If  $m$  is a vertex at level  $u$  of the tree, then  $m = p_1 \dots p_{\ell-u} q_1 \dots q_R$  and the product of the weights along the path from  $n$  to  $m$  is  $\prod_{e=0}^{L-1} (p_{\ell-t_e} - q_{1+t_e-e})$ .

**Proof:** The proof will be by induction on  $u$ . If  $u = 0$ , then  $m = n$  and the result is clear. Suppose that the lemma is true for  $m$  and its ancestors, and consider the children of  $m$ . Assume without loss of generality that  $m$  is not simple, since simple vertices have no children. To establish the lemma for the children of  $m$ , it suffices to show that the largest prime dividing  $m$  is  $p_{\ell-u}$  and that the smallest prime not dividing  $m$  is  $q_{R+1}$ . The largest prime dividing  $m$  is clearly  $\max(p_{\ell-u}, q_R)$ , and the smallest prime not dividing  $m$  is clearly  $\min(p_{\ell-u+1}, q_{R+1})$ . These two facts reduce the two assertions above to the condition  $p_{\ell-u} > q_{R+1}$ . Divide the proof of this condition into two cases. In the first case, assume that  $m$  is the right child of  $m' = p_1 \dots p_{\ell-u+1} q_1 \dots q_{R-1}$ . It follows from the construction of  $m$  that  $p_{\ell-u+1}$  is the largest prime dividing  $m'$  and that  $q_R$  is the smallest prime not dividing  $m'$ . It also follows that  $p_{\ell-u+1} > q_R$ , since  $m'$  would be simple otherwise. Hence  $p_{\ell-u} > q_{R+1}$ , because  $m$  is not simple. The proof when  $m$  is a left child is similar.  $\square$

Fix a path from  $n$  to  $s_j$ . A left child has one less prime divisor than its parent, while a right child has the same number of prime divisors as its parent. This implies that the path from  $n$  to  $s_j$  must branch to the left  $\ell - j + 1$  times, since  $s_j$  has  $j - 1$  prime factors. Let  $m$  be the vertex at level  $t_{\ell-j}$ . It follows from the proof of the previous lemma that  $p_{\ell-t_{\ell-j}}$  is the largest prime dividing  $m$ , that  $q_{1+t_{\ell-j}-(\ell-j)}$  is the smallest prime not dividing  $m$ , and that  $p_{\ell-t_{\ell-j}} > q_{1+t_{\ell-j}-(\ell-j)}$ .

Conversely, suppose that  $0 \leq t_0 < t_1 < \dots < t_{\ell-j} < \ell$  and that  $p_{\ell-t_{\ell-j}} > q_{1+t_{\ell-j}-(\ell-j)}$ . An induction argument on  $\ell - j$  shows that there is a path from  $n$  to  $s_j$  that branches to the left at levels  $t_0, \dots, t_{\ell-j}$ . If  $\ell - j = 0$ , then an induction on the level together with the previous lemma and the condition  $p_{\ell-t_0} > q_{1+t_0}$  guarantees that there is a path branching to the right at levels  $0, \dots, t_0 - 1$ . This condition also guarantees that the vertex at level  $t_0$  is not simple, since  $p_{\ell-t_0}$  and  $q_{1+t_0}$  are, respectively, the largest prime dividing the vertex and the smallest prime not dividing the vertex. Branching to the left at level  $t_0$  will give a vertex with  $\ell - 1$  prime factors, and so branching to the right at level  $t_0 + 1$  and all higher levels will give a path that terminates at  $s_\ell$ .

Assume that the claim above is true for  $\ell - j - 1$ . This implies that there is a path from  $n$  to  $s_{j+1}$  that branches to the left at levels  $t_0, \dots, t_{\ell-j-1}$ , since  $p_{\ell-t_{\ell-j-1}} > p_{\ell-t_{\ell-j}} > q_{1+t_{\ell-j}-(\ell-j)} \geq q_{1+t_{\ell-j-1}-(\ell-j-1)}$ . Take this path from  $n$  to level  $t_{\ell-j-1}$ , and then construct a path from the vertex at this level to  $s_j$  by the same method as in the previous paragraph. This proves the claim above. Non-square-free  $n$  adds a factor of  $M(n)$  to the calculations, as noted previously, and so the claim above combined with the previous lemma proves the following theorem.

**Theorem 4:** If  $k \leq j \leq \ell$ , then

$$a_j = M(n) \sum \prod_{e=0}^{\ell-j} (p_{\ell-t_e} - q_{1+t_e-e}),$$

where the sum is taken over all  $0 \leq t_0 < \dots < t_{\ell-j} < \ell$  with  $p_{\ell-t_{\ell-j}} > q_{1+t_{\ell-j}-(\ell-j)}$ . In particular,

$$a_k = M(n) \prod_{e=k}^{\ell} (p_e - q_1) \quad \text{and} \quad a_{k+1} \geq M(n) \prod_{e=k+1}^{\ell} (p_e - q_1).$$

The following section gives a necessary and sufficient criterion for determining if  $n$  has a unique reduced  $\phi$ -partition by using the previous two theorems together with the specific Cantor base representation of  $n$  described in Section 1.

#### 4. WHEN DOES $n$ HAVE A UNIQUE REDUCED $\phi$ -PARTITION?

**Theorem 5:** A positive integer  $n$  has a unique reduced  $\phi$ -partition if and only if  $n = 9$ ,  $n$  is prime, or the Cantor base representation for  $n$  is a reduced  $\phi$ -partition.

By enumerating all possible partitions of 9 consisting of simple integers, one can verify that  $3 * 1 + 3 * 2$  is the unique reduced  $\phi$ -partition of 9. The following two lemmas will complete the proof of the *if* part of the theorem.

**Lemma 6:** Primes have a unique reduced  $\phi$ -partition.

**Proof:** From Theorem 7 in [1], a  $\phi$ -partition of a prime  $q$  must be of the form  $(q-r) * 1 + r$ , where  $r$  is prime and  $r \leq q$ . The only simple prime number is 2, and so  $(q-2) * 1 + 1 * 2$  is the unique reduced  $\phi$ -partition of  $q$ .  $\square$

**Lemma 7:** Let  $\sum_{j=1}^i c_j * s_j$  be the Cantor base representation of  $n$  described in Section 1. If  $\sum_{j=1}^i c_j * s_j$  is a reduced  $\phi$ -partition, then it is the unique reduced  $\phi$ -partition for  $n$ .

**Proof:** It suffices to show that for any other partition  $\sum_{j=1}^i b_j * s_j$  of  $n$  into simple integers,  $\sum_{j=1}^i c_j \phi(s_j) < \sum_{j=1}^i b_j \phi(s_j)$ . Suppose that  $\sum_{j=1}^i b_j * s_j$  is a counterexample with  $\sum_{j=1}^i b_j$  minimal. There is an  $h$  such that  $b_h \geq P_h$  since  $\sum_{j=1}^i b_j * s_j$  is distinct from  $\sum_{j=1}^i c_j * s_j$ . Form a new partition  $\sum_{j=1}^i b'_j * s_j$  by converting  $P_h$  of the  $s_h$ 's into an  $s_{h+1}$ . This new partition is a counterexample that contradicts the minimality of  $\sum_{j=1}^i b_j$ , and hence proves the lemma.  $\square$

Suppose that  $n \neq 9$ , that  $n$  is composite, and that the Cantor base representation for  $n$  is not a reduced  $\phi$ -partition. It then follows from Theorem 2 that  $a_k \geq P_k$ , where  $\sum_{j=1}^i a_j * s_j$  is the reduced  $\phi$ -partition given by the algorithm and  $k$  the largest positive integer such that  $s_k | n$ , as defined in Theorem 2. Theorem 4 gives the formula  $a_k = M(n) \prod_{e=k}^{\ell} (p_e - P_k)$ , since  $q_1 = P_k$ . It is clear from this formula that  $a_k \neq P_k$ , since  $P_k$  is prime,  $P_k$  does not divide  $n$ , and  $P_k$  does not divide  $(p - P_k)$  for any primes  $p$  dividing  $n$ . If  $k > 1$ , then apply the following lemma with  $h = k$  to show that  $n$  has a second reduced  $\phi$ -partition. If  $k = 1$ , then  $n$  is odd,  $q_1 = 2$ , and the inequality  $a_2 \geq M(n) \prod_{e=2}^{\ell} (p_e - 2)$  is a result of Theorem 4. It is a straightforward consequence of this inequality that  $a_2 > 3$  if  $n \neq 15$ , and so it follows from the following lemma with  $h = 2$  that  $n$  has a second reduced  $\phi$ -partition. The observation that  $3 + 1 + 3 * 2 + 6$  and  $1 + 7 * 2$  are reduced  $\phi$ -partitions for 15 completes the proof of the theorem.

**Lemma 8:** Let  $\sum_{j=1}^i b_j * s_j$  be a reduced  $\phi$ -partition of  $n$ . If  $b_h > P_h$  for some  $h > 1$ , then  $n$  has a second reduced  $\phi$ -partition.

**Proof:** To prove the lemma, it will be necessary to show that for each  $j > 1$  there is a partition  $\sum_{f=1}^{j-1} \beta_f * s_f$  of  $s_j$  such that  $\sum_{f=1}^{j-1} \beta_f \phi(s_f) = 2\phi(s_j)$ . This will be shown by induction on  $j$ . If  $j = 2$ , then  $2 = 2 * 1$  is the desired partition. If  $j > 2$ , then, by the induction hypothesis,  $s_{j-1}$  has a partition  $\sum_{f=1}^{j-2} \beta'_f * s_f$  with the desired property. Hence,  $s_j = \sum_{f=1}^{j-2} [\beta'_f (P_{j-1} - 2)] * s_f + 2 * s_{j-1}$  is a partition of  $s_j$  with the desired property.

Now, suppose  $h$  is a positive integer such as in the hypothesis of the lemma and let  $\sum_{f=1}^{h-1} \beta_f * s_f$  be a partition of  $s_h$  with the above property. Construct a new reduced  $\phi$ -partition for  $n$  by combining  $P_h$  of the  $s_h$  terms into one  $s_{h+1}$  term. There is a net loss of  $\phi(s_h)$  when the sum of the  $\phi$  values in the partition is taken, since  $\phi(s_{h+1}) = (P_h - 1)\phi(s_h)$ . Breaking up one of the remaining  $s_h$  terms compensates for this loss. The second reduced  $\phi$ -partition for  $n$  is

$$\sum_{f=1}^{h-1} (b_f + \beta_f) * s_f + (b_h - P_h - 1) * s_h + (b_{h+1} + 1) * s_{h+1} + \sum_{f=h+2}^i b_f * s_f. \quad \square$$

# REFERENCE

1. Patricia Jones. " $\phi$ -Partitions." *The Fibonacci Quarterly* **29.4** (1991):347-50.

AMS Classification Numbers: 11P81, 11P83



## FIBONACCI ENTRY POINTS AND PERIODS FOR PRIMES 100,003 THROUGH 415,993

A Monograph  
by Daniel C. Fielder and Paul S. Bruckman  
Members, The Fibonacci Association

In 1965, Brother Alfred Brousseau, under the auspices of The Fibonacci Association, compiled a two-volume set of Fibonacci entry points and related data for the primes 2 through 99,907. This set is currently available from The Fibonacci Association as advertised on the back cover of *The Fibonacci Quarterly*. Thirty years later, this new monograph complements, extends, and triples the volume of Brother Alfred's work with 118 table pages of Fibonacci entry-points for the primes 100,003 through 415,993.

In addition to the tables, the monograph includes 14 pages of theory and facts on entry points and their periods and a complete listing with explanations of the *Mathematica* programs use to generate the tables. As a bonus for people who must calculate Fibonacci and Lucas numbers of all sizes, instructions are available for "stand-alone" application of a fast and powerful Fibonacci number program which outclasses the stock Fibonacci programs found in *Mathematica*. The Fibonacci portion of this program appears through the kindness of its originator, Dr. Roman Maeder, of ETH, Zürich, Switzerland.

The price of the book is \$20.00; it can be purchased from the Subscription Manager of *The Fibonacci Quarterly* whose address appears on the inside front cover of the journal.

# ON THE STRUCTURE OF QUADRATIC IRRATIONALS ASSOCIATED WITH GENERALIZED FIBONACCI AND LUCAS NUMBERS

Edward B. Burger and Christopher S. Kollett

Department of Mathematics, Williams College, Williamstown, MA 01267

(Submitted July 1994)

## 1. INTRODUCTION

In 1970 C. T. Long and J. H. Jordan completed a series of two papers, [3] and [4], in which they analyzed the arithmetical structure of certain classes of quadratic irrationals and the effects on their structure after multiplication by rational numbers. In particular, for a positive integer  $a$ , let  $\mathcal{F}_n = \mathcal{F}_n(a)$  and  $\mathcal{L}_n = \mathcal{L}_n(a)$  be the  $n^{\text{th}}$  *generalized Fibonacci* and *generalized Lucas numbers*, respectively. That is,  $\mathcal{F}_0 = 0$ ,  $\mathcal{F}_1 = 1$ ,  $\mathcal{L}_0 = 2$ ,  $\mathcal{L}_1 = a$  and, for  $n > 1$ ,  $\mathcal{F}_n = a\mathcal{F}_{n-1} + \mathcal{F}_{n-2}$ ,  $\mathcal{L}_n = a\mathcal{L}_{n-1} + \mathcal{L}_{n-2}$ . We denote the *generalized golden ratio* by  $\varphi_a$ . Thus,

$$\varphi_a = \frac{a + \sqrt{a^2 + 4}}{2} = [a, a, \dots] = [\bar{a}],$$

where the last expression denotes the (simple) continued fraction expansion for  $\varphi_a$  and the bar indicates the periodicity. It follows that  $\lim_{n \rightarrow \infty} \mathcal{F}_{n+1}/\mathcal{F}_n = \varphi_a$ . We note that in the case in which  $a = 1$  we have  $\mathcal{F}_n = F_n$ ,  $\mathcal{L}_n = L_n$ , and  $\varphi_a = \varphi$ .

Among their other interesting results, Long and Jordan investigated and compared the continued fraction expansions of  $\frac{\mathcal{F}_n}{\mathcal{L}_n} \varphi_a$  and  $\frac{\mathcal{L}_n}{\mathcal{F}_n} \varphi_a$  when  $r$  and  $s$  are consecutive generalized Fibonacci numbers or consecutive generalized Lucas numbers. These results led them to consider the structure of numbers of the form  $\frac{\mathcal{F}_n}{\mathcal{L}_n} \varphi_a$  and  $\frac{\mathcal{L}_n}{\mathcal{F}_n} \varphi_a$  where  $r = \mathcal{F}_n$  and  $s = \mathcal{L}_n$ . They wrote (in the present notation) [4]:

"In view of the preceding results, one would expect an interesting theorem concerning the simple continued fraction of

$$\frac{\mathcal{F}_n}{\mathcal{L}_n} \varphi_a \quad \text{and} \quad \frac{\mathcal{L}_n}{\mathcal{F}_n} \varphi_a$$

but we were unable to make a general assertion value for all  $a$ . To illustrate the difficulty, note that, when  $a = 2$  and  $\varphi_2 = 1 + \sqrt{2}$ , we have

$$\begin{aligned} \frac{\mathcal{F}_4}{\mathcal{L}_4} \varphi_2 &= [0, 1, \overline{5, 1, 3, 5, 1, 7}], \\ \frac{\mathcal{F}_5}{\mathcal{L}_5} \varphi_2 &= [0, 1, \overline{5, 1, 5, 3, 1, 4, 1, 7}], \\ \frac{\mathcal{F}_6}{\mathcal{L}_6} \varphi_2 &= [0, 1, \overline{5, 1, 4, 1, 3, 5, 1, 4, 1, 7}]. \end{aligned}$$

They do, however, discover the following two beautiful identities for the case in which  $a = 1$ . We state them here as

**Theorem 1:** For  $n \geq 4$ ,

$$\frac{F_n}{L_n} \varphi = \left[ 0, 1, 2, \underbrace{1, 1, \dots, 1, 1}_{n-4 \text{ times}}, 3, \underbrace{1, 1, \dots, 1, 1}_{n-3 \text{ times}}, 4 \right] \quad (1.1)$$

and

$$\frac{L_n}{F_n} \varphi = \left[ 3, \underbrace{1, 1, \dots, 1, 1}_{n-3 \text{ times}}, 3, \underbrace{1, 1, \dots, 1, 1}_{n-4 \text{ times}}, 2, 4 \right].$$

Our first objective here is to extend their result to the more general case for arbitrary  $a$ . We begin with the elementary observation that

$$\lim_{n \rightarrow \infty} \frac{F_n}{L_n} \varphi = \frac{5 + \sqrt{5}}{10} = [0, 1, 2, \overline{1}],$$

and, thus, the initial string of 1's in (1.1) is not surprising. It is the beautiful near mirror symmetry of the interior portion of the periodic part of (1.1) that is unexpected. More generally, one has

$$\lim_{n \rightarrow \infty} \frac{\mathcal{F}_n}{\mathcal{L}_n} \varphi_a = \frac{a^2 + 4 + a\sqrt{a^2 + 4}}{2(a^2 + 4)} = [0, 1, a^2 + 1, \overline{1, a^2}].$$

Thus, for large  $n$ , we would expect the continued fraction expansion for  $(\mathcal{F}_n / \mathcal{L}_n) \varphi_a$  to begin with  $[0, 1, a^2 + 1, 1, a^2, 1, a^2, 1, \dots]$ . As Long and Jordan remark, however, in this case we appear to lose the symmetry. In fact, the near mirror symmetry in (1.1) is somewhat deceptive. Perhaps it is better to view (1.1) as a "recursive system" in the following sense. We define the strings or "words"  $\vec{W}_n = W_n$  for  $n \geq 4$  by  $W_4 = (3, 1)$  and, for  $n > 4$ ,  $W_n = (\vec{W}_{n-1}, 1, 1)$ , where  $\vec{W}_{n-1}$  is the word  $W_{n-1}$  read *backwards*. For example,  $W_5 = (1, 3, 1, 1)$  and  $W_6 = (1, 1, 3, 1, 1, 1)$ . Thus, we may now reformulate (1.1) as

$$\frac{F_n}{L_n} \varphi = [0, 1, 2, \overline{W_n}, 4].$$

We note that the continued fraction expansions given above for  $(\mathcal{F}_n / \mathcal{L}_n) \varphi_a$  obey a similar recursive behavior. This leads to our first result.

**Theorem 2:** Let  $\mathcal{F}_n = \mathcal{F}_n(a)$  and  $\mathcal{L}_n = \mathcal{L}_n(a)$  be the  $n^{\text{th}}$  generalized Fibonacci and Lucas numbers, respectively. Let  $\vec{W}_4 = W_4(a) = (1, a^2 - 1, a^2 + 1, 1)$  and, for  $n > 4$ , let  $\vec{W}_n = W_n(a) = (\vec{W}_{n-1}, a^2, 1)$ . Then, for  $n \geq 4$ ,

$$\frac{\mathcal{F}_n}{\mathcal{L}_n} \varphi_a = \left[ 0, 1, a^2 + 1, \overline{\vec{W}_n}, a^2 + 3 \right], \quad (1.2)$$

and

$$\frac{\mathcal{L}_n}{\mathcal{F}_n} \varphi_a = \left[ a^2 + 2, \overline{\vec{W}_n}, a^2 + 1, a^2 + 3 \right]. \quad (1.3)$$

We remark that for  $a = 1$ ,

$$[{}^{\circ}W_4] = 1 + \frac{1}{0 + \frac{1}{2 + \frac{1}{1}}} = 1 + 2 + \frac{1}{1} = 3 + \frac{1}{1} = [W_4],$$

thus, Theorem 1 and Theorem 2 are equivalent when  $a = 1$ .

One may define the words  ${}^{\circ}W_n$  occurring in Theorem 2 explicitly rather than iteratively. In particular, a simple induction argument reveals that, for  $n \geq 4$  even,

$${}^{\circ}W_n = (\{1, a^2\}^{(n-4)/2}, 1, a^2 - 1, a^2 + 1, 1, \{a^2, 1\}^{(n-4)/2}), \quad (1.4)$$

and, for  $n > 4$  odd,

$${}^{\circ}W_n = (\{1, a^2\}^{(n-5)/2}, 1, a^2 + 1, a^2 - 1, 1, \{a^2, 1\}^{(n-3)/2}),$$

where by  $\{1, a^2\}^n$  we mean the word  $(1, a^2)$  repeated  $n$  times.

As Long and Jordan implicitly note with respect to Theorem 1, Theorem 2 immediately implies that  $(\mathcal{F}_n / \mathcal{L}_n)\varphi_a$  and  $(\mathcal{L}_n / \mathcal{F}_n)\varphi_a$  are not equivalent numbers. Recall that two real numbers are said to be *equivalent* if, from some point on, their continued fraction expansions agree (see [5]).

Next, we extend Theorem 1 in a different direction. We wish to analyze the structure of quadratic irrationals of the form  $(\mathcal{F}_m / \mathcal{L}_n)\varphi_a$ . If  $m$  is even, then  $\mathcal{F}_m / \mathcal{L}_n$  is an integer (see [7]); thus, we consider only the case in which  $m$  is odd. We first state an extension of Theorem 1 in this context for the case  $m = 3$ .

**Theorem 3:** For  $n \geq 4$ , if  $n$  is even, then

$$\frac{F_{3n}}{L_n} \varphi = \left[ F_{2n+1} - 1, \underbrace{3, 1, 1, \dots, 1, 1}_{n-2 \text{ times}}, L_{2n} - 2, \underbrace{2, 1, 1, \dots, 1, 1}_{n-4 \text{ times}}, 2, 1, L_{2n} - 2 \right].$$

If  $n > 4$  is odd, then

$$\frac{F_{3n}}{L_n} \varphi = \left[ F_{2n+1}, \underbrace{1, 2, 1, 1, \dots, 1, 1}_{n-4 \text{ times}}, L_{2n}, \underbrace{1, 1, \dots, 1, 1}_{n-2 \text{ times}}, 3, L_{2n} \right].$$

The general formulation of Theorem 3 appears to be more complicated and requires us to define several useful sums. For odd integers  $m$ , we let

$$\begin{aligned} F_1(m) &= \sum_{k=1}^{(m-1)/2} (-1)^k \mathcal{F}_{2k+1}, & F(m) &= \sum_{k=1}^{(m-1)/2} \mathcal{F}_{2k+1}, \\ L_1(m) &= \sum_{k=1}^{(m-1)/2} (-1)^k \mathcal{L}_{2k}, & L(m) &= \sum_{k=1}^{(m-1)/2} \mathcal{L}_{2k}. \end{aligned}$$

We remark that  $F_1(m)$  and  $L_1(m)$  are positive integers if and only if  $m \equiv 1 \pmod{4}$ . We believe that one may generalize the proof of Theorem 3 to prove the following conjecture.

**Conjecture 4:** Let  $\mathcal{F}_n = \mathcal{F}_n(a)$  and  $\mathcal{L}_n = \mathcal{L}_n(a)$  be the  $n^{\text{th}}$  generalized Fibonacci and Lucas numbers, respectively, and  $m$  an odd integer. Suppose  $m \geq 3$  is an odd integer and  $n \geq 4$ . For  $n$  even,



let  $\tilde{u}_n = u_n(a) = (1, a^2 + 1, 1, \{a^2, 1\}^{(n-4)/2}, a^2 - 1, 1)$  and  $\tilde{v}_n = v_n(a) = (\{a^2, 1\}^{(n-2)/2}, a^2 + 2)$ ; for  $n$  odd, let  $\tilde{w}_n = w_n(a) = (\{a^2, 1\}^{(n-5)/2})$ . If  $n$  is odd, then

$$\frac{\mathcal{F}_{mn}}{\mathcal{L}_n} \varphi_a = \left[ \mathbf{F}(m), \overline{1, a^2 + 1, 1, \tilde{w}_n, a^2 + 1, a^2 \mathbf{L}(m) + a^2 - 1, \tilde{w}_{n+2}, 1, a^2 + 2, \mathbf{L}(m)} \right].$$

If  $n$  is even and  $m \equiv 1 \pmod{4}$ , then

$$\frac{\mathcal{F}_{mn}}{\mathcal{L}_n} \varphi_a = \left[ \mathbf{F}_1(m), \overline{\tilde{u}_n, \mathbf{L}_1(m), \tilde{v}_n, \mathbf{L}_1(m)} \right].$$

If  $n$  is even and  $m \equiv 3 \pmod{4}$ , then

$$\frac{\mathcal{F}_{mn}}{\mathcal{L}_n} \varphi_a = \left[ -\mathbf{F}_1(m) - 1, \overline{\tilde{v}_n, -\mathbf{L}_1(m) - 2, \tilde{u}_n, -\mathbf{L}_1(m) - 2} \right].$$

One may also find analogous expansions for  $(\mathcal{L}_{mn}/\mathcal{F}_n)\varphi_a$ . For example, one may adopt the method of proof of Theorem 3 to deduce

**Theorem 5:** For  $n \geq 4$ , if  $n$  is even, then

$$\frac{L_{3n}}{F_n} \varphi = \left[ 5F_{2n+1} + 3, \overline{3, 1, \underbrace{1, \dots, 1}_{n-3 \text{ times}}, 1, 2, L_{2n}, \underbrace{1, 1, \dots, 1}_{n-3 \text{ times}}, 2, 5L_{2n} + 4} \right].$$

If  $n > 4$  is odd, then

$$\frac{L_{3n}}{F_n} \varphi = \left[ 5F_{2n+1} - 4, \overline{2, \underbrace{1, 1, \dots, 1}_{n-3 \text{ times}}, 1, L_{2n} - 2, 2, \underbrace{1, 1, \dots, 1}_{n-3 \text{ times}}, 1, 5L_{2n} - 6} \right].$$

Long and Jordan [4] concluded their investigation by proving the surprising result that, for any positive integers  $m$  and  $n$ ,  $(\mathcal{F}_m/\mathcal{F}_n)\varphi_a$  and  $(\mathcal{F}_n/\mathcal{F}_m)\varphi_a$  are equivalent numbers. They remarked, however, that it is not always the case that  $(\mathcal{L}_m/\mathcal{L}_n)\varphi_a$  and  $(\mathcal{L}_n/\mathcal{L}_m)\varphi_a$  are equivalent numbers. To illustrate this, they noted that

$$\frac{L_2}{L_4} \varphi = [0, 1, \overline{2, 3, 1, 4}] \quad \text{and} \quad \frac{L_4}{L_2} \varphi = [3, 1, \overline{3, 2, 4}].$$

We observe that, in their example, the indices 2 and 4 are *not* relatively prime. Here we prove that this is the only possible case in which two such numbers are not equivalent. In particular, we prove

**Theorem 6:** If  $\mathcal{L}_n = \mathcal{L}_n(a)$  is the  $n^{\text{th}}$  generalized Lucas number, then for relatively prime positive integers  $m$  and  $n$ ,

$$\frac{\mathcal{L}_m}{\mathcal{L}_n} \varphi_a \quad \text{and} \quad \frac{\mathcal{L}_n}{\mathcal{L}_m} \varphi_a$$

are equivalent numbers.

More recently, Long [2] studied the arithmetical structure of classes of quadratic irrationals involving generalized Fibonacci and Lucas numbers of the form

$$\frac{aS_n + T_m\sqrt{a^2 + 4}}{2}, \quad (1.5)$$

where  $S_n$  is either  $\mathcal{F}_n$  or  $\mathcal{L}_n$  and  $T_m$  is either  $\mathcal{F}_m$  or  $\mathcal{L}_m$ . For example, he investigated

$$\frac{a\mathcal{F}_n + \mathcal{L}_m\sqrt{a^2 + 4}}{2}. \quad (1.6)$$

For numbers of the form (1.5), Long showed that their continued fraction expansions have the general shape

$$[a_0, \overline{a_1, a_2, \dots, a_r}],$$

where the  $a_0$  and  $a_r$  were explicitly computed. He also proved that  $(a_1, a_2, \dots, a_{r-1})$  is a palindrome, but was unable to determine the precise value of  $a_n$  for  $0 < n < r$ . Long also observed that the period length  $r$  appeared always to be even and that the value of  $r$  appeared not to be bounded as a function of  $a$ ,  $m$ , and  $n$ . Here we claim that the continued fraction for such numbers may be completely determined. As an illustration, in Section 6 we provide the precise formula for the continued fraction expansion for numbers of the form (1.6). As the expansion is somewhat complicated in general, we do not state it here in the introduction; instead, we state it explicitly in Section 6 as Theorems 7 and 8. As a consequence of our results, we are able to prove that Long's first observation is true while his second observation is false.

## 2. BASIC IDENTITIES AND CONTINUED FRACTIONS

We begin with a list of well-known identities involving Fibonacci and Lucas numbers that will be utilized in our arguments (for proofs, see, e.g., [7]). For  $n \geq 1$ ,

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}, \quad (2.1)$$

$$F_n = F_{n-1} + F_{n-2}, \quad L_n = L_{n-1} + L_{n-2}, \quad L_n = F_{n+1} + F_{n-1}, \quad (2.2)$$

$$F_{n+m} - (-1)^m F_{n-m} = F_m L_n, \quad (2.3)$$

$$L_{n+m} + (-1)^m L_{n-m} = L_m L_n, \quad (2.4)$$

$$L_n^2 + 4(-1)^{n+1} = 5F_n^2, \quad (2.5)$$

$$F_{2n} = F_n L_n. \quad (2.6)$$

If  $\mathcal{F}_n = \mathcal{F}_n(a)$  and  $\mathcal{L}_n = \mathcal{L}_n(a)$  denote the  $n^{\text{th}}$  generalized Fibonacci and Lucas numbers, respectively, then for  $n \geq 1$ ,

$$\begin{pmatrix} a^2 + 1 & a^2 \\ 1 & 1 \end{pmatrix}^n = \begin{pmatrix} \mathcal{F}_{2n+1} & a\mathcal{F}_{2n} \\ a^{-1}\mathcal{F}_{2n} & \mathcal{F}_{n-1} \end{pmatrix}, \quad (2.7)$$

$$\mathcal{L}_n = a\mathcal{F}_n + 2\mathcal{F}_{n-1}, \quad (2.8)$$

$$\mathcal{L}_n^2 = 4\mathcal{F}_{n+1}\mathcal{F}_{n-1} + a^2\mathcal{F}_n^2, \quad (2.9)$$

$$\mathcal{F}_n\mathcal{F}_{n+2} - \mathcal{F}_{n+1}^2 = (-1)^{n+1}, \quad (2.10)$$

$$\mathcal{F}_{n+2} \varphi_a + \mathcal{F}_{n+1} = \varphi_a (\mathcal{F}_{n+1} \varphi_a + \mathcal{F}_n), \quad (2.11)$$

$$(\alpha^2 + 4)\mathcal{F}_n^2 + 4(-1)^n = \mathcal{L}_n^2. \quad (2.12)$$

For a real number  $\alpha$ , we write  $\alpha = [a_0, a_1, \dots]$  for the simple continued fraction expansion of  $\alpha$ . That is,

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots}}},$$

where all the  $a_n$  are integers and  $a_n > 0$  for all  $n > 0$  (for further details, see [5]). Basic to our method is a fundamental connection between  $2 \times 2$  matrices and formal continued fractions. This connection has been popularized recently by Stark [6] and by van der Poorten [8] and [9]. Let  $c_0, c_1, \dots, c_N$  be real numbers. Then the *fundamental correspondence* may be stated as follows: If

$$\begin{pmatrix} c_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} c_N & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_N & p_{N-1} \\ q_N & q_{N-1} \end{pmatrix},$$

then

$$\frac{p_N}{q_N} = [c_0, c_1, \dots, c_N].$$

We remark that since  $c_0, c_1, \dots, c_N$  are real numbers,  $p_N / q_N$  may not necessarily be rational.

### 3. THE PROOF OF THEOREM 2

We first consider the case in which  $n$  is even. Let  $\alpha$  be the quadratic irrational defined by

$$\alpha = \overline{a^2 + 1, \{1, a^2\}^{(n-4)/2}, 1, a^2 - 1, a^2 + 1, 1, \{a^2, 1\}^{(n-4)/2}, a^2 + 3}.$$

We will compute  $\alpha$  via the fundamental correspondence between matrices and continued fractions. Thus, if we express the following matrix product as

$$\begin{pmatrix} a^2 + 1 & 1 \\ 1 & 0 \end{pmatrix} \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a^2 & 1 \\ 1 & 0 \end{pmatrix} \right\}^{(n-4)/2} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a^2 - 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a^2 + 1 & 1 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \left\{ \begin{pmatrix} a^2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}^{(n-4)/2} \begin{pmatrix} a^2 + 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix},$$

then it follows that  $\alpha = r / t$ . In view of (2.7), we may express the above as

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} a^2 + 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mathcal{F}_{n-3} & a^{-1}\mathcal{F}_{n-4} \\ a\mathcal{F}_{n-4} & \mathcal{F}_{n-5} \end{pmatrix} \begin{pmatrix} a^2 & 1 \\ a^2 - 1 & 1 \end{pmatrix} \\ \begin{pmatrix} a^2 + 2 & a^2 + 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \mathcal{F}_{n-3} & a\mathcal{F}_{n-4} \\ a^{-1}\mathcal{F}_{n-4} & \mathcal{F}_{n-5} \end{pmatrix} \begin{pmatrix} a^2 + 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}.$$

The functional equation  $\mathcal{F}_k = a\mathcal{F}_{k-1} + \mathcal{F}_{k-2}$  enables us to simplify the above product and carry out the multiplication to deduce

$$\begin{aligned} \begin{pmatrix} r & s \\ t & u \end{pmatrix} &= \begin{pmatrix} \mathcal{F}_{n+1}^2 + 2\mathcal{F}_n^2 & \mathcal{F}_n^2 \\ (a^2 + 4)\mathcal{F}_{n-1}^2 - \mathcal{F}_{n-2}^2 & \mathcal{F}_{n-1}^2 \end{pmatrix} \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} (\mathcal{F}_{n+1}^2 + 2\mathcal{F}_n^2)\alpha + \mathcal{F}_n^2 & \mathcal{F}_{n+1}^2 + 2\mathcal{F}_n^2 \\ ((a^2 + 4)\mathcal{F}_{n-1}^2 - \mathcal{F}_{n-2}^2)\alpha + \mathcal{F}_{n-1}^2 & (a^2 + 4)\mathcal{F}_{n-1}^2 - \mathcal{F}_{n-2}^2 \end{pmatrix} \end{aligned}$$

Thus, we have

$$\alpha = \frac{r}{t} = \frac{(\mathcal{F}_{n+1}^2 + 2\mathcal{F}_n^2)\alpha + \mathcal{F}_n^2}{((a^2 + 4)\mathcal{F}_{n-1}^2 - \mathcal{F}_{n-2}^2)\alpha + \mathcal{F}_{n-1}^2}$$

or, equivalently,

$$((a^2 + 4)\mathcal{F}_{n-1}^2 - \mathcal{F}_{n-2}^2)\alpha^2 + (\mathcal{F}_{n-1}^2 - 2\mathcal{F}_n^2 - \mathcal{F}_{n+1}^2)\alpha - \mathcal{F}_n^2 = 0. \quad (3.1)$$

For ease of exposition, we make the following change of variables: let

$$A = (a^2 + 4)\mathcal{F}_{n-1}^2 - \mathcal{F}_{n-2}^2, \quad B = \mathcal{F}_{n-1}^2 - 2\mathcal{F}_n^2 - \mathcal{F}_{n+1}^2, \quad C = -\mathcal{F}_n^2.$$

Since  $\alpha > 0$ , equation (3.1) gives

$$\alpha = \frac{-B + \sqrt{B^2 - 4AC}}{2A}.$$

Next, if we let  $x = [0, 1, \alpha] = \alpha / (\alpha + 1)$ , then

$$x = \frac{2C - B + \sqrt{B^2 - 4AC}}{2(A - B + C)}.$$

The expressions  $2C - B$ ,  $B^2 - 4AC$ , and  $A - B + C$  may be simplified slightly by successive applications of the functional equation for  $\mathcal{F}_n$ . It is an algebraically complicated but straightforward task to verify that

$$x = \frac{\mathcal{F}_n}{2} \left( \frac{a(a\mathcal{F}_n + 2\mathcal{F}_{n-1}) + \sqrt{(a^2 + 4)(4\mathcal{F}_{n+1}\mathcal{F}_{n-1} + a^2\mathcal{F}_n^2)}}{4\mathcal{F}_{n+1}\mathcal{F}_{n-1} + a^2\mathcal{F}_n^2} \right). \quad (3.2)$$

Finally, by (2.8) and (2.9), we have

$$\mathcal{L}_n^2 = (a\mathcal{F}_n + 2\mathcal{F}_{n-1})^2 = 4\mathcal{F}_{n+1}\mathcal{F}_{n-1} + a^2\mathcal{F}_n^2,$$

and therefore, (3.2) implies

$$x = \frac{\mathcal{F}_n (a\mathcal{L}_n + \mathcal{L}_n \sqrt{a^2 + 4})}{2\mathcal{L}_n^2} = \frac{\mathcal{F}_n (a + \sqrt{a^2 + 4})}{2\mathcal{L}_n} = \frac{\mathcal{F}_n}{\mathcal{L}_n} \varphi_a,$$

which, by (1.4), is precisely equation (1.2) for even  $n$ .

The proof of (1.2) for  $n$  odd is similar to the even case given above. In particular, for  $n$  odd, we let

$$\alpha = \left[ a^2 + 1, \{1, a^2\}^{(n-5)/2}, 1, a^2 + 1, a^2 - 1, 1, \{a^2, 1\}^{(n-3)/2}, a^2 + 3 \right].$$

Thus, in the language of matrices, we have

$$\begin{pmatrix} a^2+1 & 1 \\ 1 & 0 \end{pmatrix} \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a^2 & 1 \\ 1 & 0 \end{pmatrix} \right\}^{(n-5)/2} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a^2+1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a^2-1 & 1 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \left\{ \begin{pmatrix} a^2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}^{(n-3)/2} \begin{pmatrix} a^2+3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

with  $\alpha = r/t$ . Simplifying the matrix product, as in the case for  $n$  even, reveals

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} \mathcal{F}_{n+1}^2 + 2\mathcal{F}_n^2 & \mathcal{F}_n^2 \\ (a^2+4)\mathcal{F}_{n-1}^2 - \mathcal{F}_{n-2}^2 & \mathcal{F}_{n-1}^2 \end{pmatrix} \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}.$$

Equation (1.2) for  $n$  odd now follows from the previous argument.

Equation (1.3) follows immediately from (1.2) and Theorem 11 of [4], which completes the proof.

#### 4. THE PROOF OF THEOREM 3

We essentially adopt the argument used in the proof of Theorem 2. First, we consider the case in which  $n$  is even. Let  $\alpha$  be the quadratic irrational defined by

$$\alpha = \overline{[3, \{1\}^{n-2}, L_{2n}-2, 2, \{1\}^{n-4}, 2, 1, L_{2n}-2]}.$$

By the fundamental correspondence between matrices and continued fractions, we observe that if we express the following matrix product as

$$\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n-2} \begin{pmatrix} L_{2n}-2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n-4} \\ \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} L_{2n}-2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix}, \quad (4.1)$$

then we have  $\alpha = r/t$ . Using (2.1), (2.2), (2.3), and (2.4) together with the fact that  $n$  is even, we multiply and simplify the products within the parentheses to produce

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} L_{3n}-L_{n-2} & L_n \\ F_{3n-1}+2F_{n-2} & F_{n-1} \end{pmatrix} \begin{pmatrix} L_{3n}-F_{n-1} & L_n \\ L_{3n-2}+F_{n+3}+L_{n-3} & L_{n-2} \end{pmatrix} \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} \\ = \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}, \quad (4.2)$$

where

$$\begin{aligned} k_1 &= L_{6n} - F_{4n-1} - F_{2n+1} + 1, \\ k_2 &= L_{3n}L_n, \\ k_3 &= (F_{3n-1} + 2F_{n-2})(L_{3n} - F_{n-1}) + F_{n-1}(L_{3n-2} + F_{n+3} + L_{n-3}), \\ k_4 &= F_{4n-1} + F_{2n+1} - 1. \end{aligned} \quad (4.3)$$

We note that identities (4.1) and (4.2) lead to a complicated, but useful, identity involving Fibonacci and Lucas numbers. In particular, we observe that

$$\det \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} = (-1)^{2n},$$

and thus we have

$$k_1 k_4 - k_2 k_3 = 1. \quad (4.4)$$

By identity (4.2), we have

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} k_1 \alpha + k_2 & k_1 \\ k_3 \alpha + k_4 & k_2 \end{pmatrix},$$

and since  $\alpha = r/t$ , this implies

$$\alpha = \frac{k_1 \alpha + k_2}{k_3 \alpha + k_4}.$$

Therefore,  $k_3 \alpha^2 + (k_4 - k_1) \alpha - k_2 = 0$ , hence,

$$\alpha = \frac{k_1 - k_4 + \sqrt{(k_4 - k_1)^2 + 4k_2 k_3}}{2k_3}.$$

If we now let  $x = [F_{n+1} - 1, \alpha]$ , then

$$\begin{aligned} x &= F_{n+1} - 1 + \frac{2k_3}{k_1 - k_4 + \sqrt{(k_4 - k_1)^2 + 4k_2 k_3}} \\ &= F_{n+1} - 1 + \frac{k_1 - k_4 - \sqrt{(k_4 - k_1)^2 + 4k_2 k_3}}{-2k_2}. \end{aligned} \quad (4.5)$$

By (4.3), we note that  $k_1 + k_4 = L_{6n}$ . This, together with (4.4), reveals that

$$\begin{aligned} (k_4 - k_1)^2 + 4k_2 k_3 &= (k_4 + k_1)^2 - 4k_1 k_4 + 4k_2 k_3 \\ &= L_{6n}^2 - 4(k_1 k_4 - k_2 k_3) = L_{6n}^2 - 4. \end{aligned}$$

In view of (2.5) and the fact that  $n$  is even, we may express the above as  $(k_4 - k_1)^2 + 4k_2 k_3 = 5F_{6n}^2$ .

This, along with (4.5), (2.2), (2.3), (2.4), and (2.6), yields

$$\begin{aligned} [F_{2n+1} - 1, \alpha] &= F_{2n+1} - 1 + \frac{L_{6n} - 2F_{4n-1} - 2F_{2n+1} + 2 - \sqrt{5}F_{6n}}{-2(L_{3n}L_n)} \\ &= \frac{-2F_{2n+1}L_{3n}L_n + 2L_{3n}L_n + L_{6n} - 2F_{4n-1} - 2F_{2n+1} + 2 + \sqrt{5}F_{6n}}{-2(L_{3n}L_n)} \\ &= \frac{-F_{6n} - \sqrt{5}F_{6n}}{-2L_{3n}L_n} = \frac{L_{3n}F_{3n} + L_{3n}F_{3n}\sqrt{5}}{2L_{3n}L_n} = \frac{F_{3n} + F_{3n}\sqrt{5}}{2L_n} = \frac{F_{3n}}{L_n} \varphi, \end{aligned}$$

which completes the proof for  $n$  even.

The proof for  $n$  odd is similar to the even case given above with the exception that the change of variables of (4.3) is replaced by

$$\begin{aligned} k_1 &= L_{6n} - F_{4n+1} - F_{2n-1} - 1, \\ k_2 &= L_{3n}L_n, \\ k_3 &= F_{3n+1}(L_{3n} - F_{n+1}) + F_{n+1}(L_{3n-1} + L_{n+1} + F_{n-2}), \\ k_4 &= F_{4n+1} - F_{2n-1} + 1. \end{aligned}$$

### 5. THE PROOF OF THEOREM 6

It is a classical result from the theory of continued fractions that  $\alpha$  and  $\beta$  are equivalent numbers if and only if there exist integers  $a$ ,  $b$ ,  $c$ , and  $d$  so that  $\alpha = (a\beta + b)/(c\beta + d)$  with  $ad - bc = \pm 1$  (see [5]). Since  $m$  and  $n$  are relatively prime positive integers, we may find positive integers  $x$  and  $y$  so that  $nx - my = 1$ . Thus, if we let  $k = 2ym$ , then we also have  $k = 2xn - 2$ . We now define

$$a = \frac{\mathcal{L}_m \mathcal{F}_{k+2}}{\mathcal{L}_n}, \quad b = c = \mathcal{F}_{k+1}, \quad d = \frac{\mathcal{L}_n \mathcal{F}_k}{\mathcal{L}_m}.$$

As we remarked in the introduction, since  $\mathcal{F}_{k+2} = \mathcal{F}_{(2x)n}$  and  $\mathcal{F}_k = \mathcal{F}_{(2y)m}$ ,  $\mathcal{F}_{k+2}/\mathcal{L}_n$  and  $\mathcal{F}_k/\mathcal{L}_m$  are both integers. Thus,  $a$ ,  $b$ ,  $c$ , and  $d$  are all integers. Also, by (2.10), we note that

$$ad - bc = \mathcal{F}_k \mathcal{F}_{k+2} - \mathcal{F}_{k+1}^2 = (-1)^{k+1} = \pm 1.$$

Next, in light of (2.11), we have

$$\frac{a \left( \frac{\mathcal{L}_n}{\mathcal{L}_m} \varphi_a \right) + b}{c \left( \frac{\mathcal{L}_n}{\mathcal{L}_m} \varphi_a \right) + d} = \frac{\mathcal{L}_m}{\mathcal{L}_n} \left( \frac{\mathcal{F}_{k+2} \varphi_a + \mathcal{F}_{k+1}}{\mathcal{F}_{k+1} \varphi_a + \mathcal{F}_k} \right) = \frac{\mathcal{L}_m}{\mathcal{L}_n} \varphi_a.$$

Hence,  $(\mathcal{L}_m / \mathcal{L}_n) \varphi_a$  and  $(\mathcal{L}_n / \mathcal{L}_m) \varphi_a$  are equivalent numbers.

### 6. A RELATED CLASS OF QUADRATIC IRRATIONALS

For integers  $n > 2$  and  $m > 0$ , we define the quadratic irrational  $\mathcal{R}(n, m) = \mathcal{R}(a; n, m)$  by

$$\mathcal{R}(n, m) = \frac{a\mathcal{F}_n + \mathcal{L}_m \sqrt{a^2 + 4}}{2}.$$

It will also be useful to define the integer  $N = N(n, m)$  to be  $N = a\mathcal{F}_n + (a^2 + 4)\mathcal{F}_m$ . We now examine the continued fraction expansion for  $\mathcal{R}(n, m)$ . We consider separately the case of  $N$  even and the case of  $N$  odd. As will be evident, the case of  $N$  odd is substantially more complicated than the case of  $N$  even.

**Theorem 7:** If  $N$  is even, then

(i) if  $m$  is even,

$$\mathcal{R}(n, m) = \left[ N/2, \overline{\mathcal{F}_m, (a^2 + 4)\mathcal{F}_m} \right];$$

(ii) if  $m$  is odd and  $\mathcal{F}_m > 2$ ,

$$\mathcal{R}(n, m) = \left[ (N-2)/2, 1, \overline{\mathcal{F}_m-2, 1, (a^2 + 4)\mathcal{F}_m-2} \right].$$

**Theorem 8:** If  $N$  is odd, then

(i) if  $m$  is even,  $\mathcal{F}_m \equiv 0 \pmod{4}$  and  $\mathcal{F}_m > 4$ ,

$$\mathcal{R}(n, m) = \left[ (N-1)/2, 1, 1, \overline{(\mathcal{F}_m-4)/4, 1, 1, (a^2 + 4)\mathcal{F}_m-1} \right];$$

(ii) if  $m$  is even,  $\mathcal{F}_m \equiv 1 \pmod{4}$  and  $\mathcal{F}_m > 5$ ,

$$\mathcal{R}(n, m) = \left[ (N-1)/2, \overline{\mathcal{W}_1, 4\mathcal{F}_m}, \mathcal{W}_1, (\alpha^2 + 4)\mathcal{F}_m - 1 \right],$$

where  $\mathcal{W}_1 = (1, 1, (\mathcal{F}_m - 5)/4, 1, 3, ((\alpha^2 + 4)\mathcal{F}_m - 1)/4)$ ;

(iii) if  $m$  is even,  $\mathcal{F}_m \equiv 3 \pmod{4}$  and  $\mathcal{F}_m > 3$ ,

$$\mathcal{R}(n, m) = \left[ (N-1)/2, \overline{\mathcal{W}_2, 4\mathcal{F}_m}, \mathcal{W}_2, (\alpha^2 + 4)\mathcal{F}_m - 1 \right],$$

where  $\mathcal{W}_2 = (1, 1, (\mathcal{F}_m - 3)/4, 3, 1, ((\alpha^2 + 4)\mathcal{F}_m - 3)/4)$ ;

(iv) if  $m$  is odd,  $\mathcal{F}_m \equiv 1 \pmod{4}$  and  $\mathcal{F}_m > 5$ ,

$$\mathcal{R}(n, m) = \left[ (N-1)/2, \overline{\mathcal{W}_3, \mathcal{F}_m - 1}, \mathcal{W}_3, (\alpha^2 + 4)\mathcal{F}_m - 1 \right],$$

where  $\mathcal{W}_3 = (2, (\mathcal{F}_m - 5)/4, 1, 2, 1, ((\alpha^2 + 4)\mathcal{F}_m - 5)/4, 2)$ ;

(v) if  $m$  is odd,  $\mathcal{F}_m \equiv 2 \pmod{4}$  and  $\mathcal{F}_m > 6$ ,

$$\mathcal{R}(n, m) = \left[ (N-1)/2, \overline{\mathcal{W}_4, 4(\alpha^2 + 4)\mathcal{F}_m - 2}, \mathcal{W}_4, (\alpha^2 + 4)\mathcal{F}_m - 1 \right],$$

where  $\mathcal{W}_4 = (2, (\mathcal{F}_m - 6)/4, 1)$ .

Since the proof of Theorem 8 involves the same ideas as the proof of Theorem 7, we include only the (less complicated) proof of Theorem 7. Before proceeding with the proof of Theorem 7, we make three remarks.

First, it may appear that Theorem 8 is not complete in the sense that three cases seem to be missing; in particular, the cases:  $m$  even,  $\mathcal{F}_m \equiv 2 \pmod{4}$ ;  $m$  odd,  $\mathcal{F}_m \equiv 0 \pmod{4}$ ;  $m$  odd,  $\mathcal{F}_m \equiv 3 \pmod{4}$ . It is a straightforward calculation to verify that none of these cases can occur when  $N$  is odd. For example, one has that  $\mathcal{F}_m \equiv 2 \pmod{4}$  only if either  $\alpha \equiv 1 \pmod{4}$  and  $m \equiv 3 \pmod{6}$  or  $\alpha \equiv 3 \pmod{4}$  and  $m \equiv 3 \pmod{6}$  or  $\alpha \equiv 2 \pmod{4}$  and  $m \equiv 2 \pmod{4}$ . In the first two cases,  $m$  is odd, and in the third case  $\alpha$  is even; thus,  $N$  must be even. So if  $\mathcal{F}_m \equiv 2 \pmod{4}$ , then we cannot have both  $m$  even and  $N$  odd. Similarly, the other two remaining cases may be shown not to occur. Therefore, Theorem 8 gives the complete situation for odd  $N$ . Our second remark involves the numbers  $((\alpha^2 + 4)\mathcal{F}_m - 1)/4$ ,  $((\alpha^2 + 4)\mathcal{F}_m - 3)/4$ , and  $((\alpha^2 + 4)\mathcal{F}_m - 5)/4$  occurring in cases (ii), (iii), and (iv), respectively. Of course, we must require that these be integers. It is easy to see that each is an integer in the appropriate case if and only if  $\alpha$  is odd. However, again, if  $\alpha$  were even, then  $N$  would be even and Theorem 7 would apply. Hence, if  $N$  is odd, then  $\alpha$  is also odd; therefore, the three numbers above are indeed integers as required. Third, we note that the period length for  $\mathcal{R}(n, m)$  is either 2, 4, 6, 8, 14, or 16. This proves an observation made by Long [2] that the period is always even, but it also shows that the period length is, in fact, a bounded function of  $\alpha$ ,  $n$ , and  $m$  which Long believed not to be the case.

**Proof of Theorem 7:** We consider first the case of  $m$  even and let

$$\alpha = \left[ N/2, \overline{\mathcal{F}_m}, (\alpha^2 + 4)\mathcal{F}_m \right].$$

We now examine the corresponding matrix product:



$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} N/2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mathcal{F}_m & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} (\alpha^2 + 4)\mathcal{F}_m & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} (\alpha^2 + 4)\mathcal{F}_m + \alpha - N/2 & 1 \\ 1 & 0 \end{pmatrix}.$$

It follows that  $\alpha = r/t$ , in particular,

$$\alpha = \frac{(N\mathcal{F}_m/2 + 1)((\alpha^2 + 4)\mathcal{F}_m + \alpha - N/2) + N/2}{\mathcal{F}_m((\alpha^2 + 4)\mathcal{F}_m + \alpha - N/2) + 1}.$$

Thus, we have

$$\begin{aligned} \mathcal{F}_m \alpha^2 + (\mathcal{F}_m((\alpha^2 + 4)\mathcal{F}_m - N/2) - N\mathcal{F}_m/2)\alpha \\ + (N/2)^2 \mathcal{F}_m - (\alpha^2 + 4)\mathcal{F}_m - N(\alpha^2 + 4)\mathcal{F}_m^2/2 = 0 \end{aligned}$$

which, together with our definition of  $N$  yields

$$\alpha = \frac{\alpha\mathcal{F}_m + \sqrt{((\alpha^2 + 4)\mathcal{F}_m^2 + 4)(\alpha^2 + 4)}}{2}.$$

As  $m$  is even, identity (2.12) becomes  $(\alpha^2 + 4)\mathcal{F}_m^2 + 4 = \mathcal{L}_m^2$ ; hence,  $\alpha = \mathcal{R}(n, m)$ .

If  $m$  is odd, we again let

$$\alpha = \left[ (N-2)/2, 1, \overline{\mathcal{F}_m - 2, 1, (\alpha^2 + 4)\mathcal{F}_m - 2} \right],$$

and proceed in a similar manner to deduce

$$\alpha = \frac{N - (\alpha^2 + 4)\mathcal{F}_m + \sqrt{((\alpha^2 + 4)\mathcal{F}_m^2 - 4)(\alpha^2 + 4)}}{2}.$$

In view of identity (2.12) with  $m$  odd, together with the definition of  $N$ , we have  $\alpha = \mathcal{R}(n, m)$ , which completes the proof.

As a consequence of the two previous theorems and a result of Long [2], we are able to deduce immediately the continued fraction expansion for numbers of the form

$$\mathcal{S}(n, m) = \frac{\alpha\mathcal{L}_n + \mathcal{L}_m\sqrt{\alpha^2 + 4}}{2}.$$

Long proved (Theorem 8, [2]) that the continued fraction expansions of  $\mathcal{R}(n, m)$  and  $\mathcal{S}(n, m)$  are identical after the first partial quotient. In view of the two theorems of this section, it appears clear that one may explicitly express the continued fraction expansion for

$$\frac{\alpha\mathcal{F}_n + \mathcal{L}_m\sqrt{\alpha^2 + 4}}{2}$$

and, thus, by Theorem 9 of [2], the expansion for

$$\frac{\alpha\mathcal{F}_n + \mathcal{F}_m\sqrt{\alpha^2 + 4}}{2}.$$

It seems very reasonable to conjecture that these period lengths will again be even and bounded.

## ACKNOWLEDGMENT

Part of the work herein resulted from the Number Theory Group [1] of the Williams College SMALL Undergraduate Research Project, Summer 1993. The Group members were Christopher French, Christopher Kollett, Michael Pelsmayer, Jeffrey Vander Clute, and Aaron Williams, with Edward Burger as the faculty advisor. Research was supported, in part, by a grant from The National Science Foundation Research Experiences for Undergraduates Program.

## REFERENCES

1. C. French, C. Kollett, M. Pelsmayer, J. Vander Clute, & A. Williams. "Recurrence Relations and Simple Continued Fractions." SMALL Undergraduate Research Project Report, Williams College, 1993.
2. C. T. Long. "A Limited Arithmetic on Simple Continued Fractions—III." *The Fibonacci Quarterly* **19.2** (1981):163-75.
3. C. T. Long & J. H. Jordan. "A Limited Arithmetic on Simple Continued Fractions." *The Fibonacci Quarterly* **5.2** (1967):113-28.
4. C. T. Long & J. H. Jordan. "A Limited Arithmetic on Simple Continued Fractions—II." *The Fibonacci Quarterly* **8.2** (1970):135-57.
5. C. D. Olds. *Continued Fractions*. Washington, D.C.: Mathematical Association of America, 1963.
6. H. M. Stark. *An Introduction to Number Theory*. Cambridge, MA: The MIT Press, 1991.
7. S. Vajda. *Fibonacci and Lucas Numbers, and the Golden Section: Theory and Applications*. New York: Halsted Press, 1989.
8. A. J. van der Poorten. "An Introduction to Continued Fractions." In *Diophantine Analysis*, ed. J. H. Loxton and A. J. van der Poorten. London Math. Soc. Lecture Note Series 109. Cambridge: Cambridge University Press, 1986.
9. A. J. van der Poorten. "Fractions of the Period of the Continued Fraction Expansion of Quadratic Integers." *Bull. Austral. Math. Soc.* **44** (1991):155-69.

AMS Classification Numbers: 11A55, 11J70



# AN EXTENSION OF STIRLING NUMBERS

**David Branson**

Department of Mathematics, University of Essex, Wivenhoe Park, Colchester CO4 3SQ, England

(Submitted August 1994)

## 1. INTRODUCTION

Stirling numbers may be defined as the coefficients in an expansion of positive integral powers of a variable in terms of factorial powers, or vice-versa:

$$(x)_n = \sum_{k=0}^n s(n, k)x^k, \quad n \geq 0, \quad (1.1)$$

$$x^n = \sum_{k=0}^n S(n, k)(x)_k, \quad n \geq 0, \quad (1.2)$$

where

$$\begin{aligned} (x)_n &= x(x-1) \cdots (x-n+1), \quad n \geq 1, \\ (x)_0 &= 1. \end{aligned} \quad (1.3)$$

The numbers  $s(n, k)$  and  $S(n, k)$  are, in the notation of Riordan [6], Stirling numbers of the first and second kind, respectively.

Writing (1.3) as

$$(x)_n = \Gamma(x+1) / \Gamma(x-n+1) \quad (1.4)$$

we may generalize factorial powers to negative integral values of  $n$ :

$$(x)_{-n} = \frac{1}{(x+1)(x+2) \cdots (x+n)}, \quad n \geq 1.$$

The question then arises as to whether we can extend Stirling numbers to negative integral values of one or both of their arguments. Several authors have discussed the case where both  $n$  and  $k$  are negative integers (for a brief history, see Knuth [4]), and we briefly discuss this case in Section 3. We shall refer to such numbers as Negative-Negative Stirling Numbers (NNSN) whereas we call the numbers defined by (1.1) and (1.2) Positive-Positive Stirling Numbers (PPSN). It is clearly impossible to have an expansion of the form (1.1) or (1.2), where  $n$  is a positive integer and  $k$  is summed over negative values: in the first case, the left-hand side is a polynomial whereas the right-hand side has a singularity at  $x=0$ ; in the second case, taking the limit as  $x$  goes to infinity, the left-hand side goes to infinity whereas the right-hand side goes to zero (for a proof of the uniform convergence required to take the limit term-by-term, see, for example, Milne-Thomson [5]). However, it is possible to extend (1.1) and (1.2) to the case where  $n$  is a negative integer and  $k$  is summed over positive integers. We call the resulting coefficients Negative-Positive Stirling Numbers (NPSN), and the purpose of this article is to discuss these numbers and some of their properties.

In Section 2 we summarize some well-known properties of PPSN. In Section 3 we describe four urn models: the first two illustrate PPSN and the second two demonstrate the connection between NNSN and PPSN. We define NPSN in Section 4 and obtain explicit expressions for them by means of two further urn models. Finally, in Section 5 we give some alternative representations of NPSN, tabulate some values and derive some properties.

## 2. PROPERTIES OF POSITIVE-POSITIVE STIRLING NUMBERS

In this section we list, for future reference, some well-known properties of PPSN. For more details, see, for example, Jordan [3], Chapter IV.

By using the definition (1.1) and the identity

$$(x)_{n+1} = (x)_n(x-n), \quad (2.1)$$

and by equating coefficients of powers of  $x$ , we may derive the recurrence relation

$$s(n+1, k) = s(n, k-1) - ns(n, k). \quad (2.2)$$

Similarly, the definition (1.2) and the identity

$$x^{n+1} = x^n(x-k+k), \quad (2.3)$$

and the equating of factorial powers of  $x$ , leads to

$$S(n+1, k) = S(n, k-1) + kS(n, k). \quad (2.4)$$

Numerical values for PPSN may readily be generated using (2.2) or (2.4) together with the boundary values [which follow immediately from (1.1) and (1.2)]

$$s(n, n) = 1, \quad s(n+1, 0) = 0, \quad n \geq 0, \quad (2.5)$$

$$S(n, n) = 1, \quad S(n+1, 0) = 0, \quad n \geq 0. \quad (2.6)$$

We may define a generating function for  $S(n, k)$  (with respect to  $n$ ) by

$$A_k(t) = \sum_{n=k}^{\infty} t^n S(n, k).$$

By using (2.4), we can obtain a first-order linear difference equation for  $A_k$  which, with the initial condition  $A_0(t) = 1$ , can be solved to give

$$\frac{t^k}{(1-t)(1-2t) \cdots (1-kt)} = \sum_{n=k}^{\infty} t^n S(n, k), \quad k \geq 1. \quad (2.7)$$

The left-hand side of (2.7) can be expressed in partial fractions:

$$\frac{1}{k!} \sum_{r=0}^k (-1)^{k-r} \binom{k}{r} \frac{1}{1-rt}.$$

Expanding the last factor by the binomial theorem and comparing with (2.7) gives the following representation, known as Stirling's formula:

$$S(n, k) = \frac{1}{k!} \sum_{r=1}^k (-1)^{k-r} \binom{k}{r} r^n. \quad (2.8)$$

## 3. URN MODELS AND STIRLING NUMBERS

In all the models of this section and the next, an urn contains white balls and black balls. Some, but not necessarily all, of the balls are of unit mass. Balls are drawn one at a time with replacement, and the probability that a particular ball is drawn is proportional to its mass.

**Model A**

An urn originally contains only white balls of total mass  $x$  ( $> n-1$ ) including at least  $n-1$  balls of unit mass. We successively draw  $n$  balls with replacement. After a white ball is drawn (and replaced) and before the next ball is drawn, we substitute a unit mass white ball in the urn by a unit mass black ball. Then the probability that the number of white balls drawn is  $k$  is equal to

$$P_n^A(k) = \sum \frac{x}{x} \left(\frac{1}{x}\right)^{a_1} \frac{x-1}{x} \left(\frac{2}{x}\right)^{a_2} \frac{x-2}{x} \cdots \left(\frac{k-1}{x}\right)^{a_{k-1}} \frac{x-k+1}{x} \left(\frac{k}{x}\right)^{a_k}, \quad a \leq k \leq n, \quad (3.1)$$

where the sum is over all nonnegative integers  $a_i$  satisfying  $a_1 + \cdots + a_k = n-k$ . It is clear that, for  $n \geq 1$ ,  $P_n^A(0) = 0$ , so (3.1) may be rewritten as

$$P_n^A(k) = \frac{(x)_k}{x^n} b(n, k), \quad (3.2)$$

with

$$b(n, k) = \sum u_1 u_2 \cdots u_{n-k}, \quad 1 \leq k < n, \quad (3.3)$$

where the sum is over all integers  $u_i$  ( $i = 1, 2, \dots, n-k$ ) satisfying

$$1 \leq u_1 \leq u_2 \leq \cdots \leq u_{n-k} \leq k; \\ b(n, 0) = 0, \quad b(n, n) = 1.$$

In terms of the urn model, if  $n = 0$ , then certainly  $k = 0$ , so (3.2) continues to hold if we put  $b(0, 0) = 1$ .

From the condition  $\sum_{k=0}^n P_n^A(k) = 1$  and equation (3.2), we deduce

$$x^n = \sum_{k=0}^n (x)_k b(n, k).$$

Comparing this expression with (1.2), we conclude that a representation for  $S(n, k)$  is provided by

$$S(n, k) = b(n, k). \quad (3.4)$$

**Model B**

An urn originally contains only white balls of total mass  $y$ . We successively draw  $n$  balls with replacement. After each ball is drawn (and replaced) and before the next ball is drawn, we add one black ball of unit mass to the urn. The probability that the number of white balls drawn is  $k$  is equal to

$$P_n^B(k) = \frac{y^k \sum v_1 v_2 \cdots v_{n-k}}{y(y+1) \cdots (y+n-1)}, \quad 1 \leq k < n, \quad (3.5)$$

where the sum is over all integers  $v_i$  ( $i = 1, 2, \dots, n-k$ ) satisfying

$$1 \leq v_1 < v_2 < \cdots < v_{n-k} \leq n-1. \quad (3.6)$$

The factors in the denominator of (3.5) represent the total mass of the balls in the urn at successive drawings; the factor  $y^k$  arises from drawing a white ball on  $k$  occasions, and the factor  $v_i$  arises from the drawing of a black ball at a time when the urn contains  $v_i$  black balls.

Note that, for  $n \geq 1$ ,  $P_n^B(0) = 0$  and  $P_n^B(n) = y^n / [y(y+1) \cdots (y+n-1)]$ , so that (3.5) may be written as

$$P_n^B(k) = \frac{y^k c(n, k)}{y(y+1) \cdots (y+n-1)}, \quad 0 \leq k \leq n, \quad (3.7)$$

with

$$c(n, k) = \sum v_1 v_2 \cdots v_{n-k}, \quad 1 \leq k < n, \quad (3.8)$$

under the restriction (3.6);  $c(n, 0) = 0$ ,  $c(n, n) = 1$ .

Putting  $y = -x$ , (3.7) may be written as

$$P_n^B(k) = \frac{x^k}{(x)_n} (-1)^{n+k} c(n, k). \quad (3.9)$$

As in Model A, if  $n = 0$  then  $k = 0$ , so (3.9) holds if  $c(0, 0) = 1$ . The probabilities in (3.9) must add to one; hence,

$$(x)_n = \sum_{k=0}^n x^k (-1)^{n+k} c(n, k).$$

Comparing this with (1.1), we see that

$$s(n, k) = (-1)^{n+k} c(n, k) \quad (3.10)$$

where  $c(n, k)$  is given by (3.8).

The PPSN representations derived above by means of Model A and Model B are, of course, well known and have been derived by other methods (see, for example, Jordan [3]). We now consider two urn models of relevance to Negative-Negative Stirling Numbers. By analogy with (1.1) and (1.2) the NNSN of the first and second kind, respectively, are defined by

$$(x)_{-n} = \sum_{k=0}^{\infty} s(-n, -k) x^{-k}, \quad n \geq 0, \quad (3.11)$$

$$x^{-n} = \sum_{k=0}^{\infty} S(-n, -k) (x)_{-k}, \quad n \geq 0. \quad (3.12)$$

### Model C

The situation here is the same as in Model B except that now we continue to draw balls until we have drawn  $n+1$  white balls. The probability that the total number of balls drawn is  $k+1$  is equal to

$$P_{n+1}^C(k+1) = \frac{y^{n+1} \sum v_1 v_2 \cdots v_{k-n}}{y(y+1) \cdots (y+k)}, \quad 1 \leq n < k, \quad (3.13)$$

where  $1 \leq v_1 < v_2 < \cdots < v_{k-n} \leq k-1$ . If all the balls drawn are white, we have

$$P_{n+1}^C(n+1) = y^{n+1} / [y(y+1) \cdots (y+n)]$$

whereas, if  $n = 0$ , then certainly  $k = 0$ . It follows from (3.8) that (3.13) may be written as

$$P_{n+1}^C(k+1) = y^n (y)_{-k} c(k, n), \quad 0 \leq n \leq k. \quad (3.14)$$

Suppose that after the  $(i+1)^{\text{th}}$  ball is drawn all the remaining balls drawn are black. The probability of this event is given by the infinite product

$$\prod_{m=1}^{\infty} \frac{i+m}{y+i+m} = \prod_{m=1}^{\infty} \left( 1 - \frac{y}{y+i+m} \right) = 0$$

(see, for example, Ferrar [2], p. 147). It follows that the probability distribution (3.14) is proper and sums to one. Hence,

$$y^{-n} = \sum_{k=n}^{\infty} (y)_{-k} c(k, n).$$

The coefficients in an expansion such as this are unique (see Milne-Thomson [5], p. 288), so, by comparison with (3.12) and using (3.10), we see that

$$S(-n, -k) = c(k, n) = (-1)^{n+k} s(k, n), \quad 0 \leq n \leq k \quad (3.15)$$

[and  $S(-n, -k) = 0$  for  $0 \leq k < n$ ].

#### Model D

This is the same as Model A, except that the white balls originally in the urn have total mass  $x$  ( $> n$ ) and include at least  $n$  balls of unit mass. We now continue to draw balls until we have drawn  $n+1$  white balls. The probability that the total number of balls drawn is  $k+1$  is equal to

$$P_{n+1}^D(k+1) = \sum \frac{x}{x} \left( \frac{1}{x} \right)^{a_1} \frac{x-1}{x} \left( \frac{2}{x} \right)^{a_2} \frac{x-2}{x} \dots \left( \frac{n}{x} \right)^{a_n} \frac{x-n}{x}, \quad 0 \leq n \leq k,$$

where  $a_1 + \dots + a_n = k - n$ .

Using the notation of (3.3), we can write

$$P_{n+1}^D(k+1) = \frac{x(x-1) \dots (x-n) b(k, n)}{x^{k+1}}, \quad 0 \leq n \leq k. \quad (3.16)$$

The probability that after the  $i^{\text{th}}$  white ball is drawn all the remaining balls drawn are black is

$$\lim_{m \rightarrow \infty} \left( \frac{i}{x} \right)^m = 0,$$

so the probability distribution (3.16) is proper and sums to one.

Putting  $x = -y$ , (3.16) may be written as

$$P_{n+1}^D(k+1) = \frac{(-1)^{n+k}}{(y)_{-n} y^k} b(k, n), \quad 0 \leq n \leq k.$$

If we sum over  $k$  and rearrange this equation, we obtain

$$(y)_{-n} = \sum_{k=n}^{\infty} y^{-k} (-1)^{n+k} b(k, n).$$

Comparing this with (3.11) (using the uniqueness of Laurent series coefficients) and using (3.4), we conclude

$$s(-n, -k) = (-1)^{n+k} b(k, n) = (-1)^{n+k} S(k, n), \quad 0 \leq n \leq k, \quad (3.17)$$

[and  $s(-n, -k) = 0$  for  $0 \leq k < n$ ].

Equations (3.15) and (3.17) show the interesting fact, noted by other authors (see Knuth [4]), that, apart from a sign, NNSN of the first (second) kind are obtained from PPSN of the second (first) kind by a reflection in the line  $n = -k$ .

#### 4. NEGATIVE-POSITIVE STIRLING NUMBERS

Negative-Positive Stirling Numbers of the first and second kind may be defined by the obvious modifications of (1.1) and (1.2), respectively:

$$(x)_{-n} = \sum_{k=0}^{\infty} s(-n, k)x^k, \quad n \geq 1, \quad (4.1)$$

$$x^{-n} = \sum_{k=1}^{\infty} S(-n, k)(x)_k, \quad n \geq 0. \quad (4.2)$$

(The reason for the limits on  $n$  and  $k$  will become clear later.)

Two further urn models allow us to give explicit representations for these NPSN.

##### Model E

Originally the urn contains white balls of mass  $x$  ( $< 1$ ) and black balls of mass  $1-x$ . Balls are drawn one at a time with replacement. After a black ball is drawn (and replaced) and before the next ball is drawn, we add one black ball of unit mass to the urn. We continue until  $n+1$  white balls have been drawn. For  $n \geq 0$ , the probability that the number of black balls drawn is  $k-1$  is equal to

$$P_{n+1}^E(k-1) = \sum \left( \frac{x}{1} \right)^{a_1} \frac{1-x}{1} \left( \frac{x}{2} \right)^{a_2} \frac{2-x}{2} \cdots \left( \frac{x}{k-1} \right)^{a_{k-1}} \frac{k-1-x}{k-1} \left( \frac{x}{k} \right)^{a_{k+1}}, \quad k \geq 2,$$

where the sum is over all nonnegative integers  $a_i$  satisfying  $a_1 + \cdots + a_k = n$ ; if all the balls drawn are white, then  $P_{n+1}^E(0) = x^{n+1}$ . We may therefore write

$$P_{n+1}^E(k-1) = x^n (x)_k (-1)^{k-1} a(n, k) / k! \quad (4.3)$$

with

$$a(n, k) = \sum \frac{1}{u_1 u_2 \cdots u_n}, \quad n \geq 1, \quad (4.4)$$

where the sum is over all integers  $u_i$  ( $i = 1, 2, \dots, n$ ) satisfying

$$1 \leq u_1 \leq u_2 \leq \cdots \leq u_n \leq k; \\ a(0, k) = 1.$$

The probability that after the  $i^{\text{th}}$  black ball is drawn all the remaining balls drawn are black is

$$\prod_{m=1}^{\infty} \frac{i+m-x}{i+m} = \prod_{m=1}^{\infty} \left( 1 - \frac{x}{i+m} \right) = 0.$$

We conclude that the probabilities in (4.3) sum to one, and hence,

$$x^{-n} = \sum_{k=1}^{\infty} (x)_k (-1)^{k-1} a(n, k) / k!. \quad (4.5)$$



An expansion of  $x^{-n}$  of this form in terms of factorial powers  $(x)_k$  has unique coefficients. The reason for this is that we have effectively put the coefficient of  $(x)_0$  equal to zero (see Milne-Thomson [5], pp. 305-06).

Comparison of (4.5) and (4.2) gives

$$S(-n, k) = (-1)^{k-1} a(n, k) / k!, \quad (4.6)$$

with  $a(n, k)$  given by (4.4).

### Model F

The rules for this model are the same as for Model E, except that now we continue until  $n$  black balls have been drawn. For  $n \geq 1$ , the probability that the number of white balls drawn is  $k$  is equal to

$$P_n^F(k) = \sum \left( \frac{x}{1} \right)^{a_1} \frac{1-x}{1} \left( \frac{x}{2} \right)^{a_2} \frac{2-x}{2} \cdots \left( \frac{x}{n} \right)^{a_n} \frac{n-x}{n}, \quad k \geq 0,$$

where  $a_1 + \cdots + a_n = k$ .

Using (4.4), we may write

$$P_n^F(k) = x^k (1-x) \cdots (n-x) a(k, n) / n!. \quad (4.7)$$

The probability that after the  $(i-1)^{\text{th}}$  black ball is drawn all the remaining balls drawn are white is

$$\lim_{m \rightarrow \infty} \left( \frac{x}{i} \right)^m = 0$$

so, again, the probabilities must add to one.

Putting  $x = -y$ , (4.7) becomes

$$P_n^F(k) = \frac{y^k}{(y)_{-n}} (-1)^k a(k, n) / n!.$$

Summing over  $k$  gives

$$(y)_{-n} = \sum_{k=0}^{\infty} y^k (-1)^k a(k, n) / n!,$$

and a comparison with (4.1) gives

$$s(-n, k) = (-1)^k a(k, n) / n!. \quad (4.8)$$

## 5. PROPERTIES OF NEGATIVE-POSITIVE STIRLING NUMBERS

At the end of Section 3 we noted that

$$|S(-n, -k)| = |s(k, n)| \quad (5.1)$$

whenever  $n$  and  $k$  have the same sign. Equations (4.6) and (4.8) show that NPSN are related by the same reflection in the line  $n = -k$ , that is, (5.1) continues to hold if  $n$  is positive and  $k$  is negative. The consequence is that NPSN of the first and second kinds are (apart from a sign) the

same set of numbers, but differently indexed, so that any property of NPSN of one kind can be immediately expressed as a property of the other kind. Explicitly,

$$S(-n, k) = (-1)^{n+k-1} s(-k, n). \quad (5.2)$$

### Different Representations

If we regard (4.1) as a Taylor series, it follows, using (5.2), that

$$S(-n, k) = \frac{(-1)^{n+k-1}}{n!} \left[ \frac{d^n}{dx^n} \left( \frac{1}{(x+1)(x+2) \cdots (x+k)} \right) \right]_{x=0}. \quad (5.3)$$

It is not difficult to show directly the equivalence of (4.6) and (5.3).

If we expand (5.3) by partial fractions, perform the  $n$ -fold differentiation, and put  $x = 0$ , we obtain

$$S(-n, k) = \frac{1}{k!} \sum_{r=1}^k (-1)^{k-r} \binom{k}{r} r^{-n}. \quad (5.4)$$

Thus, we note that Stirling's formula (2.8) continues to hold if  $n$  is negative.

### Recurrence Formulas and Table of Values

The recurrence relations for PPSN, (2.2) and (2.4), were derived from the identities (2.1) and (2.3). These identities hold whatever the sign of  $n$ , and it follows that (2.2) and (2.4) continue to hold for NPSN. These relations can therefore be used, together with appropriate boundary values, to generate numerical values. For NPSN of the first kind, we may rewrite (2.2) as

$$s(-n+1, k) = s(-n, k-1) + ns(-n, k), \quad n \geq 2, k \geq 1. \quad (5.5)$$

On putting, respectively,  $n = 1$  and  $x = 0$  in the definition (4.1), we obtain

$$s(-1, k) = (-1)^k, \quad s(-n, 0) = 1/n!. \quad (5.6)$$

Combining (5.5) with (5.6), we can generate the values for  $s(-n, k)$  given in Table 1. Values for  $S(-n, k)$  are then given by (5.2).

TABLE 1. Values of  $s(-n, k)$

$n \backslash k$	0	1	2	3
1	1	-1	1	-1
2	$\frac{1}{2}$	$-\frac{3}{4}$	$\frac{7}{8}$	$-\frac{15}{16}$
3	$\frac{1}{6}$	$-\frac{11}{36}$	$\frac{85}{216}$	$-\frac{575}{1296}$
4	$\frac{1}{24}$	$-\frac{25}{288}$	$\frac{415}{3456}$	$-\frac{5845}{41472}$

### Generating Functions

We derive a number of generating functions for NPSN. They can easily be translated into generating functions for the other kind of NPSN by use of (5.2).

The definition (4.1) itself provides a generating function for  $s(-n, k)$ . An exponential generating function can be obtained from (5.4):

$$\sum_{n=0}^{\infty} S(-n, k) \frac{y^n}{n!} = \frac{1}{k!} \sum_{r=1}^k (-1)^{k-r} \binom{k}{r} \exp\left(\frac{y}{r}\right).$$

Two double generating functions can be obtained from (4.1) as follows:

$$\begin{aligned} \sum_{n=1}^{\infty} \sum_{k=0}^{\infty} s(-n, k) x^k y^n &= \sum_{n=1}^{\infty} \frac{\Gamma(x+1)}{\Gamma(x+n+1)} y^n \quad \text{by (4.1) and (1.4)} \\ &= M(1, 1+x, y) - 1, \end{aligned}$$

where  $M$  is a confluent hypergeometric function (see [1], p. 504). Similarly,

$$\begin{aligned} \sum_{n=1}^{\infty} \sum_{k=0}^{\infty} s(-n, k) x^k \frac{y^n}{n!} &= {}_0F_1(1+x, y) - 1 \\ &= [\Gamma(x+1) I_x(2\sqrt{y}) / y^{x/2}] - 1, \end{aligned}$$

where  ${}_0F_1$  and  $I_x$  are, respectively, a generalized hypergeometric function and a modified Bessel function (see [1], pp. 556, 374, 377).

Another pair of double generating functions can be obtained from (4.2):

$$\begin{aligned} \sum_{n=0}^{\infty} \sum_{k=1}^{\infty} S(-n, k)(x)_k y^n &= \frac{x}{x-y}, \\ \sum_{n=0}^{\infty} \sum_{k=1}^{\infty} S(-n, k)(x)_k \frac{y^n}{n!} &= \exp(y/x). \end{aligned}$$

### Asymptotic Behavior

If  $n$  is taken to infinity in (5.4), only the  $r = 1$  term survives. Hence,

$$\lim_{n \rightarrow \infty} S(-n, k) = (-1)^{k-1} / (k-1)!.$$

The definition (4.4) implies that we can express  $a(n, k)$  as  $h_n(1, \frac{1}{2}, \dots, \frac{1}{k})$ , where  $h_n$  is a homogeneous product sum symmetric function (see Riordan [6], p. 47). Riordan shows that  $n!h_n$  can be expressed as a (Bell) polynomial  $Y_n$  in the variables  $s_i$  ( $i = 1, \dots, n$ ), where

$$s_i = 1 + \frac{1}{2^i} + \dots + \frac{1}{k^i}.$$

As  $k \rightarrow \infty$ , all  $s_i$  tend to a finite limit apart from  $s_1$  which behaves like  $\ln k$ . It is clear that the term involving the highest power of  $s_1$  in  $Y_n$  is  $s_1^n$ . Hence, as  $k \rightarrow \infty$ ,  $Y_n \sim (\ln k)^n$ . From (4.6), we conclude that

$$|S(-n, k)| \sim \frac{(\ln k)^n}{k!n!} \text{ as } k \rightarrow \infty.$$

### Orthogonality and Other Relations

For  $n \geq m \geq 1$ , we have

$$(x)_n / (x)_m = (x-m)(x-m-1) \cdots (x-n+1) = (x-m)_{n-m},$$

and

$$\frac{1}{(x)_m} = \frac{1}{x(x-1)\cdots(x-m+1)} = \frac{(-1)^{m-1}}{x(-x+1)\cdots(-x+m-1)} = \frac{(-1)^{m-1}(-x)_{-m+1}}{x}.$$

Hence,

$$(x-m)_{n-m} = (-1)^{m-1}(x)_n(-x)_{-m+1}/x. \quad (5.7)$$

If, for  $m \geq 2$ , we expand the factorial powers by (1.1) and (4.1) we obtain

$$\sum_{k=0}^{n-m} s(n-m, k)(x-m)^k = (-1)^{m-1}x^{-1} \sum_{p=0}^n s(n, p)x^p \sum_{q=0}^{\infty} s(-m+1, q)(-x)^q. \quad (5.8)$$

Expanding the term  $(x-m)^k$  on the left-hand side by the binomial theorem, and equating coefficients of like powers of  $x$ , gives, for  $0 \leq r \leq n-m$ , the following relation between PPSN and NPSN

$$\sum_{k=r}^{n-m} (-1)^k \binom{k}{r} s(n-m, k) m^{k-r} = \sum_{p=0}^{r+1} (-1)^{m+p} s(n, p) s(-m+1, r+1-p), \quad (5.9)$$

and for  $r > n-m$ , the orthogonality relation

$$\sum_{p=0}^{\min(r+1, n)} (-1)^p s(n, p) s(-m+1, r+1-p) = 0. \quad (5.10)$$

When  $m > n \geq 1$ , the left-hand side of (5.7) is replaced by

$$\frac{1}{(x-n)(x-n-1)\cdots(x-m+1)}. \quad (5.11)$$

If we express this function in partial fractions and then expand each term as a power series in  $x$ , we can again equate the coefficients of powers of  $x$  with those on the right-hand side of (5.8), obtaining, for  $r \geq 0$ ,

$$\sum_{k=n}^{m-1} \frac{(-1)^k}{(k-n)!(m-1-k)!k^{r+1}} = \sum_{p=0}^{\min(r+1, n)} (-1)^{p+r} s(n, p) s(-m+1, r+1-p). \quad (5.12)$$

It is possible to obtain equivalent results involving NNSN [and hence, by (3.17), PPSN] instead of NPSN by using (3.11) to expand the term  $(-x)_{-m+1}$  in (5.7). For  $n \geq m \geq 1$  and  $0 \leq r \leq n-m$ , the only difference from (5.9) is that the sum on the right-hand side now goes from  $p = m+r$  to  $p = n$ ; if  $r < 0$ , the sum on the left-hand side of (5.10) now goes from  $p = \max(m+r, 0)$  to  $p = n$ . Similarly, if  $m > n > 0$ , we expand the terms in the partial fraction version of (5.11) as power series in  $(1/x)$  and equate coefficients of like powers. For  $r \leq -(m-n)$ , the right-hand side of (5.12) acquires an extra factor of  $(-1)$  and the sum now goes from  $p = \max(m+r, 0)$  to  $n$ .

#### ACKNOWLEDGMENT

I should like to thank the referee for some helpful suggestions.

## REFERENCES

1. M. Abramowitz & I. A. Stegun, eds. *Handbook of Mathematical Functions*. New York: Dover, 1965.
2. W. L. Ferrar. *Convergence*. Oxford: Clarendon, 1938.
3. C. Jordan. *Calculus of Finite Differences*, 3rd ed. New York: Chelsea, 1965.
4. D. E. Knuth. "Two Notes on Notation." *Amer. Math. Monthly* **99** (1992):403-22.
5. L. M. Milne-Thomson. *The Calculus of Finite Differences*. London: Macmillan, 1933.
6. J. Riordan. *An Introduction to Combinatorial Analysis*. New York: Wiley, 1958.

AMS Classification Numbers: 11B73, 60C05



## APPLICATIONS OF FIBONACCI NUMBERS

### VOLUME 6

*New Publication*

**Proceedings of The Sixth International Research Conference  
on Fibonacci Numbers and Their Applications,  
Washington State University, Pullman, Washington, USA, July 18-22, 1994**

***Edited by G.E. Bergum, A.N. Philippou, and A.F. Horadam***

This volume contains a selection of papers presented at the Sixth International Research Conference on Fibonacci Numbers and Their Applications. The topics covered include number patterns, linear recurrences, and the application of the Fibonacci Numbers to probability, statistics, differential equations, cryptography, computer science, and elementary number theory. Many of the papers included contain suggestions for other avenues of research.

For those interested in applications of number theory, statistics and probability, and numerical analysis in science and engineering:

**1996, 560 pp. ISBN 0-7923-3956-8  
Hardbound Dfl. 345.00 / £155.00 / US\$240.00**

AMS members are eligible for a 25% discount on this volume providing they order directly from the publisher. However, the bill must be prepaid by credit card, registered money order, or check. A letter must also be enclosed saying: "I am a member of the American Mathematical Society and am ordering the book for personal use."

### KLUWER ACADEMIC PUBLISHERS

**P.O. Box 322, 3300 AH Dordrecht  
The Netherlands**

**P.O. Box 358, Accord Station  
Hingham, MA 02018-0358, U.S.A.**

Volumes 1-5 can also be purchased by writing to the same addresses.

# THE ASYMPTOTIC BEHAVIOR OF THE GOLDEN NUMBERS

**Helmut Prodinger**

Department of Algebra and Discrete Mathematics, Technical University of Vienna, Austria

(Submitted August 1994)

In [2] the "Golden polynomials"

$$G_{n+2}(x) = xG_{n+1}(x) + G_n(x), \quad G_0(x) = -1, \quad G_1(x) = x - 1,$$

and their maximal real root  $g_n$  (the "golden numbers") were investigated. It was observed that, as  $n \rightarrow \infty$ ,  $g_n \rightarrow 3/2$ ; furthermore, it was suggested there might be a more precise formula, since numerical experiments seemed to indicate a dependency on the parity of  $n$  of the lower order terms.

This open question will be solved in the present paper.

Solving the recursion for the Golden polynomials by standard methods, we get the explicit formula

$$G_n(x) = A\lambda^n + B\mu^n,$$

with

$$\lambda = \frac{x + \sqrt{x^2 + 4}}{2}, \quad \mu = \frac{x - \sqrt{x^2 + 4}}{2},$$

$$A = \frac{1}{2\sqrt{x^2 + 4}}(3x - 2 - \sqrt{x^2 + 4}), \quad B = -\frac{1}{2\sqrt{x^2 + 4}}(3x - 2 + \sqrt{x^2 + 4}).$$

Everything is much nicer when we substitute

$$x = u - \frac{1}{u}.$$

$G_n(x) = 0$  can be rephrased as  $-B/A = (\lambda/\mu)^n$ , or

$$\frac{(2u+1)(u-1)}{(u+1)(u-2)} = (-u^2)^n.$$

Now it is plain to see that, for large  $n$ , this equation can only hold if  $u$  is either close to 2 or to  $u = -1/2$ . In both cases, this would mean  $x$  is close to  $3/2$ . Let us assume that  $u$  is close to 2. It is clear that the cases when  $n$  is even or odd have to be distinguished. We start with  $n = 2m$  and rewrite the equation as

$$u - 2 = \frac{(2u+1)(u-1)}{(u+1)} u^{-4m}.$$

We get the asymptotic behavior of the desired solution by a process known as "bootstrapping" which is explained in [1]. First, we set  $u = 2 + \delta$ , insert  $u = 2$  into the right-hand side, and get an approximation for  $\delta$ . Then we insert  $u = 2 + \delta$  into the right-hand side, expand, and get the next term. This procedure can be repeated to get as many terms as needed. In this way, we get

$$\delta \sim \frac{5}{3} \cdot 16^{-m},$$

and with

$$u = 2 + \frac{5}{3} \cdot 16^{-m} + \varepsilon,$$

we find

$$\varepsilon \sim -\frac{25}{6} m \cdot 256^{-m}.$$

From

$$u \sim 2 + \frac{5}{3} \cdot 16^{-m} - \frac{50}{9} m \cdot 256^{-m}$$

we find by substitution

$$x \sim \frac{3}{2} + \frac{25}{12} \cdot 16^{-m} - \frac{125}{18} m \cdot 256^{-m}.$$

Now let us consider the case  $n$  is odd,  $n = 2m + 1$ . Then our equation is

$$u - 2 = -\frac{(2u+1)(u-1)}{(u+1)u^2} u^{-4m},$$

and we find as above

$$u \sim 2 - \frac{5}{12} \cdot 16^{-m} - \frac{25}{72} m \cdot 256^{-m},$$

and also

$$x \sim \frac{3}{2} - \frac{25}{48} \cdot 16^{-m} - \frac{125}{288} m \cdot 256^{-m}.$$

Confining ourselves to two terms, we write our findings in a single formula as

$$g_n \sim \frac{3}{2} + (-1)^n \frac{25}{12} \cdot 4^{-n},$$

which matches perfectly with the empirical data from [2].

## REFERENCES

1. D. Greene & D. Knuth. *Mathematics for the Analysis of Algorithms*. Birkhäuser, 1981.
2. G. Moore. "The Limit of the Golden Numbers is  $3/2$ ." *The Fibonacci Quarterly* **32.3** (1994): 211-17.

AMS Classification Numbers: 11B39, 11B37, 11C08



# DIGRAPHS FROM POWERS MODULO $p$

**Caroline Lucheta**

Box 1121 GCC, 100 Campus Drive, Grove City, PA 16127

**Eli Miller**

PO Box 410, Sumneytown, PA 18084

**Clifford Reiter**

Department of Mathematics, Lafayette College, Easton, PA 18042-1781

(Submitted August 1994)

## 1. INTRODUCTION

Given any function  $f$  defined modulo  $m$ , we can consider the digraph that has the residues modulo  $m$  as vertices and a directed edge  $(a, b)$  if and only if  $f(a) \equiv b \pmod{m}$ . This digraph can be thought of as a geometric representation of all the sequences generated by iterating  $f$  modulo  $m$ . The digraph associated with squaring modulo  $p$ , a prime, has been studied in [1]. In that paper the cycle lengths and the number of cycles appearing were characterized. The structure of the trees attached to cycle elements was also completely described. Our paper will generalize those results to the digraph associated with the function  $x^k$  modulo a prime  $p$  with  $k$  any positive integer. Since zero is an isolated cycle for all  $p$  and  $k$ , we will consider the digraph generated by the nonzero residues. Hence, the vertex set of the digraph is equal to  $Z_p^*$ . We will let  $G_p^k$  denote the digraph on the nonzero residues modulo  $p$  with edges given by  $x^k \pmod{p}$ . For example,  $G_{53}^3$  is shown in Figure 1 and  $G_{41}^4$  is shown in Figure 2. Note that, when  $p = 2$ ,  $G_p^k$  consists of the vertex 1 in a loop. Thus, we need only consider  $G_p^k$  when  $p$  is an odd prime. We will use  $p$  to denote an odd prime throughout this paper.

Elementary results about these digraphs are described in Section 2. In particular, we see that each component contains a single cycle and we can determine when there are noncycle vertices. Section 3 characterizes the cycle lengths that appear. Section 4 explores the relationship of geometric subsets of the digraph to subgroups of the group of units modulo  $p$ . Section 5 considers some special cases where long cycles occur. Section 6 returns to the basic structure of the digraph and shows that all the forests appearing must be isomorphic and characterizes their heights. Section 7 explores the simplifications of the structures that appear when  $k$  is prime.

We begin by enumerating six well-known elementary theorems which will be used. Proofs can be found in standard texts.

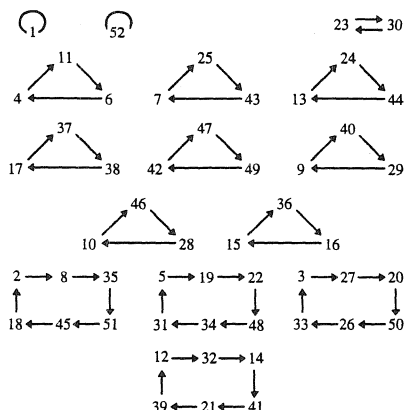
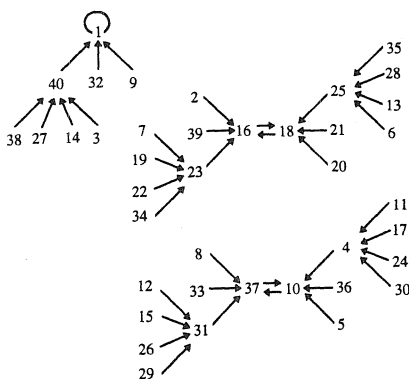
**Theorem 1:** If  $a \neq 0$ , there are 0 or  $\gcd(k, p-1)$  solutions to  $x^k \equiv a \pmod{p}$ .

*Proof:* See [3], p. 47.  $\square$

**Theorem 2:** If  $d$  is a positive integer such that  $d|p-1$ , then there are exactly  $\phi(d)$  incongruent residues of order  $d$  modulo  $p$ .

*Proof:* See [3], p. 48.  $\square$




 FIGURE 1. The Digraph of  $G_{53}^3$ 

 FIGURE 2. The Digraph of  $G_{41}^4$ 

**Theorem 3:** If  $n$  is a positive integer, then

$$\sum_{d|n, d>0} \Phi(d) = n.$$

*Proof:* See [5], p. 83.  $\square$

**Theorem 4:** If  $a$  is an integer such that  $\gcd(a, m) = 1$  and  $i$  is a positive integer, then

$$\text{ord}_m a^i = \frac{\text{ord}_m a}{\gcd(i, \text{ord}_m a)}.$$

*Proof:* See [5], p. 132.  $\square$

**Theorem 5:** A primitive root modulo  $m$  exists if and only if  $m$  is of the form 2, 4,  $p^n$ , or  $2p^n$ , where  $p$  is an odd prime.

*Proof:* See [3], p. 49.  $\square$

**Theorem 6:** If  $a$  and  $b$  are elements of  $Z_p^*$  such that  $\alpha = \text{ord}_p a$ ,  $\beta = \text{ord}_p b$ , and  $\gcd(\alpha, \beta) = 1$ , then  $\text{ord}_p ab = \alpha\beta$ .

*Proof:* See [4], p. 46.  $\square$

## 2. BASIC PROPERTIES

The following lemmas are easy to prove but fundamental to the understanding of the digraph structure of  $G_p^k$ . We will see that, for all  $G_p^k$ , each graph component contains a unique cycle which may have forest structures attached to it.

**Lemma 7:** The outdegree of any vertex in  $G_p^k$  is one.

**Proof:** The function  $x^k \pmod{p}$  maps the vertex  $a$  to  $a^k$  and only  $a^k$ .  $\square$

**Lemma 8:** Given any element in  $G_p^k$ , repeated iteration of  $x^k \pmod{p}$  will eventually lead to a cycle.

**Proof:** Because there are  $p-1$  vertices in  $G_p^k$ , iterating  $x^k \pmod{p}$  must eventually produce a repeated value.  $\square$

**Lemma 9:** Every component of  $G_p^k$  contains exactly one cycle.

**Proof:** Suppose a component has more than one cycle; then, somewhere along the undirected path connecting any two cycles, there exists a vertex with outdegree at least 2, which is impossible.  $\square$

**Lemma 10:** The set of noncycle vertices leading to a fixed cycle vertex forms a forest.

**Proof:** Since each component contains exactly one cycle, the vertices leading to a cycle vertex cannot contain a cycle; thus, they are a forest.  $\square$

**Lemma 11:** The indegree of any vertex in  $G_p^k$  is 0 or  $\gcd(k, p-1)$ .

**Proof:** This result is an immediate application of Theorem 1.  $\square$

**Lemma 12:** Every component of  $G_p^k$  is cyclical if and only if  $\gcd(k, p-1) = 1$ .

**Proof:** ( $\Rightarrow$ ) If all digraph components are cyclical both the indegree and outdegree are one, which implies from Lemma 11 that  $\gcd(k, p-1) = 1$ .

( $\Leftarrow$ ) Conversely, if  $\gcd(k, p-1) = 1$ , the indegree of every vertex is 0 or 1. If some component were not cyclical, there would exist a cycle vertex with indegree  $\geq 2$ , a contradiction.  $\square$

For example, each component of  $G_{53}^3$  is cyclical because  $\gcd(3, 52) = 1$ ; this is apparent in Figure 1. Likewise,  $G_{41}^4$  has vertices outside the cycles because  $\gcd(4, 40) = 4$  (see Figure 2). We will refer to a *child* of a vertex  $a$  as a vertex  $v$  that satisfies the equation  $v^k \equiv a \pmod{p}$ . These are the predecessors of  $a$  in  $G_p^k$ . Note that our child vertices are children in the sense of the forest structure but not in the standard sense of direction. Predecessors that are not in a cycle will be called *noncycle* children. For example, in  $G_{41}^4$ , 37 has the three noncycle children 8, 31, and 33.

**Lemma 13:** Any cycle vertex,  $c$ , has  $\gcd(k, p-1) - 1$  noncycle children.

**Proof:** From Lemma 11, the indegree of  $c$  is 0 or  $\gcd(k, p-1)$ . Since  $c$  is a cycle vertex, the indegree is not zero but  $\gcd(k, p-1)$ . The number of noncycle children is  $\gcd(k, p-1) - 1$ .  $\square$

Above we saw some of the basic results about  $G_p^k$ . Notice that if we fix  $k$  and vary  $p$  the number of vertices changes and infinitely many different digraphs result. However, if  $p$  is fixed, only finitely many distinct digraphs result as  $k$  varies. The next theorem identifies the powers that result in identical digraphs.

**Theorem 14:**  $k_1 \equiv k_2 \pmod{p-1}$  if and only if  $G_p^{k_1} = G_p^{k_2}$ .

**Proof:** ( $\Rightarrow$ ) Suppose  $k_1 \equiv k_2 \pmod{p-1}$  and without loss of generality  $k_1 \geq k_2$ . If  $a$  is any vertex in the reduced residue set,  $\text{ord}_p a \mid (p-1) \mid (k_1 - k_2)$ , so  $a^{k_1 - k_2} \equiv 1$  implies  $a^{k_1} \equiv a^{k_2} \pmod{p}$ . Hence,  $G_p^{k_1} = G_p^{k_2}$ .

( $\Leftarrow$ ) Suppose  $G_p^{k_1} = G_p^{k_2}$ , and assume  $k_1 \geq k_2$ . Then  $a^{k_1} \equiv a^{k_2} \pmod{p}$  implies  $\text{ord}_p a \mid (k_1 - k_2)$  for all vertices  $a$ . So  $(p-1) \mid (k_1 - k_2)$ , and the conclusion follows.  $\square$

The 12 different digraphs for  $G_{13}^k$  are shown in Figure 3. Notice that some have only cycles and some have forest structures. This theorem gives a condition for equality of digraphs, but does not settle the question of when two digraphs can be *isomorphic* for different values of  $k$ . For example,  $G_{11}^2 \neq G_{11}^8$  but  $G_{11}^2 \approx G_{11}^8$ .

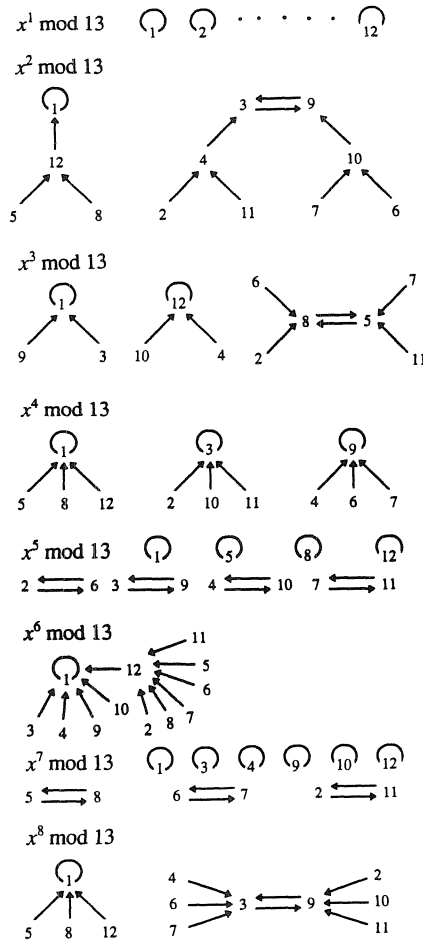
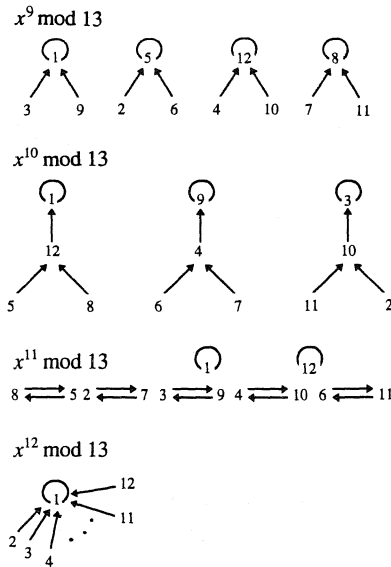


FIGURE 3. All Possible Digraphs of  $G_{13}^k$

FIGURE 3. All Possible Digraphs of  $G_{13}^k$  (continued)

### 3. CHARACTERIZING CYCLES

When considering the cycle structure of  $G_p^k$ , it is convenient to factor  $p-1$  as  $wt$ , where  $t$  is the largest factor of  $p-1$  relatively prime to  $k$ . So  $\gcd(k, t) = 1$  and  $\gcd(w, t) = 1$ . For example, if  $p = 41$  and  $k = 6$ , then  $p-1 = 2^3 \cdot 5$ , so  $w = 8$  and  $t = 5$ . Similarly, if  $p = 47$  and  $k = 4$ , then  $w = 2$  and  $t = 23$ ; also, if  $p = 19$  and  $k = 6$ , then  $w = 18$  and  $t = 1$ . In all the theorems below, we will be considering the digraph  $G_p^k$  with  $p-1 = wt$  as described.

**Theorem 15:** The vertex  $c$  is a cycle vertex if and only if  $\text{ord}_p c | t$ .

**Proof:** ( $\Rightarrow$ ) Since  $c$  is in a cycle there exists some  $x \geq 1$  such that  $c^{k^x} \equiv c \pmod{p}$  and thus  $c^{k^x-1} \equiv 1 \pmod{p}$ . Hence,  $\text{ord}_p c | k^x - 1$ , which implies that  $\gcd(\text{ord}_p c, k) = 1$ , so  $\gcd(\text{ord}_p c, w) = 1$  also. We know that  $\text{ord}_p c | p-1 = wt$ , and so  $\text{ord}_p c$  must divide  $t$ .

( $\Leftarrow$ ) Suppose  $c \in G_p^k$  and  $\text{ord}_p c | t$ ; therefore,  $\gcd(\text{ord}_p c, k) = 1$ . On repeated iteration,  $c$  must eventually end up in a cycle. If  $y$  is the number of steps to reach the cycle and  $x$  is the cycle length, then  $c^{k^y(k^x-1)} \equiv 1 \pmod{p}$ . Therefore,  $\text{ord}_p c | k^y(k^x-1)$ , but since  $\gcd(\text{ord}_p c, k) = 1$ ,  $\text{ord}_p c | k^x - 1$ . Hence,  $c^{k^x} \equiv c \pmod{p}$ , which implies that  $c$  is a cycle vertex.  $\square$

**Corollary 16:** There are  $t$  vertices in cycles.

**Proof:** From Theorem 15, the total number of cycle vertices is  $\sum_{d|t} N(d)$ , where  $N(d)$  is the number of elements of order  $d \pmod{p}$ . Theorems 2 and 3 imply that this is  $t$ .  $\square$

**Theorem 17:** Vertices in the same cycle have the same order  $\pmod{p}$ .

**Proof:** Assume  $a$  and  $b$  are in the same cycle. Hence, there exists an  $e$  such that  $a^e \equiv b \pmod{p}$ . Let  $\alpha = \text{ord}_p a$  and  $\beta = \text{ord}_p b$ . It follows that  $b^\alpha \equiv a^{e\alpha} \equiv 1 \pmod{p}$  and thus  $\beta | \alpha$ . Similarly,  $\alpha | \beta$ ; hence, the orders are equal.  $\square$

Theorem 17 shows that the order (mod  $p$ ) of vertices in the same cycle are equal. Hence, the notion of the *order of a cycle* is well defined. We now look at the relationship between the order of a cycle and its length.

**Theorem 18:** Let  $x$  be the length of a cycle of order  $d$  (mod  $p$ ), then  $k^x - 1$  is the smallest number of the form  $k^n - 1$  divisible by  $d$ .

**Proof:** Let  $c$  be a vertex in the cycle. Since the cycle is of length  $x$ ,  $c^{k^x-1} \equiv 1 \pmod{p}$ . It follows that  $d = \text{ord}_p c$  divides  $k^x - 1$ . If  $\text{ord}_p c \nmid k^s - 1$  for some  $s < x$ , then  $c^{k^s} \equiv c$ , a contradiction.  $\square$

Theorem 18 shows that the length of a cycle depends entirely on its order. If we let  $\ell(d)$  denote the *length of cycles* with order  $d$ , we get the following theorem.

**Theorem 19:** Let  $a$ ,  $b$ , and  $d$  be orders of cycles in  $G_p^k$ . Then:

- (i)  $\ell(d) = \text{ord}_d k$ .
- (ii) There are  $\phi(d) / \ell(d)$  cycles of order  $d$ .
- (iii)  $\ell(\text{lcm}(a, b)) = \text{lcm}(\ell(a), \ell(b))$ .
- (iv) The longest cycle length is  $\ell(t) = \text{ord}_t k$ .

**Proof:**

- (i) By Theorem 18,  $\ell(d) = \min\{n : d \mid k^n - 1\}$ ; hence,  $\ell(d) = \text{ord}_d k$ .
- (ii) By Theorem 2, there are  $\phi(d)$  elements of order  $d$ , and there are  $\ell(d)$  in each cycle by (i), hence the result.
- (iii.a) By (i),  $k^{\ell(a)} \equiv 1 \pmod{a}$  and  $k^{\ell(b)} \equiv 1 \pmod{b}$ ; thus,  $k^{\text{lcm}(\ell(a), \ell(b))} \equiv 1 \pmod{a}$  and  $k^{\text{lcm}(\ell(a), \ell(b))} \equiv 1 \pmod{b}$ . It follows that  $k^{\text{lcm}(\ell(a), \ell(b))} \equiv 1 \pmod{\text{lcm}(a, b)}$ . Therefore,  $\ell(\text{lcm}(a, b)) \mid \text{lcm}(\ell(a), \ell(b))$ .
- (iii.b) We know that  $k^{\ell(\text{lcm}(a, b))} \equiv 1 \pmod{\text{lcm}(a, b)}$ . Therefore,  $k^{\ell(\text{lcm}(a, b))} \equiv 1 \pmod{a}$  and  $k^{\ell(\text{lcm}(a, b))} \equiv 1 \pmod{b}$ . Thus,  $\ell(a) \mid \ell(\text{lcm}(a, b))$  and  $\ell(b) \mid \ell(\text{lcm}(a, b))$ , which implies that  $\text{lcm}(\ell(a), \ell(b)) \mid \ell(\text{lcm}(a, b))$ .

Putting (iii.a) and (iii.b) together gives  $\ell(\text{lcm}(a, b)) = \text{lcm}(\ell(a), \ell(b))$ .

- (iv) All orders of cycles divide  $t$  and if  $d \mid t$  then  $\ell(t) = \ell(\text{lcm}(t, d)) = \text{lcm}(\ell(t), \ell(d))$ , which implies  $\ell(d) \mid \ell(t)$ . Thus,  $\ell(t)$  is the maximal cycle length.  $\square$

We are now in a position to identify the number of cycles of every length appearing in the digraph of  $G_p^k$ . For example, consider  $G_{53}^3$  (Fig. 1); in this case  $p-1=52$  so  $w=1$  and  $t=52$ . The possible orders of the cycle elements are the divisors of  $t$ : 1, 2, 4, 13, 26, and 52. There are  $\phi(52)=24$  elements of order 52, and these 24 elements are in cycles of length  $\ell(52) = \text{ord}_{52} 3 = 6$ , contributing four cycles of length 6. Similarly, the elements of order 26 appear in 4 cycles of length 3; and those of order 13 are in 4 cycles of length 3. There are 2 elements of order 4 in one cycle and two cycles of length one with orders 1 and 2. Table 1 gives some details about cycles in  $G_p^k$  for selected  $p$  and  $k$ .

TABLE 1. Cycle Lengths in  $G_p^k$ 

$k$	2			3			4			5			6		
$p$	$d$	$\ell(d)$	#	$d$	$\ell(d)$	#	$d$	$\ell(d)$	#	$d$	$\ell(d)$	#	$d$	$\ell(d)$	#
41	1 5	1 4	1 1	1 2 4 5 8 10 20 40	1 1 2 1 2 4 4 4	1 1 1 1 2 1 2 4	1 5	1 2	1 2	1 2 4 8	1 1 1 2 2	1 1 2 2	1 5	1 1	1 4
43	1 3 7 21	1 2 3 6	1 1 2 2	1 2 7 14	1 1 6 6	1 1 1 1	1 3 7 21	1 1 3 3	1 2 2 4	1 2 3 6 7 14 21 42	1 1 2 2 1 6 6 6 2 2	1 1 1 1 1 1 2 2	1 7	1 2	1 3
47	1 23	1 11	1 2	1 2 23 46	1 1 11 11	1 1 2 2	1 23	1 11	1 2	1 2 23 46	1 1 1 22 22	1 1 1 1	1 23	1 11	1 2
53	1 13	1 12	1 1	1 2 4 13 26 52	1 1 2 3 3 6	1 1 1 4 4 4	1 13	1 6	1 2	1 2 4 13 26 52	1 1 1 4 4 4 6	1 1 2 3 3 6	1 13	1 12	1 1

4. SUBGROUPS OF  $Z_p^*$  IN  $G_p^k$ 

We now consider orders of elements throughout  $G_p^k$ . We will be able to associate elements of various orders with subgroups of  $Z_p^*$ , which allows for the identification of certain subgroups of  $Z_p^*$  with geometric subsets of the digraph. In later sections we will return to characterizing the cycle and forest structure of these digraphs.

**Lemma 20:** If  $H_d$  is the set of residues with orders dividing  $d$ ,  $d \geq 1$ , then  $H_d$  is a cyclic subgroup of  $Z_p^*$ .

**Proof:** Since  $Z_p^*$  is a finite cyclic group, we need only show that  $H_d$  is nonempty and closed under multiplication. Clearly  $H_d$  is not empty because it has the identity. To show closure, suppose that  $a, b \in H_d$  and let  $\alpha = \text{ord}_p a$  and  $\beta = \text{ord}_p b$ . Since  $(ab)^{\text{lcm}(\alpha, \beta)} \equiv 1 \pmod{p}$ ,  $\text{ord}_p ab$  divides  $\text{lcm}(\alpha, \beta)$  which in turn divides  $d$ . Therefore,  $H_d$  is a subgroup of  $Z_p^*$ .  $\square$

For instance, if we consider the group  $Z_{41}^*$ , the elements of order 1 and 2 form the subgroup  $H_2$ , while  $H_{10}$  contains those elements of order 1, 2, 5, and 10.

We will now introduce a notation for the forest originating from any given cycle vertex. Let  $F_c^n$  represent the set of vertices in the  $n^{\text{th}}$  level of the forest originating from the cycle vertex  $c$ . Of course,  $F_c^n$  depends on  $G_p^k$ . For example, in  $G_{41}^4$  (Fig. 2),  $F_{16}^1 = \{2, 23, 39\}$  and  $F_{16}^2 = \{7, 19, 22, 34\}$ . Similarly,  $F^n$  refers to the vertices in the  $n^{\text{th}}$  level of all forests and  $F_c$  refers to all forest

vertices associated with the cycle vertex  $c$  at all levels  $n \geq 1$ . Note that the cycle vertices are not a part of the forests but for convenience we will denote the set of cycle elements by  $F^0$  and also  $F_c^0 = \{c\}$  but  $c \notin F_c$ .

The next theorem and corollary explain the subgroup structures present in the digraphs. First, it will be shown that the order of an element is constrained by its height in the forest structure.

**Theorem 21:** Let  $a \in F_c$  and  $\text{ord}_p c = d|t$ . Then  $\text{ord}_p a | k^h d$  if and only if  $a \in F_c^x$ , where  $x \leq h$ .

**Proof:** ( $\Rightarrow$ ) Suppose  $\text{ord}_p a | k^h d$ . Then  $(a^{k^h})^d \equiv 1 \pmod{p}$ . Now, using Theorem 4,

$$1 = \text{ord}_p 1 = \text{ord}_p (a^{k^h})^d = \frac{\text{ord}_p a^{k^h}}{\gcd(d, \text{ord}_p a^{k^h})}.$$

Since  $\gcd(d, \text{ord}_p a^{k^h}) = \text{ord}_p a^{k^h}$ ,  $\text{ord}_p a^{k^h}$  divides  $d$  which divides  $t$ . From Theorem 15,  $a^{k^h}$  must be a cycle element, and hence  $a \in F_c^x$ , where  $x \leq h$ .

( $\Leftarrow$ ) If  $a \in F_c^x$  and  $x \leq h$ , then  $a^{k^x}$  is a cycle element of order  $d$ . Furthermore,

$$d = \text{ord}_p a^{k^x} = \frac{\text{ord}_p a}{\gcd(k^x, \text{ord}_p a)};$$

hence,  $d \cdot \gcd(k^x, \text{ord}_p a) = \text{ord}_p a$ , and thus  $\text{ord}_p a | d \cdot k^x | d \cdot k^h$ .  $\square$

From Theorem 21, it can be ascertained that various geometric subsets of the digraph form subgroups of  $Z_p^*$ , as stated in the next corollary.

**Corollary 22:** For all  $d$  dividing  $t$  and all  $h$ ,  $\bigcup_{\substack{0 \leq x \leq h \\ \text{ord}_p c | d}} F_c^x$  is a subgroup of  $Z_p^*$ , namely  $H_{k^h d}$ .

**Proof:** The union over all  $c$  such that  $\text{ord}_p c | d$  and over all  $x \leq h$  contains all  $a \in Z_p^*$  such that  $\text{ord}_p a | k^h d$  by Theorem 21. This is the subgroup  $H_{k^h d}$  of  $Z_p^*$  by Lemma 20.  $\square$

Corollary 22 indicates that the union of cycle vertices with orders dividing a fixed  $d$  and vertices in their associated forest structures up to a fixed height form a subgroup of  $Z_p^*$ . In particular, if  $d = 1$ , all the vertices in  $F_1$  up to any fixed level (along with 1) form a subgroup. On the other extreme, if  $d = t$ , all the vertices in all the components up to a fixed height form subgroups. Examining the digraph of  $G_{41}^4$  (Fig. 2), one finds the following subgroups:

$$\begin{aligned} d = 1, h = 0: & F_1^0 = \{1\} = H_1; \\ d = 1, h = 1: & F_1^0 \cup F_1^1 = \{1, 9, 32, 40\} = H_4; \\ d = 1, h = 2: & F_1^0 \cup F_1^1 \cup F_1^2 = \{1, 3, 9, 14, 27, 32, 38, 40\} = H_{16}; \\ d = 5, h = 0: & F^0 = \{1, 10, 16, 18, 37\} = H_5; \\ d = 5, h = 1: & F^0 \cup F^1 = \{1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40\} = H_{20}; \\ d = 5, h = 2: & F^0 \cup F^1 \cup F^2 = \{1, \dots, 40\} = Z_{41}^* = H_{80}. \end{aligned}$$

These algebraic properties imply that the highest level of the digraph, which will be referred to as the *canopy*, must contain at least half of the vertices. For example, in  $G_{41}^4$  (Fig. 2) the canopy is  $F^2$ .

**Corollary 23:** If  $h_0$  is the maximal height attained by the forest elements in  $G_p^k$ , then  $|F^{h_0}| \geq (p-1)/2$ .

**Proof:**

(i) If  $h_0 = 0$ , then all vertices are in cycles, so  $|F^0| = p-1 \geq (p-1)/2$ .

(ii) If  $h_0 \geq 1$ , then from Corollary 22,  $H_{k^{h_0-1}} = \bigcup_{0 \leq n \leq h_0-1} F^n$  is a proper subgroup of  $Z_p^*$ . The number of elements in  $H_{k^{h_0-1}}$  must be a proper divisor of  $|Z_p^*| = p-1$ . Since the largest proper divisor of  $p-1$  is  $(p-1)/2$ , there are at least  $(p-1)/2$  vertices remaining in the canopy.  $\square$

We also see a relationship between forest elements, cycle elements, and their products in the following corollary.

**Corollary 24:** The product of a forest element and a cycle element is a forest element.

**Proof:** The cycle elements of  $G_p^k$  form a closed multiplicative subgroup of  $Z_p^*$ ; hence, the product of a forest element and a cycle element must be a forest element.  $\square$

## 5. OCCURRENCE OF LONG CYCLES

Control over the lengths of cycles is highly desirable. This is essential for applications to pseudo-random number generation and data encryption. The first theorem below provides an upper bound for the cycle lengths appearing in  $G_p^k$ . Special cases where long cycles can be guaranteed are then considered.

**Theorem 25:** Let  $p > 5$  be prime. Then the length of the longest cycle in  $G_p^k$  is less than or equal to  $(p-3)/2$ .

**Proof:** Consider two cases depending on  $\gcd(k, p-1)$ .

(i) Suppose  $\gcd(k, p-1) \neq 1$ . By Lemma 12,  $G_p^k$  is not entirely cyclical and by Corollary 23 it has a forest structure with at least  $(p-1)/2$  vertices in the canopy. Therefore, there are at most  $(p-1)/2$  vertices in cycles. Since  $p > 5$ , we know we are not interested in longest cycles of length 1, and since 1 is in a loop, it is not part of any longest cycle of interest; hence, the maximal length cannot exceed  $[(p-1)/2] - 1 = (p-3)/2$ .

(ii) Suppose  $\gcd(k, p-1) = 1$ ; thus,  $G_p^k$  consists entirely of cycles. From Theorem 19, the longest cycle length is associated with the elements of order  $t = p-1$ , which can be factored as  $2^s \tau$ , where  $s \geq 1$  and  $\tau$  is odd.

(a) If  $\tau \neq 1$ , then the number of elements of order  $p-1$  is  $\phi(p-1) = \phi(2^s \tau) = 2^{s-1} \phi(\tau) < 2^{s-1} \tau = (p-1)/2$ . Now, since  $\phi(p-1)$  is an integer,  $\phi(p-1) \leq (p-3)/2$ . Hence, even if all elements of order  $p-1$  were together in one cycle, the length could not exceed  $(p-3)/2$ .

(b) If  $\tau = 1$ , then  $p = 2^s + 1$  is a Fermat prime larger than 5, so  $s > 2$ . By Theorem 19, the length of the longest cycle is  $\ell(t) = \ell(2^s) = \text{ord}_2 k$ . However,  $Z_{2^s}^*$  does not have a primitive



root for  $s > 2$  (Theorem 5). Thus,  $\text{ord}_{2^s} k < \phi(2^s) = (p-1)/2$ ; hence,  $\ell(t) \leq (p-3)/2$  in this case as well.  $\square$

While Theorem 25 gives an upper bound for the cycle lengths in  $G_p^k$ , it does not specify whether this bound is ever attained. The next theorem shows that, for Sophie Germain primes, these maximal cycle lengths can be attained.

**Theorem 26:** Let  $p = 2q + 1$ , where  $q$  is an odd Sophie Germain prime. If  $k$  is a primitive root mod  $q$ , then  $G_p^k$  contains a cycle of length  $(p-3)/2$ .

**Proof:** Because  $\gcd(k, q) = 1$  and  $q|t$ , the elements with order  $q$  are in cycles of length  $\text{ord}_q k = q - 1 = (p-3)/2$ .  $\square$

**Corollary 27:** Let  $p = 2q + 1$ , where  $q$  is an odd Sophie Germain prime. If  $k$  is an odd primitive root mod  $q$ , then  $G_p^k$  contains two cycles of length  $(p-3)/2$ .

**Proof:** Since  $k$  is odd,  $t = 2q$  and the graph is entirely cyclical. The elements of order  $q$  are in a cycle of length  $\text{ord}_q k = q - 1 = (p-3)/2$ . The elements of order  $t = 2q$  are, by Theorem 19, in the longest cycles of the digraphs. So the elements of order  $2q$  are also in a cycle of length  $(p-3)/2$ .  $\square$

For example, consider  $G_{23}^2$  (Fig. 4);  $p = 23 = 2(11) + 1$ , and 2 is a primitive root mod 11. As expected,  $G_{23}^2$  contains one cycle of length 10. Corollary 27 is illustrated by  $G_{47}^5$ , where  $p = 47 = 2(23) + 1$ , 5 is a primitive root mod 23, and the digraph has two cycles of length 22.

Given a prime of the form  $2q + 1$ , where  $k$  is a primitive root mod  $q$ , it is simple to iterate through a cycle of length  $(p-3)/2$ . Any residue between 2 and  $p-2$  is either in a long cycle or is one step away. Beginning with any such residue, we can iterate  $x^k \pmod{p}$  to produce  $(p-3)/2$  incongruent values. For example, consider the prime  $9887 = 2(4943) + 1$ , where 4943 is also prime. Since 7 is a primitive root of 4943, iteration of  $x^7 \pmod{9887}$  beginning with any  $x$  from 2 to 9885 will yield 4942 incongruent values.

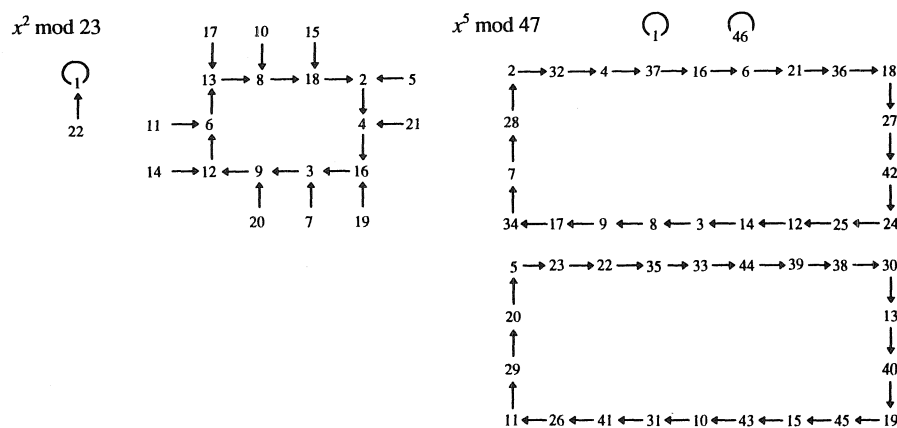


FIGURE 4. The Digraphs  $G_{23}^2$  and  $G_{47}^5$

## 6. CHARACTERIZING FORESTS

Having completely characterized the cycles for the digraph generated by  $x^k \pmod{p}$ , we turn our attention to characterizing the noncyclical elements of  $G_p^k$ . In each of our examples, we notice that the forests in any particular digraph are isomorphic. This turns out to be true in general, and will be proved by constructing a one-to-one correspondence between  $F_1$  and  $F_c$ . The next lemma gives the essence of how the correspondence will be constructed.

**Lemma 28:** If  $a \in F_1^h$  and  $c$  is a cycle vertex, then  $ac \in F_{c^{k^h}}^h$ .

**Proof:** Using Corollary 24, it follows immediately that  $ac \notin F^0$ . Furthermore,  $(ac)^{k^h} \equiv c^{k^h} \pmod{p}$  is a cycle element but  $(ac)^{k^{h-1}}$  is a forest element, which implies that  $ac \in F_{c^{k^h}}^h$ .  $\square$

**Theorem 29:** Let  $c$  be a cycle element, then  $F_1 \approx F_c$ .

**Proof:**

(i) First, we show that there exists a one-to-one correspondence between the vertices of  $F_1^h$  and  $F_c^h$  for all heights  $h$ , and hence between  $F_1$  and  $F_c$ . Let  $h$  be fixed and let  $c_h$  denote the unique cycle element such that  $c_h^{k^h} \equiv c \pmod{p}$ . Define  $f_h: F_1^h \rightarrow F_c^h$  by  $f_h(a) \equiv a \cdot c_h \pmod{p}$ . Next, we check that  $f_h$  is one-to-one and onto. Let  $b \in F_c^h$ . Then  $(b \cdot c_h^{-1})^{k^h} \equiv b^{k^h} (c_h^{k^h})^{-1} \equiv c \cdot c^{-1} \equiv 1 \in F_1^0$  and  $(b \cdot c_h^{-1})^{k^{h-1}} \notin F^0$  because  $b^{k^{h-1}} \notin F^0$  and  $c_h^{k^{h-1}} \in F^0$ . It follows that  $b \cdot c_h^{-1} \in F_1^h$ . Furthermore,  $f_h(b \cdot c_h^{-1}) \equiv b \cdot c_h^{-1} \cdot c_h \equiv b \pmod{p}$ , so  $f_h$  is onto  $F_c^h$ . Suppose  $f_h(a_1) \equiv f_h(a_2) \pmod{p}$  for  $a_1, a_2 \in F_1^h$ . Then  $a_1 \cdot c_h \equiv a_2 \cdot c_h$  implies  $a_1 \equiv a_2 \pmod{p}$ . Thus,  $f_h$  is one-to-one.

(ii) It remains to be shown that there exists a one-to-one correspondence between the edges of  $F_1$  and  $F_c$ . We want to define  $g: E(F_1) \rightarrow E(F_c)$  by  $g(a, a^k) = (f_h(a), f_{h-1}(a^k))$ , where  $h$  is the height of  $a$  in  $F_1$ . If  $(f_h(a), f_{h-1}(a^k))$  is in fact in  $E(F_c)$ , then  $g$  will inherit the one-to-one and onto properties from  $f_h$  and  $f_{h-1}$ . We have an edge  $(f_h(a), f_{h-1}(a^k))$  if and only if  $(f_h(a))^k \equiv f_{h-1}(a^k) \pmod{p}$ . Now  $f_h(a) \equiv a \cdot c_h \pmod{p}$ , where  $c_h^{k^h} \equiv c$  and  $f_{h-1}(a) \equiv a \cdot c_{h-1} \pmod{p}$ , where  $c_{h-1}^{k^{h-1}} \equiv c \pmod{p}$ ; thus,  $c_h^{k^h} \equiv c \Rightarrow (c_h^k)^{k^{h-1}} \equiv c \pmod{p}$ . By the uniqueness of  $c_h$ ,  $c_{h-1} \equiv c_h^k$  and  $f_{h-1}(a) \equiv a \cdot c_h^k \pmod{p}$ . Now  $(f_h(a))^k \equiv (a \cdot c_h)^k \equiv a^k \cdot c_h^k \equiv f_{h-1}(a^k) \pmod{p}$ . Hence,  $(f_h(a), f_{h-1}(a^k)) \in E(F_c)$  and, by the argument above, the edges and vertices are in one-to-one correspondence, so  $F_1 \approx F_c$ .  $\square$

There is another property of this mapping that can be addressed. Consider  $a \in F_1$  and  $c \in F^0$ ; the order of the element  $ac \pmod{p}$  will be  $(\text{ord}_p a)(\text{ord}_p c)$ . That is, the isomorphism "preserves" orders between  $F_1$  and  $F_c$  in that the orders of corresponding elements in  $F_c$  are multiplied by the order of  $c$ .

**Theorem 30:** If  $a \in F_1$  and  $b \in F_c$  with  $c_h$  the cycle element such that  $b \equiv a \cdot c_h \pmod{p}$ , then  $\text{ord}_p b = (\text{ord}_p a)(\text{ord}_p c)$ .

**Proof:** By Theorem 21,  $\text{ord}_p a \mid k^h$  and thus  $\gcd(\text{ord}_p a, t) = 1$ . By Theorem 15,  $\text{ord}_p c = \text{ord}_p c_h \mid t$ , hence  $\gcd(\text{ord}_p a, \text{ord}_p c) = 1$ , and applying Theorem 6 gives the desired result.  $\square$

Some examples of the isomorphism described in Theorem 29 and Theorem 30 can be seen in Table 2.

**TABLE 2. Some Orders and Products in  $G_{41}^4$**

$a$	$c$	$ac$	$\text{ord}_p a$	$\text{ord}_p c$	$\text{ord}_p ac$
1	10	10	1	5	5
9	37	5	4	5	20
3	10	30	8	5	40

Finally, we prove a result that determines the height of the forests.

**Theorem 31:** If  $h_0$  is the minimal  $h$  such that  $p-1 \mid k^h t$ , then  $h_0$  is the height of the forests in  $G_p^k$ .

**Proof:**

- (i) If  $\gcd(k, p-1) = 1$ , then  $h_0 = 0$  and all the vertices are in cycles.
- (ii) If  $\gcd(k, p-1) \neq 1$ , then  $h_0 \geq 1$ . Let  $a$  be a vertex of order  $p-1$ . From Theorem 21,  $a$  must be at height  $h_0$  because  $\text{ord}_p a \mid k^{h_0} t$  but  $\text{ord}_p a \nmid k^{h_0-1} t$ . There are no vertices at a greater height since, for any vertex  $b$  in  $G_p^k$ ,  $\text{ord}_p b \mid p-1 \mid k^{h_0} t$ ; thus,  $b$  is at level  $h_0$  or lower in  $G_p^k$ .  $\square$

For example, in  $G_{41}^4$  we see that  $t = 5$  and  $41-1 = 40 \mid 4^2 5$ , which implies that the height of the forest is 2. This value is apparent in Figure 2.

## 7. PRIME POWERS

In the special case where the powers are prime, many of our results simplify. In particular, while we were able to prove that the forest structures were isomorphic with a general exponent  $k$ , we can completely characterize that structure if the exponent is prime. We will consider the digraph associated with a prime exponent  $q$ , letting  $p-1 = q^s t$ , where  $t$  is relatively prime to  $q$ .

**Corollary 32:** The indegree of a vertex in  $G_p^q$  is  $\begin{cases} 0 \text{ or } q & \text{if } p \equiv 1 \pmod{q}, \\ 1 & \text{otherwise.} \end{cases}$

**Proof:** This follows from Lemma 11 and Lemma 12 with  $k = q$ .  $\square$

This result implies that all the digraph components are cyclical if and only if  $p \not\equiv 1 \pmod{q}$ .

**Corollary 33:** If  $p \equiv 1 \pmod{q}$ , then any cycle vertex has  $q-1$  noncycle children.

**Proof:** This follows from Lemma 13.  $\square$

**Theorem 34:** If  $p \equiv 1 \pmod{q}$ , the  $q-1$  noncycle children of each cycle element are roots of complete  $q$ -nary trees.

**Proof:** Since the  $t$  forests in  $G_p^q$  are isomorphic and there are  $q^s t$  elements in the digraph,  $|F_1| = q^s - 1$ . Furthermore, Theorem 31 implies that the height of  $F_1$  is  $s$ . If  $F_1$  is not composed of

$q-1$  complete  $q$ -nary trees, there exists a vertex that has indegree 0 but is not at height  $s$ . This would imply that  $|F_1| < q^s - 1$ , a contradiction. Since all the forests are isomorphic to  $F_1$ , and  $F_1$  consists of complete  $q$ -nary trees, all the forests in  $G_p^q$  are complete  $q$ -nary trees as well.  $\square$

As an example, consider  $F_1$  in the digraph  $G_{109}^3$ , as shown in Figure 5. Since  $109-1 = 3^3(4)$  and  $45^3 \equiv 63^3 \equiv 1 \pmod{109}$ , 45 and 63 are roots of complete ternary trees with height  $3-1 = 2$ .

When the power is prime, we can say more about the orders of elements in the digraph  $G_p^q$ .

**Theorem 35:** A vertex  $a \in F_1^h$  if and only if  $\text{ord}_p a = q^h$ .

**Proof:** Consider Theorem 21 with  $k = q$  and  $c = 1$ , and hence  $d = 1$ . Then  $\text{ord}_p a | q^h$  if and only if  $a \in F_1^x$  for  $x \leq h$ . Having elements of order  $q^h$  in a level  $x$  less than  $h$  would imply that  $q^h | q^x$ , where  $x < h$ , a contradiction.  $\square$

Returning to  $G_{109}^3$  (Fig. 5), one can check that the orders of 3, 9, and 27 correspond to  $F_1^1$ ,  $F_1^2$ , and  $F_1^3$ .

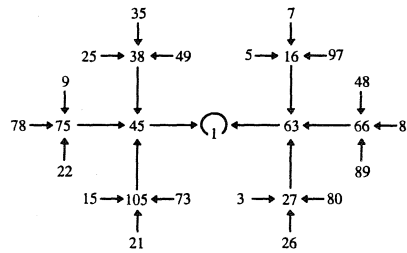


FIGURE 5. The Forest  $F_1$  in  $G_{109}^3$

**Corollary 36:** If  $a \in F_c^h$  then  $\text{ord}_p a = q^h \text{ord}_p c$ .

**Proof:** Theorem 35 and the multiplying principle of Theorem 30 give the desired result.  $\square$

## CONCLUSIONS

We have seen that many of the features of the digraph  $G_p^k$  can be determined in terms of properties of  $p$  and  $k$ . In particular, we have seen that the digraphs consist of components with exactly one cycle per component and that the forest structures associated with each cycle vertex throughout the digraph are isomorphic. The cycle lengths depend on the orders of the elements. We can also determine the height of the forests. In special cases, long cycles can be found and complete  $q$ -nary trees can be guaranteed.

While we have found a very rich structure for the digraphs associated with  $x^k \pmod p$ , it is natural to ask what other digraphs arising from functions such as these have a rich structure. The function  $x^k \pmod m$ , where  $m$  is not prime, will have a much different digraph since 0 will not necessarily be in a trivial cycle and primitive roots may not exist. In [2], the authors start to investigate this problem. On the other hand, looking at  $x^k$  in a finite field where 0 must be trivial and primitive roots always exist ought to lead to a theory like that seen in this paper. Digraphs

from functions such as  $x^k + 1 \pmod{p}$  will be difficult to handle because we cannot lean on the theory of orders of elements as in this paper. It would be interesting to know what kind of control on the digraphs can be obtained in such cases.

### ACKNOWLEDGMENT

This work was supported in part by NSF-REU grant DMS-9300555.

### REFERENCES

1. Earle L. Blanton, Jr., Spencer P. Hurd, & Judson S. McCranie. "On a Digraph Defined by Squaring Modulo  $n$ ." *The Fibonacci Quarterly* **30.4** (1992):322-34.
2. Earle L. Blanton, Jr., Spencer P. Hurd, & Judson S. McCranie. "On the Digraph Defined by Squaring mod  $m$ , When  $m$  Has Primitive Roots." *Cong. Numerantium* **82** (1991):167-77.
3. Hua Loo Keng. *Introduction to Number Theory*. Tr. Peter Shiu. Berlin: Springer-Verlag, 1982.
4. Nathan Jacobson. *Basic Algebra*, I. San Francisco: W. H. Freeman and Co., 1974.
5. James Strayer. *Elementary Number Theory*. Boston: PWS Publishing Co., 1994.

AMS Classification Numbers: 05C20, 11B50



### Author and Title Index

The AUTHOR, TITLE, KEY-WORD, ELEMENTARY PROBLEMS, and ADVANCED PROBLEMS indices for the first 30 volumes of *The Fibonacci Quarterly* have been completed by Dr. Charles K. Cook. Publication of the completed indices is on a 3.5-inch, high density disk. The price for a copyrighted version of the disk will be \$40.00 plus postage for non-subscribers, while subscribers to *The Fibonacci Quarterly* need only pay \$20.00 plus postage. For additional information, or to order a disk copy of the indices, write to:

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

The indices have been compiled using WORDPERFECT. Should you wish to order a copy of the indices for another wordprocessor or for a non-compatible IBM machine, please explain your situation to Dr. Cook when you place your order and he will try to accommodate you. **DO NOT SEND PAYMENT WITH YOUR ORDER.** You will be billed for the indices and postage by Dr. Cook when he sends you the disk. A star is used in the indices to indicate unsolved problems. Furthermore, Dr. Cook is working on a SUBJECT index and will also be classifying all articles by use of the AMS Classification Scheme. Those who purchase the indices will be given one free update of all indices when the SUBJECT index and the AMS Classification of all articles published in *The Fibonacci Quarterly* are completed.

# CONSTRUCTION OF SMALL CONSECUTIVE NIVEN NUMBERS

Brad Wilson

Department of Mathematics, SUNY College at Brockport, Brockport, NY 14420

(Submitted August 1994)

## 1. DEFINITIONS AND NOTATION

A Niven number is a number divisible by its digital sum. In [1] it is shown there can exist at most twenty consecutive Niven numbers; moreover, an infinite family of such is constructed where the first example requires over 4 billion digits. Here we get a lower bound on the number of digits in each of twenty consecutive Niven numbers and construct an example with nearly this few digits.

We start by recalling

**Definition:** A positive integer is called a *Niven number* if it is divisible by its digital sum.

**Example:** The number 12 is a Niven number since  $(1+2)|12$ . The number 11 is not a Niven number since  $(1+1) \nmid 11$ .

For  $n \in \mathbb{Z}$ , let  $s(n)$  denote the digital sum of  $n$ . Examples of 20 consecutive Niven numbers have a large number of digits. To represent these numbers nicely, we concatenate digits or blocks of digits. If  $a$  and  $b$  are blocks of digits, let  $ab$  be the concatenation of these blocks. To denote multiplication, we use  $a * b$ . Finally,  $a_k$  denotes the concatenation of  $k$  copies of  $a$ .

## 2. PRELIMINARY LEMMA

In [1], Cooper and Kennedy show that any sequence of twenty consecutive Niven numbers begins with a number congruent to 90 modulo 100. We push this idea further.

**Definition:** Let  $n \in \mathbb{Z}^+$ . A positive integer is a  $10^n$ -mark if it is congruent to  $9_{n-1}0$  modulo  $10^n$  but not congruent to  $9_n0$  modulo  $10^{n+1}$ .

What Cooper and Kennedy actually show is that a sequence of twenty consecutive Niven numbers must begin with a  $10^{2*n_1}$ -mark for some  $n_1 \in \mathbb{Z}^+$ .

**Lemma 1:** A sequence of twenty consecutive Niven numbers begins with a  $10^{280*n_2}$ -mark for some  $n_2 \in \mathbb{Z}^+$ .

**Proof:** Since twenty consecutive Niven numbers begin with a  $10^{2*n_1}$ -mark for some  $n_1 \in \mathbb{Z}^+$ , the digital sums of the first ten Niven numbers in our sequence are consecutive, as are the digital sums of the second ten Niven numbers in our sequence. Therefore, there is at least one number, say  $m$ , in the first ten Niven numbers whose digital sum is divisible by  $2^3$ . By the definition of a Niven number, this means  $m$  is divisible by  $2^3$ . Similarly, there exists such a number, say  $m'$ , among the second ten. We can take  $m$  and  $m'$  to differ by exactly 8. Then

$$s(m) - s(m') = 9 * 2 * n_1 - 8$$

as  $2 * n_1$  nines are converted to zeros upon crossing from the first to the second ten numbers if we start at a  $10^{2*n_1}$ -mark. Since  $9 * 2 * n_1 - 8 = s(m) - s(m') \equiv 0 \pmod{8}$ , we see that  $2 * n_1$  is a multiple of 8.

Using the same method, we see  $2 * n_1$  must also be a multiple of 5 and of 7. Taken together, this means that the first of our twenty consecutive Niven numbers is a  $10^{280*n_2}$ -mark with  $n_2 = \frac{2*n_1}{280} \in \mathbb{Z}^+$ .  $\square$

### 3. CONGRUENCE RESTRICTIONS OF THE DIGITAL SUM

In this section we develop congruence restrictions on the digital sum of our first Niven number. To do this, we assume  $\beta$  is the first of twenty consecutive Niven numbers, that it is a  $10^{280*n_2}$ -mark for fixed  $n_2 \in \mathbb{Z}^+$ , and that  $s(\beta) = \alpha$ . Then

$$\begin{aligned} (\alpha + i) | (\beta + i) \quad \text{for } i = 0, 1, \dots, 9, \\ (\alpha + j - 2520 * n_2) | (\beta + j) \quad \text{for } j = 10, 11, \dots, 19. \end{aligned}$$

Let

$$\gamma = \text{lcm}(\alpha, \alpha + 1, \dots, \alpha + 9)$$

and

$$\gamma' = \text{lcm}(\alpha + 10 - 2520 * n_2, \alpha + 11 - 2520 * n_2, \dots, \alpha + 19 - 2520 * n_2).$$

This gives us

$$\beta \equiv \alpha \pmod{\gamma}$$

and

$$\beta \equiv \alpha - 2520 * n_2 \pmod{\gamma'}.$$

By the Chinese remainder theorem, these are consistent if and only if

$$\gcd(\gamma, \gamma') | 2520 * n_2. \quad (1)$$

This condition reduces to congruence conditions on the prime divisors of  $A = \{2520 * n_2 - 19, 2520 * n_2 - 18, \dots, 2520 * n_2 - 1\}$ , the set of possible differences between  $\{\alpha, \alpha + 1, \dots, \alpha + 9\}$  and  $\{\alpha + 10 - 2520 * n_2, \dots, \alpha + 19 - 2520 * n_2\}$ . Let  $P$  be the set of prime divisors of the numbers in  $A$ . For  $p \in P$ , let  $v(p)$  be such that  $p^{v(p)} | 2520 * n_2$  but  $p^{v(p)+1} \nmid 2520 * n_2$ . Then condition (1) implies  $p^{v(p)+1} \nmid \gcd(\gamma, \gamma')$ , so  $p^{v(p)+1} \nmid \gamma$  or  $p^{v(p)+1} \nmid \gamma'$ , which can be restated as

$$\begin{aligned} \alpha \equiv 1, 2, \dots, p^{v(p)+1} - 10 \pmod{p^{v(p)+1}} \quad \text{or} \\ \alpha + 10 - 2520 * n_2 \equiv 1, 2, \dots, p^{v(p)+1} - 10 \pmod{p^{v(p)+1}}. \end{aligned} \quad (2)$$

Conversely, condition (2) assures  $p^{v(p)+1} \nmid \gcd(\gamma, \gamma')$  and  $p | \gcd(\gamma, \gamma')$  implies  $p \in P$ , so we get  $\gcd(\gamma, \gamma') | 2520 * n_2$ . Further,  $\alpha$  satisfies some additional congruences modulo powers of 2 and 5. Since  $\beta$  is a  $10^{280*n_2}$ -mark,  $\beta \equiv 990 \pmod{1000}$ . Then  $\beta \equiv 6 \pmod{8}$ , so

$$\alpha \equiv 6 \pmod{8}. \quad (3)$$

Similarly  $\beta \equiv 0 \pmod{5}$  means

$$\alpha \equiv 0 \pmod{5}. \quad (4)$$

These lead to

**Lemma 2:** A sequence of twenty consecutive Niven numbers must begin at a  $10^{560*n_3}$ -mark for some  $n_3 \in \mathbb{Z}^+$ .

**Proof:** Suppose not, i.e., suppose we have twenty consecutive Niven numbers beginning at a  $10^{280*n_2}$ -mark with  $n_2$  odd. Then by (2) we have

$$\begin{aligned}\alpha &\equiv 1, 2, \dots, 6 \pmod{16} \quad \text{or} \\ \alpha + 10 - 2520 * n_2 &\equiv 1, 2, \dots, 6 \pmod{16},\end{aligned}$$

so  $\alpha \equiv 0, 1, \dots, 6, 15 \pmod{16}$ . By (3) this means  $\alpha \equiv 6 \pmod{16}$ . Further,  $\beta \equiv 9990 \pmod{10000}$ , so  $\beta \equiv 6 \pmod{16}$ . Then  $\alpha + 18 - 2520 * n_2 \equiv 0 \pmod{16}$ , so  $16 | (\beta + 18)$ , which is a contradiction.  $\square$

As a result of Lemma 2, we see that  $2520 * n_2 \equiv 0 \pmod{16}$ , so the digital sums of  $\beta, \beta + 1, \dots, \beta + 19$  are consecutive modulo 16. Since  $\beta \equiv 6 \pmod{16}$ , we get

$$\alpha \equiv 6 \pmod{16}. \quad (5)$$

#### 4. OUTLINE OF METHOD

Assume  $n_2 \in 2\mathbb{Z}^+$  fixed and  $\alpha$  satisfies (2), (4), and (5). We outline how to construct the first of twenty consecutive Niven numbers  $\beta$  so that  $s(\beta) = \alpha$ . By our choice of  $\alpha$ , we can find a solution to

$$x \equiv \alpha - 2520 * n_2 \pmod{\gamma'} \quad (6)$$

and

$$x \equiv \alpha \pmod{\gamma}. \quad (7)$$

In fact, we can find infinitely many solutions differing from each other by multiples of  $\delta = \text{lcm}(\gamma, \gamma')$ . Let  $b$  be the least positive solution. We modify  $b$  by adding multiples of  $\delta$  so that the resulting number,  $b'$ , still satisfies (6) and (7) and is a  $10^{280*n_2}$ -mark. Finally, we may be able to modify  $b'$  by adding multiples of  $\delta$  so that the resulting number,  $\beta$ , still satisfies (6) and (7), is still a  $10^{280*n_2}$ -mark, and has a digital sum  $\alpha$ . Such a  $\beta$  is the first of twenty consecutive Niven numbers.

#### 5. AN EXAMPLE OF A SEQUENCE OF SMALL NIVEN NUMBERS

We construct a  $10^{280*4}$ -mark. This means  $n_2 = 4$ . We can solve the congruences (2), (4), and (5) for  $\alpha$  modulo  $p \in P$  to get  $\alpha = 15830$ . This leads to

$$\begin{aligned}\delta &= \text{lcm}(\alpha, \alpha + 1, \dots, \alpha + 19 - 10080) \\ &= 3048830655878437890226799866816603 \\ &\quad 2162694822826657046395002360702080.\end{aligned}$$

Solving for  $x$  in (6) and (7), we get

$$\begin{aligned}b = x &= 3634662087332653678027291977866148 \\ &\quad 019043614233737117568189046296950.\end{aligned}$$

Adding a suitable multiple of  $\delta$  (to get a  $10^{1120}$ -mark), we get

$$\begin{aligned}b' &= 21222185596541538670917359810786534 \\ &\quad 2621517582273610535177825131059_{1119}0.\end{aligned}$$



Continue to add multiples of  $\delta$  so as not to disturb the terminal 1121 digits of  $b'$ . In short, add multiples of  $5^6 * 10^{1114} * \delta$ . Doing this, we get

$$\beta = 49814979458796395830735187579935382447 \\ 76448858055060558725279140729_{601}59_{1119}0.$$

It is easy to check that this is a number with 1788 digits and digital sum 15830 and that  $\beta$  is the first of twenty Niven numbers.

## 6. LOWER BOUNDS ON THE NUMBER OF DIGITS

**Theorem 1:** The smallest sequence of twenty consecutive Niven numbers begins with a  $10^{1120}$ -mark of digital sum 15830.

**Proof:** Let  $\beta$  be the first of twenty consecutive Niven numbers and let  $\alpha = s(\beta)$ . Suppose  $\beta$  has fewer than 1789 digits (i.e., no more than in our example in the previous section). Since  $\beta$  is a  $10^{280*n_2}$ -mark with  $n_2$  even,  $n_2 = 2, 4$ , or  $6$ . A computer search shows there is no  $\alpha$  less than  $9 * 1789$  satisfying (2), (4), and (5) with  $n_2 = 2, 4$ , or  $6$  other than  $\alpha = 15830$  for  $n_2 = 4$ .  $\square$

In the last section we saw an example with 1788 digits. This need not be the smallest, but it is close to the smallest.

**Theorem 2:** The smallest sequence of twenty consecutive Niven numbers begins with a number having at least 1760 digits.

**Proof:** By Theorem 1, we know the digital sum of the first number is 15830. Given that the terminal digit is a zero, there are at least  $1+15830/9$  digits.  $\square$

## REFERENCE

1. C. Cooper & R. Kennedy. "On Consecutive Niven Numbers." *The Fibonacci Quarterly* 31.2 (1993):146-51.

AMS Classification Number: 11A63



# SUMS OF POWERS OF INTEGERS VIA GENERATING FUNCTIONS

F. T. Howard

Wake Forest University, Winston-Salem, NC 27109

(Submitted August 1994)

## 1. INTRODUCTION

Let

$$S_{k,n}(a, d) = a^k + (a+d)^k + (a+2d)^k + \cdots + [a+(n-1)d]^k, \quad (1.1)$$

where  $k$  and  $n$  are nonnegative integers with  $n > 0$ , and  $a$  and  $d$  are complex numbers with  $d \neq 0$ . We shall use the notation

$$S_{k,n} = S_{k,n}(1, 1) = 1^k + 2^k + \cdots + n^k. \quad (1.2)$$

Similarly, let  $T_{k,n}(a, d)$  be the alternating sum

$$T_{k,n}(a, d) = a^k - (a+d)^k + (a+2d)^k - \cdots + (-1)^{n-1}[a+(n-1)d]^k, \quad (1.3)$$

and let

$$T_{k,n} = T_{k,n}(1, 1) = 1^k - 2^k + 3^k - \cdots + (-1)^{n-1}n^k. \quad (1.4)$$

It is, of course, well known that

$$S_{k,0} = n, \quad S_{k,1} = n(n+1)/2, \quad S_{k,2} = n(n+1)(2n+1)/6;$$

and so on. Many different writers have worked on the problem of finding simple formulas for  $S_{k,n}$ , and many different methods have been used; see [3], [5], [6], [9], [10] for just a small sampling of recent articles. The formulas for  $T_{k,n}$  are certainly less well known.

In the present paper we use generating functions to find new recurrences for  $S_{k,n}(a, d)$  and  $T_{k,n}(a, d)$ . We also show how  $S_{k,n}(a, d)$  and  $T_{k,n}(a, d)$  can be determined from  $S_{k-1,n}(a, d)$  and  $T_{k-1,n}(a, d)$ , respectively, and we show how  $S_{k,n}(a, d)$  and  $T_{k,n}(a, d)$  can be expressed in terms of Bernoulli numbers. One of the main results is a new "lacunary" recurrence formula for  $S_{k,n}$  with gaps of 6 (Theorem 3.1); that is, we can use the formula to find  $S_{m,n}$  for  $m = 0, 1, \dots, 5$ ; then, using only  $S_{m,n}$ , we can find  $S_{6+m,n}$ ; then, using only  $S_{m,n}$  and  $S_{6+m,n}$ , we can find  $S_{12+m,n}$ , and so on. There is a similar recurrence for  $T_{k,n}$ .

There are several motivations for this paper: (1) A recent article by Wiener [10] dealt with equation (1.1) and generalized some well-known properties of  $S_{k,n}$ . We show how the formulas of [10] can be derived very quickly and how they can be extended. (2) In a recent article by Howard [4], formulas were found which connected Bernoulli numbers to  $T_{k,n}$ . Evidently, the properties of  $T_{k,n}$  are not well known, so the results of [4] are a stimulus to study  $T_{k,n}$  and  $T_{k,n}(a, d)$  in some detail. (3) The new lacunary recurrences mentioned above are useful and easy to use, and (in the writer's opinion) they are of considerable interest. In Section 3 we illustrate the formulas by computing  $S_{6,n}$ ,  $S_{12,n}$ , and  $S_{18,n}$ ; in Section 6 we compute  $T_{4,n}$ ,  $T_{10,n}$ , and  $T_{16,n}$ . (4) Perhaps the main purpose of the paper is to show how generating functions provide a simple, unified approach to the study of sums of powers of integers. The many, and often repetitious

articles on  $S_{k,n}$  that have appeared in the last twenty-five years seem to indicate a need for such a unified approach.

## 2. RECURRENCES FOR $S_{k,n}(a, d)$

We first note that by (1.1) the exponential generating function for  $S_{k,n}(a, d)$  is

$$\sum_{k=0}^{\infty} S_{k,n}(a, d) \frac{x^k}{k!} = e^{ax} + e^{(a+d)x} + \dots + e^{[a+(n-1)d]x} = \frac{e^{(a+nd)x} - e^{ax}}{e^{dx} - 1}. \quad (2.1)$$

We can use (2.1) to prove the next two theorems in a very direct way.

**Theorem 2.1:** Let  $k \geq 0$  and  $n > 0$ . We have the following recurrences for  $S_{k,n}(a, d)$ :

$$\sum_{j=0}^k \binom{k+1}{j} d^{k+1-j} S_{j,n}(a, d) = (a+nd)^{k+1} - a^{k+1}, \quad (2.2)$$

$$\sum_{j=0}^k (-1)^j \binom{k+1}{j} d^{k+1-j} S_{j,n}(a, d) = (-1)^k [(a+nd-d)^{k+1} - (a-d)^{k+1}]. \quad (2.3)$$

**Proof:** From (2.1) we have

$$(e^{dx} - 1) \sum_{k=0}^{\infty} S_{k,n}(a, d) \frac{x^k}{k!} = e^{(a+nd)x} - e^{ax}, \text{ i.e.,} \\ \sum_{j=1}^{\infty} d^j \frac{x^j}{j!} \cdot \sum_{k=0}^{\infty} S_{k,n}(a, d) \frac{x^k}{k!} = \sum_{j=0}^{\infty} [(a+nd)^j - a^j] \frac{x^j}{j!}. \quad (2.4)$$

If we examine both sides of (2.4) and equate coefficients of  $x^{k+1}/(k+1)!$ , we have (2.2). Now if we replace  $x$  by  $-x$  in (2.1), we have, after simplification,

$$\sum_{k=0}^{\infty} (-1)^k S_{k,n}(a, d) \frac{x^k}{k!} = \frac{e^{(d-a)x} - e^{(d-a-nd)x}}{e^{dx} - 1}. \quad (2.5)$$

Multiplying both sides of (2.5) by  $e^{dx} - 1$  and equating coefficients of  $x^{k+1}/(k+1)!$ , we have (2.3). This completes the proof.

Formulas (2.2) and (2.3) generalize known formulas for  $a = d = 1$  [8, p. 159]. We note that (2.2) was found by Wiener [10]; see also [2, p. 169]. Bachmann [1, p. 28] found a recurrence for  $S_{k,n}(a, d)$  involving only  $S_{j,n-1}$  for  $j = 1, \dots, k$ .

We now add (2.2) and (2.3) to obtain the next theorem.

**Theorem 2.2:** For  $k = 1, 2, 3, \dots$ , we have

$$2 \sum_{j=0}^{k-1} \binom{2k}{2j} d^{2k-2j} S_{2j,n}(a, d) = (a+nd)^{2k} - (a+nd-d)^{2k} + (a-d)^{2k} - a^{2k},$$

and for  $k = 2, 3, \dots$ , we have

$$2 \sum_{j=1}^{k-1} \binom{2k-1}{2j-1} d^{2k-2j} S_{2j-1,n}(a, d) = (a+nd)^{2k-1} - (a+nd-d)^{2k-1} + (a-d)^{2k-1} - a^{2k-1}.$$

Theorem 2.2 can be compared to results of Wiener [10] and Riordan [8, p. 160].

### 3. RECURRENCES WITH INDICES $6K + M$

We now show how to find formulas of the type (2.2) where the index  $j$  varies only over integers of the form  $6k + m$ , with  $0 \leq m \leq 5$ . To the writer's knowledge, these formulas are new. After stating Theorem 3.1 and its corollary, we give some applications; the proof of Theorem 3.1 is given at the end of this section.

Let  $\theta$  be the complex number  $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$ , so

$$\theta^3 = 1 \quad \text{and} \quad \theta^2 + \theta + 1 = 0, \quad (3.1)$$

and define the sequence  $\{w_j\}$  in the following way:

$$\begin{aligned} w_j &= 1 + (-1)^j (\theta^j + \theta^{6-j}) \quad \text{for } j = 0, 1, \dots, 5, \\ w_j &= w_{6+j} \quad \text{for } j = 0, \pm 1, \pm 2, \dots \end{aligned} \quad (3.2)$$

For example,  $w_{-1} = w_5 = 2$ . The values of  $w_j$  for  $j = 0, 1, \dots, 5$  are given in the following table:

$j$	0	1	2	3	4	5
$w_j$	3	2	0	-1	0	2

(3.3)

**Theorem 3.1** Let  $w_j$  be defined by (3.2) and (3.3). Then, for  $m = 0, 1, \dots, 5$  and  $n > 0, k \geq 0$ , we have:

$$\begin{aligned} & 6 \sum_{j=0}^k \binom{6k+m+3}{6j+m} d^{6k-6j+3} S_{6j+m,n}(a, d) \\ &= \sum_{j=1}^{6k+m+1} \binom{6k+m+3}{j} d^{6k+m+3-j} w_{m-j} [(a-d+nd)^j - (a-d)^j]. \end{aligned}$$

**Corollary:** For  $m = 0, 1, \dots, 5$  and  $n > 0, k \geq 0$ , we have:

$$\binom{6k+m+3}{3} S_{6k+m,n} = - \sum_{j=0}^{k-1} \binom{6k+m+3}{6j+m} S_{6j+m,n} + \frac{1}{6} \sum_{j=1}^{6k+m+1} \binom{6k+m+3}{j} w_{m-j} n^j.$$

The corollary gives us an easy way to write  $S_{k,n}$  as a polynomial in  $n$  of degree  $k+1$ . In particular, we have for  $m = 0, 1, \dots, 5$ :

$$\binom{m+3}{3} S_{m,n} = \frac{1}{6} \sum_{j=1}^{m+1} \binom{m+3}{j} w_{m-j} n^j.$$

Using the corollary, we easily compute  $S_{0,n} = n$  and

$$\binom{9}{3} S_{6,n} = -n + \frac{1}{6} \sum_{j=1}^7 \binom{9}{j} w_{-j} n^j,$$

By (3.2) and (3.3), the numbers  $w_{-j}$  are easy to find. We have  $w_{-j} = 2$  for  $j = 1, 5, 7$ ;  $w_{-j} = 0$  for  $j = 2$  and  $4$ ;  $w_{-j} = -1$  for  $j = 3$ ;  $w_{-j} = 3$  for  $j = 6$ . Thus, we have

$$S_{6,n} = \frac{1}{42} n - \frac{1}{6} n^3 + \frac{1}{2} n^5 + \frac{1}{2} n^6 + \frac{1}{7} n^7.$$

Continuing in the same way, we have

$$\binom{15}{3} S_{12,n} = -n - \binom{15}{6} S_{6,n} + \frac{1}{6} \sum_{j=1}^{13} \binom{15}{j} w_{-j} n^j,$$

so

$$S_{12,n} = -\frac{691}{2730} n + \frac{5}{3} n^3 - \frac{33}{10} n^5 + \frac{22}{7} n^7 - \frac{11}{6} n^9 + n^{11} + \frac{1}{2} n^{12} + \frac{1}{13} n^{13}.$$

It is easy to keep going:

$$\binom{21}{3} S_{18,n} = -n - \binom{21}{6} S_{6,n} - \binom{21}{12} S_{12,n} + \frac{1}{6} \sum_{j=1}^{19} \binom{21}{j} w_{-j} n^j,$$

which gives

$$\begin{aligned} S_{18,n} = & \frac{43867}{798} n - \frac{3617}{10} n^3 + 714 n^5 - \frac{23494}{35} n^7 + \frac{1105}{3} n^9 - \frac{663}{5} n^{11} \\ & + 34 n^{13} - \frac{34}{5} n^{15} + \frac{3}{2} n^{17} + \frac{1}{2} n^{18} + \frac{1}{19} n^{19}. \end{aligned}$$

Another application of Theorem 3.1, involving Bernoulli numbers, is given in Section 4.

**Proof of Theorem 3.1:** Let

$$A(x) = \frac{e^{(a+nd)x} - e^{ax}}{e^{dx} - 1} = \sum_{k=0}^{\infty} S_{k,n}(a, d) \frac{x^k}{k!}, \quad (3.4)$$

and define  $A_0(x)$ ,  $A_1(x)$ , and  $A_2(x)$  as follows:

$$A_0(x) = \frac{1}{3} [A(x) + A(\theta x) + A(\theta^2 x)] = \sum_{k=0}^{\infty} S_{3k,n}(a, d) \frac{x^{3k}}{(3k)!}, \quad (3.5)$$

$$A_1(x) = \frac{1}{3} [(A(x) + \theta^2 A(\theta x) + \theta A(\theta^2 x))] = \sum_{k=0}^{\infty} S_{3k+1,n}(a, d) \frac{x^{3k+1}}{(3k+1)!}, \quad (3.6)$$

$$A_2(x) = \frac{1}{3} [A(x) + \theta A(\theta x) + \theta^2 A(\theta^2 x)] = \sum_{k=0}^{\infty} S_{3k+2,n}(a, d) \frac{x^{3k+2}}{(3k+2)!}. \quad (3.7)$$

The equalities on the extreme right of (3.5), (3.6), and (3.7) follow from (3.1) and (3.4). Using (3.4) and the equalities on the extreme left of (3.5), (3.6), and (3.7), we can write

$$A_m(x) = \frac{N_m}{3D_m} \quad (m = 0, 1, 2),$$

with  $D_0 = D_1 = D_2 = (e^{dx} - 1)(e^{\theta dx} - 1)(e^{\theta^2 dx} - 1)$ . Using (3.1), it is easy to compute

$$D_0 = D_1 = D_2 = 6 \sum_{k=0}^{\infty} d^{6k+3} \frac{x^{6k+3}}{(6k+3)!}.$$

The formulas for  $N_0$ ,  $N_1$ , and  $N_2$  are more complicated, but they are easy to work out from (3.4), (3.5), (3.6), and (3.7). We first note that, for  $m = 0, 1, 2$ , we have

$$A_m(x) = \frac{1}{3} [A(x) + \theta^{3-m} A(\theta x) + \theta^m A(\theta^2 x)] = \sum_{k=0}^{\infty} S_{3k+m,n}(a, d) \frac{x^{3k+m}}{(3k+m)!}.$$

Thus, we have:

$$\begin{aligned} N_m &= (e^{(a+nd)x} - e^{ax})(e^{-dx} - e^{d\theta x} - e^{d\theta^2 x} + 1) \\ &\quad + \theta^{3-m} (e^{(a+nd)\theta x} - e^{a\theta x})(e^{-d\theta x} - e^{dx} - e^{d\theta^2 x} + 1) \\ &\quad + \theta^m (e^{(a+nd)\theta^2 x} - e^{a\theta^2 x})(e^{-d\theta^2 x} - e^{d\theta x} - e^{dx} + 1). \end{aligned} \quad (3.8)$$

We now multiply, regroup, and expand the terms in (3.8). For example, we have

$$\begin{aligned} e^{(a+nd-d)x} + \theta^{3-m} e^{(a+nd-d)\theta x} + \theta^m e^{(a+nd-d)\theta^2 x} &= \sum_{j=0}^{\infty} (a+nd-d)^j (1 + \theta^{3-m+j} + \theta^{m+2j}) \frac{x^j}{j!} \\ &= 3 \sum_{j=0}^{\infty} (a+nd-d)^{3j+m} \frac{x^{3j+m}}{(3j+m)!}. \end{aligned}$$

Regrouping and expanding the other terms in (3.8), we have, for  $m = 0, 1$ , and  $2$ ,

$$\begin{aligned} \frac{1}{3} N_m &= \sum_{j=0}^{\infty} [(a+nd+d)^{3j+m} + (a+nd)^{3j+m} + (a+nd-d)^{3j+m} - (a+d)^{3j+m} - a^{3j+m} \\ &\quad - (a-d)^{3j+m}] \frac{x^{3j+m}}{(3j+m)!} - 3 \sum_{j=0}^{\infty} d^{3j} \frac{x^{3j}}{(3j)!} \cdot \sum_{j=0}^{\infty} [(a+nd)^{3j+m} - a^{3j+m}] \frac{x^{3j+m}}{(3j+m)!}. \end{aligned}$$

Since

$$D_m \sum_{k=0}^{\infty} S_{3k+m,n}(a, d) \frac{x^{3k+m}}{(3k+m)!} = \frac{1}{3} N_m, \quad (3.9)$$

we can equate coefficients of  $x^{3k+m} / (3k+m)!$  in (3.9) and state the following: For  $m = 0, 1, 2$ ,

$$\begin{aligned} &3 \sum_{j=0}^k [1 + (-1)^{k-j+1}] \binom{3k+m}{3j+m} d^{3k-3j} S_{3j+m,n}(a, d) \\ &= (a+nd+d)^{3k+m} + (a+nd)^{3k+m} + (a+nd-d)^{3k+m} - (a+d)^{3k+m} \\ &\quad - a^{3k+m} - (a-d)^{3k+m} - 3 \sum_{j=0}^k \binom{3k+m}{3j+m} [(a+nd)^{3j+m} - a^{3j+m}] d^{3k-3j}. \end{aligned} \quad (3.10)$$

At this point we observe how the sums in (3.10) can be simplified. By using properties of  $\theta$  and the binomial theorem, we see that

$$\begin{aligned}
 & 3 \sum_{j=0}^k \binom{3k+m}{3j+m} (a+nd)^{3j+m} d^{3k-3j} \\
 &= (d+a+nd)^{3k+m} + \theta^{2m} (d+a\theta + nd\theta)^{3k+m} + \theta^m (d+a\theta^2 + nd\theta^2)^{3k+m} \\
 &= (d+a+nd)^{3k+m} + \theta^{2m} [-d\theta^2 + \{(a-d)+nd\}\theta]^{3k+m} + \theta^m [-d\theta + \{(a-d)+nd\}\theta^2]^{3k+m} \\
 &= (d+a+nd)^{3k+m} + \sum_{j=0}^{3k+m} \binom{3k+m}{j} (-1)^{k+m-j} d^{3k+m-j} (\theta^{m-j} + \theta^{2m+j}) (a-d+nd)^j \\
 &= (d+a+nd)^{3k+m} + \sum_{j=0}^{3k+m} \binom{3k+m}{j} (-1)^k d^{3k+m-j} (-1+w_{m-j}) (a-d+nd)^j. \tag{3.11}
 \end{aligned}$$

We substitute (3.11) [and also (3.11) with  $n=0$ ] into (3.10), and we consider the two cases of  $k$  even and  $k$  odd. Then using the binomial theorem and the fact that  $w_{m-j}=0$  when  $j=6k+m+2$ , we can easily simplify (3.10) to get Theorem 3.1. This completes the proof.

#### 4. $S_{k,n}(a, d)$ IN TERMS OF BERNOULLI NUMBERS

The Bernoulli polynomial  $B_k(x)$  may be defined by means of the generating function

$$\frac{xe^{xz}}{e^x - 1} = \sum_{k=0}^{\infty} B_k(z) \frac{x^k}{k!}. \tag{4.1}$$

When  $z=0$ , we have the ordinary Bernoulli number  $B_k$ , i.e.,  $B_k(0)=B_k$ . It is well known [2, pp. 48-49] that  $B_0=1$ ,  $B_1=-\frac{1}{2}$ ,  $B_2=\frac{1}{6}$ , and  $B_{2m+1}=0$  for  $m>0$ . It follows from (4.1) that

$$B_k(z) = \sum_{j=0}^k \binom{k}{j} B_{k-j} z^j. \tag{4.2}$$

Comparing (4.1) and (1.2), we see

$$S_{k,n}(a, d) = \frac{d^k}{k+1} \left[ B_{k+1} \left( \frac{a}{d} + n \right) - B_{k+1} \left( \frac{a}{d} \right) \right]. \tag{4.3}$$

Now, for fixed  $a$  and  $d$ , suppose we write  $S_{k,n}(a, d)$  as a polynomial in  $(a-d+nd)$ ; i.e.,

$$\begin{aligned}
 S_{k,n}(a, d) &= S_{k,n-1}(a, d) + [a + (n-1)d]^k \\
 &= v_{k,0} + v_{k,1}(a-d+nd) + v_{k,2}(a-d+nd)^2 + \cdots + v_{k,k+1}(a-d+nd)^{k+1}. \tag{4.4}
 \end{aligned}$$

By (4.2) and (4.3), we have the following result.

**Theorem 4.1:** If  $S_{k,n}(a, d)$  is written as a polynomial in  $(a-d+nd)$  and  $v_{k,j}$  is defined by (4.4) for  $j=1, 2, \dots, k+1$ , then

$$\begin{aligned}
 v_{k,j} &= \frac{1}{k+1} \binom{k+1}{j} d^{k-j} B_{k+1-j} \quad (1 \leq j \leq k-1), \\
 v_{k,k} &= \frac{1}{2}, \quad v_{k,k+1} = \frac{1}{d(k+1)}, \quad v_{k,0} = \frac{d^k}{k+1} \left[ B_{k+1} - B_{k+1} \left( \frac{a}{d} \right) \right].
 \end{aligned}$$

When  $a = d = 1$ , Theorem 4.1 gives the well-known result [2, pp. 154-55]:

$$S_{k,n} = S_{k,n}(1, 1) = n^k + \frac{1}{k+1} \sum_{j=1}^{k+1} \binom{k+1}{j} B_{k+1-j} n^j.$$

Here, we can give another application of Theorem 3.1. Since  $v_{k,1} = B_k$  for  $k > 1$ , and  $a = d = 1$ , we see from the corollary to Theorem 3.1 that, for  $m = 0, \dots, 5$  and  $6k + m > 1$ ,

$$\binom{6k+m+3}{3} B_{6k+m} = - \sum_{j=1}^{k-1} \binom{6k+m+3}{6j+m} B_{6j+m} + \frac{1}{6} (6k+m+3) w_{m-1}. \quad (4.5)$$

Formula (4.5) is a lacunary recurrence for the Bernoulli numbers that is equivalent to a formula of Ramanujan [7, pp. 3-4]. See also [8, pp. 136-37].

### 5. FINDING $S_{k,n}(a, d)$ FROM $S_{k-1,n}(a, d)$

Several writers, like Khan [6], have pointed out that when  $a = d = 1$ , if we know just  $S_{k-1,n}$ , we can evaluate  $S_{k,n}$ . Using (2.1), it is easy to prove this and to generalize it. First of all, we can use mathematical induction on (2.2) to prove that  $S_{k,n}(a, d)$  is a polynomial in  $n$  of degree  $k+1$ , with constant term equal to 0. (That also follows from Section 4.) Thus, for fixed  $a$  and  $d$ , we can write

$$S_{k,n}(a, d) = c_{k,1}n + c_{k,2}n^2 + \dots + c_{k,k+1}n^{k+1}. \quad (5.1)$$

**Theorem 5.1:** For fixed  $a$  and  $d$ , let  $c_{k,j}$  be defined by (5.1) for  $j = 1, \dots, k+1$ . Then, for  $k \geq 1$ , we have

$$c_{k,j} = \frac{kd}{j} c_{k-1,j-1} \quad (j = 2, \dots, k+1), \quad (5.2)$$

$$c_{k,1} = a^k - c_{k,2} - c_{k,3} - \dots - c_{k,k+1}. \quad (5.3)$$

**Proof:** Define the polynomial  $P_k(z)$  by means of the generating function

$$\sum_{k=0}^{\infty} P_k(z) \frac{x^k}{k!} = \frac{e^{(a+zd)x} - e^{ax}}{e^{dx} - 1}, \quad (5.4)$$

so  $P_k(n) = S_{k,n}(a, d)$ . This implies that

$$P_k(z) = c_{k,1}z + c_{k,2}z^2 + \dots + c_{k,k+1}z^{k+1} \quad (5.5)$$

for all positive integers  $z$ , and hence for all complex numbers  $z$ . Now we differentiate both sides of (5.4) with respect to  $z$  to obtain

$$\sum_{k=0}^{\infty} P'_k(z) \frac{x^k}{k!} = \frac{dx e^{(a+zd)x}}{e^{dx} - 1} = \frac{dx (e^{(a+zd)x} - e^{ax})}{e^{dx} - 1} + \frac{dx e^{ax}}{e^{dx} - 1}. \quad (5.6)$$

We recall the definition of the Bernoulli polynomials, formula (4.1), and we see that

$$\frac{dx e^{ax}}{e^{dx} - 1} = \sum_{k=0}^{\infty} d^k B_k \left( \frac{a}{d} \right) \frac{x^k}{k!}, \quad (5.7)$$



and we note that  $B_k\left(\frac{a}{d}\right)$  is independent of  $z$ . From (5.4), (5.6), and (5.7), we have

$$\sum_{k=0}^{\infty} P'_k(z) \frac{x^k}{k!} = d \sum_{k=0}^{\infty} P_k(z) \frac{x^{k+1}}{k!} + \sum_{k=0}^{\infty} d^k B_k\left(\frac{a}{d}\right) \frac{x^k}{k!}. \quad (5.8)$$

Equating coefficients of  $x^k / k!$  in (5.8), we have

$$P'_k(z) = dkP_{k-1}(z) + d^k B_k\left(\frac{a}{d}\right). \quad (5.9)$$

Thus, by using (5.5) and equating coefficients of  $z^{j-1}$  in (5.9), we have

$$c_{k,j} = \frac{kd}{j} c_{k-1,j-1} \quad (j = 2, \dots, k+1).$$

Also, by (5.1) and the fact that  $S_{k,1}(a, d) = a^k$ , we have

$$d^k B_k\left(\frac{a}{d}\right) = c_{k,1} = a^k - c_{k,2} - c_{k,3} - \dots - c_{k,k+1},$$

and the proof is complete.

Thus, if we know the coefficients of  $S_{k-1,n}(a, d)$ , we can determine the coefficients  $c_{k,j}$  of  $S_{k,n}(a, d)$  for  $j = 2, \dots, k+1$  from (5.2) and then compute  $c_{k,1}$  from (5.3). For example,

$$S_{0,n}(a, d) = c_{0,1}n = n,$$

so, by (5.2) and (5.3), we have  $c_{1,2} = \frac{d}{2} c_{0,1} = \frac{d}{2}$ , and  $c_{1,1} = a - \frac{d}{2}$ ; that is,

$$S_{1,n}(a, d) = c_{1,1}n + c_{1,2}n^2 = \left(a - \frac{d}{2}\right)n + \frac{d}{2}n^2. \quad (5.10)$$

Equivalently, by (5.9), we can integrate to find  $P_k(z)$ :

$$P_k(z) = dk \int P_{k-1}(z) dz + d^k B_k\left(\frac{a}{d}\right)z, \quad (5.11)$$

[The  $dz$  in (5.11) should not be confused with the complex variable  $d$ .] The constant of integration is 0, and  $c_{k,1} = d^k B_k\left(\frac{a}{d}\right)$  can be found by means of (5.3). When  $a = d = 1$  and  $k > 1$ ,  $B_k\left(\frac{a}{d}\right)$  is the  $k^{\text{th}}$  Bernoulli number. We illustrate (5.11) by finding  $S_{2,n}(a, d)$ . From (5.10) and (5.11) we have, after integrating  $S_{1,n}(a, d)$  with respect to  $n$  and multiplying by  $3d$ ,

$$S_{2,n}(a, d) = d^2 B_2\left(\frac{a}{d}\right)n + \left(ad - \frac{d^2}{2}\right)n^2 + \frac{d^2}{3}n^3,$$

so by (5.3) we have

$$S_{2,n}(a, d) = \left(a^2 - ad + \frac{d^2}{6}\right)n + \left(ad - \frac{d^2}{2}\right)n^2 + \frac{d^2}{3}n^3.$$

# 6. RECURRENCES FOR $T_{k,n}(a, d)$

Let  $T_{k,n}(a, d)$  be defined by (1.3), with  $k \geq 0$ ,  $n > 0$ , and  $d \neq 0$ . This type of sum is discussed briefly by Bachmann [1, pp. 27-29] and Turner [9]. We note that  $T_{k,n}(a, d)$  can be expressed in terms of  $S_{k,n}(a, d)$  in the following ways:

$$\begin{aligned} T_{k,2n+1}(a, d) &= S_{k,n+1}(a, 2d) - S_{k,n}(a + d, 2d), \\ T_{k,2n}(a, d) &= S_{k,n}(a, 2d) - S_{k,n}(a + d, 2d). \end{aligned}$$

Also, if  $a = d = 1$ , then

$$T_{k,2n} = S_{k,2n} - 2^{k-1}S_{k,n}, \quad (6.1)$$

which makes some of the formulas for  $T_{k,n}$  trivial in light of the results of Sections 1-5.

In the remainder of the paper, we find formulas for  $T_{k,n}(a, d)$  that correspond to the ones for  $S_{k,n}(a, d)$ . The essential tool is the generating function

$$\sum_{k=0}^{\infty} T_{k,n}(a, d) \frac{x^k}{k!} = e^{ax} - e^{(a+d)x} + \dots + (-1)^{n-1} e^{(a+nd-d)x} = \frac{(-1)^{n-1} e^{(a+nd)x} + e^{ax}}{e^{dx} + 1}. \quad (6.2)$$

The following three theorems are analogs of Theorems 2.1, 2.2, and 3.1, and they are proved in exactly the same way as those earlier theorems. The proofs, which use (6.2) instead of (2.1), are omitted.

**Theorem 6.1:** We have the following two recurrences for  $T_{k,n}(a, d)$ : For  $k \geq 1, n > 0$ ,

$$2T_{k+1,n}(a, d) + \sum_{j=0}^k \binom{k+1}{j} d^{k+1-j} T_{j,n}(a, d) = (-1)^{n-1} (a + nd)^{k+1} + a^{k+1}, \quad (6.3)$$

$$2T_{k+1,n}(a, d) + \sum_{j=0}^k \binom{k+1}{j} (-d)^{k+1-j} T_{j,n}(a, d) = (-1)^{n+1} (a + nd - d)^{k+1} + (a - d)^{k+1}. \quad (6.4)$$

Formula (6.3) generalizes a formula of Turner [9].

**Theorem 6.2:** For  $k = 1, 2, 3, \dots$ , we have

$$\begin{aligned} &2 \sum_{j=0}^{k-1} \binom{2k-1}{2j} d^{2k-2j-1} T_{2j,n}(a, d) \\ &= (-1)^{n-1} (a + nd)^{2k-1} + (-1)^n (a + nd - d)^{2k-1} - (a - d)^{2k-1} + a^{2k-1}, \end{aligned}$$

and

$$\begin{aligned} &2 \sum_{j=1}^k \binom{2k}{2j-1} d^{2k-2j+1} T_{2j-1,n}(a, d) \\ &= (-1)^{n-1} (a + nd)^{2k} + (-1)^n (a + nd - d)^{2k} - (a - d)^{2k} + a^{2k}. \end{aligned}$$

**Theorem 6.3:** Let  $w_j$  be defined by (3.2) and (3.3). Then, for  $m = 0, 1, \dots, 5$ , and  $n > 0, k \geq 0$ , we have

$$\begin{aligned}
 8T_{6k+m,n}(a, d) = & -6 \sum_{j=0}^{k-1} \binom{6k+m}{6j+m} a^{6k-6j} T_{6j+m,n}(a, d) \\
 & + \sum_{j=0}^{6k+m-1} \binom{6k+m}{j} a^{6k+m-j} w_{m-j} [(-1)^{n-1} (a-d+nd)^j + (a-d)^j] \\
 & + 4[(-1)^{n-1} (a-d+nd)^{6k+m} + (a-d)^{6k+m}].
 \end{aligned}$$

**Corollary:** Let  $n > 0$ ,  $k \geq 0$ . For  $m = 0, 1, \dots, 5$ , and  $m$  and  $k$  not both 0, we have

$$\begin{aligned}
 8T_{6k+m,n} = & -6 \sum_{j=0}^{k-1} \binom{6k+m}{6j+m} T_{6j+m,n} + (-1)^{n-1} \sum_{j=0}^{6k+m-1} \binom{6k+m}{j} w_{m-j} n^j \\
 & + 4(-1)^{n-1} n^{6k+m} + [1 + (-1)^{n-1}] w_m.
 \end{aligned}$$

Note that, for  $m = 1, 2, \dots, 5$ , we have

$$8T_{m,n} = (-1)^{n-1} \sum_{j=1}^{m-1} \binom{m}{j} w_{m-j} n^j + 4(-1)^{n-1} n^m + [1 + (-1)^{n-1}] w_m.$$

To illustrate Theorem 6.3, we first calculate  $T_{4,n}$ :

$$8T_{4,n} = (-1)^{n-1} \left[ 4n^4 + \binom{4}{3} 2n^3 + \binom{4}{2} 0n^2 + \binom{4}{1} (-1)n + 0 \right];$$

so

$$T_{4,n} = (-1)^{n-1} \left( -\frac{1}{2}n + n^3 + \frac{1}{2}n^4 \right).$$

Then

$$8T_{10,n} = -6 \binom{10}{4} T_{4,n} + (-1)^{n-1} \sum_{j=1}^9 \binom{10}{j} w_{4-j} n^j + (-1)^{n-1} 4n^{10},$$

which gives us

$$T_{10,n} = (-1)^{n-1} \left( \frac{155}{2}n - \frac{255}{2}n^3 + 63n^5 - 15n^7 + \frac{5}{2}n^9 + \frac{1}{2}n^{10} \right).$$

Continuing in the same way, we have

$$8T_{16,n} = -6 \binom{16}{4} T_{4,n} - 6 \binom{16}{10} T_{10,n} + (-1)^{n-1} \sum_{j=1}^{15} \binom{16}{j} w_{4-j} n^j + (-1)^{n-1} 4n^{16},$$

which gives us

$$\begin{aligned}
 T_{16,n} = & (-1)^{n-1} \left( -\frac{929569}{2}n + 764540n^3 - 377286n^5 + 88660n^7 \right. \\
 & \left. - 12155n^9 + 1092n^{11} - 70n^{13} + 4n^{15} + \frac{1}{2}n^{16} \right).
 \end{aligned}$$

# $T_{k,n}(a, d)$ IN TERMS OF GENOCCHI NUMBERS

The Euler polynomial  $E_k(z)$  may be defined by the generating function [2, pp. 48-49]

$$\frac{2e^{xz}}{e^x + 1} = \sum_{k=0}^{\infty} E_k(z) \frac{x^k}{k!}. \quad (7.1)$$

For  $z = 1$ , we have

$$E_k(1) = \frac{2(2^{k+1} - 1)}{k+1} B_{k+1} = -\frac{1}{k+1} G_{k+1}, \quad (7.2)$$

where  $B_{k+1}$  is a Bernoulli number and  $G_{k+1}$  is called a Genocchi number [2, p. 49]. The Genocchi numbers are integers such that  $G_{2m+1} = 0$  for  $m > 0$ ; the first few are  $G_0 = 0$ ,  $G_1 = 1$ ,  $G_2 = -1$ ,  $G_3 = 1$ ,  $G_4 = -3$ . It follows from (7.1) that

$$E_k(z) = \sum_{j=0}^k \binom{k}{j} \frac{G_{k-j+1}}{k-j+1} z^j. \quad (7.3)$$

Comparing (7.1) and (6.2), we see that

$$T_{k,n}(a, d) = \frac{d^k}{2} \left[ (-1)^{n-1} E_k\left(\frac{a}{d} + n\right) + E_k\left(\frac{a}{d}\right) \right]. \quad (7.4)$$

By (7.3) and (7.4), we have the following result. For fixed  $a$  and  $d$ , if we write  $T_{k,n}(a, d)$  as a polynomial in  $(a - d + nd)$ , i.e.,

$$\begin{aligned} T_{k,n}(a, d) &= T_{k,n-1}(a, d) + (a - d + nd)^k \\ &= u_{k,0} + u_{k,1}(a - d + nd) + u_{k,2}(a - d + nd)^2 + \cdots + u_{k,k}(a - d + nd)^k, \end{aligned} \quad (7.5)$$

then we have explicit formulas for the coefficients  $u_{k,j}$  in terms of Genocchi numbers.

**Theorem 7.1:** If  $T_{k,n}(a, d)$  is written as a polynomial in  $(a - d + nd)$  and  $u_{k,j}$  is defined by (7.5) for  $j = 0, 1, \dots, k$ , then

$$\begin{aligned} u_{k,j} &= \frac{(-1)^n d^{k-j}}{2(k-j+1)} \binom{k}{j} G_{k-j+1} \quad (1 \leq j \leq k-1), \\ u_{k,0} &= \frac{(-1)^n d^k}{2(k+1)} G_{k+1} + \frac{d^k}{2} E_k\left(\frac{a}{d}\right), \quad u_{k,k} = \frac{(-1)^{n-1}}{2}. \end{aligned}$$

When  $a = d = 1$ , we have

$$T_{k,n} = T_{k,n}(1, 1) = \frac{(-1)^{n-1}}{2} n^k + \frac{(-1)^n}{2} \sum_{j=0}^{k-1} \binom{k}{j} \frac{G_{k-j+1}}{k-j+1} n^j - \frac{G_{k+1}}{2(k+1)}. \quad (7.6)$$

When  $n$  is even, (7.6) follows from (6.1) and the formulas in Section 6 [1, p. 27].

For example,  $T_{3,n} = 1^3 - 2^3 + \cdots + (-1)^{n-1} n^3$

$$= \frac{(-1)^{n-1}}{2} n^3 + \frac{3(-1)^n}{4} G_2 n^2 + \frac{(-1)^n}{2} G_3 n + \frac{[(-1)^n - 1]}{8} G_4 = \frac{(-1)^{n-1}}{8} [4n^3 + 6n^2 - 1 + (-1)^n].$$

An application of Theorem 6.3 that is analogous to (4.5) is the following. If  $n$  is odd and  $a = d = 1$ , by Theorem 7.1 we have  $u_{k,0} = -G_{k+1}/(k+1)$ . Thus, by Theorems 7.1 and 6.3 we have, for  $m = 1, 2, \dots, 5$ ,

$$8G_{6k+m+1} = -6 \sum_{j=0}^{k-1} \binom{6k+m+1}{6j+m+1} G_{6j+m+1} - 2(6k+m+1)w_m,$$

which is equivalent to a formula of Ramanujan [7, p. 12].

### 8. FINDING $T_{k,n}(a, d)$ FROM $T_{k-1,n}(a, d)$

We proceed as we did for  $S_{k,n}(a, d)$ . By using induction on (6.3), we can prove that  $T_{k,n}(a, d)$  is a polynomial in  $n$  of degree  $k$ , and the constant term is 0 if  $n$  is even. That also follows from the results of Section 7. Thus, for fixed  $a$  and  $d$ , we can write

$$T_{k,n}(a, d) = \begin{cases} t_{k,1}n + t_{k,2}n^2 + \dots + t_{k,k}n^k & (n \text{ even}), \\ h_{k,0} + h_{k,1}n + \dots + h_{k,k}n^k & (n \text{ odd}). \end{cases} \quad (8.1)$$

Using the generating function (6.2), we prove the next theorem just as we proved Theorem 5.1.

**Theorem 8.1:** For fixed  $a$  and  $d$ , let  $t_{k,j}$  and  $h_{k,j}$  be defined by (8.1) for  $j = 0, \dots, k$ . Then for  $k \geq 1$  we have

$$\begin{aligned} t_{k,j} &= \frac{kd}{j} t_{k-1,j-1} \quad (j = 2, \dots, k); & h_{k,j} &= \frac{kd}{j} h_{k-1,j-1} \quad (j = 2, \dots, k); \\ t_{k,1} &= -\frac{kd^k}{2} E_{k-1}\left(\frac{a}{d}\right) = \frac{1}{2} [a^k - (a+d)^k] - (2t_{k,2} + 2^2 t_{k,3} + \dots + 2^{k-1} t_{k,k}); \\ h_{k,0} &= a^k - h_{k,1} - \dots - h_{k,k}; \\ h_{k,1} &= -\frac{kd^k}{2} E_{k-1}\left(\frac{a}{d}\right) + kd h_{k-1,0} = t_{k,1} + kd h_{k-1,0}. \end{aligned}$$

Thus, if we know  $T_{k-1,n}(a, d)$ , we can use Theorem 8.1 to find  $T_{k,n}(a, d)$ . For example,

$$T_{0,n}(a, d) = \begin{cases} 0 & (n \text{ even}), \\ 1 & (n \text{ odd}); \end{cases} \quad T_{1,n}(a, d) = \begin{cases} -(d/2)n & (n \text{ even}), \\ (a-d/2) + (d/2)n & (n \text{ odd}). \end{cases}$$

Then, for  $n$  even, we have  $T_{2,n}(a, d) = t_{2,1}n + t_{2,2}n^2$ , with

$$t_{2,2} = dt_{1,1} = -d^2/2; \quad t_{2,1} = \frac{1}{2} [a^2 - (a+d)^2] + d^2 = -ad + d^2/2.$$

Thus,

$$T_{2,n}(a, d) = \left(\frac{1}{2}d^2 - ad\right)n - \frac{1}{2}d^2n^2 \quad (n \text{ even}).$$

For  $n$  odd,  $T_{2,n}(a, d) = h_{2,0} + h_{2,1}n + h_{2,2}n^2$ , with

$$h_{2,2} = dh_{1,1} = d^2/2; \quad h_{2,1} = t_{2,1} + 2dh_{1,0} = ad - d^2/2; \quad h_{2,0} = a^2 - h_{2,1} - h_{2,2} = a^2 - ad.$$

Thus,

$$T_{2,n}(a, d) = (a^2 - ad) + \left(ad - \frac{1}{2}d^2\right)n + \frac{1}{2}d^2n^2 \quad (n \text{ odd}).$$

Equivalently, by Theorem 8.1, we can integrate to find  $S_{k,n}(a, d)$ :

$$S_{k,n}(a, d) = kd \int S_{k-1,n}(a, d) dn - \frac{kd^k}{2} E_{k-1}\left(\frac{a}{d}\right)n + h_k(n),$$

where  $E_{k-1}\left(\frac{a}{d}\right)$  can be found by means of Theorem 8.1, and

$$h_k(n) = \begin{cases} 0 & (n \text{ even}), \\ h_{k,0} = a^k - h_{k,1} - h_{k,2} - \cdots - h_{k,k} & (n \text{ odd}). \end{cases}$$

## 9. FINAL COMMENTS

In summary, we have used generating functions to prove and generalize some of the basic formulas for sums of powers of integers. In particular, we have used the generating function technique to find: recurrence relations for  $S_{k,n}(a, d)$  and  $T_{k,n}(a, d)$ ; explicit formulas (involving Bernoulli numbers) for  $S_{k,n}(a, d)$  and  $T_{k,n}(a, d)$  if they are written as polynomials in  $n$ ; methods for finding  $S_{k,n}(a, d)$  and  $T_{k,n}(a, d)$  from  $S_{k-1,n}(a, d)$  and  $T_{k-1,n}(a, d)$ . Some of the results are old (and scattered in the literature), and most of the proofs are straightforward. However, the writer believes that many of the generalizations are new, and he believes that Theorems 3.1 and 6.1 give us new recurrence formulas that are of interest.

## ACKNOWLEDGMENT

I thank the referee for several thoughtful and constructive suggestions.

## REFERENCES

1. P. Bachmann. *Niedere Zahlentheorie II*. New York: Chelsea, 1968.
2. L. Comtet. *Advanced Combinatorics*. Dordrecht: Reidel, 1974.
3. G. F. C. de Bruyn & J. M. de Villiers. "Formulas for  $1^p + 2^p + 3^p + \cdots + n^p$ ." *The Fibonacci Quarterly* **32.3** (1994):271-76.
4. F. T. Howard. "Applications of a Recurrence for the Bernoulli Numbers." *Journal of Number Theory* **52** (1995):157-72.
5. D. Kalman. "Sums of Powers by Matrix Methods." *The Fibonacci Quarterly* **28.1** (1990): 60-71.
6. R. A. Kahn. "A Simple Derivation of a Formula for  $\sum_{k=1}^n k^r$ ." *The Fibonacci Quarterly* **19.2** (1981):177-80.
7. S. Ramanujan. "Some Properties of Bernoulli's Numbers." *Journal of the Indian Mathematical Society* **3** (1911):219-34.
8. J. Riordan. *Combinatorial Identities*. New York: Wiley, 1968.
9. B. Turner. "Sums of Powers of Integers via the Binomial Theorem." *Math. Magazine* **53** (1980):92-96.
10. J. Wiener. "A Calculus Exercise for the Sums of Integer Powers." *Math. Magazine* **65** (1992):249-51.

AMS Classification Numbers: 05A15, 11B37, 11B68



# A FIBONACCI MODEL OF INFECTIOUS DISEASE

**F. Dubeau**

Département de mathématiques et d'informatique, Faculté des Sciences,  
Université de Sherbrooke, 2500 Boul. Université, Sherbrooke (Québec), Canada, J1K 2R1

**A. G. Shannon**

School of Mathematical Sciences, University of Technology, Sydney, 2007, Australia

(Submitted September 1994)

## 1. INTRODUCTION

The Fibonacci rabbit population model is often regarded as one of the first studies of population growth using mathematics. Later, an analytic model of population dynamics was introduced by Volterra (Deakin & McElwain [2]). Systematic epidemic modeling in age-structured populations was first carried out in this century by Hoppensteadt [6].

Dubeau [3], in revisiting the Fibonacci rabbit growth model, has developed an approach that can be applied to population dynamics and epidemiology where censoring occurs either by inability to procreate or by death. It is the purpose of this note to apply Dubeau's method to Fibonacci's model of infectious diseases which was developed by Makhmudov [9] and to combine it with the approach of Shannon et al. [12] who attempted to refine the work of Makhmudov.

## 2. THE MODEL

Following Makhmudov [9], three epidemiological stages in the process of spreading infectious diseases are postulated:

- (i) an initial (incubation) stage of  $r$  periods (periods  $0, 1, 2, \dots, r-1$ ) during which those who are ill with the disease do not affect others,
- (ii) a mature (infectious) stage of  $t$  periods (periods  $r, r+1, \dots, r+t-1$ ) when each person infects  $s$  healthy people, and
- (iii) a removal stage of  $m$  periods (periods  $r+t, \dots, r+t+m-1$ ) when those who have been infected are no longer infectious.

An example might be the common cold which, on average, takes about two days to develop ( $r=2$ ), a person is then infectious for about three days ( $t=3$ ), and the symptoms persist for about seven days ( $r+t+m=7$ , hence  $m=2$ ). In general,  $s$  is variable, but we shall treat it as a constant in the absence of other information. For background material on the structure of general epidemic models, the reader is referred to Billiard & Zhen Zhao [1].

In terms of a modification to Fibonacci's rabbit problem, these correspond in turn to

- (i) the infancy stage,
- (ii) the reproductive stage, and
- (iii) the post reproductive stage,

respectively, and instead of infectives we have male-female pairs of rabbits. For the original Fibonacci model, we take  $r=2$ ,  $s=1$ , and  $t=m=+\infty$ .

## 2.1 A Direct Approach

Following Dubeau [3], let

$u_n$  be the total number of disease carriers at the  $n^{\text{th}}$  period, and

$v_n^i$  be the number of  $i$ -period old disease carriers at the  $n^{\text{th}}$  period.

More precisely,  $v_n^i$  represents the disease carriers in the

- (i) initial stage for  $i = 0, \dots, r-1$ ,
- (ii) mature stage for  $i = r, \dots, r+t-1$ ,
- (iii) removal reproductive stage for  $i = r+t, \dots, r+t+m-1$ ,

and for  $i = r+t+m, \dots$ ,  $v_n^i$  represents the disease carriers who have been infected in the past but have already recovered.

It will be convenient to define  $u_n$  and  $v_n^i$  for all  $n \in Z = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$  and  $i \in N = \{0, 1, 2, 3, \dots\}$ . We consider the following initial conditions on  $v_n^i$ :

$$v_n^i = \begin{cases} 0 & \text{for } \begin{cases} n < 0 \text{ and } i = 0, 1, 2, \dots, \\ n = 0 \text{ and } i = 1, 2, 3, \dots, \end{cases} \\ 1 \text{ (or } v_0^0) & \text{for } n = 0 \text{ and } i = 0. \end{cases}$$

As a consequence, for any  $n \in Z$ ,

$$v_n^i = v_{n-1}^{i-1} \quad \text{for } i > 0,$$

and

$$v_n^0 = \begin{cases} 1 & \text{for } n = 0, \\ s\{v_n^r + \dots + v_n^{r+t-1}\} & \text{for } n \neq 0. \end{cases}$$

We obtain

$$v_n^0 = v_{n-1}^0 + s\{v_{n-r}^0 - v_{n-r-t}^0\} \quad (1)$$

for  $n > 1$ . From the definition we have, for any  $n \in Z$ ,

$$u_n = \sum_{i=0}^{r+t+m-1} v_n^i.$$

It follows that

$$u_n = \begin{cases} 0 & \text{for } n < 0, \\ u_0 + s \sum_{k=r}^{r+t-1} u_{n-k} & \text{for } n = 0, \dots, r+t+m-1, \\ s \sum_{k=r}^{r+t-1} u_{n-k} & \text{for } n \geq r+t+m, \end{cases} \quad (2)$$

or

$$u_n = u_{n-1} - \delta_{n, r+t+m} u_0 + s\{u_{n-r} - u_{n-r-t}\} \quad (3)$$

for  $n \geq 1$ , where  $\delta_{i,j} = 0$  if  $i \neq j$ , or 1 if  $i = j$ .



**Example 1:** Table 1 contains values of  $v_n^j$  and  $u_n$  for  $r = 2, t = 3, m = 2$ , and  $s = 1$ .

**TABLE 1.**  $r = 2, t = 3, m = 2$ , and  $s = 1$

$n \backslash i$	$u_n$							$u_n$
	0	1	2	3	4	5	6	
0	1	0	0	0	0	0	0	1
1	0	1	0	0	0	0	0	1
2	1	0	1	0	0	0	0	2
3	1	1	0	1	0	0	0	3
4	2	1	1	0	1	0	0	5
5	2	2	1	1	0	1	0	7
6	4	2	2	1	1	0	1	11
7	5	4	2	2	1	1	0	15
8	8	5	4	2	2	1	1	23
9	11	8	5	4	2	2	1	33
10	17	11	8	5	4	2	2	49
11	24	17	11	8	5	4	2	71
12	36	24	17	11	8	5	4	105
13	52	36	24	17	11	8	5	153
14	77	52	36	24	17	11	8	225
15	112	77	52	36	24	17	11	329
16	165	112	77	52	36	24	17	483
17	241	165	112	77	52	36	24	707
18	354	241	165	112	77	52	36	1037
19	518	354	241	165	112	77	52	1519
20	760	518	354	241	165	112	77	2227

**Remark—The Effect of  $m$ :** Let  $\{u_n\}_{n=0}^{+\infty}$  and  $\{\tilde{u}_n\}_{n=0}^{+\infty}$  be the sequences generated with  $m$  and  $m + 1$  for the same values of  $r, t$ , and  $s$ . From (3) we have, for  $n \geq 1$ ,

$$u_n = u_{n-1} - \delta_{n,r+t+m}u_0 + s\{u_{n-r} - u_{n-r-t}\}$$

and

$$\tilde{u}_n = \tilde{u}_{n-1} - \delta_{n,r+t+m+1}u_0 + s\{\tilde{u}_{n-r} - \tilde{u}_{n-r-t}\}.$$

Let  $\Delta_n u = u_n - \tilde{u}_n$ , then from (3)

$$\Delta_n u = \Delta_{n-1} u + (\delta_{n,r+t+m} - \delta_{n,r+t+m+1}) u_0 + s\{\Delta_{n-r} u - \Delta_{n-r-t} u\}.$$

It follows from (1) that  $\Delta_{r+t+m+n} u = v_n^0$  for  $n \geq 0$ .

## 2.2 A Generating Function Approach

Following Weland [13], Hoggatt [4], Hoggatt & Lind [5], and Parberry [11], we can use the generating function method to obtain the recurrence relation (1), (2), or (3).

Let us define the generating function for the sequence  $\{u_n\}_{n=0}^{+\infty}$ :

$$U(x) = \sum_{n=0}^{+\infty} u_n x^n.$$

The function  $U(x)$  can be expressed in terms of (i) the generating function of the infectious process (a polynomial)

$$B(x) = \sum_{n=0}^{+\infty} b_n x^n \quad (b_0 = 0),$$

where  $b_n$  indicates the number of infected healthy people by an  $n$ -period old disease carrier, and (ii) the "total recovering" polynomial  $D(x) = x^{r+t+m}$ .

Let

$$V(x) = \sum_{n=0}^{+\infty} v_n^0 x^n$$

be the generating function associated to the sequence  $\{v_n^0\}_{n=0}^{+\infty}$ , where

$$\begin{aligned} v_0^0 &= 1, \\ v_1^0 &= b_0 v_1^0 + b_1 v_0^0, \\ v_2^0 &= b_0 v_2^0 + b_1 v_1^0 + b_2 v_0^0 \\ &\text{etc.,} \end{aligned}$$

and, in general,

$$v_n^0 = \sum_{j=0}^n b_j v_{n-j}^0$$

for  $n \geq 1$ . It follows that

$$V(x) = \frac{1}{1 - B(x)}.$$

Let  $u_n^*$  be the number of disease carriers at the  $n^{\text{th}}$  period, assuming no recovery, and

$$U^*(x) = \sum_{n=0}^{+\infty} u_n^* x^n.$$

Then

$$u_n^* = \sum_{j=0}^n v_j^0$$

and we obtain

$$U^*(x) = \frac{1}{(1-x)}, V(x) = \frac{1}{(1-x)(1-B(x))}.$$

If we now allow for recoveries, since each disease carrier recovers  $r+t+m$  periods after its infection, the number  $h_n$  of recovering people at the  $n^{\text{th}}$  period is given by  $h_n = v_{n-(r+t+m)}^0$ . Therefore,

$$H(x) = \sum_{n=0}^{+\infty} h_n x^n = D(x)V(x) = \frac{D(x)}{1-B(x)}.$$

Let  $r_n$  be the total number of people who recovered up to the  $n^{\text{th}}$  period, then

$$r_n = \sum_{j=0}^n h_j$$

and

$$R(x) = \sum_{n=0}^{+\infty} r_n x^n = \frac{1}{1-x} H(x) = \frac{D(x)}{(1-x)(1-B(x))}.$$

Now,  $u_n = u_n^* - r_n$  ( $n \geq 0$ ), so that

$$U(x) = U^*(x) - R(x) = \frac{1-D(x)}{(1-x)(1-B(x))}.$$

From the model, we have

$$B(x) = s \sum_{n=r}^{r+t-1} x^n, \quad D(x) = x^{r+t+m},$$

and

$$U(x) = \frac{1-x^{r+t+m}}{1-x-sx^r+sx^{r+t}}.$$

It follows that  $u_0 = 1$  and, for  $n \geq 1$ ,  $u_n = u_{n-1} - \delta_{n,r+t+m} u_0 + s\{u_{n-r} - u_{n-(r+t)}\}$ . Moreover, since

$$V(x) = \frac{1}{1-s \sum_{n=r}^{r+t-1} x^n},$$

it follows that  $v_0^0 = 1$ , and  $v_n^0 = s\{v_{n-r}^0 + \dots + v_{n-(r+t-1)}^0\}$  for  $n \geq 1$ .

### 2.3 A Matrix Approach

Following Klarner [8], let us consider the sequence of  $(r+t+m)$ -vectors  $\{v_n\}_{n=0}^{+\infty}$ :

$$v_n = [v_n^0, v_n^1, \dots, v_n^{r+t+m-1}] \quad (n = 0, 1, 2, \dots).$$

They are related by the equation

$$v_{n+1} = v_n F = \dots = v_0 F^{n+1}, \quad (4)$$

where  $v_0 = [1, 0, \dots, 0]$  and  $F = (f_{ij})$  is a square matrix of order  $r+t+m$  with entries  $f_{ij}$  ( $i = 0, \dots, r+t+m-1$ ;  $j = 0, \dots, r+t+m-1$ ) such that

$$v_{n+1}^j = \sum_{i=0}^{r+t+m-1} v_n^i f_{ij}.$$

For our problem,

$$f_{i0} = \begin{cases} s & \text{for } i = r, \dots, r+r-1, \\ 0 & \text{elsewhere,} \end{cases}$$

and for  $j = 1, \dots, r+t+m-1$ ,

$$f_{ij} = \begin{cases} 1 & \text{if } i = j-1, \\ 0 & \text{elsewhere.} \end{cases}$$

The characteristic polynomial of  $F$  is  $\det(xI - F) = x^{r+t+m} - s(x^{t+m} + \dots + x^{1+m}) = c_F(x)$ . From the Cayley-Hamilton theorem, the matrix  $F$  satisfies its characteristic equation, and we have  $c_F(F) = 0$ . Hence,  $F^n c_F(F) = 0$  for any  $n \geq 0$ . It follows that  $F^n - s(F^{n-r} + \dots + F^{n-(r+t-1)}) = 0$  for  $n \geq r+t+m$ . Finally, from (4), we have

$$v_n - s(v_{n-r} + \dots + v_{n-(r+t-1)}) = 0$$

and, since  $u_n = v_n 1$ , where  $1 = [1, \dots, 1]^T$ ,

$$u_n - s(u_{n-r} + \dots + u_{n-(r+t-1)}) = 0$$

for  $n \geq r+t+m$ .

### 3. A RELATED ARRAY

Let  $w_n^i(k)$  be the number of  $i$ -period old disease carriers of the  $k^{\text{th}}$  generation at the  $n^{\text{th}}$  period, and  $w_n(k)$  be the number of disease carriers of the  $k^{\text{th}}$  generation at the  $n^{\text{th}}$  period. We have

$$w_n(k) = \sum_{i=0}^{r+t+m-1} w_n^i(k)$$

and, for  $i \geq r+t+m$ ,  $w_n^i(k)$  indicates the number of people of the  $k^{\text{th}}$  generation at the  $n^{\text{th}}$  period infected  $i$  periods ago and who have already recovered.

We also have

$$\begin{aligned} w_n^i(k) &= 0 & \text{for } n < 0 \text{ or } i < 0, \\ w_n^i(k) &= \delta_{ni} & \text{for } n \geq 0 \text{ and } i \geq 0, \end{aligned}$$

and, for  $k \geq 1, n \geq 0$ , and  $i \geq 0$ ,

$$w_n^i(k) = \begin{cases} s\{w_n^r(k-1) + \dots + w_n^{r+t-1}(k-1)\} & \text{for } i = 0, \\ w_{n-1}^{i-1}(k) & \text{for } i \geq 1. \end{cases}$$

We can deduce that  $w_n^0(k) \neq 0$  for  $kr \leq n \leq k(r+t-1)$ ,  $k = 0, 1, 2, \dots$ . It follows that  $w_n(k) \neq 0$  only for  $k \geq 0$  and  $n \geq 0$  such that  $kr = n_L(k) \leq n \leq n_U(k) = (r+t+m-1) + k(r+t-1)$ . Then, for a given  $n$ , let

$$k_L(n) = \min \left\{ k \in N \mid k \geq 0 \text{ and } k \geq \frac{n - (r + t + m - 1)}{r + t - 1} \right\},$$

$$k_U(n) = \max \left\{ k \in N \mid k \leq \frac{n}{r} \right\};$$

hence,  $w_n(k) = 0$  for  $k < k_L(n)$  and  $k > k_U(n)$ . To relate the  $w_n(k)$  and  $w_n^i(k)$  to the  $u_n$  and  $v_n^i$ , we have

$$u_n = \sum_{k=0}^{+\infty} w_n(k) = \sum_{k=k_L(n)}^{k_U(n)} w_n(k),$$

$$v_n^i = \sum_{k=0}^{+\infty} w_n^i(k) = \sum_{k=0}^{k_U(n)} w_n^i(k).$$

Also, for  $k \geq 1$ ,

$$w_n(k) = \sum_{i=0}^{r+t+m-1} w_n^i(k) = \sum_{i=0}^{r+t+m-1} w_{n-i}^0(k)$$

$$= \sum_{i=0}^{r+t+m-1} s \sum_{\ell=r}^{r+t-1} w_{n-i}^\ell(k-1) = s \sum_{\ell=r}^{r+t-1} \sum_{i=0}^{r+t+m-1} w_{n-i}^\ell(k-1)$$

$$= s \sum_{\ell=r}^{r+t-1} \sum_{i=0}^{r+t+m-1} w_{n-\ell}^i(k-1) = s \sum_{\ell=r}^{r+t-1} w_{n-\ell}(k-1).$$

As a consequence, using the generating function, we have

$$G_k(x) = \sum_{n=0}^{+\infty} w_n(k) x^n = s \sum_{n=0}^{+\infty} \left( \sum_{\ell=r}^{r+t-1} w_{n-\ell}(k-1) \right) x^n$$

$$= s \sum_{n=0}^{+\infty} \left( \sum_{\ell=n-(r+t-1)}^{n-r} w_\ell(k-1) \right) x^n = s(x^r + \dots + x^{r+t-1}) \sum_{n=0}^{+\infty} w_n(k-1) x^n$$

$$= s(x^r + \dots + x^{r+t-1}) G_{k-1}(x).$$

Also,

$$G_0(x) = \sum_{n=0}^{+\infty} w_n(0) x^n = 1 + x + \dots + x^{r+t+m-1},$$

thus

$$G_k(x) = s^k \left[ x^r (1 + x + \dots + x^{t-1}) \right]^k G_0(x)$$

and

$$G_k(1) = (st)^k (r + t + m) = \sum_{n=n_L(k)}^{u_U(k)} w_n(k).$$

**Example 2:** Table 2 illustrates the values of  $w_n^i(k)$  and  $w_n(k)$  for  $r = 2$ ,  $t = 3$ ,  $m = 2$ , and  $s = 1$ .

**TABLE 2.**  $r = 2, t = 3, m = 2$ , and  $s = 1, n_L(k) = 2k, n_U(k) = 4k + 6$ ,  
 $k_L(n) = \min\left\{k \in N \mid k \geq 0 \text{ and } k \geq \frac{n-6}{4}\right\}$ ,  $k_U(n) = \max\left\{k \in N \mid k \leq \frac{n}{2}\right\}$

		$w_n^i(k)$							$w_n(k)$
		$i$							
$n$	$k_L(n) \leq k \leq k_U(n)$	0	1	2	3	4	5	6	
0	$k_L(0) = 0 = k_U(0)$	1	0	0	0	0	0	0	1
1	$k_L(1) = 0 = k_U(1)$	0	1	0	0	0	0	0	1
2	$k_L(2) = 0$	0	0	1	0	0	0	0	1
	$1 = k_U(2)$	1	0	0	0	0	0	0	1
3	$k_L(3) = 0$	0	0	0	1	0	0	0	1
	$1 = k_U(3)$	1	1	0	0	0	0	0	2
4	$k_L(4) = 0$	0	0	0	0	1	0	0	1
	1	1	1	1	0	0	0	0	3
	$2 = k_U(4)$	1	0	0	0	0	0	0	1
5	$k_L(5) = 0$	0	0	0	0	0	1	0	1
	1	0	1	1	1	0	0	0	3
	$2 = k_U(5)$	2	1	0	0	0	0	0	3
6	$k_L(6) = 0$	0	0	0	0	0	0	1	1
	1	0	0	1	1	1	0	0	3
	2	3	2	1	0	0	0	0	6
	$3 = k_U(6)$	1	0	0	0	0	0	0	1
7	$k_L(7) = 1$	0	0	0	1	1	1	0	3
	2	2	3	2	1	0	0	0	8
	$3 = k_U(7)$	3	1	0	0	0	0	0	4
8	$k_L(8) = 1$	0	0	0	0	1	1	1	3
	2	1	2	3	2	1	0	0	9
	3	6	3	1	0	0	0	0	10
	$4 = k_U(8)$	1	0	0	0	0	0	0	1
9	$k_L(9) = 1$	0	0	0	0	0	1	1	2
	2	0	1	2	3	2	1	0	9
	3	7	6	3	1	0	0	0	17
	$4 = k_U(9)$	4	1	0	0	0	0	0	5

#### 4. LIMIT OF RATIOS $u_{n+1}/u_n$

We consider the linear difference equation (2) of order  $r+t-1$ :

$$u_n = s \sum_{k=r}^{r+t-1} u_{n-k} \quad (n \geq r+t+m).$$

The sequence  $\{u_n\}_{n=r+t+m}^{+\infty}$  is completely defined if we assume that the values  $u_{m+1}, u_{m+2}, \dots, u_{r+t+m-1}$  are known.

For our model (2) or (3), we observe that the finite sequence  $\{u_n\}_{n=0}^{r+t+m-1}$  is a sequence of non-decreasing integers with  $u_0 = 1$  (or any initial value  $u_0 > 0$ ).

We consider two cases for the analysis of the ratios  $u_{n+1}/u_n$ : the case  $t = 1$  and the case  $t > 1$ .

#### 4.1 The Case $t = 1$

We have  $u_n = su_{n-r}$  ( $n \geq r + m + 1$ ). It follows that

$$\frac{u_{n+r+1}}{u_{n+r}} = \frac{u_{n+1}}{u_n} \quad (n \geq m + 1)$$

and the sequence of ratios  $u_{n+1}/u_n$  is a sequence of length  $r$  repeated infinitely many times. It is completely characterized by the finite sequence

$$\frac{u_{n+1}}{u_n} \quad \text{for } n = m + 1, \dots, m + r.$$

Using (2), for the initial value  $u_0 = 1$ , we have

$$u_n = \sum_{i=0}^k s^i \quad \text{for } \begin{cases} n \leq r + m, \text{ and} \\ kr \leq n < (k + 1)r \end{cases}$$

and

$$u_n = \sum_{i=0}^{\lfloor \frac{n}{r} \rfloor} s^i \quad \text{for } n = 0, \dots, r + m.$$

Let

$$\rho_U = \left\lfloor \frac{r + m}{r} \right\rfloor \quad \text{and} \quad \rho_L = \left\lfloor \frac{1 + m}{r} \right\rfloor,$$

then  $\rho_U = \rho_L$  or  $\rho_L + 1$ . Hence, the sequence  $\left\{ \frac{u_{n+1}}{u_n} \right\}_{n=m+1}^{m+r}$  is such that

$$\frac{u_{n+1}}{u_n} = \begin{cases} 1 & r - 2 \text{ times,} \\ s^{\rho_L} \sum_{i=0}^{\rho_L} s^i / \sum_{i=0}^{\rho_U} s^i & 1 \text{ time,} \\ \sum_{i=0}^{\rho_U} s^i / \sum_{i=0}^{\rho_L} s^i & 1 \text{ time.} \end{cases} \quad (6)$$

It can be shown that the set

$$\left\{ \frac{u_{n+1}}{u_n} \mid n = m + 1, \dots, m + r \right\}$$

converges to the set  $\{1, s\}$  when  $m$  goes to  $+\infty$ .

**Example 3:** Table 3 contains the values of (6) for  $r = 4$ ,  $t = 1$ , and  $s = 2$ .

TABLE 3.  $r = 4$ ,  $t = 1$ , and  $s = 2$ 

$\frac{u_{m+i+1}}{u_{m+i}}$	$m$								
$i$	1	2	3	4	5	6	7	8	9
1	1	3	1	1	1	7/3	1	1	1
2	3	1	1	1	7/3	1	1	1	15/7
3	1	1	1	7/3	1	1	1	15/7	1
4	2/3	2/3	2	6/7	6/7	6/7	2	14/15	14/15

#### 4.2 The Case $t > 1$

Let  $K = r + t - 1$ . The linear difference equation (5) is equivalent to the following linear difference equation of order  $K$ ,

$$u_{n+K} = s \sum_{k=0}^{t-1} u_{n+k} \quad (n \geq 0)$$

if the sequence  $\{u_n\}_{n=0}^{K-1}$  for (7) corresponds to the sequence  $\{u_n\}_{n=m+1}^{m+K}$  for (5). Hence, the limit of  $u_{n+1}/u_n$  is the same for both equations.

Let us recall some definitions and results about linear difference equations of the form

$$u_{n+K} - b_1 u_{n+K-1} - \cdots - b_{K-1} u_{n+1} - b_K u_n = 0 \quad (n \geq 0). \quad (8)$$

##### Definitions:

- (a) The polynomial  $\varphi(\lambda) = \lambda^K - b_1 \lambda^{K-1} - \cdots - b_K$  is called the characteristic polynomial for (8).
- (b) The equation  $\varphi(\lambda) = 0$  is the characteristic equation for (8).
- (c) The solutions  $\lambda_1, \dots, \lambda_\ell$  of the characteristic equation are the characteristic roots.

The first result is a standard result about the general solution of (8).

**Theorem 1:** Suppose (8) has characteristic roots  $\lambda_1, \dots, \lambda_k$  with multiplicities  $j_1, \dots, j_k$ , respectively. Then (8) has  $n$  independent solutions  $n^j \lambda_\ell^n$ ,  $j = 0, \dots, j_\ell - 1$ ;  $\ell = 1, \dots, k$ . Moreover, any solution of (8) is of the form

$$u_n = \sum_{\ell=1}^k \sum_{j=0}^{j_\ell-1} \beta_{\ell,j} n^j \lambda_\ell^n \quad (n \geq 0),$$

where the  $\beta_{\ell,j}$  are obtained from the values of  $u_n$  for  $n = 0, \dots, K-1$ .

**Proof:** See, for example, Kelley & Peterson [7].  $\square$

The next two results depend on the form of (8).



**Theorem 2:** Assume the  $b_i$  are nonnegative in (8).

- (a) If at least one  $b_i$  is strictly positive, then (8) has a unique simple characteristic root  $\sigma > 0$  and all other characteristic roots of (8) have moduli not greater than  $\sigma$ .
- (b) If the indices of the  $b_i$  that are strictly positive have the common greatest divisor 1, then (8) has a unique simple characteristic root  $\sigma > 0$ , and the moduli of all other characteristic roots of (8) is strictly less than  $\sigma$ .

**Proof:** See Ostrowski [10, pp. 91-92].  $\square$

**Theorem 3:** If in (8) the  $b_i$  are nonnegative and  $\{u_n\}_{n=0}^{+\infty}$  is a sequence satisfying (8) such that  $u_0, u_1, \dots, u_{K-1}$  are strictly positive, then we have  $u_n \geq \alpha \sigma^n$  ( $n \geq 0$ ), where  $\alpha > 0$  is given by

$$\alpha = \min \left\{ \frac{u_n}{\sigma^n} \mid n = 0, \dots, K-1 \right\}.$$

**Proof:** See Ostrowski [10, p. 93].  $\square$

Since

$$b_i = \begin{cases} 0 & \text{for } i = 1, \dots, r-1, \\ s & \text{for } i = r, \dots, r+t-1, \end{cases}$$

and the common greatest divisor of  $r, \dots, r+t-1$  is 1 for  $t > 1$ , it follows from Theorem 2(b) that (7) as a unique simple characteristic root  $\sigma > 0$  and the moduli of all other characteristic roots are less than  $\sigma$ .

Let  $\lambda_1, \dots, \lambda_k$  and  $\sigma$  be the characteristic roots of (7), then, from Theorem 1,

$$u_n = \beta \sigma^n + \sum_{\ell=1}^k \sum_{j=0}^{j_\ell-1} \beta_{\ell,j} n^j \lambda_\ell^n.$$

Moreover, since  $u_0 \geq 1$  and  $\{u_n\}_{n=0}^{K-1}$  is a nondecreasing sequence, we obtain, from Theorem 3,  $u_n \geq \alpha \sigma^n$  for

$$\alpha = \min \left\{ \frac{u_n}{\sigma^n} \mid n = 0, \dots, K-1 \right\}.$$

It follows that

$$\alpha \leq \frac{u_n}{\sigma^n} = \beta + \sum_{\ell=1}^k \sum_{j=0}^{j_\ell-1} \beta_{\ell,j} n^j \left( \frac{\lambda_\ell}{\sigma} \right)^n,$$

and taking the limit on both sides we have  $\lim_{n \rightarrow +\infty} u_n / \sigma^n = \beta \geq \alpha > 0$  as a consequence of the following lemma.

**Lemma:** If  $|\rho| < 1$ , then  $\lim_{n \rightarrow +\infty} n^\alpha \rho^n = 0$  for any  $\alpha = 0, 1, 2, \dots$ .  $\square$

Finally,

$$\frac{u_{n+1}}{u_n} = \sigma \frac{u_{n+1} / \sigma^{n+1}}{u_n / \sigma^n}$$

and we obtain  $\lim_{n \rightarrow +\infty} u_{n+1}/u_n = \sigma$ , where  $\sigma$  is the unique positive root of

$$\varphi(x) = x^{r+t-1} - s \sum_{i=0}^{t-1} x^i \quad (t > 1).$$

## 5. A MORE REALISTIC MODEL

In any real population, the epidemiological status of members is as follows: (i) susceptibles, (ii) infected, and (iii) resistants. Thus, there is not an unlimited supply of susceptibles.

Let

$N$  be the total population,

$S_n$  be the number of susceptibles at the  $n^{\text{th}}$  period,

$U_n$  be the number of infected and carriers at the  $n^{\text{th}}$  period, and

$R_n$  be the number of resistants at the  $n^{\text{th}}$  period.

Then  $N = S_n + U_n + R_n$ , and the initial conditions are  $S_0 = N - 1$ ,  $U_0 = 1$ , and  $R_0 = 0$ . Using the notation of Section 2, we have

$$U_n = \sum_{i=0}^{r+t+m-1} v_n^i$$

$$R_n = \sum_{i=r+t+m}^{+\infty} v_n^i = \sum_{i=r+t+m}^{+\infty} v_{n-i}^0 = \begin{cases} 0 & \text{if } n < r+t+m, \\ \sum_{i=r+t+m}^n v_{n-i}^0 & \text{if } n \geq r+t+m, \end{cases}$$

and

$$S_n = N - U_n - R_n.$$

However, the number of susceptibles is limited, so

$$v_n^0 = \min \left\{ S_{n-1}, s \sum_{i=r}^{r+t-1} v_n^i \right\}$$

and

$$S_n = S_{n-1} - v_n^0,$$

$$U_n = U_{n-1} + v_n^0 - v_n^{r+t+m},$$

$$R_n = R_{n-1} + v_n^{r+t+m}.$$

For  $R_n$  we have

$$\begin{aligned} R_n &= R_{n-(r+t+m)} + \sum_{i=0}^{r+t+m-1} v_{n-i}^{r+t+m} \\ &= R_{n-(r+t+m)} + \sum_{i=0}^{r+t+m-1} v_{n-(r+t+m)}^i \\ &= R_{n-(r+t+m)} + U_{n-(r+t+m)} = N - S_{n-(r+t+m)}. \end{aligned}$$

It follows that

$$S_n - S_{n-(r+t+m)} + U_n = 0$$

or

$$U_n = S_{n-(r+t+m)} - S_n$$

and, if  $S_n = 0$ , then  $U_n = S_{n-(r+t+m)}$ .

**Example 4:** Table 4 illustrates this model for  $r = 2, t = 3, m = 2, s = 1$ , and  $N = 200$ .

**TABLE 4.  $r = 2, t = 3, m = 2, s = 1$ , and  $N = 200$**

$n \backslash i$	$v_n^i$							$U_n$	$R_n$	$S_n$
	0	1	2	3	4	5	6			
0	1	0	0	0	0	0	0	1	0	199
1	0	1	0	0	0	0	0	1	0	199
2	1	0	1	0	0	0	0	2	0	198
3	1	1	0	1	0	0	0	3	0	197
4	2	1	1	0	1	0	0	5	0	195
5	2	2	1	1	0	1	0	7	0	193
6	4	2	2	1	1	0	1	11	0	189
7	5	4	2	2	1	1	0	15	1	184
8	8	5	4	2	2	1	1	23	1	176
9	11	8	5	4	2	2	1	33	2	165
10	17	11	8	5	4	2	2	49	3	148
11	24	17	11	8	5	4	2	71	5	124
12	36	24	17	11	8	5	4	105	7	88
13	52	36	24	17	11	8	5	153	11	36
14	36	52	36	24	17	11	8	184	16	0
15	0	36	52	36	24	17	11	176	24	0
16	0	0	36	52	36	24	17	165	35	0
17	0	0	0	36	52	36	24	148	52	0
18	0	0	0	0	36	52	36	124	76	0
19	0	0	0	0	0	36	52	88	112	0
20	0	0	0	0	0	0	36	36	164	0
21	0	0	0	0	0	0	0	0	200	0

# REFERENCES

1. L. Billiard & Zhen Zhao. "The Stochastic General Epidemic Model Revisited and a Generalization." *IMA Journal of Mathematics Applied in Medicine and Biology* **10** (1993):67-75.
2. M. A. B. Deakin & D. L. S. McElwain. "Approximate Solution for an Integro-Differential Equation." *International Journal of Mathematical Education in Science and Technology* **25** (1994):1-4.
3. F. Dubeau. "The Rabbit Problem Revisited." *The Fibonacci Quarterly* **31.3** (1993):268-74.
4. V. E. Hoggatt, Jr. "Generalized Rabbits for Generalized Fibonacci Numbers." *The Fibonacci Quarterly* **6.2** (1968):105-12.
5. V. E. Hoggatt, Jr., & D. A. Lind. "The Dying Rabbit Problem." *The Fibonacci Quarterly* **7.6** (1969):482-87.
6. F. C. Hoppensteadt. "An Age-Dependent Epidemic Model." *Journal of the Franklin Institute* **297** (1974):325-33.
7. W. G. Kelley & A. C. Peterson. *Difference Equations: An Introduction with Applications*. San Diego: Academic Press, 1991.
8. D. A. Klarner. "A Model for Population Growth." *The Fibonacci Quarterly* **14.3** (1976): 277-81.
9. A. Makhmudov. "On Fibonacci's Model of Infectious Disease." In *Mathematical Modelling in Immunology and Medicine*, pp. 319-23. Ed. G. I. Marchuk and L. N. Belyk. North Holland: Amsterdam, 1983.
10. A. M. Ostrowski. *Solution of Equations in Euclidean and Banach Spaces*. New York: Academic Press, 1973.
11. E. A. Parberry. "A Recurrence Relation for Populations of Diatoms." *The Fibonacci Quarterly* **7.6** (1969):449-57, 463.
12. A. G. Shannon, J. H. Clarke, & L. J. Hills. "Contingency Relations for Infectious Diseases." In *Mathematical Models in Medicine* 2:829-33. Ed. M. Witten. Oxford: Pergamon, 1988.
13. K. Weland. "Some Rabbit Production Results Involving Fibonacci Numbers." *The Fibonacci Quarterly* **5.3** (1967):195-200.

AMS Classification Numbers: 11B37, 11B39, 92D30



# ON THE FIBONACCI NUMBERS WHOSE SUBSCRIPT IS A POWER

**Piero Filippini**

Fondazione Ugo Bordoni, Via B. Castiglione 59, I-00142 Rome, Italy

(Submitted October 1994)

## 1. AIM OF THE PAPER

The well-known identity (e.g., see [1], p. 127)

$$F_{2^n} = \prod_{i=1}^{n-1} L_{2^i} \quad (1.1)$$

led us to investigate the Fibonacci numbers of the form  $F_{k^n}$  with  $k$  and  $n$  positive integers. The principal aim of this note is to present some new identities involving  $F_{k^n}$ , some of which generalize (1.1). This is done in Sections 2 and 3. In Section 4, a first-order recurrence relation for  $F_{k^n}$  is established which involves certain combinatorial quantities whose properties will be investigated in a future paper. A glimpse of analogous results concerning the Lucas numbers  $L_{k^n}$  is caught in Section 5.

The formulas established in this note encompass the trivial case  $n = 1$  under the usual assumptions

$$\prod_{i=a}^b f(i) = 1 \text{ if } b < a \quad (1.2)$$

and

$$\sum_{i=a}^b f(i) = 0 \text{ if } b < a. \quad (1.3)$$

## 2. MAIN RESULT

**Proposition 1:** If  $k$  is even and  $n \geq 1$ , then

$$F_{k^n} = F_k \prod_{i=1}^{n-1} \left[ \sum_{j=1}^{k/2} L_{(2^{j-1})k^i} \right]. \quad (2.1)$$

We can immediately observe that, if  $k = 2$ , identity (2.1) reduces to (1.1).

**Proof of Proposition 1:** Write

$$F_{k^n} = F_k \cdot \frac{F_{k^2}}{F_k} \cdot \frac{F_{k^3}}{F_{k^2}} \cdot \dots \cdot \frac{F_{k^n}}{F_{k^{n-1}}} = F_k \prod_{i=1}^{n-1} \frac{F_{k^{i+1}}}{F_{k^i}} \quad (2.2)$$

whence, following the notation used in [2] [namely,  $R_s(t) = F_{st} / F_t$ ], we can rewrite (2.2) as

$$F_{k^n} = F_k \prod_{i=1}^{n-1} R_k(k^i). \quad (2.3)$$

Using (2.3) along with (2.1) of [2] yields

$$F_{k^n} = F_k \prod_{i=1}^{n-1} \left\{ \sum_{j=1}^{k/2} [F_{k^i(2j-1)-1} + F_{k^i(2j-1)+1}] \right\}. \quad (2.4)$$

The right-hand side of (2.4) clearly equals that of (2.1). Q.E.D.

**Proposition 2:** If  $k$  is odd and  $n \geq 1$ , then

$$F_{k^n} = (-1)^{(n-1)(k-1)/2} F_k \prod_{i=1}^{n-1} \left[ 1 + \sum_{j=1}^{(k-1)/2} (-1)^j L_{2jk^i} \right]. \quad (2.5)$$

Observe that, if  $k = 3$ , identity (2.5) reduces beautifully to

$$F_{3^n} = 2 \prod_{i=1}^{n-1} (L_{2 \cdot 3^i} - 1). \quad (2.6)$$

In order to prove Proposition 2, we need the identity

$$\sum_{i=1}^r (-1)^i L_{ai} = \frac{(-1)^{a+r} L_{ar} + (-1)^r L_{a(r+1)} - L_a - 2(-1)^a}{L_a + 1 + (-1)^a}, \quad (2.7)$$

which can readily be proved by using the Binet form for Lucas numbers and the geometric series formula. We also need the identity

$$L_{a+b} - (-1)^b L_{a-b} = 5F_a F_b, \quad (2.8)$$

which can be obtained from identities  $I_{21} - I_{24}$  of [3].

**Proof of Proposition 2:** The proof has to be split into two cases according to the residue of  $k$  modulo 4.

**Case 1.**  $k \equiv 1 \pmod{4}$  [i.e.,  $(k-1)/2$  is even]

By (2.2), we can write

$$\begin{aligned} F_{k^n} &= F_k \prod_{i=1}^{n-1} \frac{F_{k^{i+1}}}{F_{k^i}} = F_k \prod_{i=1}^{n-1} \left[ 1 + \frac{5F_{k^{i+1}}F_{k^i}}{5F_{k^i}^2} - 1 \right] \\ &= F_k \prod_{i=1}^{n-1} \left[ 1 + \frac{L_{k^{i+1}-k^i} + L_{k^{i+1}+k^i}}{L_{2k^i} + 2} - 1 \right] \quad (\text{by (2.8) and } I_{17} \text{ of [3]}) \\ &= F_k \prod_{i=1}^{n-1} \left[ 1 + \frac{L_{2k^i(k-1)/2} + L_{2k^i(k+1)/2} - L_{2k^i} - 2}{L_{2k^i} + 2} \right] \\ &= F_k \prod_{i=1}^{n-1} \left[ 1 + \sum_{h=1}^{(k-1)/2} (-1)^h L_{2hk^i} \right] \quad [\text{by (2.7)}]. \end{aligned}$$

Observe that, since  $(k-1)/2$  is even by hypothesis, the above expression does not vary if we multiply it by  $(-1)^{(n-1)(k-1)/2}$ .

**Case 2.**  $k \equiv 3 \pmod{4}$  [i.e.,  $(k-1)/2$  is odd]

Analogously, we can write

$$\begin{aligned} F_{k^n} &= (-1)^{n-1} F_k \prod_{i=1}^{n-1} \left[ -\frac{5F_{k^{i+1}}F_{k^i}}{5F_{k^i}^2} - 1 + 1 \right] \\ &= (-1)^{n-1} F_k \prod_{i=1}^{n-1} \left[ 1 + \frac{-L_{2k^i(k-1)/2} - L_{2k^i(k+1)/2} - L_{2k^i} - 2}{L_{2k^i} + 2} \right] \\ &= (-1)^{n-1} F_k \prod_{i=1}^{n-1} \left[ 1 + \sum_{h=1}^{(k-1)/2} (-1)^h L_{2hk^i} \right]. \end{aligned}$$

Observe that, since  $(k-1)/2$  is odd by hypothesis, the factor  $(-1)^{n-1}$  in the above expression can be rewritten as  $(-1)^{(n-1)(k-1)/2}$ . Q.E.D.

### 3. RELATED RESULTS

Some results related to those established in Section 2 can be obtained readily. Observe that, if the exponent  $n$  in (2.1) is composite (say,  $n = st$ ), then  $F_{k^n}$  ( $k$  even) can be expressed as

$$F_{k^n} = F_{k^{st}} = F_{k^s} \prod_{i=1}^{t-1} \left[ \sum_{j=1}^{k^s/2} L_{(2j-1)k^{si}} \right] \quad (k \text{ even}), \quad (3.1)$$

where  $s$  and  $t$  can obviously be interchanged. For example, by (1.1) and (3.1), we have

$$F_{2^{2n}} = F_{4^n} = \prod_{i=1}^{2n-1} L_{2^i} = F_{2^n} \sum_{j=1}^{2^{n-1}} L_{(2j-1)2^n} = 3 \prod_{i=1}^{n-1} (L_{4^i} + L_{3 \cdot 4^i}). \quad (3.2)$$

For  $k$  odd, the analog of (3.1) can be obtained immediately.

An expression analogous to (2.1) can be established for  $F_{mk^n}$  when  $mk$  is even. If  $mk$  is odd, the corresponding expression is somewhat unattractive and its presentation is omitted.

**Proposition 3:** If  $n \geq 1$ ,

$$F_{mk^n} = F_{mk} \prod_{i=1}^{n-1} \left[ \sum_{j=1}^{k/2} L_{(2j-1)mk^i} \right] \quad (k \text{ even, } m \text{ arbitrary}) \quad (3.3)$$

and

$$F_{mk^n} = F_{mk} \prod_{i=1}^{n-1} \left[ 1 + \sum_{j=1}^{(k-1)/2} L_{2jmk^i} \right] \quad (k \text{ odd, } m \text{ even}). \quad (3.4)$$

**Proof:** Write

$$F_{mk^n} = F_{mk} \prod_{i=1}^{n-1} \frac{F_{mk^{i+1}}}{F_{mk^i}} = F_{mk} \prod_{i=1}^{n-1} R_k(mk^i)$$

and use (2.1) and (2.2) of [2]. Q.E.D.

If we let  $m = k$  in (3.3), we see that an equivalent form for (2.1) is

$$F_{k^n} = F_{k^2} \prod_{i=1}^{n-2} \left[ \sum_{j=1}^{k/2} L_{(2^{j-1})k^{i+1}} \right] \quad (k \text{ even}, n \geq 2). \quad (3.5)$$

Moreover, if we let  $n = u + v$  ( $u, v \geq 1$ ) and  $m = k^u$  in (3.3), we get the relation

$$F_{k^n} = F_{k^{u+v}} = F_{k^u k^v} = F_{k^{u+1}} \prod_{i=1}^{v-1} \left[ \sum_{j=1}^{k/2} L_{(2^{j-1})k^{u+i}} \right] \quad (k \text{ even}), \quad (3.6)$$

which generalizes (3.5).

#### 4. A RECURRENCE RELATION FOR $F_{k^n}$

A problem [6] that appeared in this journal led us to discover the first-order nonlinear homogeneous recurrence relation

$$F_{3^{n+1}} = 5F_{3^n}^3 - 3F_{3^n} \quad (n \geq 0). \quad (4.1)$$

The aim of this section is to obtain an analogous relation valid for all positive subscripts  $k^{n+1}$  with  $k$  odd and  $n$  an arbitrary nonnegative integer.

**Proposition 4:** If  $k$  is a positive odd integer and  $n$  is a nonnegative integer, then

$$F_{k^{n+1}} = 5^{(k-1)/2} F_{k^n}^k - \sum_{i=0}^{(k-3)/2} 5^i C_{i,k} F_{k^n}^{2i+1}, \quad (4.2)$$

where the coefficients  $C_{i,k}$  are given by

$$C_{i,k} = (-1)^{(k+1)/2+i} \binom{(k+1)/2+i}{2i+1} \frac{k}{(k+1)/2+i} \quad [0 \leq i \leq (k-3)/2]. \quad (4.3)$$

As an example, for  $k = 3, 5, 7$ , and  $9$ , (4.2) gives (4.1),

$$F_{3^{n+1}} = 25F_{3^n}^5 - 25F_{3^n}^3 + 5F_{3^n}, \quad (4.4)$$

$$F_{7^{n+1}} = 125F_{7^n}^7 - 175F_{7^n}^5 + 70F_{7^n}^3 - 7F_{7^n}, \quad (4.5)$$

and

$$F_{9^{n+1}} = 625F_{9^n}^9 - 1125F_{9^n}^7 + 675F_{9^n}^5 - 150F_{9^n}^3 + 9F_{9^n}, \quad (4.6)$$

respectively.

**Proof of Proposition 4:** First, let us write

$$F_{k^n}^k = \frac{1}{(\sqrt{5})^k} \sum_{j=0}^k \binom{k}{j} (-1)^j \beta^{jk^n} \alpha^{(k-j)k^n}, \quad (4.7)$$

where  $\alpha = 1 - \beta = (1 + \sqrt{5})/2$ . After several simple but tedious manipulations involving the use of the Binet forms for Fibonacci and Lucas numbers, and the relation  $\alpha\beta = -1$ , (4.7) yields the following identities which may be of some interest *per se*:



$$F_{k^n}^k = \frac{1}{5^{(k-1)/2}} \left[ F_{k^{n+1}} + \sum_{j=1}^{(k-1)/2} \binom{k}{j} F_{(k-2j)k^n} \right] \quad (k \text{ odd}, n \geq 0), \quad (4.8)$$

$$F_{k^n}^k = \frac{1}{5^{k/2}} \left[ (-1)^{k/2} \binom{k}{k/2} + \sum_{j=0}^{(k-2)/2} (-1)^j \binom{k}{j} L_{(k-2j)k^n} \right] \quad (k \text{ even}, n \geq 1). \quad (4.9)$$

By (4.8), we immediately obtain

$$F_{k^{n+1}} = 5^{(k-1)/2} F_{k^n}^k - \sum_{j=1}^{(k-1)/2} \binom{k}{j} F_{(k-2j)k^n} \quad (k \text{ odd}). \quad (4.10)$$

Then, using (4.10) along with Theorem 1 of [4] leads to the expression

$$F_{k^{n+1}} = 5^{(k-1)/2} F_{k^n}^k - \sum_{j=1}^{(k-1)/2} \sum_{i=0}^{(k-1)/2-j} (-1)^{(k-1)/2+i-j} \frac{k-2j}{(k+1)/2+i-j} 5^i \binom{k}{j} \binom{(k+1)/2+i-j}{2i+1} F_{k^n}^{2i+1} \quad (4.11)$$

which, after reversing the summation order, can be rewritten as

$$F_{k^{n+1}} = 5^{(k-1)/2} F_{k^n}^k - \sum_{i=0}^{(k-1)/2} 5^i A_{i,k} F_{k^n}^{2i+1}, \quad (4.12)$$

where

$$A_{i,k} = (-1)^i \sum_{j=1}^{(k-1)/2-i} (-1)^{(k-1)/2-j} \frac{k-2j}{(k+1)/2+i-j} \binom{k}{j} \binom{(k+1)/2+i-j}{2i+1}. \quad (4.13)$$

Since  $A_{(k-1)/2,k} = 0$  by (1.3), expression (4.12) becomes

$$F_{k^{n+1}} = 5^{(k-1)/2} F_{k^n}^k - \sum_{i=0}^{(k-3)/2} 5^i A_{i,k} F_{k^n}^{2i+1}. \quad (4.14)$$

Now it remains to show that the numbers  $A_{i,k}$  [defined by (4.13)] and the numbers  $C_{i,k}$  [defined by (4.3)] coincide. To do this, consider the combinatorial identity

$$\begin{aligned} & \sum_{j=1}^m (-1)^j \frac{k-2j}{k-m-j} \binom{k}{j} \binom{k-m-j}{m-j} \\ &= -\frac{k}{k-m} \binom{k-m}{m} \quad [1 \leq m \leq (k-1)/2], \end{aligned} \quad (4.15)$$

which can be obtained by [5, p. 58], and replace  $m$  by  $(k-1)/2-i$  in (4.15) to obtain the desired result  $C_{i,k} = A_{i,k}$ . Q.E.D.

## 5. CONCLUDING REMARKS

Some properties of the numbers  $F_{k^n}$  have been investigated in this note. In particular, expressions for these numbers in terms of products involving Lucas numbers have been established. Analogous expressions for  $L_{k^n}$  appeared to be rather unpleasant, so we confine ourselves to show some partial results whose proofs are left to the perseverance of the reader. In particular, we show the identity

$$L_{k^n} = 2 + (L_{k^2} - 2) \prod_{i=1}^{n-2} \left[ \sum_{j=1}^{k/2} L_{(2j-1)k^{i+1/2}} \right]^2 \quad (k \text{ even}, n \geq 2) \quad (5.1)$$

which, for  $k = 2$ , reduces to

$$L_{2^n} = 2 + 5 \prod_{i=1}^{n-2} L_{2^i}^2 \quad (n \geq 2). \quad (5.2)$$

We also have

$$L_{3^n} = 4 \prod_{i=1}^{n-1} (L_{2 \cdot 3^i} + 1) \quad (n \geq 1). \quad (5.3)$$

Observe that the identity

$$F_{2 \cdot 3^n} = 8 \prod_{i=1}^{n-1} (L_{2 \cdot 3^i}^2 - 1) = 8 \prod_{i=1}^{n-1} (L_{4 \cdot 3^i} + 1) \quad (n \geq 1) \quad (5.4)$$

can be obtained either by (2.6) and (5.3), or by (3.4).

## ACKNOWLEDGMENT

This work has been carried out in the framework of an agreement between the Italian PT Administration (Istituto Superiore PT) and the Fondazione Ugo Bordoni. The author wishes to express his gratitude to an anonymous referee whose suggestions have greatly improved this paper.

## REFERENCES

1. R. M. Capocelli, ed. *Sequences*. New York: Springer-Verlag, 1990.
2. P. Filippini & H. T. Freitag. "The Zeckendorf Representation of  $F_{kn} / F_n$ ." In *Applications of Fibonacci Numbers* 5:217-19. Dordrecht: Kluwer, 1993.
3. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin, 1969; rpt. The Fibonacci Association, 1979.
4. D. Jennings. "Some Polynomial Identities for the Fibonacci and Lucas Numbers." *The Fibonacci Quarterly* 31.2 (1993):134-37.
5. J. Riordan. *Combinatorial Identities*. New York: Wiley, 1968.
6. Problem B-746. *The Fibonacci Quarterly* 31.3 (1993):278.



# ON THE DIOPHANTINE EQUATION $\left(\frac{x(x-1)}{2}\right)^2 = \frac{y(y-1)}{2}$

Ming Luo

Department of Mathematics, Chongqing Teachers' College  
Sichuan Province, 630047, People's Republic of China  
(Submitted October 1994)

Positive integers of the form  $\frac{1}{2}m(m-1)$  are called *triangular numbers*. The Diophantine equation

$$\left(\frac{x(x-1)}{2}\right)^2 = \frac{y(y-1)}{2} \quad (1)$$

corresponds to the question: For which triangular numbers are their squares still triangular [1]? In 1946, Ljunggren [2] solved this problem when he proved the following.

**Theorem:** The Diophantine equation (1) has only the following solutions in positive integers:  $(x, y) = (1, 1)$ ,  $(2, 2)$ , and  $(4, 9)$ .

That is, only the two triangular numbers 1 and 36 can be represented as squares of numbers of the same form. However, Ljunggren used his knowledge of the biquadratic field  $Q(2^{1/4})$  and the  $p$ -adic method, so his proof is somewhat complex. In 1965, Cassels [3] gave a much simpler proof, but he also used his knowledge of the biquadratic field  $Q((-2)^{1/4})$ . In 1989, Cao [4] conjectured that (1) could be solved by the method of recurrent sequences. We verify his conjecture in this paper by giving the theorem and an elementary as well as simple proof by the method of recurrent sequences without using anything deeper than reciprocity.

**Proof of the Theorem:** Let  $X = 2x - 1$  and  $Y = 2y - 1$ , then equation (1) may be reduced to  $Y^2 - 2\left(\frac{X^2-1}{4}\right)^2 = 1$ . Since  $u + v\sqrt{2} = u_n + v_n\sqrt{2} = (1 + \sqrt{2})^n$  gives the general solution of the Pellian equation  $u^2 - v^2 = (-1)^n$ , where  $1 + \sqrt{2}$  is its fundamental solution and  $n$  is an arbitrary integer (see, e.g., [1]), we get

$$X^2 = 4v_n + 1, \quad 2|n. \quad (2)$$

The following relations may be derived easily from the general solution of Pell's equation:

$$u_{n+2} = 2u_{n+1} + u_n, \quad u_0 = 1, \quad u_1 = 1; \quad (3)$$

$$v_{n+2} = 2v_{n+1} + v_n, \quad v_0 = 0, \quad v_1 = 1; \quad (4)$$

$$u_{2n} = u_n^2 + 2v_n^2, \quad v_{2n} = 2u_nv_n; \quad (5)$$

$$v_{-n} = (-1)^{n+1}v_n; \quad (6)$$

$$v_{n+2k} \equiv (-1)^{k+1}v_n \pmod{u_k}. \quad (7)$$

If  $n < 0$ , then  $4v_n + 1 < 0$ , and (2) is impossible. Hence, it is necessary that  $n \geq 0$ . We shall prove that (2) cannot hold for any  $n > 4$  by showing that  $4v_n + 1$  is a quadratic nonresidue modulo some positive integer.

First, we consider the following three cases:

**Case 1.** If  $n \equiv 0 \pmod{6}$  and  $n > 0$ , then we write  $n = 3^r(6k \pm 2)$ ,  $4 \geq 1$ . Let  $m = 3^r$ , then, by (6) and (7), we get  $v_n \equiv v_{\pm 2m} \equiv \pm v_{2m} \pmod{u_{3m}}$ . Since  $u_{3m} = u_m(u_m^2 + 6v_m^2)$ , we obtain  $4v_n + 1 \equiv \pm 4v_{2m} + 1 \pmod{u_m^2 + 6v_m^2}$ .

Note that  $2 \nmid m$  implies  $u_m^2 + 6v_m^2 \equiv 7 \pmod{8}$  and  $v_m \equiv 1 \pmod{4}$  so, by (5), we obtain

$$\begin{aligned} \left(\frac{4v_{2m} + 1}{u_m^2 + 6v_m^2}\right) &= \left(\frac{8u_mv_m - u_m^2 + 2v_m^2}{u_m^2 + 6v_m^2}\right) = \left(\frac{8v_m(u_m + v_m)}{u_m^2 + 6v_m^2}\right) \\ &= \left(\frac{(u_m + v_m)/2^s}{u_m^2 + 6v_m^2}\right) \quad (\text{where } 2^s \parallel u_m + v_m) \\ &= \left(\frac{-1}{(u_m + v_m)/2^s}\right) \left(\frac{u_m^2 + 6v_m^2}{(u_m + v_m)/2^s}\right) \\ &= \left(\frac{-1}{(u_m + v_m)/2^s}\right) \left(\frac{7}{(u_m + v_m)/2^s}\right) = \left(\frac{u_m + v_m}{7}\right). \end{aligned}$$

Similarly,

$$\left(\frac{-4v_{2m} + 1}{u_m^2 + 6v_m^2}\right) = \left(\frac{-u_m + v_m}{7}\right).$$

Equations (3) and (4) modulo 7 yield two residue sequences with the same period of 6. Since  $m \equiv 3 \pmod{6}$ , we have  $\pm u_m + v_m \equiv 5 \pmod{7}$ , so that

$$\left(\frac{4v_n + 1}{u_m^2 + 6v_m^2}\right) = \left(\frac{5}{7}\right) = -1,$$

and (2) cannot hold.

**Case 2.** If  $n \equiv 2 \pmod{4}$  and  $n > 2$ , then we write  $n = 2 + 2 \cdot 3^r \cdot m$ , where  $r \geq 0$ ,  $m \equiv \pm 2 \pmod{6}$ . By (7), we have  $4v_n + 1 \equiv -4v_2 + 1 \equiv -7 \pmod{u_m}$ ,

$$\left(\frac{4v_n + 1}{u_m}\right) = \left(\frac{-7}{u_m}\right) = \left(\frac{u_m}{7}\right) = \left(\frac{3}{7}\right) = -1,$$

so that (2) cannot hold.

**Case 3.** If  $n \equiv 4 \pmod{60}$  and  $n > 4$ , then we write  $n = 4 + 2 \cdot 3 \cdot 5 \cdot k \cdot 2^r$ , where  $r \geq 1$ ,  $2 \nmid k$ . Let  $m = 2^r$  or  $3 \cdot 2^r$  or  $15 \cdot 2^r$  (to be determined). By (7), we have  $4v_n + 1 \equiv -4v_4 + 1 \equiv -47 \pmod{u_m}$ ,

$$\left(\frac{4v_n + 1}{u_m}\right) = \left(\frac{-47}{u_m}\right) = \left(\frac{u_m}{47}\right).$$

The residue sequence of (3) modulo 47 has period 46. The period, with respect to  $r$ , of the residue sequence of  $\{2^r\}$  modulo 46 is 11. We determine our choice of  $m$  as follows:

$$\text{ON THE DIOPHANTINE EQUATION } \left( \frac{x(x-1)}{2} \right)^2 = \frac{y(y-1)}{2}$$

$$m = \begin{cases} 2^r, & \text{if } r \equiv 3, 5, 6, 7, 8, 9 \pmod{11}, \\ 3 \cdot 2^r, & \text{if } r \equiv 0, 1, 10 \pmod{11}, \\ 15 \cdot 2^r & \text{if } r \equiv 2, 4 \pmod{11}, \end{cases}$$

from which we obtain the following table.

$r \pmod{11}$	0	1	2	3	4	5	6	7	8	9	10
$2^r \pmod{46}$				8		32	18	36	26	6	
$3 \cdot 2^r \pmod{46}$	26	6									36
$15 \cdot 2^r \pmod{46}$			14		10						
$u_m \pmod{47}$	35	5	33	13	26	33	15	26	35	5	26

It is easy to verify that each of the  $u_m$  in this table is a quadratic nonresidue modulo 47, from which it follows that (2) is impossible.

The three cases above tell us that, for (2) to hold,  $n$  must satisfy one of the following conditions:

$$n = 0, 2, 4;$$

or

$$n \equiv 8, 16, 20, 28, 32, 40, 44, 52, 56 \pmod{60}. \quad (8)$$

We now exclude all residues in (8) by considering some moduli of the sequence  $\{4v_n + 1\}$ .

First, consider modulo 5. The residue sequence of  $\{4v_n + 1\}$  has period 12. If  $n \equiv 8 \pmod{12}$ , then  $4v_n + 1 \equiv 3 \pmod{5}$ , which implies that (2) is impossible. Thus, we exclude  $n \equiv 8, 20, 32, 44, 56 \pmod{60}$  in (8).

Second, consider modulo 31. We get the residue sequence of  $\{4v_n + 1\}$  having a period 30. If  $n \equiv 10, 16, 22, 28 \pmod{30}$ , then  $4v_n + 1 \equiv 27, 17, 12, 24 \pmod{31}$ , respectively. However, all of these are quadratic nonresidue modulo 31; thus, (2) cannot hold. Hence, we can exclude in (8) the other four residue classes of  $n \equiv 16, 28, 40, 52 \pmod{60}$ .

Finally, we look at the three values of  $n = 0, 2, 4$ , which give  $X = 1, 3, 7$ , respectively, in (2). Therefore, we see that all positive integer solutions of (1) are  $(x, y) = (1, 1), (2, 2)$ , and  $(4, 9)$  and the proof is complete.

## REFERENCES

1. L. J. Mordell. *Diophantine Equations*, pp. 268-69. London: Academic Press, 1969.
2. W. Ljunggren. "Solution complète de quelques équations du sixième degré à deux indéterminées." *Arch. Math. Naturv.* **48.7** (1946):26-29.
3. J. W. S. Cassels. "Integral Points on Certain Elliptic Curves." *Proc. Lond. Math. Soc.* (3) **14A** (1965):55-57.
4. Z. Cao. *Introduction to Diophantine Equations* (in Chinese), pp. 290-91. Harbin Industrial University Press, 1989.

AMS Classification Numbers: 11D25



# GENERALIZED HOCKEY STICK IDENTITIES AND N-DIMENSIONAL BLOCKWALKING

Charles H. Jones

P.O. Box 1716, Rosamond, CA 93560

(Submitted October 1994)

## 1. INTRODUCTION

Traditionally, the word "abracadabra" was encrypted onto amulets and other magical paraphernalia to help ward off evil. George Pólya ([8], [9]) provided the cryptic form of this word shown in Figure 1 and asked how many ways abracadabra can be spelled out using this diagram. If we replace the diagram in Figure 1 with the grid shown in Figure 2 where letters in the original diagram are placed at points of intersection of the grid, then the question is equivalent to asking how many paths there are from the top of the grid to the spade at the bottom of the grid where each step is either down and left or down and right. One such path that spells out abracadabra is shown. By considering this grid as a city street map, we can think of such paths as walking city blocks—or *blockwalking*.

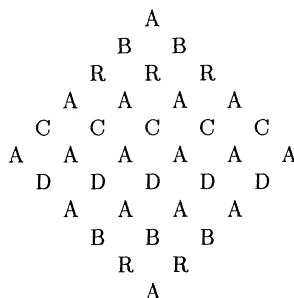
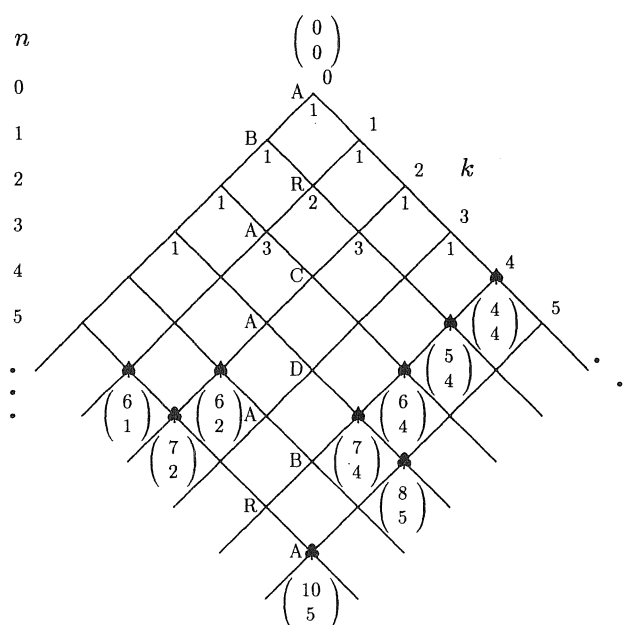


FIGURE 1. How many ways can you spell ABRACADABRA in the above diagram?

We can represent a blockwalking path by a series of *R*'s (right turns) and *L*'s (left turns). For example, the abracadabra path illustrated in Figure 2 can be represented by *LRLRLRLRLR*. It is easy to see that any path which spells abracadabra will have 5 *R*'s and 5 *L*'s. More generally, we can see that any corner of the map can be determined uniquely by how many *L*'s and *R*'s it takes to get there. If there are  $n$  total steps in the path to get to a corner and there are  $k$  *L*'s, then there are  $n - k$  *R*'s. The number of paths to that corner is thus the number of combinations of  $k$  *L*'s and  $n - k$  *R*'s. As is well known, this is the binomial coefficient  $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ . In particular, the number of ways abracadabra can be spelled out in the diagram is  $\binom{10}{5} = 252$ . Thus, we use the binomial coefficients to label the corners, and it should be apparent that we are constructing Pascal's triangle. When looking at the binomial coefficient for a particular corner, remember that the  $n$ 's indicate the row of the triangle whereas the  $k$ 's count the number of lefts taken. For an excellent history of Pascal's triangle, see [3], which includes an English translation of Pascal's original treatise [7].



A different sieve leads us to the *Hockey Stick Identity*:

$$\sum_{i=k}^n \binom{i}{k} = \binom{n+1}{k+1}. \quad (2)$$

Consider that for any path there must be a last  $L$  after which all other choices are  $R$ 's. Thus, we may partition paths to  $\binom{n+1}{k+1}$  into classes depending on how many consecutive  $R$ 's are at the end of the path. The sum of the sizes of these classes thus equals the number of paths to  $\binom{n+1}{k+1}$ . This proves (2). Again, the equivalence classes can be associated with a sieve of corners. For example, the four spades from  $\binom{4}{4}$  to  $\binom{7}{4}$  form a sieve for  $\binom{8}{5}$ . This example also illustrates the use of the name *Hockey Stick Identity*. (This is also called the *Stocking Identity*. Does anyone know who first used these names?)

The following sections provide two distinct generalizations of the blockwalking technique. They are illustrated by proving distinct generalizations of the Hockey Stick Identity. We will be using the standard Hockey Stick Identity several times to prove these generalized forms. When we wish to do so by referencing its pictorial representation, we will refer to "summing the spades into the club."

## 2. MULTITIERED BLOCKWALKING

A somewhat obvious variation of the Hockey Stick Identity is to multiply the binomial coefficient inside the summation by  $i$ . Surprisingly, the author has not been able to find a reference for this variation (including [4] and [12]). We will give a generalized blockwalking argument to provide a closed form for this variation which we will call the *Extended Hockey Stick Identity*:

$$\sum_{i=k}^n i \binom{i}{k} = n \binom{n+1}{k+1} - \binom{n+1}{k+2}. \quad (3)$$

As illustrated in Figure 3, stack copies of Pascal's triangle on top of each other in tiers. The multitiered blockwalking technique follows these rules:

1. On each tier, you may walk blocks in the normal 2-dimensional fashion.
2. Your starting point may be at the apex on any tier.
3. At the end of a walk on your starting tier, you may step into an elevator and be raised a given number of tiers.
4. After having been elevated, you are at your final destination.

Any such path may be considered a series of  $L$ 's and  $R$ 's followed by some number of  $U$ 's (ups). (The alternative interpretation, which allows moving up at *any* point along a path, will be discussed under multinomial blockwalking in the next section.)

As with the standard single-tiered case, we label a corner with the number of paths to that corner. Using the specified rules, the  $\binom{n}{k}$  corner on Tier  $t$  counts  $t \binom{n}{k}$  paths;  $\binom{n}{k}$  paths for each of  $t$  tiers. Figure 3 shows the path  $LRLRLUUU$  which starts on Tier 3 and ends at  $6 \binom{7}{3}$ . (For pictorial convenience, Figures 3 and 4 have the  $k$ 's count  $R$ 's instead of  $L$ 's. This is symmetric to the standard representation of Pascal's triangle in Figure 2.)



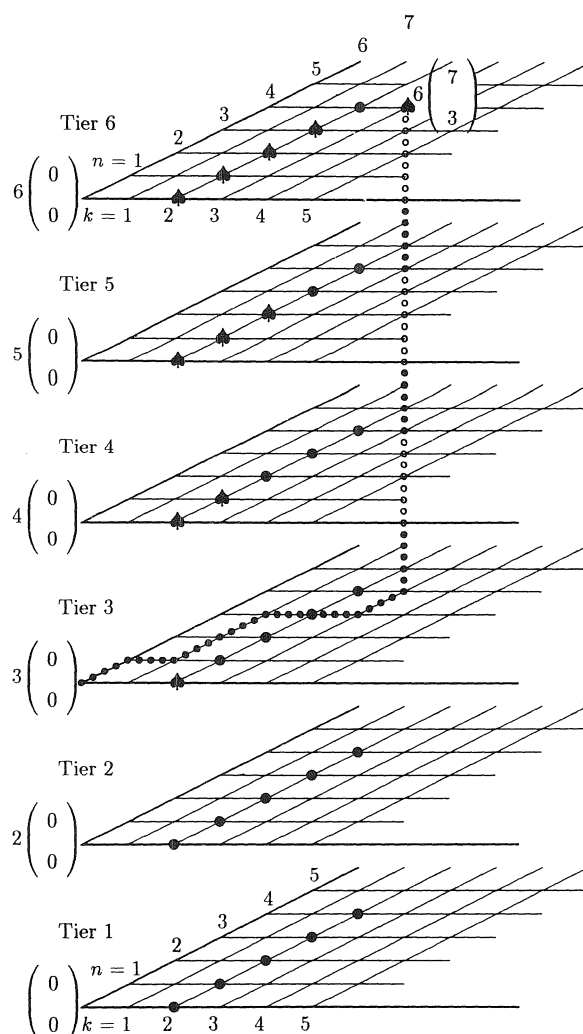


FIGURE 3. Multitiered Blockwalking

We can partition the paths to  $n \binom{n+1}{k+1}$  into equivalence classes based on how many  $U$ 's are at the end and how many consecutive  $L$ 's precede the  $U$ 's. We illustrate this with  $n = 6$  and  $k = 2$  in Figure 3. The sieve for  $6 \binom{7}{3}$  is shown using spades and filled circles. This illustrates:

$$n \binom{n+1}{k+1} = n \sum_{i=k}^n \binom{i}{k} = \sum_{i=k}^n n \binom{i}{k}. \quad (4)$$

By splitting the corners in the sieve appropriately, we illustrate:

$$\sum_{i=k}^n n \binom{i}{k} = \sum_{i=k}^n i \binom{i}{k} + \sum_{i=k}^n (n-i) \binom{i}{k}. \quad (5)$$

The filled circles in Figure 3 represent the first summation on the right-hand side of (5) and the spades represent the second summation. By rearranging (5) and applying (4), we get

$$\sum_{i=k}^n i \binom{i}{k} = n \binom{n+1}{k+1} - \sum_{i=k}^n (n-i) \binom{i}{k}. \quad (6)$$

In order to complete the proof of (3), we need to find a closed form for the subtrahend in (6).

A copy of Pascal's triangle can be formed by slicing a plane through the tiers as shown in Figure 4. That is, consider the plane that slices in front of the circles and through the last spade on each tier. This newly formed Pascal triangle consists of one street from each tier starting on Tier  $t = k + 1$ . In the example, the corner labeled  $3 \binom{0}{0}$  is the apex of the new slicing Pascal triangle. Other nodes on this new Pascal triangle are labeled the same as they originally were except that the binomial coefficient is not multiplied by the tier number.

Using the standard Hockey Stick Identity on the spades on each tier (i.e., sum the spades into the clubs in Figure 4), we see that

$$\sum_{i=k}^n (n-i) \binom{i}{k} = \sum_{i=k}^{n-1} \sum_{j=k}^i \binom{j}{k} = \sum_{i=k}^{n-1} \binom{i+1}{k+1}.$$

Applying the standard Hockey Stick Identity on the slicing plane (i.e., summing the clubs into the circle at  $\binom{7}{4}$  in Figure 4) gives

$$\sum_{i=k}^n (n-i) \binom{i}{k} = \sum_{i=k}^{n-1} \binom{i+1}{k+1} = \binom{n+1}{k+2}. \quad (7)$$

Combining (6) with (7) gives (3).

In personal correspondences to the author William Webb proved (3) using the "Snake Oil Method" of [14] and Bruce Berndt proved (3) using Vandermonde's theorem involving hypergeometric series (see [1]). However, a telescoping series gives the *Generalized Extended Hockey Stick Identity*:

$$\begin{aligned} \sum_{i=k}^n i^p \binom{i}{k} &= k^p \sum_{i=k}^n \binom{i}{k} + ((k+1)^p - k^p) \sum_{i=k+1}^n \binom{i}{k} + \cdots + (n^p - (n-1)^p) \sum_{i=n}^n \binom{i}{k} \\ &= k^p \binom{n+1}{k+1} + \sum_{i=k+1}^n (i^p - (i-1)^p) \left[ \binom{n+1}{k+1} - \binom{i}{k+1} \right]. \end{aligned}$$

Note that  $i^p - (i-1)^p$  is a polynomial of degree  $p-1$ . Thus, the  $p^{\text{th}}$  case can be determined recursively.

Let us consider this generalized form in terms of multitiered blockwalking. When  $p = 1$ , the structure used to slice through the multitiered sieve is a line (between the spades and circles). Similar (though much more complicated) arguments could be provided for the  $p^{\text{th}}$  case by slicing the sieve with a curve of the form  $i^p$ .

s is to

This is also called a *Pascal hyperpyramid* or a *Pascal polytope*. Generalizations of Pascal's original results to hyperpyramids can be found in [10] and [11]. An excellent survey and an extensive bibliography of Pascal hyperpyramids can be found in [2].

Figure 5 illustrates blockwalking in 5 dimensions:

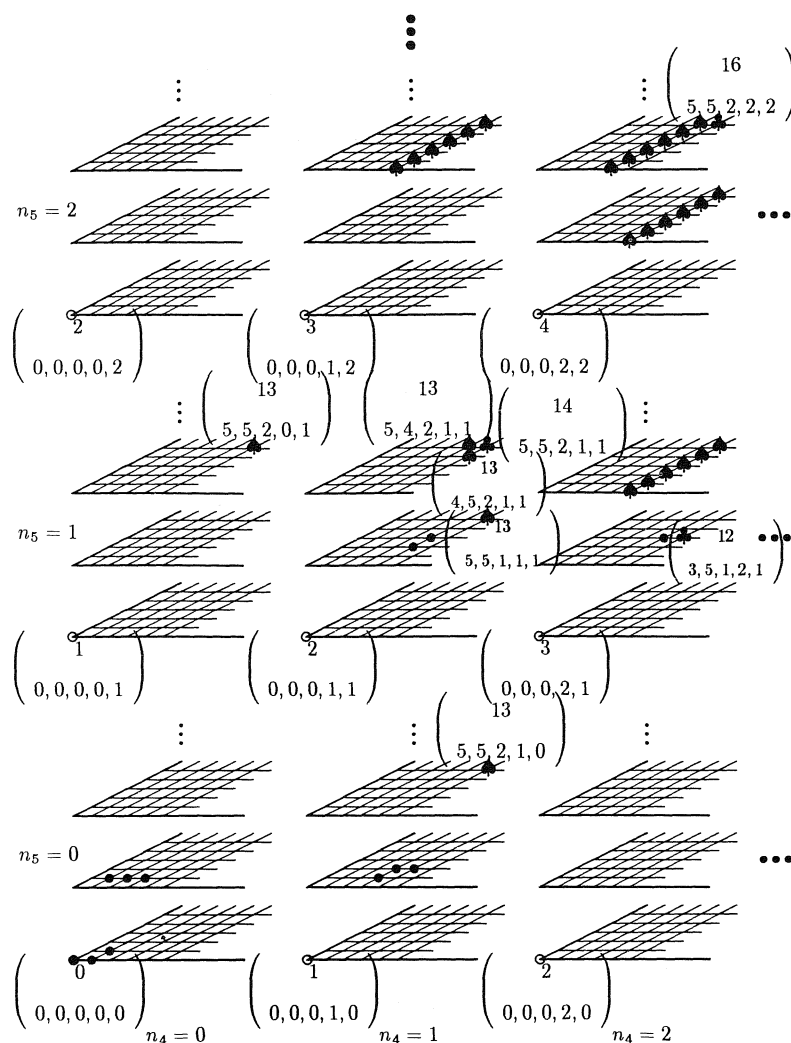


FIGURE 5. Blockwalking in 5 dimensions

Here, each tier represents a 2-dimensional blockwalk; tiers stacked on top of each other represent the 3<sup>rd</sup> dimension; the 4<sup>th</sup> dimension is represented by a row of 3-dimensional tiers going from left to right; the 5<sup>th</sup> dimension is represented by copies of the 4-dimensional rows stacked one above another. In 5 dimensions, we consider combinations of  $L$ 's,  $R$ 's,  $U$ 's,  $H$ 's

(hyperspaces), and  $W$ 's (warps). The path  $RLURRHLRWLHR$  is illustrated by circles in Figure 5. This path starts at the origin and ends at

$$\begin{pmatrix} 12 \\ 3, 5, 1, 2, 1 \end{pmatrix}.$$

The recurrence relation (1) for Pascal's triangle generalizes for hyperpyramids:

$$\begin{pmatrix} n \\ n_1, n_2, \dots, n_j \end{pmatrix} = \sum_{k=1}^j \begin{pmatrix} n-1 \\ n_1, \dots, n_k-1, \dots, n_j \end{pmatrix}.$$

The blockwalking argument also generalizes. That is, partition the paths depending on what the last step is. For example, in Figure 5, the club at

$$\begin{pmatrix} 14 \\ 5, 5, 2, 1, 1 \end{pmatrix}$$

has a sieve of five spades—each of which is one step away in one of five dimensions.

This brings us to the *Multinomial Hockey Stick Identity*:

$$\begin{pmatrix} n \\ n_1, n_2, \dots, n_j \end{pmatrix} = \sum_{k=2}^j \sum_{i=n_2}^{n_1+n_2} \begin{pmatrix} i+n_3+n_4+\dots+n_j-1 \\ i-n_2, n_2, n_3, \dots, n_k-1, \dots, n_j \end{pmatrix}.$$

The sieve for this identity has  $j-1$  copies of the sieve for the standard Hockey Stick Identity. This is illustrated in Figure 5 (with  $j=5$ ) by the four rows of spades that form a sieve for the club at

$$\begin{pmatrix} 16 \\ 5, 5, 2, 2, 2 \end{pmatrix}.$$

#### 4. COMMENTS

The beauty of Pólya's blockwalking is that it provides a geometric interpretation of algebraic equations and, in so doing, gives a way of visualizing the concepts involved. The attempt here has been to utilize this idea to provide geometric and visual aids for more complex equations and higher dimensions. In developing the presentation of this visualization, the author conceived of the 2-dimensional representation of 5 dimensions shown in Figure 5. Although the 4-dimensional tesseract is often drawn in 2 dimensions, the author has never seen an attempt to represent 5 dimensions on a flat surface. The final comments consider how the representation in Figure 5 can be generalized to more dimensions.

The basic concept is to represent the  $n^{\text{th}}$  dimension by making copies of the  $(n-1)^{\text{st}}$  dimension. Thus, to visualize the 6<sup>th</sup> dimension, we make copies of Figure 5, say, by stacking pages on top of each other. Notice that this gives us a 3-dimensional array of 3-dimensional arrays. We can visualize further dimensions by considering larger and larger 3-dimensional arrays. For example, we can consider our 6-dimensional stack of pages as a ream of paper. Obtain the next 3 dimensions by considering a 3-dimensional array of reams. Continuing in this fashion, call the

array of reams a box; consider a 3-dimensional array of boxes, call this a pallet; consider a 3-dimensional array of pallets; etc. The structure just described, up through a 3-dimensional array of pallets, represents a 15-dimensional nonnegative lattice. The limiting factor in this method is our ability to establish a mnemonically reasonable ordering of containers to describe each level of 3-dimensional arrays. This approach can be compared to a Mandelbrot set in that we are maintaining the same visual picture only at larger and larger scales.

The visualization just described is aided by the discrete nature of the lattice (i.e., the blocks of the blockwalking) and by restricting the picture to the nonnegative "hyperquadrant" of the lattice. In order to eliminate the discrete nature of our picture, instead of making discrete copies of the  $(n-1)$ -dimensional representation, move the  $(n-1)$ -dimensional representation in a continuous motion. To remove the restriction of only visualizing the nonnegative hyperquadrant of  $n$ -space, consider  $2^n$  copies of the hyperquadrant to represent the  $2^n$  hyperquadrants that exist in  $n$ -space.

### REFERENCES

1. W. N. Bailey. *Generalized Hypergeometric Series*. Cambridge: Cambridge University Press, 1935.
2. B. A. Bondarenko. *Generalized Pascal Triangles and Pascal Pyramids: Their Fractals, Graphs, and Applications*. Trans. R. Bollinger. Originally published in Russian, 1990; rpt. Santa Clara, Calif.: The Fibonacci Association, 1993.
3. A. Edwards. *Pascal's Arithmetical Triangle*. Oxford: Oxford University Press, 1987.
4. H. W. Gould. *Combinatorial Identities*. Morgantown: Morgantown Printing and Binding Co., 1972.
5. B. Jackson & D. Thoro. *Applied Combinatorics with Problem Solving*. New York: Addison-Wesley, 1990.
6. J. F. Lucas. "Paths and Pascal Numbers." *College Math. J.* **14** (1983):329-41.
7. B. Pascal. *Traité du triangle arithmétique*. Paris: Desprez, 1665.
8. G. Pólya. *Mathematical Discovery: On Understanding, Learning, and Teaching Problem Solving*. Vol. I. New York: John Wiley & Sons, 1962.
9. G. Pólya, R. E. Tarjan, & D. R. Woods. *Notes on Introductory Combinatorics*. Vol. 4 of *Progress in Computer Science*. Boston: Birkhäuser, 1983.
10. J. F. Putz. "The Pascal Polytope: An Extension of Pascal's Triangle to  $n$  Dimensions." *College Math. J.* **17.2** (1986):133-55.
11. J. F. Putz. "Pascal Polytopes." Ph.D. dissertation, St. Louis University, 1981.
12. J. Riordan. *Combinatorial Identities*. Huntington, New York: Robert E. Krieger Publishing Co. (rpt with corrections ed.), 1979.
13. A. Tucker. *Applied Combinatorics*, 2nd ed. New York: John Wiley & Sons, 1984.
14. H. S. Wilf. *Generatingfunctionology*. New York: Academic Press, 1990.

AMS Classification Numbers: 05A19, 05A10, 11B65



## SUSTAINING MEMBERS

*H.L. Alder	L.A.G. Dresel	R.E. Kennedy	A.G. Shannon
G.L. Alexanderson	U. Dudley	C.H. Kimberling	L.W. Shapiro
P. G. Anderson	M. Faccio	Y.H.H. Kwong	J.R. Siler
S. Ando	D.R. Farmer	J. Lahr	L. Somer
R. Andre-Jeannin	D.C. Fielder	B. Landman	P. Spears
*J. Arkin	P. Filippini	L.H. Lange	W.R. Spickerman
C. Ashbacher	C.P. Flynn	*C.T. Long	Paul K. Stockmeyer
M.K. Azarian	Fondazione Ugo Bordon	G. Lord	J. Suck
N. Balasubramania	Anthony Gioia	*J. Maxwell	M.N.S. Swamy
J.G. Bergart	M.F. Goode	F.U. Mendizabal	*D. Thoro
G. Bergum	*H.W. Gould	J.L. Miller	J.C. Turner
G. Berzsenyi	P. Hags, Jr.	M.G. Monzingo	T.P. Vaughan
*M. Bicknell-Johnson	H. Harborth	J.F. Morrison	J.N. Vitale
P.S. Bruckman	P. Haukkanen	S.A. Obaid	M. Waddill
M.F. Bryn	*A.P. Hillman	S. Palsson	J.E. Walton
G.D. Chakerian	*A.F. Horadam	J. Pla	W.A. Webb
C. Chouteau	Y. Horibe	A. Prince	G.E. Weekly
C.K. Cook	F.T. Howard	S. Rabinowitz	D.L. Wells
M.J. DeBruin	R.J. Howell	I. Sadoveanu	R.E. Whitney
M.J. DeLeon	J.P. Jones	S. Sato	B.E. Williams
J. De Kerf		J.A. Schumaker	* Charter Members

## INSTITUTIONAL MEMBERS

CALIFORNIA STATE UNIVERSITY  
SACRAMENTO  
*Sacramento, California*

ETH-BIBLIOTHEK  
*Zurich, Switzerland*

CHALMERS UNIVERSITY OF TECHNOLOGY  
AND UNIVERSITY OF GÖTEBORG  
*Göteborg, Sweden*

GONZAGA UNIVERSITY  
*Spokane, Washington*

HOWELL ENGINEERING COMPANY  
*Bryn Mawr, California*

INDIANA UNIVERSITY  
*Bloomington, Indiana*

KLEPCO, INC.  
*Sparks, Nevada*

KØBENHAVNS UNIVERSITY  
Matematisk Institut  
*Copenhagen, Denmark*

LAURENTIAN UNIVERSITY  
*Sudbury, Ontario, Canada*

MATHEMATISCHES FORSCHUNGS INSTITUT  
*Lorenzenhof, Germany*

MISSOURI SOUTHERN STATE COLLEGE  
*Joplin, Missouri*

NATIONAL LIBRARY OF EDUCATION  
*Copenhagen, Denmark*

SAN JOSE STATE UNIVERSITY  
*San Jose, California*

SANTA CLARA UNIVERSITY  
*Santa Clara, California*

UNIVERSITY OF NEW ENGLAND  
*Armidale, N.S.W. Australia*

UNIVERSITY OF TECHNOLOGY  
*Sydney, N.S.W. Australia*

WAKE FOREST UNIVERSITY  
*Winston-Salem, North Carolina*

WASHINGTON STATE UNIVERSITY  
*Pullman, Washington*

YESHIVA UNIVERSITY  
*New York, New York*

## **BOOKS AVAILABLE THROUGH THE FIBONACCI ASSOCIATION**

*Introduction to Fibonacci Discovery* by Brother Alfred Brousseau, Fibonacci Association (FA), 1965.

*Fibonacci and Lucas Numbers* by Verner E. Hoggatt, Jr. FA, 1972.

*A Primer for the Fibonacci Numbers.* Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1972.

*Fibonacci's Problem Book,* Edited by Marjorie Bicknell and Verner E. Hoggatt, Jr. FA, 1974.

*The Theory of Simply Periodic Numerical Functions* by Edouard Lucas. Translated from the French by Sidney Kravitz. Edited by Douglas Lind. FA, 1969.

*Linear Recursion and Fibonacci Sequences* by Brother Alfred Brousseau. FA, 1971.

*Fibonacci and Related Number Theoretic Tables.* Edited by Brother Alfred Brousseau. FA, 1972

*Number Theory Tables.* Edited by Brother Alfred Brousseau. FA, 1973.

*Tables of Fibonacci Entry Points, Part One.* Edited and annotated by Brother Alfred Brousseau. FA, 1965

*Tables of Fibonacci Entry Points, Part Two.* Edited and annotated by Brother Alfred Brousseau. FA, 1965

*A Collection of Manuscripts Related to the Fibonacci Sequence—18th Anniversary Volume.* Edited by Verner E. Hoggatt, Jr. and Marjorie Bicknell-Johnson. FA, 1980.

*Applications of Fibonacci Numbers, Volumes 1-6.* Edited by G.E. Bergum, A.F. Horadam and A.N. Philippou

*Generalized Pascal Triangles and Pyramids Their Fractals, Graphs and Applications* by Boris A. Bondarenko. Translated from the Russian and edited by Richard C. Bollinger. FA, 1993.

*Fibonacci Entry Points and Periods for Primes 100,003 through 415,993* by Daniel C. Fielder and Paul S. Bruckman.

**Please write to the Fibonacci Association, Santa Clara University, Santa Clara, CA 95053, U.S.A., for more information and current prices.**