The Fibonacci Quarterly

THE OFFICIAL JOURNAL OF
THE FIBONACCI ASSOCIATION

VOLUME 17 **NUMBER 1**

CONTENTS

FEBRUARY **1979**

The Fibonacci Quarterly

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

All subscription correspondence should be addressed to Prof. Leonard Klosinski, Mathematics Department, University of Santa Clara, Santa Clara, California 95053. All checks ($15.00 per year) should be made out to the Fibonacci Association or Fibonacci Quarterly. Two copies of manuscripts intended for publication in the *Quarterly* should be sent to Verner E. Hoggatt, Jr., Mathematics Department, San Jose State University, San Jose, California 95192. *All manuscripts should be typed, double-spaced. Drawings should be made the same size as they will appear in the Quarterly, and should be drawn in India ink on either vellum or bond paper. Authors should keep a copy of the manuscripts sent to the editors.*

The *Quarterly* is entered as 3rd-class mail at the University of Santa Clara Post Office, Calif., as an official publication of The Fibonacci Association.

The Fibonacci Quarterly is published in February, April, October, and December each year.

PYTHAGOREAN TRIPLES CONTAINING FIBONACCI NUMBERS: SOLUTIONS FOR $F_n^2 \pm F_k^2 = K^2$

MARJORIE BICKNELL-JOHNSON
A.C. Wilcox High School, Santa Clara, CA 95051

1. INTRODUCTION

When can Fibonacci numbers appear as members of a Pythagorean triple? It has been proved by Hoggatt [1] that three distinct Fibonacci numbers cannot be the lengths of the sides of any triangle. L. Carlitz [8] has shown that neither three Fibonacci numbers nor three Lucas numbers can occur in a Pythagorean triple. Obviously, one Fibonacci number could appear as a member of a Pythagorean triple, because any integer could so appear, but $F_{3(2m+1)}$ cannot occur in a primitive triple, since it contains a single factor of 2. However, it appears that two Fibonacci lengths can occur in a Pythagorean triple only in the two cases 3 - 4 - 5 and 5 - 12 - 13, two Pell numbers only in 5 - 12 - 13, and two Lucas numbers only in 3 - 4 - 5. Further, it is strongly suspected that two members of any other sequence formed by evaluating the Fibonacci polynomials do not appear in a Pythagorean triple.

Here, we define the Fibonacci polynomials $\{F_n(x)\}$ by

$$F_0(x) = 0, \quad F_1(x) = 1, \quad F_{n+1}(x) = xF_n(x) + F_{n-1}(x), \tag{1.1}$$

and the Lucas polynomials $\{L_n(x)\}$ by

$$L_n(x) = F_{n+1}(x) + F_{n-1}(x) \tag{1.2}$$

and form the sequences $\{F_n(a)\}$ by evaluating $\{F_n(x)\}$ at $x = a$. The Fibonacci numbers are $F_n = F_n(1)$, the Lucas numbers $L_n = L_n(1)$, and the Pell numbers $P_n = F_n(2)$.

While it would appear that $F_n(a)$ and $F_k(a)$ cannot appear in the same Pythagorean triple (except for 3 - 4 - 5 and 5 - 12 - 13), we will restrict our proofs to primitive triples, using the well-known formulas for the legs a and b and hypotenuse c,

$$a = 2mn, \quad b = m^2 - n^2, \quad c = m^2 + n^2, \tag{1.3}$$

where $(m,n) = 1$, m and n not both odd, $m > n$. We next list Pythagorean triples containing Fibonacci, Lucas, and Pell numbers. The preparation of the tables was elementary; simply set $F_k = a$, $F_k = b$, $F_k = c$ for successive values of k and evaluate all possible solutions.

Table 1

PYTHAGOREAN TRIPLES CONTAINING F_k, $1 \leq k \leq 18$

m	n	$2mn$	$m^2 - n^2$	$m^2 + n^2$	
2	1	4	$3 = F_4$	$5 = F_5$	
3	2	12	$5 = F_5$	$13 = F_7$	
3	1	6	$8 = F_6$	10	(not primitive)
4	1	$8 = F_6$	15	17	
7	6	84	$13 = F_7$	85	
5	2	20	$21 = F_8$	29	
11	10	220	$21 = F_8$	221	
5	3	30	16	$34 = F_9$	(not primitive)
17	1	$34 = F_9$	288	290	(not primitive)
8	3	48	$55 = F_{10}$	73	
28	27	1512	$55 = F_{10}$	1513	
8	5	80	39	$89 = F_{11}$	
45	44	3960	$F_{11} = 89$	3961	
37	35	2590	$144 = F_{12}$	2594	(not primitive)
20	16	640	$144 = F_{12}$	656	(not primitive)
15	9	270	$144 = F_{12}$	306	(not primitive)
13	5	130	$144 = F_{12}$	194	(not primitive)
9	8	$144 = F_{12}$	17	145	
72	1	$144 = F_{12}$	5183	5185	
36	2	$144 = F_{12}$	1292	1300	(not primitive)
24	3	F_{12}	567	585	(not primitive)
18	4	F_{12}	308	340	(not primitive)
12	6	F_{12}	108	180	(not primitive)
13	8	208	105	$233 = F_{13}$	
117	116	27144	$233 = F_{13}$	27145	
16	11	352	135	$377 = F_{14}$	
19	4	152	345	$377 = F_{14}$	
189	188	71064	$377 = F_{14}$	71065	
21	8	336	$377 = F_{14}$	505	
21	13	546	272	$610 = F_{15}$	(not primitive)
23	9	414	448	$610 = F_{15}$	(not primitive)
305	1	$610 = F_{15}$	93024	93026	(not primitive)
61	5	$610 = F_{15}$	3696	3746	(not primitive)
494	493	487084	$987 = F_{16}$	487085	
166	163	54116	$987 = F_{16}$	54125	
34	13	884	$987 = F_{16}$	1325	
74	67	9916	$987 = F_{16}$	9965	
34	21	1428	715	$1597 = F_{17}$	
799	798	1275204	$1597 = F_{17}$	1275205	
647	645	834630	$2584 = F_{18}$	834634	(not primitive)
325	321	208650	$2584 = F_{18}$	208666	(not primitive)
53	15	1590	$2584 = F_{18}$	3034	(not primitive)
55	21	2310	$2584 = F_{18}$	3466	(not primitive)
1292	1	$2584 = F_{18}$	1669263	1669265	
646	2	$2584 = F_{18}$	417312	417320	(not primitive)
323	4	$2584 = F_{18}$	104313	104345	

Table 1 (continued)

m	n	$2mn$	$m^2 - n^2$	$m^2 + n^2$	
76	17	$2584 = F_{18}$	5487	6065	
68	19	$2584 = F_{18}$	4263	4985	
38	34	$2584 = F_{18}$	288	2600	(not primitive)
F_{n+1}	F_n	$2F_nF_{n+1}$	$F_{n-1}F_{n+2}$	F_{2n+1}	
		$2F_k$	$F_k^2 - 1$	$F_k^2 + 1$	
		F_{6m}	$(F_{6m}^2 - 4)/4$	$(F_{6m}^2 + 4)/4$	
		$(F_{3m\pm1}^2 - 1)/2$	$F_{3m\pm1}$	$(F_{3m\pm1}^2 + 1)/2$	
F_{k+1}	F_{k-1}	$2F_{k+1}F_{k-1}$	F_{2k}	$F_k^2 + 2F_{k-1}F_{k+1}$	

Table 2

PYTHAGOREAN TRIPLES CONTAINING L_k, $1 \leq k \leq 18$

m	n	$2mn$	$m^2 - n^2$	$m^2 + n^2$	
2	1	$4 = L_3$	$3 = L_2$	5	
4	3	24	$7 = L_4$	25	
6	5	60	$11 = L_5$	61	
9	1	$18 = L_6$	80	82	(not primitive)
5	2	20	21	$29 = L_7$	
15	14	420	$29 = L_7$	421	
24	23	1104	$47 = L_8$	1105	
20	18	720	$76 = L_9$	724	(not primitive)
19	2	$76 = L_9$	357	365	
38	1	$76 = L_9$	1443	1445	
62	61	7564	$123 = L_{10}$	7565	
22	19	836	$123 = L_{10}$	845	
100	99	19800	$199 = L_{11}$	19801	
23	7	$322 = L_{12}$	480	578	(not primitive)
161	1	$322 = L_{12}$	25920	25922	(not primitive)
20	11	440	279	$521 = L_{13}$	
261	260	135720	$521 = L_{13}$	135721	
422	421	355324	$843 = L_{14}$	355325	
142	139	39476	$843 = L_{14}$	39485	
42	20	1680	$1364 = L_{15}$	2164	(not primitive)
342	340	232560	$1364 = L_{15}$	232564	(not primitive)
682	1	$1364 = L_{15}$	465123	465125	
341	2	$1364 = L_{15}$	116277	116285	
62	11	$1364 = L_{15}$	3723	3985	
31	22	$1364 = L_{15}$	471	1445	
1104	1103	2435424	$2207 = L_{16}$	2435425	
1786	1785	637020	$3571 = L_{17}$	6376021	
2889	1	$5778 = L_{18}$	8346320	8346322	(not primitive)

Table 2 (continued)

m	n	$2mn$	$m^2 - n^2$	$m^2 + n^2$	
963	3	$5778 = L_{18}$	927360	927378	(not primitive)
321	9	$5778 = L_{18}$	102960	103122	(not primitive)
107	27	$5778 = L_{18}$	10720	12178	(not primitive)

Table 3

PYTHAGOREAN TRIPLES CONTAINING PELL NUMBERS P_k, $1 \leq k \leq 8$

m	n	$2mn$	$m^2 - n^2$	$m^2 + n^2$	
2	1	4	3	$5 = P_3$	
3	2	$12 = P_4$	$5 = P_3$	13	
6	1	$12 = P_4$	35	37	
5	2	20	21	$29 = P_5$	
15	14	420	$29 = P_5$	421	
35	1	$70 = P_6$	1224	1226	(not primitive)
7	5	$70 = P_6$	24	74	(not primitive)
12	5	120	119	$169 = P_7$	
85	84	14280	$169 = P_7$	14281	
103	101	20806	$408 = P_8$	20810	(not primitive)
53	49	5194	$408 = P_8$	5210	(not primitive)
204	1	$408 = P_8$	41615	41617	
102	2	$408 = P_8$	10400	10408	(not primitive)
51	4	$408 = P_8$	2585	2617	
68	3	$408 = P_8$	4615	4633	
34	6	$408 = P_8$	1120	1192	(not primitive)
17	12	$408 = P_8$	145	433	
P_{n+1}	P_n	$2P_nP_{n+1}$	$P_{n-1}P_{n+2}$	P_{2n+1}	

We note that in 3-4-5 and 5-12-13, the hypotenuse is a prime Fibonacci number, and one leg and the hypotenuse are Fibonacci lengths. These are the only solutions with two Fibonacci lengths where a prime Fibonacci number gives the length of the hypotenuse. If F_p is prime, then p is odd, because $F_w \mid F_{2w}$. If F_p is a prime of the form $4k - 1$, then there are no solutions to $m^2 + n^2 = F_p$, and if F_p is a prime of the form $4k + 1$, then $m^2 + n^2$ has exactly one solution: $m = F_{k+1}$, $n = F_k$, or, the triple

$$a = 2F_kF_{k+1}, \quad b = F_{k-1}F_{k+2}, \quad c = F_{2k+1} \quad \text{(see [2]).}$$

In either case, F_{2k+1} does not appear as the hypotenuse in a triple containing two Fibonacci numbers if F_{2k+1} is prime. These remarks also hold for the generalized Fibonacci numbers $\{F_n(a)\}$.

Also note that some triples contain numbers from more than one sequence. We have, in 3-4-5, F_4-L_3-F_5, or L_2-L_3-F_5, or F_4-L_3-P_3, while 5-12-13 has F_5-P_4-F_7, or P_3-P_4-F_7, and 20-21-29 has F_8 and L_7 or F_8 and P_5. There also are a few "near misses," which are close enough to being Pythagorean triples to fool the eye if a triangle were constructed: 55 - 70 - 89, 21 - 34 - 40, and 8 - 33 - 34. However, 3 - 4 - 5 and 5 - 12 - 13 seem to be the only Pythagorean triples which contain two members from the same sequence.

Lastly, note that numbers of the form $4m + 2$ cannot be used as members of a primitive triple, since one leg is always divisible by four, so that Fibonacci numbers of the form F_{6k+3} are excluded from primitive Pythagorean triples.

2. SQUARES AMONGST THE GENERALIZED FIBONACCI NUMBERS $\{F_n(a)\}$

Squares are very sparse amongst the sequences $\{F_n(a)\}$, beyond $F_0(a) = 0$ and $F_1(a) = 1$. In the Fibonacci sequence, the only squares are 0, 1, and 144 [3]; in the lucas sequence, 1 and 4; and in the Pell sequence, 0, 1, and 169. There are no small squares other than 0 and 1 in $\{F_n(a)\}$, $3 \leq a \leq 10$; it is unknown whether other squares exist in $\{F_n(a)\}$, except when $a = k^2$, of course.

Cohn [3] has proved the first two theorems below, which we shall need later.

Theorem 2.1: If $L_n = x^2$, then $n = 1$ or 3.
If $L_n = 2x^2$, then $n = 0$ or $n = \pm 6$.

Theorem 2.2: If $F_n = x^2$, then $n = 0, \pm 1, 2$, or 12.
If $F_n = 2x^2$, then $n = 0, \pm 3$, or 6.

We shall need the following lemma:

Lemma 2.1: For the Fibonacci and Lucas polynomials,

$$F_{m+2k}(x) = L_k(x)F_{m+k}(x) + (-1)^{k+1}F_m(x).$$

Proof: Lemma 2.1 appears in [4] with only a change in notation.

We will use Lemma 2.1 with $x = 2$, so that $F_n(2) = P_n$ and $L_n(2) = R_n$, the Pell numbers and their related sequence.

Conjecture 2.3: If $P_n = x^2$, $n = 0, \pm 1$, or ± 7.

Partial Proof: Let $R_k = P_{k-1} + P_{k+1}$ so that $R_k = L_k(2)$. Then

$$R_{2m} = 8P_m^2 + (-1)^m \cdot 2, \text{ or, } R_{2m} \equiv \pm 2 \pmod 8 \text{ so that } R_{2m} \neq K^2.$$

$$\begin{aligned} R_{2k+1} &= P_{2k} + P_{2k+2} = P_{2k} + 2P_{2k+1} + P_{2k} \\ &= 2(P_{2k+1} + P_{2k}) = 2(2M + 1) \end{aligned}$$

since $2 | P_n$ if and only if $2 | n$. Thus, $R_{2k+1} \neq K^2$ and $R_n \neq K^2$ for any n.

Suppose n is even. Since $P_{2k} = P_k R_k$, if $n = 4p + 2$, then

$$P_n = P_{2p+1}R_{2p+1} \text{ where } (P_{2p+1}, R_{2p+1}) = 1.$$

Then $P_n = K^2$ if and only if $R_{2p+1} = x^2$ *and* $P_{2p+1} = y^2$, but $R_{2p+1} \neq x^2$, so $P_n \neq K^2$. If $n = 4p$, then

$$P_n = P_{2p}R_{2p} \text{ where } (P_{2p}, R_{2p}) = 2,$$

so $P_n = K^2$ if $P_{2p} = 2x^2$ and $R_{2p} = 2y^2$, but since $R_{2p} = 8P_p^2 \pm 2 = 2(X^2 \pm 1)$, $R_{2p} = 2y^2$ only for $p = 0$, giving P_0 as the only solution. Thus, $P_n \neq K^2$ for n even, unless $n = 0$.

Since $P_{m+8} \equiv P_m \pmod 8$ and $P_{8m\pm 1} \equiv 1 \pmod 8$ and $P_{8m\pm 3} \equiv 5 \pmod 8$, since all odd squares are congruent to 1 (mod 8), if n is odd, $n = 8m \pm 1$ if $P_n = K^2$. Of course, $P_n = k^2$ for $n = \pm 1, \pm 7$. The conjecture is not resolved.

Conjecture 2.4: If $P_n = 5k^2$, then $n = 0$ or $n = \pm 3$.

Partial Proof: If $P_n = 5k^2$, then $P_n \equiv 5 \cdot 0 \equiv 0 \pmod 8$, or $P_n \equiv 5 \cdot 1 \equiv 5 \pmod 8$, or $P_n \equiv 5 \cdot 4 \equiv 4 \pmod 8$, so that $n = 8m$, $8m+4$, $8m+3$, or $8m+5$, since $P_{8m} \equiv 0 \pmod 8$, $P_{8m+4} \equiv 4 \pmod 8$, and $P_{8m\pm 3} \equiv 5 \pmod 8$.

If n is even, then $n = 4k$, and $P_n = P_{4k} = P_{2k}R_{2k}$ where $(P_{2k}, R_{2k}) = 2$ and $R_{2k} \neq x^2$, $R_{2k} \neq 2x^2$, and $R_{2k} \neq 5x^2$ since $5 \nmid R_{2k}$. We have $P_{4k} \neq K^2$ unless $k = 0$, or, $P_n \neq K^2$ when n is even, unless $n = 0$.

If n is odd, then $n = 8m \pm 3$. Now, $n = \pm 3$ gives a solution. If $n \neq \pm 3$, then $n = 8m \pm 3 = 2 \cdot 4w \pm 3$, and since $P_{-3} = P_3 = 5$, both of these give $P_n = -P_3 \pmod{R_{4w}} = -5 \pmod{R_{4w}}$ by way of Lemma 2.1 and

$$P_{m+2k} = R_k P_{m+k} + (-1)^{k+1} P_m \tag{2.1}$$

where $m = \pm 3$ and $k = 4w$. Now, if w is odd, then R_4 divides R_{4w}, and we can write, from (2.1),

$$P_{2\cdot 4w \pm 3} = R_4 \cdot K \cdot P_{4w\pm 3} - P_{\pm 3}$$

so that, since $R_4 = 34$, $P_n \equiv -5 \pmod{34}$, where -5 is not a quadratic residue of 34. It is strongly suspected that -5 is not a quadratic residue of R_{4w}, but the conjecture is not established if w is even.

Theorem 2.5: If $F_n = 5x^2$, then $n = 0$ or $n = \pm 5$.

Proof: If n is even, $F_n = F_{2k} = F_k L_k = 5x^2$ if $F_k = 5x^2$ and $L_k = y^2$, or $F_k = x^2$ and $L_k = 5k^2$ (impossible), which has solutions for $k = 0$ only.

If n is odd, then $n \equiv 3 \pmod 4$ or $n \equiv 1 \pmod 4$. If $n \equiv 3 \pmod 4$, then write $n = 3 + 4M = 3 + 2 \cdot 3^n \cdot k$, where $2|k$, $3\nmid k$, and

$$5F_n \equiv -5F_3 \equiv -10 \pmod{L_k},$$

but $L_k \equiv 3 \pmod 4$ if $2|k$, $3\nmid k$, so -10 is not a quadratic residue, and

$$5F_n \neq k^2 \text{ so } F_n \neq 5k^2.$$

If $n \equiv 1 \pmod 4$, $n = 5$ is a solution. If $n \neq 5$

$$n = 1 + 4M = 1 + 2 \cdot 3^r \cdot k,$$

where $2|k$, $3\nmid k$, and

$$5F_n \equiv -5F_1 \equiv -5 \pmod{L_k},$$

but -5 is not a quadratic residue, and

$$5F_n \neq k^2 \text{ so } F_n \neq 5K^2 \text{ when } n \text{ is odd, unless } n = 5.$$

Since $F_{-n} = (-1)^{n+1}F_n$, $n = -5$ is also a solution. Thus, $F_n \neq 5x^2$ unless $n = 0, \pm 5$.

We will find another relationship between squares of the generalized Fibonacci numbers useful.

Theorem 2.6:

$$F_n^2(x) = (-1)^{n+k}F_k^2(x) + F_{n-k}(x)F_{n+k}(x).$$

Proof: For simplicity, we will prove Theorem 2.6 for Fibonacci numbers, or for $x = 1$, noting that every identity used is also an identity for the Fibonacci polynomials [4]. In particular, we use

(2.2) $$(-1)^{n+1}F_n(x) = F_{-n}(x)$$

(2.3) $$F_{p+r}(x) = F_{p-1}(x)F_r(x) + F_p(x)F_{r+1}(x)$$

(2.4) $$F_n^2(x) = (-1)^{n+1} + F_{n-1}(x)F_{n+1}(x)$$

(2.5) $$F_{n+1}^2(x) + F_n^2(x) = F_{2n+1}(x)$$

Proof is by mathematical induction. Theorem 2.6 is true for $k = 1$ by (2.4) Set down the theorem statement as $P(k)$ and $P(k + 1)$:

$$P(k):\quad F_n^2 = (-1)^{n+k}F_k^2 + F_{n-k}F_{n+k}$$

$$P(k+1):\quad F_n^2 = (-1)^{n+k+1}F_{k+1}^2 + F_{n-k-1}F_{n+k+1}$$

Equating $P(k)$ and $P(k + 1)$,

$$\begin{aligned}(-1)^{n+k+1}\left(F_{k+1}^2 + F_k^2\right) &= F_{n-k}F_{n+k} + F_{n-k-1}F_{n+k+1}\\ &= (-1)^{k-n+1}F_{k-n}F_{n+k} + (-1)^{k-n+1}F_{k+1-n}F_{n+k+1}\end{aligned}$$

by (2.2). By (2.5) and (2.3), the left-hand and right-hand members become

$$(-1)^{n+k+1}F_{2k+1} = (-1)^{k-n+1}F_{2k+1}.$$

Since all the steps reverse,

$$(-1)^{n+k+1}F_{k+1}^2 + F_{n-k-1}F_{n+k+1} = (-1)^{n+k}F_k^2 + F_{n-k}F_{n+k} = F_n^2$$

so that $P(k + 1)$ is true whenever $P(k)$ is true. Thus, Theorem 2.6 holds for all positive integers n.

3. SOLUTIONS FOR $F_n^2(a) + F_n^2(a) = K^2$

By Theorem 2.6, when n and k have opposite parity,

(3.1) $$F_n^2(a) + F_k^2(a) = F_{n-k}(a)F_{n+k}(a).$$

Since $\left(F_n(a), F_k(a)\right) = 1 = F_{(n,k)}(a)$ by the results of [5], $(n,k) = 1$ and opposite parity for n and k means that $(n - k, n + k) = 1$ so that

$$\left(F_{n-k}(a), F_{n+k}(a)\right) = 1.$$

Thus, $F_{n-k}(a)F_{n+k}(a) = K^2$ if and only if both $F_{n-k}(a) = x^2$ and $F_{n+k}(a) = y^2$. We would expect a very limited number of solutions, then, since squares are scarce amongst $\{F_n(a)\}$.

Since one leg is divisible by 4 in a Pythagorean triple, one of n or k is a multiple of 6 if a is odd, and a multiple of 2 if a is even; thus, n and k cannot both be odd. Also, n and k cannot both be even, since $F_2(a)$ is a factor of $F_{2m}(a)$ and $F_2(a) > 1$ for all sequences except $F_n(1) = F_n$.

Restated,

Theorem 3.1: Any solution to $F_n^2(a) + F_k^2(a) = K^2$ in positive integers, $a \geq 2$, occurs only for such values of n and k that $F_{n-k}(a) = x^2$ *and* $F_{n+k}(a) = y^2$.

Conjecture 3.2: $F_n^2(2) + F_k^2(2) = K^2$, $n > k > 0$, where $F_n(2) = P_n$, the nth Pell number, has the unique solution $n = 4$, $k = 3$, giving 5 - 12 - 13.

Proof: Apply Theorems 3.1 and Conjecture 2.3.

Theorem 3.3: If $F_n^2 + F_k^2 = K^2$, $n > k > 0$, then both n and k are even.

Proof: Apply Theorems 3.1 and 2.2.

Theorem 3.4: If $F_n^2 + F_k^2 = K^2$, $n > k > 0$, then $F_{10} = 55$, $F_8 = 21$, $F_{18} = 2584$, $F_6 = 8$, and $F_4 = 3$ each divide either F_n or F_k, and 13 is the smallest prime factor possible for K.

Proof: Since 3 divides one leg of a Pythagorean triple, F_4 divides F_k or F_n. Since 4 divides one leg of a Pythagorean triple, and the smallest F_n divisible by 4 is F_6, F_6 divides F_k or F_n. That F_{10} divides either F_n or F_k follows by examining the quadratic residues of 11. The quadratic residues of 11 are 1, 3, 4, 5, and 9. It is not difficult to calculate

$$F_{10w}^2 \equiv 0 \pmod{11}$$
$$F_{10w\pm 2}^2 \equiv 1 \pmod{11}$$
$$F_{10w\pm 4}^2 \equiv 9 \pmod{11}$$

where we need only consider even subscripts by Theorem 3.3. Notice that $F_{10w}^2 + F_{10w\pm 2}^2 \equiv 1 \pmod{11}$ and $F_{10w}^2 + F_{10w\pm 4}^2 \equiv 9 \pmod{11}$, where 1 and 9 are quadratic residues of 11, so that these are possible squares, but $F_{10w\pm 2}^2 + F_{10w\pm 4}^2 \equiv 10 \pmod{11}$, where 10 is not a residue. $F_{10w\pm 2}^2 + F_{10w\pm 2}^2$ produces the nonresidue 2, and similarly $F_{10w\pm 4}^2 + F_{10w\pm 4}^2 \equiv 7 \pmod{11}$, so that either $F_n = F_{10w}$ or $F_k = F_{10w}$. In either case, F_{10} divides one of F_n or F_k.

Similarly, we examine the quadratic residues of 7, which are 0, 1, 2, and 4. We find

$$F_{8m}^2 \equiv 0 \pmod{7}$$
$$F_{8m\pm 2}^2 \equiv 1 \pmod{7}$$
$$F_{8m\pm 4}^2 \equiv 2 \pmod{7}$$

where $F_{8m}^2 + F_{8m\pm 2}^2 \equiv 1 \pmod{7}$ and $F_{8m}^2 + F_{8m\pm 4}^2 \equiv 2 \pmod{7}$ are possible squares but $F_{8m\pm 2}^2 + F_{8m\pm 4}^2 \equiv 3 \pmod{7}$ is not a possible square. But, F_{8m}^2 and $F_{8m\pm 4}^2$, or F_{8m}^2 and $F_{8m^*}^2$, or $F_{8m\pm 4}^2$ and $F_{8m^*\pm 4}^2$, cannot occur in the same primitive triple, since they have common factor F_4. $F_{8m\pm 2}^2$ and $F_{8m^*\pm 2}^2$ cannot be in the same triple, because F_4 divides one leg, and neither subscript is divisible by 4. Thus, F_{8m} is one leg in the only possible cases, forcing F_8 to be a factor of F_n or of F_k.

Using 17 for the modulus, with quadratic residues 0, 1, 2, 4, 8, 9, 13, 15, 16, we find

$$F_{18m}^2 \equiv 0 \pmod{17}$$
$$F_{18m\pm 2}^2 \equiv 1 \pmod{17}$$
$$F_{18m\pm 4}^2 \equiv 9 \pmod{17}$$
$$F_{18m\pm 6}^2 \equiv 13 \pmod{17}$$
$$F_{18m\pm 8}^2 \equiv 16 \pmod{17}$$

Now, F_{18m}^2 can be added to any of the other forms to make a quadratic residue (mod 17). $F_{18m\pm 2}^2 + F_{18m\pm 2}^2 \equiv 2$ (mod 17), but one subscript must be divisible by 6. $F_{18m\pm 2}^2 + F_{18m\pm 4}^2 \equiv 10$ (mod 17) is not a residue. $F_{18m\pm 2}^2 + F_{18m\pm 6}^2 \equiv 14$ (mod 17) is not a residue. $F_{18m\pm 2}^2 + F_{18m\pm 8}^2 \equiv 0$ (mod 17), but one subscript must be divisible by 6. $F_{18m\pm 4}^2 + F_{18m\pm 6}^2 \equiv 5$ (mod 17) is not a residue, while $F_{18m\pm 4}^2 + F_{18m\pm 8}^2 \equiv 8$ (mod 17), but one subscript must be divisible by 6. $F_{18m\pm 4}^2 + F_{18m\pm 4}^2$ and $F_{18m*\pm 8}^2 + F_{18m\pm 8}^2$ are also discarded because one subscript is not divisible by 6. $F_{18m\pm 6}^2 + F_{18m\pm 6}^2$ have a common factor of F_6 so cannot be in the same primitive triple, and $F_{18m\pm 6}^2 + F_{18m\pm 8}^2$ produce the nonresidue 12 (mod 17). The only possibility, then, is that F_{18m} appears as one leg, or that F_{18} divides either F_n or F_k.

Since K cannot have any factors in common with F_n or with F_k, we note that the prime factors 2, 3, 5, 7, and 11 occur in F_{10}, F_8, F_{18}, F_6, and F_4, but 13 does not, making 13 the smallest possible prime factor for K.

Theorem 3.5: If $F_n^2 + F_k^2 = K^2$, $n > k > 0$, has a solution in positive integers, then the smallest leg $F_k \geq F_{50}$, which has 11 digits.

Proof: Consider the required form of the subscripts n and k in the light of Theorem 3.4. Because $4|F_n$ or $4|F_k$, and both subscripts are even, we can write $F_{6m}^2 + F_{2p}^2$, where $p = 3j \pm 1$, making the required form $F_{6m}^2 + F_{6j\pm 2}^2$. Since 3 divides one subscript or the other, 4 divides one subscript or the other, leading to

(i) $F_{6m}^2 + F_{12w\pm 4}^2$, for j odd,

and to

(ii) $F_{12m}^2 + F_{12w\pm 2}^2$, for j even.

First, consider (i). Since $F_8 = 21$ divides one leg or the other, F_8 must divide $F_{12w\pm 4}$ to avoid a common factor of $F_4 = 3$, so w is odd, making $F_{6m}^2 + F_{24q\pm 8}^2$ the required form. Next, F_{18} divides a leg. If F_{18} divides $F_{12w\pm 4}$, then $F_6 | F_{12w\pm 4}$, but $6 \nmid (12w \pm 4)$. So, $F_{18} | F_{6m}$, making the required form become $F_{18m}^2 + F_{24q\pm 8}^2$. Next, since F_{10} divides a leg, we obtain the two final forms,

(1) $F_{90m}^2 + F_{24q\pm 8}^2$ or (2) $F_{18m}^2 + F_{120s\pm 40}^2$.

Next, consider (ii). Since $F_8 = 21$ divides a leg, we must have $F_8 | F_{12m}$ to avoid a common factor of $F_4 = 3$, making the form become $F_{24m}^2 + F_{12w\pm 2}^2$. Also, F_{18} divides a leg, but must divide F_{24m} to avoid a common factor of F_6, making the form be $F_{72m}^2 + F_{12m\pm 2}^2$. Since we also have F_{10} as the divisor of a leg, we have the two possible final forms

(3) $F_{360r}^2 + F_{12w\pm 2}^2$ or (4) $F_{72m}^2 + F_{60p\pm 10}^2$.

Now, if F_k is the odd leg, then $F_k = m^2 - n^2$, and the even leg is $F_n = 2mn$. The largest value for $2mn$ occurs for $(m + n) = F_k$ and $(m - n) = 1$, so we do not need to know the factors of F_k. Solving to find the largest values of m and n, we find $m = (F_k + 1)/2$ and $n = (F_k - 1)/2$, making the largest possible even leg $F_n = 2mn = (F_k^2 - 1)/2$. We have available a table of Fibonacci numbers F_n, $0 \leq n \leq 571$ [6].

We look at the four possible forms again. In form (1), F_{90} has 19 digits, the smallest possible even leg. Possible odd legs are F_{16}, F_{32}, F_{40}, F_{56}, ... where F_{40} has 9 digits, so that $(F_{40}^2 - 1)/2$ has less then 19 digits, making the smallest possible leg in form (1) be F_{56}. In form (2), $F_{18m}^2 + F_{120q \pm 40}^2$, the smallest leg occurs for $m = 1$, known not to occur in such a triple from Table 1; $m = 2$ gives a common factor of 4 with the other subscript, making $m = 3$ the smallest usable value, or the smallest possible leg F_{54}. Now, form (3) has F_{360}, a number of 75 digits, as the smallest value for the even leg, making the smallest possible odd leg greater than F_{170}, which has 36 digits. Lastly, form (4) has its smallest leg F_{50}, which has 11 digits. Comparing smallest legs in the four forms, we see that the smallest leg possible is F_{50}.

Theorem 3.6: $L_n^2 + L_k^2 = K^2$, $n > k > 0$, has the unique solution $n = 3$, $k = 2$, or the triple 3 - 4 - 5.

Proof: Since $4|L_n$ or $4|L_k$, either $n = 3(2k + 1)$ or $k = 3(2k + 1)$, so that one subscript is odd. Since 3 divides one leg in a Pythagorean triple, one leg has to have a subscript of $2(2k + 1)$, which is even, since $L_p|L_q$ if and only if $q = (2k + 1)p$ (see [1]). Thus, n and k must have opposite parity. If n and k have opposite parity, then $(n - k)$ is odd. Since $L_{-n} = (-1)^n L_n$, from [1] we have both

$$(3.2) \qquad L_{n-k}L_{n+k} - L_n^2 = 5(-1)^{n+k}F_k^2,$$

$$(-1)^{n-k}L_{n-k}L_{n+k} - L_k^2 = 5(-1)^{n+k}F_n^2,$$

where $n - k$ is odd. Adding the two forms of (3.1),

$$L_n^2 + L_k^2 = 5(F_k^2 + F_n^2) = 5F_{n-k}F_{n+k}$$

by (3.1). Now, $5F_{n-k}F_{n+k} = K^2$ if and only if either $F_{n-k} = 5x^2$ and $F_{n+k} = y^2$ or $F_{n-k} = y^2$ and $F_{n+k} = 5x^2$. By Theorems 2.5 and 2.2, either $n + k = 1$ and $n - k = 5$ or $n - k = 1$ and $n + k = 5$, making the only solution $n = 3$, $k = 2$.

4. SOLUTIONS FOR $F_n^2(a) - F_k^2(a) = K^2$

By Theorem 2.6, when n and k have the same parity,

$$(4.1) \qquad F_n^2(a) - F_k^2(a) = F_{n-k}(a)F_{n+k}(a).$$

As in Section 3, $F_{n-k}(a)F_{n+k}(a) = K^2$ if and only if both $F_{n-k}(a) = x^2$ and $F_{n+k}(a) = y^2$, indicating a limited number of solutions in positive integers. Note that n and k cannot both be even if $a \geq 2$, because $F_{2p}(a)$ and $F_{2r}(a)$ have the common factor $F_2(a)$, precluding a primitive triple.

Lemma 4.1: If a is odd, $2|F_{3k}(a)$, $3|F_{4k}(a)$, and $4|F_{6k}(a)$.

Proof: We list $F_0(a) = 0$, $F_1(a) = 1$, $F_2(a) = a$, $F_3(a) = a^2 + 1$, $F_4(a) = a^3 + 2a$, $F_5(a) = a^4 + 3a^2 + 1$, and $F_6(a) = a^5 + 4a^3 + 3a$. If a is odd, then $F_3(a)$ is even. If $a = 2m + 1$, then

$$\begin{aligned} F_4(a) &= (8m^3 + 12m^2 + 6m + 1) + (4m + 2) \\ &= (8m^3 + 4m) + (12m^2 + 6m + 3) \\ &= 4m(2m^2 + 1) + 3(4m^2 + 2m + 1) \\ &= 3M + 3K = 3W, \end{aligned}$$

since either $3|m$ or $3|(2m^2 + 1)$. Also, $a = 2m + 1$ makes

$$\begin{aligned} F_6(a) &= (2m + 1)^5 + 4(2m + 1)^3 + 3(2m + 1) \\ &= (4K + 10m + 1) + 4M + (6m + 3) \\ &= 4K + 4M + 16m + 4 = 4P. \end{aligned}$$

Since $F_m(a)|F_{mk}(a)$, $m > 0$, the lemma follows.

Lemma 4.2: If a is even, $2|F_{2k}(a)$, $3|F_{4k}(a)$, and $4|F_{4k}(a)$.

Proof: Refer to the proof of Lemma 4.1 and let $a = 2m$. Then $F_2(a) = 2m$, and $F_4(a) = 8m^3 + 4m = 4[m(2m^2 + 1)] = 4 \cdot 3M$, and the Lemma follows as before.

Theorem 4.1: If $F_n^2(a) - F_k^2(a) = K^2$, $n > k > 0$, has solutions in positive integers, then $n \neq 4k$. If a is even, n cannot be even. If a is odd, $n \neq 3k$ and $n \neq 4k$.

Proof: Lemmas 4.1 and 4.2 show that $3|F_{4k}(a)$, and since 3 divides one leg in a Pythagorean triple, $n = 4k$ would cause a common factor of 3, preventing a primitive triple. For similar reasons, $n \neq 2k$ if a is even, and $n \neq 3k$ if a is odd.

Conjecture 4.2: Any possible solution for $P_n^2 - P_k^2 = K^2$, $n > k > 0$, occurs only if $n = 2p + 1$ and $k = 4w$, or if P_n is odd and P_k is a multiple of 12.

Proof: Considering (4.1), there is no solution to $P_{n-k} = x^2$, $P_{n+k} = y^2$ if n and k have the same parity, if Conjecture 2.3 holds. Also, n cannot be even, because $2|P_{2m}$ and 4 divides one leg in a Pythagorean triple, precluding a primitive triple. If k is even, then P_k is even, and the even leg is divisible by 4, making P_k have the form P_{4w}. Since $P_4 = 12$, P_{4w} is a multiple of 12.

Theorem 4.3: $F_n^2 - F_k^2 = K^2$ has solutions in positive integers for $n = 7$, $k = 5$, forming the triple 5-12-13, and for $n = 5$, $k = 4$, forming the triple 3-4-5. Any other solutions occur only if n and k have opposite parity, where either $n = 12w \pm 2$ and k is odd, or $n = 6m \pm 1$ and k is even.

Proof: Using (4.1) and Theorem 2.2, the only solution for $F_{n-k} = x^2$ and $F_{n+k} = y^2$ where n and k have the same parity is $n = 7$, $k = 5$, making the triple 5-12-13. If any other solutions exist, n and k have opposite parity. It is known that $n = 5$, $k = 4$ provides a solution, giving the triple 3-4-5. If n is even, $n \neq 3k$, $n \neq 4k$, so $n = 12w \pm 2$, and k is odd. If n is odd, $n \neq 3k$, so $n = 6m \pm 1$ and k is even.

Theorem 4.4: If n and k have different parity, any solutions for $F_n^2 - F_k^2 = K^2$ other than $n = 5$, $k = 4$, or the triple 3-4-5, must have $n \geq k + 5$.

Proof: $F_{n+1}^2 - F_n^2 = F_{n-1}F_{n+2}$, where $(F_{n-1}, F_{n+2}) = 1$ or 2, so that $F_{n-1}F_{n+2} = K^2$ either if $F_{n-1} = x^2$ and $F_{n+2} = y^2$, or if $F_{n-1} = 2x^2$ and $F_{n+2} = 2y^2$. By Theorem 2.2, there are no solutions to $F_{n-1} = x^2$ and $F_{n+2} = y^2$, but $F_{n-1} = 2x^2$ and $F_{n+2} = 2y^2$ is solved by $n = 4$, yielding the 3-4-5 triple. There are no other solutions for subscripts differing by 1. Since n and k have opposite parity, they differ by an odd number.

$$F_{n+3}^2 - F_n^2 = 4F_{n+1}F_{n+2} \neq K^2 \text{ unless } n = 0 \text{ or } -1 \text{ by Theorem 2.2.}$$

Thus, the hypotenuse has a subscript at least five greater than the leg.

Theorem 4.5: $F_n^2(a) - F_k^2(a) = K^2$ has no solution in positive integers if $F_n(a)$ is prime.

Proof: See the discussion at the end of Section 1.

Theorem 4.6: If $L_n^2 - L_k^2 = K^2$, $n > k > 0$, has solutions in positive integers, then either $n = 4m$ and k is odd, or $n = 6p \pm 1$ and k is even.

Proof: We parallel the proof of Theorem 3.6, except here we take n and k with the same parity, so that $n + k$ is even, and subtract:

$$L_{n-k}L_{n+k} - L_n^2 = 5(-1)^{n+k}F_k^2$$

$$(-1)^{n-k}L_{n-k}L_{n+k} - L_k^2 = 5(-1)^{n+k}F_n^2$$

$$L_n^2 - L_k^2 = 5(F_n^2 - F_k^2) = 5F_{n-k}F_{n+k} = K^2$$

if and only if $F_{n-k} = 5x^2$ and $F_{n+k} = y^2$, or $F_{n+k} = 5x^2$ and $F_{n-k} = y^2$. By Theorem 2.5, the only solution for n and k the same parity is $n - k = 0$, which does not solve our equation.

If n and k do not have the same parity, consider n even. Then, $n = 4k$ or $n = 4k + 2$, but $n = 4k + 2$ is impossible because the hypotenuse would have the factor 3 in common with a leg. Thus, $n = 4k$, and k is odd. If n is odd, then $n = 6p \pm 1$ to avoid a factor of $L_2 = 3$, and k is even.

Conjecture: The only solutions to $F_n^2(a) \pm F_k^2(a) = K^2$, $n > k > 0$, in positive integers, are found in the two Pythagorean triples 3-4-5 and 5-12-13. If $a \geq 3$ and $a \neq k^2$, the only squares in $\{F_n(a)\}$ are 0 and 1.

I wish to thank Professor L. Carlitz for suggesting reference [9] and for reading this paper.

REFERENCES

1. Verner E. Hoggett, Jr., *Fibonacci and Lucas Numbers*, The Houghton-Mifflin Mathematics Enrichment Series (Boston: Houghton-Mifflin, 1969).
2. G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers* (4th ed.; Oxford: Oxford University Press, 1960).
3. John H. E. Cohn, "Square Fibonacci Numbers," *The Fibonacci Quarterly* 2, No. 2 (1964):109-113.
4. Marjorie Bicknell, "A Primer for the Fibonacci Numbers, Part VII: An Introduction to Fibonacci Polynomials and Their Divisibility Properties," *The Fibonacci Quarterly* 8, No. 4 (1970):407-420.
5. V. E. Hoggatt, Jr., & Marjorie Bicknell-Johnson, "Divisibility Properties of Polynomials in Pascal's Triangle," *The Fibonacci Quarterly* 16, No. 6 (1978):501-513.
6. S. L. Basin & V. E. Hoggatt, Jr., "The First 571 Fibonacci Numbers," *Recreational Mathematics Magazine*, No. 11 (October 1962):19-30.
7. John H. Halton, "Some Properties Associated with Square Fibonacci Numbers," *The Fibonacci Quarterly* 5, No. 4 (1967):347-355.
8. L. Carlitz, "A Note on Fibonacci Numbers," *The Fibonacci Quarterly* 2, No. 1 (1964):15-28.
9. A. Eswarathasan, "On Square Pseudo-Lucas Numbers," *Canadian Mathematics Bulletin* 21 (1978):297-303.

*****

STRONG DIVISIBILITY SEQUENCES AND SOME CONJECTURES

CLARK KIMBERLING
University of Evansville, Evansville, IN 47702

1. INTRODUCTION

Which recurrent sequences $\{t_n : n = 0, 1, \ldots\}$ satisfy the following equation for greatest common divisors:

(1) $$(t_m, t_n) = t_{(m,n)} \quad \text{for all } m, n \geq 1,$$

or the weaker divisibility property:

(2) $$t_m | t_n \quad \text{whenever} \quad m | n?$$

In case the sequence $\{t_n\}$ is a *linear* recurrent sequence, the question leads directly to an unproven conjecture of Morgan Ward. (See [3] for further discussion of this question.) Nevertheless, certain examples have been studied in detail. If t_n is the nth Fibonacci number F_n, then (1) holds and continues to hold if t_n is generalized to the Fibonacci polynomial $F_n(x,z)$, as defined in Hoggatt and Long [2]. Not only does (1) hold for these second-order linear recurrent sequences, but (1) holds also for certain higher-order linear sequences and certain nonlinear sequences. For example, if $\{s_n\}$ and $\{t_n\}$ are sequences of nonnegative integers satisfying (1), then for fixed $m \geq 2$ the sequences $\{t_n^m : n = 0, 1, \ldots\}$ and $\{t_{s_n} : n = 0, 1, \ldots\}$ also satisfy (1). Other examples include Vandermonde sequences, resultant sequences and their divisors, and elliptic divisibility sequences. These are discussed below in Sections 3 and 4, in connection with the main theorem (Theorem 1) of this note.

In the sequel, the term *sequence* always refers to a sequence t_0, t_1, t_2, ... of integers or polynomials (in some finite number of indeterminates) all of whose coefficients are integers. With this understanding, a sequence is a *divisibility sequence* if (2) holds, and a *strong divisibility sequence* if (1) holds. Here, all divisibilities refer to the arithmetic in the appropriate ring; that is, the ring I of integers if $t_n \in I$ for all n, and the ring $I[x_1, \ldots, x_j]$ if the t_n are polynomials in the indeterminates $x_1, \ldots, x_j$.

A sequence $\{t_n\}$ in I (or $I[x_1, \ldots, x_j]$) is a kth-*order linear recurrent sequence* if

(3) $$t_{n+k} = a_1 t_{n+k-1} + \cdots + a_k t_n \qquad n = 0, 1, \ldots,$$

where the a_i's and $t_0, \ldots, t_{n-1}$ lie in I (or $I[x_1, \ldots, x_j]$). A kth-*order divisibility sequence* is a kth-order linear recurrent sequence satisfying (2), and a kth-*order strong divisibility sequence* is a kth-order linear recurrent sequence satisfying (1).

2. CYCLOTOMIC QUOTIENTS

For any sequence $\{t_n\}$ we define *cyclotomic quotients* $Q_1, Q_2, \ldots$ as follows: for $n \geq 2$, let $P_1, P_2, \ldots, P_r$ be the distinct prime factors of n; let

$$\Pi_0 = t_n,$$

and for $1 \leq k \leq r$, let

$$\Pi_k = \Pi t_{n/P_{i_1} P_{i_2} \ldots P_{i_k}},$$

the product extending over all the k indices i_j which satisfy the conditions

$$1 \leq i_1 < i_2 < \cdots < i_k \leq r.$$

Let $Q_1 = 1$, and for $n \geq 2$, define

$$Q = \frac{\Pi_0 \Pi_2 \cdots}{\Pi_1 \Pi_3 \cdots}. \tag{3}$$

The following lemma is a special case of the inclusion-exclusion principle:

Lemma 1: Let H be a set of τ real numbers. For $i = 1, 2, \ldots, \tau$, let $\mathcal{H}_i$ be the family of subsets of H which consist of i elements. Let

$$m_i = \sum_{A \in \mathcal{H}_i} \min A.$$

Then

$$m_1 - m_2 + m_3 - \cdots - (-1)^{\tau} m_{\tau} = \max H.$$

Proof: We list the elements of H as $h_1 \leq h_2 \leq \cdots \leq h_{\tau} = \max H$. Clearly

$$m_i = \binom{\tau - 1}{i - 1} h_1 + \binom{\tau - 2}{i - 1} h_2 + \cdots + \binom{i - 1}{i - 1} h_{\tau - i + 1}$$

for $i = 1, 2, \ldots, \tau$, so that

$$\begin{aligned} &m_1 - m_2 + m_3 - \cdots - (-1)^{\tau} m_{\tau} \\ &= h_1 \sum_{i=0}^{\tau-1} (-1)^i \binom{\tau - 1}{i} + h_2 \sum_{i=0}^{\tau-2} (-1)^i \binom{\tau - 2}{i} + \cdots + h_{\tau-1} \sum_{i=0}^{1} (-1)^i \binom{1}{i} + h_{\tau} \\ &= h_{\tau}. \end{aligned}$$

Theorem 1: Let $\{t_n : n = 0, 1, \ldots\}$ be a strong divisibility sequence. Then the product $\Pi_1 \Pi_3 \ldots$ divides the product $\Pi_0 \Pi_2 \ldots$. [That is, the quotients (3) are integers (or polynomials with integer coefficients).]

Proof: Let $n = P_1^{f_1} \ldots P_{\nu}^{f_{\nu}}$, and write $t_n = q_1^{h_1} \ldots q_{\tau}^{h_{\tau}}$. Then

$$\Pi_0 \Pi_2 \Pi_4 \cdots = t_n \Pi t_{n/P_{i_1} P_{i_2}} \Pi t_{n/P_{i_1} P_{i_2} P_{i_3} P_{i_4}} \cdots, \text{ and} \tag{4}$$

$$\Pi_1 \Pi_3 \Pi_5 \cdots = \Pi t_{n/P_i} \Pi t_{n/P_{i_1} P_{i_2} P_{i_3}} \Pi t_{n/P_{i_1} P_{i_2} P_{i_3} P_{i_4} P_{i_5}} \cdots. \tag{5}$$

Now $t_{n/P_i} = q_1^{h_{i1}} q_2^{h_{i2}} \ldots q_{\tau}^{h_{i\tau}}$ for $i = 1, 2, \ldots, \nu$, where

$$h_j \geq h_{ij} \text{ for } j = 1, 2, \ldots, \tau, \text{ and } i = 1, 2, \ldots, \nu. \tag{6}$$

Further,

$$t_{n/P_{i_1} P_{i_2}} = \left(t_{n/P_{i_1}},\ t_{n/P_{i_2}}\right) = \prod_{j=1}^{\tau} q_j^{\min\{h_{i_1 j}, h_{i_2 j}\}},$$

$$t_{n/P_{i_1} P_{i_2} P_{i_3}} = \left(t_{n/P_{i_1} P_{i_2}},\ t_{n/P_{i_1} P_{i_3}},\ t_{n/P_{i_2} P_{i_3}}\right) = \prod_{j=1}^{\tau} q_j^{\min\{h_{i_1 j}, h_{i_2 j}, h_{i_3 j}\}},$$

and so on. Consider now for any j satisfying $1 \leq j \leq \tau$ the set

$$H = \left\{h_{1j},\ h_{2j},\ \ldots,\ h_{\nu j}\right\}.$$

For $1 \leq i \leq \nu$, let $\mathcal{H}_i$ and m_i be as in Lemma 1. Then the exponent of q_i in $\Pi_0\Pi_2 \ldots$ is $h_j + m_2 + m_4 + \cdots$ and the exponent of q_i in $\Pi_1\Pi_3 \ldots$ is $m_1 + m_3 + \cdots$. Consequently, the exponent of q_i in (3) is

$$h_j - \left[m_1 - m_2 + m_3 - \cdots - (-1)^{\tau} m_{\tau}\right].$$

By Lemma 1, this exponent is $h_j - \max H$, which according to (6) is nonnegative.

It is easily seen that Equation (2) would not be sufficient for the conclusion of Theorem 1: define

$$t_n = \begin{cases} n & \text{for } n = 0, 1, 2, 4, 6, 8, \ldots \\ 2 & \text{for } n = 3 \\ 2n & \text{for } n = 5, 7, 9, 11, \ldots \end{cases}$$

Then Equation (2) is satisfied, but, for example, the cyclotomic quotient $t_6 t_1 / t_2 t_3$ is not an integer.

3. RESULTANT SEQUENCES AND THEIR DIVISORS

Suppose

$$X(t) = \prod_{i=1}^{p} (t - x_i) = t^p - X_1 t^{p-1} + \cdots + (-1)^p X_p \tag{7}$$

and

$$Y(t) = \prod_{j=1}^{q} (t - y_j) = t^q - Y_1 t^{q-1} + \cdots + (-1)^q Y_q \tag{8}$$

are polynomials; here any number of the roots x_i and y_j may be indeterminates, and we assume that the coefficients X_k and Y_ℓ lie in the ring $I[x_1, \ldots, x_p, y_1, \ldots, y_q]$. Thus all roots which are not indeterminates must be algebraic integers. Instead of regarding the roots as given indeterminates, we may regard any number of the coefficients X_k and Y_ℓ as the given indeterminates; in this case the roots x_i and y_j are regarded as indeterminates having functional interdependences.

The *resultant sequence* based on $\{x_1, \ldots, x_p, y_1, \ldots, y_q\}$ (or $\{X_1, \ldots, X_p, Y_1, \ldots, Y_q\}$) is the sequence $\{t_n : n = 0, 1, \ldots\}$ given by

$$t_n = \prod_{j=1}^{q} \prod_{i=1}^{p} \frac{x_i^n - y_j^n}{x_i - y_j}. \tag{9}$$

Note that $t_n = R_n / R_1$, where R_n is the resultant of the polynomials

$$\prod_{i=1}^{p} (t - x_i^n) \quad \text{and} \quad \prod_{j=1}^{q} (t - y_j^n).$$

By a *divisor-sequence* of a resultant sequence $\{t_n\}$, we mean a linear divisibility sequence $\{s_n : n = 0, 1, \ldots\}$ such that $s_n \mid t_n$ for $n = 1, 2, \ldots$.

We may now state Ward's conjecture mentioned in Section 1: every linear divisibility sequence is (essentially) a divisor-sequence of a resultant sequence. We further conjecture: every linear *strong* divisibility sequence of *integers* must lie in the class T of second-order sequences (i.e., Fibonacci sequences) or else be a product-sequence $\{t_{1n}t_{2n}\ldots t_{mn} : n = 0, 1, \ldots\}$ where each divisor-sequence $\{t_{jn} : n = 0, 1, \ldots\}$ lies in T, for $j = 1, 2, \ldots, m$. The interested reader may wish to consult especially Theorem 5.1 of Ward [8].

One salient class of divisor-sequences of resultant sequences are the *Vandermonde sequences*, as discussed in [3]. Briefly, a Vandermonde sequence $\{t_n : n = 0, 1, \ldots\}$ arises from the polynomial (7) by

$$t_n = \prod_{1 \le i \le j \le p} \frac{x_i^n - x_j^n}{x_i - x_j}.$$

Thus, t_n is akin to the discriminant of the polynomial

$$\Xi(t) = \prod_{i=1}^{p} (t - x_i^n),$$

as well as the resultant of $\Xi(t)$ and its derivative $\Xi'(t)$. (See, for example, van der Waerden [5, pp. 86-87].)

If one or more of the roots x_i and y_j underlying a divisor-sequence of a resultant sequence is an indeterminate, then, except for certain possible irregularities which need not be mentioned here, the sequence is a strong linear divisibility sequence.

As an example of a strong linear divisibility sequence of polynomials, we mention the 6th-order Vandermonde sequence which arises from

$$X(t) = t^3 - \sqrt[3]{x}t^2 - 1.$$

With generating function

$$\frac{t(t^2 + t + 1)^2}{(t^2 + t + 1)^3 + xt^2(t + 1)^2},$$

this sequence $\{t_n\}$ has, for its first few terms, $t_0 = 0$, $t_1 = 1$, $t_2 = -1$, $t_3 = -x$, $t_4 = 2x + 1$, $t_5 = x^2 + x - 1$, $t_6 = -3x^2 - 8x$, $t_7 = -x^3 - x^2 + 9x + 1$, $t_8 = 4x^3 + 18x^2 + 6x - 1$. If $x = -1$, then $\{t_n\}$ is no longer a *strong* linear divisibility sequence, but is, of course, still a divisibility sequence. As reported in [3], we have

$$|t_n| \le F_n \qquad (= n\text{th Fibonacci number})$$

for $1 \le n \le 100$. It is not yet known if this inequality holds for all n.

Another conjecture follows: for any strong linear divisibility sequence of polynomials $t_0, t_1, t_2, \ldots$ which has no proper divisor-sequences, the polynomial t_n is irreducible if and only if n is a prime. A stronger conjecture is that the cyclotomic quotients (3) are all irreducible polynomials.

4. ELLIPTIC DIVISIBILITY SEQUENCES

Consider the sequence of polynomials in x, y, z defined recursively as follows:

$$t_0 = 0,\ t_1 = 1,\ t_2 = x,\ t_3 = y,\ t_4 = xz,$$

$$t_{2n+1} = t_{n+2}t_n - t_{n-1}t_{n+1} \quad \text{for } n \ge 2$$

$$t_{2n+2} = \frac{1}{x}(t_{n+3}t_{n+1}t_n - t_{n+1}t_{n-1}t_{n+2}) \quad \text{for } n \ge 2.$$

The sequence $\{t_n : n = 0, 1, \ldots\}$ is an *elliptic divisibility sequence.* If x, y, or z is an indeterminate then $\{t_n\}$ is a strong divisibility sequence. In this case, we conjecture, as in Section 3 for linear sequences, that the cyclotomic quotients (3) are the irreducible divisors of the polynomials t_n.

If x, y, and z are all integers, then $\{t_n\}$ is a strong divisibility sequence if and only if the greatest common divisor of y and xz is 1, as proved in [11].

We conclude with a list of the first several terms of a numerical elliptic strong divisibility sequence:

$t_0 = 0$
$t_1 = 1$
$t_2 = 1$
$t_3 = -1$
$t_4 = 1$
$t_5 = 2$
$t_6 = -1$
$t_7 = -3$
$t_8 = -5$
$t_9 = 7$
$t_{10} = -4$
$t_{11} = -23$
$t_{12} = 29$
$t_{13} = 59$
$t_{14} = 129$
$t_{15} = -314$
$t_{16} = -65$
$t_{17} = 1529$
$t_{18} = -3689$
$t_{19} = -8209$
$t_{20} = -16264$
$t_{21} = 83313$
$t_{22} = 113689$
$t_{23} = -620297$
$t_{24} = 2382785$
$t_{25} = 7869898$
$t_{26} = 7001471$
$t_{27} = -126742987$
$t_{28} = -398035821$
$t_{29} = 1687054711$
$t_{30} = -7911171596.$

REFERENCES

1. Marshall Hall, "Divisibility Sequences of Third Order," *Amer. J. Math.* 58 (1936):577-584.
2. V. E. Hoggatt, Jr., & C. T. Long, "Divisibility Properties of Generalized Fibonacci Polynomials," *The Fibonacci Quarterly* 2, No. 2 (1974):113-120.
3. Clark Kimberling, "Generating Functions of Linear Divisibility Sequences," *The Fibonacci Quarterly* (to appear).
4. Clark Kimberling, "Strong Divisibility Sequences with Nonzero Initial Term," *The Fibonacci Quarterly* 16, No. 6 (1978):541-544.
5. B. L. van der Waerden, *Modern Algebra* (New York: Ungar, 1953).
6. Morgan Ward, "Note on Divisibility Sequences," *Bull. AMS* 42 (1936):843-845.
7. Morgan Ward, "Linear Divisibility Sequences," *Transactions AMS* 41 (1937):276-286.
8. Morgan Ward, "Arithmetical Properties of Sequences in Rings," *Annals of Math.* 39 (1938):210-219.
9. Morgan Ward, "A Note on Divisibility Sequences," *Bull. AMS* 45 (1939):334-336.
10. Morgan Ward, "The Law of Apparition of Primes in a Lucasian Sequence," *Transactions AMS* 44 (1948):68-86.
11. Morgan Ward, "Memoir on Elliptic Divisibility Sequences," *Amer. J. Math.* 70 (1948):31-74.
12. Morgan Ward, "The Law of Repetition of Primes in an Elliptic Divisibility Sequence," *Duke Math. J.* 15 (1948):941-946.

*****

GREATEST COMMON DIVISORS OF SUMS AND DIFFERENCES OF FIBONACCI, LUCAS, AND CHEBYSHEV POLYNOMIALS

CLARK KIMBERLING
University of Evansville, Evansville, IN 47702

It is well known that the Fibonacci polynomials $F_n(x)$, the Lucas polynomials $L_n(x)$, and the Chebyshev polynomials of both kinds satisfy many "trigonometric" identities. For example, the identity

$$F_{2m}(x) + F_{2n}(x) = F_{m+n}(x)L_{|m-n|}(x) \text{ for even } m + n$$

is analogous to the trigonometric identity

$$\sin A + \sin B = 2 \sin \frac{1}{2}(A + B) \cos \frac{1}{2}(A - B).$$

Just below, we list eight well-known identities in the form which naturally results from direct proofs using the usual four identities for sums and differences of hyperbolic sines and cosines, together with certain identities in Hoggatt and Bicknell [4]:

$$F_{2n}(x) = \frac{\sinh 2n\theta}{\cosh \theta} \qquad F_{2n+1}(x) = \frac{\cosh (2n+1)\theta}{\cosh \theta}$$

$$L_{2n}(x) = 2 \cosh 2n\theta \qquad L_{2n+1}(x) = 2 \sinh (2n+1)\theta,$$

where $x = 2 \sinh \theta$. Writing simply F_n and L_n for $F_n(x)$ and $L_n(x)$ and assuming $m \geq n > 0$, the eight identities are as follows:

$$F_{2m} + F_{2n} = \begin{cases} F_{m+n}L_{m-n} & \text{if } m+n \text{ is even} \\ F_{m-n}L_{m+n} & \text{if } m+n \text{ is odd} \end{cases} \tag{1}$$

$$F_{2m} - F_{2n} = \begin{cases} F_{m-n}L_{m+n} & \text{if } m+n \text{ is even} \\ F_{m+n}L_{m-n} & \text{if } m+n \text{ is odd} \end{cases} \tag{2}$$

$$F_{2m+1} + F_{2n+1} = \begin{cases} F_{m+n+1}L_{m-n} & \text{if } m+n \text{ is even} \\ F_{m-n}L_{m+n+1} & \text{if } m+n \text{ is odd} \end{cases} \tag{3}$$

$$F_{2m+1} - F_{2n+1} = \begin{cases} F_{m-n}L_{m+n+1} & \text{if } m+n \text{ is even} \\ F_{m+n+1}L_{m-n} & \text{if } m+n \text{ is odd} \end{cases} \tag{4}$$

$$L_{2m} + L_{2n} = \begin{cases} L_{m+n}L_{m-n} & \text{if } m+n \text{ is even} \\ (x^2+4)F_{m+n}F_{m-n} & \text{if } m+n \text{ is odd} \end{cases} \tag{5}$$

$$L_{2m} - L_{2n} = \begin{cases} (x^2+4)F_{m+n}F_{m-n} & \text{if } m+n \text{ is even} \\ L_{m+n}L_{m-n} & \text{if } m+n \text{ is odd} \end{cases} \tag{6}$$

$$L_{2m+1} + L_{2n+1} = \begin{cases} L_{m-n}L_{m+n+1} & \text{if } m+n \text{ is even} \\ (x^2+4)F_{m+n+1}F_{m-n} & \text{if } m+n \text{ is odd} \end{cases} \tag{7}$$

$$L_{2m+1} - L_{2n+1} = \begin{cases} (x^2+4)F_{m+n+1}F_{m-n} & \text{if } m+n \text{ is even} \\ L_{m-n}L_{m+n+1} & \text{if } m+n \text{ is odd} \end{cases} \tag{8}$$

These identities are derived in [2] in a manner much less directly dependent on hyperbolic or trigonometric identities. See especially identities (72)-(79) in [2], which generalize considerably the present identities. An intermediate level of generalization is at the level of the generalized Fibonacci polynomials $F_n = F_n(x,z)$ and the generalized Lucas polynomials $L_n = L_n(x,z)$. For example, (5) becomes

$$L_{2m} + L_{2n} = (x^2 + 4z)F_{m+n}F_{m-n} \quad \text{if } m+n \text{ is odd.}$$

Let us recall the substitutions which link the F_n's and L_n's with Chebyshev polynomials $T_n(x)$ of the first kind and $U_n(x)$ of the second kind:

$$T_n(x) = \frac{1}{2}L_n(2x,-1), \quad n = 0, 1, \ldots$$

$$U_n(x) = F_{n+1}(2x,-1), \quad n = 0, 1, \ldots .$$

Clearly, our discussions involving F_n's and L_n's carry over immediately to T_n's and U_n's; bearing this in mind, we make no further mention of Chebyshev polynomials in this paper.

Identities (1)-(8) show that greatest common divisors for certain sums and differences of the various polynomials can be found in terms of the irreducible divisors of individual generalized Fibonacci polynomials and generalized Lucas polynomials. In [7], we showed these divisors to be the generalized Fibonacci-cyclotomic polynomials $\mathcal{F}_n(x,z)$. The interested reader should consult [7] for a definition of these polynomials. Theorems 6 and 10 in [7] may be restated for $n \geq 1$ as follows:

$$F_n(x,z) = \prod_{d|n} \mathcal{F}_d(x,z) \tag{I}$$

$$L_n(x,z) = \prod_{d|q} \mathcal{F}_{2^{t+1}d}(x,z), \text{ where } n = 2^t q,\ q \text{ odd},\ t \geq 0. \tag{II}$$

The (ordinary) Fibonacci and Lucas polynomials are given by $F_n(x) = F_n(x,1)$ and $L_n(x) = L_n(x,1)$, and their factorizations as products of the irreducible polynomials $\mathcal{F}(x) = \mathcal{F}(x,1)$ are given by (I) and (II). With these factorizations, we are able to prove the following theorem.

Theorem 1: For any nonnegative integers a, b, c, d, the greatest common divisor of L_aF_b and L_cF_d is given by

$$(L_aF_b, L_cF_d) = F_{(b,d)}\ \frac{F_{(b,2c)}\cdot F_{(b,c,d)}\cdot F_{(2a,d)}\cdot F_{(a,b,d)}\cdot F_{(2a,2c)}\cdot F_{(a,c)}}{F_{(b,c)}\cdot F_{(b,2c,d)}\cdot F_{(a,d)}\cdot F_{(2a,b,d)}\cdot F_{(2a,c)}\cdot F_{(a,2c)}} \text{ times}$$

$$\frac{F_{(2a,b,c)}\cdot F_{(a,b,2c)}\cdot F_{(2a,c,d)}\cdot F_{(a,2c,d)}\left[F_{(2a,b,2c,d)}\cdot F_{(a,b,c,d)}\right]^2}{F_{(2a,b,2c)}\cdot F_{(a,b,c)}\cdot F_{(2a,2c,d)}\cdot F_{(a,c,d)}\left[F_{(2a,b,c,d)}\cdot F_{(a,b,2c,d)}\right]^2}.$$

Proof: Write $a = 2^s\alpha$, α odd, and $c = 2^t\gamma$, γ odd. Let

$$A = \left\{\delta : \delta = 2^{s+1}q \text{ for some } q \text{ satisfying } q|\alpha\right\}$$

$$C = \left\{\delta : \delta = 2^{t+1}q \text{ for some } q \text{ satisfying } q|\gamma\right\}$$

$$B = \left\{\delta : \delta|b\right\} \quad\text{and}\quad D = \left\{\delta : \delta|d\right\}.$$

In terms of these sets, let

$$S_1 = B \cap D$$

$$S_2 = B \cap C - B \cap C \cap D$$

$$S_3 = A \cap D - A \cap B \cap D$$

$$S_4 = A \cap C - A \cap S_2 - C \cap S_3.$$

Then,

$$(L_aF_b, L_cF_d) = \left(\prod_{\delta\in A}\mathcal{F}_\delta\prod_{\delta\in B}\mathcal{F}_\delta, \prod_{\delta\in C}\mathcal{F}_\delta\prod_{\delta\in D}\mathcal{F}_\delta\right) = \prod_{i=1}^{4}\ \prod_{\delta\in S_i}\mathcal{F}_\delta.$$

One may now readily verify that $\prod_{\delta\in S_1}\mathcal{F}_\delta = F_{(b,d)}$,

$$\prod_{\delta\in S_2}\mathcal{F}_\delta = \frac{F_{(b,2c)}}{F_{(b,c)}} \div \frac{F_{(b,2c,d)}}{F_{(b,c,d)}} \quad\text{and}\quad \prod_{\delta\in S_3}\mathcal{F}_\delta = \frac{F_{(2a,d)}}{F_{(a,d)}} \div \frac{F_{(2a,b,d)}}{F_{(a,b,d)}}.$$

For the product involving S_4, we have

$$\prod_{\delta\in A\cap C}\mathcal{F}_\delta = \frac{F_{(2a,2c)}\cdot F_{(a,c)}}{F_{(2a,c)}\cdot F_{(a,2c)}},$$

$$\prod_{\delta\in A\cap S_2}\mathcal{F}_\delta = \frac{F_{(2a,b,2c)}\cdot F_{(a,b,c)}}{F_{(2a,b,c)}\cdot F_{(a,b,2c)}} \div \frac{F_{(2a,b,c,d)}\cdot F_{(a,b,2c,d)}}{F_{(2a,b,2c,d)}\cdot F_{(a,b,c,d)}}, \text{ and}$$

$$\prod_{\delta\in A\cap S_3}\mathcal{F}_\delta = \frac{F_{(2a,d,2c)}\cdot F_{(a,d,c)}}{F_{(2a,d,c)}\cdot F_{(a,d,2c)}} \div \frac{F_{(2a,b,c,d)}\cdot F_{(a,b,2c,d)}}{F_{(2a,b,2c,d)}\cdot F_{(a,b,c,d)}}.$$

Now using

$$\prod_{\delta \in S_4} \mathcal{F}_\delta = \prod_{\delta \in A \cap C} \mathcal{F}_\delta \div \prod_{\delta \in A \cap S_2} \mathcal{F}_\delta \div \prod_{\delta \in A \cap S_3} \mathcal{F}_\delta ,$$

the desired formula is easily put together.

Corollary: $(L_a, L_c) = \dfrac{F_{(2a,2c)} \cdot F_{(a,c)}}{F_{(2a,c)} \cdot F_{(a,2c)}}$.

It is easy to obtain formulas for $(F_a F_b, F_c F_d)$ and $(L_a L_b, L_c L_d)$ using the method of proof of Theorem 1. The Lucas-formula has the same form as that in Theorem 1, but even more factors. The Fibonacci-formula too has this form, but few enough factors that we choose to include it here:

$$(F_a F_b, F_c F_d) = F_{(b,d)} \frac{F_{(b,c)} \cdot F_{(a,d)} \cdot F_{(a,c)} \cdot F^2_{(a,b,c,d)}}{F_{(b,c,d)} \cdot F_{(a,b,d)} \cdot F_{(a,b,c)} \cdot F_{(a,c,d)}} .$$

Returning now to sums and differences of polynomials, we find from identities (1) and (3), for example, that

(1′) $\quad F_{4k+n} + F_n = L_{2k} F_{2k+n}$ for any nonnegative integers k and n.

Thus, Theorem 1 enables us to write out the greatest common divisor of any two terms of the sequence

$$F_4,\ F_5 + F_1,\ F_6 + F_2,\ F_7 + F_3,\ \ldots$$

or of the sequence

$$F_1 + 1,\ F_5 + 1,\ F_9 + 1,\ F_{13} + 1,\ \ldots .$$

With the help of (3′) below, we can refine the latter sequence to

$$F_1 + 1,\ F_3 + 1,\ F_5 + 1,\ F_7 + 1,\ \ldots$$

and still find greatest common divisors. (But what about the sequence $\{F_n + 1\}$ for *all* positive integers n?)

Following is a list of double-sequence identities like (1′). These are easily obtained from identities (1)-(8).

(1′) $\quad F_{4k+n} + F_n = L_{2k} F_{2k+n}$

(2′) $\quad F_{4k+n} - F_n = F_{2k} L_{2k+n}$

(3′) $\quad F_{4k+n+2} + F_n = L_{2k+n+1} F_{2k+1}$

(4′) $\quad F_{4k+n+2} - F_n = F_{2k+n+1} L_{2k+1}$

(5′) $$L_{4k+n} + L_n = L_{2k}L_{2k+n}$$

(6′) $$L_{4k+n} - L_n = (x^2 + 4)F_{2k}F_{2k+n}$$

(7′) $$L_{4k+n+2} + L_n = (x^2 + 4)F_{2k+1}F_{2k+n+1}$$

(8′) $$L_{4k+n+2} - L_n = L_{2k+1}L_{2k+n+1}.$$

We note that the divisibility properties of some of these sequences are much the same as those of the sequence of Fibonacci polynomials [namely, $(F_m, F_n) = F_{(m,n)}$ with F_p irreducible over the integers whenever p is a prime] or the sequence of Lucas polynomials. For example, the sequence s_0, s_1, s_2, ..., given by

$$0,\ L_2 + 2,\ L_4 - 2,\ L_6 + 2,\ L_8 - 2,\ \ldots,$$

has $(s_m, s_n) = (x^2 + 4)F^2_{(m,n)}$ for all positive integers m and n.

One might expect Theorem 1 to apply to sequences other than (1′)-(8′) in the manner just exemplified. A good selection of forty identities, some admitting applications of Theorem 1, is found in [3], pp. 52-59.

REFERENCES

1. G. E. Bergum & V. E. Hoggatt, Jr., "Irreducibility of Lucas and Generalized Lucas Polynomials," *The Fibonacci Quarterly* 12, No. 1 (1974):95-100.
2. G. E. Bergum & V. E. Hoggatt, Jr., "Sums and Products for Recurring Sequences," *The Fibonacci Quarterly* 13, No. 2 (1975).
3. V. E. Hoggatt, Jr., *Fibonacci and Lucas Numbers* (Boston, Mass.: Houghton-Mifflin, 1969).
4. V. E. Hoggatt, Jr., & Marjorie Bicknell, "Roots of Fibonacci Polynomials," *The Fibaoncci Quarterly* 11, No. 3 (1973):271-274.
5. V. E. Hoggatt, Jr., & C. T. Long, "Divisibility Properties of Generalized Fibonacci Polynomials," *The Fibonacci Quarterly* 12, No. 2 (1974):113-120.
6. C. Kimberling, "Divisibility Properties of Recurrent Sequences," *The Fibonacci Quarterly* (to appear).
7. C. Kimberling, "Generalized Cyclotomic Polynomials, Fibonacci-Cyclotomic Polynomials, and Lucas-Cyclotomic Polynomials," *The Fibonacci Quarterly* (to appear).

*****

PROBABILITY VIA THE *N*TH ORDER FIBONACCI-*T* SEQUENCE

STEPHEN JOHN TURNER
St. Mary's University, Halifax, Nova Scotia B3H3C3

Suppose we repeat a Bernoulli (p) experiment until a success appears twice in a row. What is the probability that it will take exactly four trials when $p = .5$? Answer: There are 2^4 equi-probable sequences of trial outcomes. Of these, there are exactly two with their last two entries labeled success with no other consecutive entries successes. Hence, there is a $1/(2^3)$ chance that the experiment will be repeated exactly four times.

Immediately, questions arise: What is the probability that it takes 5, 6, 7, ..., n trials? What are these probabilities when $p \neq .5$? What answers can be provided when we require N successes in a row?

The answers for the most general case of N successes involve a unique approach. However, it is instructive to treat the case for $N = 2$ first in order to set the framework.

THE CASE FOR $N = 2$

We shall use the idea of "category."

Definition: Category S is the set of all $S + 1$ sequences of trial outcomes (denoted in terms of s and f) such that each has its last two entries as s and no other consecutive entries are s.

Now we have a means for designating those outcome sequences of interest.

Notation: $N(S)$ denotes the number of elements in category S,

$$S = 1, 2, 3, \ldots .$$

There is but one way to observe two successes in two trials so that category one contains the one element (s,s). Also, category two contains one element (f,s,s). The value of $N(3)$ is determined by appending an f to the left of every element in category two and then an s to the left of each element in category two beginning with an f. Thus, category three has two elements:

$$(f,f,s,s) \quad \text{and} \quad (s,f,s,s).$$

Observe that this idea of "left-appending may be continued to construct the elements of category $S + 1$ from the elements of category S by appending an f on the left to each element in category S and an s on the left to each element in category S beginning with an f. There can be no elements in category $S + 1$ exclusive of those accounted for by this "left-appending" method.

A result we can observe is that

$$N(S + 1) = N(S) + \text{"the number of } S\text{-category elements that begin with an } f\text{"}$$
$$= N(S) + N(S - 1).$$

So we obtain the amazing result that the recursion formula for category size is the same as the recursion formula for the Fibonacci sequence! Since $N(1) = N(2) = 1$, we see that when $p = .5$ the probability that it will take $S + 1$ trials to observe two successes in a row is given by

$$(N(S)/(2^{S+1})) = (F_S)/(2^{S+1})$$

where F_S denotes entry S in the Fibonacci sequence.

If $p \neq .5$, then each category element must be examined in order to count its exact number of f entries (or s entries). Such an examination is not difficult.

Suppose category $S - 1$ has a_i elements which contain exactly i entries that are f, and that category S has b_i elements which contain exactly i entries that are f, $i = 0, 1, 2, \ldots, S - 2$. Then category $S + 1$ contains exactly $a_i + b_i$ elements which contain exactly $i + 1$ entries that are f. Justification for this statement comes quickly as a benefit of the "left-appending" approach to the problem. Hence, we can construct the following partial table:

Category	Number of Elements Containing Exactly i Entries Which Are f							
$i =$	0	1	2	3	4	5	6	...
1	1	0	0	0	0	0	0	
2	0	1	0	0	0	0	0	
3	0	1	1	0	0	0	0	
4	0	0	2	1	0	0	0	
5	0	0	1	3	1	0	0	
6	0	0	0	3	4	1	0	
7	0	0	0	1	6	5	1	
⋮								

Observe that nonzero entries of the successive columns are the successive rows of the familiar Pascal triangle! This observation is particularly useful because the kth entry of the ith row in the Pascal triangle is

$$\binom{i-1}{k-1} = \frac{(i-1)!}{((i-1)-(k-1))!(k-1)!}.$$

Also, since category i contains exactly one element containing $i - 1$ entries which are f, we know the ith row of the Pascal triangle will always begin in row i and column $i - 1$ of the table. Thus, if we move along the nonzero entries of row t of the table (from left to right) we encounter the following successive numbers:

$$\binom{t-1}{0}, \binom{t-2}{1}, \binom{t-3}{2}, \ldots, \binom{a}{b}.$$

To characterize $\binom{a}{b}$, notice that row k of the Pascal triangle ends in row $2k - 1$ of the table. Thus, if $t > 1$ is odd, then $a = b = (t-1)/2$. And if $t > 1$ is even, then $a = t/2$ and $b = (t/2) - 1$.

Thus, whenever $t > 1$, we know that the probability that "it takes $t + 1$ trials" is given by

$$\sum_{i=0}^{(t-X)/2} \binom{t-(i+1)}{i} (1-p)^{t-(i+1)} p^{(t+1)-(t-(i+1))},$$

where $X = \begin{cases} 1, & \text{if } t \text{ is odd} \\ 2, & \text{if } t \text{ is even} \end{cases}$

THE GENERAL CASE

Now we will be answering the question of the probability that it takes k trials to observe n successes in a row, $k \geq n$. To begin, we generalize the concepts of category, Fibonacci sequence, and Pascal triangle.

Definition: Category x is the set of all $n + (x - 1)$ sequences of f's and s's (denoting failure and success, respectively) such that the last n entries in each sequence are s, and no other n consecutive entries in the sequence are s.

Definition: The nth order Fibonacci-T sequence, denoted f^n, is the sequence $a_1, a_2, a_3, \ldots, a_i, \ldots$, where $a_1 = 1$ and

$$a_i = \begin{cases} \displaystyle\sum_{k=1}^{(i-1)} a_k, & \text{if } 2 \leq i \leq n \\ \displaystyle\sum_{k=i-n}^{(i-1)} a_k, & \text{if } i > n. \end{cases}$$

It is instructive to first define the nth order Pascal-T triangle by example:

(1) If $n = 2$, the Pascal-T triangle is the familiar Pascal triangle;

(2) If $n = 3$, the Pascal-T triangle is of the form

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & 1 & 1 & & & & \\
 & & & 1 & 2 & 3 & 2 & 1 & & & \\
 & & 1 & 3 & 6 & 7 & 6 & 3 & 1 & & \\
 & 1 & 4 & 10 & 16 & 19 & 16 & 10 & 4 & 1 & \\
1 & 5 & 15 & 30 & 45 & 51 & 45 & 30 & 15 & 5 & 1
\end{array}$$

(3) If $n = 4$, the Pascal-T triangle is of the form

$$\begin{array}{cccccccccc}
 & & & & 1 & & & & & \\
 & & & 1 & 1 & 1 & 1 & & & \\
 & & 1 & 2 & 3 & 4 & 3 & 2 & 1 & \\
1 & 3 & 6 & 10 & 12 & 12 & 10 & 6 & 3 & 1
\end{array}$$

The nth order Pascal-T triangle has $(j - 1)n - (j - 2)$ entries in the jth row. Letting the first to last of these be denoted by $j_1, j_2, j_3, \ldots, j_{(j-1)n-(j-2)}$, the kth entry in row $j + 1$ is given by

$$\sum_{i=\max(1,k-n+1)}^{\min(k,(j-1)n-(j-2))} j_i \quad \text{for } k = 1, 2, 3, \ldots, jn - (j - 1).$$

We can now proceed by enlisting the "left-appending" procedure outlined earlier. There is but one way to observe n successes in n trials. So $N(1) = 1$. Likewise, there is but one element in category two. To obtain the elements of category three, we append an f to the left of each element in category two and then append an s to the left of each element in category two. So category three contains the two elements

$$(f,f,s,s,\ \ldots,\ s) \quad \text{and} \quad (s,f,s,s,\ \ldots,\ s)$$

where $s,s,\ \ldots,\ s$ signifies that the entry s occurs n times in succession. We may proceed in this manner for each category k, $k \leq n + 1$.

It is clear that category $n + 1$ will contain exactly one element which has the entry s in its first $n - 1$ positions. Thus, category $n + 2$ will have $2(N(n + 1)) - 1$ elements.

Now note that when constructing category $k + n$, we proceed by appending an f to the left of each element in category $(k + n) - 1$ and an s to the left of each element in category $(k + n) - 1$ which does not begin with the entry s in its first $n - 1$ positions. But the number of elements in category $(k + n) - 1$ containing the entry s in their first $n - 1$ positions is the same as the number of elements in category k which begin with an f! Hence,

$$\begin{aligned} N(n + k) &= 2(N(n + k - 1)) - \text{"number of elements in category } k \text{ which begin with an } f\text{"} \\ &= 2N(n + k - 1) - N(k - 1). \end{aligned}$$

We now prove the following useful

Theorem:

$$N(n + k) = \sum_{i=1}^{n} N(n + k - i),\ k = 1,\ 2,\ 3,\ \ldots$$

Proof: We use simple induction.

(1) $$\begin{aligned} N(n + 1) = 2^{n-1} &= 1 + \sum_{i=2}^{n} 2^{i-2} \\ &= N(1) + (N(2) + N(3) + N(4) + \cdots + N(n)) \\ &= \sum_{i=1}^{n} N(n + 1 - i). \end{aligned}$$

(2) Supposing truth for the case k, we have

$$\begin{aligned} N(n + k) + 1 = 2N(n + k) - N(k) &= 2\sum_{i=1}^{n} N(n + k - i) - N(k) \\ &= \sum_{i=1}^{n-1} N(n + k - i) + \sum_{i=1}^{n} N(n + k - i) \\ &= \sum_{i=1}^{n-1} N(n + k - i) + N(n + k) \\ &= \sum_{i=1}^{n} N[(n + k) + 1 - i]. \blacksquare \end{aligned}$$

Now note that since $N(1) = 1$, the sequence $N(1)$, $N(2)$, $N(3)$, ... is an nth order Fibonacci-T sequence via the theorem!

Thus, if $p = .5$, then the probability that it will take $n + (k - 1)$ trials to observe n successes in a row, $k \geq 1$, is given by

$$N(k)/(2^{n+k-1}) = (f_k^n)/(2^{n+k-1}),$$

where f_k^n denotes the kth entry in the nth order Fibonacci-T sequence.

We will now determine the probabilities when $p \neq .5$. A foundation is set by observing that if category $k - n + i$ has an element M which has exactly x entries that are f, then the element $(s, s, \ldots, s, f, M)$, beginning with $n - (i + 1)$ entries which are s, is a member of category k and it contains $x + 1$ entries that are f. This is true for $i = 0, 1, 2, \ldots, n - 1$. If we let a_i, $i = 0, 1, 2, \ldots, n - 1$ represent the number of elements in category $k - n + 1$ which have x elements that are f, then category k contains $a_0 + a_1 + a_2 + \cdots + a_{n-1}$ elements which have $x + 1$ entries that are f. This is the recursive building block for the nth order Pascal-T triangle where row i begins in category i and ends in category $(i - 1)n + 2$! The following table partially displays the situation.

Category	Number of Elements Containing Exactly i Entries Which Are f				
	$i =$ 0	1	2	3	...
1	1	0	0	0	
2	0	1	0	0	
3	0	1	1	0	
4	0	1	2	1	
5	0	1	3	3	
$\vdots$	$\vdots$	$\vdots$			
$n + 1$	0	1			
$n + 2$	0	1	$\vdots$		
$n + 3$	0	0			
$\vdots$	$\vdots$	$\vdots$		$\vdots$	
$2n$	0	0	3		
$2n + 1$	0	0	2		
$2n + 2$	0	0	1		
$2n + 3$	0	0	0		
$\vdots$	$\vdots$	$\vdots$	$\vdots$		
$3n + 1$	0	0	0	3	
$3n + 2$	0	0	0	1	
$3n + 3$	0	0	0	0	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Since the number of entries in two successive rows of the nth order Pascal-T triangle always differ by n, then moving from left to right in the table, the ith category row will see its first nonzero entry in column $m - 1$ where $(m - 2)n + 2 \leq i \leq (m - 1)n + 1$, $i > 1$ and $m > 1$.

Let $\begin{bmatrix} i \\ k \end{bmatrix}_n$ denote the kth entry in the ith row of the nth order Pascal-T triangle, $k = 1, 2, 3, \ldots, (i - 1)n - (i - 2)$. Suppose $i \geq 2$. Then the successive nonzero entries in the ith category row, listing from right to left are

$$\begin{bmatrix} i \\ 1 \end{bmatrix}_n, \begin{bmatrix} i-1 \\ 2 \end{bmatrix}_n, \begin{bmatrix} i-2 \\ 3 \end{bmatrix}_n, \ldots, \begin{bmatrix} i-(i-m) \\ (i-m)+1 \end{bmatrix}_n$$

where $(m - 2)n + 2 \leq i \leq (m - 1)n + 1$ for some $m \geq 2$.

Thus, the probability that "it will take $n + (i - 1)$ trials," $i \geq 2$, is given by

$$\sum_{k=0}^{i-m} \begin{bmatrix} i-k \\ k+1 \end{bmatrix} (1 - p)^{(i-k)-1} p^{n+(i-1)-((i-k)-1)}$$

where $(m - 2)n + 2 \leq i \leq (m - 1)n + 1$ for some $m \geq 2$.

AUTHOR'S NOTE

The machinery used in the above solution generates a number of ideas which the reader may wish to explore. A few examples are:

1. If f_k^2 denotes the kth entry in the second order Fibonacci-T sequence, then it can be shown that the sequence $\left\{f_{k+1}^2/f_k^2\right\}$ is a Cauchy sequence and so being, has a limit g_2. From this, it follows that $g_2 = 1 + 1/g_2$ so that g_2 is the golden ratio. This brings up the question of the identity of $g_n = \lim_{k\to\infty} f_{k+1}^n/f_k^n$ when $n \geq 3$. (Here, f_k^n denotes the kth entry in the nth order Fibonacci-T sequence.) It can be argued that $g_n <$ 2 for any value of n and $\lim_{n\to\infty} g_n = 2$.

2. It has been shown that
$$f_k^2 = \left[(g_2)^k - (-g_2)^{-k}\right]/\left[g_2 + (g_2)^{-1}\right].$$
Can we find a similar expression for f_k^n when $n \geq 3$?

3. We can generalize the nth order Fibonacci-T sequence by specifying the first n entries arbitrarily. For instance, the first three cases would be
$$\begin{aligned} n = 1&: \; a, a, a, a, a, a, \ldots; \\ n = 2&: \; a, b, a+b, a+2b, 2a+3b, 3a+5b, \ldots; \\ n = 3&: \; a, b, c, a+b+c, a+2(b+c), 2a+3(b+c)+c, \ldots, \end{aligned}$$
where a, b, and c are arbitrarily chosen. The investigation of the properties and relationships between these generalized sequences could provide some interesting results.

REFERENCE

H. S. M. Coxeter, *Introduction to Geometry*, 1969, pp. 166, 167.

*****

SOME CONGRUENCES INVOLVING GENERALIZED FIBONACCI NUMBERS

CHARLES R. WALL
University of South Carolina, Columbia S.C. 29208

1. INTRODUCTION

Throughout this paper, let $\{H_n\}$ be the generalized Fibonacci sequence defined by

(1) $$H_0 = q, \quad H_1 = p, \quad H_{n+1} = H_n + H_{n-1},$$

and let $\{V_n\}$ be the generalized Lucas sequence defined by

(2) $$V_n = H_{n+1} + H_{n-1}.$$

If $q = 0$ and $p = 1$, $\{H_n\}$ becomes $\{F_n\}$, the Fibonacci sequence, and $\{V_n\}$ becomes $\{L_n\}$, the Lucas sequence. We use the recursion formula to extend to negative subscripts the definition of each of these sequences.

Our purpose here is to examine several consequences of the identities

(3) $$H_{n+r} + (-1)^r H_{n-r} = L_r H_n$$

and

(4) $$H_{n+r} - (-1)^r H_{n-r} = F_r V_n,$$

both of which were given several years ago in my master's thesis [12]. Identity (3) has been reported several times: by Tagiuri [5], by Horadam [8], and more recently by King and Hosford [10]. However, identity (4) seems to have escaped attention.

We will first establish identities (3) and (4), and then show how they can be used to solve several problems which have appeared in these pages in the past. We close with a generalization of the identities.

2. PROOF OF THE IDENTITIES

The Binet formulas

$$F_n = (\alpha^n - \beta^n)/\sqrt{5} \quad \text{and} \quad L_n = \alpha^n + \beta^n,$$

where $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$, easily generalize to

$$H_n = (A\alpha^n - B\beta^n)/\sqrt{5} \quad \text{and} \quad V_n = A\alpha^n + B\beta^n,$$

where $A = p - q\beta$ and $B = p - q\alpha$. Any of these formulas may be obtained easily by standard finite difference techniques, or may be verified by induction.

Since $\alpha\beta = -1$, we have

$$\begin{aligned} H_{n+r} + (-1)^r H_{n-r} &= \left\{A\alpha^{n+r} - B\beta^{n+r} + \alpha^r\beta^r A\alpha^{n-r} - \alpha^r\beta^r B\beta^{n-r}\right\}/\sqrt{5} \\ &= \left\{A\alpha^n\alpha^r + A\alpha^n\beta^r - B\beta^n\alpha^r - B\beta^n\beta^r\right\}/\sqrt{5} \\ &= \left\{\alpha^r + \beta^r\right\}\cdot\left\{A\alpha^n - B\beta^n\right\}/\sqrt{5} \\ &= L_r H_n. \end{aligned}$$

Therefore, (3) is established.

Similarly,

$$\begin{aligned} H_{n+r} - (-1)^r H_{n-r} &= \left\{A\alpha^{n+r} - B\beta^{n+r} - \alpha^r\beta^r A\alpha^{n-r} + \alpha^r\beta^r B\beta^{n-r}\right\}/\sqrt{5} \\ &= \left\{A\alpha^n\alpha^r + B\beta^n\alpha^r - A\beta^n\alpha^r - B\beta^n\beta^r\right\}/\sqrt{5} \\ &= \left\{A\alpha^n + B\beta^n\right\}\cdot\left\{\alpha^r - \beta^r\right\}/\sqrt{5} \\ &= F_r V_n, \end{aligned}$$

so (4) is also verified.

3. CONSEQUENCES OF THE IDENTITIES

It is sometimes more convenient to rewrite identities (3) and (4) as

$$H_{k+2h} - H_k = \begin{cases} L_h H_{k+h} & (h \text{ odd}) \\ F_h V_{k+h} & (h \text{ even}) \end{cases} \tag{5}$$

and

$$H_{k+2h} + H_k = \begin{cases} F_h V_{k+h} & (h \text{ odd}) \\ L_h H_{k+h} & (h \text{ even}). \end{cases} \tag{6}$$

In the discussion which follows, it is helpful to remember that:

i. If $H_n = F_n$, then $V_n = L_n$.

ii. If $H_n = L_n$, then $V_n = 5F_n$.

iii. For all k, F_n divides F_{nk}.

iv. If k is odd, then L_n divides L_{nk}.

By (5), we have

$$H_{n+24} - H_n = F_{12}V_{n+12} = 144V_{n+12}.$$

Therefore, with $H_n = F_n$,

$$F_{n+24} \equiv F_n \pmod 9,$$

as asserted in problem B-3 [9].

Direct application of (5) yields

$$H_{n+4m+2} - H_n = L_{2m+1}H_{n+2m+1}$$

so that

$$F_{n+4m+2} - F_n = L_{2m+1}F_{n+2m+1},$$

as claimed in problem B-17 [13].

Since $L_0 = 2$, identity (4) gives us

$$\begin{aligned} L_{2k} - 2(-1)^k &= L_{k+k} - (-1)^k L_{k-k} \\ &= F_k(5F_k) = 5F_k^2. \end{aligned}$$

Therefore, $L_{2k} \equiv 2(-1)^k \pmod 5$, which was the claim of problem B-88 [14].

If k is odd, then (5) tells us that

$$H_{nk+2k} - H_{nk} = L_k H_{nk+k},$$

so

$$F_{(n+2)k} \equiv F_{nk} \pmod{L_k} \quad (k \text{ odd})$$

as asserted in problem B-270 [6].

By (6) we have

$$F_{8n-4} + F_{8n} + F_{8n+4} = F_n + F_{8n+4} + F_{8n-4}$$
$$= F_{8n} + L_4 F_{8n} = (1 + 7)F_{8n} = 8F_{8n}.$$

Since $21 = F_8$ divides F_{8n}, it follows that

$$F_{8n-4} + F_{8n} + F_{8n+4} \equiv 0 \pmod{168}$$

as claimed in problem B-203 [7].

In problem B-31 [11], Lind asserted that if n is even, then the sum of $2n$ consecutive Fibonacci numbers is divisible by F_n. We will establish a stronger result. Horadam [8] showed that

$$H_1 + H_2 + \cdots + H_{2n} = H_{2n+2} - H_2.$$

If n is even, then by (5) we have

$$H_1 + H_2 + \cdots + H_{2n} = H_{2n+2} - H_2 = F_n V_{n+2},$$

which is clearly divisible by F_n. Because the sum of $2n$ consecutive generalized Fibonacci numbers is the sum of the first $2n$ terms of another generalized Fibonacci sequence (obtained by a simple shift), Lind's result holds for generalized Fibonacci numbers. In addition, we may similarly conclude from (5) that if n is odd, the sum of $2n$ consecutive generalized Fibonacci numbers is divisible by L_n.

By (5),

$$H_{2n(2k+1)} - H_{2n} = H_{2n+4nk} - H_{2n}$$
$$= F_{2nk} V_{2n+2nk} = F_{2nk} V_{2n(k+1)}.$$

Therefore (with $H_n = L_n$ and $V_n = 5F_n$)

$$L_{2n(2k+1)} - L_{2n} = 5F_{2nk} F_{2n(k+1)},$$

so not only is it true that

$$L_{2n(2k+1)} \equiv L_{2n} \pmod{F_{2n}},$$

as asserted in problem B-277 [1], but indeed

$$L_{2n(2k+1)} \equiv L_{2n} \pmod{F_{2n}^2}$$

since F_{2n} divides both F_{2nk} and $F_{2n(k+1)}$.

In a similar fashion,

$$H_{(2n+1)(4k+1)} - H_{2n+1} = H_{2n+1+4k(2n+1)} - H_{2n+1}$$
$$= F_{2k(2n+1)} V_{2n+1+2k(2n+1)}$$
$$= F_{2k(2n+1)} V_{(2k+1)(2n+1)}$$

so that

$$L_{(2n+1)(4k+1)} - L_{2n+1} = 5F_{2k(2n+1)} F_{(2k+1)(2n+1)}.$$

Therefore,

$$L_{(2n+1)(4k+1)} \equiv L_{2n+1} \pmod{F_{2n+1}^2}$$

and in particular

$$L_{(2n+1)(4k+1)} \equiv L_{2n+1} \pmod{F_{2n+1}}$$

as claimed in problem B-278 [2].

Also,

$$\begin{aligned} H_{2n(4k+1)} - H_{2n} &= H_{2n+8nk} - H_{2n} \\ &= F_{4nk} V_{2n+4nk} \\ &= F_{4nk} V_{2n(2k+1)}. \end{aligned}$$

Therefore,

$$F_{2n(4k+1)} - F_{2n} = F_{4nk} L_{2n(2k+1)},$$

so

$$F_{2n(4k+1)} \equiv F_{2n} \pmod{L_{2n(2k+1)}}.$$

Since L_{2n} divides $L_{2n(2k+1)}$, we have

$$F_{2n(4k+1)} \equiv F_{2n} \pmod{L_{2n}},$$

which establishes problem B-288 [3].

Now let us consider

$$H_{(2n+1)(2k+1)} - H_{2n+1} = H_{2n+1+2k(2n+1)} - H_{2n+1}.$$

By (5) we have

$$\begin{cases} L_{k(2n+1)} H_{(k+1)(2n+1)} & \text{if } k \text{ is odd,} \\ F_{k(2n+1)} V_{(k+1)(2n+1)} & \text{if } k \text{ is even.} \end{cases}$$

Therefore

$$F_{(2n+1)(2k+1)} - F_{2n+1} = \begin{cases} L_{k(2n+1)} F_{(k+1)(2n+1)} & \text{if } k \text{ is odd} \\ F_{k(2n+1)} L_{(k+1)(2n+1)} & \text{if } k \text{ is even.} \end{cases}$$

If k is odd, $L_{k(2n+1)}$ is divisible by L_{2n+1}; if k is even, then $k+1$ is odd, so L_{2n+1} divides $L_{(k+1)(2n+1)}$. Hence, in any case,

$$F_{(2n+1)(2k+1)} \equiv F_{2n+1} \pmod{L_{2n+1}},$$

which was the claim in problem B-289 [4].

Finally, we note that adding (3) and (4) yields

$$F_{n+r} = (L_r F_n + F_r L_n)/2$$

if $H_n = F_n$ (and $V_n = L_n$), and

$$L_{n+r} = (L_r L_n + 5F_r F_n)/2$$

if $H_n = L_n$ (and $V_n = 5F_n$). Subtraction of the same two identities gives us

$$F_{n-r} = (-1)^r (L_r F_n - F_r L_n)/2$$

and

$$L_{n-r} = (-1)^r (L_r L_n - 5F_r F_n)/2.$$

These results appear to be new.

4. GENERALIZATION OF THE IDENTITIES

Let $\{u_n\}$ be the generalized second order recurring sequence defined by

$$u_0 = q, \quad u_1 = p, \quad u_{n+1} = gu_n + hu_{n-1},$$

where $g^2 + 4h \neq 0$ (to avoid having repeated roots of the associated finite difference equation). Define $\{v_n\}$ by

$$v_n = u_{n+1} + hu_{n-1},$$

let $\{s_n\}$ be defined by

$$s_0 = 0, \quad s_1 = 1, \quad s_{n+1} = gs_n + hs_{n-1},$$

and let $\{t_n\}$ be defined by

$$t_n = s_{n+1} + hs_{n-1}.$$

Extend each sequence to negative subscripts by means of the recurrence relation.

Then if

$$\alpha = \left(g + \sqrt{g^2 + 4h}\right)/2 \quad \text{and} \quad \beta = \left(g - \sqrt{g^2 + 4h}\right)/2,$$

the Binet-like identities are easy to prove:

$$s_n = (\alpha^n - \beta^n)/(\alpha - \beta)$$
$$t_n = \alpha^n + \beta^n$$
$$u_n = (A\alpha^n - B\beta^n)/(\alpha - \beta)$$
$$v_n = A\alpha^n + B\beta^n,$$

where $A = p - q\beta$ and $B = p - q\alpha$.

Then it is a simple matter to establish that

$$u_{n+r} + (-h)^r u_{n-r} = t_r u_n$$

and

$$u_{n+r} - (-h)^r u_{n-r} = s_r v_n.$$

REFERENCES

1. P. Bruckman, Problem B-277, *The Fibonacci Quarterly* 12, No. 2 (1974):101.
2. P. Bruckman, Problem B-278, *The Fibonacci Quarterly* 12, No. 2 (1974):101.
3. P. Bruckman, Problem B-288, *The Fibonacci Quarterly* 12, No. 4 (1974):313.
4. P. Bruckman, Problem B-289, *The Fibonacci Quarterly* 12, No. 4 (1974):313.
5. L. Dickson, *History of the Theory of Numbers*, Vol. I (Chelsea, 1952), p. 404.
6. H. Freitag, Problem B-270, *The Fibonacci Quarterly* 11, No. 6 (1973):550.
7. R. Grassi, Problem B-203, *The Fibonacci Quarterly* 9, No. 2 (1971):106.
8. A. Horadam, "A Generalized Fibonacci Sequence," *Amer. Math. Monthly* 68 (1961);455-459.
9. J. Householder, Problem B-3, *The Fibonacci Quarterly* 1, No. 1 (1963):73.
10. J. King & P. Hosford, Problem E2497, *Amer. Math. Monthly* 81 (1974):902.
11. D. Lind, Problem B-31, *The Fibaoncci Quarterly* 2, No. 1 (1964):72.
12. C. Wall, "Sums and Differences of Generalized Fibonacci Numbers" (Master's thesis, Texas Christian University, 1964).
13. C. Wall, Problem B-17, *The Fibonacci Quarterly* 1, No. 1 (1963):75.
14. J. Wessner, Problem B-88, *The Fibonacci Quarterly* 4, No. 2 (1966):190.

*****

ENUMERATION OF TRUNCATED LATIN RECTANGLES

F. W. LIGHT, JR.

229 W. Swatara Dr., P.O. Box 276, Jonestown, PA 17038

NOMENCLATURE

An $r \times k$ *rectangle* is a rectangular array of *elements* (natural numbers) with r rows and k columns. A row with no repeated element is an *R-row*. A column with no repeated element is a C-column; otherwise, it is a $\overline{C}$-column. If all rows of a rectangle are R-rows, it is an *R-rectangle*. An R-rectangle subject to no further restrictions will be called, for emphasis, *free*. One whose first row is prescribed (elements arranged in increasing numerical order) is a *normalized* R-rectangle.

An R-rectangle all of whose columns are C-columns is an *R-C-rectangle*; one whose columns are all $\overline{C}$-columns is an *R-$\overline{C}$-rectangle*. An $r \times n$ R-C-rectangle each of whose rows consists of the same n elements is a *Latin rectangle* (L-rectangle). (R-C-rectangles whose rows do not all consist of the same elements are the "truncated" L-rectangles of the title.)

ENUMERATION OF CERTAIN R-RECTANGLES

The most obvious enumerational question about L-rectangles is, probably: How many distinct normalized $r \times n$ L-rectangles are there? Denoting this number as M_n^r, we have, as in [1],

$$M_n^r = \sum_{k=0}^{n} (-1)^k \frac{\alpha_{r,n}^k}{k!}[(n-k)!]^{r-1}, \tag{1}$$

where $\alpha_{r,n}^k$ is the number of free $r \times k$ R-$\overline{C}$-rectangles that can be built up with $\overline{C}$-columns constructed from elements selected from r rows each of which consists of the elements $1, 2, \ldots, n$.

The number of free $r \times n$ L-rectangles is

$$N_n^r = \sum_{s=0}^{n} (-1)^s \binom{n}{s} [(n-s)!]^r \alpha_{r,n}^s, \tag{2}$$

since $N_n^r = n!M_n^r$.

Such formulas are effective numerically, of course, only if all the $\alpha_{r,n}^k$ are known. This is the case for $r \leq 4$, viz. ($\alpha_{r,n}^0 \equiv 1$, by definition):

$\alpha_{1,n}^k = 0$ for all $k > 0$ and all n.

$\alpha_{2,n}^k = n^{(k)}$, where $n^{(k)} = n(n-1) \ldots (n-k+1)$, a notation used throughout this report.

$\alpha_{3,n}^k = n(3n-2k)\alpha_{3,n-1}^{k-1} + 2(k-1)n(n-1)\alpha_{3,n-2}^{k-2}$, a result easily obtained by eliminating the β_i from the pair of formulas given in [1].

$\alpha_{4,n}^k$ may be found by using the 13 recurrences given in [1].

Except for $k \leq 4$ (see below), the $\alpha_{r,n}^k$ for $r > 4$ are, in general, not known.

Consider now R-C-rectangles that are not necessarily L-rectangles. Let

r = number of rows,

m = number of columns ($m \leq n$)

n = number of elements available for each row (the same set of elements for each row).

$N^r_{m,n}$ = number of free R-C-rectangles with the indicated specifications.

We have

$$N^r_{m,n} = \sum_{s=0}^{m} (-1)s\binom{m}{s}[(n-s)^{(m-s)}]^r \alpha^s_{r,n}. \tag{3}$$

Formula (3) may be derived by using the same n^r-cube that was used ([1]) to get the formula for M^r_n. In this instance, we work with only the first m of the structures of highest dimensional level (thus with stripes, if $r = 4$). Proceeding as in the earlier case, and making appropriate adjustments in the multipliers that arise (e.g., if $r = 4$, the number of k-tuples of bad cells in any m ($\geq k$) stripes is now

$$\frac{m^{(k)}}{n^{(k)}}\alpha^k_{4,n};$$

each k-tuple of bad cells combines with $[(n-k)^{(m-k)}]^3$ cells—of any kind), we get a formula for $M^r_{m,n}$ (the normalized counterpart of $N^r_{m,n}$) and finally, since $N^r_{m,n} = n^{(m)}M^r_{m,n}$, formula (3).

The free R-C-rectangles are more convenient in many respects than the normalized ones. It is immediate that there is a reciprosity between m and r:

$$N^r_{m,n} = N^m_{r,n}. \tag{4}$$

Formula (3) may be inverted, to give:

$$\alpha^m_{r,n} = \sum_{s=0}^{m} (-1)^s\binom{m}{s}[(n-s)^{(m-s)}]^r N^r_{s,n}. \tag{5}$$

Formulas (3) and (5) are identical, the self-inversive property being, of course, inherest in the definitions of $\alpha^m_{r,n}$ and $N^r_{m,n}$. By utilizing (4) and (5), we can find $\alpha^m_{r,n}$ for $m \leq 4$, for any values of r and n. Thus, the first few terms of (2) are known for $r > 4$.

A more general formula of the sort discussed above can be given, covering cases in which some columns are C-columns and some are $\overline{C}$-columns. Let

$N^r_{m,k;n}$ = number of free R-rectangles in which:

r = total number of rows,

k = total number of columns,

m = number of C-columns (the other $k - m$ being $\overline{C}$-columns),

n = number of elements available for each row (the same set for each row).

Clearly, $m \leq k \leq n$.

Then

$$N^r_{m,k;n} = \binom{k}{m}\sum_{s=0}^{m}(-1)^s\binom{m}{s}[(n-k+m-s)^{(m-s)}]^r\alpha^{k-m+s}_{r,n}. \tag{6}$$

The derivation resembles that of (3), the diagram for the n^r-cube again being helpful.

A few special cases are:

If $m = 0$, we have $N^r_{0,k;n} = \alpha^k_{r,n}$.

If $m = k$, we have $N^r_{m,m;n} = N^r_{m,n}$.

If $k = n$, we have $N^r_{m,n;n}$, the number of free $r \times n$ R-rectangles each of whose rows consists of the elements 1, 2, ..., n, having m C-columns and $n - m$ $\overline{C}$-columns.

Note that $N^r_{m,k;n}$ is divisible by $k!$ (giving the number of normalized R-rectangles with the specified properties). That result is further divisible by $\binom{k}{m}$ (giving the number of normalized R-rectangles with the m C-columns preceding the $k - m$ $\overline{C}$-columns). That result is still further divisible by $\binom{n}{k}$ (giving the number of normalized R-rectangles whose C-columns start with 1, 2, ..., m in that order, and whose $\overline{C}$-columns start with $m + 1$, $m + 2$, ..., k in that order). Thus, $N^r_{m,k;n}$ is divisible by $\binom{k}{m}n^{(k)}$. For example, if $r = 2$, $k = 5$, $m = 3$, $n = 6$,

$N^2_{3,5;6} = 79{,}200$, the number of free R-rectangles;

$\dfrac{79{,}200}{5!} = 660$, the number of normalized R-rectangles;

$\dfrac{660}{\binom{5}{3}} = 66$, the number with C-columns preceding $\overline{C}$-columns;

and finally,

$\dfrac{66}{\binom{6}{5}} = 11$, the number with 3 C-columns headed by 1, 2, 3 and 2 $\overline{C}$-columns headed by 4, 5 in that order, as may be verified easily by direct count.

REFERENCE

1. F. W. Light, Jr., "A Procedure for the Enumeration of $4 \times n$ Latin Rectangles," *The Fibonacci Quarterly* 11, No. 3 (1973):241-246.

*****

THE NORMAL MODES OF A HANGING OSCILLATOR OF ORDER N

JOHN BOARDMAN
Brooklyn College, Brooklyn N.Y. 11210

ABSTRACT

The normal frequencies are computed for a system of N identical oscillators, each hanging from the one above it, and the highest oscillator hanging from a fixed point. These frequencies are obtainable from the roots of the Chebyshev polynomials of the second kind.

A massless spring of harmonic constant k is suspended from a fixed point, and from it is suspended a mass m. This system will oscillate with an angular frequency $\omega_0 = (k/m)^{1/2}$. If N such oscillators are thus suspended, each one from the one above it, we will call this system a hanging oscillator of order N.

The Lagrangian for this system is

$$L(q_1, \ldots, q_n, \dot{q}_1, \ldots, \dot{q}_n) = \frac{1}{2} m \sum_{i=1}^{N} \dot{q}_1^2 - \frac{1}{2} k q_1^2 - \frac{1}{2} k \sum_{i=2}^{N} (q_i - q_{i-1})^2, \tag{1}$$

where q_i is the displacement of the ith mass from its equilibrium position. This Lagrangian can also be written in the language of matrix algebra as

$$L = \frac{1}{2} m \dot{q}^T T \dot{q} - \frac{1}{2} m \omega_0^2 q^T U q \tag{2}$$

where q and $\dot{q}$ are, respectively, the column vectors $\mathrm{col}(q_1, q_2, \ldots, q_N)$ and $\mathrm{col}(\dot{q}_1, \dot{q}_2, \ldots, \dot{q}_N)$. It is obvious that $T = I$, where I is the $N \times N$ identity matrix. For U, we state the following theorem.

Theorem 1: $u_{ii} = 2$ and $u_{i,i+1} = u_{i+1,i} = -1$ for $i = 1, 2, \ldots, N - 1$; $u_{NN} = 1$, and all other values of u_{ij} are zero.

This can be demonstrated by mathematical induction. It is obvious for $N = 1$. For $N = n$ the last two terms in (1) are

$$-\frac{1}{2} m \omega_0^2 (q_{n-1} - q_{n-2})^2 - \frac{1}{2} m \omega_0^2 (q_n - q_{n-1})^2. \tag{3}$$

From these terms come the matrix elements $u_{n-1,n-1} = 2$, $u_{n-1,n} = u_{n,n-1} = -1$, $u_{nn} = 1$. For $N = n + 1$, these terms are added to (1):

$$\frac{1}{2} m \dot{q}_{n+1}^2 - \frac{1}{2} m \omega_0^2 (q_{n+1} - q_n)^2. \tag{4}$$

The matrix element u_{nn} is now increased to 2, and the additional elements $u_{n,n+1} = u_{n+1,n} = -1$, $u_{n+1,n+1} = 1$ now appear in the new $(n + 1) \times (n + 1)$ matrix U.

The characteristic function for this problem is $\det(-m\omega^2 T + m\omega_0^2 U)$. If we let $x = \omega/\omega_0$, then the normal frequencies for a hanging oscillator of order N are given by the N positive roots of the polynomial $\det(-x^2 I + U) = 0$. Each of the diagonal elements of this determinant is $(-x^2 + 2)$ except for the last, which is $(-x^2 + 1)$. The only other nonzero elements are those immediately next to the diagonal elements; they are each -1.

In the solution of this problem, the Fibonacci polynomials [1] will be useful. These polynomials are defined by the recurrence relation

$$F_{n+2}(x) = xF_{n+1}(x) + F_n(x), \text{ where } F_1(x) = 1 \text{ and } F_2(x) = x.$$

By repeated application of this recurrence relation, we can prove:

Theorem 2: $F_{n+4}(x) = (x^2 + 2)F_{n+2}(x) - F_n(x)$.

Theorem 2 can be used to prove:

Theorem 3: The characteristic function for the hanging oscillator of order N is

$$(m\omega_0^2)^N F_{2N+1}(ix). \tag{5}$$

The factor $(m\omega_0^2)^N$ comes out of the determinant, leaving $\det(-x^2I + U)$. Theorem 3 thus reduces to the evaluation of the determinant

$$|V| = \begin{vmatrix} -x^2+2 & -1 & 0 & \dots & 0 & 0 \\ -1 & -x^2+2 & -1 & \dots & 0 & 0 \\ 0 & -1 & \ddots & & \vdots & \vdots \\ \vdots & \vdots & & \ddots & -1 & 0 \\ 0 & 0 & \dots & -1 & -x^2+2 & -1 \\ 0 & 0 & \dots & 0 & -1 & -x^2+1 \end{vmatrix} \tag{6}$$

to show that it equals $F_{2N+1}(ix)$.

If $N = 1$, Theorem 3 obviously holds, and $F_3(x) = -x^2 + 1$. Let us assume that the determinant (6) is $F_{2n+1}(ix)$ for $N = n$. Then for $N = n + 1$ we will expand the determinant by minors. It is v_{11} times the minor of v_{11} minus v_{12} times the minor of v_{12}. But the minor of $v_{11} = -x^2 + 2$ is the characteristic function $F_{2n+1}(ix)$ for $N = n$. The minor of v_{12} is (-1) times the characteristic function $F_{2n-1}(ix)$ for $N = n - 1$. The determinant (6) is therefore

$$(-x^2 + 2)F_{2n+1}(ix) - F_{2n-1}(ix),$$

which by Theorem 2 is equal to

$$F_{2(n+1)+1}(ix).$$

Theorem 3 is thus proved by mathematical induction.

Theorem 4: The characteristic frequencies of a hanging oscillator of order N are

$$\omega_0 x_j = \omega_j = 2\omega_0 \cos\frac{j\pi}{2N+1}, \quad j = 1, 2, \dots, N. \tag{7}$$

The Fibonacci polynomials and the Chebyshev polynomials of the second kind $U_N(x)$ are related by [2]:

$$F_{N+1}(x) = i^{-N}U_N\left(\frac{1}{2}ix\right). \tag{8}$$

The Fibonacci polynomials of imaginary argument then become:

$$F_{N+1}(ix) = i^{-N}U_N\left(-\frac{1}{2}x\right) \tag{9}$$

and the Fibonacci polynomials of interest in this problem become:

(10) $$F_{2N+1}(ix) = (-1)^N U_{2N}\left(\frac{1}{2}x\right).$$

The roots of the eigenvalue equation obtained by setting the characteristic function (5) equal to zero are those given by (7) [3]. Theorem 4 is thus proved.

Two interesting special cases present themselves when $2N + 1$ is an integral multiple of 3 or of 5.

If $2N + 1 = 3P$, where P is an integer, then the root corresponding to $j = P$ is $\omega = \omega_0$. Thus, one of the normal frequencies is equal to the frequency of a single oscillator in the combination.

If $2N + 1 = 5Q$, where Q is an integer, then the roots corresponding to $j = Q$ and to $j = 2Q$ are, respectively, $\omega = \phi\omega_0$ and $\omega = \phi^{-1}\omega_0$, where

$$\phi = 1.6180339885\ldots$$

is the larger root of $x^2 - x - 1 = 0$, the famous "golden ratio." This ratio occurs frequently in number theory and in the biological sciences [4], but its appearances in physics are very few, and usually seem contrived [5].

The coordinates q as functions of time are given by [6]

(11) $$q_j(t) = \sum_{k=1}^{N} a_j k \cos\,(\omega_k t - \delta_k)$$

where a_{jk} is the kth component of the eigenvector a_j which correspond to the normal frequency ω_j given by (7). These eigenvectors are obtained from the equation

(12) $$m(-\omega_j^2 T + \omega_0^2 U)a_j = m\omega_0^2(-x_j^2 I + U)a_j = 0,$$

and their components therefore obey the following equations:

(13) $$\begin{aligned} &-2a_{j1} \cos \frac{2j\pi}{2N+1} - a_{j2} = 0; \\ &-a_{j,k-2} - 2a_{j,k-1} \cos \frac{2j\pi}{2N+1} - a_{jk} = 0, \; k = 3, 4, \ldots, N. \end{aligned}$$

The components of a_j are therefore

(14) $$\begin{aligned} a_{j2} &= -2a_{j1} \cos \frac{2j\pi}{2N+1}; \\ a_{jk} &= -2a_{j,k-1} \cos \frac{2j\pi}{2N+1} - a_{j,k-2}, \text{ for } k = 3, 4, \ldots, N. \end{aligned}$$

The components a_{jk} can be evaluated from this recursion relation for the Chebyshev polynomials of the second kind [3, p. 782]:

(15) $$U_k(x) = 2xU_{k-1}(x) - U_{k-2}(x)$$

and we obtain

(16) $$a_{jk} = (-1)^{k-1} a_{j1} U_k\left(\cos \frac{2j\pi}{2N+1}\right),$$

where a_{j1} is arbitrary.

If the initial position and velocity of the jth mass are, respectively, X_j and V_j, then the normal coordinates are [6, p. 431]

$$\zeta_k(t) = Re\sum_{j=1}^{N} ma_{jk}\,e^{i\omega_k t}\left(X_j - \frac{i}{\omega_k}V_j\right) \tag{17}$$

$$= Re\sum_{j=1}^{N} m(-1)^{k-1}a_{j1}U_k\left(\cos\frac{2k\pi}{2N+1}\right)\exp\left[2i\omega_0 t\cos\frac{k\pi}{2N+1}\right] \times\left(X_j - \frac{iV_j}{2\omega_0\cos\frac{k\pi}{2N+1}}\right)$$

REFERENCES

1. M. Bicknell, *The Fibonacci Quarterly* 8, No. 5 (1970):407.
2. V. E. Hoggatt, Jr., & D. A. Lind, *The Fibonacci Quarterly* 5, No. 2 (1967): 141.
3. U. W. Hochstrasser, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables* (U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., 1964), p. 787.
4. M. Gardner, *Scientific American* 201 (1959):128.
5. B. Davis, *The Fibonacci Quarterly* 10, No. 7 (1972):659.
6. J. Marion, *Classical Dynamics of Particles and Systems* (2nd ed.; New York: Academic Press, 1970), p. 425.

*****

CONGRUENCES FOR CERTAIN FIBONACCI NUMBERS

NORVALD MIDTTUN
Norwegian Naval Academy, Post Box 25, Norway

The purpose of this note is to prove some of the well-known congruences for the Fibonacci numbers U_p and U_{p-1}, where p is prime and $p \equiv \pm 1 \pmod 5$. We also prove a congruence which is analogous to

$$U_n = \frac{\alpha^\mu - \beta^\mu}{\alpha - \beta}, \text{ where } \alpha \text{ and } \beta \text{ are the roots of } x^2 - x - 1 = 0.$$

We start by considering the congruence

(1) $x^2 - x - 1 \equiv 0 \pmod p$, which can also be written

(2) $y^2 \equiv 5 \pmod p$,

on putting $2x - 1 = y$.

It is well known that 5 is a quadratic residue of primes of the form $5m \pm 1$ and a quadratic nonresidue of primes of the form $5m \pm 3$. Therefore, (2) has a solution p if p is a prime and $p \equiv \pm 1 \pmod 5$.

It also has $-y$ as a solution, and these solutions are different in the sense that

$$y \not\equiv -y \pmod p.$$

This obviously gives two different solutions x_1 and x_2 of (1).

(1) is now written

(3) $$x^2 \equiv x + 1 \pmod{p},$$

or, which is the same,

$$X^2 \equiv U_1X + U_2 \pmod{p},$$

where U_1 and U_2 are the first and second Fibonacci numbers.

When multiplied by x, (3) gives

$$x^3 \equiv x^2 + x \equiv x + 1 + x \equiv 2x + 1 \pmod{p},$$

or, which is the same,

$$X^3 \equiv U_3X + U_2 \pmod{p}.$$

Suppose, therefore, that

(4) $$X_k \equiv U_kX + U_{k-1} \pmod{p} \text{ for some } k.$$

Now (4) implies

$$X^{k+1} \equiv U_kX^2 + U_{k-1}X \equiv U_k(X + 1) + U_{k-1}X \equiv (U_{k-1} + U_k)X + U_k$$

$$= U_{k+1}X + U_k \pmod{p},$$

which, together with (3) shows that (4) holds for $k \geq 2$.

For the two solutions x_1 and x_2, we now have

$$X_1^k \equiv U_kX_1 + U_{k-1} \pmod{p}$$

and

$$X_2^k \equiv U_kX_2 + U_{k-1} \pmod{p}.$$

Subtraction gives

(5) $$X_1^k - X_2^k \equiv U_k(X_1 - X_2) \pmod{p}.$$

Putting $k = p - 1$ in (5) and using Fermat's theorem, we get

$$X_1^{p-1} - X_2^{p-1} \equiv U_{p-1}(X_1 - X_2) \equiv 1 - 1 = 0 \pmod{p}.$$

Since $X_1 \not\equiv X_2 \pmod{p}$, this proves

$$U_{p-1} \equiv 0 \pmod{p}.$$

Putting $k = p$ in (5), we get in the same manner

(6) $$X_1^p - X_2^p \equiv X_1 - X_2 \equiv U_p(X_1 - X_2) \pmod{p},$$

which proves

$$U_p \equiv 1 \pmod{p}.$$

At last, (6) can formally be written

$$U_p \equiv \frac{X_1^p - X_2^p}{X_1 - X_2} \pmod{p},$$

which shows the analogy with the formula

$$U_n = \frac{\alpha^\mu - \beta^\mu}{\alpha - \beta}.$$

*****

SOME DIVISIBILITY PROPERTIES OF GENERALIZED FIBONACCI SEQUENCES

PAUL S. BRUCKMAN

4213 Lancelot Drive, Concord, CA 94521

1. INTRODUCTION

Let c be any square-free integer, p any odd prime such that $(c/p) = -1$, and n any positive integer. The quantity $\sqrt{c}$, which would ordinarily be defined (mod p^n) as one of the two solutions of the congruence: $x^2 \equiv c$ (mod p^n), does not exist. Nevertheless, we may deal with objects of the form $a + b\sqrt{c}$ (mod p^n), where a and b are integers, in much the same way that we deal with complex numbers, the essential difference being that $\sqrt{-1}$'s role is assumed by $\sqrt{c}$. Since we are dealing with congruences (mod p^n), we may without loss of generality restrict a and b to a particular residue class (mod p^n), the most convenient for our purpose being the minimal residue class (mod p^n). Accordingly, we define the sets $R_n(p)$ and $R_n(p,c)$ as follows:

(1) $$R_n(p) = \left\{a : a \text{ an integer, } |a| \le \tfrac{1}{2}(p^n - 1)\right\};$$

(2) $$R_n(p,c) = \left\{z : z = a + b\sqrt{c}, \text{ where } a,b \in R_n(p)\right\}.$$

In the sequel, congruences will be understood to be (mod p^n), unless otherwise indicated, and we will omit the modulus designation, for brevity, provided no confusion is likely to arise. The symbol "$\equiv$" denotes congruence and should not be confused with the identity relation.

We also define the set $R(p,c)$ as follows:

(3) $$R(p,c) = \left\{z : z = a + b\sqrt{c}, \text{ where } a \text{ and } b \text{ are rational numbers whose numerators and denominators are prime to } p\right\}.$$

The set $R_n(p,c)$ satisfies all of the usual laws of algebra, and its elements may be manipulated in much the same way as complex numbers, provided we identify the "real" and "imaginary" parts of $z = a + b\sqrt{c}$, namely a and b, respectively.

If $z = (a + b\sqrt{c}) \in R_n(p,c)$ and $(ab,p) = 1$, then z has a multiplicative inverse in $R_n(p,c)$, denoted by z^{-1}, given by

(4) $$z^{-1} \equiv (a^2 - b^2c)^{-1}(a - b\sqrt{c}),$$

where $(a^2 - b^2c)^{-1}$ is the inverse of $(a^2 - b^2c)$, all operations reduced (mod p^n), in such a manner that $(a^2 - b^2c)$, its inverse, and z^{-1} are in $R_n(p,c)$. The condition $(ab,p) = 1$ is both necessary and sufficient to ensure that z^{-1} exists. Two elements $z_k = a_k + b_k\sqrt{c}$, $k = 1, 2$, of $R(p,c)$ are said to be *congruent (mod p^n)* (or more simply *congruent*) iff $a_1 \equiv a_2$ and $b_1 \equiv b_2$. They are said to be *conjugate* iff $a_1 \equiv a_2$ and $b_1 \equiv -b_2$. Hence, every element of $R_n(p,c)$ has a unique conjugate in $R_n(p,c)$, and every element of $R_n(p)$ is (trivially) self-conjugate.

It is not difficult to show that $R_n(p,c)$, which is the set in which we are really interested, is a commutative ring with identity; moreover, $R_1(p,c)$ is a field.

Next, we recall some basic results of "ordinary" number theory. For all $z \in R_n(p)$, such that $(z,p) = 1$,

(5) $$z^{\frac{1}{2}\phi(p^n)} \equiv \left(\frac{z}{p}\right),$$

(6) $$z^{\phi(p^n)} \equiv 1 \text{ [where } \phi(p^n) = (p-1)p^{n-1} \text{ is the Euler (totient) function].}$$

Note that (5) implies (6), which is a generalization of Fermat's Theorem. A more general formulation of (6) is the following:

(7) $$z^{p^n} \equiv z^{p^{n-1}}, \text{ for all } z \in R_n(p).$$

The following theorem generalizes the last result even further.

Theorem 1: For all $z \in R_n(p,c)$,

(8) $$z^{p^n} \equiv (\bar{z})^{p^{n-1}}.$$

Proof: We will first prove (8) for the case $n = 1$, then proceed by induction on n. Suppose $z = (a + b\sqrt{c}) \in R_n(p,c)$. Then, by the binomial theorem,

$$z^p = (a + b\sqrt{c})^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k}(b\sqrt{c})^k \equiv a^p + (b\sqrt{c})^p \pmod{p},$$

since $p \left| \binom{p}{k} \right.$ for $k = 1, 2, \ldots, p-1$. But $a^p \equiv a$ and $b^p \equiv b \pmod{p}$ [by (7), with $n = 1$]. Since $\left(\frac{c}{p}\right) = -1$, thus $z^p \equiv \bar{z} \pmod{p}$, which is the result of (8) for the case $n = 1$, $[(\sqrt{c})^p = c^{\frac{1}{2}(p-1)}\sqrt{c} \equiv \left(\frac{c}{p}\right)\sqrt{c} = -\sqrt{c}$, by (5)].

Let S denote the set of natural numbers n such that (8) holds for all $z \in R_n(p,c)$. We have just shown that $1 \in S$. Suppose $m \in S$. Then $z^{p^m} = \bar{z}^{p^{m-1}} + wp^m$, for some $w \in R_1(p,c)$. Therefore,

$$(z^{p^m})^p = z^{p^{m+1}} = (\bar{z}^{p^{m-1}} + wp^m)^p \equiv \bar{z}^{p^m} + p\bar{z}^{(p-1)p^{m-1}}wp^m \equiv \bar{z}^{p^m} \pmod{p^{m+1}}.$$

Thus, $m \in S \Rightarrow (m+1) \in S$. The result now follows by induction.

Given any $z = (a + b\sqrt{c}) \in R(p,c)$, there exists a unique

$$z^* = (a^* + b^*\sqrt{c}) \in R_n(p,c),$$

such that $a \equiv a^*$, $b \equiv b^*$, i.e., $z \equiv z^*$. Moreover, $1/z = (a - b\sqrt{c})/(a^2 - b^2c)$ and $(z^*)^{-1}$ both exist and $1/z \equiv (z^*)^{-1}$. These properties may be deduced from the preceding discussion. Therefore, when no confusion is likely to arise, we will omit the "starred" notation in the sequel, and treat elements of $R(p,c)$ as elements of $R_n(p,c)$ interchangeably, though the reader should bear the technical distinction in mind.

2. APPLICATIONS TO GENERALIZED FIBONACCI SEQUENCES

Suppose $u = (a + b\sqrt{c}) \in R(p,c)$, $v = \bar{u} = a - b\sqrt{c}$, where $2a$ is an integer, $(a^2 - b^2c) = \pm 1$. Define the sequences $\{\varphi_k\}$ and $\{\lambda_k\}$ as follows:

(9) $$\varphi_k = \frac{u^k - v^k}{u - v},$$

(10) $\lambda_k = u^k + v^k,\ k = 0, 1, 2, \ldots .$

As is commonly known, the φ's and λ's are integers and satisfy the same recursion:

(11) $\gamma_{k+2} = 2a\gamma_{k+1} + (b^2c - a^2)\gamma_k.$

Note that $b \not\equiv 0 \pmod p$, which implies $(u - v)^{-1} = (2b\sqrt{c})^{-1} \equiv w \in R_n(p,c)$. Hence, we may treat $\{\varphi_k\}$ and $\{\lambda_k\}$ as sequences in $R_n(p)$. By application of Theorem 1, we may deduce certain divisibility properties of these sequences (mod p^n). To illustrate, we prove the following

Theorem 2: Given u and v as defined above, if $m = m(p,n) = (p + 1)p^{n-1}$, then

(12) $\varphi_m \equiv 0$, and

(13) $\lambda_m \equiv 2(a^2 - b^2c).$

Proof: By Theorem 1,

$$u^{p^n} \equiv v^{p^{n-1}},\quad v^{p^n} \equiv u^{p^{n-1}}.$$

Hence,

$$u^{p^n}u^{p^{n-1}} \equiv v^{p^n}v^{p^{n-1}} \equiv (uv)^{p^n},$$

i.e.,

$$u^m \equiv v^m \equiv (a^2 - b^2c)^{p^n} \equiv (a^2 - b^2c).$$

Note that $(u - v)^{-1}$ exists. Hence, applying the definitions in (9) and (10), the result of Theorem 2 now follows.

The preceding theorem eloquently illustrates the power of the method of "complex residues." By dealing with certain nebulous objects of the form $a + b\sqrt{c}$ (mod p^n), which have no "real" meaning in the modular arithmetic, we have deduced some purely number-theoretic results about generalized Fibonacci and Lucas sequences. The analogy with bona fide complex numbers and their applications should now be more evident.

A somewhat stronger result than (13) is actually true, but the method of complex residues does not appear to be of help in such fortification. We will first state the strengthened result, then state and prove a number of lemmas, returning finally to the proof.

Theorem 3: Let u, v, and m be defined as in Theorem 2. Then

(14) $\lambda_m \equiv 2(a^2 - b^2c) \pmod{p^{2n}}.$

Lemma 1: Let λ_k be as given in (10). Then

(15) $$\sum_{i=0}^{[\frac{1}{2}n]} (-1)^i \frac{n}{n-i}\binom{n-i}{i}\lambda_{2s}^{n-2i} = \lambda_{2ns} \quad (s = 0, 1, 2, \ldots;\ n = 1, 2, 3, \ldots).$$

Proof: We may prove the result by generating functions. Alternatively, the following, essentially, is formula (1.64) in [1]:

(16) $$\sum_{i=0}^{[\frac{1}{2}n]} \frac{\binom{n-i}{i}}{n-i}\left(\frac{1}{4}z\right)^i = \frac{1}{n2^{n-1}}\left(\frac{x^n+y^n}{x+y}\right), \text{ where } x = 1+\sqrt{z+1},\ y = 1-\sqrt{z+1}.$$

In (16), let $z = -4/\lambda_{2s}^2$ (note $\lambda_{2s} \neq 0\ \forall\ s$). Then

$$\sqrt{z+1} = \frac{\sqrt{\lambda_{2s}^2 - 4}}{\lambda_{2s}} = \frac{u^{2s} - v^{2s}}{\lambda_{2s}} = \frac{(u-v)\varphi_{2s}}{\lambda_{2s}}.$$

Hence,

$$x = 2u^{2s}/\lambda_{2s},\quad y = 2v^{2s}/\lambda_{2s},\quad x+y = 2.$$

Substituting in (16), we obtain:

$$\sum_{i=0}^{[\frac{1}{2}n]} \frac{\binom{n-i}{i}}{n-i}(-1)^i\lambda_{2s}^{-2i} = \frac{1}{n2^{n-1}}\left(\frac{2^n(u^{2ns}+v^{2ns})}{\lambda_{2s}^n \cdot 2}\right).$$

This simplifies to (15), proving the lemma.

Lemma 2:

$$\sum_{i=0}^{[\frac{1}{2}n]} (-1)^i \frac{n}{n-i}\binom{n-i}{i}2^{n-2i} = 2 \qquad (n = 1, 2, 3, \ldots).$$

Proof: Let $s = 0$ in Lemma 1.

Lemma 3:

$$\sum_{i=0}^{[\frac{1}{2}n]} (-1)^i \binom{n-i}{i}2^{n-2i} = n+1 \qquad (n = 0, 1, 2, \ldots).$$

Proof: This is formula (1.72) in [1].

Lemma 4:

(17) $$\sum_{i=0}^{[\frac{1}{2}n]} (-1)^i (n-2i)\frac{n}{n-i}\binom{n-i}{i}2^{n-1-2i} = n^2 \qquad (n = 1, 2, 3, \ldots).$$

Proof: The left member of (17) is equal to

$$\sum_{i=0}^{[\frac{1}{2}n]} (-1)^i (2n-2i-n)\frac{n}{n-i}\binom{n-i}{i}2^{n-1-2i}$$

$$= n\sum_{i=0}^{[\frac{1}{2}n]} (-1)^i\binom{n-i}{i}2^{n-2i} - \frac{1}{2}n\sum_{i=0}^{[\frac{1}{2}n]} (-1)^i\frac{n}{n-i}\binom{n-i}{i}2^{n-2i}$$

$$= n(n+1) - \frac{1}{2}n \cdot 2 = n^2 \qquad \text{(using Lemmas 2 and 3).}$$

Proof of Theorem 3: From Theorem 1, with $n = 1$, $u^p \equiv v$, $v^p \equiv u \pmod p$. Hence, since $\bar{u} = v$, there exists $w \in R_1(p,c)$, such that

(18) $$u^p \equiv v + pw,\quad v^p \equiv u + p\bar{w} \pmod{p^2}.$$

Multiplying these last two congruences, we have:

$$(uv)^p \equiv uv + p(uw + \overline{uw}) \pmod{p^2}.$$

However, $uv = a^2 - b^2c = \pm 1$, so $(uv)^p = uv$. Hence, it follows that

(19) $$uw + \overline{uw} \equiv 0 \pmod{p}.$$

If, in (18), we multiply throughout by u and v, respectively, we obtain:

$$u^{p+1} \equiv uv + puw, \quad v^{p+1} \equiv uv + p\overline{uw} \pmod{p^2}.$$

Now adding these last two congruences and using (19), we obtain the result

(20) $$\lambda_{p+1} \equiv 2(a^2 - b^2c) \pmod{p^2}.$$

This is (13) for the case $n = 1$. Let T be the set of natural numbers n for which (13) holds; we have shown that $1 \in T$. Suppose $r \in T$, and let

$$m_1 = (p+1)p^{r-1}.$$

By Lemma 1, since m_1 is even,

$$\lambda_{pm_1} = \sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \frac{p}{p-i}\binom{p-i}{i}\lambda_{m_1}^{p-2i}.$$

But, by the inductive hypothesis, $\lambda_{m_1} = 2uv + Kp^{2r}$, for some integer K. Hence,

$$\begin{aligned}
\lambda_{pm_1} &= \sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \frac{p}{p-i}\binom{p-i}{i}(2uv + Kp^{2r})^{p-2i} \\
&= \sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \frac{p}{p-i}\binom{p-i}{i}\sum_{j=0}^{p-2i}\binom{p-2i}{j}(2uv)^{p-2i-j}(Kp^{2r})^j \\
&= \sum_{j=0}^{p}(Kp^{2r})^j \sum_{i=0}^{\left[\frac{1}{2}(p-j)\right]} (-1)^i \frac{p}{p-i}\binom{p-i}{i}\binom{p-2i}{j}(2uv)^{p-2i-j} \\
&\equiv \sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \frac{p}{p-i}\binom{p-i}{i}(2uv)^{p-2i} \\
&\quad + Kp^{2r}\sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \left(\frac{p}{p-i}\right)(p-2i)\binom{p-i}{i}(2uv)^{p-2i-1} \pmod{p^{2r+2}} \\
&\equiv uv\sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \frac{p}{p-i}\binom{p-i}{i}2^{p-2i} \\
&\quad + Kp^{2r}\sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \frac{p}{p-i}\binom{p-i}{i}(p-2i)2^{p-2i-1} \pmod{p^{2r+2}} \\
&\equiv 2uv + Kp^{2r+2} \pmod{p^{2r+2}} \equiv 2uv \pmod{p^{2r+2}}
\end{aligned}$$

(using Lemmas 2 and 4). Hence, $r \in T \Rightarrow (r+1) \in T$. The result of the theorem now follows by induction.

Corollary 1 (of Theorems 2 and 3):

Let p be any odd prime such that $\left(\frac{5}{p}\right) = -1$, n be any natural number, and $m = m(p,n) = (p+1)p^{n-1}$. Then

(21) $F_m \equiv 0 \pmod{p^n}$, and

(22) $L_m \equiv -2 \pmod{p^{2n}}$.

Proof: Let $a = b = \frac{1}{2}$, $c = 5$, and apply (12) and (14) and the definitions of Fibonacci and Lucas sequences.

3. THE CASE $\left(\frac{c}{p}\right) = 1$

We will now deal with the case where $\left(\frac{c}{p}\right) = 1$, starting our discussion anew. We soon find that this case is much simpler than the first, since now $\sqrt{c}$ is an element of $R_n(p)$, in the modular sense, and thus has a "real" meaning. In fact, if all the definitions of the preceding discussion are retained with the exception that now $\left(\frac{c}{p}\right) = 1$, we see that objects $(a + b\sqrt{c})$ of $R(p,c)$ are actually congruent (mod p^n) to objects of $R_n(p)$, and that we do not need to concern ourselves with $R_n(p,c)$ at all. In other words, the theory of "complex residues" is irrelevant in this simpler case. With this idea in mind, we may "rethink" the results of the previous section. Thus, Theorem 1 is replaced by (7), for the case $\left(\frac{c}{p}\right) = 1$. The counterpart of Theorem 2 is the following, for this case.

Theorem 4: Let the sequences $\{\varphi_k\}$ and $\{\lambda_k\}$ be given by (9) and (10), and let $M = (p-1)p^{n-1} = \phi(p^n)$. Then

(23) $\varphi_M \equiv 0$, and

(24) $\lambda_M \equiv 2$.

Proof: By (6), $u^M \equiv v^M \equiv 1$, which implies: $u^M - v^M \equiv 0$, $u^M + v^M \equiv 2$. Since $(u-v)^{-1} = (2b\sqrt{c})^{-1}$ exists, we may apply the definitions in (9) and (10), thereby proving the result.

The counterpart of Theorem 3 is the following fortification of (24):

Theorem 5:

(25) $\lambda_M \equiv 2 \pmod{p^{2n}}$.

Proof: BY (7), with $n = 1$, $u^p \equiv u$, $v^p \equiv v \pmod{p}$. Thus, there exist x and y in $R_1(p)$ such that

(26) $u^p \equiv u + px, \quad v^p \equiv v + py \pmod{p^2}$.

Multiplying these two congruences, we obtain: $(uv)^p \equiv uv + p(uy + vx)$ (mod p^2). But $uv = \pm 1$, so $(uv)^p = uv$. Hence, we have

(27) $$uy + vx \equiv 0 \pmod{p}.$$

Returning to (26), if we multiply throughout by v and u, respectively, we obtain: $u^{p-1}(uv) \equiv uv + p(vx)$, $v^{p-1}(uv) \equiv uv + p(uy) \pmod{p^2}$. Now, adding these last two congruences and using (27), we have: $uv(u^{p-1} + v^{p-1}) \equiv 2uv \pmod{p^2}$, which implies (25) for the case $n = 1$.

The remainder of the proof of Theorem 5 is nearly identical to that of Theorem 3, except that in the latter, we replace m_1 by $M_1 = (p - 1)p^{r-1}$.

4. SUMMARY AND CONCLUSION

We may combine Theorems 2 thru 5 thus far derived into the following main theorem. For the sake of completeness and clarity, we will incorporate the necessary definitions in the hypothesis of the theorem.

Theorem 6: Let c be any square-free integer, p any odd prime such that $c \not\equiv 0 \pmod{p}$, and n any positive integer. Let a and b be any rational numbers such that neither their numerators nor their denominators are divisible by p, $2a$ is an integer, and $(a^2 - b^2c) = \pm 1$. Let

$$u = a + b\sqrt{c},\ v = a - b\sqrt{c},\ \varphi_n = (u^n - v^n)/(u - v),\ \lambda_n = u^n + v^n.$$

Finally, let

$$m = m(n,p) = \left\{p - \left(\frac{c}{p}\right)\right\}p^{n-1}.$$

Then

(28) $$\varphi_m \equiv 0 \pmod{p^n}, \text{ and}$$

(29) $$\lambda_m \equiv 1 + uv + (1 - uv)\left(\frac{c}{p}\right) \pmod{p^{2n}}.$$

Corollary 2: Let $\{F_k\}$ and $\{L_k\}$ be the Fibonacci and Lucas sequences. Let p be any odd prime $\neq 5$, and $m = \left\{p - \left(\frac{5}{p}\right)\right\}p^{n-1}$, $n = 1, 2, 3, \ldots$. Then

(30) $$F_m \equiv 0 \pmod{p^n}, \text{ and}$$

(31) $$L_m \equiv 2\left(\frac{5}{p}\right) \pmod{p^{2n}}.$$

Proof: Let $a = b = \frac{1}{2}$, $c = 5$ in Theorem 6.

Corollary 3: Let $\{P_k\}$ and $\{Q_k\}$ be the Pell and "Lucas-Pell" sequences ($a = b = 1$, $c = 2$ in Theorem 6). Let p be any odd prime, and $m = \left\{p - \left(\frac{2}{p}\right)\right\}p^{n-1}$, $n = 1, 2, 3, \ldots$. Then

(32) $$P_m \equiv 0 \pmod{p^n}, \text{ and}$$

(33) $$Q_m \equiv 2\left(\frac{2}{p}\right) \pmod{p^{2n}}.$$

Theorem 6 is the main result of this paper. However, it should be clear to the reader that the basic result of Theorem 1 may be used to obtain other types of congruences, where the indices of the generalized Fibonacci or Lucas sequences are other than the "m" of Theorem 6. The corresponding results, however, do not appear to be quite as elegant as that of Theorem 6. Nevertheless, some information may be gathered about the periodicity (mod p^n) of the sequences in question. For example, using the methods of this paper, we may deduce that, if $P(N)$ denotes the period (mod N) of the Fibonacci and Lucas sequence (the periods for the two sequences *are* the same, except when $5|N$, cf. [2]), and if p is any odd prime $\neq 5$, then

(34) $$p(p^n) \text{ divides } \frac{1}{2}\left(3p + 1 - (p + 3)\left(\frac{5}{p}\right)\right)p^{n-1},\ n = 1, 2, 3, \ldots .$$

We will leave the proof of this result to the reader.

REFERENCES

1. H. W. Gould, *Combinatorial Identities* (Morgantown, W.Va.: The Morgantown Printing and Binding Co., 1972).
2. Dov Jarden, *Recurring Sequences* (Jerusalem: Riveon Lematematika, 1973), p. 103.
3. G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers* (4th ed., reprinted; Oxford: The Clarendon Press, 1962), pp. 221-223.

A NOTE ON A PELL-TYPE SEQUENCE

WILLIAM J. O'DONNELL
George Washington High School, Denver, CO

The Pell sequence is defined by the recursive relation

$$P_1 = 1,\ P_2 = 2, \text{ and } P_{n+2} = 2P_{n+1} + P_n, \text{ for } n \geq 1.$$

The first few terms of the sequence are 1, 2, 5, 12, 29, 70, 169, 408, ... It is well known that the nth term of the Pell sequence can be written

$$P_n = \frac{1}{\sqrt{8}}\left[\left(\frac{2 + \sqrt{8}}{2}\right)^n - \left(\frac{2 - \sqrt{8}}{2}\right)^n\right].$$

It is also easily proven that $\lim_{n\to\infty} \frac{P_n}{P_{n+1}} = \frac{-2 + \sqrt{8}}{2}$.

For the sequence $\{V_n\}$ defined by the recursive formula

$$V_1 = 1,\ V_2 = 2, \text{ and } V_{n+2} = kV_{n+1} + V_n, \text{ for } k \geq 1,$$

we know that

$$\lim_{n\to\infty} \frac{V_n}{V_{n+1}} = \frac{-k + \sqrt{k^2 + 4}}{2}.$$

If we let $k = 1$, the sequence $\{V_n\}$ becomes the Fibonacci sequence and the limit of the ratio of consecutive terms is $\frac{-1 + \sqrt{5}}{2} = .618$, which is the "golden ratio." For $k = 2$ the ratio becomes .4142, which is the limit of the ratio of consecutive terms of the Pell sequence.

Both of the previous sequences were developed by adding two terms of a sequence or multiples of two terms to generate the next term. We now consider the ratio of consecutive terms of the sequence $\{G_n\}$ defined by the recursive formula

$$G_1 = a_1,\ G_2 = a_2,\ \ldots,\ G_n = a_n, \text{ and}$$

and

$$G_{n+1} = na_n + (n - 1)a_{n-1} + (n - 2)a_{n-2} + \cdots + 2a_2 + a_1$$

where a_i is an integer > 0.

Suppose that when this sequence is continued a sufficient number of terms it is possible to find n consecutive terms such that the limit of the ratio of any two consecutive terms approaches r. The sequence could be written

$$G_m, \frac{G_m}{r}, \frac{G_m}{r^2}, \frac{G_m}{r^3}, \ldots, \frac{G_m}{r^{n-1}}.$$

The next term, $\frac{G_m}{r^n}$, may be written as

$$\frac{G_m}{r^n} = n\left(\frac{G_m}{r^{n-1}}\right) + (n - 1)\left(\frac{G_m}{r^{n-2}}\right) + \cdots + 2\frac{G_m}{r} + G_m.$$

Simplifying,

$$G_m = nrG_m + (n - 1)r^2G_m + \cdots + 2r^{n-1}G_m + r^nG_m.$$

Dividing by G_m, we obtain

$$1 = nr + (n - 1)r^2 + \cdots + 2r^{n-1} + r^n$$

or

$$r^n + 2r^{n-1} + \cdots + (n - 2)r^3 + (n - 1)r^2 + nr - 1 = 0. \tag{1}$$

The limiting value of r is seen to be the root of equation 1.

If we let $n = 4$, $G_1 = 2$, $G_2 = 4$, $G_3 = 3$, and $G_4 = 1$, the corresponding sequence is 2, 4, 3, 1, 23, 105, 494, 2338, 11067, 52375, ... The ratios of consecutive terms are

$$\frac{2}{4} = 0.5000 \qquad \frac{105}{494} = 0.2125$$

$$\frac{4}{3} = 1.3333 \qquad \frac{494}{2338} = 0.2113$$

$$\frac{3}{1} = 3.0000 \qquad \frac{2338}{11067} = 0.2113$$

$$\frac{1}{23} = 0.0434 \qquad \frac{11067}{52375} = 0.2113$$

$$\frac{23}{105} = 0.2190$$

The computed ratio approaches .2113. Using equation 1 we have, for this sequence, $r^4 + 2r^3 + 3r^2 + 4r - 1 = 0$. By successive approximation, we find $r \approx .2113$. The reader may also wish to verify this conclusion for other initial values for the sequence as well as for a different number of initial terms.

REFERENCE

M. Bicknell, "A Primer on the Pell Sequence and Related Sequences," *The Fibonacci Quarterly* 13, No. 4 (1975):345-349.

*****

PERIODS AND ENTRY POINTS IN FIBONACCI SEQUENCE

A. ALLARD and P. LECOMTE
Université de Liège, Liège, Belgium

1. INTRODUCTION

Let the F 's be defined as follows:

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

Let $k > 0$ be any integer. There is then a smallest positive m such that $k|F_m$ [if a, b denote integers, we sometimes write $a|b$ instead of $b \equiv 0 \pmod{a}$, $a||b$ instead of $b \equiv 0 \pmod{a}$, and $b \not\equiv 0 \pmod{a^2}$]. This unique m will be denoted by β_k; F_{β_k} is usually called the *entry point* of k. Moreover, the sequence $F_n \pmod{k}$ is well known to be periodical. We denote by 1_k the period and we let $\gamma_k = 1_k/\beta_k$.

Our purpose in this paper is to compute (at least in a theorical way) γ_p for each prime p. In [1], Vinson also computes γ_p, but our point of view and our methods are really different from those of Vinson, so that we obtain new results regarding γ_p and additional information about β_p.

This paper is based on a few results which are summarized in Section 2 and proved in Section 6. Some of these are well known and their proofs (elementary) are given for the benefit of the reader.

2. PROPOSITIONS

We now state those propositions that will be useful later.

Let p be a prime with $p > 5$. For simplicity, we let $\beta = \beta_p$, $1 = 1_p$, and $\gamma = \gamma_p$. Then

(1) $$p|F_m \Longleftrightarrow \beta|m, \quad \forall\, m.$$

This shows that γ is an integer.

(2) $\gamma \in \{1, 2, 4\}$; *to be more precise*,

$$\gamma = 1 \Longleftrightarrow F_{\beta-1} \equiv 1 \pmod{p}$$
$$\gamma = 2 \Longleftrightarrow F_{\beta-1} \equiv -1 \pmod{p}$$
$$\gamma = 4 \Longleftrightarrow F^2_{\beta-1} \equiv -1 \pmod{p}$$

(3) $\gamma = 4 \Longleftrightarrow \beta$ *is odd*

$$4|\beta \Rightarrow \gamma = 2$$

(4) *The following holds for any* $j \in \{0, 1, \ldots, \beta - 1\}$ *and any* $k > 0$:

$$F_{k\beta-j} \equiv F^{k-1}_{\beta-1}F_{\beta-j} \pmod{p}.$$

In particular, letting $j = 1$, we obtain

$$F_{k\beta-1} \equiv F^k_{\beta-1} \pmod{p}.$$

(5) *For all* a, $b > 0$, *we have*

$$F_{ab} = \sum_{k=1}^{b} C^k_b F^k_a F^{b-k}_{a-1} F_k \quad \left(C^k_b = \frac{b!}{k!\,(b-k)!}\right).$$

[Note that if p is a prime, then $p|C_p^k$ for $k = 1, \ldots, p - 1$. Then the above formula with $a = q$ and $b = p$ together with Fermat's theorem implies that

$$F_{pq} \equiv F_p F_q \pmod p$$

for all prime p and all integers q.]

(6) *If* $p = 10m \pm 1$, *then* $F_p \equiv 1 \pmod p$ *and* $\beta|(p - 1)$.
If $p = 10m \pm 3$, *then* $F_p \equiv -1 \pmod p$ *and* $\beta|(p + 1)$.

(7) $$2\beta|(p \pm 1) \Longleftrightarrow p \equiv 1 \pmod 4$$

[*according that p is* $(p - 1)$ *or is not* $(p + 1)$ *a quadratic residue* mod 5].

We are now in a position to state our main results. We will investigate separately the cases $p = 10m \pm 1$ and $p = 10m \pm 3$. The conclusions are of very different natures.

3. COMPUTATION OF γ WHEN $p = 10m \pm 3$

Theorem 1: Let p be of the form $10m \pm 3$. Then either $p = 4m' - 1$, $\gamma = 2$, and $4|\beta$, or $p = 4m' + 1$, $\gamma = 4$, and β is odd.

This theorem allows us to calculate γ by a simple examination of the number p. Such a result does not hold in the case where $p = 10m \pm 1$.

Proof: By (6) above, we can write $p = \mu\beta - 1$ and $F_p \equiv -1 \pmod p$. Thus, by (4), we have

(3.1) $$F_{\beta-1}^{\mu} \equiv -1 \pmod p.$$

Since $\gamma = 1$ implies $F_{\beta-1} \equiv 1 \pmod p$ and since $F_{\beta-1}^4 \equiv 1 \pmod p$, we conclude from (3.1) that $\gamma > 1$ and $4 \nmid \mu$.

Suppose β is even. Then $\gamma = 2$ and $F_{\beta-1} \equiv -1 \pmod p$. From (3.1), this implies that μ is odd. Suppose $2||\beta$. Then $p = \mu\beta - 1 \equiv 1 \pmod 4$, so that by (7), $2\beta|(p + 1)$, which is a contradiction. Thus, $4|\beta$ and $p \equiv -1 \pmod 4$.

Suppose β is odd. Then $\gamma = 4$ and $F_{\beta-1}^2 \equiv -1 \pmod p$. From (3.1), this implies that $2||\mu$. Hence, $p = \mu\beta - 1 \equiv 1 \pmod 4$. The theorem is proved.

From the preceding proof, we obtain another statement.

Theorem 2: If $\gamma = 1$, then $p = 10m \pm 1$.

4. COMPUTATION OF γ WHEN $p = 10m \pm 1$

This case is more complicated and it is convenient to introduce the *characteristic exponent* α *of* p, well defined [recall (6)] by

$$= 2^{\alpha}\nu\beta + 1, \ \nu \text{ odd}.$$

The explicit computation of α will be made later, by means of the following lemma.

Lemma: If $p = 10m \pm 1 = 2^{\alpha}\nu\beta + 1$ with ν odd, then

(8) $$\gamma = 1 \Rightarrow \frac{F_{p-1}}{F_{\nu\beta}} \equiv 2^{\alpha} \pmod p$$

(9) $$\gamma = 2 \Rightarrow \frac{F_{p-1}}{F_{\nu\beta}} \equiv -2^{\alpha} \pmod p$$

(10) $$\gamma = 4 \Rightarrow \frac{F_{p-1}}{F_{\nu\beta}} \equiv -2^{\alpha}F^{\nu}_{\beta-1} \pmod{p}.$$

In fact, apply (5), with $a = \nu\beta$ and $b = 2^{\alpha}$. Then

$$F_{p-1} = \sum_{k=1}^{2^{\alpha}} C^{k}_{2^{\alpha}} F^{k}_{\nu\beta} F^{2^{\alpha}-k}_{\nu\beta} F_{k}.$$

This implies that

(4.1) $$\frac{F_{p-1}}{F_{\nu\beta}} \equiv 2^{\alpha}F^{\nu(2^{\alpha}-1)}_{\beta-1} \pmod{p}.$$

On the other hand, (6) and (4) imply

(4.2) $$F^{2^{\alpha}\nu}_{\beta-1} \equiv 1 \pmod{p}.$$

Then, from (4.1) and (4.2):

(4.3) $$F^{\nu}_{\beta-1} \cdot \frac{F_{p-1}}{F_{\nu\beta}} \equiv 2^{\alpha} \pmod{p}.$$

Suppose $\gamma = 1$, then $F_{\beta-1} \equiv 1 \pmod{p}$ and (8) follows from (4.3).

Suppose $\gamma = 2$, then $F_{\beta-1} \equiv -1 \pmod{p}$, and since ν is odd, (9) follows from (4.3).

Suppose $\gamma = 4$, then $F^{2}_{\beta-1} \equiv -1 \pmod{p}$. Since ν is odd, we have $F^{2}_{\beta-1} \equiv -1 \pmod{p}$, so that (10) follows from (4.3).

Theorem 4: Let $p = 10m \pm 1$. Then, p can be written uniquely as $p = 2^{r}s + 1$ with s odd, and we have

$$\gamma = 4 \Longleftrightarrow \frac{F_{p-1}}{F_{s}} \not\equiv 0 \pmod{p}$$

$$\gamma = 1 \Longleftrightarrow \frac{F_{p-1}}{F_{2s}} \equiv 2^{r-1} \pmod{p}$$

$$\gamma = 2 \Longleftrightarrow \frac{F_{p-1}}{F_{s}} \equiv 0 \quad \text{and} \quad \frac{F_{p-1}}{F_{2s}} \not\equiv 2^{r-1} \pmod{p}.$$

(The statement concerning $\gamma = 2$ will be made more precise later.)

Proof: Suppose $\gamma = 4$. Then, β is odd and, thus, $\alpha = r$, $\nu\beta = s$, so that, by the lemma, we have

$$\frac{F_{p-1}}{F_{s}} \quad -2^{r}F^{\nu}_{\beta-1} \not\equiv 0 \pmod{p}.$$

Suppose $\gamma = 1$. Then, β is even, but $2\|\beta$, since $4|\beta$ implies $\gamma = 2$. So $\alpha = r - 1$ and $\nu\beta = 2s$; thus, by the lemma, we have

$$\frac{F_{p-1}}{F_{2s}} \equiv 2^{r-1} \pmod{p}.$$

Conversely, suppose $\dfrac{F_{p-1}}{F_s} \not\equiv 0 \pmod{p}$. Then $p|F_s$, since $p|F_{p-1}$. Thus, $\beta|s$, and so β is odd, proving that $\gamma = 4$. Suppose that $\dfrac{F_{p-1}}{F_{2s}} \equiv 2^{r-1} \pmod{p}$. We want to prove that $\gamma = 1$ in this case. We now have $\beta|2s$. If β is odd, then $\gamma = 4$ and, as seen above, $\dfrac{F_{p-1}}{F_s} \equiv -2^r F^{\nu}_{\beta-1} \pmod{p}$. But, since $\beta|s$,

$$F_{s-1} + F_{s+1} \equiv F_{\nu\beta-1} + F_{\nu\beta+1} \equiv 2F^{\nu}_{\beta-1} \pmod{p},$$

so that

$$2^{r-1} \equiv \frac{F_{p-1}}{F_2} \equiv \frac{F_{p-1}}{F_s(F_{s-1} + F_{s+1})} \equiv \frac{-2^r F^{\nu}_{\beta-1}}{2F^{\nu}_{\beta-1}} \equiv -2^{r-1} \pmod{p}.$$

This is clearly a contradiction, since p is odd. If $2||\beta$ and $\gamma = 2$, we have $\alpha = r - 1$ and $\nu\beta = 2s$. So, by the lemma, $\dfrac{F_{p-1}}{F_{2s}} \equiv -2^{r-1} \pmod{p}$. But, we assume that $\dfrac{F_{p-1}}{F_2} \equiv 2^{r-1} \pmod{p}$. Hence, a contradiction. Thus $\gamma = 1$, and the lemma follows.

Corollary: If $p = 10m \pm 1 = 4m' - 1$, then $\gamma = 1$.

In fact, one has $4m' - 1 = 2^r s + 1$, s odd, if and only if $r = 1$. In this case, $F_{p-1} = F_{2s}$ and, by Theorem 4, $\gamma = 1$.

We are now in a position to compute the characteristic exponent α of p. It is clear that if $\gamma = 4$, then $\alpha = r$; if $\gamma = 1$, then $\alpha = r - 1$. We have only to look at the case $\gamma = 2$.

Theorem 5: Let $1 < k \le r$. Then $\alpha = r - k$ and $\gamma = 2$ if and only if

$$\frac{F_{p-1}}{F_s} \equiv \cdots \equiv \frac{F_{p-1}}{F_{2^{k-1}s}} \equiv 0 \quad \text{and} \quad \frac{F_{p-1}}{F_{2^k s}} \equiv -2^{r-k} \pmod{p}. \tag{4.4}$$

We see that α is determined by the rank of the first nonvanishing $\dfrac{F_{p-1}}{F_{2^j s}}$ (mod p).

Proof: Suppose that $\gamma = 2$ and $\alpha = r - 1$. By the lemma, we can conclude that $\dfrac{F_{p-1}}{F_{2^k s}} \equiv -2^{r-k} \pmod{p}$. On the other hand, since $2^j s \not\equiv 0 \pmod{p}$ for $j = 0, \ldots, k - 1$, we see that (4.4) holds.

Conversely, suppose (4.4) holds. Then, by Theorem 4, since $k > 1$, $\gamma < 4$, and $\gamma \neq 1$, that is $\gamma = 2$. Moreover, $\beta|2^k s$, but $\beta\nmid 2^{k-1}s$. Thus $\nu\beta = 2^k s$ and $\alpha = r - k$. Hence the result.

5. FURTHER PROPERTIES OF γ AND SOME INTERESTING RESULTS

Proposition 1: For any prime p, $\gamma = 2$ implies $4|\beta$.

In fact, when $p = 10m \pm 3$, this follows from Theorem 1. When $p = 10m \pm 1$, we prove that $2||\beta$ implies $\gamma = 1$. As $2||\beta$, $\gamma < 4$, and $p|F_{2s}$, but $p\nmid F_s$ and so

$$F_{s-1} + F_{s+1} \equiv 0 \pmod{p}.$$

But $F_{2s-1} \equiv F_{s-1}^2 + F_s^2$ and, as s is odd, $F_{s-1}F_{s+1} = F_s^2 - 1$. Thus, since $2s = \nu\beta$, we can write

$$F_{\beta-1} \equiv F_{\beta-1} \equiv F_{2s-1} \equiv -F_{s-1}F_{s+1} + F_s^2 \equiv 1 \pmod{p}.$$

Hence $\gamma = 1$, and the result is proved.

Proposition 2: If $p = 10m \pm 1$, then $\gamma = 2$ if and only if $\dfrac{F_{p-1}}{F_s} \equiv \dfrac{F_{p-1}}{F_{2s}} \equiv 0 \pmod{p}$.

This is obvious from what precedes. Practically, however, this can be of some interest: to compute γ, compute $F_s \pmod{p}$. If $F_s \not\equiv 0 \pmod{p}$, then $\dfrac{F_{p-1}}{F_s} \equiv 0 \pmod{p}$ and, thus, $\gamma \neq 4$. Compute then $F_{s-1} + F_{s+1} \pmod{p}$. If it does not vanish, then $F_{2s} \not\equiv 0 \pmod{p}$ so that $\gamma \neq 1$ and, thus, $\gamma = 2$.

Proposition 3: Let p be any given prime number. Then the greatest t such that $p^t | F_{\beta_p}$ is the greatest t such that $p^t | F_{p\pm1}$.

In fact, either $p = 10m \pm 1$, $p = \lambda\beta + 1$, or $p = 10m \pm 3$, $p = \mu\beta - 1$. By (5), this implies

$$\frac{F_{p-1}}{F_\beta} \equiv \lambda F_{\beta-1}^{\lambda-1} \not\equiv 0 \pmod{p} \quad \text{or} \quad \frac{F_{p-1}}{F_\beta} \equiv \mu F_{\beta-1}^{\mu-1} \not\equiv 0 \pmod{p},$$

respectively. Hence, Proposition 3.

6. PROOFS OF PROPOSITIONS

This section is devoted to the proofs of the propositions stated in Section 2, except for (7), for which the reader is referred to *The Fibonacci Quarterly* 8, No. 1 (1970):23-30.

Proof of (4): Since the sequence $F_n \pmod{p}$ starts with

$$F_1 \equiv 1, \quad F_2 \equiv 1, \quad F_3 \equiv 2, \; \ldots, \; F_{\beta-1}, 0,$$

it follows from $F_{n+2} = F_{n+1} + F_n$ that the following β members of this sequence are obtained by multiplying the first β one by $F_{\beta-1}$ so that, for any $j = 0, \ldots, \beta - 1$, $F_{2\beta-j} \equiv F_{\beta-1}F_{\beta-j} \pmod{p}$. The argument can be applied again to prove that $F_{3\beta-j} \equiv F_{\beta-1}F_{\beta-j}$ and, more generally, that $F_{k\beta-1} \equiv F_{\beta-1}F_{(k-1)\beta-1} \pmod{p}$. Proposition (4) then holds in an obvious way.

Proof of (5): Recall that

$$F_n = \frac{\varphi}{\varphi^2+1}\left[\varphi^n - \left(-\frac{1}{\varphi}\right)^n\right]$$

where φ and $-\dfrac{1}{\varphi}$ satisfy $y^2 = y + 1$. From this, it is clear that

$$\varphi^n = \varphi F_n + F_{n-1} \quad \text{and} \quad \left(-\frac{1}{\varphi}\right)^n = \left(-\frac{1}{\varphi}\right)F_n + F_{n-1}.$$

Then

$$F_{ab} = \frac{\varphi}{\varphi^2+1}\left[\varphi^{ab} - \left(-\frac{1}{\varphi}\right)^{ab}\right] = \frac{\varphi}{\varphi^2+1}\left[(\varphi F_a + F_{a-1})^b - \left(-\frac{1}{\varphi}F_a + F_{a-1}\right)^b\right]$$

$$= \sum_{k=1}^{b} C^k F^k F_{a-1}^{b-k} F_k, \text{ using binomial expansion and } F_0 = 0.$$

Proof of (1) and (2): Recall that for any integer m we have

$$F_{m-1}F_{m+1} = F_m^2 + (-1)^m.$$

Let $m = \beta$ in this formula. Thus,

$$F_{\beta-1}^2 \equiv (-1)^\beta \pmod{p}, \tag{6.1}$$

taking account of $F_{\beta+1} \equiv F_{\beta-1} \pmod{p}$. On the other hand, 1 is the smaller m such that $F_{\beta-1}^m \equiv F_{m\beta-1} \equiv 1 \pmod{p}$. Recall also that $1 = \gamma\beta$, by the very definition of γ. Then,

(a) suppose β odd. Thus, by (6.1),

$$F_{\beta-1}^2 \equiv -1 \text{ so that } F_{\beta-1} \not\equiv 1 \text{ and } F_{\beta-1}^4 \equiv 1.$$

Thus $\gamma = 4$.

(b) suppose β even. Then (6.1) implies that

$$F_{\beta-1}^2 \equiv 1.$$

Since p is a prime, either

$$F_{\beta-1} \equiv 1 \text{ and } \gamma = 1, \text{ or } F_{\beta-1} \equiv -1 \text{ and } \gamma = 2.$$

Hence (2) is proved.

Proof of (3): To prove (3), we have only to show that $4|\beta$ implies $\gamma = 2$. For this, we show that

$$\left.\begin{aligned} F_{4\lambda} &\equiv 0 \pmod{p} \\ F_{4\lambda+1} &\equiv 1 \pmod{p} \end{aligned}\right\} \Rightarrow F_{2\lambda} \equiv 0 \pmod{p}. \tag{6.2}$$

Suppose that the left member of this implication holds. Then from well-known formulas:

$$\begin{aligned} F_{4\lambda+1} &= F_{2\lambda}^2 + F_{2\lambda+1}^2 = F_{2\lambda}^2 + F_{2\lambda}F_{2\lambda+2} - (-1)^{2\lambda+1} \\ &= F_{2\lambda}(F_{2\lambda} + F_{2\lambda+2}) + 1 \equiv 1 \pmod{p}. \end{aligned}$$

Hence

$$F_{2\lambda}(F_{2\lambda} + F_{2\lambda+2}) \equiv 0 \pmod{p}.$$

To prove (6.2), it suffices to show that $\text{GCD}(F_{2\lambda} + F_{2\lambda+2}, p) = 1$. To do this, since $p|F_{4\lambda}$, it suffices to prove that $\text{GCD}(F_{4\lambda}, F_{2\lambda} + F_{2\lambda+2}) = 1$. But

$$\delta = \text{GCD}(F_{4\lambda}, F_{2\lambda} + F_{2\lambda+2}) = \text{GCD}\big(F_{2\lambda}(F_{2\lambda+1} + F_{2\lambda-1}), F_{2\lambda} + F_{2\lambda+2}\big)$$

and, as $\text{GCD}(F_{2\lambda}, F_{2\lambda+2}) = 1$,

$$\delta = \text{GCD}(F_{2\lambda+1} + F_{2\lambda-1}, F_{2\lambda+2} + F_{2\lambda}).$$

It is then easily seen that

$$\delta|(F_{2\lambda+1} + F_{2\lambda-1}),\ \delta|(F_{2\lambda-1} + F_{2\lambda-3}),\ \ldots,\ \delta|F_2 = 1.$$

Hence (3).

Proof of (6): Recall first that $\left(\frac{p}{5}\right) = 1$ or -1, according that p is or is not a quadratic residue mod 5, that is, $p = 10m \pm 1$ or $p = 10m \pm 3$, respectively. Thus, we have to show that

$$\left(\frac{p}{5}\right) = \pm 1 \Rightarrow F_p \equiv \pm 1 \pmod{p} \quad \text{and} \quad \beta|(p \mp 1).$$

Recall also that $\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right) \equiv 5^{\frac{p-1}{2}} \pmod{p}$. Now we prove that $F_p \equiv \pm 1 \pmod{p}$. We have

$$F_p = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^p - \left(\frac{1-\sqrt{5}}{2}\right)^p\right] = \frac{1}{2^{p-1}\sqrt{5}} \sum_{k \text{ odd}}^{p} C_p^k(\sqrt{5})$$
$$= \frac{1}{2^{p-1}}\left(\sum_{k=0}^{\frac{p-3}{2}} C_p^{2k+1}5^k + 5^{\frac{p-1}{2}}\right) = \frac{1}{2^{p-1}}\left(pK + 5^{\frac{p-1}{2}}\right)$$

since $p \mid C_p^{2k+1}$ for each $k \in \left\{0, 1, \ldots, \frac{p-3}{2}\right\}$. As $2^{p-1} \equiv 1 \pmod{p}$, we have

$$F_p \equiv 5^{\frac{p-1}{2}} \pmod{p},$$

so that $\left(\frac{p}{5}\right) \equiv F_p \pmod{p}$. When $\left(\frac{5}{p}\right) = 1$, we can give another proof. There exists a ρ such that $\rho^2 \equiv 5 \pmod{p}$. Then, for such a ρ, $\theta = \frac{1}{2}(\rho + 1)$ and $\theta' = \frac{1}{2}(\rho - 1)$ are roots of $x^2 - x - 1 \equiv 0 \pmod{p}$ and thus,

$$\theta^n \equiv \theta^{n-1} + \theta^{n-2}, \quad \theta'^n \equiv \theta'^{n-1} + \theta'^{n-2} \pmod{p}.$$

It is then easily seen that

$$F_n \equiv \frac{1}{\rho}[\theta^n - \theta'^n] \pmod{p}. \tag{6.3}$$

But, as p is a prime, $\theta^{p-1} \equiv \theta'^{p-1} \equiv 1 \pmod{p}$ by Fermat's theorem. Now from (6.3) it is obvious that

$$F_{p-1} \equiv 0 \pmod{p}$$
$$F_p \equiv 1 \pmod{p}.$$

Now, to prove that $\beta \mid (p+1)$ according that $\left(\frac{5}{p}\right) = -1$, it will suffice to develop F_{p+1} in a way similar to the method used above for F_p.

ACKNOWLEDGMENT

We are grateful to Dr. E. Zeckendorf for his encouragement and fruitful discussions.

REFERENCES

1. J. Vinson, "The Relation of the Period Modulo m to the Rank of Apparition of m," *The Fibonacci Quarterly* 1, No. 2 (1963).
2. D. E. Daykin & L. A. G. Dresel, "Factorization of Fibonacci Numbers," *The Fibonacci Quarterly* 8, No. 1 (1970).
3. A. Andreassian, "Fibonacci Sequence Modulo m," *The Fibonacci Quarterly* 12, No. 1 (1974).

*****

GENERATING FUNCTIONS OF CENTRAL VALUES IN GENERALIZED PASCAL TRIANGLES

CLAUDIA SMITH and VERNER E. HOGGATT, JR.

San Jose State University, San Jose, CA 95112

1. INTRODUCTION

In this paper we shall examine the generating functions of the central (maximal) values in Pascal's binomial and trinomial triangles. We shall compare the generating functions to the generating functions obtained from partition sums in Pascal's triangles.

Generalized Pascal triangles arise from the multinomial coefficients obtained by the expansion of

$$(1 + x + x^2 + \cdots + x^{j-1}) \ , \quad j \geq 2, \ n \geq 0,$$

where "n" denotes the row in each triangle. For $j = 2$, the binomial coefficients give rise to the following triangle:

1				
1	1			
1	2	1		
1	3	3	1	
1	4	6	4	1
etc.				

For $j = 3$, the trinomial coefficients produce the following triangle:

1						
1	1	1				
1	2	3	2	1		
1	3	6	7	6	3	1

The partition sums are defined

$$S(n,j,k,r) = \sum_{i=0}^{M} \left[\!\left[\begin{matrix} n \\ r+ik \end{matrix} \right]\!\right]_j; \quad 0 \leq r \leq k-1,$$

where

$$M = \left[\frac{(j-1)n - r}{k}\right],$$

[ ] denoting the greatest integer function. To clarify, we give a numerical example. Consider $S(6,3,4,2)$. This denotes the partition sums in the sixth row of the trinomial triangle in which every fourth element is added, beginning with the second column. The $S(6,3,4,2) = 15 + 45 + 1 = 61$. (Conventionally, the column of 1's at the far left is the 0th column and the top row is the 0th row.)

In the nth row of the j-nomial triangle the sum of the elements is j^n. This is expressed by

$$S(n,j,k,0) + S(n,j,k,1) + \cdots + S(n,j,k,k-1) = j^n.$$

Let

$$S(n,j,k,0) = (j^n + A_n)/k$$

$$S(n,j,k,1) = (j^n + B_n)/k \;\ldots$$
$$S(n,j,k,k-1) = (j^n + Z_n)/k.$$

Since $S(0,j,k,0) = 1$,

$$S(0,j,k,1) = 0 \;\ldots\; S(0,j,k,k-1) = 0,$$

we can solve for A_0, B_0, ..., Z_0 to get $A_0 = k - 1$, $B_0 = -1$, ..., $Z_0 = -1$.

Now a departure table can be formed with A_0, B_0, ..., Z_0 as the 0th row. The term "departure" refers to the quantities, A_n, B_n, ..., Z_n that depart from the average value j^n/k. Pascal's rule of addition is the simplest method for finding the successive rows in each departure table. The departure tables for 5 and 10 partitions in the binomial triangle appear below. Notice the appearance of Fibonacci and Lucas numbers.

Table 1

SUMS OF FIVE PARTITIONS IN THE BINOMIAL TRIANGLE

4	-1	-1	-1	-1
3	3	-2	-2	-2
1	6	1	-4	-4
-3	7	7	-3	-8
-11	5	14	4	-11
-22	-7	18	18	-7

Table 2

SUMS OF TEN PARTITIONS IN THE BINOMIAL TRIANGLE

9	-1	-1	-1	-1	-1	-1	-1	-1	-1
8	8	-2	-2	-2	-2	-2	-2	-2	-2
6	16	6	-4	-4	-4	-4	-4	-4	-4
2	22	22	2	-8	-8	-8	-8	-8	-8
-6	24	44	24	-6	-16	-16	-16	-16	-16
-22	18	68	68	18	-22	-32	-32	-32	-32

The primary purpose of this paper is to show that the limit of the generating functions for the $(H - L)/k$ sequences is precisely the generating functions for the central values in the rows of the binomial and trinomial triangles. The $(H - L)/k$ sequences are obtained from the difference of the maximum and minimum value sequences in a departure table, divided by k, where k denotes the number of partitions.

2. GENERATING FUNCTIONS OF THE $(H - L)/k$ SEQUENCES IN THE BINOMIAL TRIANGLE

Table 3 is a table of the $(H - L)/k$ sequences for $k = 3$ to $k = 15$ partitions.

The generating function of the maximum values in the binomial triangle is

$$\frac{1}{\sqrt{1 - 4x^2}}\left(\frac{1 + 2x - \sqrt{1 - 4x^2}}{2x}\right).$$

We shall examine this and show it to be the limit of the generating functions of the $(H - L)/k$ sequences.

Table 3

$(H - L)/k$ SEQUENCES FOR $k = 3$ TO $k = 15$

$k = 3$	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1
1	2	2	2	2	2	2	2	2	2	2	2	2
1	2	3	3	3	3	3	3	3	3	3	3	3
1	4	5	6	6	6	6	6	6	6	6	6	6
1	4	8	9	10	10	10	10	10	10	10	10	10
1	8	13	18	19	20	20	20	20	20	20	20	20
1	8	21	27	33	34	35	35	35	35	35	35	35
1	16	34	54	61	68	69	70	70	70	70	70	70
1	16	55	81	108	116	124	125	126	126	126	126	126
1	32	89	162	197	232	241	250	251	252	252	252	252
1	32	144	243	352	396	440	450	460	461	462	462	462
1	64	233	496	638	792	846	900	911	922	923	924	924
1	64	377	729	1145	1352	1560	1625	1690	1702	1714	1715	1716
1	128	610	1458	2069	2704	2977	3250	3327	3404	3417	3430	3431

Consider the relation $S_{n+2} = S_{n+1} - x^2 S_n$, expressed by the equation

$$K^2 - K + x^2 = 0.$$

The two roots are

$$K_1 = \frac{1 + \sqrt{1 - 4x^2}}{2} \quad \text{and} \quad K_2 = \frac{1 - \sqrt{1 - 4x^2}}{2}, \quad K_1 > K_2.$$

Therefore,

$$\lim_{n\to\infty} \frac{S_{n+1}}{S_n} = K_1 = L$$

by Gauss's theorem that the limit is the root of the maximum modulus.

The generating functions for the odd partitions, $k = 2m + 1$, were found to have the form

$$\frac{S_{m-1}}{S_m - xS_{m-1}}.$$

The generating functions for the even partitions, $k = 2m$, were found to have the form

$$\frac{S_{m-1} + S_{m-2}}{S_m - x^2 S_{m-2}}.$$

We show these two forms have the same limit.

$$\lim_{n\to\infty} \frac{S_{n-1}}{S_n - xS_{n-1}} = \frac{\dfrac{S_{n-1}}{S_{n-1}}}{\dfrac{S_n}{S_{n-1}} - \dfrac{xS_{n-1}}{S_{n-1}}} = \frac{1}{L - x}$$

$$\lim_{n\to\infty}\frac{S_{n-1}+S_{n-2}}{S_n - x^2S_{n-2}} = \frac{\dfrac{S_{n-1}}{S_{n-2}}+\dfrac{xS_{n-2}}{S_{n-2}}}{\dfrac{S_n}{S_{n-2}}-\dfrac{x^2S_{n-2}}{S_{n-2}}} = \frac{L+x}{L^2-x^2} = \frac{1}{L-x}$$

where

$$\frac{1}{L-x} = \frac{1}{\dfrac{1+\sqrt{1-4x^2}-2x}{2}} = \frac{2}{1-2x+\sqrt{1-4x^2}}$$

$$= \frac{1}{\sqrt{1-4x^2}}\left(\frac{1+2x-\sqrt{1-4x^2}}{2x}\right).$$

We pause now to consider the generating function for

$$1 + 2x + 6x^2 + 20x^3 + 70x^4 + \cdots + \binom{2n}{n}x^n + \cdots = \frac{1}{\sqrt{1-4x}},$$

(see [1], p. 41).

Now the Catalan number $\frac{1}{n+1}\binom{2n}{n}$ generating function is

$$C(x) = \frac{1-\sqrt{1-4x}}{2x}.$$

Thus,

$$\frac{1}{\sqrt{1-4x}}\left(\frac{1-\sqrt{1-4x}}{2x}\right) = 1 + 3x + 10x^2 + 35x^3 + \cdots,$$

(see [2], p. 8).

We observe the following relationship between these two series:

$$(1 + 2x + 6x^2 + 20x^3 + 70x^4 + \cdots - 1)/2x$$

$$= \frac{2x(1 + 3x + 10x^2 + 35x^3 + \cdots}{2x} = \frac{1}{\sqrt{1-4x}}\left(\frac{1-\sqrt{1-4x}}{2x}\right).$$

Next we wish to blend these two series. Replace x with x^2.

$$\frac{1}{\sqrt{1-4x^2}} = 1 + 2x^2 + 6x^4 + 20x^6 + 70x^8 + \cdots .$$

We multiply the latter by x, after replacing x with x^2.

$$x \quad \frac{1}{\sqrt{1-4x^2}}\left(\frac{1-\sqrt{1-4x^2}}{2x^2}\right) = x + 3x^3 + 10x^5 + 35x^7 + \cdots .$$

Therefore, the generating function for the blend,

$$1 + x + 2x^2 + 3x^3 + 6x^4 + 10x^5 + 20x^6 + \cdots$$

is

$$\frac{1}{\sqrt{1-4x^2}}\left(1 + \frac{1-\sqrt{1-4x^2}}{2x}\right) = \frac{1}{\sqrt{1-4x^2}}\left(\frac{1+2x-\sqrt{1-4x^2}}{2x}\right)$$

which is precisely the value of $\frac{1}{L - x}$. Thus, we see that the limit of the generating functions for the $(H - L)/k$ sequences is precisely the generating function for the maximum values in the rows of the binomial triangle.

3. GENERATING FUNCTIONS OF THE $(H - L)/k$ SEQUENCES IN THE TRINOMIAL TRIANGLE

Table 4 exhibits the $(H - L)/k$ sequences for $k = 4$ to $k = 16$ partitions. The generating function of the maximum values in the trinomial triangle is

$$1/\sqrt{1 - 2x - 3x^2}.$$

Table 4

$(H - L)/k$ SEQUENCES FOR $k = 4$ TO $k = 16$

$k = 4$	5	6	7	8	9	10	11	12	13	14	15	16
1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1
1	2	3	3	3	3	3	3	3	3	3	3	3
1	3	5	6	7	7	7	7	7	7	7	7	7
1	5	11	14	17	18	19	19	19	19	19	19	19
1	8	21	31	41	45	49	50	51	51	51	51	51
1	13	43	70	99	114	129	134	139	140	141	141	141
1	21	85	157	239	288	337	358	379	385	391	392	393

Consider the relation $F_{n+2} = F_{n+1} + F_n$, which is expressed by the equation

$$x^2 - x - 1 = 0.$$

$$\lim_{n \to \infty} \frac{F_{n+1}}{F_n} = L$$

and

$$\frac{F_{n+2}}{F_{n+1}} = 1 + \frac{1}{\frac{F_{n+1}}{F_n}},$$

thus

$$L = 1 + \frac{1}{L},$$

so

$$L^2 = L + 1,$$

or

$$L^2 - L - 1 = 0.$$

Next consider the relation $S_{n+3} = S_{n+2} - xS_{n+1} + x^3S_n$, expressed by the equation

$$K^3 - K^2 + xK - x^3 = 0,$$

or in factored form

$$(K - x)\left(K^2 - (1 - x)K + x^2\right) = 0.$$

$$\lim_{n\to\infty} \frac{S_{n+1}}{S_n} = L,$$

which is the root of the maximum modulus by Gauss's theorem. Further,

$$\lim_{n\to\infty} \frac{S_n}{S_{n+1} - x^2 S_{n-1}} = \frac{1}{\sqrt{1 - 2x - 3x^2}},$$

which is the generating function of the maximum values of the trinomial triangle.

Assume

$$\frac{S_n}{S_{n+1} - x^2 S_{n-1}} = \frac{\dfrac{S_n}{S_{n-1}}}{\dfrac{S_{n+1}}{S_{n-1}} - x^2} = \frac{L}{L^2 - x^2},$$

where

$$L = \lim_{n\to\infty} \frac{S_n}{S_{n-1}}$$

and

$$L^2 = \lim_{n\to\infty} \frac{S_{n+1}}{S_n} \cdot \frac{S_n}{S_{n-1}}.$$

The roots of

$$K^3 - K^2 + xK - x^3 = 0$$

are

$$x, \frac{1 - x - \sqrt{1 - 2x - 3x^2}}{2},$$

and

$$\frac{1 - x - \sqrt{1 - 2x - 3x^2}}{2}.$$

The dominant root is $\dfrac{1 - x + \sqrt{1 - 2x - 3x^2}}{2}$, which is L. Thus,

$$L^2 = \frac{(1 - x)^2 - 2x^2 + (1 - x)\sqrt{1 - 2x - 3x^2}}{2}$$

and

$$L^2 - x^2 = \frac{(1 - x)^2 - 4x^2 + (1 - x)\sqrt{1 - 2x - 3x^2}}{2}.$$

Therefore,

$$\begin{aligned}\frac{L}{L^2 - x^2} &= \frac{1 - x + \sqrt{1 - 2x - 3x^2}}{(1 - x)^2 - 4x^2 + (1 - x)\sqrt{1 - 2x - 3x^2}} \\ &= \frac{1 - x + \sqrt{1 - 2x - 3x^2}}{(1 - 2x - 3x^2) + (1 - x)\sqrt{1 - 2x - 3x^2}} \\ &= \frac{1}{\sqrt{1 - 2x - 3x^2}}.\end{aligned}$$

The generating functions for the odd cases were found to have the form

$$\frac{S_n(x)}{S_{n+1}(x) - x^2S_{n-1}(x)}.$$

The polynomials S_n with the recurrence $S_{n+3} = S_{n+2} - xS_{n+1} + x^3S_n$ are listed as follows:

$$S_0 = 0$$
$$S_1 = 1$$
$$S_2 = 1$$
$$S_3 = 1 - x$$
$$S_4 = 1 - 2x + x^3$$
$$S_5 = 1 - 3x + x^2 + 2x^3$$
$$S_6 = 1 - 4x + 3x^2 + 3x^3 - 2x^4$$
$$S_7 = 1 - 5x + 6x^2 + 3x^3 - 6x^4 + x^6$$

etc.

Thus, the generating functions for $N = 2n + 1$ are as follows:

$$N = 5 \text{ is } \frac{S_2}{S_3 - x^2S_1} = \frac{1}{1 - x - x^2}$$

$$N = 7 \text{ is } \frac{S_3}{S_4 - x^2S_2} = \frac{1 - x}{1 - 2x - x^2 - x^3}$$

$$N = 9 \text{ is } \frac{S_4}{S_5 - x^2S_3} = \frac{1 - 2x + x^3}{1 - 3x + 3x^3}$$

$$N = 11 \text{ is } \frac{S_5}{S_6 - x^2S_4} = \frac{1 - 3x + x^2 + 2x^3}{1 - 4x + 2x^2 + 5x^3 - 2x^4 - x^5}$$

$$N = 13 \text{ is } \frac{S_6}{S_7 - x^2S_5} = \frac{1 - 4x + 3x^2 + 3x^3 - 2x^4}{1 - 5x + 5x^2 + 6x^3 - 7x^4 - 2x^5 + x^6}$$

$$N = 15 \text{ is } \frac{S_7}{S_8 - x^2S_6} = \frac{1 - 5x + 6x^2 + 3x^3 - 6x^4 + x^6}{1 - 6x + 9x^2 + 5x^3 - 15x^4 + 5x^6}$$

Before the generating functions for the even cases are given, the Lucas, $L_n(x)$, and Fibonacci, $F_n(x)$, polynomials for the factor $K^2 - (1 - x)K + x^2$ will be derived. The Lucas and Fibonacci polynomials are defined:

$$L_n(x) = a^n(x) + b^n(x)$$
$$F_n(x) = a^n(x) - b^n(x)/a(x) - b(x)$$

where a and b are the roots of the polynomial equation

$$K^2 - A(x)K + B(x) = 0.$$

The recurrence relation for the Lucas polynomials is

$$L_{n+2}(x) = (1 - x)L_{n+1}(x) - x^2L_n(x).$$

The polynomials are

$$L_0 = 2$$
$$L_1 = 1 - x$$
$$L_2 = 1 - 2x - x^2$$
$$L_3 = 1 - 3x + 2x^3$$
$$L_4 = 1 - 4x + 2x^2 + 4x^3 - x^4$$
$$L_5 = 1 - 5x + 5x^2 + 5x^3 - 5x^4 - x^5$$

etc.

The recurrence relation for the Fibonacci polynomials is

$$F_{n+2}(x) = (1 - x)F_{n+1}(x) - x^2 F_n(x).$$

The polynomials are

$$F_0 = 0$$
$$F_1 = 1$$
$$F_2 = 1 - x$$
$$F_3 = 1 - 2x$$
$$F_4 = 1 - 3x + x^2 + x^3$$
$$F_5 = 1 - 4x + 3x^2 - 2x^3 - x^4$$

etc.

The generating functions for $N = 4n$ were found to have the form

$$\frac{F_n}{L_n}$$

and the generating functions for $N = 4n + 2$ were found to be

$$\frac{F_n - x^2 F_{n-1}}{L_n - x^2 L_{n-1}}.$$

They are listed below.

$$N = 4 \text{ is } \frac{F_1}{L_1} = \frac{1}{1 - x}$$

$$N = 6 \text{ is } \frac{F_1 - x^2 F_0}{L_1 - x^2 L_0} = \frac{1}{1 - x - 2x^2}$$

$$N = 8 \text{ is } \frac{F_2}{L_2} = \frac{1 - x}{1 - 2x - x^2}$$

$$N = 10 \text{ is } \frac{F_2 - x^2 F_1}{L_2 - x^2 L_1} = \frac{1 - x - x^2}{1 - 2x - 2x^2 + x^3}$$

$$N = 12 \text{ is } \frac{F_3}{L_3} = \frac{1 - 2x}{1 - 3x + 2x^3}$$

$$N = 14 \text{ is } \frac{F_3 - x^2F_2}{L_3 - x^2L_2} = \frac{1 - 2x - x^2 + x^3}{1 - 3x - x^2 + 4x^3 + x^4}$$

$$N = 16 \text{ is } \frac{F_4}{L_4} = \frac{1 - 3x + x^2 + x^3}{1 - 4x + 2x^2 + 4x^3 - x^4}$$

Lastly, we show

$$\lim_{n\to\infty} \frac{F_n}{L_n} = \frac{1}{\sqrt{1 - 2x - 3x^2}} \quad \text{and} \quad \lim_{n\to\infty} \frac{F_n - x^2F_{n-1}}{L_n - x^2L_{n-1}} = \frac{1}{\sqrt{1 - 2x - 3x^2}}.$$

We recall that the equation

$$K^2 - (1 - x)K + x^2 = 0$$

has roots

$$K_1 = \frac{(1 - x) + \sqrt{(1 - x)^2 - 4x^2}}{2} \quad \text{and} \quad K_2 = \frac{(1 - x) - \sqrt{(1 - x)^2 - 4x^2}}{2}.$$

We define

$$F_n = \frac{K_1^n - K_2^n}{K_1 - K_2}$$

and

$$L_n = K_1^n + K_2^n.$$

Note that

$$K_1 - K_2 = \sqrt{1 - 2x - 3x^2}.$$

Thus,

$$\frac{F_n}{L_n} = \frac{K_1^n - K_2^n}{(K_1 - K_2)(K_1^n + K_2^n)} = \frac{1 - \left(\dfrac{K_2}{K_1}\right)^n}{1 + \left(\dfrac{K_2}{K_1}\right)^n (K_1 - K_2)}$$

Now, since $K_1 > K_2$,

$$\lim_{n\to\infty} \frac{1 - \left(\dfrac{K_2}{K_1}\right)^n}{1 + \left(\dfrac{K_2}{K_1}\right)^n (K_1 - K_2)} = \frac{1}{\sqrt{1 - 2x - 3x^2}} = L.$$

We use this result to prove the second limit $= L$.

$$\lim_{n\to\infty} \frac{F_n - x^2F_{n-1}}{L_n - x^2L_{n-1}} = \frac{\dfrac{F_n}{L_{n-1}} - x^2\dfrac{F_{n-1}}{L_{n-1}}}{\dfrac{L_n}{L_{n-1}} - x^2\dfrac{L_{n-1}}{L_{n-1}}} = \frac{L^2 - x^2L}{L - x^2} = L,$$

since

$$\frac{F_n}{L_{n-1}} = \frac{F_n}{F_{n-1}}\,\frac{F_{n-1}}{L_{n-1}} = L^2.$$

4. GENERATING FUNCTIONS OF THE $(H - L)/k$ SEQUENCES IN A MULTINOMIAL TRIANGLE

We challenge the reader to find the generating functions of the $(H - L)/k$ sequences in the quadrinomial triangle. We surmise that the limits would be the generating functions of the central values in Pascal's quadrinomial triangle.

REFERENCES

1. John L. Brown, Jr., & V. E. Hoggatt, Jr., "A Primer for the Fibonacci Numbers, Part XVI: The Central Column Sequence," *The Fibonacci Quarterly* 16, No. 1 (1978):41.
2. Michel Y. Rondeau, "The Generating Functions for the Vertical Columns of $(N + 1)$-Nomial Triangles" (Master's thesis, San Jose State University, San Jose, California, May 1978).
3. Claudia R. Smith, "Sums of Partition Sets in the Rows of Generalized Pascal's Triangles" (Master's thesis, San Jose State University, San Jose, California, May 1978).

*****

SOLUTION OF $\binom{y+1}{x} = \binom{y}{x+1}$ IN TERMS OF FIBONACCI NUMBERS

JAMES C. OWINGS, JR.
University of Maryland, College Park, MD 20742

In [2, pp. 262-263] we solved the Diophantine equation $\binom{y+1}{x} = \binom{y}{x+1}$ and found that (x,y) is a solution iff for some $n \geq 0$,

$$(x + 1, y + 1) = \left(\sum_{k=0}^{n} f(4k + 1),\ \sum_{k=0}^{n} f(4k + 3)\right),$$

where

$$f(0) = 0,\ f(1) = 1,\ f(n + 2) = f(n) + f(n + 1).$$

We show here that (x,y) is a solution iff for some $n \geq 0$,

$$(x + 1, y + 1) = \big(f(2n + 1)f(2n + 2),\ f(2n + 2)f(2n + 3)\big),$$

incidentally deriving the identities

$$f(2n + 1)f(2n + 2) = \sum_{k=0}^{n} f(4k + 1),$$

$$f(2n + 2)f(2n + 3) = \sum_{k=0}^{n} f(4k + 3).$$

Briefly, in [2], we solved $\binom{y+1}{x} = \binom{y}{x+1}$ as follows. When multiplied out this equation becomes

$$x^2 + y^2 - 3xy - 2x - 1 = 0.$$

Now, if (x,y) is a solution of this polynomial equation, so are (x',y) and (x,y'), where $x' = -x + 3y + 2$ and $y' = -y + 3x$, because

$$\begin{aligned} 0 &= x^2 + y^2 - 3xy - 2x - 1 = y^2 + x(x - 3y - 2) - 1 \\ &= y^2 + x(-x') - 1 = y^2 + x'(-x) - 1 \\ &= y^2 + x'(x' - 3y - 2) - 1 = (x')^2 + y^2 - 3x'y - 2x' - 1, \end{aligned}$$

and similarly for (x,y'). So from the basic solution $x = 0$, $y = 1$ we get the four-tuple

$$(y',x,y,x') = (-1,0,1,5)$$

in which each adjacent pair of integers forms a solution. Repeating the process gives

$$(-1,-1,0,1,5,14);$$

doing it twice more we get

$$(-3,-2,-1,-1,0,1,5,14,39,103).$$

We have now found three solutions to $\binom{y+1}{x} = \binom{y}{x+1}$, namely (0,1), (5,14), (39,103). In [2] we showed, with little trouble, that all integral solutions to the given polynomial equation may be found somewhere in the two-way infinite chain generated by (0,1). (See Mills [1] for the genesis of this type of argument.) Hence (x,y) is a solution to the binomial equation iff $0 \leq x < y$ and (x,y) occurs somewhere in this chain. If we let

$$(x(0),y(0)) = (0,1),\ (x(1),y(1)) = (5,14), \text{ etc.},$$

and use our equations for x' and y', we find that

$$x(n + 1) = -x(n) + 3y(n) + 2,$$
$$y(n + 1) = -y(n) + 3x(n).$$

(WARNING: In [2] the roles of x and y are reversed.)

We prove our assertion by induction on n, appealing to the well-known identities

$$f^2(2n + 2) + 1 = f(2n + 1)f(2n + 3),$$
$$f^2(2n + 1) - 1 = f(2n)f(2n + 2).$$

Obviously, $x(0) + 1 = f(1)f(2)$, $y(0) + 1 = f(2)f(3)$. So assume

$$(x(n) + 1, y(n) + 1) = (f(2n + 1)f(2n + 2), f(2n + 2)f(2n + 3)).$$

Then

$$\begin{aligned} x(n + 1) + 1 &= 3y(n) - x(n) + 3 = 3(y(n + 1) + 1) - (x(n) + 1) + 1 \\ &= 3f(2n + 2)f(2n + 3) - f(2n + 1)f(2n + 2) + 1 \\ &= 2f(2n + 2)f(2n + 3) + f(2n + 2)(f(2n + 1) + f(2n + 2)) \\ &\qquad - f(2n + 1)f(2n + 2) + 1 \\ &= 2f(2n + 2)f(2n + 3) + (f^2(2n + 2) + 1) \\ &= 2f(2n + 2)f(2n + 3) + f(2n + 1)f(2n + 3) \\ &= f(2n + 2)f(2n + 3) + f^2(2n + 3) = f(2n + 3)f(2n + 4). \end{aligned}$$

So,

$$\begin{aligned} y(n+1) + 1 &= 3x(n+1) - y(n) + 1 \\ &= 3\big(x(n+1) + 1\big) - \big(y(n) + 1\big) - 1 \\ &= 3f(2n+3)f(2n+4) - f(2n+2)f(2n+3) - 1 \\ &= 2f(2n+3)f(2n+4) + f(2n+3)\big(f(2n+2) + f(2n+3)\big) \\ &\qquad - f(2n+2)f(2n+3) - 1 \\ &= 2f(2n+3)f(2n+4) + \big(f^2(2n+3) - 1\big) \\ &= 2f(2n+3)f(2n+4) + f(2n+2)f(2n+4) \\ &= f(2n+3)f(2n+4) + f^2(2n+4) \\ &= f(2n+4)f(2n+5), \end{aligned}$$

completing the proof.

REFERENCES

1. W. H. Mills, "A Method for Solving Certain Diophantine Equations," *Proc. Amer. Math. Soc.* 5 (1954):473-475.
2. James C. Owings, Jr., "An Elementary Approach to Diophantine Equations of the Second Degree," *Duke Math. J.* 37 (1970):261-273.

*****

THE DIOPHANTINE EQUATION $Nb^2 = c^2 + N + 1$

DAVID A. ANDERSON and MILTON W. LOYER
Montana State University, Bozeman, Mon. 59715

Other than $b = c = 0$ (in which case $N = -1$), the Diophantine equation $Nb^2 = c^2 + N + 1$ has no solutions. This family of equations includes the 1976 Mathematical Olympiad problem $a^2 + b^2 + c^2 = a^2b^2$ (letting $N = a^2 - 1$) and such problems as $6b^2 = c^2 + 7$, $a^2b^2 = a^2 + c^2 + 1$, etc.

Noting that $b^2 \neq 1$ (since $N \neq c^2 + N + 1$), one may restate the problem as follows:

$$\begin{aligned} Nb^2 &= c^2 + N + 1 \\ Nb^2 - N &= c^2 + 1 \\ N(b^2 - 1) &= c^2 + 1 \\ N &= (c^2 + 1)/(b^2 - 1). \end{aligned}$$

Thus the problem reduces to showing that, except as noted, $(c^2 + 1)/(b^2 - 1)$ cannot be an integer. [This result domonstrates the interesting fact that $c^2 \not\equiv -1 \pmod{b^2 - 1}$, i.e., that none of the Diophantine equations $c^2 \equiv 2 \pmod 3$, $c^2 \equiv 7 \pmod 8$, etc., has a solution.]

It is well known [1, p. 25] that for any prime p, $p \mid c^2 + 1 \Rightarrow p = 2$ or $p = 4m + 1$.*

$$\begin{aligned} b^2 - 1 \mid c^2 + 1 \Rightarrow b^2 - 1 &= 2^s(4m_1 + 1)(4m_2 + 1) \cdots (4m \;\; + 1) \\ &= 2^s(4M + 1) \\ b^2 &= 2^s(4M) + 2^s + 1 \end{aligned}$$

---

*The result of this article is not merely a special case of this theorem [e.g., according to the theorem $(c^2 + 1)/8$ could be an integer].

$$
\begin{aligned}
s \neq 0, \text{ since } s = 0 &\Rightarrow b^2 = 4M + 2\\
&\Rightarrow b^2 \text{ is even}\\
&\Rightarrow b \text{ is even}\\
&\quad (b/2)(b) \text{ is even}\\
\text{but } (b/2)(b) &= b^2/2 = 2M + 1, \text{ which is odd}\\
s > 0 &\Rightarrow b^2 \text{ is odd}\\
&\Rightarrow b \text{ is odd, so let } b = 2k + 1
\end{aligned}
$$

$$
\begin{aligned}
(2k + 1)^2 &= 2^s(4M) + 2^s + 1\\
4k^2 + 4k + 1 &= 2^s(4M) + 2^s + 1\\
4(k^2 + k - 2^sM) &= 2^s\\
&\Rightarrow s \geq 2\\
&\Rightarrow 4 \text{ is a factor of } b^2 - 1\\
&\Rightarrow 4 \mid c^2 + 1\\
&\Rightarrow c^2 + 1 = 4n\\
&\qquad c^2 = 4n - 1\\
&\Rightarrow c^2 \text{ is odd}\\
&\Rightarrow c \text{ is odd, so let } c = 2h + 1\\
(2h + 1)^2 &= 4n - 1\\
4h^2 + 4h + 1 &= 4n - 1\\
4h^2 + 4h + 2 &= 4n\\
2h^2 + 2h + 1 &= 2n
\end{aligned}
$$

But this is a contradiction (since the right-hand side of the equation is even, and the left-hand side of the equation is odd). So, $(c^2 + 1)/(b^2 - 1)$ cannot be an integer, and the Diophantine equation $Nb^2 = c^2 + N + 1$ has no nontrivial solution.

Following through the above proof, one can readily generalize

$$Nb^2 = c^2 + N + 1$$

to

$$Nb^2 = c^2 + N(4k + 1) + 1.$$

Just letting $N = 1$, one includes in the above result such Diophantine equations as

$$b^2 - c^2 = 6, \quad b^2 - c^2 = 10,$$

and, in general,

$$b^2 - c^2 \equiv 2 \pmod 4.$$

REFERENCE

1. I. M. Niven & H. S. Zuckerman, *Theory of Numbers* (New York: Wiley, 1960).

*****

MATRIX GENERATORS OF PELL SEQUENCES

JOSEPH ERCOLANO
Baruch College, CUNY

SECTION 1

The Pell sequence $\{P_n\}$ is defined recursively by the equation

$$P_{n+1} = 2P_n + P_{n-1}, \tag{1}$$

$n = 2, 3, \ldots$, where $P_1 = 1$, $P_2 = 2$. As is well known (see, e.g., [1]), the members of this sequence are also generated by the matrix

$$M = \begin{vmatrix} 2 & 1 \\ 1 & 0 \end{vmatrix},$$

since by taking successive positive powers of M one can easily establish that

$$M^n = \begin{vmatrix} P_{n+1} & P_n \\ P_n & P_{n-1} \end{vmatrix}.$$

Related to the sequence $\{P_n\}$ is the sequence $\{R_n\}$, which is defined recursively [1] by

$$R_{n+1} = 2R_n + R_{n-1},$$

$n = 2, 3, \ldots$, $R_1 = 2$, $R_2 = 6$. In what follows, we will require two other Pell sequences; they are best motivated by considering the following problem (cp. [2]): do there exist sequences $\{p_n\}$, $p_1 = 1$, satisfying (1) which are also "geometric" (i.e., the ratio between terms is constant)? These two requirements are easily seen to be equivalent to p_n satisfying the so-called "Pell equation" [1]:

$$p^2 = 2p + 1. \tag{2}$$

The positive root of this equation is $\psi = \frac{1}{2}(2 + \sqrt{8})$, and one easily checks that the sequence $\{\psi^n\}$ is a "geometric" Pell sequence. In a similar manner, by considering the negative root in (2), $\psi' = \frac{1}{2}(2 - \sqrt{8})$, one obtains a second geometric Pell sequence $\{\psi'^n\}$. (Since $\psi' = \frac{-1}{\psi}$, these two sequences are by no means distinct. However, it will be convenient in what follows to consider them separately.) That these four sequences are related to each other is apparent from the following well-known Binet-type formulas, which are verified mathematically by induction [1]:

$$P_n = \frac{\psi^n - \psi'^n}{\psi - \psi'}, \quad R_n = \psi^n + \psi'^n, \quad \psi^n = \frac{1}{2}(R_n + P_n\sqrt{8}).$$

Our purpose in this paper is threefold: we will give a constructive method for finding all possible matrix generators of the above Pell sequences; we show that, in fact, all such matrices are naturally related to each other; and finally, by applying well-known results from matrix algebra, we establish the above Binet-type formulas and several other well-known Pell identities.

SECTION 2

A direct calculation shows that the matrix

$$M = \begin{vmatrix} 2 & 1 \\ 1 & 0 \end{vmatrix}$$

satisfies the Pell equation; i.e.,

$$M^2 = 2M + I,$$

where $I = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}$. Let $A = \begin{vmatrix} x & y \\ u & v \end{vmatrix}$, where x, y, u, v are to be determined subject only to the condition that $xv - yu \neq 0$. Substitution of A into (2) results in the following system of scalar equations:

(3.1) $\quad x^2 - 2x - 1 + yu = 0$

(3.2) $\quad (x + v - 2)y = 0$

(3.3) $\quad (x + v - 2)u = 0$

(3.4) $\quad v^2 - 2v - 1 + yu = 0$

We now investigate possible solutions of these equations. Since the techniques are similar to those used in [3], we omit most of the details.

Case 1: $y = 0$

Equations (3.1), (3.4) reduce to the Pell equation, implying

$$x = \{\psi, \psi'\}, \; v = \{\psi, \psi'\}.$$

(a) If $u = 0$, we obtain the following matrix generators:

$$\Psi_0 = \begin{vmatrix} \psi & 0 \\ 0 & \psi' \end{vmatrix}, \qquad \Psi_1 = \begin{vmatrix} \psi & 0 \\ 0 & \psi \end{vmatrix},$$

$$\Psi_2 = \begin{vmatrix} \psi' & 0 \\ 0 & \psi \end{vmatrix}, \qquad \Psi_3 = \begin{vmatrix} \psi' & 0 \\ 0 & \psi' \end{vmatrix}.$$

(b) If $u \neq 0$, (3.3) implies $x + v = 2$, and hence, that

$$\Psi_{0u} = \begin{vmatrix} \psi & 0 \\ u & \psi' \end{vmatrix}, \qquad \Psi_{2u} = \begin{vmatrix} \psi' & 0 \\ u & \psi \end{vmatrix}.$$

The nth power of the matrix Ψ_{0u} is easily shown to be

$$\Psi_{0u}^n = \begin{vmatrix} \psi^n & 0 \\ P_n u & \psi'^n \end{vmatrix},$$

where $\{P_n\}$ is the sequence defined in (1).

Case 2: $y \neq 0$

(a) If $u = 0$, the situation is similar to that of Case 1(b), and we omit the details.

(b) Suppose $u \neq 0$. Equation (3.3) implies $x = 2 - v$—this is consistent with (3.2)—and substitution for x in (3.1) gives, after collecting terms

$$v^2 - 2v - 1 + yu = 0,$$

which is consistent with (3.4). Thus, the assumptions $y \neq 0$, $u \neq 0$ result in the following reduced system of equations:

$$v = \frac{1}{2}(2 \pm \sqrt{8 - 4yu}) \tag{4.1}$$

$$x = 2 - v. \tag{4.2}$$

Before investigating some matrix generators corresponding to solutions of the equations (4.1), (4.2), we pause to summarize our results.

We have been tacitly assuming that for a matrix A to be a generator of Pell sequences it must satisfy (2), the Pell equation. However, since our prototype generator is the matrix

$$M = \begin{vmatrix} 2 & 1 \\ 1 & 0 \end{vmatrix},$$

whose characteristic equation is easily seen to be the Pell equation (2), and since this latter equation is also the minimal equation for M, we would like to restrict our matrices A to those which also have the latter property. The initial assumption on A, $xv - yu \neq 0$, rules out, e.g., a matrix of the form

$$A = \begin{vmatrix} \psi & 0 \\ 0 & 0 \end{vmatrix},$$

which evidently satisfies (2). We would, however, also like to rule out matrices of the form Ψ_1 and Ψ_3 which satisfy (2) but do not have (2) as minimal equation. Thus, the following

Definition: A 2×2 matrix $A = \begin{vmatrix} x & y \\ u & v \end{vmatrix}$ is said to be a nontrivial generator of Pell sequences if $xv - yu \neq 0$, and its minimal equation is the Pell equation (2).

The above discussion then completely characterizes nontrivial generators of Pell sequences, which we summarize in the following:

Theorem: A 2×2 matrix A is a nontrivial generator of Pell sequences if and only if it is similar to

$$\Psi_0 = \begin{vmatrix} \psi & 0 \\ 0 & \psi' \end{vmatrix}.$$

Remark 1: Evidently, M is similar to Ψ_0. [We show below that M is obtained as a nontrivial generator by an appropriate choice of solutions to the system (4.1), (4.2).] In light of this similarity an indirect way of obtaining nontrivial generators is to form the product $Q\Psi_0Q^{-1}$, for any nonsingular matrix Q.

SECTION 3

Example 1: If we limit y, u to be positive integer values in (4.1), then there is a unique pair which keeps the radicand positive: $y = u = 1$. This results in two sets of solutions:

$$y = 1,\quad u = 1,\quad v = 2,\quad x = 0$$

and

$$y = 1,\quad u = 1,\quad v = 0,\quad x = 2.$$

The latter set results in the "M-matrix"

$$M = \begin{vmatrix} 2 & 1 \\ 1 & 0 \end{vmatrix},$$

where

$$M^n = \begin{vmatrix} P_{n+1} & P_n \\ P_n & P_{n-1} \end{vmatrix}.$$

(Cp. §1.) Since M^n is similar to Ψ_0^n, we conclude that the traces and determinants of these two matrices are the same. Hence,

$$(5)\qquad P_{n+1} + P_{n-1} = \psi^n + \psi'^n$$

$$(6)\qquad P_{n+1}P_{n-1} - P_n^2 = (-1)^n,$$

two well-known Pell identities [1].

Example 2: In (4.1), take $y = 2$, $u = 1$. Then one obtains

$$N = \begin{vmatrix} 1 & 2 \\ 1 & 1 \end{vmatrix},$$

and one easily checks that

$$N^n = \begin{vmatrix} \frac{1}{2}R_n & 2P_n \\ P_n & \frac{1}{2}R_n \end{vmatrix}.$$

Similarity of N^n with Ψ_0^n implies (trace invariance) that

$$(7)\qquad R_n = \psi^n + \psi'^n$$

and that (determinant invariance)

$$(8)\qquad R_n^2 - 8P_n^2 = 4(-1)^n.$$

Whereas, similarity of N^n with M^n implies, respectively (by trace and determinant invariance), that (cp. [1])

$$(9)\qquad R_n = P_{n+1} + P_{n-1}$$

$$(10)\qquad R_n^2 = 4(P_{n+1}P_{n-1} + P_n^2).$$

Example 3: In (4.1), take $y = 2$, $u = -1$; one possible set of solutions for x and v is, respectively, $x = 3$, $v = -1$, and we obtain

$$H = \begin{vmatrix} -1 & 2 \\ -1 & 3 \end{vmatrix},$$

$$H^n = \begin{vmatrix} -\frac{1}{2}R_{n-1} & 2P_n \\ -P_n & \frac{1}{2}R_{n+1} \end{vmatrix}.$$

Similarity of H^n with Ψ_0^n gives (cp. [1])

(11) $$R_{n+1} - R_{n-1} = 2(\psi^n + \psi'^n)$$

(12) $$8P_n^2 - R_{n+1}R_{n-1} = 4(-1)^n.$$

Note 1: Lines (12) and (8) imply that

$$R_n^2 - R_{n+1}R_{n-1} = 8(-1)^n,$$

or

$$R_{n+1}R_{n-1} - R_n^2 = 8(-1)^{n+1}.$$

(Cp. [1].)

Similarity of H^n with M^n gives

(13) $$P_{n+1} + P_{n-1} = \frac{1}{2}(R_{n+1} - R_{n-1})$$

(14) $$R_{n+1}R_{n-1} = 4(3P_n^2 - P_{n+1}P_{n-1}).$$

Similarity of H^n with N^n gives (cp. [1])

(15) $$R_{n+1} - R_{n-1} = 2R_n$$

(16) $$R_n^2 + R_{n+1}R_{n-1} = 16P_n^2.$$

Remark 2: Clearly, the computing of further matrix generators can be carried out in the same fashion as above. (The reader who is patient enough may obtain as his/her reward a new Pell identity.) In the next section, we concentrate our efforts on establishing the classical Binet-type formulas mentioned in §1. To this end, we will require not only the eigenvalues but the eigenvectors of two of our matrix generators.

SECTION 4

In (4.1), set $y = 0$, $u \neq 0$, but, for the time being, u otherwise arbitrary. From §1, we know that

$$\Psi_{0u} = \begin{vmatrix} \psi & 0 \\ u & \psi' \end{vmatrix},$$

$$\Psi_{0u}^n = \begin{vmatrix} \psi^n & 0 \\ P_n u & \psi'^n \end{vmatrix}.$$

An eigenvector corresponding to the eigenvalue ψ is computed to be

$$\begin{vmatrix} \dfrac{2\sqrt{2}}{u} \\ 1 \end{vmatrix};$$

while an eigenvector corresponding to ψ' is $\begin{vmatrix} 0 \\ 1 \end{vmatrix}$. Now take $u = \sqrt{2}$, set $S = \begin{vmatrix} 2 & 0 \\ 1 & 1 \end{vmatrix}$, and simply denote $\Psi_{0\sqrt{2}}$ by $\Psi_{\sqrt{2}}$. By similarity, $\Psi_{\sqrt{2}} = S\Psi_0 S^{-1}$, which implies that $\Psi^n_{\sqrt{2}} = S\Psi^n_0 S^{-1}$, and finally that

$$\Psi^n_{\sqrt{2}} S = S\Psi^n_0. \tag{17}$$

Writing out line (17) gives

$$\begin{vmatrix} \psi^n & 0 \\ P_n\sqrt{2} & \psi'^n \end{vmatrix} \begin{vmatrix} 2 & 0 \\ 1 & 1 \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 1 & 1 \end{vmatrix} \begin{vmatrix} \psi^n & 0 \\ 0 & \psi'^n \end{vmatrix}. \tag{18}$$

Multiplying out in (18), we have

$$\begin{vmatrix} 2\psi^n & 0 \\ P_n 2\sqrt{2} + \psi'^n & \psi'^n \end{vmatrix} = \begin{vmatrix} 2\psi^n & 0 \\ \psi^n & \psi'^n \end{vmatrix},$$

which implies that $P_n 2\sqrt{2} + \psi'^n = \psi^n$; or, recalling that $\psi - \psi' = 2\sqrt{2}$, we have

$$P_n = \frac{\psi^n - \psi'^n}{\psi - \psi'}, \tag{19}$$

the classical Binet-type formula.

To obtain the last of the Binet-type formulas, viz., $\psi^n = \frac{1}{2}(R_n + P_n\sqrt{8})$, we use the matrix

$$N = \begin{vmatrix} 1 & 2 \\ 1 & 1 \end{vmatrix}.$$

A pair of eigenvectors corresponding to ψ, ψ' are computed to be $\begin{vmatrix} \sqrt{2} \\ 1 \end{vmatrix}$, $\begin{vmatrix} -\sqrt{2} \\ 1 \end{vmatrix}$. Setting $T = \begin{vmatrix} \sqrt{2} & -\sqrt{2} \\ 1 & 1 \end{vmatrix}$, and proceeding as above, we have that

$$N^n T = T\Psi^n_0;$$

i.e., that

$$\begin{vmatrix} \frac{1}{2}R_n & 2P_n \\ P_n & \frac{1}{2}R_n \end{vmatrix} \begin{vmatrix} \sqrt{2} & -\sqrt{2} \\ 1 & 1 \end{vmatrix} = \begin{vmatrix} \sqrt{2} & -\sqrt{2} \\ 1 & 1 \end{vmatrix} \begin{vmatrix} \psi^n & 0 \\ 0 & \psi'^n \end{vmatrix}.$$

Multiplying out gives

$$\begin{vmatrix} \frac{\sqrt{2}}{2}R_n + 2P_n & \frac{-\sqrt{2}}{2}R_n + 2P_n \\ \sqrt{2}P_n + \frac{1}{2}R_n & -\sqrt{2}P_n + \frac{1}{2}R_n \end{vmatrix} = \begin{vmatrix} \sqrt{2}\psi^n & -\sqrt{2}\psi'^n \\ \psi^n & \psi'^n \end{vmatrix}$$

which implies that

$$\psi^n = \sqrt{2}P_n + \frac{1}{2}R_n = \frac{1}{2}(\sqrt{8}P_n + R_n).$$

REFERENCES

1. Marjorie Bicknell, "A Primer on the Pell Sequence and Related Sequences," *The Fibonacci Quarterly* 13, No. 4 (1975):345-349.
2. H. E. Huntley, *The Divine Proportion* (New York: Dover Pub., 1970).
3. Joseph Ercolano, "Golden Sequences of Matrices with Applications to Fibonacci Algebra," *The Fibonacci Quarterly* 14, No. 5 (1976):419-426.

*****

TWO THEOREMS CONCERNING HEXAGONAL NUMBERS

WILLIAM J. O'DONNELL
Sayre School, Lexington, KY 40506

Hexagonal numbers are the subset of polygonal numbers which can be expressed as $H_n = 2n^2 - n$, where $n = 1, 2, 3, \ldots$. Geometrically hexagonal numbers can be represented as shown in Figure 1.

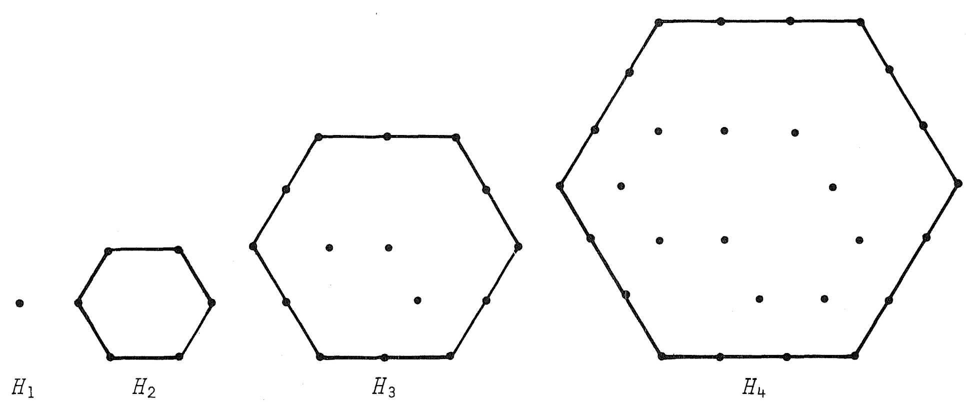

Figure 1

THE FIRST FOUR HEXAGONAL NUMBERS

Previous work by Sierpinski [1] has shown that there are an infinite number of triangular numbers which can be expressed as the sum and difference of triangular numbers, while Hansen [2] has proved a similar result for pentagonal numbers. This paper will present a proof that there are an infinite number of hexagonal numbers which can be expressed as the sum and difference of hexagonal numbers.

A table of hexagonal numbers is shown in Table 1.

Table 1

THE FIRST 100 HEXAGONAL NUMBERS

1	6	15	28	45	66	91	120	153	190
231	276	325	378	435	496	561	630	703	780
861	946	1035	1128	1225	1326	1431	1540	1653	1770
1891	2016	2145	2278	2415	2556	2701	2850	3003	3160
3321	3486	3655	3828	4005	4186	4371	4560	4753	4950
5151	5356	5565	5778	5995	6216	6441	6670	6903	7140
7381	7626	7875	8128	8385	8646	8911	9180	9453	9730
10011	10296	10585	10878	11175	11476	11781	12090	12403	12720
13041	13366	31695	14028	14365	14706	15051	15400	15753	16110
16471	16836	17205	17578	17955	18336	18721	19110	19503	19900

It is noted that

$$\begin{aligned} H_n - H_{n-1} &= [2n^2 - n] - [2(n-1)^2 - (n-1)] \\ &= 2n^2 - n - 2n^2 + 5n - 3 \\ &= 4n - 3. \end{aligned}$$

We observe that

(a) $H_{12} = H_5 + H_{11}$

(b) $H_{39} = H_9 + H_{38}$

(c) $H_{82} = H_{13} + H_{81}$

In each instance $H_m = H_{4n+1} + H_{m-1}$ for $n = 1, 2, 3, \ldots$. We note that

$$\begin{aligned} H_{4n+1} &= 2(4n+1)^2 - (4n+1) \\ &= 32n^2 + 12n + 1. \end{aligned}$$

From the previous work, it is clear that

$$H_j - H_{j-1} = 4j - 3 = 32n^2 + 12n + 1, \text{ for some } n.$$

Solving for j, we find that

$$j = 8n^2 + 3n + 1,$$

which is an integer. These results yield the following theorem.

Theorem 1: $H_{8n^2+3n+1} = H_{4n+1} + H_{8n^2+3n}$ for any integer $n \geq 1$.

For $n = 1, 2, 3, \ldots$, we have directly from Theorem 1 that

$$H_{8(4n)^2+3(4n)+1} = H_{4(4n)+1} + H_{8(4n)^2+3(4n)}$$

or

(1) $$H_{128n^2+12n+1} = H_{16n+1} + H_{128n^2+12n}.$$

Now consider $H_{128n^2+12n+1} = H_k - H_{k-1} = 4k - 3$. Then,

$$\begin{aligned} H_{128n^2+12n+1} &= 2(128n^2 + 12n + 1)^2 - (128n^2 + 12n + 1) \\ &= 32768n^4 + 6144n^3 + 672n^2 + 36n + 1 = 4k - 3. \end{aligned}$$

Solving for k, we find

$$k = 8192n^4 + 1536n^3 + 168n^2 + 9n + 1,$$

which is an integer. We now have

$$H_{128n^2+12n+1} = H_{8192n^4+1536n^3+168n^2+9n+1} - H_{8192n^4+1536n^3+168n^2+9n}. \tag{2}$$

Combining equations (1) and (2), we have the following theorem.

Theorem 2: For any integer $n \geq 1$,

$$\begin{aligned} H_{128n^2+12n+1} &= H_{16n+1} + H_{128n^2+12n} \\ &= H_{8192n^4+1536n^3+168n^2+9n} \\ &\quad - H_{8192n^4+1536n^3+168n^2+9n} \end{aligned}$$

For $n = 1, 2$, we have

$$\begin{aligned} H_{141} &= H_{17} + H_{140} \\ &= H_{9906} - H_{9905} \end{aligned}$$

or

$$\begin{aligned} 39{,}621 &= 561 + 39{,}061 \\ &= 196{,}247{,}766 - 196{,}208{,}145 \end{aligned}$$

and

$$\begin{aligned} H_{537} &= H_{33} + H_{536} \\ &= H_{144051} - H_{144050} \end{aligned}$$

or

$$\begin{aligned} 576{,}201 &= 2145 + 574{,}056 \\ &= 41{,}501{,}237{,}151 - 41{,}500{,}660{,}950. \end{aligned}$$

CONCLUSION

Theorem 2 establishes that there are an infinite number of hexagonal numbers which can be expressed as the sum and difference of hexagonal numbers. This result, along with the results of Sierpinski and Hansen, suggests that for any fixed polygonal number there are an infinite number of polygonal numbers which can be expressed as the sum and difference of similar polygonal numbers. A proof of this fact, though, is unknown to the author.

REFERENCES

1. W. Sierpinski, "Un théorème sur les nombres triangulaires," *Elemente der Mathematik* 23 (March 1968):31-32.
2. R. T. Hansen, "Arithmetic of Pentagonal Numbers," *The Fibonacci Quarterly* 8, No. 1 (1970):83-87.

*****

SOME SEQUENCES LIKE FIBONACCI'S

B. H. NEUMANN and L. G. WILSON
CSIRO Division of Mathematics and Statistics,
POB 1965, Canberra City, ACT 2601, Australia

INTRODUCTION

Define a sequence (T_n) of integers by

$$T_n = T_{n-1} + T_{n-2} + T_{n-3} + 1 \quad \text{when } n \text{ is even,}$$

$$T_n = T_{n-1} + T_{n-2} + T_{n-3} - 1 \quad \text{when } n \text{ is odd,}$$

or, more concisely, by

$$T_n = T_{n-1} + T_{n-2} + T_{n-3} + (-1) \ , \tag{1}$$

with initial values

$$T_1 = 0,\ T_2 = 2,\ T_3 = 3. \tag{2}$$

One of us (L.G.W.), playing with this sequence, had observed a number of apparent regularities, of which the most striking was that all positive prime numbers p divide T_p—at least as far as hand computation was practicable. He then communicated his observations to the other of us, who—being a professional mathematician—did not know the reason for this phenomenon, but knew whom to ask. Light was shed on the properties of the sequence by D. H. Lehmer,* who proved that, indeed, T_p is divisible by p whenever p is a positive prime number, and also confirmed the other observations made by one of us by experiment on some 200 terms of the sequence. [These further properties will not be referred to in the sequel—the reader, however, may wish to play with the sequence.]

In this note we shall present Lehmer's proof and state a conjecture of his, and then look at some other sequences with the same property.

LEHMER'S PROOF

It is convenient to replace the definition (1) of our sequence (T_n) by one that does not involve the parity of the suffix n, namely

$$T_n = 2T_{n-2} + 2T_{n-3} + T_{n-4}. \tag{3}$$

This is arrived at by substituting

$$T_{n-1} = T_{n-2} + T_{n-3} + T_{n-4} + (-1)^{n-1}$$

in (1) and observing that $(-1)^{n-1} + (-1)^n = 0$. As the recurrence relation (3) is of order 4, we now need 4 initial values, say

$$T_0 = 2,\ T_1 = 0,\ T_2 = 2,\ T_3 = 3. \tag{4}$$

It is well known that the general term of the sequence defined by (3) is of the form

$$T_n = A\alpha^n + B\beta^n + C\gamma^n + D\delta^n, \tag{5}$$

*The authors are greatly indebted, and deeply grateful, to Professor Lehmer for elucidating the properties of this sequence.

where α, β, γ, δ are the roots of the "characteristic equation" of (3),

(6) $$f(x) \equiv x^4 - 2x^2 - 2x - 1 = 0,$$

and where the constants A, B, C, D are determined from the initial values (4)

Put

$$S_n = \alpha^n + \beta^n + \gamma^n + \delta^n,$$

so that the sequence (S_n) satisfies the same recurrence relation as (T_n). If σ_1, σ_2, σ_3, σ_4 are the elementary symmetric functions of the roots of (6), that is

$$\sigma_1 = \alpha + \beta + \gamma + \delta = 0,$$

$$\sigma_2 = \alpha\beta + \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta + \gamma\delta = -2,$$

$$\sigma_3 = \alpha\beta\gamma + \alpha\beta\delta + \alpha\gamma\delta + \beta\gamma\delta = +2,$$

$$\sigma_4 = \alpha\beta\gamma\delta = -1,$$

where the values are read off the identity

$$f(x) \equiv x^4 - \sigma_1 x^3 + \sigma_2 x^2 - \sigma_3 x + \sigma_4,$$

then

$$S_1 = \sigma_1 = 0,$$

$$S_2 = \sigma_1^2 - 2\sigma_2 = 4,$$

$$S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 = 6,$$

and, of course,

$$S_0 = \alpha^0 + \beta^0 + \gamma^0 + \delta^0 = 4.$$

Thus, the initial values of (S_n) are just twice those of (T_n)—see (4)—and it follows that

$$T_n = \frac{1}{2}S_n$$

for all n, or, equivalently, that

$$A = B = C = D = \frac{1}{2}$$

in (5).

We now use the formula

(7) $$(x + y + z + y)^p = x^p + y^p + z^p + t^p + p \cdot F_p(x,y,z,t),$$

where p is a prime number, x, y, z, t are arbitrary integers, and $F_p(x,y,z,y)$ is an integer that depends on them and on p. This identity stems from the fact that in the multinomial expansion of the left-hand side of (7), each term is of the form

$$\frac{p!}{i!j!k!l!}x^i y^j z^k t^l$$

with $i + j + k + l = p$; and the coefficient $\frac{p!}{i!j!k!l!}$ is divisible by p unless one of the i, j, k, l equals p and the other three are zero. In our case, putting

$$x = \alpha,\ y = \beta,\ z = \gamma,\ t = \delta,$$

and recalling that $\alpha + \beta + \gamma + \delta = S_1 = 0$, we see that

$$S_p = -p \cdot F_p(\alpha, \beta, \gamma, \delta),$$

which is divisible by p. Thus also, $T_p = \frac{1}{2}S_p$ is divisible by p when p is an odd prime. But for $p = 2$ we also have this divisibility, as $T_2 = 2$. Thus, the following result is proved.

Theorem 1: If p is a positive prime number, then T_p, defined by the recurrence relation (3) with initial values (4), is divisible by p.

D. H. Lehmer calls a composite number q a *pseudoprime* for the sequence (T_n) if q divides T_q, and he conjectures that there are infinitely many such pseudoprimes. The smallest such pseudoprime is 30, and we have found no other. It may be remarked that when q is a power of a prime number, say $q = p^d$, then T_q is divisible by p but not, as far as we have been able to check, by any higher power of p.

OTHER SEQUENCES

Lehmer's argument presented above gives us immediately a prescription for making sequences of numbers, say (U_n), defined by a linear recurrence relation and with the property that for prime numbers p the pth term is divisible by p. All we have to ensure is that the roots of the characteristic equation add up to zero, and that the initial values give the sequence the right start. Thus, we have the following theorem.

Theorem 2: Let the sequence (U_n) of numbers be defined by the linear recurrence relation of degree $d > 1$:

(8) $$U_n = a_2U_{n-2} + a_3U_{n-3} + \cdots + a_dU_{n-d}$$

with integer coefficients $a_2, a_3, \ldots, a$ and initial values

(9) $$U_0 = d,\ U_1 = 0,\ U_2 = 2a_2,\ U_3 = 3a_3,\ \ldots,$$

and, generally,

(10) $$U_i = \alpha_1^i + \alpha_2^i + \cdots + \alpha_d^i,$$

where $\alpha_1, \alpha_2, \ldots, \alpha$ are the roots of the characteristic equation

$$x^d - a_2x^{d-2} - a_3x^{d-3} - \cdots - a_d = 0,$$

and $i = 0, 1, 2, \ldots, d - 1$. Then U_p is divisible by p for every positive prime number p.

The proof is the same, *mutatis mutandis*, as that of Theorem 1, and we omit it here.

We remark that $d = 2$ is uninteresting: we get $U_{2m} = 2a_2^m$ when $n = 2m$ is even, and $U_n = 0$ when n is odd. Thus, the first sequences of interest occur when $d = 3$. We briefly mention some examples.

Example 1: Put $d = 3$, $a_2 = 2$, $a_3 = 1$. The sequence can be defined by

$$U_n = U_{n-1} + U_{n-2} + (-1)^n,$$

which has the same growth rate, for $n \to \infty$, as the Fibonacci sequence. The pseudoprimes of this sequence, that is to say the positive composite integers q that divide U_q, appear to include the powers 4, 8, 16, ... of 2.

Example 2: Put $d = 3$, $a_2 = 1$, $a_3 = 1$. The sequence becomes

$$3, 0, 2, 3, 2, 5, 5, 7, 10, 12, \ldots,$$

with a much slower rate, for $n \to \infty$, than the Fibonacci sequence. The roots, say α, β, γ, of the characteristic equation are approximately

$$\alpha = 1.324718,$$
$$\beta = -0.662359 + i \cdot 0.5622795,$$
$$\gamma = -0.662359 - i \cdot 0.5622795,$$

and as $n \to \infty$, the ratio of successive terms of our sequence tends to α. This is substantially less than the ratio $\frac{1}{2} + \frac{1}{2}\sqrt{5} = 1.61803\ldots$ to which successive terms of the Fibonacci sequence tend. We have found no pseudoprimes for this sequence.

If the "dominant" root of the characteristic equation, that is the root with the greatest absolute value, is not single, real, and positive (if it is not real, then there is in fact a pair of dominant roots; and also in other cases there may be several dominant roots or repeated dominant roots), the sequence may oscillate between positive and negative terms, as it will also, in general, if continued backward to negative n.

Example 3: The sequence defined by

$$U_n = 3U_{n-2} - 2U_{n-3}$$

with initial values

$$U_0 = 3, \ U_1 = 0, \ U_2 = 6$$

has the property that positive prime numbers p divide U_p. It can also be described, explicitly, by

$$U_n = (-2)^n + 2.$$

For positive n, from $n = 2$ on, the terms are alternatingly positive and negative.

These sequences have, like the Fibonacci sequence, suggested to one of the authors an investigation of certain groups, but this is not the place to describe the problems and results. They are related to those of Johnston, Wamsley, and Wright [1].

REFERENCE

1. D. L. Johnston, J. W. Wamsley, & D. Wright, "The Fibonacci Groups," *Proc. London Math. Soc.* (3), 29 (1974):577-592.

*****

NEARLY LINEAR FUNCTIONS

V. E. HOGGATT, JR.
San Jose State University, San Jose, CA 95192

and

A. P. HILLMAN
University of New Mexico, Albuquerque, N.M. 87131

Let $\alpha = (1 + \sqrt{5})/2$, $[x]$ be the greatest integer in x, $a_1(n) = [\alpha n]$, and $a_2(n) = [\alpha^2 n]$. A partial table follows:

n	1	2	3	4	5	6	7	8	9	10	11
$a_1(n)$	1	3	4	6	8	9	11	12	14	16	17
$a_2(n)$	2	5	7	10	13	15	18	20	23	26	28

It is known (see [1]) that $a_1(n)$ and $a_2(n)$ form the nth safe-pair of Wythoff's variation on the game Nim. These sequences have many interesting properties and are closely connected with the Fibonacci numbers. For example, let

$$\sigma(n) = a_1(n + 1) - 1;$$

then

$$\sigma^2(n) = \sigma[\sigma(n)] = a_2(n + 1) - 2,$$

$$\sigma(F_n) = F_{n+1} \text{ for } n > 1,$$

and

$$\sigma(L_n) = L_{n+1} \text{ for } n > 2.$$

Here we generalize by letting d be in $\{2, 3, 4, \ldots\}$ and letting h_n be the dth-order generalized Fibonacci number defined by the initial conditions

(I) $\qquad h_i = 2^{i-1} \text{ for } 1 \leq i \leq d$

and the recursion

(R) $\qquad h_{n+d} = h_n + h_{n+1} + \cdots + h_{n+d-1}.$

The recursion (R) easily implies

(R′) $\qquad h_{n+d+1} = 2h_{n+d} - h_n \text{ or } h_n = 2h_{n+d} - h_{n+d+1}.$

The first of these is convenient for calculation of h_n for increasing values of n and the second for decreasing n.

Representations for integers as sums of distinct terms h_n will be used below to study some nearly linear functions from $N = \{0, 1, 2, \ldots\}$ to itself; these will include generalizations of the Wythoff sequences. Associated partitions of $Z^+ = \{1, 2, 3, \ldots\}$ will also be presented.

1. CHARACTERISTIC SEQUENCES

Let T be the set of all sequences $\{e_n\} = e_1, e_2, \ldots$ with each e_n in $\{0, 1\}$ and with an n_0 such that $e_n = 0$ for $n > n_0$. Let $z = z(E)$ be the smallest n with $e_n = 0$ and let E^* be the $\{e_n^*\}$ in T given by $e_n^* = 0$ for $n < z$, $e_z^* = 1$, and $e_n^* = e_n$ for $n > z$. If some $e_n = 1$, let $u(E)$ be the smallest such n.

If $E = \{e_n\}$ is in T and $Y = \{y_n\} = y_1, y_2, \ldots$ is any sequence of integers, then $e_1 y_1 + e_2 y_2 + \cdots$ is really a finite sum which we denote by $E \cdot Y$. For each integer j, let $H_j = \{h_{n+j}\} = h_{j+1}, h_{j+2}, \ldots$ where the h_n are defined by (I) and (R). Also, let $H = H_0$.

Lemma 1: Let $z = z(E)$ and $b = E^* \cdot H_j - E \cdot H_j$. Then

(a) $u(E^*) = z$.

(b) If $z = 1$, $b = h_{j+1}$. If $z > 1$, $b = h_{z+j} - h_{z+j-1} - h_{z+j-2} - \cdots - h_{j+1}$.

(c) If $1 \leq z \leq d$ and $j = 0$, $b = 1$.

Proof: Parts (a) and (b) follow immediately from the relevant definitions. Then (c) follows from (b), the initial conditions (I), and the fact that

$$1 + 2 + \cdots + 2^{z-2} = 2^{z-1} - 1.$$

2. THE SUBSET S OF T

Let S consist of the $\{c_n\}$ in T with

$$c_n c_{n+1} \cdots c_{n+d-1} = 0 \quad \text{for all } n \text{ in } Z^+.$$

Lemma 2: If C is in S then:

(a) $1 \leq z(C) \leq d$,

and

(b) $C^* \cdot H - C \cdot H = 1$.

Proof: Part (a) follows from the defining condition, with $n = 1$, for the subset S. Then Lemma 1(c) implies the present part (b).

Lemma 3: If $C \cdot H = C' \cdot H$ with C and C' in S, then $C = C'$.

Proof: Let $C = \{c_n\}$ and $C' = \{c'_n\}$. We assume $C \neq C'$ and seek a contradiction. Then $c_k \neq c'_k$ for some k, and there is a largest such k since $c_n = 0 = c'_n$ for n large enough. We use this maximal k and without loss of generality assume that $c_k = 0$ and $c'_k = 1$. Then

$$C' \cdot H - C \cdot H = \sum_{i=1}^{k} (c'_i - c_i)h_i \leq h_k - \sum_{i=1}^{k-1} c_i h_i, \tag{1}$$

since $h_i > 0$ for $i > 0$. Let $k = qd + r$, where q and r are integers with $0 \leq r < d$. Then one can use (R) to show that

$$h_k = (h_1 + h_2 + h_3 + \cdots + h_{k-1}) - (h_r + h_{r+d} + h_{r+2d} + \cdots + h_{k-d}) + 1. \tag{2}$$

(The interpretation of this formula when $1 \leq k < d$ is not difficult.) Since $c_n = 0$ for at least one of any d consecutive values of n and $h_n < h_{n+1}$ for $n > 0$, (2) implies that

$$h_k > c_1 h_1 + c_2 h_2 + \cdots + c_{k-1} h_{k-1}.$$

This and (1) give us the contradiction $C' \cdot H > C \cdot H$. Hence $C' = C$, as desired.

Lemma 4: For every E in T there is a C in S such that:

(a) $E \cdot H_j = C \cdot H_j$ for all j,

(b) $z(E) \equiv z(C) \pmod{d}$,

(c) $u(E) \equiv u(C) \pmod{d}$.

(d) This C is uniquely determined by E.

Proof: We may assume that $E = \{e_n\}$ is not in S. Then

$$e_k e_{k+1} \cdots e_{k+d-1} = 1 \text{ for some } k.$$

There is a largest such k since $e_n = 0$ for large enough n. Using this maximal k, one has $e_{k+d} = 0$ and we let $E' = \{e'_n\}$ be given by $e'_n = 0$ for $k \leq n < k + d$, $e'_{k+d} = 1$, and $e'_n = e_n$ for all other n. The recursion (R) implies that $E \cdot H_j = E' \cdot H_j$ for all j. It is also clear that $z(E) \equiv z(E') \pmod{d}$ and $u(E) \equiv u(E') \pmod{d}$. If E' is not in S, we give it the same treatment given E. After a finite number of such steps, one obtains a C in S with the desired properties. Lemma 3 tells us that this C is uniquely determined by E.

3. THE BIJECTION BETWEEN N AND S

We next establish a 1-to-1 correspondence $m \longleftrightarrow C_m = \{c_{mn}\}$ between the nonnegative integers m and the sequences of S.

Lemma 5: S is a sequence $C_0, C_1, \ldots$ of sequences C_m such that $C_m \cdot H = m$ and $u(C_{m+1}) \equiv z(C_m) \pmod{d}$.

Proof: The only C in S with $C \cdot H = 0$ is

$$C_0 = \{c_{0n}\} = 0, 0, 0, \ldots .$$

Now, assume inductively that for some k in N there is a unique C_k in S with $C_k \cdot H = k$. Then Lemma 2(b) tells us that $C_k^* \cdot H = C_k \cdot H + 1 = k + 1$. It follows from Lemma 4 that there is a unique C_{k+1} in S with $C_{k+1} \cdot H = C_k^* \cdot H = k + 1$. Finally, $u(C_{m+1}) \equiv z(C_m) \pmod{d}$ is a consequence of Lemma 1(a) and Lemma 4(c). The desired results then follow by induction.

Lemma 6: Let E be in T and $E \cdot H = m$. Then $E \cdot H_j = C_m \cdot H_j$, for all j, $z(E) \equiv z(C_m) \pmod{d}$, and $u(E) \equiv u(C_m) \pmod{d}$.

Proof: Lemma 4 tells us that there us a C in S with $E \cdot H_j = C \cdot H_j$ for all integers j, $z(E) \equiv z(C) \pmod{d}$, and $u(E) \equiv u(C) \pmod{d}$. The hypothesis $E \cdot H = m$ and Lemma 5 then imply that $C = C_m$.

4. THE SHIFT FUNCTIONS

Let functions $\sigma^i(m)$ from $N = \{0, 1, \ldots\}$ into $Z = \{\ldots, -2, -1, 0, 1, \ldots\}$ be given for all integers i by

(3) $$\sigma^i(m) = C_m \cdot H_i .$$

That is, $\sigma^i(C_m \cdot H) = C_m \cdot H_i$. Using this, one sees easily that

$$\sigma^i[\sigma^j(m)] = \sigma^{i+j}(m)$$

for all integers i and j and all m in N. We also note that

$$\sigma^0(m) = C_m \cdot H = m.$$

Lemma 7:

(a) $\sigma^j(0) = 0$ and $\sigma^j(h_n) = h_{n+j}$ for all integers j and n.

(b) $\sigma^j(E \cdot H) = E \cdot H_j$ for all integers j and all E in T.

(c) If E and E' are in T, $E \cdot E' = 0$, $E \cdot H = m$, and $E' \cdot H = n$, then

$$\sigma^j(m + n) = \sigma^j(m) + \sigma^j(n) \text{ for all } j \text{ in } Z.$$

Proof: Part (a) is clear. Part (b) follows from (3) and Lemma 6. For (c), let $E = \{e_n\}$, $E' = \{e'_n\}$, and $y_n = e_n + e'_n$. The hypothesis $E \cdot E'$ implies that $Y = \{y_n\}$ is in T. Then $Y \cdot H = E \cdot H + E' \cdot H = m + n$. This and (b) tell us that $\sigma^j(m + n) = Y \cdot H_j$, which equals $E \cdot H_j + E' \cdot H_j = \sigma^j(m) + \sigma^j(n)$, as desired.

5. A PARTITION OF Z^+

For $i = 1, 2, \ldots, d$ let A_i be the set of all positive integers m for which $u(C_m) \equiv i \pmod{d}$. Clearly these A_i partition Z^+, i.e., they are disjoint and their union is Z^+.

Lemma 8: Let k be in A_i. Then $k = h_i + C \cdot H_i$ for some C in S.

Proof: Let $u(C_k) = u$. Then

(4) $$k = h_u + c_{k,u+1}h_{u+1} + \cdots = h_u + C' \cdot H_u \text{ for some } C' \text{ in } S.$$

Since k is in A_i, $u \equiv i \pmod{d}$. If $u > i$, we use (4) and the recursion (R) to obtain

$$k = h_{u-d} + h_{u-d+1} + \cdots + h_{u-1} + C' \cdot H_u = h_{u-d} + C'' \cdot H_{u-d},$$

with C'' in S.

If $u - d > i$, we continue this process until we have $k = h_i + C \cdot H_i$ with C in S. This completes the proof.

Now, for every integer j, we define a function a_j from Z^+ into Z by

$$a_j(n) = h_j + \sigma^j(n-1).$$

Clearly this means that, for m in N,

(5) $$a_j(m+1) = h_j + C_m \cdot H_j = h_j + c_{m1}h_{j+1} + c_{m2}h_{j+2} + \cdots.$$

It follows from (5) that, for constant k, $a_n(k)$ has the same recursion formulas as the h_n. In particular,

(6) $$a_{j+1}(n) = 2a_j(n) - a_{j-d}(n).$$

Lemma 9: $\{a_i(r) \mid r \in Z^+\} = A_i$ for $1 \le i \le d$.

Proof: Let r be in Z^+ and $m = r - 1$. One sees from (5) that

$$a = a_i(r) = a_i(m+1)$$

if of the form $E \cdot H$ with $u(E) = i$. Then $i \equiv u(C_a) \pmod{d}$ by Lemma 6. Hence a is in A_i.

Now let $k \in A_i$. Then Lemma 8 tells us that $k = h_i + C \cdot H_i$ with C in S. Let $C \cdot H = m$. Then $C = C_m$ and it follows from (5) that

$$k = a_i(m+1) \in \{a_i(r) \mid r \in Z^+\}.$$

This completes the proof.

6. SELF-GENERATING SEQUENCES

Next we define b_{ij} for $1 \le i \le d$ and all integers j by

(7) $$b_{1j} = h_{j+1},\ b_{ij} = h_{i+j} - h_{i+j-1} - h_{i+j-2} - \cdots - h_{j+1} \text{ for } 2 \le i \le d.$$

We will use these b_{ij} to show that the sets A_i are self-generating and to count the integers in $A_i \cap \{1, 2, \ldots, n\}$.

One can show that the b_{ij} could be defined alternatively by the initial conditions $b_{i0} = 1$ for $1 \le i \le d$ and the recursion formulas

$$b_{i,j+1} = b_{1j} + b_{i+1,j} \text{ for } 1 \le i < d;\ b_{d,j+1} = b_{1j} = b_{j+1}.$$

These show, for example, that

(8) $$b_{i1} = 2 \text{ for } 1 \le i < d \quad\text{and}\quad b_{d1} = 1.$$

The definition (7) for b_{in} in terms of the h's implies that, for fixed i, the b_{in} satisfy the same recursion formulas as the h_n; in particular, one has

$$b_{in} = 2b_{i,n+d} - b_{i,n+d+1}.$$

This can be used to show that

(9) $$b_{i,-i} = 1 \text{ for } 1 \leq i \leq d, \; b_{ij} = 0 \text{ for } -d \leq j < 0 \text{ and } i \neq -j.$$

Theorem 1: Let $b_j(m) = a_j(m + 1) - a_j(m)$. Then $b_j(m) = b_{ij}$ for m in A_i.

Proof: It follows from (5) that $b_j(m) = C_m \cdot H_j - C_{m-1} \cdot H_j$. In the proof of Lemma 5, we saw that $C_m \cdot H_j = C^*_{m-1} \cdot H_j$; hence

(10) $$b_j(m) = C_{m-1} \cdot H_j - C^*_{m-1} \cdot H.$$

Let $u = u(C_m)$ and $z = z(C_{m-1})$. The hypothesis $m \in A_i$ means that $u \equiv i \pmod d$. Then $z \equiv i \pmod d$ by Lemma 5. This, the fact that $1 \leq i \leq d$, and Lemma 2(a) imply that $z = i$. Finally, $z = i$ and Lemma 1 tell us that the $b_j(m)$ of (10) is equal to the b_{ij} defined in (7).

Theorem 2: For $1 \leq i \leq d$, $b_{-i}(m)$ equals 1 when m is in A_i and equals 0 when m is not in A_i.

Proof: This follows from Theorem 1 and the formulas in (9).

Theorem 3: The number of integers in the intersection of A_i and $\{1, 2, \ldots, m\}$ is $a_{-i}(m + 1)$ for $1 \leq i < d$ and is $a_{-d}(m + 1) - 1$ for $i = d$.

Proof: One sees that $a_{-i}(1) = h_{-i} + C_0 \cdot H_{-i} = h_{-i} = 0$ for $1 \leq i < d$ and that $a_{-d}(1) = h_{-d} = 1$. It is also clear that

$$a_{-i}(m + 1) = a_{-i}(1) + b_{-i}(1) + b_{-i}(2) + \cdots + b_{-i}(m).$$

This and Theorem 2 give us the desired result.

7. COMPOSITES

First we note that

(11) $$a_i\,[a_j(n)] = h_i + \sigma^i[a_j(n) - 1] = h_i + \sigma^i[h_j - 1 + \sigma^j(n - 1)].$$

For $1 \leq j \leq d$, we have $h_j = 2^{j-1}$ and hence we have

$$h_j - 1 = h_1 + h_2 + \cdots + h_{j-1} \quad \text{for } 1 < j \leq d.$$

Also, we know that $\sigma^j(n - 1)$ is of form $c_1h_{j+1} + c_2h_{j+2} + \cdots$ with c_k in $\{0, 1\}$. Hence (11) leads to

$$\begin{aligned} a_i[a_j(n)] &= h_i + \sigma^i[h_1 + h_2 + \cdots + h_{j-1} + c_1h_{j+1} + \cdots] \\ &= h_i + h_{i+1} + h_{i+2} + \cdots + h_{i+j-1} + c_1h_{i+j+1} + \cdots \\ &= h_i + h_{i+1} + \cdots + h_{i+j-1} + \sigma^{i+j}(n - 1) \end{aligned}$$

(12) $$= h_i + h_{i+1} + \cdots + h_{i+j-1} - h_{i+j} + a_{i+j}(n)$$

for $1 < j \leq d$ and all integers i.

Letting $i = -d$ and using the facts that $h_{-d} = 1 = h_0$ and $h_n = 0$ for $-d < n < 0$, (12) implies that

(13) $$a_{-d}[a_j(n)] = 1 + a_{j-d}(n) \quad \text{for } 1 \leq j < d, \quad a_{-d}[a_d(n)] = a_0(n) = n.$$

Our derivation applies for $1 < j \leq d$, but the result in (13) for $j = 1$ can also be seen to be true.

One may note that (12) implies

$$a_i[a_j(n)] - a_j[a_i(n)] = h_i + h_{i+1} + \cdots + h_{j-1} \text{ for } 1 \le i < j \le d.$$

Theorem 4: For $1 \le j < d$, $a_{j+1}(n)$ is $2a_j(n)$ minus the number of integers in the intersection of A_d and

$$\{1, 2, 3, \ldots, a_j(n) - 1\}.$$

Proof: Since the $a_n(m)$, for fixed m, satisfy the same recursion formula as the h_n, we see from (R′) that

$$a_{j+1}(n) = 2a_j(n) - a_{j-d}(n).$$

This and (13) give us

$$a_{j+1}(n) = 2a_j(n) + \{a_{-d}[a_j(n)] - 1\} \text{ for } 1 \le j < d. \tag{14}$$

Using Theorem 3, we note that the expression in braces in (14) counts the integers that are in both A_d and $\{1, 2, \ldots, a_j(n) - 1\}$. This establishes the theorem.

Theorem 4 provides a very simple procedure for calculating the $a_j(n)$ for $1 \le j \le d$. We know that $a_1(1) = 1$. Then the theorem gives us $a_j(1)$ for $1 < j \le d$. Next, $a_1(2)$ must be the smallest positive integer not among the $a_j(1)$ and the theorem gives us the remaining $a_j(2)$. Thus, one obtains the $a_j(3)$, and $a_j(4)$, etc.

Theorem 5: For $1 \le j < d$, let $g_j(m) = a_{j+1}(m) - a_j(m)$, and $G_j = \left\{g_j(m) \,\middle|\, m \in Z^+\right\}$. Then $G_1, G_2, \ldots, G_{d-1}$ form a partition of Z^+.

Proof: Let Z^* be the set of positive integers that are not in A_d. For every n in Z^* there are integers m and j with $n = a_j(m)$, $m \ge 1$, and $1 \le j < d$; we let $x(n)$ be $g_j(m)$ for this m and j. Let $a_d(m) = a_m$ for m in Z^+.

Then it follows from Theorem 4 that

$$x(n) = a_{j+1}(m) - a_j(m) = a_j(m) = n \text{ for } n = 1, 2, \ldots, a_1 - 1;$$

$$x(n) = a_j(m) - 1 = n - 1 \text{ for } n = a_1 + 1, a_1 + 2, \ldots, a_2 - 1;$$

and in general that

$$x(n) = n - r \text{ for } n = a_r + 1, a_r + 2, \ldots, a_{r+1} - 1.$$

This shows that every positive integer is an $x(n)$ for exactly one n in Z^* and hence is in exactly one of the G_j, as desired.

8. BIBLIOGRAPHY

This paper is self-contained except for motivation. Related material is contained in [1], [2], and [3] and in the papers of the bibliography in [2]. It is expected to have sequels to the present paper.

REFERENCES

1. L. Carlitz, Richard Scoville, & V. E. Hoggatt, Jr., "Fibonacci Representations," *The Fibonacci Quarterly* 10, No. 1 (1972):29-42.
2. A. F. Horadam, "Wythoff Pairs," *The Fibonacci Quarterly* 16, No. 2 (1978): 147-151.
3. V. E. Hoggatt, Jr., and A. P. Hillman, "A Property of Wythoff Pairs," *The Fibonacci Quarterly* 16, No. 5 (1978):472.

*****

ELEMENTARY PROBLEMS AND SOLUTIONS

Edited by
A. P. HILLMAN
University of New Mexico, Albuquerque, NM 87131

Send all communications regarding ELEMENTARY PROBLEMS AND SOLUTIONS *to* Professor A. P. Hillman, 709 Solano Dr., S.E., Albuquerque, New Mexico 87108. *Each solution or problem should be on a separate sheet (or sheets). Preference will be given to those typed with double spacing in the format used below. Solutions should be received within 4 months of the publication date.*

DEFINITIONS

The Fibonacci numbers F_n and Lucas numbers L_n satisfy $F_{n+2} = F_{n+1} + F_n$, $F_0 = 0$, $F_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$, $L_0 = 2$, $L_1 = 1$. Also a and b designate the roots $(1 + \sqrt{5})/2$ and $(1 - \sqrt{5})/2$, respectively, of $x^2 - x - 1 = 0$.

PROBLEMS PROPOSED IN THIS ISSUE

B-394 *Proposed by Phil Mana, Albuquerque, NM.*

Let $P(x) = x(x - 1)(x - 2)/6$. Simplify the following expression:

$P(x + y + z) - P(y + z) - P(x + z) - P(x + y) + P(x) + P(y) + P(z)$.

B-395 *Proposed by V. E. Hoggatt, Jr., San Jose State University, San Jose, CA.*

Let $c = (\sqrt{5} - 1)/2$. For $n = 1, 2, 3, \ldots$, prove that

$$1/F_{n+2} < c^n < 1/F_{n+1}.$$

B-396 *Based on the solution to B-371 by Paul S. Bruckman, Concord, CA.*

Let $G_n = F_n(F_n + 1)(F_n + 2)(F_n + 3)/24$. Prove that 60 is the smallest positive integer m such that $10 | G_n$ implies $10 | G_{n+m}$.

B-397 *Proposed by Gregory Wulczyn, Bucknell University, Lewisburg, PA.*

Find a closed form for the sum

$$\sum_{k=0}^{2s} \binom{2s}{k} F_{n+kt}^2.$$

B-398 *Proposed by Herta T. Freitag, Roanoke, Va.*

Is there an integer K such that

$$K - F_{n+6} + \sum_{j=1}^{n} j^2 F_j$$

is an integral multiple of n for all positive integers n?

B-399 *Proposed by V. E. Hoggatt, Jr., San Jose State University, San Jose, CA.*

Let $f(x) = u_1 + u_2x + u_3x^2 + \cdots$ and $g(x) = v_1 + v_2x + v_3x^2 + \cdots$, where $u_1 = u_2 = 1$, $u_3 = 2$, $u_{n+3} = u_{n+2} + u_{n+1} + u_n$, and $v_{n+3} = v_{n+2} + v_{n+1} + v_n$. Find initial values v_1, v_2, and v_3 so that $e^{g(x)} = f(x)$.

SOLUTIONS

Nonhomogeneous Difference Equation

B-370 *Proposed by Gregory Wulczyn, Bucknell University, Lewisburg, PA.*

Solve the difference equation: $u_{n+2} - 5u_{n+1} + 6u_n = F_n$.

Solution by Phil Mana, Albuquerque, NM.

Let E be the operator with $Ey_n = y_{n+1}$. The given equation can be rewritten as

$$(E - 2)(E - 3)U_n = F_n.$$

Operating on both sides of this with $(E - a)(E - b)$, where a and b are the roots of $x^2 - x - 1 = 0$, one sees that the solutions of the original equation are among the solutions of

$$(E - a)(E - b)(E - 2)(E - 3)U_n = 0.$$

Hence, $U_n = ha^n + kb^n + 2^n c + 3^n d$. Here, c and d are arbitrary constants. But h and k can be determined using $n = 0$ and $n = 1$, and one finds that $ha^n + kb^n = L_{n+3}/5$. Thus, $U_n = (L_{n+3}/5) + 2^n c + 3^n d$.

Also solved by Paul S. Bruckman, C. B. A. Peck, Bob Prielipp, Sahib Singh, and the proposer.

No, No, Not Always

B-371 *Proposed by Herta T. Freitag, Roanoke, VA.*

Let $S_n = \sum_{k=1}^{F_n} \sum_{j=1}^{k} T_j$, where T_j is the triangular number $j(j+1)/2$. Does each of $n \equiv 5 \pmod{15}$ and $n \equiv 10 \pmod{15}$ imply that $S_n \equiv 0 \pmod{10}$? Explain.

I. Solution by Sahib Singh, Clarion College, PA.

The answer to both questions is in the negative as explained below:

$$\sum_{j=1}^{k} T_j = \sum_{j=1}^{k} \binom{j+1}{2} = \binom{k+2}{3}$$

$$S_n = \sum_{k=1}^{F_n} \binom{k+2}{3} = \binom{F_n+3}{4} = F_n(F_n+1)(F_n+2)(F_n+3)/24.$$

One can show that $S_{25} \not\equiv 0 \pmod{10}$ and $S_{35} \not\equiv 0 \pmod{10}$ even though $25 \equiv 10 \pmod{15}$ and $35 \equiv 5 \pmod{15}$.

II. From the solution by Paul S. Bruckman, Concord, CA.

It can be shown that $S \equiv 0 \pmod{10}$ if and only if $n \equiv r \pmod{60}$ where $r \in \{0, 5, 6, 7, 10, 12, 17, 18, 20, 24, 29, 30, 31, 32, 34, 36, 43, 44, 46, 53, 54, 56, 58\}$.

Also solved by Bob Prielipp, Gregory Wulcyzn, and the proposer.

Still No

B-372 *Proposed by Herta T. Freitag, Roanoke, VA.*

Let S_n be as in B-371. Does $S_n \equiv 0 \pmod{10}$ imply that n is congruent to either 5 or 10 modulo 15? Explain.

Solution by Paul S. Bruckman, Concord, CA.

$S_6 = \binom{F_6+3}{4} = \binom{11}{4} = 11 \cdot 10 \cdot 9 \cdot 8/24 = 330 \equiv 0 \pmod{10}$ but 6 is not congruent to 5 or 10 modulo 15.

Also solved by Bob Prielipp, Sahib Singh, Gregory Wulczyn, and the proposer.

Golden Cosine

B-373 *Proposed by V. E. Hoggatt, Jr., San Jose State University, San Jose, CA and P. L. Mana, Albuquerque, NM.*

The sequence of Chebyshev polynomials is defined by

$$C_0(x) = 1,\ C_1(x) = x, \text{ and } C_n(x) = 2xC_{n-1}(x) - C_{n-2}(x)$$

for $n = 2, 3, \ldots$. Show that $\cos[\pi/(2n+1)]$ is a root of

$$[C_{n+1}(x) + C_n(x)]/(x+1) = 0$$

and use a particular case to show that $2\cos(\pi/5)$ is a root of

$$x^2 - x - 1 = 0.$$

Solution by A. G. Shannon, Linacre College, University of Oxford.

It is known that if $x = \cos\theta$ then $C_n(x) = \cos n\theta$. Letting

$$\theta = \pi/(2n+1),$$

one has

$$x + 1 = \cos\theta + 1 \neq 0$$

and

$$C_{n+1}(x) + C_n(x) = \cos[(n+1)\pi/(2n+1)] + \cos[n\pi/(2n+1)]$$
$$= -\cos[n\pi/(2n+1)] + \cos[n\pi/(2n+1)] = 0$$

as required, since $\cos(\pi - \alpha) = -\cos\alpha$.

The special case $n = 2$ shows us that $\cos(\pi/5)$ is a solution of

$$[C_3(x) + C_2(x)]/(x+1) = 0,$$

which turns out to be

$$(2x)^2 - 2x - 1 = 0.$$

Hence, $2\cos(\pi/5)$ satisfies $x^2 - x - 1 = 0$.

Also solved by Paul S. Bruckman, Bob Prielipp, Sahib Singh, and the proposer.

Fibonacci in Trigonometric Form

B-374 *Proposed by Frederick Stern, San Jose State University, San Jose, CA.*

Show both of the following:

$$F_n = \frac{2^{n+2}}{5}\left[\left(\cos\frac{\pi}{5}\right)^n \sin\frac{\pi}{5}\sin\frac{3\pi}{5} + \left(\cos\frac{3\pi}{5}\right)^n \sin\frac{3\pi}{5}\sin\frac{9\pi}{5}\right],$$

$$F_n = \frac{(-2)^{n+2}}{5}\left[\left(\cos\frac{2\pi}{5}\right)^n \sin\frac{2\pi}{5}\sin\frac{6\pi}{5} + \left(\cos\frac{4\pi}{5}\right)^n \sin\frac{4\pi}{5}\sin\frac{12\pi}{5}\right].$$

Solution by A. G. Shannon, Linacre College, University of Oxford.

Let $x_n = [2\cos(\pi/5)]^n$ and $y_n = [2\cos(3\pi/5)]^n$. It follows from B-373 that $x_{n+2} = x_{n+1} + x_n$, and it follows similarly that $y_{n+2} = y_{n+1} + y_n$. Hence the first result in this problem is established by verifying it for $n = 0$ and $n = 1$ and then using the recursion formulas for F_n, x_n, and y_n. The second result follows from the first using

$$\cos(3\pi/5) = -\cos(2\pi/5) \quad \text{and} \quad \cos(\pi/5) = -\cos(4\pi/5).$$

Also solved by Sahib Singh, Herta T. Freitag, Bob Prielipp, Douglas A. Fults, Paul S. Bruckman, and the proposer.

Fibonacci or Nil

B-375 *Proposed by V. E. Hoggatt, Jr., San Jose State University, San Jose, CA.*

Express $\dfrac{2^{n+1}}{5}\displaystyle\sum_{k=1}^{4}\left[\left(\cos\frac{k\pi}{5}\right)\cdot\sin\frac{k\pi}{5}\cdot\sin\frac{3k\pi}{5}\right]$ in terms of Fibonacci number F_n.

Solution by Herta T. Freitag, Roanoke, VA.

Using the relationships established in B-374, the expression of this problem becomes $F_n[1 + (-1)\ ]/2$, which is F_n for even n and zero for odd n.

Also solved by Paul S. Bruckman, Douglas A. Fults, Bob Prielipp, A. G. Shannon, Sahib Singh, and the proposer.

*****

ADVANCED PROBLEMS AND SOLUTIONS

Edited by
RAYMOND E. WHITNEY
Lock Haven State College, Lock Haven, PA 17745

Send all communications concerning ADVANCED PROBLEMS AND SOLUTIONS *to* Raymond E. Whitney, Mathematics Department, Lock Haven State College, Lock Haven, Pennsylvania 17745. *This department especially welcomes problems believed to be new or extending old results. Proposers should submit solutions or other information that will assist the editor. To facilitate their consideration, solutions should be submitted on separate signed sheets within 2 months after publication of the problems.*

H-295 *Proposed by G. Wulczyn, Bucknell University, Lewisburg, PA.*

Establish the identities

(a) $F_k F_{k+6r+3}^2 - F_{k+8r+4}^2 F_{k+2r+1} = (-1)^{k+1} F_{2r+1}^3 L_{2r+1} L_{k+4r+2}$

and

(b) $F_k F_{k+6r}^2 - F_{k+8r} F_{k+2r}^2 = (-1)^{k+1} F_{2r}^3 L_{2r} L_{k+4r}$.

H-296 *Proposed by C. Kimberling, University of Evansville, Evansville, IN.*

Suppose x and y are positive real numbers. Find the least positive integer n for which

$$\left[\frac{x}{n+y}\right] = \left[\frac{x}{n}\right]$$

where $[z]$ denotes the greatest integer less than or equal to z.

H-297 *Proposed by V. E. Hoggatt, Jr., San Jose State University, San Jose, CA.*

Let $P_0 = P_1 = 1$, $P_n(\lambda) = P_{n-1}(\lambda) - \lambda P_{n-2}(\lambda)$. Show

$$\lim_{n\to\infty} P_{n-1}(\lambda)/P_n(\lambda) = (1 - \sqrt{1 - 4\lambda})/2\lambda = \sum_{n=0}^{\infty} C_{n+1}x^n,$$

where C_n is the nth Catalan number. Note that the coefficients of $P_n(\lambda)$ lie along the rising diagonals of Pascal's triangle with alternating signs.

H-298 *Proposed by L. Kuipers, Mollens, Valais, Switzerland.*

Prove:

(i) $F_{n+1}^6 - 3F_{n+1}^5 F + 5F_{n+1}^3 F_n^3 - 3F_{n+1}F_n^5 - F_n^6 = (-1)^n$, $n = 0, 1, \ldots;$

(ii) $F_{n+6}^6 - 14F_{n+5}^6 - 90F_{n+4}^6 + 350F_{n+3}^6 - 90F_{n+2}^6 - 14F_{n+1}^6 + F_n^6$

$= (-1)^n 80$, $n = 0, 1, \ldots;$

(iii) $F_{n+6}^6 - 13F_{n+5}^6 + 41F_{n+4}^6 - 41F_{n+3}^6 + 13F_{n+2}^6 - F_{n+1}^6$

$\equiv -40 + \frac{1}{2}(1 + (-1)^n)80 \pmod{144}$.

SOLUTIONS

A Soft Matrix

H-274 *Proposed by George Berzsenyi, Lamar University, Beaumont, TX.*

It has been shown [*The Fibonacci Quarterly* 2, No. 3 (1964):261-266] that

$$\text{if } Q = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}, \text{ then } Q^n = \begin{pmatrix} F_{n-1}^2 & F_{n-1}F_n & F_n^2 \\ 2F_{n-1}F_n & F_{n+1} - F_{n-1}F_n & 2F_nF_{n+1} \\ F_n^2 & F_nF_{n+1} & F_{n+1}^2 \end{pmatrix}.$$

Generalize the matrix Q to solutions of the difference equation

$$U_n = rU_{n-1} + sU_{n-2},$$

where r and s are arbitrary real numbers, $U_0 = 0$ and $U_1 = 1$.

Solved by the proposer.

The key to the extension is the identity

$$F_{n+1}^2 - F \quad F = F^2 + F \quad F_{n+1},$$

which allows one to generalize the central entry of Q . It is easily established then by mathematical induction that

$$\text{if } R = \begin{pmatrix} 0 & 0 & s^2 \\ 0 & s & 2rs \\ 1 & r & r^2 \end{pmatrix}, \text{ then } R^n = \begin{pmatrix} s^2U_{n-1}^2 & s^2U_{n-1}U_n & s^2U_n^2 \\ 2sU_{n-1}U & s(U_n^2 + U_{n-1}U_{n+1}) & 2sU_nU_{n+1} \\ U^2 & U_nU_{n+1} & U_{n+1}^2 \end{pmatrix}.$$

A Corrected Oldie

H-225 *Proposed by G. A. R. Guillotte, Quebec, Canada.*

Let p denote an odd prime and $x^p + y^p = z^p$ for positive integers x, y, and z. Show that

A) $p < x/(z - x) + y/(z - y)$

and

B) $z/2(z - x) < p < y/(z - y)$.

Solved by the proposer.

Consider $(x/z)^i + (y/z)^i = 1 + \varepsilon_i$ for $\varepsilon_0 = 1$, $\varepsilon_p = 0$, and $\varepsilon_i \in (0, 1)$, for $1 \leq i \leq p - 1$. Then

$$\sum_{i=0}^{p} (x/z)^i + \sum_{i=0}^{p} (y/z)^i = p + 1 + \sum_{i=0}^{p} \varepsilon_i$$

becomes

$$(1 - (x/z)^{p+1})/(1 - x/z) + (1 = (y/z)^{p+1})/(1 - y/z) = p + 1 + \sum_{i=0}^{p} \varepsilon_i .$$

Now

$$1/(1 - x/z) + 1/(1 - y/z) > p + 1 + \sum_{i=0}^{p} \varepsilon_i .$$

Hence

$$z/(z - x) + z/(z - y) > p + 1 + 1 + \sum_{i=1}^{p-1} \varepsilon_i ,$$

since $\varepsilon_0 = 1$ and $\varepsilon_p = 0$. But

$$z/(z - x) - 1 = x/(z - x) \text{ and } z/(z - y) - 1 = y/(z - y).$$

Therefore

$$x/(z - x) + y/(z - y) > p + \sum_{i=1}^{p-1} \varepsilon_i > p.$$

Similar reasoning leads to part B).

Editorial Note: Please keep working on those oldies!

Special Note: It has long been known that any solution for the basic pair of equations for 103 as a *congruent number* would entail enormous numbers. For that reason, 103 had not been proved congruent: on the other hand, it had not been proved noncongruent.

Then, in 1975, two brilliant computer experts—Dr. Katelin Gallyas and Mr. Michael Buckley—finally proved 103 to be congruent, working along lines suggested by J. A. H. Hunter. The big IBM 370 computer of the University of Toronto was used for this achievement.

For the system

$$X^2 - 103Y^2 = Z^2, \; X^2 + 103Y^2 = W^2,$$

the minimal solution was found to be:

$X =$	134	13066	49380	47228	37470	20010	79697
$Y =$	7	18866	17683	65914	78844	74171	61240
$Z =$	112	55362	67770	44455	63954	40707	12753
$W =$	152	68841	36166	82668	99188	22379	29103

REFERENCE

"Fibonacci Newsletter," September 1975.

*****